TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA KANUNU'NDA BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE KARŞI SUÇLAR

Tezli Yüksek Lisans Tezi

Ayşe Nur LİMAN

Ankara, 2024

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA KANUNU'NDA BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE KARŞI SUÇLAR

Tezli Yüksek Lisans Tezi

Ayşe Nur LİMAN

Tez Danışmanı
Prof. Dr. Devrim GÜNGÖR

Ankara, 2024

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU ANABİLİM DALI

TÜRK CEZA KANUNU'NDA BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE KARŞI SUÇLAR

Yüksek Lisans Tezi

Tez Danışmanı

Prof. Dr. Devrim GÜNGÖR

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı

1- **Prof. Dr. Devrim GÜNGÖR**

2- **Prof. Dr. Muharrem ÖZEN**

3- **Doç. Dr. Önder TOZMAN**

Tez Savunması Tarihi

02.10.2024

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Prof. Dr. Devrim GÜNGÖR danışmanlığında hazırladığım "**Türk Ceza Kanunu'nda Bilişim Sistemine ve Sistemdeki Verilere Karşı Suçlar (Ankara, 2024)**" adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

04.11.2024

Ayşe Nur LİMAN

ÖNSÖZ

Başta tüm eğitim hayatım boyunca bugünlere gelmemin hayalini kuran ve beni her koşulda destekleyen biricik anne ve babam olmak üzere; tez konusunu seçerken isteklerimi göz önünde bulundurup bana yardımcı olan tez danışmanım Prof. Dr. Devrim GÜNGÖR'e; tez çalışmamda ilgi ve desteğini esirgemeyen hocam Dr. Öğr. Üyesi Dilaver NİŞANCI'ya; tez konusunu belirlememde ve kapsamını oluşturmamda yardımcı olan Prof. Dr. Murat Volkan DÜLGER'e ve tezime engin bilgileriyle katkı sunan değerli jüri üyeleri Prof. Dr. Muharrem ÖZEN ve Doç. Dr. Önder TOZMAN'a teşekkürlerimi borç bilirim.

Son olarak, yüksek lisans süresi zarfında beni *"2210 - Yurt İçi Yüksek Lisans Burs Programı"* kapsamında bursiyerliğe layık gören, maddi ve manevi desteklerini esirgemeyen TÜBİTAK'a şükranlarımı sunarım.

İÇİNDEKİLER

İKİNCİ BÖLÜM
BİLİŞİM SİSTEMİNE GİRME VEYA KALMA, SİSTEME GİRMEDEN VERİLERİ TEKNİK ARAÇLARLA İZLEME SUÇU

ÜÇÜNCÜ BÖLÜM
SİSTEMİ ENGELLEME, BOZMA; VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU (TCK m. 244)

KISALTMALAR CETVELİ

ABD : Amerika Birleşik Devletleri

AHBVÜD : Ankara Hacı Bayram Veli Üniversitesi Dergisi

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

b. : Bent

Bkz. veya bkz. : Bakınız

C. : Cilt

CD : Yargıtay Ceza Dairesi

CHD : Ceza Hukuku Dergisi

CGK : Ceza Genel Kurulu

CMK : Ceza Muhakemesi Kanunu

Çev. : Çeviren

Der. : Derleyen

DoS : Denial of Service

DDoS : Distributed Denial of Service

E. : Esas

Ed. : Editör

ENIAC : Elektronik Numerical Integrator and Computer

ETCK : Eski Türk Ceza Kanunu

f. : Fıkra

HSK : Hâkim ve Savcılar Kurulu

HÜHFD : Hacettepe Üniversitesi Hukuk Fakültesi Dergisi

IP : İnternet Protokolü

İÜHFM : İstanbul Üniversitesi Hukuk Fakültesi Mecmuası

K. : Karar

KVKK : Kişisel Verilerin Korunması Kanunu

m. : Madde

MİT : Millî İstihbarat Teşkilâtı

R.G. : Resmî Gazete

s. : Sayfa

S. : Sayı

SÜHFD : Selçuk Üniversitesi Hukuk Fakültesi Dergisi

TAAD : Türkiye Adalet Akademisi Dergisi

TBB : Türkiye Barolar Birliği

T.C. : Türkiye Cumhuriyeti

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

THY : Türk Hava Yolları

TÜİK : Türkiye İstatistik Kurumu

Vol. : Volume

Yay. : Yayıncılık

Y. : Yıl

GİRİŞ

Teknolojideki ilerlemeler toplumdaki pek çok yeniliğin de öncüsü olmuştur. Artık insanlık, alışverişten bankacılık işlemlerine kadar her türlü işini evinden çıkmadan kâğıt kadar ince akıllı cep telefonları ve laptoplar üzerinden yapabilir hale gelmiştir. Ekonomi, sanayi, ulaşım, hizmet ve bankacılık başta olmak üzere çeşitli sektörlerdeki kurum ve kuruluşlar dijital alandaki faaliyetlerini artırmış, dijitalleşme çağına ayak uyduramayan işletmeler piyasadan silinme tehdidiyle karşı karşıya kalmıştır. Özellikle pandemi döneminde, eğitim ve öğretim başta olmak üzere pek çok meslek dalındaki faaliyetler bilgisayarlar üzerinden çevrimiçi olarak yürütülmüştür.

Bundan 60 yıl öncesine kadar bilişim sistemlerinin esamesi okunmazken, bugün bir gücün dünyadaki bütün bilişim sistem ağını kullanılmaz hale getirdiği ihtimalinde dünya nüfusunun hemen hemen hepsinin günlük yaşamı durma noktasına gelecek, önemli bir çoğunluğu maddi ve manevi olarak telafisi mümkün olmayan zarara uğrayacaktır.

Bilişim alanındaki gelişmeler öyle baş döndürücü bir hızla gerçekleşmiştir ki, bundan 20 yıl öncesinde çağın ilerisinde mucizevi bir buluş olarak nitelendirilen masaüstü bilgisayarlar günümüzde artık hantal ve işlevsiz olmakla suçlanarak terk edilmiştir. 21. yüzyılın başlarında web teknolojisinin bilgiye ulaşma doğrultusunda en büyük adımlardan biri olan, kendisinden istenilen bilgileri verebilmek için internetteki verileri depolayıp rapor oluşturan Google arama motoru günümüzde artık sıradanlaşmıştır. Bugün artık kendisine verilen karmaşık girdileri derleyip toparlayarak başarılı çıktılar verebilen, bununla da kalmayıp bu çıktılar için özgün yorumlar ve değerlendirmeler yapabilen, insan seviyesinde metin yazma kabiliyetine sahip yapay zekâlardan bahsedilmektedir. Yakın gelecekte bu yapay zekâların pek çok mesleği icra edebilecek hale geleceği, örneğin avukat ve hâkimin yerine geçip bir uyuşmazlık

hakkında dilekçe yazabileceği, tez ve antitezleri değerlendirip hukuka uygun karar verebileceği düşüncesi, bundan 20 yıl öncesindeki kadar olağanüstü gözükmemektedir[1].

Küresel toplum her alanda bilişim sistemlerinin fonksiyonlarına giderek daha bağımlı hale geldikçe, bu bağımlılığı kötü niyetli amaçlar doğrultusunda kullanmak için sistemlere ve verilere müdahale edebilecek kişilerin oranı da artmaktadır. Bilişim sistemlerini suç işleme aracı olarak kullanan bu kişilerle birlikte ceza hukukunda *"Bilişim Suçları"* adıyla yeni bir suç alanı doğmuştur. Günümüzde bilişim suçu failleri tek bir *'tıklamayla'* milyonlarca dolar parayı kendi hesabına geçirebilmekte, bir devletin istihbarat sırlarına ulaşabilmekte, uçakların uçuşunu engelleyebilmekte[2], bir devletin haberleşme ve bankacılık sistemi çökertilebilmektedir[3].

Bilişim sistemine ve verilere karşı müdahalelerin sosyal yaşama ve kamu düzenine karşı büyük bir tehdit olmasının en önemli sebeplerinden biri, toplumun günlük yaşamının her alanında bilişim sistemlerinin gücünden faydalanmasıdır. Günümüzde toplum başta olmak üzere devletin her türlü kurum ve kuruluşu bilişim

---

[1] Kaldı ki bugün dahi bu hususa ilişkin örnekler görülmeye başlanmıştır. Örneğin İngiltere meydana gelen bir olayda bir üniversite öğrencisi, kendisine gelen hatalı park sebebiyle yazılmış idari para cezasına itiraz etmek için ChatGPT denen yapay zekâ sistemiyle bir dilekçe örneği yazarak belediyeye başvurmuş ve belediye bu dilekçeye binaen idari para cezasını kaldırmıştır. Ayrıntılı bilgi için bkz. https://www.bbc.com/news/uk-england-york-north-yorkshire-65126772 (E.T. 16.04.2023)

[2] Amerikan havacılık şirketi RavnAir, 22.12.2019 tarihinde gerçekleşen siber saldırılar neticesinde bilişim sistemlerinin devre dışı kaldığını ve bu sebeple o günkü pek çok uçuşu iptal etmek zorunda kaldıklarını açıklamıştır. Ayrıntılı haber için bkz. https://www.usatoday.com/story/travel/news/2019/12/22/alaska-airline-cancels-flights-after-malicious-cyber-attack/2727709001/ (E.T. 16.04.2023)

[3] 2007'de Estonya'ya karşı gerçekleştirilen siber saldırılar sonucunda ülkenin altı büyük haberleşme kuruluşunun üçü ve en büyük iki banka sunucusu yanıt veremez hale gelmiştir. Ayrıntılı haber için bkz. https://www.haberturk.com/dunya/haber/23642-ilk-siber-savas (E.T. 16.04.2023)

sistemlerine dayalı faaliyet gösterdiği için bilişim sistemleri üzerinde işlenen suçlar ulusal ve küresel boyutta büyük hasarlara yol açma potansiyeline sahiptirler.

Bilişim sistemlerinin haberleşmeden havayolları sistemlerine, eğitimden bankacılık işlemlerine kadar pek çok alanda hayatımızın vazgeçilmez bir parçası olması, bu sistemlerin güvenliğine ve işleyişine yönelik farklı suçların oluşmasının yanı sıra ceza kanunlarında yer alan bazı suçların da işlenme şekline bir yenisini katmıştır. Örneğin bilişim sistemlerinden önce var olan dolandırıcılık, müstehcenlik, hırsızlık gibi suçlar bilişim sistemleriyle birlikte yeni bir işleniş biçimi kazanmıştır. Buna yabancı öğretide *"yeni şişede eski şarap (old wine in new bottle)"* benzetmesi yapılmaktadır[4].

Her ne kadar geleneksel birtakım suçların bilişim sistemleri aracılığıyla işlenmesi de *"bilişim suçları"* kapsamında ele alınmaktaysa da, bu tip suçlar bilişim sistemlerine ve verilere karşı işlenen suçlardan olmayıp bilişim sistemleri aracılığıyla işlenebilen suçlardır.

Anlatılanların ışığında, belirtmek gerekir ki çalışmada yalnızca bilişim sistemlerinin icadıyla birlikte ortaya çıkan, bu sistemleri veya sistemin içindeki verileri hedef alan ve TCK'da düzenleme alanı bulmuş suçlar incelenecektir.

---

[4] *"Around the turn of the last century, researchers began to discuss the ways that cybercrime differed from traditional crime (Grabosky, 2001; Wall, 1998). These initial debates were largely informed by both the novel nature of the Internet at that time and the increasingly ubiquitous presence of technology in daily life. David Wall (1998) argued that some forms of cybercrime have direct analogues to real world crimes like fraud. In these cases, cybercrimes may be considered '**old wine in new bottles**,' meaning that the offense is consistent but the medium in which offenders operate is new."* **HOLT**, Thomas J. – **BOSSLER**, Adam M., Cybercrime in Progress: Theory and prevention of technology-enabled offenses, Routledge, New York 2016, s. 65, 66.

BİRİNCİ BÖLÜM

GENEL BİLGİLER

I. BİLİŞİM, BİLİŞİM SİSTEMİ, BİLGİSAYAR, BİLİŞİM SUÇU VE VERİ KAVRAMLARI

A. BİLİŞİM KAVRAMI

Bilişim sistemlerine ve verilere karşı suçların maddi konusunu ve özünü oluşturan bilişim sistemleri ve verilerin anlaşılabilmesi için bilişim sözcüğünün tanımını yapmak elzemdir. Bilişim, Fransızca'daki *"informatique"* İngilizce'deki *"information"* kelimelerinin Türkçe karşılığına tekabül etmektedir[5]. Informatique kelimesinin etimolojisi incelenecek olursa, kavram Fransızca *"information"* (bilgi) ve *"automatique"* (otomatik) kelimelerinin bir bütün haline getirilmesiyle oluşmuştur[6].

Yargıtay 12. CD., bilişim ifadesini TDK çevrimiçi sözlüğüyle paralel olarak *"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve*

[5] **DÜLGER**, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, B. 10, Seçkin Yay., Ankara 2023, s. 73, 74.; **ÖZBEK**, Veli Özer – **DOĞAN**, Koray – **BACAKSIZ**, Pınar, Türk Ceza Hukuku Özel Hükümler, B. 17, Seçkin Yay., Ankara 2022, s. 983.; **TURAN**, Metin, Bilişim Hukuku, B. 7, Seçkin Yay., Ankara 2023, s. 47.; **ERDOĞAN**, Yavuz, Türk Ceza Kanunu'nda Bilişim Suçları, Legal Yay., İstanbul 2012, s. 5.; **KETİZMEN**, Muammer, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yay., Ankara 2008, s. 9.; **KURT**, Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yay., Ankara 2005, s. 24. **APAYDIN**, Cengiz, Bilişim Suçları ve Bilişim Ceza Hukuku, Acar Matbaacılık, İstanbul 2017, s. 283.; **YENİDÜNYA**, Caner – **DEĞİRMENCİ**, Olgun, Mukayeseli Hukukta Ve Türk Hukukunda Bilişim Suçları, Legal Yay., İstanbul 2003, s. 27.

[6] TURAN, s. 44.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 5.

bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi"[7] şeklinde tanımlamıştır.

Bilişim kelimesini Türkiye'de ilk kez 1971 yılında Prof. Dr. Aydın Köksal kullanmıştır[8]. Bu tarihten önce, Fransızca terimden türetilen enformasyon sözcüğü kullanılmaktaydı[9]. Köksal, bilişim kavramını nasıl türettiğini ve bu kavramın ne ifade ettiğini şu şekilde açıklamıştır: *"Bil eylem kökünden bilişmek eylemini, oradan da ad olarak bilişim sözcüğünü türettim, bilginin akışkan durumunu anlatmak için"*[10].

Bilişim kavramı Türk hukukunda ise, ilk defa ortaya çıktığı tarihten 18 yıl sonra, 1989 tarihli TCK ön tasarısında kullanılmış ve 342. maddesinin gerekçesinde bilişim alanının tanımı *"bilgileri depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan"* şeklinde yapılmıştır[11].

Bilişim en geniş tanımıyla her çeşit bilginin bilgisayar başta olmak üzere elektronik araçlar aracılığıyla verimli ve düzenli biçimde düzenlenmesi, analiz edilmesi, değerlendirilmesi, depolanması, aktarılması[12] ve yorumlanması gibi çeşitli fonksiyonel işlemleri inceleyen uygulamalı bilim dalıdır.

---

[7] E. 2015/10388, K. 2017/1556, 1.3.2017 tarihli kararı. https://karararama.yargitay.gov.tr/ (E.T. 29.03.2023)

[8] https://www.nisanyansozluk.com/kelime/bilişim (E.T. 13.04.2023)

[9] DÜLGER, s. 74.

[10] https://www.hurriyet.com.tr/yerel-haberler/ankara/turk-aydinindan-once-uzaylilar-bilgisayar-sozcugunu-kullandi-5338222 (E.T. 13.04.2023)

[11] Türk Ceza Kanunu Öntasarısı, İkinci Komisyon Tarafından Yapılan Değerlendirme Sonucunda Hazırlanan Metin, Ankara, Mart 1989.

[12] **APAYDIN**, Cengiz, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, Seçin Yay., Ankara 2023, s. 46, 47.; TURAN, s. 47.

Bilişim çağında çok kısa zaman içinde yeni teknolojilerin üretildiği, elektronik araçlar vasıtasıyla bilginin üzerinde gerçekleşen fonksiyonların çeşitlenebildiği göz önünde bulundurulduğunda bilişim kavramının tanımının zamanla değişebileceği ve dönüşebileceği unutulmamalıdır. Zira bilişim kavramının kapsam ve tanımına *"bilginin yorumlanması"* faaliyetinin girmesi son birkaç yıl içinde, bilgileri insan seviyesinde ve özgün bir içerikle yorumlayabilen yapay zekânın insanlığın hizmetine sunulması sayesinde gerçekleşmiştir.

B. BİLİŞİM SİSTEMİ KAVRAMI

1. Bilişim Sisteminin Tanımı ve Türk Hukukundaki Tarihçesi

Bilişim kavramının tanımı yukarıda yapılmıştı. Sistem ise, TDK çevrimiçi sözlüğünde *"bir sonuç elde etmeye yarayan yöntemler düzeni"* şeklinde tanımlanmıştır.

Bilişim sistemi ise bilgi teknolojilerinin kullanıldığı ve bilgi işleme faaliyetlerinin gerçekleştirildiği, bilgisayarlar, veri tabanları, yazılım, ağ altyapıları ve diğer teknolojik bileşenleri içeren yöntemler düzeni olarak tanımlanabilir. Bilişim sistemleri esasında, kaynak paylaşımlarını gerçekleştirmek için bilgisayarları birbirine bağlayan ağlar ve bu ağlardan faydalanan kullanıcıları kapsar[13].

[13] **ÖZKUL**, Davut, *"Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi"*, Sayıştay Dergisi, Ocak-Şubat 2002, C. 13, S. 44-45, s. 14.

Bilişim sistemi kavramının Türk hukukunda kullanılması ilk defa 2003 tarihli TCK tasarısıyla gerçekleşmiştir[14]. Bu tasarının 346. maddesinin gerekçesinde bilişim sistemleri *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemler"* olarak tanımlanmıştır. Bahsedilen tanım, 5237 sayılı TCK'nın "Bilişim alanında suçlar" başlığı altındaki 243. maddesinin gerekçesinde de tekrarlanmıştır[15].

2003 tarihli TCK tasarısından önce, 1991'de yürürlüğe giren ve 3756 sayılı *"765 sayılı Türk Ceza Kanunu'nun Bazı Maddelerini Değiştiren Kanun"*un 20 ve 24. maddeleri arasında *"Bilişim Alanında Suçlar"* ilk defa düzenlenmiş, ancak burada bilişim sistemi değil, *"bilgileri otomatik olarak işleme tabi tutmuş bir sistem"* ifadesi tercih edilmiştir[16].

*"Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkında Yönetmelik"*in[17] 3. maddesinde bilişim sisteminin tanımı *"bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem"* şeklinde yapılmıştır.

[14] 12.05.2003 tarihli Türk Ceza Kanunu Tasarısı için bkz. https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c059/tbmm22059119ss0664.pdf (14.04.2023)

[15] KURT, s. 26.

[16] **KARAGÖZ,** Mehmet Can, Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, On İki Levha Yay., İstanbul 2020, s. 9.

[17] R.G. 20.09.2011 T., 28060 S.

2. Bilişim Sisteminin Özellikleri

a. Bilgileri Otomatik İşleme Tabi Tutma

Bilişim sistemlerinin ön plana çıkan en temel özelliği, bilgileri otomatik işleme tabi tutabilmesidir.

Bilgilerin otomatik işlenmesi, bilgileri insan müdahalesi veya çabası olmaksızın işleyebilme ve veri haline getirebilme becerisi olarak tanımlanabilir[18]. Buna göre bilişim sistemleri, verilen görevleri kendi kendine tamamlayabilir ve başarılı sonuçlar üretebilir.

b. Manyetik Sistem Olma

5237 sayılı TCK'nın 243. maddesinin gerekçesinde, bilişim sistemleri tanımlanırken manyetik bir sistem olması gerektiğinden bahsedilmiştir. Manyetik sistemlerin tanımı ise yapılmamıştır.

Manyetik sistemler, veri toplama ve bu verileri işleme faaliyetini manyetik kartlar veya manyetik şeritler aracılığıyla gerçekleştiren sistemlerdir. Bu sistemler veri toplama ve işleme süreçlerini otomatik ve güvenilir hale getirmektedirler.

---

[18] **KİŞİSEL VERİLERİ KORUMA KURUMU**, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar Kitapçığı, s. 18. İnternet Erişim: https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar (E.T. 14.04.2023)

c. Belirli Bir Amaca Özgülenmeme

Her elektronik cihaz bilişim sistemi sayılmaz[19]. Belli bir işlemin yapılmasına özgülenmiş olan ve genel amaçlı işlem yapabilme özelliğine sahip olmayan aletler bilişim sistemine dahil değildir[20]. Bu çerçevede örneğin çamaşır makinesi, bulaşık makinesi, ev telefonları, hesap makinaları, yiyecek-içecek otomatları gibi yalnızca belirli bir amaca yönelik faaliyet gösteren elektronik aletler bilişim sistemi olarak adlandırılamazlar[21].

d. Bilgisayar Sistemlerine Temellenerek İşlem Gerçekleştirme

Bilişim sistemlerinin bir diğer özelliği de bilgisayar sistemleri olmadan vazifelerini yerine getiremiyor olması, yani bilgisayar sistemlerine temellenerek faaliyet göstermesidir.

CGK da bir kararında bilgisayar sistemlerine temellenerek faaliyet gerçekleştiren aygıtların bilişim sistemi olduğu ve yapılan faaliyetlerin de bilişim

[19] **TAŞKIN**, Şaban Cankat, Bilişim Suçları, Beta Yay., Bursa 2008, s. 9.

[20] KURT, s. 141.

[21] **KARAKEHYA,** Hakan, *"Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu",* TBB Dergisi, S. 81, 2009, s. 194.; **BAYRAKTAR**, Köksal – **EVİK**, Vesile Sonay – **KANGAL**, Zeynel Temel – **YILDIZ**, Ali Kemal – **EVİK**, Ali Hakan – **AKSOY RETORNAZ**, Eylem – **MEMİŞ KARTAL**, Pınar – **BOSTANCI BOZBAYINDIR**, Gülşah – **EROĞLU**, Fulya – **AYTEKİN İNCEOĞLU**, Asuman, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar – Bilişim Alanında Suçlar, On İki Levha Yay., İstanbul 2021, s. 236.

faaliyeti olduğunu belirtmiştir[22]. CGK, bankanın ATM sistemlerinin bağlı olduğu bilgisayar sistemleri çöktüğünde, ATM'lerin de çalışamaz hale geleceğinden, ATM'lerin bilişim sistemi olduğunu ifade etmiştir[23]. Kararda bilgisayar sisteminin yardımcı bir unsur olarak kullanıldığı faaliyetlerin bilişim faaliyeti olmadığı, dolayısıyla bu faaliyeti gerçekleştiren aygıtların da bilişim sistemi olmadığına dikkat çekilmiştir. Yargıtay, aynı kararda havayolu firmalarının bilgisayar sistemlerinden bilet satışı için yararlanmalarının bilişim faaliyeti olarak düşünülemeyeceğini belirtmiştir[24].

C. BİLGİSAYAR KAVRAMI

Bilgisayar, bilginin işlenmesinde kullanılan en yaygın araç olması sebebiyle bilişim sistemleri denince akla ilk gelen cihazdır. TDK, bilgisayarı; *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"* olarak tanımlanmıştır[25].

Bilgisayar en genel tanımıyla, verilen komutlar dahilinde bilgiyi belirli bir düzen çerçevesinde işleme, bunlara dayalı sonuçlar üretme, bilgileri başka bir yere iletme ve başka yerdeki bilgilere ulaşma yetkisine sahip elektronik makinelerdir[26].

---

[22] CGK, E. 2006/136, K. 2007/150, T. 19.06.2007. https://karararama.yargitay.gov.tr/ (E.T. 29.12.2023)

[23] Benzer yönde: 8 CD., E. 2016/3214, K. 2016/10758, T. 24.11.2016. https://karararama.yargitay.gov.tr/ (E.T. 29.12.2023)

[24] Sebebini ise "*Çünkü bu sistemler bu firmaların faaliyetini kolaylaştırmakla hızlandırmakla ve daha verimli kılmakla birlikte faaliyetin tarif edici unsuru değildir.*" şeklinde açıklamıştır.

[25] https://sozluk.gov.tr/ (E.T. 04.01.2024)

[26] **ÇAKIR**, Hüseyin (Ed.) – **KILIÇ**, Mehmet Serkan (Ed.), Adli Bilişim ve Elektronik Deliller, Seçkin Yay., Ankara 2014, s. 25.

İlk bilgisayar, 1946 yılında Amerikan ordusunun uzun menzilli top ve füzelerinin kullanılması için oluşturulmuştur[27]. Adı ENIAC[28] olan bu bilgisayar, veri işleme özelliğini haiz, 30 ton ağırlığında devasa bir aygıttı[29]. Bilgisayarın icat edildiği Amerika'da bu makineye İngilizce *"to compute"* (hesaplamak) sözcüğünden türemiş olan *"computer"* adı verilmiştir[30].

Öğretide, bilgisayarın *"elektronik olma"* özelliğinin zaruri bir unsur olduğunu düşünenler olduğu gibi[31]; optik, manyetik ve başka tekniklerle çalışan bilgisayarlar da olduğu, tanımdaki *"elektronik olma"* unsuru bilgisayarın kapsamını daralttığı gerekçesiyle eleştirenler de bulunmaktadır[32].

Bilgisayar, "donanım (hardware)" ve "yazılım (software)" olarak iki farklı temel unsurdan oluşmaktadır. Buna göre "donanım" bir bilgisayarın gözle görülebilen fiziki bileşenlerine (klavye, ekran, sabit disk, monitör vb.); "yazılım" ise bilgisayarın işlem yapmasını sağlayan programların bütününe verilen isimdir[33].

---

[27] **İKİNCİ**, Özlem, *"30 Tonluk Hayal Artık Cepte: Bilgisayar"*, TÜBİTAK Bilim ve Teknik Dergisi, S. 508, 2010, s. 22.; DÜLGER, s. 94.; https://www.ntv.com.tr/turkiye/ilk-bilgisayar-65-yasinda (E.T. 04.01.2024)

[28] ENIAC, İngilizce *"Electronic Numerical Integrator and Computer (Elektronik sayısal entegrelenmiş bilgisayar)"* kelimelerinin baş harflerinin kısaltmasından oluşmaktadır.

[29] İKİNCİ, s. 22.

[30] DÜLGER, s. 62.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 18.; KETİZMEN, s. 14.

[31] Bkz. KURT, s. 28.; **BOZDOĞAN AKBULUT**, Berrin, *"Bilişim Suçları"*, SÜHFD, C. 8, S. 1-2, 2000, s. 545.

[32] Bkz. **YAZICIOĞLU**, Yılmaz, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, Alfa Yay., İstanbul 1997, s. 133.

[33] DÜLGER, s. 66.

Bilişim sistemi, bilgisayarı da kapsayan çatı bir terimdir[34]. Yargıtay CGK da 2007/136 E., 2007/150 K. ve 19.06.2007 T. ilamında *"Bilişim sisteminde veri iletişimi, bilgisayarla birlikte, elektronik, manyetik veya bazı mekanik araçlarla bir ağ üzerinden sağlanabilir."* şeklindeki ifadesiyle bilişim sistemi kavramının bilgisayara nazaran daha üst bir kavram olduğu sonucuna varmıştır.

D. VERİ KAVRAMI

Veri kavramı, bilişim sistemlerinin özünü oluşturmaktadır. En genel tanımıyla veri, bilgilerin belirlenmiş bir formata dönüştürülmüş halidir[35]. Bilgisayarlar veya diğer bilişim sistemleri tarafından depolanabilen, işlem yapılıp sonuca ulaşılabilen, işlenebilen, iletilebilen ve saklanabilen her türlü kavram veya bilgi veri olabilir[36]. Tanımdan da anlaşılacağı üzere bilgi ve veri kavramları eşdeğer anlamda değillerdir. Veri, bilişim faaliyeti sonucunda işlenmiş olan bilgiyi ifade etmektedir[37].

---

[34] DÜLGER, s. 74.

[35] BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 221.; **AKARSLAN**, Hüseyin, Bilişim Suçları, B. 2, Seçkin Yay., Ankara 2015, s. 30, 31.; **TEZCAN**, Durmuş – **ERDEM**, Mustafa Ruhan – **ÖNOK**, Rıfat Murat, Ceza Özel Hukuku, B. 20, Seçkin Yay., Ankara 2022, s. 1167.; YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 29.; DÜLGER, s. 83.; KURT, s. 37.

[36] **DEĞİRMENCİ**, Olgun, *"2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi"*, TBB Dergisi, S. 58, 2005, s. 200.; YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 29.; DÜLGER, s. 83.

[37] ÇAKIR – KILIÇ, Adli Bilişim ve Elektronik Deliller, s. 25.; ÖZKUL, s. 13.; KURT, s. 38.

Taraf olduğumuz uluslararası sözleşme niteliğindeki AKSSS'nin 1/b. maddesinde veri, *"bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlarda dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgi"* olarak tanımlanmıştır.

Ulusal düzenlemelere bakıldığında, veri teriminin tanımı kanun koyucu tarafından *"5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*un[38] 2. maddesinin 1. fıkrasında yapılmıştır. Buna göre veri *"bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer"* olarak ifade edilmiştir.

Öte yandan, kanuni düzenlemeyle verinin kapsamının çizilmesi ise 5237 Sayılı TCK ile olmuştur. Buna göre TCK'nın 243. maddesinin gerekçesinde *"sistem içindeki bütün soyut unsurlar, fıkrada geçen veri teriminin kapsamındadır."* denilerek veri kavramının kapsamı belirlenmiştir. Bilgisayar programlarının da sistem içerisinde soyut bir unsur olması ve veriler bütününden oluşması neticesinde, bu programların da veri kavramının kapsamında olduğu kabul edilmelidir[39].

E. BİLİŞİM SUÇU KAVRAMI

Bilişim sistemlerinin yaygınlaşmasıyla birlikte bu sistemlerin kötüye kullanılması söz konusu olmuş, buna yönelik gerçekleştirilen birtakım antisosyal fiiller ülkelerin ceza kanunlarında suç olarak düzenlenmiş ve bu suçlar için de çeşitli terimler

[38] R.G. 23.05.2007 T., 26530 S.

[39] BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 237.; DEĞİRMENCİ, s. 200.

kullanılmıştır. Bu terimlerden bazıları siber suç, internet suçu, bilgisayar suçu, çevrimiçi suçlar şeklinde sıralanabilir.

Dünya'da kayıtlara geçmiş haliyle ilk bilişim suçu 1958 senesinde Amerika'da işlenmiştir[40]. Hal böyle olunca, yeni ortaya çıkan bu "suç tipine" bir ad verilmesi de Amerika'da olmuştur[41]. Amerika'da, bu suçlar için üst başlık olarak *computer crime* (bilgisayar suçları) ve *cybercrime* (siber suçlar) kavramları kullanılmaktadır.

Alman Hukukunda ise *bilgisayar suçları* ifadesinin Almanca karşılığı olan *Computerkriminialität* kavramı tercih edilmektedir[42].

İtalyan Hukukunda gerek öğretide gerekse İtalyan Ceza Kanunu'nda *"la criminalita informatica"* (bilişim suçluluğu) terimi kabul görmektedir[43].

Türk hukukunda genel olarak *bilişim suçları* ifadesinin gerek öğretide gerek Yargıtay kararlarında yerleşik bir hal aldığını görmek mümkündür. Öte yandan Kanunumuzda da bilişim suçları ifadesiyle benzer şekilde *"Bilişim Alanında Suçlar"* terimi tercih edilmiştir.

Bilişim suçları kavramı, 765 sayılı ETCK zamanında gerçekleşen 1991 tarihli düzenlemeyle[44] ceza mevzuatımıza girmiştir. Bu düzenlemeyle, Türk Ceza Kanunu'na ilk kez *"Bilişim Alanında Suçlar"* başlığı eklenmiştir.

---

[40] **ORTA**, Mesut, Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim), Yetkin Yay., Ankara 2015, s. 79.

[41] ORTA, s. 79.

[42] **ERDAĞ**, Ali İhsan, *"Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)"*, GÜHFD, C. 14, S. 2, 2010, s. 287.

[43] **PICOTTI**, Lorenzo, *"Diritto Penale, technologie informatiche ed intelligenza artificiale: una visione d'insieme"*, Cybercrime içinde (Ed. Alberto Cadoppi – Stefano Canestrari –Adelmo Manna – Michele Papa), B. 2, Wolters Kluver Italia, 2023, s. 46.; YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 128.

Öğretide, bu tür suçlar için *'bilişim suçları'* ifadesinden sonra en sık kullanılan başlıklar *'bilgisayar suçları'*, *'siber suçlar'* ve *'internet suçları'* şeklindedir.

Bilgisayar suçları, bu suçların yalnızca bilgisayar üzerinden işlenebileceğini, sözgelimi akıllı cep telefonları üzeri veya diğer bilişim sistemleri üzerinden işlenen suçları kapsamadığı için eksiktir. Öte yandan, internet suçları ifadesi ise, bu suçların intranet ve ekstranet üzerinden de işlenebileceği göz ardı edildiği için kabul görmemiştir[45]. Siber suç, yani Türkçesi *"sanal suç"* kavramı ise öğretide, işlenen suçların sanal değil gerçek olduğu, bu suçların sanal alemde işlenmesinin fiziki gerçeklikten yoksun olduğu anlamına gelmeyeceği gerekçesiyle eleştirilmiştir[46].

Terim zenginliğinin uygulamaya da yansıdığı görülmektedir. Örneğin bu suçlarla etkin mücadele kapsamında EGM bünyesinde *"Siber Suçlarla Mücadele Daire Başkanlığı"* adıyla bir birim kurulmuşken; Ankara ve İstanbul başta olmak üzere pek çok şehrin Cumhuriyet Başsavcılığı'na bağlı olarak *"Bilişim Suçları Soruşturma Bürosu"* açılmıştır.

Bilişim suçları teriminin genel geçer bir tanımı olmamakla beraber, bu kalıbın esasen çok çeşitli suçları kapsayan bir şemsiye işlevi gördüğü söylenebilir.

Bir görüşe göre bilişim suçları, bir bilgisayar ya da ağına yönelik veya bu araçları kullanarak gerçekleştirilen yasadışı eylemlerdir[47]. Bu görüş, bilişim sistemlerini bilgisayar ve ağlarına indirgediği için eksiktir. Gerçekten bu tanıma göre, sözgelimi

---

[44] 3756 sayılı *"765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun*", R.G., T. 14.06.1991, S. 20901.

[45] **ÜNVER**, Yener, *"Türk Ceza Kanunu'nun ve Ceza Kanunu (2000) Tasarısının İnternet Açısından Değerlendirilmesi"*, İÜHFM İnternet Özel Bölümü, C. LIX, S. 1-2, 2001, s. 78, 79.; TAŞKIN, Bilişim Suçları, s. 11.; DÜLGER, s. 79.

[46] ÜNVER, s. 79, 80.

[47] **ÖZSOY**, Nevzat, *"Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK. 243 ve 244)"*, Yaşar Hukuk Dergisi, C. 1, S. 2, 2019, s. 296.

akıllı telefonlarla işlenen bilişim sistemine girme eylemi bilişim suçu sayılmayacaktır. Oysaki Yargıtay, akıllı telefonların da bilişim sistemi kapsamında yer aldığını açıkça ifade etmiştir[48].

Diğer bir görüşe göre bilişim suçu, verilerle yahut veri işlemle konu bağlantılı, bilişim sistemleri aracılığıyla işlenen ve/veya bilişim sistemlerine karşı işlenen suçlar olarak tanımlanabilir[49]. Benim fikrim, bu görüşün daha kapsayıcı olduğudur.

Bilişim suçları, temelde iki ayrı suç kümesini içerir. İlki, bilişim sistemlerinin icat edilmesiyle ortaya çıkan ve bilişim sistemleri olmadan işlenmesi mümkün olmayan suçlardır. Bu suçlara örnek olarak "Bilişim sistemlerine girme veya sistemde kalma (TCK m. 243)" ve "Bilişim sistemine veya sistem içindeki verilere müdahale etme (TCK m. 244)" verilebilir.

İkinci tip suçlar, bilişim sistemlerinden önce var olan ancak bilişim sistemlerinin icat edilmesiyle birlikte bu sistemler aracılığıyla da işlenebilen, hatta çoğu zaman bilişim sistemleri aracılığıyla işlenmesi daha kolay olan geleneksel suçlardır.

Yabancı öğretide bu ikili ayrım *cyber-enabled crimes* (siber etkin suçlar) ve *cyber-dependent crimes* (siber bağımlı suçlar) başlıklarıyla ifade edilmektedir[50]. Türk öğretisinde ise çoğunlukla doğrudan bilişim suçları-dolaylı bilişim suçları başlıkları tercih edilmektedir[51]. Bunun yanı sıra kimi yazarlar gerçek bilişim suçları-bilişim bağlantılı suçlar başlıklarını[52] tercih etmektedir.

---

[48] 8. CD., T. 18.3.2015, E. 2014/30037, K. 2015/2015. (DÜLGER, s. 76.)

[49] BOZDOĞAN AKBULUT, *"Bilişim Suçları"*, s. 551.

[50] **SELZER**, Nicole – **OELRICH**, Sebastian, *"Saint or Satan? Moral Development and Dark Triad Infuences on Cybercriminal Intent"*, Cybercrime in Context The human factor in victimization, offending, and policing içinde (Ed. Marleen Weulen Kranenbarg - Rutger Leukfeldt), Springer Nature, Switzerland 2021, s. 176.

[51] **GÜL,** Ahmet, Doğrudan – Dolaylı Bilişim Suçları, B. 3, Seçkin Yay., Ankara 2021, s. 33 vd.; ÖZSOY, s. 295.; AKARSLAN, s. 162.

[52] KAYAER, s. 84, 85.

II. BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE KARŞI SUÇLARIN İŞLENME BİÇİMLERİ (MODUS OPERANDİ)

A. BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE MÜDAHALE HAKKINDA GENEL BİLGİLER VE MODUS OPERANDİ KAVRAMI

Bilişim sistemine ve verilere müdahale ifadesi, İngilizce dilindeki *"hacking"*, bilişim sistemlerine veya bilişim sistemlerinin içindeki verilere karşı gerçekleştirilen yasadışı eylemleri tanımlamaktadır. Ancak buradaki müdahale eyleminin sistemin içindeki soyut unsurlara, yani yazılıma yönelik olduğu belirtilmelidir. Sistemin fiziki bileşenlerini oluşturan donanım kısmına, örneğin bilgisayarın monitörüne zarar vermek, bilişim sistemlerine ve verilere müdahale olarak kabul edilmeyecektir.

Bilişim sistemine ve verilere müdahale etme, günlük hayatta sıklıkla kullanılan diğer adıyla hackleme eyleminin temel özellikleri basitlik, ustalık ve yasadışı olmasıdır[53]. Buna göre hack eylemi basit fakat etkileyici özellik göstermeli, karmaşık teknik bilgi içermeli ve kanunlara aykırı olmalıdır. Bilişim sistemlerine ve verilere karşı suçların ortaya çıktığı tarihten bugüne kadar, bu eylemin gerçekleştirilebilmesi için pek çok teknik kullanılmış, bu teknikler bir dizi *modus operandi* oluşturmuştur. Modus operandi kavramı, Latincedir. Bir suçu başarıyla işleyebilmek için gerçekleştirilen davranışlarla alakalı olan terim, suç işleme metotları olarak ifade edilebilir[54]. Bu

[53] **TAYLOR**, Paul A., Hackers: Crime in the Digital Sublime, Routledge, London 1999, s. 16.

[54] **KARAGÜLMEZ,** Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, B. 5, Seçkin Yay., Ankara 2014, s. 64.

kavramla bir suçun meydana getirilebilmesi için kullanılan araçlar, yöntem ve davranışlar bütünü kastedilir[55]. Yani esasen kavram, suçun maddi unsuru olan fiille yakından ilişkilidir.

Bu başlık altında ise bilişim sistemine ve verilere karşı suçların *modus operandilerine*, yani çeşitli işlenme şekillerine yer verilmiştir. Ancak belirtmek gerekir ki bu metotların aşağıda sayılanlardan ibaret olduğunu söylemek, teknolojinin her gün yeni bir boyut kazanması gerçeği karşısında sahici olmayacaktır. Zira bu yeni boyutlar, bilişim sistemine ve verilere karşı suçlarda her gün yeni *modus operandilerin* ortaya çıkmasına yol açmaktadır[56]. Dahası bu sınırlama, bilişim suçlarıyla mücadelede daha en başından geride kalmak demektir[57]. Özetle, aşağıda sayılan teknikler dışında pek çok teknik bulunmaktadır. Bu çalışmada yalnızca bilişim sistemlerine ve verilere müdahalede sıkça kullanıldığı tespit edilen tekniklere değinilmiştir.

[55] KARAGÜLMEZ, s. 64.

[56] **ÖZEN**, Muharrem – **BAŞTÜRK**, İhsan, Temel Hak ve Özgürlükler Bağlamında Bilişim - İnternet ve Ceza Hukuku, Adalet Yay., Ankara 2011, s. 91.

[57] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 151.

B. BİLİŞİM SİSTEMİNE VE VERİLERE MÜDAHALE ÇEŞİTLERİ (MODUS OPERANDİ)

1. Bilişim Sistemine ve Verilere Yasadışı Erişmek İçin Kullanılan Teknikler

a. Phishing (Oltalama)

Phishing terimi, ilk defa 1966'da Usenet adlı haber sunucusunda bir grup bilgisayar korsanının Amerikan bir şirketin web sitesindeki kullanıcılarının bilgilerini çalması üzerine kullanılmıştır[58].

İngilizce'de "password" (şifre) "harvesting" (hasat) "fishing" (balık avlamak) kelimelerinin kombinasyonuyla oluşturulan phishing, saldırganların en çok başvurduğu saldırı türlerinden biridir[59]. Bu yöntemde, sosyal mühendislik ve teknik yanıltmacalar kullanılarak internet kullanıcıların bankacılık hesapları başta olmak üzere kişisel verilerine ulaşmak amaçlanır[60].

Bu yöntem, binlerce kullanıcıya e-posta veya SMS olarak gönderilen bir metinde onları sahte bir web sayfasına girmeye teşvik eden bir kurgu oluşturulur. Bu teşvik, çoğu zaman kullanıcının bir ödül kazandığını duyurarak bunu teslim alabilmesi için sahte bir bankacılık sistemin linkini göndermek şeklinde olmaktadır. Kullanıcı, bu fırsatı kaçırmamak adına gerçeğinden farksız url uzantısına sahip olan sahte linke

---

[58] **ORUNSOLU**, A. A. – **SODIYA**, A. S. – **AKINWALE**, A. T., *"A predictive model for phishing detection",* Journal of King Saud University – Computer and Information Sciences, Vol. 34, 2022, s. 233.

[59] DÜLGER, s. 123.

[60] MARION – TWEDE, s. 316.

tıklayıp ekrandaki alana T.C kimlik numarası veya banka müşteri numarasıyla şifresini girer. Saldırgan, elde ettiği bu bilgilerle mağdurun mobil bankacılık yahut resmi kuruluş sitesindeki hesabını ele geçirerek kullanıcının verilerini yahut parasını ele geçirir[61].

Europol (Avrupa Polis Teşkilatı), 27 Mart 2023 tarihinde ChatGPT yapay zekâ programının kolluk kuvvetleri üzerindeki etkisiyle alakalı yayınladığı raporda, ChatGPT'nin yaygınlaşmasının phishing ve sosyal mühendislik saldırılarının artmasına sebep olabileceğine yönelik endişelerini dile getirmiştir[62].

b. Sosyal Mühendislik

Sosyal mühendislik, türlü hilelerle insanların güvenlerini kazanarak ve onların zaaflarını kullanarak bilişim sistemine ve verilere erişmeyi amaçlayan bir siber saldırı

---

[61] **SEMİZ**, Murat, Bilişim Suçları ve Soruşturma Yöntemleri, B. 3, Adalet Yay., Ankara 2022, s. 39.; **ÇAKIR**, Hüseyin (Ed.) – **KILIÇ**, Mehmet Serkan (Ed.), Güncel Tehdit: Siber Suçlar, Seçkin Yay., Ankara 2014, s. 30.

[62] Metin için bkz. Europol: *"ChatGPT The impact of Large Language Models on Law Enforcement"* https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf (E.T. 05.05.2023) Nitekim ChatGPT'nin oldukça özgün ve insan elinden çıkmış metinler yazabildiği düşünüldüğünde, saldırganların ChatGPT ile olay örgüsü yönünden mağduru örneğin kendisinin bir ödül kazandığına ikna edebilecek kadar güçlü paragraflar yazabilecektir. Önceleri saldırganların phishing saldırı maillerinde fark edilebilecek otomatik yazım, dil bilgisi ve bağlam hataları artık fark edilmeyecek düzeye gelebilecek ve bu husus da mağdurların phishing e-maillerine inanarak gelen linke tıklamalarına yol açabilecektir. Benzer yönde bkz. PICOTTI, *"Diritto Penale, technologie informatiche ed intelligenza artificiale: una visione d'insieme"*, s. 54.

türüdür[63]. Bu siber saldırı tekniği, mağdurda toplumda itibar gören mesleklerden birine sahip kişi tarafından kendisiyle iletişime geçiliyormuş güveni yaratarak onun kötü amaçlı bir bağlantıya tıklamasını sağlama fikri üzerine kurulmuştur.

Amerika'ın Telekomünikasyon devi Verizon şirketi, 2021 Veri İhlali Araştırmaları Raporu'nda 2020 yılında dünya çapında tespit edilebilen 3841 sosyal mühendislik vakası gerçekleştiği kaydedilmiştir[64].

ABD Adalet Bakanlığı verilerine göre sosyal mühendislik saldırıları 2016 yılında Amerika'yı 121 milyar dolarlık bir zarara uğratmıştır[65].

c. Şifre Kırıcı Saldırılar (Password Cracker Attacks)

Bilgisayar korsanlarının kullandığı sisteme ve verilere yasadışı erişebilme araçlarından bir diğeri de şifre kırıcı saldırılardır.

Şifre kırıcı metotlardan ilki *"brute-force"* yani kaba kuvvet saldırılardır. Bu tür saldırılarda karakter, kelime veya cümle kombinasyonları denenerek esas şifreyi bulmak

---

[63] **GIBONEY**, Justin Scott – **SCHUETZLER**, Ryan M. – **GRIMES**, G. Mark, *"Know your enemy: Conversational agents for security, education, training, and awareness at scale"*, Computer&Security Journal, Vol. 129, No. 2, 2023. İnternet Erişim: https://doi.org/10.1016/j.cose.2023.103207 (E.T. 27.06.2023); **HEKİM**, Hakan, *"Oltalama (Phishing) Saldırıları"*, Siber Suçlar: Tehditler, Farkındalık ve Mücadele içinde (Ed. Fatih Tombul, Murat Güneştaş, Oğuzhan Başıbüyük), Global Politika ve Strateji Yay., Ankara 2015, s. 59.

[64] GIBONEY – SCHUETZLER – GRIMES, s. 1.

[65] **AKDEMİR**, Naci (Ed.) – **TUNCER**, Can Ozan (Ed.), Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım, Pegem Akademi Yay., Ankara 2021, s. 545.

amaçlanır[66]. Örneğin İngiltere'de 1984'teki Prestel Korsanlığında, Edinburgh Dükünün e-posta adresi, bir bilgisayar korsanının şifre denemeleri sonucunda gerçek şifrenin bulunmasıyla (222222 1234) ele geçirilmiştir[67].

Şifre kırıcı metotlardan bir diğeri gökkuşağı tablosu saldırısıdır. Bu yöntemde fail, kullanıcıların sisteme girmek için yazdıkları parolaların kaydettiği hash (karma) değerlerin[68] depolandığı bir tablodan faydalanır[69]. Saldırgan, brute-force yöntemindeki gibi şifreyi kendi tahmin etmeye çalışmak yerine, bunu şifrelerin hash (karma) değerlerinin kaydedildiği bir algoritmaya bırakır. Bu saldırılar bir program aracılığıyla otomatikleştirilebilir ve doğru olan bulunana kadar çok sayıda parola kombinasyonu üzerinden çalıştırılabilir[70].

Belirtmek gerekir ki kanun koyucu TCK m. 245/A gereği, örneğin şifre kırıcı program (gökkuşağı tablosu programı vs) veya yazılımların suçta kullanılmasa dahi bu program ve yazılımların bilişim sistemlerine ve verilere müdahale amacıyla oluşturulması, depolanması, satılması, satın alınması, nakledilmesi vb. gibi hazırlık hareketlerini tek başına suç olarak düzenlemiştir[71].

---

[66] **YELDAN**, Didem, Siber Suçlar, Seçkin Yay., Ankara 2022, s. 78.; DÜLGER, s. 124.

[67] **JORDAN**, Tim – **TAYLOR**, Paul, *"A sociology of hackers",* Sociological Review, Vol. 46, No. 4, 1998, s. 759. Bu olaydan sonra İngiltere'de bilişim sistemlerine ve verilere karşı suçların cezalandırılmasına ilişkin başta 1990 Bilgisayarı Kötüye Kullanma Yasası olmak üzere birtakım düzenlemelere gidilmiştir.

[68] Hash, belirli bir girdinin (mesela bir metin veya dosya) benzersiz bir temsilini veren matematiksel bir fonksiyondur. Her şifrenin bir hash değeri vardır.

[69] AKDEMİR (Ed.), – TUNCER (Ed.), s. 521.

[70] KILIÇ – ÇAKIR, Adli Bilişim ve Elektronik Deliller, s. 297.

[71] **PARLAR**, Ali **– ÖZTÜRK**, Mustafa, Doğrudan ve Dolaylı Bilişim Suçları, B. 1, Aristo Yay., İstanbul 2020, s. 273.

Yargıtay, bir bilişim sistemine, örneğin bir Facebook kullanıcısının hesabına şifresinin kırılarak girilmesini TCK m. 243'te düzenleme alanı bulan *"Bilişim Sistemine Girme"* suçu olarak değerlendirmekte; buna karşılık erişimden sonra şifrenin değiştirilerek kullanıcının hesaba erişiminin engellenmesi, hesaptaki veri veya bilgiler değiştirilmesi veya bozulması eylemlerine ilişkin yalnızca TCK m. 244/2'de düzenlenen *"Verileri bozma, yok etme, değiştirme veya erişilmez kılma"* suçundan hüküm kurmaktadır[72].

Parola kırma saldırıları, unutulan bir parolayı sahibinin isteği doğrultusunda kurtarmak veya sahibinin izni dahilinde bir sistemin güvenliğini test etmek için kullanıldığında suç oluşturmamaktadır.

2. Verilere Müdahale Edebilmek İçin Kötü Niyetli Yazılım Bulaştırma Teknikleri

a. Bilgisayar Solucanları (Worms)

Bilgisayar solucanları, sistem zaafiyeti ve açıklarından yararlanarak bilgisayarlara LAN ağı veya internet üzerinden bulaşan ve bulaştığı bilgisayara sistemin

[72] 8. CD., E. 2016/7582, K. 2016/10690, T. 23.11.2016.: "*Katılana ait elektronik posta adresinin şifresini kırarak, erişilmez kıldığından bahisle açılan davada ... katılanın mail adresinin şifresinin kim tarafından değiştirildiğinin e- posta adresinin bağlı olduğu firmadan sorulması, şifre değiştirildiğinin tespiti halinde TCK.nun 244/2, aksi halde aynı yasanın 243. maddesi kapsamında değerlendirilmesi gerektiğinin gözetilmemesi…".* Benzer yönde: 8. CD, E. 2017/24009, K. 2019/6266, T. 06.05.2019. https://kararara ma.yargitay.gov.tr/ (E.T. 29.07.2023); 8. CD., E. 2019/19923, K. 2021/80, T. 11.01.2021. https://kararara ma.yargitay.gov.tr/ (E.T. 29.07.2023).

güvenlik duvarını aşabilen çeşitli zararlı yazılımlar (fidye yazılım, casus yazılım) yükleyebilme özelliği bulunan yazılımlardır[73]. Solucanlar bir bilgisayara bulaştığı zaman kendisinin kopyasını üretir ve kendini kopyalayabileceği diğer savunmasız bilgisayarları aramaya başlar. Kopya üretme süreci, otomatik zamanlama mekanizmasının süreci kendiliğinden durdurmasıyla sona erebileceği gibi, bu mekanizma olmadığı durumda sonsuza kadar devam edebilir[74].

Solucanı, tipik bir virüsten ayıran özelliklerden ilki kullanıcı etkileşimi olmadan etkin olabilme, yayılabilme ve çoğalabilme fonksiyonudur[75]; zira bilgisayar virüsleri kullanıcının kendisini aktif etmediği müddetçe etkin olamaz ve yayılamazlar. İkinci fark, solucanların sisteme zarar verme amacı olmaksızın da sistemin içinde dolaşabilme özelliğine sahip olmasıdır[76]. Son olarak solucanlar mümkün olduğunca çok sayıda savunmasız sistemlere yayılma hedefiyle tasarlanmışken, virüsler genellikle verileri bozmak, silmek veya elde etmek ve bulaştığı sisteme başka şekillerde zarar vermek gibi işlevlere sahiptir.

2019'da açıklanan Symantec İnternet Güvenliği Tehdidi Raporu'na göre 2018'de bilişim sistemlerine karşı gerçekleşen müdahalelerin büyük çoğunluğunu solucanlar oluşturmaktadır[77]. Gerçekten, solucanların yayılım ve çoğalma gücü sebebiyle binlerce

[73] AKDEMİR (Ed.) – TUNCER (Ed.), s. 526.

[74] **ERBSCHOLE**, Michael, Trojans, Worms, And Spyware: A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth-Heinemann, USA 2005, s. 23.

[75] **OORSCHOT**, Paul C. Van, Siber Güvenliğe Giriş: Bilgisayar Güvenliği ve İnternet (Çev. Kemal Bıçakçı), Palme Yay., Ankara 2022, s. 187.; AKARSLAN, s. 93.

[76] DÜLGER, s. 115.

[77] **SYMANTEC**, Internet Security Threat Report, Volume 24, 2019, s. 20. İnternet Erişim: https://docs.broadcom.com/doc/internet-security-threat-report-volume-24-en (E.T. 29.07.2023)

müşterisi olan şirket ve finans kurumlarına ait olan bilişim sistemlerine yapılan müdahalelerde sıklıkla solucanlar (worms) tercih edilmektedir[78].

b. Mantık Bombaları

Mantık bombaları belirli sayıda işlem yapılması veya belirli bir zaman gelmesi gibi mantıksal koşullarla tetiklenerek çalışmak üzere ayarlanmış zararlı yazılımlardır[79]. Bu koşullar gerçekleşmeden önce, mantık bombaları sistemde etkisiz haldedirler.

Mantık bombası, etkinleştirildiğinde sistemdeki dosyaları silmek, verileri değiştirmek veya erişilmez kılmak, bir virüs veya solucan yerleştirmek üzere tasarlanabilmektedirler[80]. Amacı ne olursa olsun, ortak özellikleri tetiklenen olay gerçekleştiğinde sistemde tek bir yıkıcı patlama gerçekleştirmesidir[81].

Kendisini yazan kişi tarafından bir konferansta zararsız olarak tanıtılıp misafirlerin sistemlerine yüklenen ve 26 Nisan tarihinde faaliyete geçerek sistemleri çökerten Çernobil virüsü mantık bombalarına örnek verilebilir[82].

---

[78] AKARSLAN, s. 93.

[79] **HILL**, Josua B. – **MARION**, Nancy E., Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century, Praeger, USA 2016, s. 79.; AKDEMİR (Ed.) – TUNCER (Ed.), s. 304.; ERBSCHOLE, s. 25.; DÜLGER, s. 117.

[80] **CLOUGH**, Paul – **MUNGO**, Bryan, Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals, Random House, USA 2013, s. 105.

[81] CLOUGH – MUNGO, s. 105.

[82] DÜLGER, s. 117, 118.

c. Truva Atı

Truva atı, Yunan mitolojisinde Troyalılar ile Akhalıların yaptığı savaşta Akhalıların büyük bir tahta atı Troyalılara hediye görüntüsü vererek sunduğu, içinden ise Akhalı askerlerin çıktığı ve Troyalıların savaşı kaybetmesine neden olduğu bir savaş hilesidir[83].

Truva atı yazılımları da aynen bu şekilde çalışmaktadır[84]. Görünürde güvenli bir yazılım izlenimi vererek kullanıcıda güven uyandırsa da aldatıcı görünümünün altında verilere zarar verdirecek özellik barındırırlar.

Truva atı yazılımı bir bilgisayara bulaştığında, saldırgana bilgisayardaki dosyaların ayarlarını değiştirme, dosyaları çalma, dosyalara zarar verme veya ağdaki kullanıcı etkinliklerini izleme olanağı verir[85]. Bu kapsamda her ne kadar verilere müdahale amacıyla tasarlanmış olsa da truva atı yazılımıyla bilişim sistemlerine ve verilere karşı suçların hemen hemen hepsi işlenebilir[86].

Truva atları, virüs ve solucanlardan farklı olarak kendi kendine çoğalarak yayılabilme özelliğine sahip değildirler[87].

---

[83] DÜLGER, s. 110.

[84] DÜLGER, s. 110.

[85] ERBSCHOLE, s. 25.

[86] DÜLGER, s. 110.; AKARSLAN, s. 94.

[87] **CANBEK**, Gürol – **SAĞIROĞLU**, Şeref, *"Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma"*, Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, C. 22, N. 1, 2007, s. 125.; ÇAKIR (Ed.) – KILIÇ (Ed.), Güncel Tehdit: Siber Suçlar, s. 28.; AKDEMİR (Ed.) – TUNCER (Ed.), s. 581, 582.; AKARSLAN, 94.

d. Tavşanlar

Tavşanlar İngilizcede *"Rabbits", "Wabbits"*[88] veya *"Fork Bomb"*[89] olarak adlandırılmaktadır. Tavşanlar ilk defa 1974 yılında ortaya çıkmıştır[90]. Bu yazılımın özelliği, sisteme manasız komutlar zinciri vererek işlemcinin işleyişi sağlayan faaliyet göstermesini engellemektir[91].

Bu virüsler, bir bilişim sistemine girdiklerinde tıpkı ağ solucanları gibi hızla çoğalabilirler ve sistemlerde geri dönülmez tahribatlara yol açabilirler. Tavşanlar bu yönüyle ağ solucanlarına benzese de ağ solucanlarının aksine bunlar ağ üzerinden yayılmazlar. Bu tür virüsler e-posta, yazılım indirmeleri veya dosya paylaşımı yoluyla bulaşabilmektedir.

e. Formjacking

Formjacking, kullanıcıların bir web sitesinde özellikle online alışverişlerde paylaştıkları kredi kartı numaraları, adresleri ve kimlik bilgileri gibi kişisel bilgileri

---

[88] **MARION**, Nancy E. – **TWEDE**, Johnson, Cybercrime: An Encyclopedia of Digital Crime, ABC-CLIO, California 2020, s. 251.

[89] **ÖZÇELİK**, İlker – **BROOKS**, Richard, Distributed Denial of Service Attacks: Real-world Detection and Mitigation, CRC Press, 2020, s. 22.

[90] MARION – TWEDE, s. 251.

[91] DÜLGER, s. 116.; **ERGÜN**, İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, Adalet Yay., Ankara 2008, s. 24.

çalmak için faillerin bir web sitesinin form sayfasına kötü amaçlı kod yerleştirdiği bir siber saldırı türüdür[92].

2019'da yayınlanan Symantec İnternet Güvenliği Tehdidi Raporu'nda ayda ortalama 4800 sitenin formjacking saldırısı gerçekleştirildiği belirtilmiştir[93].

3. Bilişim Sisteminin Verimli Çalışmasını Engellemek İçin Kullanılan Teknikler

a. Fidye Yazılımlar

Fidye yazılımlar, bilişim korsanına bir miktar para ödenene dek kullanıcının bilişim sistemine, ağlarına veya verilerine erişimini engellemek için tasarlanmış zararlı bir yazılımdır[94]. Fidye yazılımlar bir bilgisayara e-posta yoluyla yerleşebileceği gibi, güvenli olmayan internet adreslerinden indirilen yazılımlar aracılığıyla veya disk, bellek gibi harici donanımlar vasıtasıyla bulaşabilir.

Fidye yazılımlar bir bilgisayara girdikten sonra bilgisayar üzerindeki verilere ve dosyalara kullanıcıların çözemeyecekleri şifreler koyar. Bilgisayar korsanı, bu şifrelerin çözülebilmesi için bir miktar para vermesi gerektiğini, aksi takdirde dosyaların imha

[92] SYMANTEC, Internet Security Threat Report, s. 14.

[93] SYMANTEC, Internet Security Threat Report, s. 14.

[94] AKDEMİR (Ed.) – TUNCER (Ed.), s. 206.

edileceğini kullanıcıya bildirir[95]. Failin istediği meblağın çoğu kez Bitcoin veya diğer sanal para birimleri üzerinden ödenmesini talep eder[96]. Bu bildirimi elektronik iletişim araçlarıyla, genellikle e-posta yoluyla yapar. Bu yöntemde korsanlar para yatırıldığı takdirde şifrenin mutlaka çözüleceği yönünde kullanıcılara güven vererek çok yüklü miktarlarda paralar istemeyip sürümden kazanmaktadırlar[97]. Kullanıcılar istenen paranın çok yüksek olmaması sebebiyle ve bu paranın yatırıldığı takdirde dosyalarındaki şifrelerin çözüleceği inancıyla fidyeleri ödemekte ve suç duyurusunda bulunmamaktadır[98].

Turkish Crime Family adlı İngiltere'de yaşayan Türkler tarafından[99] oluşturulmuş bir bilişim korsanı örgütü, 2017 yılında milyonlarca iCloud hesabına erişimleri olduğunu iddia ederek talep edilen paranın ödenmemesi halinde hesapların silineceği tehdidiyle Apple'dan fidye istemiştir. Suç örgütünün lideri daha sonra İngiltere mahkemeleri tarafından yargılanarak iki yıl hapis cezasına mahkûm edilmiştir[100].

---

[95] **CAPPELLINI**, Alberto, *"I Dellitti Contro L'integrità Dei Dati, Dei Programmi e Dei Sistemi Informatici"*, Cybercrime içinde (Ed. Alberto Cadoppi – Stefano Canestrari – Adelmo Manna – Michele Papa), B. 2, Wolters Kluver Italia, Italy 2023, s. 813.

[96] MARION – TWEDE, s. 249.

[97] DÜLGER, s. 128.

[98] DÜLGER, s. 128, 129.

[99] Örgüt ile yapılan röportaj için bkz. https://www.applefoni.com/applei-tehdit-ederek-fidye-talep-eden-turkish-crime-family-ile-roportaj-yaptik/ (E.T. 29.07.2023)

[100] https://www.sozcu.com.tr/2019/dunya/son-dakika-applea-dava-acan-turk-hacker-ile-ilgili-sicak-gelisme-5525031/ (E.T. 29.07.2023)

b. DoS (Hizmet Reddi Saldırıları) ve DDoS (Dağıtılmış Hizmet Reddi Saldırıları)

DoS (Denial of Service) atakları, bir bilişim sisteminden diğer bir sistemin sunucusuna yoğun istekler gönderilerek sunucunun işlevsiz kılınması için yapılan saldırılardır[101]. Bu ataklar bilgisayar sistemlerine veya yazılıma maddi olarak zarar vermekten ziyade, saldırıya uğrayan sistemin düzenli işleyişini ve veri akışını tıkamak için koordine edilirler[102].

DDoS (Distributed Denial of Service) saldırısı ise sunucuya giden istek yükünün farklı bilişim sistemlerine dağıtılması üzerine kurulmuştur[103]. Bu çerçevede DDoS saldırılarında bilişim korsanı, önceden ele geçirdiği bilgisayarlar aracılığıyla bir hedef sisteme aynı anda karşılanamayacak sayıda istek göndererek, o hedef sistemi hizmet veremeyecek duruma getirmektedir. Saldırganın hedef bilgisayarın trafiğini arttırarak işleyişini engellemek amacıyla önceden ele geçirdiği bilgisayarlara *"zombi bilgisayar (köle bilgisayar)"* adı verilmektedir[104]. *"Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği"*nin 3-j fıkrasında "*Köle Bilgisayar: herhangi bir amaçla kullanılmak üzere, zararlı yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayar"* şeklinde bir tanım yapılmıştır.

Zombi bilgisayarlara programlar yerleştirilerek, saldırgana bilgisayarı uzaktan kontrol etme imkânı verilmektedir. Uzaktan kontrol imkânı sayesinde saldırgan, zombi

---

[101] AKDEMİR (Ed.) – TUNCER (Ed.), s. 233.

[102] PICOTTI, *"Diritto Penale, technologie informatiche ed intelligenza artificiale: una visione d'insieme",* s. 71.

[103] ÖZÇELİK – BROOKS, s. 6.

[104] ÖZÇELİK – BROOKS, s. 6, 7.

bilgisayarlarla fiziksel bir yakınlık içinde olmadan hedef bilgisayara yönelik kısa sürede pek çok istek yollayarak sistemi erişilmez hale getirir[105]. Bu sebeple zombi bilgisayarlar bir nevi piyon işlevi görürler. DDoS saldırılarını, dolayısıyla zombi bilgisayarlardan gelen istekleri önleyebilmek için webde pek çok sunucuda *"Gerçek kişi olduğunuzu doğrulayın"* şeklinde, yalnızca gerçek bir kişinin başarıyla geçebileceği karmaşık testler yapılmaktadır.

Yargıtay CGK önüne gelen bir davada *"koordineli olarak yapılan bu işlemin hem saldırının boyutunu artırdığının hem de saldırıyı yapan kişinin gizlenmesini sağladığı, bu nedenle de saldırganı bulmanın zorlaştığı, çünkü saldırının merkezinde bulunan saldırganın aslında saldırıya katılmadığı…"* ifadeleriyle DDoS ataklarının fonksiyonu itibariyle gerçek failin bulunmasını engellediğine yönelik önemli bir tespitte bulunmuştur[106].

Saldırılar zombi bilgisayarlar tarafından yapıldığı için saldırının gerçekleştirildiği bilgisayara ulaşılmaya çalışıldığında "zombi bilgisayar"ların IP adresleri bulunduğundan, bu IP adreslerin arkasına gizlenen gerçek saldırgana ulaşmak mümkün olmamaktadır[107]. Ceza Genel Kurulu'nun incelediği yukarıdaki uyuşmazlıkta da DDoS ataklarını yapan zombi bilgisayarlardan bazılarının statik IP adreslerine sahip olmasına karşın erişim sağlayıcıdan gelen müzekkere cevabında bu IP adreslerinin davadaki sanıklarla bir ilgisi olmadığı ortaya çıkmıştır. Gerçek faili saklayabilme özelliği olan DDoS atakları, pek çok suçun siyah sayıda kalmasına yol açmaktadır.

---

[105] **ÖZOCAK**, Gürkan, *"DDoS Saldırısı ve Failin Cezai Sorumluluğu",* Ankara 29. Ulusal Bilişim Kurultayı Bildiriler Kitabı içinde, Ankara 2012, s. 24.

[106] Yargıtay CGK, E. 2016/544, K. 2020/127, T. 25.02.2020. https://karararama.yargitay.gov.tr/ (E.T. 01.07.2023)

[107] ÖZOCAK, s. 24.

Tarihin kayda geçen en büyük DDoS saldırısı, 19 Ağustos 2022 tarihinde Google Cloud'a karşı yapılan DDoS saldırısıdır[108]. Google yaptığı açıklamada, sunucuya zombi bilgisayarlardan saniyede 46 milyon istek geldiğini ve saldırının 69 saniye boyunca sürdüğünü belirtmiştir[109].

Yapılan araştırmalar, DDoS ataklarının bir amaç olmaksızın, yalnızca bir eğlence uğruna yapılabileceği gibi dini, siyasi veya hacktivizm gibi politik amaçlar doğrultusunda da gerçekleştiğini göstermektedir[110]. Gerçekten, aktivist bilişim korsan grupları çoğu zaman DDoS ataklarını kullanarak sistemi felce uğratmayı tercih etmektedirler[111]. Bunun sebebi, DDoS ataklarının sivil itaatsizlikte bulunmaya elverişli olması, kolay öğrenilebilir olması ve ustalık düzeyinde yazılım ve bilişim bilgisi gerektirmemesidir[112].

---

[108] https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps (E.T. 08.07.2023). Google, saldırıdan önce kayda geçmiş en büyük DDoS saldırısı olarak adlandırılan, DDoS koruması, internet güvenliği ve alan adı sunucusu hizmetleri sağlayan ABD merkezli *"CloudFlare"*'ye gerçekleştirilen rekor saldırıdan %76 oranda daha büyük bir saldırıya maruz kaldığını raporunda vurgulamıştır.

[109] Açıklama için bkz. https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps (E.T. 08.07.2023).

[110] **KRANENBARG**, Marleen Weulen, *"Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives",* Cybercrime in Context The human factor in victimization, offending, and policing içinde (Ed. Marleen Weulen Kranenbarg - Rutger Leukfeldt), Springer Nature, Switzerland 2021, s. 198.

[111] DEMİRKIRAN, s. 29.

[112] DEMİRKIRAN, s. 29.

c. İstem Dışı Alınan Elektronik İletiler (Spam Bombing)

Spam, rastgele oluşturulmuş bir alıcı listesine, istenmeyen ve gereksiz içeriklerin e-posta aracılığıyla gönderilmesi anlamına gelir[113].

İstem dışı alınan postaların yaygın bir şekilde gönderilmesi, e-posta hizmet sağlayıcılarının altyapısının kaldırabileceğinden fazla bir istekle karşılaşılmasına neden olabilmektedir. Böylelikle e-posta iletişiminde yavaşlama ve kullanıcının e-posta hesabının verimli olarak işlemesini engelleme gibi sorunlar meydana gelebilmektedir. Elektronik posta bombardımanıyla sistemin kilitlenmesi halinde *"Sistemin işleyişinin engellenmesi veya bozulması (TCK m. 244/1)"* suçundan bahsedilebilecektir[114].

Örneğin, anti-spam danışmanı David O'Daniel, dakikada 50.000 civarında elektronik iletiyi kaldırabilecek bir sistemin, bir spam göndericisinin spamları sonucunda çöktüğünü söylemiştir[115].

III. ULUSLARARASI ALANDA BİLİŞİM SİSTEMİNE VE VERİLERE KARŞI SUÇLARA İLİŞKİN DÜZENLEMELER

Bilişim suçlarıyla mücadele edebilmek amacıyla gerçekleştirilen uluslararası çalışmalar hayati bir öneme sahiptir. Gerçekten, Amerika'da 1980'lerde başlayan ve sonrasında tüm dünyaya yayılan 'hacking' faaliyetleri ve diğer bilişim suçlarıyla mücadele uzun bir süre yerel düzeyde kalmıştır. Oysaki bilişim suçlarının geleneksel

[113] AKDEMİR (Ed.) – TUNCER (Ed.), s. 251.

[114] KURT, s. 164.

[115] KURT, s. 72.

suçlardan ayıran en önemli özelliklerden biri, bu suçların failleriyle mağdurları arasında binlerce kilometre mesafe olabilmesidir.

Fail ile mağdurun aynı ülkede olması durumunda dahi, failin yakalanabilmesi için gerekli olan delillerin bir başka ülkenin yargılama alanında olma ihtimali olabilir[116]. Zira, fail ile mağdurun etkileşimi çoğu zaman ikisinin de ülkesinden farklı, üçüncü taraf ülkede bulunan bir sunucuda gerçekleşmektedir[117]. Sözgelimi Bulgaristan'daki bir kişinin, Gürcistan vatandaşı olan başka bir kişinin Facebook hesabını hacklemesi olayında, Facebook sunucusu Amerika'da olduğundan taraf ülke Amerika olmaktadır.

Birleşmiş Milletler Uyuşturucu ve Suç Ofisi'nin 2013 yılında yayınladığı *"Comprehensive Study on Cybercrime"* adlı raporda, çalışmaya katılan devletlerin yarısından fazlası adli kolluğun karşılaştığı bilişim suçlarına ilişkin eylemlerinin %50'den fazlasının ulus ötesi bir unsur içerdiğini bildirmiştir[118]. Teknolojinin ülkenin sınırları olmaksızın birbirine bağlı doğası, bilişim suçlarını küresel bir sorun haline getirmektedir ve bu durum da koordineli iş birliği ihtiyacı konusunda uluslararası farkındalığı gerekli kılmaktadır[119].

---

[116] CLOUGH, s. 700.

[117] **VINCENT**, Nicole A., *"Victims of cybercrime: Definitions and challenges"*, Cybercrime and It's Victims içinde (Ed. Elena Martellozo, Emma A. Jane), Routledge, New York 2017, s. 34.

[118]Comprehensive Study on Cybercrime, s. 5. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (E.T. 16.07.2023)

[119] **YAZICIOĞLU**, Yılmaz, *"Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı",* Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001 içinde, Dokuz Eylül Üniversitesi Yayını, İzmir 2002, s. 451.; CLOUGH, s. 699.; ERGÜN, s. 43.

Öte yandan, bir davranış belirli bir ülkede suç sayılmıyorsa, o ülkedeki kişiler diğer yargı alanlarını etkileyebilecek suçları işlerken cezasız kalabilirler[120]. Bu bakımdan bir ülkede bilişim suçları suç olarak düzenlenmediği takdirde, faile dair kovuşturma yapma imkânı olmamakla kalmaz, aynı zamanda çifte suçluluğun yokluğunda kanıt toplama ve suçluların iadesi çabaları da engellenebilir[121]. Tüm bu sebepler ışığında, bilişim suçlarıyla etkin olarak mücadele edilebilmesi için uluslararası alanda tüm devletlerin mutabık olduğu düzenlemelerin yürürlüğe girmesi çok önemlidir.

A. EKONOMİK KALKINMA VE İŞ BİRLİĞİ ÖRGÜTÜ (OECD) RAPORU

Uluslararası platformda, bilişim sistemlerine ve verilere karşı suçlara ilişkin devletlerin mevzuatlarında uyumlulaştırma çalışmaları tarihte ilk kez "Ekonomik Kalkınma ve İş Birliği Örgütü (OECD)" bünyesinde gerçekleştirilmiştir[122]. Bu kapsamda Örgüt, 1982 yılında bir uzmanlık komitesi oluşturmuş ve bu uzmanlık komitesi 1986 yılında yayımladığı raporda bu tür suçların ulusötesi özelliğine dikkat çekerek uluslararası adli iş birliğinin önemini vurgulamıştır[123]. Yine bu raporda, dört fiile yer verilerek ülkelerin ceza kanunlarında en azından bu dört fiilin suç olarak tanımlanması gerektiği belirtilmiştir[124]. Bu fiiller, "bilgisayar yoluyla dolandırıcılık ve

[120] **CLOUGH**, Jonathan, *"A World Of Difference: The Budapest Convention On Cybercrıme And The Challenges Of Harmonisation"*, Monash University Law Review, Vol. 40, No. 3, s. 701.

[121] CLOUGH, s. 701.

[122] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 64.

[123] **SCHJØLBERG,** Stein, *"The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva",* 2008. https://www.cybercrimelaw.net/documents/cybercrime_history.pdf (E.T. 3.1.2024)

[124] AKARSLAN, s. 156.

sahtecilik", "bilgisayar programlarını ve verilerini değiştirme", "telif hakları ihlalleri" ve "bilgisayarların veya iletişim sistemlerinin iletişiminin yahut diğer fonksiyonlarının engellenmesi"dir.

B. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ (AKSSS)

1. Sözleşmenin Ortaya Çıkış Süreci

Bilişim suçlarına ilişkin uluslararası bir belge ihtiyacının karşılanması, 1990'lı yılların ortalarında başlayan çalışmalarla mümkün olmuştur. Avrupa Suç Sorunları Komitesi (CDPC) 1996 yılının Kasım ayında bilişim suçlarını araştıracak ve bu doğrultuda atılması gereken hukuki adımları inceleyecek bir uzmanlık komitesi kurmaya karar vermiştir[125]. Kurulan *"Siber Suç Uzmanları Komitesi (The Commitee of*

[125] **İÇEL**, Kayıhan *"Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri",* İÜHFM, C. 59, S. 1, 2001, s. 4. Komitenin uzmanlık ekibini kurma gerekçesinin bir kesiti şu şekildedir: *"İletişim ve bilgi hizmetlerine bağlanan kullanıcılar 'siber uzay' adı verilen, meşru amaçlar için kullanılan, ancak kötüye kullanıma da açık olan, ortak bir uzay yaratmışlardır. Söz konusu 'siber uzay suçları', bilgisayar sistemlerinin ve telekomünikasyon ağlarının bütünlüğüne, ulaşılabilirliğine ve gizliliğine karşı işlenebileceği gibi, bilinen bazı suçların işlenmesinde bu ağların sunduğu hizmetlerden yararlanma şeklinde de ortaya çıkabilir. Bu suçların siyasal sınırları aşabilen niteliği, örneğin internet aracılığı ile işlenebilmesi, ulusal makamların mülkilik özellikleri ile çelişik durumundadır. Bu nedenle, ceza hukuku, siber uzayın olanaklarının kötüye kullanımını ve meşru çıkarlara zarar vermek için son derece gelişmiş olanaklar sunan bu teknolojik gelişmeleri yakından izlemelidir. Bilgi ağlarının sınırlar ötesi yapılarından dolayı bu tür kötüye kullanılmalarla mücadele etmek için uluslararası düzeyde ortak çalışmaların yürütülmesi gerekmektedir. (89) 9 sayılı tavsiye kararı ile bilgisayarların kötüye kullanılma biçimleriyle ilgili ulusal kavramların birbirlerine yaklaşmaları sağlanmışsa da, bu yeni olgularla*

Experts on Crime in Cyber-Space)", bilişim suçlarına ilişkin maddi ceza hukuku ve ceza muhakemesi hukuku alanındaki uyuşmazlıklara çözüm üretebilecek ve bilişim suçları konusunda katılımcı devletler arasında uyumlulaştırmayı hedefleyecek uluslararası bir sözleşme çalışmalarını yaklaşık 4 yıl sürdürdü. Bu doğrultuda toplamda 5 yıllık bir ön hazırlığın ardından bilişim suçlarının uluslararası alandaki ilk ürünü *"Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)"* 23 Kasım 2001 tarihinde Budapeşte'de devletlerin imzasına açılmış ve 1 Temmuz 2004'te yürürlüğe girmiştir[126]. Türkiye sözleşmeyi, sözleşme imzaya açıldıktan yaklaşık 6 yıl sonra 10.11.2010 tarihinde imzalamış, sözleşme 29.09.2014 tarihinde yürürlüğe girmiştir.

2. Sözleşmenin Niteliği

Suç ve bilişim ilişkisini ele alan ilk uluslararası antlaşma, Avrupa Konseyi Siber Suç Sözleşmesidir[127]. AKSSS'nin esas amacı akit devletlerin yargılama yetkisi alanına girerek ulusal düzeyde bilişim suçlarını düzenlemek değil, devletlerin mevzuatlarını uyumlulaştırmak adına bu suçlar bakımından asgari bir standart oluşturmaktır. Bu kapsamda Sözleşme'nin bilişim sistemlerine ve verilere karşı müdahale başta olmak üzere, çocuk pornografisi gibi bilişim sistemleriyle işlenme oranı yüksek olan suçların ulusal kanunlarda suç olarak kabul edilmesine önemli katkısı olmuştur. Çerçeve

---

*mücadelede gerekli verimliliğin elde edilmesi ancak bağlayıcı uluslararası bir araçla gerçekleştirilebilir. Böyle bir araç çerçevesinde, uluslararası iş birliği önlemlerine ek olarak, maddi hukuk ve usul hukukuyla ilgili sorunlar ve bilgi teknolojisinin kullanımıyla yakından bağlantılı konular ele alınmalıdır."*Daha fazlası için bkz. İÇEL, s. 4, 5.

[126] İÇEL, s. 5, 6.

[127] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 68.; ÖNOK, s. 1241.

hükümler içeren Sözleşme, aynı zamanda Avrupa Konseyi ve AB düzeyindeki yasama girişimleri için de bir yol gösterici rehber niteliğindedir[128].

2024 yılı itibariyle Sözleşme'ye 68 ülke taraf olmuş, 50 ülke de imzalamıştır.

3. Sözleşmenin İçeriği

a. Maddi Hukuk

Sözleşme'de bilişim suçları dört suç kategorisi başlığı altında incelenmiştir: *"(1) Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar; (2) Bilgisayarla ilgili suçlar (bilgisayarla işlenilen dolandırıcılık ve sahtecilik); (3) içerik bağlantılı suçlar (çocuk pornografisi); ve (4) telif hakkı ihlali."*

Sözleşmede öngörülen suçların tamamına yakınında kusur kapsamında eylemin "kasıtlı", ve hukuka aykırılık bağlamında "haksız" olması şartı getirilmiştir. Öğretide "haksız" ifadesinin hukuka özel aykırılık olduğuna, bu ifadenin failin hukuka aykırı olarak hareket ettiğini bilmesini ve istemesini kapsadığı görüşünü savunanlar olsa da[129] ben buna katılmıyorum. Kanaatimce burada haksız kavramı bizzat hukuka aykırılık unsurunu ifade etmek için kullanılmaktadır.

---

[128] **POLYZOIDOU**, Vagia, *"Combatting the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime",* EU Internet Law in the Digital Single Market içinde (Ed. Tatiana Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou Merdi), Springer Nature, Switzerland 2021, s. 359.

[129] **MAHMUTOĞLU**, Fatih Selami, *"Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu"*, İÜHFM, C. 59, S. 1-2, 2001, s. 40.

aa. Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar

Tezin konusunu oluşturan *"Bilişim sistemlerine ve bilişim sistemindeki verilere karşı suçlar"*, esasında AKSSS'de *"Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı suçlar"* olarak düzenlenmektedir.

AKSSS'in bu bölümünde düzenlenen ilk suç, 2. maddede *düzenlenen "Yetkisiz erişim"* suçudur. Buna göre bilişim sistemlerine veya verilerine izinsiz erişim, sözleşme kapsamında suç olarak kabul edilmiş ve taraf devletlere bu suçu ulusal mevzuatlarında düzenleme yükümlülüğü getirilmiştir.

Sözleşmenin 3. maddesinde *"Yasadışı araya girme"* başlığıyla bilgisayar verilerinin kamuya açık olmayan iletimlerinin izinsiz olarak dinlenmesi fiili suç olarak düzenlenmiş ve taraf devletlere bu fiilin kanunlarda düzenlenmesi için gerekli işlemleri yapması yükümlülüğü yüklenmiştir.

4. maddede verilerin kasıtlı ve izinsiz olarak değiştirilmesi veya bir bilgisayar sisteminin işleyişine müdahale edilmesi; 5. maddede ise bilgisayar sisteminin işleyişinin bozulması yasaklanmış ve yine akit devletlerin bu fiillerin suç olarak düzenlenmesi için gerekli tedbirleri alması gerektiği belirtilmiştir.

Bu başlık altında son olarak 6. maddede Sözleşme kapsamındaki suçların işlenmesi amacıyla donanım, yazılım veya diğer cihazların bulundurulması, üretilmesi, tedavüle sokulması gibi eylemlerin cezai müeyyideye bağlanması gerektiği belirtilmiştir.

bb. Bilgisayarla ilgili suçlar, içerik bağlantılı suçlar ve telif hakkı ihlali

Sözleşmenin *"Bilgisayarlarla ilgili suçlar"* adlı 2. başlığı altında 7. ve 8. maddelerinde sırasıyla bilgisayarlarla ilgili sahtecilik ve dolandırıcılık fiilleri suç olarak düzenlenmiştir.

"İçerik bağlantılı suçlar" başlığı altında 9. maddede çocuk pornografisi suçu; *"Telif hakları ve benzer hakların ihlali ile ilgili suçlar"* adlı 4. başlığın altında 10. Maddede ise telif hakkının ihlaline ilişkin suçlar düzenlenmiştir.

b. Diğer Hükümler

Sözleşme'nin 2. kısmında usul hükümleri bakımından bazı ortak hükümler düzenlenmiştir. Yine sözleşmenin 3. kısmında uluslararası iş birliği başlığı altında bilişim suçlarına karşı küresel mücadeleyi güçlendirebilmek adına uluslararası iş birliği ve suçluların iadesine ilişkin hükümler bulunmaktadır. Son olarak 4. kısımda ise özel hükümler başlığı altında ise karşılıklı yardım ve taraf devletlerde 7/24 bağlantı noktalarının bulunması gerekliliğine ilişkin düzenlemeler yer almaktadır.

IV. BİLİŞİM SİSTEMİNE VE SİSTEMDEKİ VERİLERE KARŞI SUÇLARIN TEMEL ÖZELLİKLERİ

Bilişim sistemine ve sistemdeki verilere karşı suçların diğer suçlara nazaran birtakım farklı özellikleri bulunmaktadır. Bu özellikler aslında bilişim sistemlerinin suça farklı bir pencere açmasından kaynaklanmaktadır. Gerçekten de ekran ve klavye, fiziki dünyayı sanal dünyadan bütünüyle ayırır[130]. Sanal dünyanın içinde gerçek hayattan farklı olarak bambaşka kimlikler oluşturulabilir. Yine, sanal dünyada coğrafi sınırların ötesine geçmek salise içinde mümkün olmakta, bunun için çaba sarf etmeye ihtiyaç duyulmamaktadır. Nitekim fiziki hayatta pasaport başta olmak üzere belli birtakım prosedürler olmaksızın yurtdışına çıkılamazken, sanal dünyada sınır ötesine geçebilmek için tek bir tıklama yeterlidir.

Bilişim suçlarının ortaya çıktığı ilk zamanlarda bu suçlar beyaz yaka suçu[131] (white-collar crime) olarak tanımlanmaktaydı[132]. Zira henüz bilişim sistemlerinin yeni ortaya çıktığı ve yaygınlaşmadığı bir dünyada, bu suçları işleyebilecek yegâne kişiler yalnızca bilgisayarla irtibatlı bir işte çalışan kimseler olmaktaydı[133]. Günümüzde

---

[130] **VIANO**, Emilio C., *"Cybercrime: Definition, Typology, and Criminalization",* Cybercrime, Organized Crime, and Societal Responses içinde (Ed. Emilio C. Viano), Springer Nature, Switzerland 2017, s. 3.

[131] Beyaz yaka suçları, şiddet içermeyen ve çoğunlukla suçlunun mesleği sebebiyle sahip olduğu yetkilerin ve avantajların kötüye kullanması sonucu ortaya çıkan suç kategorisidir.

[132] **ERDOĞAN,** Yavuz, *"Bilişim Sistemine Girme ve Kalma Suçu",* Dokuz Eylül Hukuk Fakültesi Dergisi, C. 12, Özel Sayı, 2010, s. 1392.; **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, C. 19, S. 62, s. 103.; YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 98.

[133] ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu,* s. 1392.

TÜİK'in 2023 verilerine göre Türkiye'de nüfusun %87'sinin[134]; 2024 Statista verilerine göre ise dünya nüfusunun ise %67'den fazlasının[135] internete erişim sağladığı, kısacası internet ve bilgisayarın günümüzde neredeyse her hanede bulunduğu göz önünde bulundurulacak olursa, bu suçların artık beyaz yaka suçları olarak adlandırılması mümkün gözükmemektedir.

İlk olarak, bilişim sistemlerinin karmaşık yapısı sayesinde faillerin kamufle olabilme ve anonim kalabilme şansları oldukça yüksektir[136]. Bilişim korsanları arasında meşhur olan *"Eğer iyi bir hackerseniz, sizi ancak diğer iyi bir hacker yakalayabilir."* sözü de esasen bilişim korsanlarının ceza muhakemesindeki geleneksel delil toplama araçlarıyla yakalanmasının imkansıza yakın olduğunun altını çizmektedir.

İkinci önemli özellik, bilişim sistemi üzerinden yapılan müdahalelerde fail ile mağdurun fiziken bulundukları yerin önemli olmamasıdır. Gerçekten fail ile mağdur mekânsal bakımdan uzakta, farklı ülkelerde hatta farklı kıtalarda olabilmektedir[137]. Zira verilerin bilgisayar ağları içinde saniyenin yarısı kadar zaman içinde nakledilebilmesi, bilişim sistemlerine ve verilere karşı suçların sınırları aşan özelliğini güçlendirmiştir[138].

---

[134] Ayrıntılı bilgi için bkz. https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2023-49407 (E.T. 01.11.2023)

[135] Ayrıntılı bilgi için bkz. https://www.statista.com/statistics/617136/digital-population-worldwide/ (E.T. 11.07.2024)

[136] **YILMAZ**, Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, B. 2, Adalet Yay., Ankara 2023, s. 117.

[137] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 87.

[138] **SIEBER**, Ulrich, *"Bilgisayar Suçluluğu" (Çev. Yener Ünver),* Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), B. 1, Seçkin Yay., Ankara 2013, s. 21.

Bir diğer önemli özellik ise, delil elde etmenin zorluğuna ilişkindir. Nitekim bilişim suçlarındaki deliller kırılgan ve uçucudur[139]. Gerçekten, bu tip suçlar dijital ortamda gerçekleşen bu suçlardaki elektronik deliller bilişim sistemlerinin karmaşık yapısı gereği hızla değişebilmekte, silinebilmekte veya kaybolabilmektedir. Öyle ki, bu suçların işlenmiş olmasına çoğu zaman tesadüf eseri rastlanmaktadır[140].

Öte yandan, küresel ağların oluşumu, failin soruşturma işlemlerini güçleştiren hatta kimi zaman imkânsız hale getiren anonim özelliği ve modern bilgisayar sisteminin yüksek karmaşık yapısı uygulamada da bilişim suçlarında muhakeme sorunlarına yol açmaktadır[141]. Bu çerçevede devletlerin adli iş birliği ve mevzuatlarında bilişim suçlarına yer vermesi hayati bir önem arz etmektedir. Emniyet Genel Müdürlüğü tarafından yayınlanan "*Kaçakçılık ve Organize Suçlarla Mücadele 2018 Raporu"* adlı Raporda bilişim suçlarının uluslararası suçluluk olgusunun en yoğun hissedildiği suçlardan biri olduğu ve bu çerçevede polisiye iş birliği ihtiyacının önemi vurgulanmıştır[142]. Almanya Federal İçişleri Bakanlığı 2011'de yayımladığı raporda, Alman Hükumet Ağı'na, çoğu diğer ülkelerin istihbarat teşkilatlarından gelen günde dört veya beş saldırı denemesi olduğunu açıklamıştır[143].

---

[139] **YETİM**, Servet, *"Bilişim Suçları ve Etkin Mücadele Yöntemleri"*, Terazi Hukuk Dergisi, C. 9, S. 95, 2014, s. 82.

[140] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 110.; CADOPPI, s. 814.

[141] SIEBER, *"Bilgisayar Suçluluğu"*, s. 21.

[142] **EMNİYET GENEL MÜDÜRLÜĞÜ**, Kaçakçılık ve Organize Suçlarla Mücadele 2018 Raporu, Eflal Matbaacılık, Ankara 2019, s. 108. İnternet Erişim: https://www.egm.gov.tr/kurumlar/egm.gov.tr/IcSite/kom/YAYINLARIMIZ/TURKCE/2018-RAPORU-TURKCE.pdf (E.T. 29.07.2023)

[143] SIEBER, *"Bilgisayar Suçluluğu",* s. 19.

Bilişim sistemine ve sistemdeki verilere karşı suçlara ilişkin bir diğer özellik, hukukçuların uygulamada bu suçlara ilişkin zorluklar yaşamasıdır. Gerçekten, hâkim ve savcıların bilişim suçlarına ilişkin teknik ve kavram bilgisine sahip olduğunu söylemek oldukça güçtür[144]. Bilişim teknolojisinin devinim halinde olan ve sürekli yenilenen terminolojisi, yargı mensuplarına yabancı kalmaktadır. Örneğin Yargıtay 17. CD bir kararında ilk derece mahkemesinin *"Sanık ... isimli şahsın ise 11 olaya karıştığının, soruşturma dosyası kapsamında toplam 43 müştekinin...Bankası hesaplarına ait internet bankacılığı şifrelerini sahte internet sitesi tasarlayarak oltalama yöntemiyle ele geçirmek suretiyle müştekilerin banka hesaplarına erişim yaparak temin ettikleri..."* şeklindeki beyanına karşın *"...müştekinin şifresinin nasıl ele geçirildiğine dair net bir beyanda bulunmadığı, oltalama yönteminden ne kastedildiğinin açıklanmadığı..."* şeklindeki ifadeleriyle *'oltalama-phishing'* tekniğinin açıklanmasını ilk derece mahkemesinden talep etmiştir[145]. Sonuç olarak, yargı mensuplarına bilişim terminolojisine ilişkin güncel ve tam donanımlı bir eğitim verilmesi gerekmektedir[146].

Bilişim sistemine ve verilere karşı suçları önlemede en etkili araçlardan biri, teknik önlemler almaktır[147]. Teknik önlemlere bilişim sistemlerinin donanım ve işletim sistemlerinin güvenliğinin artırılması, bu çerçevede sistemde etkin bir anti-virüs programının etkin olması, internet gezintilerinde zararlı olabilecek içerikler için filtreleme özelliği olan yazılımların kullanılması, e-posta adreslerinin spam kutusuna düşen maillerdeki linklerin asla açılmaması örnek gösterilebilir.

---

[144] **ÖNOK**, Murat, *"Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği"*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 19, S. 2, 2013, s. 1232, 1233.

[145] Yargıtay 17. CD., E. 2020/1675, K. 2020/3121, T. 02.03.2020. www.kazanci.com.tr (E.T. 01.08.2023)

[146] ÖNOK, s. 1233.

[147] SIEBER, *"Bilişim Suçları"*, s. 263.

Ülke düzeyinde bilişim sistemlerine ve verilere karşı suçların işlenme sıklığına ilişkin araştırmalar yapılmıştır. 2019'da açıklanan Symantec İnternet Güvenliği Tehdidi Raporu'na göre 2018 yılında gerçekleşen siber saldırılarda Çin, %24 oranla siber saldırıların en çok gerçekleştiği birinci ülkedir[148]. Çin'i takip eden ülkeler sırasıyla Amerika, Brezilya, Rusya ve Meksika'dır. Listenin 9. sırasında ise %2.6 oranla Türkiye yer almaktadır. Her ne kadar bu gibi çalışmalar bilişim suçlarının yoğun olduğu kaynak ülkeler hakkında bir fikir verse de, devletlerin bilişim suçlarıyla mücadele düzeyi, bilişim suçlarını tespit etme ve raporlama başarıları farklılık gösterdiğinden kesin bir sonuca ulaşılamamaktadır.

[148] SYMANTEC, Internet Security Threat Report, s. 54.

V. BİLİŞİM SİSTEMİNE VE VERİLERE KARŞI SUÇLARIN FAİLLERİNE VE MAĞDURLARINA İLİŞKİN DEĞERLENDİRMELER

A. FAİLE İLİŞKİN DEĞERLENDİRMELER

1. Hacker (Bilişim Korsanı) Kavramı ve Hacker Çeşitleri

a. Tanım ve Bilgiler

Bilişim sistemine ve verilere karşı suçların faillerine genel olarak "hacker" adı verilmektedir[149]. Türkçe'de bilişim korsanlığına karşılık gelen İngilizce'deki hacker ifadesi, hack sözcüğünden türemiştir. İngilizce dilinde sözlük tanımı *'kesmek veya kabaca doğramak; (birinin yolunu) kesmek*' olan hacking terimi zaman içinde değişikliğe uğrayarak *'(bilgisayar içindeki verilere) erişim elde etmek'* fiiline karşılık olarak kullanılmaya başlanmıştır[150]. Bu doğrultuda hacker, İngilizce'de *"sisteme*

[149] **YAŞAR**, Osman – **GÖKCAN**, Hasan Tahsin – **ARTUÇ**, Mustafa, Yorumlu – Uygulamalı Türk Ceza Kanunu, C. 5, B. 2, Adalet Yay., Ankara 2014, s. 7287.

[150] TAYLOR, s. 14.; **SIEBER**, Ulrich, *"Bilişiem Suçları"* (Çev. Feridun Yenisey ve Damla Zaimoğlu), Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku içinde (Ed. Feridun Yenisey, Salih Oktar, Zehra Başer Doğan), Seçkin Yay., Ankara 2021, s. 260.

müdahale eden, müdahalede bulunan, sistemi kesen" anlamlarına karşılık gelmektedir[151].

TDK'nın çevrimiçi sözlüğüne bakıldığı zaman bilişim korsanı değil, bilgisayar korsanı ifadesinin tanımının yapılmış olduğu görülmektedir. Bu ifade ise sözlükte *"Bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse"* olarak tanımlanmıştır[152].

Bilişim korsanları, sisteme müdahale ederken niyetlerine göre dört farklı kategoride sınıflandırılabilirler.

---

[151] **YAZICIOĞLU**, Yılmaz, *"Hukukumuzda TCK 243.Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, Bilişim Hukuku Konferansı (9-10 Ekim 2008), Yargıtay Başkanlığı Yay., Ankara 2008, s. 72.; YENİDÜNYA – DEĞİRMENCİ, s. 58, 59.

[152] https://sozluk.gov.tr/ (E.T. 02.08.2023) Bilgisayar korsanı ifadesi bugün yerleşik olarak kullanılmaktadır. Oysa bilişim sistemlerinin bilgisayardan daha geniş olarak bilgisayarları da içine alan ve bilgisayarlar arasında bağlantı kuran büyük bir ağ düzenini kapsayan bir terim olduğu bahsedilmişti. Bu faillerin yalnızca bilgisayarlara değil fakat bilişim ağlarına ve diğer bilişim sistemlerine girebileceği göz önünde bulundurulursa *'bilişim korsanı'* ifadesinin daha doğru olduğu görülecektir. Kaldı ki TDK da bilgisayar korsanının tanımını yaparken "*ağlar üzerinde yasal olmayan zarar verici işler*" şeklindeki ifadesiyle bu korsanların bilişim ağlarına sızabileceğini ifade etmiş, ancak her nasılsa kavramı bu fiili işleyen korsanları da kapsayan *'bilişim korsanları'* terimini kullanmaktan imtina etmiştir.

b. Bilişim Korsanı Çeşitleri

aa. Siyah Şapkalı Bilişim Korsanları

Siyah şapkalı bilişim korsanları, gelişmiş bilgisayar bilgi, beceri ve tekniklerini bilişim sistemlerine sızmak, sistem ve ağdaki verileri ele geçirmek veya bu verilere zarar vermek için kullanan kişilerdir[153].

Bu tip korsanlar genellikle sisteme zararlı yazılım yüklemek, sistemin kontrolünü ele geçirmek veya verileri elde etmek amacı doğrultusunda hareket ederler. Bu türdeki bilişim korsanlarının gerçekleştirdiği saldırıların altında kişisel tatminden eğlence arayışına, maddi kazançtan intikam duygusuna kadar çok çeşitli nedenler yatabilmektedir[154].

bb. Beyaz Şapkalı Bilişim Korsanları (Bilişim Uzmanları)

Bilişim uzmanları, sistem veya ağ düzeyindeki güvenlik açıklıklarını test etmek ve bu doğrultuda önleyici tedbirler amacıyla güvenlik duvarına saldırırlar[155]. Bu kişiler, kurum ve kuruluşlarda *'bilişim güvenliği uzmanı'* olarak nitelendirilen, şirketin yahut kuruluşun bilişim güvenliğinden sorumlu olan kişilerdirler[156].

---

[153] **KABADAYI**, Sami, *"Bilişim Sistemine Girme Suçu (TCK m. 243)"*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2021, s. 46.; MARION – TWEDE, s. 32.

[154] WILHELM, s. 14.

[155] MARION – TWEDE, s. 206.

[156] AKARSLAN, s. 109.

Öğretide bu kişiler için *beyaz şapkalı bilişim korsanı* (white hat hacker) [157] veya *etik bilişim korsanı* (ethical hacker)[158] denmekteyse de bu ifadelerin doğru olmadığı kanaatindeyim. Nitekim bilişim korsanı terimi aşağıda da görüleceği üzere bilişim sistemine yetkisiz olarak, yasal olmayan yoldan erişen kişileri ifade etmektedir. Kaldı ki 'korsan' kelimesinin TDK anlamı da *'başkalarının hakkını zor kullanarak ele geçiren kimse'* şeklindedir. Oysaki bilişim uzmanları, bilişim sistemi sahibinin izni dahilinde sisteme test girişi yapmaktadır. Bu çerçevede bu grup için etik bilişim korsanları yahut beyaz şapkalı bilişim korsanı ifadesini kullanmak kavram karmaşasına yol açabilir. Sonuç olarak bu grup için *"bilişim uzmanı"* ifadesinin kullanılmasının daha uygun olduğu kanaatindeyim.

Bilişim uzmanlarının bir bilişim sistemine veya bu sistemdeki verilere müdahale ederken bir hukuka uygunluk nedeni olarak bilişim sisteminin sahibinin rızası olduğundan, bu kişilerin eylemleri suç teşkil etmemektedir.

Bilişim uzmanlarının ekipmanları; bağlı olduğu kurum veya kuruluşun sağladığı araştırma, geliştirme ve eğitim olanaklarından, en yeni teknolojiye sahip yazılım protokollerine ve cihazlara kadar kapsamlı bir donanım ağını içerir[159]. Öyle ki bilişim uzmanları bu teknik ekipmanlar sayesinde kimi zaman bilişim korsanlarını yakalayabilmekte ve adli kolluğa teslim edebilmektedir. Bu bakımdan bilişim sistemine ve verilere müdahale suçlarının önlenmesinde ve suçluların yakalanmasında bilişim uzmanları etkin rol oynamaktadır.

---

[157] VIANO, s. 9; MARION – TWEDE, s. 206.; YILMAZ, Türk Ceza Hukuku Sisteminde Siber Suçlar, s. 25.

[158] AKARSLAN, s. 108.; MARION – TWEDE, s. 441.

[159] **WILHELM**, Thomas, Professional Penatration Testing, B. 2, Elsevier Yay., ABD 2013, s. 16.

Her ne kadar bilişim uzmanları, bilişim korsanlarına nazaran olanaklar bakımından daha avantajlı olsalar da bilişim uzmanlarının hareket alanı daha kısıtlıdır. Bilişim dünyasının karmaşık yapısı göz önünde bulundurulduğunda, gerçekleştirdikleri iyi niyetli saldırılar neticesinde sistemin çökebileceği, hatta daha da kötüsü verilerin silinebileceği göz önünde bulundurulduğunda, bilişim uzmanları sisteme veya verilere müdahale ederken kontrollü, seçici ve dikkatli olmak zorundadır[160]. Aksi takdirde bilişim sistemi sahibinin verdiği yetki sınırlarını aşarak sisteme veya verilere zarar veren bir saldırı, tipiklik oluştuğu takdirde duruma göre TCK'nın 243. maddesi veya 244. maddesindeki suçlardan birini oluşturabilecektir.

cc. Gri Şapkalı Bilişim Korsanları

Gri şapkalı bilişim korsanları, siyah şapkalı bilişim korsanları ve bilişim uzmanları arasındaki bir gruptur[161].

Güvenlik zafiyetini test etmek için sahibinin izni olmadan bilişim sistemlerine sızabilirler. Bunu yaparken sisteme veya verilere hasar verme, ele geçirme gibi maksatları yoktur[162]. Sistemin güvenlik açıklarını tespit ettiklerinde sistem sahibiyle

[160] WILHELM, s. 16.

[161] AKARSLAN, s. 109.; MARION – TWEDE, s. 441.

[162] Her ne kadar böyle bir niyetleri olmasa da faaliyetleri sonucunda dolaylı olarak sisteme ve verilere zarar verebilmektedirler. Örneğin bir grup gri şapkalı bilişim korsanı 2017 yılında Microsoft'un Windows işletim sisteminde bir güvenlik zafiyeti keşfetmiş ve bunu Microsoft'a satmak için girişimde bulunmuşlardır. Fakat ellerindeki bilgiler birtakım siyah şapkalı bilişim korsanı tarafından çalınarak İngiltere ve İskoçya'da Ulusal Sağlık Sistemi'nin çökmesine ve 99 ülkedeki 230.000 bilgisayara bulaşmasına sebep olan WannaCry adında bir fidye virüsüne dönüştürülmüştür.

iletişime geçip sistemin zayıflıklarını, bu zayıflıklara ilişkin çözüm önerilerini ve tavsiyelerini para karşılığında satabilirler[163].

Belirtmek gerekir ki, gri şapkalı bilişim korsanlarının her ne kadar sisteme ve verilere zarar verme niyeti olmasa da sisteme yetkisiz giriş yaptıkları ve bu eylemlerinin TCK'nın 243. maddesi bağlamında suç olduğu açıktır.

Gri şapkalı bilişim korsanlarının kimi zaman devletlerin istihbaratları tarafından delil elde etmek için kullanıldığı görülmektedir. Apple-FBI 2016 olayı, gri şapkalı bilişim korsanlarının FBI tarafından kullanılarak kolluk kuvvetlerine yardımcı olmak için kullanıldığı örneklerden biridir[164]. Olay, Aralık 2015'te Syed Rizwan Farook ve Tashfeen Malik San Bernardino adlı teröristlerin Kaliforniya'da 14 kişiyi öldürmesine dayanmaktadır. FBI, Farook'un iPhone'unu ele geçirse de içindeki verilere ulaşamamış, Apple de bu verileri vermeyi reddetmiştir[165]. Bunun üzerine FBI bir grup bilişim korsanıyla anlaşarak Farook'un telefonuna sızmayı başarmıştır[166]. Bu örnekte gri şapkalı bilişim korsanlarının adli kolluğa yardımcı olduğu ve delil elde etme sürecini kolaylaştırdığı görülmekteyse de şüphesiz ki delil elde etme yöntemi hukuka aykırıdır ve eylem suç olmaktan çıkmamaktadır.

[163] AKARSLAN, s. 109.

[164] MARION – TWEDE, s. 442.

[165] MARION – TWEDE, s. 442.

[166] Ayrıntılı haber için bkz. https://www.webtekno.com/fbi-teroristin-iphoneunu-900-bin-dolara-siber-guvenlik-sirketine-actirmis-h108745.html (E.T. 02.08.2023)

dd. Aktivist Bilişim Korsanı (Hacktivist)

Aktivist bilişim korsanları, esasen kötü niyetle sisteme saldırı düzenledikleri için siyah şapkalı bilişim korsanlarına benzemekle beraber sisteme sızarken güttükleri amaç sebebiyle siyah şapkalı bilişim korsanlarından ayrılmaktadır. Aktivist bilişim korsanları, bilişim sistemine veya verilere müdahale ederken bir ideolojik etki yaratma, siyasal veya sosyal bir değişim başlatma gayesi olan faillerdir[167]. Yaptıkları bu eylemler hacktivizm olarak adlandırılmaktadır. Hacktivizm genel olarak, toplumsal bir soruna (politik, siyasi, dini vs.) ilişkin olarak tepki gösterme amacıyla bilişim sistemlerinin kötüye kullanılmasıdır[168].

Bu nitelikteki eylemler, kamu gücü otoritesine sahip bir kurumun bilişim ağına bir metin ve/veya sembol içerikli bir ileti bırakma şeklinde gerçekleşebileceği gibi bu kurumların bilişim sistemleri güvenliğinin acziyetini ortaya koymak için bilişim sisteminin ele geçirildiğini duyurmak şeklinde de olabilir[169].

---

[167] Aktivist bilişim korsanları, kendi devletinin bir politikasını eleştiri amacıyla devlet kurumlarının sistemlerine saldırabilirler. Örneğin kendini sosyalist ve Marksist olarak tanımlayan RedHack Türk bilişim korsanı grubunun 2012 yılının anneler gününde devletin kadına yönelik şiddet politikalarına dikkat çekme amaçlı Aile ve Sosyal Politikalar Bakanlığı'nın bilişim ağına sızarak bu ağın ana sayfasına bir bildiri koymuştur. Buna karşılık aktivist bilişim korsanları, başka bir ülkeye ait politikayı protesto amacıyla o ülkenin devlet kurumlarının sistemlerine de saldırabilirler. Dünyaca tanınmış bilişim korsanı grubu Anonymous'un, İsrail hükumetinin Filistin topraklarını işgalini boykot etmek amaçlı 2013'ten beri 2023'teki Gazze işgali de dahil olmak üzere her yıl İsrail'in devlet kurumlarına gerçekleştirdiği bir dizi saldırı buna örnek gösterilebilir.

[168] **DEMİRKIRAN**, Pınar, *"Hacktivzm"*, Hack Kültürü ve Hacktivzm: Yeni Bir Siyaset Bilimi içinde (Der. Ali Rıza Keleş), Alternatif Bilişim Yay., İstanbul 2023, s. 28.

[169] **AKTAŞ**, Duygu Şimşek, Bilişim Teknolojilerindeki Gelişmelerin Anayasal Fonksiyonlar Üzerindeki Dönüştürücü Etkisi, On İki Levha Yay., İstanbul 2020, s. 166.; DÜLGER, s. 194.

Aktivist bilişim korsanları, bilişim sistemlerine ve verilere müdahale ederken mutlaka siyasi bir amaç doğrultusunda hareket etmek zorunda değildir. Dini, sosyolojik, felsefi başta olmak üzere mevcut olan uygulamalara karşı eylem yaparak toplumda bir değişim ve direniş başlatma gayesi güderler. Bu doğrultuda aktivist bilişim korsanları iş uygulamalarını kınamak için büyük bir şirketin sitesini tahrif etmek isteyebilirler[170]. Örneğin RedHack grubu 2012'de havacılık meslek grubundaki işçilerin grevlerine destek amacıyla THY'nin internet sitesine DDoS atakları gerçekleştirmiştir.

2. Faillerin Genel Özellikleri

Araştırmalar, bilişim sistemine ve sistemdeki verilere müdahale eden faillerin kişilik özelliklerine ilişkin birtakım ortak bulgular ortaya koymaktadır.

Amerikan öğretisinde bilişim sistemine veya verilere müdahale eden faillerin sahip oldukları motivasyonlar içsel ve dışsal olarak ikiye ayrılmıştır. İçsel motivasyonlar; öğrenme isteği, merak, meydan okuma, sisteme sızarak tatmin olma veya bir sistemi kötüye kullanmada ne kadar ileri gidilebileceğini görmek örnek olarak sıralanabilir[171]. Buna karşılık dışsal motivasyonlar; başkalarını etkilemek, bir mesaj iletmek, sisteme kasıtlı olarak zarar vermek veya intikam, öfke ya da birine zorbalık yapmak için hareket etmek şeklinde açıklanabilir[172].

[170] MARION – TWEDE, s. 205.

[171] KRANENBARG, s. 197.

[172] KRANENBARG, s. 197.; Yargıtay 12. CD., E. 2013/11510, K. 2014/2982, T. 10.02.2014 sayılı ilamında, failin katılana karşı duyduğu ilginin karşılığını alamaması sebebiyle katılanın sosyal medya hesaplarını intikam amacıyla ele geçirerek başkalarıyla konuşmalar yaptığı, katılanın onur, şeref ve

Yapılan çalışmalar da faillerin mücadeleci, rekabetçi ve zoru seven kişiliğe sahip olduklarını ortaya koymaktadır[173]. Öyle ki, bilişim korsanları bir bilişim sistemine girdikten sonra bununla yetinmeyerek her seferinde güvenlik duvarı daha güçlü, güvenlik açıkları daha az olan bilişim sistemlerine sızabilmek ve meydan okuyabilmek için yeni bir yolculuğa başlamaktadır.

Birleşik Krallık Ulusal Suç Ajansı'nın Siber Suçlarla Mücadele biriminin 2017'de yayınlamış olduğu *"Siber Suça Giden Yollar"* adlı raporunda da bilişim sistemine ve verilere müdahale eden faillerin motivasyonlarının büyük bir kısmını zor olanı başarma, kendini kanıtlama, entelektüel tatmin gibi manevi olgulardan oluştuğu; buna karşılık maddi çıkar elde etme amaçlarının düşük olduğu vurgulanmıştır[174]. Nitekim 2009 yılında yayınlanan *"The Hackers Profiling Project"* adlı raporda, 467 bilgisayar korsanıyla gerçekleştirilen çevrimiçi anketlerde bilişim korsanlarının %43'ünün ekonomik düzeyinin ortalama üstü, %39'unun ortalama olduğu belirlenmiştir[175].

Adalet Bakanlığı'nın yayınladığı 2021 yılı Adli İstatistik Raporu'nda, TCK'nın *"Bilişim Alanında Suçlar"* başlığı altındaki suçlardan herhangi birinden sanık sıfatıyla

---

saygınlığına yönelik saldırı teşkil edecek paylaşımlarda bulunduğu olay, failin dışsal motivasyonunu ortaya koymaktadır. https://karararama.yargitay.gov.tr/ (E.T. 20.08.2023)

[173] KRANENBARG, s. 198.

[174] **NATIONAL CYBER CRIME UNIT**, Pathways Into Cyber Crime Report, 2017, s. 2 vd. İnternet Erişim: https://nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file (E.T. 20.08.2023)

[175] https://www.virusbulletin.com/uploads/pdf/conference_slides/2009/Chiesa-VB2009.pdf (E.T. 20.08.2023)

yargılanan kişilerin istatistiklerine bakıldığında, suçluların %80'inden fazlasını erkeklerin oluşturduğu görülmektedir[176].

Sisteme ve verilere müdahale eden bilişim korsanlarının pek çoğu, sorgularında yaptıkları eylemlerin kendileri için yalnızca bir eğlence olarak nitelendirdiklerini, bu eylemlerin suç olabileceğini düşünmediklerini[177] ifade etmişlerdir[178].

Öğretide bu durum *"etkisizleştirme teorisi"*yle açıklamaktadır[179]. Bu teoriye göre bilişim suçu failleri hırsızlık, cinayet, cinsel saldırı gibi geleneksel suçları gerçek bir suç olarak nitelendirmekte; buna karşılık bilişim sistemlerine yetkisiz erişim, verileri ele geçirme gibi eylemleri suç olarak görmeme, bunların sonuçlarını etkisizleştirme eğilimindelerdir[180]. Nitekim Birleşik Krallık Ulusal Suç Ajansı'nın "*Siber Suça Giden Yollar"* adlı raporunda, Birleşik Krallık'taki siber suç faillerinin geleneksel suçları

---

[176] **ADALET BAKANLIĞI**, 2021 Adli İstatistik Raporu, s. 41. İnternet Erişim: https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022140538 2021HİZMETEÖZELKİTAP.pdf (E.T. 20.08.2023)

[177] https://turk-internet.com/otistik-owen-walker-1-milyon-bilgisayarlik-botnet-yonettigi-icin-tutuklandi/ (E.T. 20.08.2023)

[178] 10 binden fazla siteye yetkisiz erişen Türk bilişim korsanı T.G kendisiyle yapılan röportajda sisteme sızdığında tatmin olduğunu ve bu eyleminin suç olduğunu bilmediğini söylemiştir: *"İlk başlarda sosyal mecralarda geziyordum. Ama oralarda pek bir şey yapamadım. Daha sonra web sitelerinin alt yapısını araştırdım. Burada bir açık bulmak beni çok tatmin ediyordu; çünkü büyük bir sitenin kurucusu kendisi her şeyi yaptığını sanırken, orada açık bulmam beni tatmin ediyordu. İlk başta yabancı web siteleriyle başladım. Türkiye'de de bazen siteler önüme çıktığında açık bulduğumda uyarı olarak bir 'indeks' atıyordum. Sitelere bu şekilde uyarı veriyordum 'şu şekilde bir açığınız var' diye; ama bunun suç olduğunu bilmiyordum.."* https://www.milliyet.com.tr/gundem/10-bin-siteye-giren-kucuk-hacker-simdi-bilgisayara-elini-suremiyor-6896251 (E.T. 21.08.2023)

[179] **KIRWAN**, Gráinne – **POWER**, Andrew, Cybercrime: The Psycologhy of Online Offenders, Cambridge University Press, Cambridge 2013, s. 23.

[180] KIRWAN – POWER, s. 23.

işleme eğilimlerinin düşük olduğu tespit edilmiştir[181]. Yine bu raporda, bilişim korsanlarının bilişim sistemlerine ve verilere karşı suçları mağduru olmayan suçlar olarak nitelendirdiklerine işaret edilmiştir[182].

Bu durumun esas sebebi, geleneksel suçlarda mağdurda maddi ve gözle görülebilir zararlar meydana gelmesi ve mağdurun haklarının doğrudan ihlal edilmesidir. Öyle ki, suç failleri, bilişim sistemlerine ve verilere karşı işlenen suçlarda bireylere doğrudan zarar verilmediğine ve haklarının doğrudan ihlal edilmediğine inanmaktadırlar. Gerçekten de bilişim korsanları psikolojisi üzerine yapılan araştırmalarda korsan topluluklarının bilişim sistemine sızarak sistemin güvenlik açıklarının keşfedilmesi noktasında sistem sahibine yardımcı olduğunu düşündüklerini göstermektedir. Bu çerçevede bilişim suçu failleri, yetkisiz erişim eylemlerinin ihlal olarak nitelendirilemeyeceğine, ihlal olarak nitelendirilse dahi bu eylemin daha büyük bir iyiliğe hizmet ettiğine inanarak kendilerini modern zamanların *"Robin Hood'ları"* olarak tanımlarlar[183].

Diğer bir taraftan, bu kişilerin sosyal hayatta hak ettikleri ilgi ve değeri görmediklerini düşündüklerini ve bu sebeple bilişim sistemine ve verilere sızarak bir çeşit savunma mekanizması geliştirmek istedikleri ortaya atılmıştır[184]. Faillerin kriminolojik bakımdan *"Robin Hood Sendromu"* şeklinde tasvir edilen davranışlar sergilemelerinin bir başka sebebi de bu sebeple açıklanmıştır. Bir bilişim korsanı kendisiyle yapılan röportajda bu hususu doğrulayan şu ifadeyi kullanmıştır: *"Dostane*

[181] NATIONAL CYBER CRIME UNIT, s. 2.

[182] NATIONAL CYBER CRIME UNIT, s. 5.

[183] SELZER – OELRICH, s. 189.; KARAGÜLMEZ, s. 88, 89.

[184] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 101.; **ERMEYDAN**, Damla, Türk Ceza Hukukunda Bilişim Suçları, B. 2, Seçkin Yay., Ankara 2023, s. 73.

olmayan yetişkinler tarafından yönetilen bir sistemde gençler kendilerini güçsüz hissetmektedirler ve kendilerini savunmanın tek yolu sistemi hacklemektir."[185].

Yapılan araştırmalarda, bilişim sistemi ve verilere karşı suçların failleriyle ve Asperger Sendromu arasında bir bağlantı olduğu öne sürülmüştür[186]. Birleşik Krallık Ulusal Suç Ajansı'nın Siber Suçlarla Mücadele biriminin 2017'de yayınlamış olduğu *"Siber Suça Giden Yollar"* adlı raporunda da bu hususa dikkat çekilmiştir[187]. Asperger Sendromu, sosyal iletişim becerilerde bozukluğa, katı ve değişmeyen düşüncelere, sınırlı sayıda aktiviteye yoğunlaşan güçlü ilgiye yol açan otistik spektrum bozukluğunun alt çeşididir[188]. Bu sendromdaki kişilerin zekâ seviyelerinin ortalamanın üstünde olduğu bilinmektedir.

Her ne kadar güncel araştırmalar ışığında Asperger Sendromunun bilişim sistemine ve verilere karşı suçların failleriyle doğrudan bir bağlantısının olduğu ortaya koyulamamışsa da, Asperger sendromuna sahip ünlü pek çok bilişim korsanı vardır. ABD Ordusu ve NASA'nın sistemlerine giren Gary McKinnon, Microsoft ve Yahoo'nun sistemlerine giren Adrian Lamo, yeni bir DDoS aracı geliştirerek Cambridge Üniversitesi, Sony gibi büyük kuruluşların sitelerinin altyapısına büyük zararlar veren Adam Mudd ve 1 milyon bilgisayarı yöneterek BotNet ağı oluşturan Owen Walker gibi bilişim korsanları Asperger Sendromuna sahip olduğu bilinen bilişim korsanlarından sadece bazılarıdır.

---

[185] TAYLOR, s. 54.

[186] KIRWAN – POWER, s. 8.

[187] Rapor için bkz. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file (E.T. 22.08.2023)

[188] **DEĞER COŞKUNFIRAT**, Nesil, *"Asperger Syndrome: An Anesthetic Point of View: Review"*, Türkiye Klinikleri Anesteziyoloji Reanimasyon Dergisi, C. 12, S. 3, s. 149.

Bilişim korsanlarının pek çoğunun, bilişim korsanlarının bir arada olduğu sanal bir topluluğun üyesi olduğu bilinmektedir. Gizliliği sağlama amacıyla topluluktaki bilişim korsanı üyeler genellikle takma ad kullanmakta, topluluk üyeleri birbirinin gerçek kimliklerini bilmemekte ve bu sayede kolluk kuvvetlerine yakalanma riski azalmaktadır[189]. Kendi aralarında iletişim kurarken anlaşılması zor ve şifrelenmiş bir dil kullandıkları da bilinmektedir[190].

Göz ardı edilmemesi gereken husus, faillerin ilk zamanlarda bilgisayarı test etmeye meraklı, inatçı ve zeki genç çocuklardan bugün artık korsanlığı uzmanlık haline getiren organize yeraltı siber suç örgütü üyelerine evrilmiş olmasıdır[191]. Dolayısıyla ilk zamanlarda yalnızca bilişim sistemine girebilme, sanal dünyada bir hareketlilik oluşturabilme saikiyle sisteme sızan asosyal, hırslı ve deha gençler bugün yerini kişileri ve şirketleri mali zararlara uğratma saikiyle hareket eden ve bu alanda uzmanlaşmış örgüt üyelerine bırakmıştır. Gerçekten de, maddi çıkar amacıyla sisteme ve verilere sızanlar çoğu zaman organize olarak hareket etmektedirler[192]. Bu sebeple, bilişim sistemine ve verilere karşı suçların failleri olan bilişim korsanlarına ilişkin bir diğer özellik ise bu suçlarda iştirak oranlarının oldukça yüksek olmasıdır[193].

[189] MARION – TWEDE, s. 207.

[190] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 116.

[191] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 90.; ORTA, s. 91.

[192] AKARSLAN, s. 38.

[193] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 105; TAYLOR, 62.

B. MAĞDUR VE SUÇTAN ZARAR GÖRENLERE İLİŞKİN DEĞERLENDİRMELER

Bilişim suçu mağdurları ve suçtan zarar gören özel hukuk ve kamu hukuku tüzel kişilikleri siber saldırılara karşı pek çok kez suskun kalmayı tercih etmekte, saldırı eylemlerini savcılığa intikal ettirmemekte, bu da pek çok suçun siyah sayıda[194] kalmasına yol açmaktadır. Bu durumun sebepleri arasında özellikle kamu hukuku ve özel hukuk tüzel kişilerinin, saygınlıklarını ve müşteri portföyünü kaybetme korkusu yer almaktadır[195]. Öte yandan bu kurumların siber saldırıları savcılığa intikal ettirdiği takdirde sorumluluk ihlali sebebiyle tazminat tehdidiyle karşılaşma korkusu da suçları ihbar etmemesine yol açmaktadır. Örneğin, bilişim sistemine saldırı neticesinde müşterilerinin verileri çalınan bir şirketin müşteri verilerini korumada ihmali olduğu tespit edilirse şirket binlerce tazminat davasıyla karşı karşıya kalabilecektir.

Yine, suçtan zarar görenlerin konuyu savcılığa intikal ettirmemesindeki bir diğer neden de bilişim sistemlerinin karmaşık yapısı ve delil uçurucu özelliği sebebiyle faillerin klasik suçlardaki gibi yakalanıp gerekli cezaya çarptırılacaklarına inanmamalarıdır[196]. Esasında, bilişim suçu failleriyle özel bir mücadele sisteminin geliştirilmesi ve topluma bu güvenin verilmesiyle resmi makamlara suçun bildirilmemesindeki kaygının önüne bir nebze olsun geçilebilecektir.

---

[194] Adli kolluğa veya savcılığa bildirilmeyen, ihbar edilmeyen; kısacası gizli kalan suç ve suçlulara kriminolojide "siyah sayılar" denmektedir.

[195] **TIEDEMANN**, Klaus, *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi"* (Çev. Feridun Yenisey), İÜHFM, C. 41, S. 1-2, 1975, s. 321.; ÖNOK, s. 1235.; YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 109.; DÜLGER, s. 115.

[196] KARAGÜLMEZ, s. 62.

Suçtan zarar gören şirketler, zaman zaman bilişim sistemlerine ve/veya verilerine yetkisiz erişen kişilerin kimliğini bir şekilde tespit ettiklerinde, bu kişilere hayranlık duyup şirkette bilişim güvenliği uzmanlığı teklifinde dahi bulunmaktadır. Örneğin Amerika'da meşhur bir bilişim korsanı olan ve pek çok şirketin bilişim sistemine sızarak tahrip eden Kevin Mitnick, hapis cezası infaz edildikten sonra şirketlere bilişim uzmanı olarak danışmanlık vermeye başlamıştır.

Bilişim sistemlerine ve verilere karşı suçlar, TCK'nın "*Topluma Karşı Suçlar*" başlığı altında düzenlendiğinden, TCK sistematiği açısından bu suçların mağduru da toplum olmaktadır. Bu sebeple suçtan zarar gören kişiler suçu savcılığa intikal ettirmemekle esasen toplumun mağduriyetinin artmasına sebep olmaktadır. Suçların büyük bir kısmının siyah sayıda kalması ise bilişim korsanları topluluğunun içinde bilinen bir olguya dönüştüğünden, onları suç işlemeye daha da cesaretlendirmektedir.

Bilişim sistemleri hakkında teknik bilgiye sahip olmayan kişiler çoğunlukla sistemlerine veya verilerine gerçekleştirilen saldırının farkına varmamaktadır. Ancak bu husus, bilişim sistemlerine ve verilere karşı suçların mağdurlarının her zaman sistem hakkında teknik bilgiye sahip olmayanlar olduğu anlamına gelmemelidir. Yapılan bir araştırmada, bilişim teknikleri hakkında daha fazla bilgi sahibi olan yazılım geliştirme uzmanlarının dahi bilişim sistemine ve sistemdeki verilerine yönelik suçların mağduru oldukları ortaya konmuştur[197].

Öte yandan, araştırmaya katılan bilişim suçu mağdurlarının %75'inin internette geçirdiği sürenin günlük 5 saat ve üzeri olduğu belirlenmiştir[198]. Bu durum ise internette

[197] **FİDAN**, Serdal – **ULUDAĞ**, Buket Cansu, *"Rutin Aktiviteler Teorisi Bağlamında Dijitalleşen Dünyada Siber Suç Mağdurları"*, HABITUS Toplumbilim Dergisi, S. 4, 2023, s. 186, 187.

[198] FİDAN – ULUDAĞ, s. 187.

geçirilen sürenin artmasıyla bilişim sistemine ve verilere karşı suçların mağduru olma olasılığının da arttığını ortaya koymaktadır.

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE GİRME VEYA KALMA, SİSTEME GİRMEDEN VERİLERİ TEKNİK ARAÇLARLA İZLEME SUÇU (TCK m. 243)

I. HUKUKA AYKIRI OLARAK BİLİŞİM SİSTEMİNE GİRME VE SİSTEMDE KALMA SUÇU (TCK m. 243/1-3)

A. GENEL BİLGİLER

Bilişim sistemine ve sistemdeki verilere karşı suçlara ilişkin TCK sistematiğinde düzenlenen ilk suç, *"Bilişim sistemine girme veya sistemde kalma"* suçudur. Bu suç, TCK'nın ikinci kitabının üçüncü kısmı olan *"Topluma Karşı Suçlar"* kısmı altındaki onuncu bölümde düzenlenen *"Bilişim Alanında Suçlar"* başlığı altında 243. maddede üç fıkra halinde düzenlenmiştir.

1. fıkrada *"Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir."* şeklindeki ifadeyle suçun temel şekli düzenlenmiş bulunmaktadır.

2. fıkrada, *"Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir."* düzenlemesiyle cezada hafifletici bir sebebe yer verilmiştir.

3. fıkrada ise suçun neticesi sebebiyle ağırlaşmış haline yer verilmiştir. Buna göre *"Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."*.

765 sayılı TCK'da bilişim sistemlerinden *"Verilerin, programların veya diğer herhangi bir unsurun yetkisiz olarak ele geçirilmesi (m. 525/a)"* suç olarak düzenlenmişken, yalnızca *"bilişim sistemine girme"* veya *"sistemde kalma"* eylemlerini cezalandıran bir hüküm mevcut değildi.

"Bilişim sistemine girme veya sistemde kalma" suçu hukukumuzda ilk kez 1997 sayılı TCK ön tasarısıyla gündeme gelmiştir. Bu tasarının 347. maddesinde, Fransız Ceza Kanunu'nun 323/1. maddesinden esinlenerek *"Bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme veya orada kalma eylemleri"* suç kabul edilmiştir[199]. Bu madde, 2000 ve 2003 tarihli TCK ön tasarılarının da sırasıyla 347. ve 346. maddelerinde yer almıştır.

2003 TCK ön tasarısının Adalet Komisyonu tarafından kabul edilen metninde, *"Bilişim sistemine girme"* suçu 245. maddede düzenlenmiştir. 5237 sayılı TCK'nın meclis görüşmeleri sırasında tasarıya ilişkin değişiklik önergesi kabul edilerek tasarıda yer alan *"hukuka aykırı olarak giren veya orada kalmaya devam eden"* ibaresi, *"hukuka aykırı olarak giren ve orada kalmaya devam eden"* şeklinde değiştirilerek kanunlaştırılmıştır. Yani düzenlemenin ilk halinde, suçun maddi unsuru *"sisteme girme ve orada kalmaya devam etme"* olarak düzenlenmişti.

2016 tarihinde 6698 sayılı *"Kişisel Verilerin Korunması Kanunu (KVKK)"*nun[200] yürürlüğe girmesiyle, hüküm, tasarının ilk halindeki gibi *"sisteme girme veya orada kalmaya devam etme"* olarak değiştirilmiştir. Yapılan bu değişiklikle, Fransız Ceza Kanunu'nun 323/3. maddesi[201] ve İtalyan Ceza Kanunu'nun 615-ter maddesiyle paralellik sağlanmıştır.

---

[199] **AKBULUT**, Berrin, Bilişim Alanında Suçlar, Adalet Yay., Ankara 2017, s. 10.

[200] R.G., 07.04.2016 T., 29677 S.

[201] Yeni Fransız CK. m.323/1-1: "*Verileri otomatik işleme tabi tutmuş bir sistemin tamamına veya bir kısmına hileyle (hukuka aykırı olarak) girme veya burada kalma fiili bir sene hapis ve 100.000 Frank*

İtalyan Ceza Kanunu'nda bilişim suçları, suçun mağduru esas alınarak *"Kişilere Karşı Suçlar"* ve *"Malvarlığına Karşı Suçlar"* başlıkları altında düzenlenmiş olup ayrıca bir bilişim alanında suçlar başlığına yer verilmemiştir[202]. İtalyan Ceza Kanunu'nun 615-ter[203] maddesinde düzenlenen bilişim sistemine yetkisiz erişim suçu ise, kişilere karşı suçlar başlığı altında düzenlenmiştir[204].

Alman Ceza Kanunu'nda ise hukuka aykırı olarak sistemlere girme veya kalma fiilleri münferit olarak bir suç sayılmamış, Kanun'un 202'a maddesinde[205] verilerin hukuka aykırı olarak elde edilmesi fiili cezalandırılmıştır[206].

Belirtmek gerekir ki, suçun düzenlenmesinde 2004 tarihinde yürürlüğe giren AKSSS ve 765 sayılı TCK döneminde öğretide bu suçun düzenlenmesi gerekliliği

---

para cezasıyla cezalandırılır" Tercüme edip aktaran: YAZICIOĞLU, *"Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, s. 76

[202] **AMATO**, Astolfo Di – **FUCITO**, Federico, Criminal Law in Italy, B. 4, Wolters Kluver, United Kingdom 2020, s. 128.

[203] İtalyan CK. m. 615-ter: *"Her kim güvenlik önlemleriyle korunmakta olan bilişim veya telekomünikasyon sisteme hukuka aykırı olarak izinsiz girer veyahut kendisini böyle bir sistemin dışında tutma hakkına sahip bir kimsenin açık veya zımni rızası hilafına kalırsa üç seneye kadar ağır hapis cezasıyla cezalandırılır."*

[204] AMATO – FUCITO, s. 128.

[205] *"Her kim yetkisi olmaksızın kendisinin bilgisine sunulmuş olmayan ve hak sahibi olmayanların girişine karşı özel olarak korunmuş olan verileri bu korumayı aşarak kendisine veya bir başkasına giriş yapma olanağı sağlarsa 3 yıla kadar hapis cezası veya adli para cezası ile cezalandırılır."* YAZICIOĞLU, *"Hukukumuzda TCK'nın 243'üncü Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, s. 78

[206] **GERKCE**, Marko, *"Siber Suç Sözleşmesi ile 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve Kusurları" (*Çev. Kerem Öz), Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), Seçkin Yay., Ankara 2013, s. 110.; ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1389, 1390.

yönündeki eleştirilerin[207] katkısı olmuştur. Nitekim 765 sayılı TCK'da *"verilerin ele geçirilmesi (m. 525/a-1)"* suçunun düzenleniş biçimine yönelik getirilen en ciddi eleştirilerden biri, failin verileri ele geçirmeden de bilişim sistemine hukuka aykırı erişmesi fiilinin cezalandırılamamasına yönelikti[208].

Söz konusu düzenlemeyle birlikte öğretideki haklı eleştiriler dikkate alınmış ve taraf olunan AKSSS'nin 2. maddesinde düzenlenen *"Yetkisiz erişim"* hükmüyle paralellik sağlanmıştır. İlgili hükümde taraf devletlere hukuka aykırı olarak sisteme girme fiilinin suç olarak düzenlenmesi yükümlülüğü getirilmiştir. Ancak belirtmek gerekir ki hukuka aykırı olarak sistemde kalma fiilinden AKSSS'nin 2. maddesinde bahsedilmemiştir. Hal böyle olmakla beraber, maddede taraf devletlerin iç hukukta yetkisiz erişim suçunu düzenlerken birtakım ek unsurlar getirilebileceğine değinilmiştir. Bu çerçevede Kanunumuzda hukuka aykırı olarak sistemde kalma fiili AKSSS'nin 2. maddesine aykırılık oluşturmaz.

B. SUÇA İLİŞKİN ÖN AÇIKLAMALAR

1. Suçun Hukuki Konusu

TCK'nın *"Özel Hükümler"* başlıklı 2. kitabında suçlar önce kısımlar halinde *"mağdur"* kriterine göre tasnif edilmekte, bunun alt ayrımı olan bölümlerde ilgili suçlar

[207] Örneğin ÜNVER, *"Bir kimsenin kasten ve haksız biçimde bir bilgisayar sisteminin tamamına veya bir kısmına erişmesini cezalandıran bir suç tipi düzenlenmelidir"* demiştir. (**ÜNVER,** Yener, *"Türk Ceza Kanunu'nun ve Ceza Kanunu (2000) Tasarısının İnternet Açısından Değerlendirilmesi"*, s. 91).

[208] TEZCAN – ERDEM – ÖNOK, s. 1164.

ise hukuki konuya göre sınıflandırılmaktadır[209]. Suçun hukuki konusu, suçun oluşabilmesi için ihlal edilen ve hukuken korunan menfaattir[210]. Her suç mutlaka bir hukuki menfaati korur.

AKSSS Açıklayıcı Raporu'nun[211] 44. paragrafında, *"Yasadışı erişim suçuyla kuruluşların ve bireylerin bilişim sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme çıkarlarının koruma altına alındığı"* belirtilmiştir.

Suçun koruduğu hukuki değere ilişkin öğretide farklı görüşlere rastlanmaktadır. Fazlasıyla taraftar bulan bir görüşe göre, suçla korunmak istenen değer karma nitelikte yani birden fazladır[212].

Karma nitelik görüşünü savunan birtakım yazarlara göre, suçun düzenlenmesiyle özel hayatın gizliliği ve haberleşmenin gizliliği gibi hukuki değerler korunmak istenmiş olsa da suçun düzenlendiği yer bakımından korunmak istenen öncelikli değer bilişim sisteminin bütünlüğü ve güvenliğidir[213].[214].

---

[209] YALÇIN – KÖPRÜLÜ, s. 156.

[210] YALÇIN – KÖPRÜLÜ, s. 156.

[211] Rapor için bkz. https://rm.coe.int/16800cce5b (E.T. 05.09.2023)

[212] TEZCAN – ERDEM – ÖNOK, s. 1164, 1165.; ÖZBEK – DOĞAN – BACAKSIZ, s. 982, 983.

[213] Suçla korunan hukuksal değerin ancak bireylere ait olabileceğini, eşyaların ve objelerin suçla korunan bir hukuksal değerin sahibi olamayacağını düşünen öğretideki bir görüşe göre 243. maddede düzenlenen suçlarla korunan hukuksal değer bilişim sisteminin güvenliği şeklinde değil, bireylerin bilişim sistemlerine olan güvenleri olarak ifade edilmelidir. Bkz. BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 233, 234.

[214] Bu kapsamda öğretide, bilişim sistemi güvenliğinin kamu düzeninin önceliği olduğu, bu sebeple bilişim sistemlerine ve verilere karşı suçların bilişim alanında suçlar adıyla yeni bir başlıkla düzenlenmemesi gerektiği ve fakat topluma karşı suçlar kısmında ayrıca yer alan *'kamunun güvenine*

Suçun koruduğu hukuki değerin karma nitelikli olduğunu düşünen diğer birtakım yazarlara göre ise korunan öncelikli hak özel hayatın gizliliği olup bilişim sisteminin güvenliği ve diğer birtakım değerler ikincil niteliktedir[215]. Bu görüşe göre sistemde bilişim sisteminin sahibinin özel hayatına ilişkin birtakım verilerin bulunacağı göz önünde bulundurulursa, hukuka aykırı sisteme girme yahut orada kalma fiiliyle öncelikli olarak özel hayatın gizliliği hakkı ihlal edilmiş bulunmaktadır.

Karma görüşü savunan yazarlar, anılan suçun düzenlenmesiyle haberleşme özgürlüğünün de korunduğunu ifade etmektedir. Buna göre, günümüzde bilişim sistemlerinin etkin bir haberleşme ağı olarak kullanıldığı göz önünde bulundurulacak olursa, failin sisteme girerek kişiler arasındaki iletişimi öğrenmesi haberleşmenin gizliliği hakkını da ihlal etmektedir.

Yine karma görüşü savunan yazarlardan bazıları bu suçun başka suçların işlenebilmesi bakımından bir ön suç niteliği taşıdığı, dolayısıyla bilişim sistemine girme suçunun *"reato ostacolo"* yani *"engelleme suçu"* işlevi gördüğüne ilişkin bir değerlendirmede bulunmaktadır[216]. Bu doğrultuda korunmak istenen bir diğer hukuki değerin de olası başka suç işlenmesinin önüne geçilmesi olduğu söylenmektedir.

Öğretideki diğer bir görüşe göre, suçun koruduğu hukuki değer karma nitelikli değildir. Bu görüşü savunan yazarlara göre korunan hukuki değer yalnızca bilişim

---

karşı suçlar' başlığı altında kategorize edilmesinin daha doğru olacağı belirtilmiştir. Bkz. **HAFIZOĞULLARI**, Zeki – **GÜNGÖR**, Devrim, *"Türk Ceza Hukukunda Suçların Tasnifi"*, TBB Dergisi, S. 69, 2007, s. 33.

[215] ERDAĞ, s. 279.; YILMAZ, Türk Ceza Hukuku Sisteminde Siber Suçlar, s. 194.

[216] Görüş için bkz. ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1371.; YAZICIOĞLU, *"Hukukumuzda TCK'nun 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, s. 81.

sisteminin güvenliğidir ve bu kamusal değer, diğer ferdi değerleri (özel hayatın gizliliği ve haberleşmenin gizliliği, kullanıcı ve sistem sahibinin çıkarları) de ihtiva eder[217].

Gerçekten, bilişim sisteminin bütünlüğü ve güvenliği, bilişim teknolojisinde son 15 yılda yaşanan gelişmeler ve bu sistemlerin insan hayatının vazgeçilmez bir parçası olmasıyla, günümüzde başlı başına hukuki korunmanın hedefi olmaya layık bir menfaattir. Nitekim Alman Federal Anayasa Mahkemesi 2008 tarihindeki bir kararında[218] ilk defa bilişim sistemlerinin gizliliği ve bütünlüğü hakkından bahsetmiştir[219]. Mahkeme bu hakkın her ne kadar Anayasa'da yer almasa da *'kişiliği serbestçe geliştirme hakkının'* özel bir görünümü olduğunu belirtmiştir[220]. Bilişim sistemlerinin bütünlüğü, güvenliği ve gizliliği hakkı; esasında sistemlerin ve verilerin hızlı ve düzgün kullanabilirliğinin garantisini teşkil etmektedir[221].

---

[217] DÜLGER, s. 260, 261. Benzer yönde bkz. **OKUYUCU ERGÜN**, Güneş, Banka veya Kredi Kartlarının Kötüye Kullanılması, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 19, S. 2, 2013, s. 1067.

[218] BVerfG 1 BvR 370/07.

[219] SIEBER, *"Bilişim Suçları",* s. 266.; **TEPE**, İlker, *"Yeni Bir Temel Hak Olarak 'Bilişim Teknolojisi Sistemlerinin Gizliliği ve Bütünlüğünün Korunması Hakkı' – Alman Federal Mahkemesi'nin 'Online Arama' Kararının Sistematik Analizi"*, Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), Seçkin Yay., Ankara 2013, s. 398.

[220] Ayrıntılı bilgi için bkz. TEPE, s. 399 vd.

[221] **PICOTTI**, Lorenzo, *"Sistemica dei reati informatici, technice di formulazione legislativa e beni giurdici tutelati"*, Il Diritto Penale Dell'Informatica Nell'epoca di Internet içinde (Ed. Lorenzo Picotti), CEDAM, Padova 2004, s. 70.

2. Suçun Maddi Konusu

Suçun konusu, kanunda belirtilen hareketin yöneldiği bir kimse veya şey, kısacası varlıktır[222]. Ancak bu ifadeden failin fiziki hareketinin üzerinde gerçekleştiği her kişi veya eşya anlaşılmamalıdır. Suçun maddi konusu, yalnızca suç normunda yapılan tanımda söz konusu olan kişi veya eşyadır[223].

243. maddenin 1. fıkrasında düzenlenen suçun konusu hukuka aykırı olarak içine girilen veya orada kalmaya devam edilen bilişim sisteminin yazılım unsurudur. Bu noktada, suçun maddi konusu bilişim sisteminin donanımını oluşturan ve gözle görülebilen bilişim sistemlerinin fiziki unsurları değil, bunların içindeki soyut unsurlardır.

Öğretide birtakım yazarlar kişinin dizüstü bilgisayarının veya Emniyet Müdürlüğünün kullandığı bilişim sisteminin bu suçun konusunu oluşturabileceği kanaatindedirler[224]. Ancak açıklandığı üzere, suçun konusu normda tanımlanan *'bilişim sistemi'* olup ferdi olarak hareketin üzerinde gerçekleştiği her bilişim sisteminin suçun konusu olması mümkün değildir. Bu sebeple ben bu görüşe katılmıyorum.

243. maddenin 2. fıkrasında düzenlenen cezada indirim sebebine ilişkin suçun maddi konusu bedeli karşılığında yararlanılan bilişim sistemlerinin yazılım unsuru; 3.

---

[222] **HAFIZOĞULLARI**, Zeki – **ÖZEN**, Muharrem, Türk Ceza Hukuku Genel Hükümler, B. 13, US-A Yay., Ankara 2021, s. 209.

[223] **TOROSLU**, Nevzat – **TOROSLU**, Haluk, Ceza Hukuku Genel Hükümler, B. 26, Savaş Yay., Ankara 2021, s. 111.

[224] YILMAZ, Türk Ceza Hukuku Sisteminde Siber Suçlar, s. 196.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 58.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 147.

fıkrada düzenlenen suçun neticesi sebebiyle ağırlaşmış halinin maddi konusu ise bilişim sisteminin içerdiği verilerdir.

Suçun oluşabilmesi bakımından mutlaka bilişim sistemine girişi engelleyici bir tedbirin (örneğin bir şifrenin) varlığı gerekmez; önemli olan isteyen herkesin dilediği zaman giremeyeceği bir sistemin mevcudiyetidir[225]. Belirtmek gerekir ki bilişim sisteminin tamamen kamu erişimine açık olması durumunda, bilişim sistemine girilmesi fiili suç oluşturmayacaktır[226].

3. Fail

Fail, kanunda suç olarak öngörülen bir fiili işleyen gerçek kişidir[227]. Her suçun muhakkak bir faili vardır ve bu fail muhakkak insandır. Tüzel kişiler suçun faili olamazlar.

Kanuni tanımında belli bir özelliğe sahip kişilerin fail olabileceği belirtilen suçlara *özgü (mahsus) suç;* kanunda herkes tarafından işlenebileceği *'her kim', 'kişi', 'kimse'* vb. gibi ifadelerle belirtilmiş olan suçlara *genel suç* denilmektedir[228]. TCK m.

[225] TEZCAN – ERDEM – ÖNOK, s. 1167.; **KOCA**, Mahmut – **ÜZÜLMEZ**, İlhan, Türk Ceza Hukuku Özel Hükümler, B. 7, Adalet Yay., Ankara 2020.; s. 900, 901.; Karşı yönde bkz. ÖZBEK – DOĞAN – BACAKSIZ, s. 986.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 133.; YAŞAR – GÖKCAN – ARTUÇ, s. 7296.

[226] DÜLGER**,** s. 286.

[227] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 373.

[228] **KOCA**, Mahmut – **ÜZÜLMEZ**, İlhan, Türk Ceza Hukuku Genel Hükümler, B. 15, Seçkin Yay., Ankara 2022, s. 115.; **BAŞ**, Eylem, Ceza Hukukunda Fail ve Mağdur, Seçkin Yay., Ankara 2021, s. 119, 120.

243/1 metninde fail için *'kimse'* tabiri kullanıldığından suçun faili herkes olabilecektir, yani suç genel bir suçtur.

Bilişim sistemlerine hukuka aykırı olarak giren ve/veya orada kalmaya devam eden gerçek kişi bu suçun failidir.

TCK'nın 20. maddesine göre, yalnızca gerçek kişiler fail olabileceğinden, tüzel kişilik bünyesinde çalışan bir kişinin bu suçu işlemesi halinde fail tüzel kişi değil, hareketi gerçekleştiren gerçek kişi olacaktır. Ancak TCK m. 246 gereğince bu suçun işlenmesiyle tüzel kişi lehine bir haksız yarar sağlanmışsa, tüzel kişiler hakkında güvenlik tedbiri uygulanacaktır.

Öğretide bilişim sisteminin güvenlik duvarının aşılarak sisteme girilebilmesi için belli bir düzeyde bilgi ve donanımına sahip olmak gerektiği ifade edilmektedir[229]. Bu görüşün haklılık payı olsa da bilişim sistemlerine dair ortalama düzeyde bilgiye sahip kişilerin de bu suçu işleyebileceği unutulmamalıdır[230]. Örneğin mağdurun Facebook veya Instagram gibi sosyal medya hesaplarına saldırgan tarafından brute-force (rastgele deneme) yöntemiyle şifre kırıcı saldırılar neticesinde erişilebilmesi mümkündür. Kaldı ki bugünün çağında, bu alana ilgi duyan kişiler bir bilişim sistemine girmek için oturduğu yerden sisteme erişmek için kullanılan programları kolaylıkla elde edebilir. Dolayısıyla basit bir bilgiye sahip kişilerin dahi bu suçu işleyebilme olanağı gittikçe artmaktadır.

---

[229] APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 56.; **KAYAER**, Nebahat, *"Türk Hukukunda Bilişim Sistemine Girme Suçu (TCK m. 243)"*, CHD, C. 14, S. 39, s. 96.; ERDOĞAN**,** *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1393.; KURT, s. 241.; AKBULUT, Bilişim Alanında Suçlar, s. 17.; TEZCAN – ERDEM – ÖNOK, s. 1165.; AKARSLAN, s. 44.; TAŞKIN, s. 23.

[230] **İHTİYAROĞLU**, Uğur, *"Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi"*, HÜHFD, C. 10, S. 2, 2020, s. 412, 413.

4. Mağdur

Suçun mağduru, suç tanımıyla korunan hak ve menfaatin sahibi olan kişidir[231]. Suçtan zarar gören kişi ile mağdur kavramı birbirlerinden farklıdır. Her ne kadar çoğu zaman suçtan zarar görenle mağdur aynı kişi olsa da suçtan zarar gören kavramı daha kapsamlıdır. Buna göre, suçun işlenmesiyle hukuki menfaatleri ve çıkarları dolaylı veya doğrudan zarar gören kişiler suçtan zarar gören olarak kabul edilir[232]. Öğretide bu suçun mağdurunun kim olduğu yönünde bir tartışma bulunmaktadır.

Ele alınacak ilk görüş, bu suçun mağdurunun kişiler olduğunu kabul etmektedir. Bu görüş de kendi içinde, tüzel kişilerin suçun mağduru olarak kabul edilip edilemeyeceğine ilişkin olarak ikiye ayrılmaktadır.

Tüzel kişilerin de mağdur olabileceğini kabul eden görüşe göre[233] bu suçun mağduru gerçek kişi ve/veya tüzel kişi olabilecektir. Nitekim bilişim sistemine girilmesi veya sistemde kalınması sonucunda birtakım hak ve menfaatlerden yoksun kalan kişi çoğu zaman tüzel kişi olmaktadır[234]. Bir bankanın bilişim sistemine hukuka aykırı giriş yapılarak müşterilerin profillerinin incelenmesi eyleminde, profili görüntülenen her bir müşteriyle birlikte "banka tüzel kişiliği" de mağdur olarak kabul edilmelidir[235].

---

[231] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 208.

[232] BAŞ, s. 804, 805.

[233] ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1394, 1395.; KURT, s. 242.; GÜL**,** s. 95.; KAYAER, s. 97.

[234] ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1394.

[235] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 145.

Suçun mağdurunun yalnızca gerçek kişiler olabileceğini kabul eden diğer görüşe[236] göre; menfaati ihlal edilen tüzel kişiler bu suç bakımından zarar gören sıfatını haiz olabilecek, fakat mağdur olarak adlandırılamayacaklardır. Yargıtay 8. CD., tüzel kişilerin mağdur olup olmayacağı hususunda bu görüşe paralel olarak, şirketin bilişim sistemine yetkisiz giriş yapılmasına ilişkin önüne gelen bir uyuşmazlıkta[237], şirketi *'suçtan zarar gören'* olarak tarif etmiştir. Ancak dairenin son yıllarda, farklı suçlara ilişkin uyuşmazlıklarda tüzel kişileri mağdur olarak nitelendirdiği istikrarlı içtihatlarıyla birlikte görüşünün farklılaştığını söylemek mümkündür[238].

Bu görüşü savunan yazarlar içinde de suçun mağduru olan gerçek kişinin kim olduğuna ilişkin de görüş ayrılıkları mevcuttur. Öğretide, gerçek kişi mağduru, bilişim

---

[236] **MAHMUTOĞLU**, Fatih Selami, *"Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi"*, İÜHFM, C. LXXI, S. 1, 2013, s. 860.; **ARTUK**, Mehmet Emin – **GÖKCEN**, Ahmet – **YENİDÜNYA**, Ahmet Caner, Türk Ceza Hukuku Özel Hükümler, B. 13, Adalet Yay., Ankara 2013, s. 834.; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, B. 7, Adalet Yay., Ankara 2020., s. 896.; İHTİYAROĞLU, s. 415.; DÜLGER, s. 270.; AKBULUT, Bilişim Alanında Suçlar, s. 19.; BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 235.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 57.

[237] E. 2013/2702, K. 2014/7400, T. 25.3.2014. https://karararama.yargitay.gov.tr/ (E.T. (E.T. 30.08.2023). Benzer yönde bkz. 8. CD. E. 2018/12187, K. 2020/10603, T. 27.02.2020 https://karararama.yargitay.gov.tr/ (E.T. 30.08.2023)

[238] 8. CD., E. 2018/2494, K. 2018/2967, T. 19.03.2018. https://karararama.yargitay.gov.tr/ (E.T. 31.08.2023); 8. CD., E. 2021/10489, K. 2021/20467, T. 08.11.2021. https://karararama.yargitay.gov.tr/ (E.T. 31.08.2023); 8. CD., E. 2021/12807, K. 2022/5727, T. 06.04.2022. https://karararama.yargitay.gov.tr/ (E.T. 31.08.2023).

sisteminin güvenliğinin ihlal edilmesiyle çıkarı zedelenen kişi[239] veya bilişim sisteminin kullanıcısı veya maliki olan kişi[240] şeklinde tanımlayan farklı fikirler bulunmaktadır.

Suçun mağdurunun, gerçek veya tüzel kişi ayırt edilmeksizin *"kişi"* olamayacağını savunan bir diğer görüş[241] de, argümanını Kanun'un sistematiğine dayandırmaktadır. Buna göre, ilgili suç Kanun sistematiğinde *"Kişilere Karşı Suçlar"* başlığı altında değil, "*Topluma Karşı Suçlar"* başlığı altında düzenlendiğinden, suçun mağduru kamu idaresidir. Nitekim TCK'nın *"Özel Hükümler"* başlıklı ikinci kitabında suçlar önce kısımlar halinde *'mağdur'* kriterine göre tasnif edilmektedir[242]. Kaldı ki mantıken güvenli bir bilişim ortamı sağlamanın kamu düzeninin önceliği olduğu göz önünde bulundurulursa, güvenliği ihlal edici bir eylem olan bilişim sistemlerine hukuka aykırı giriş suçunun birincil mağduru kamu idaresidir[243]. Anlatılanların ışığında, bu görüş kabul edildiğinde bilişim sistemine hukuka aykırı olarak girilmesinden menfaati ihlal edilenler yalnızca suçtan zarar gören olabilecektir.

---

[239] DÜLGER, s. 270.; PARLAR – ÖZTÜRK, s. 26.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 57.

[240] BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 235.

[241] **HAFIZOĞULLARI,** Zeki – **ÖZEN,** Muharrem, Topluma Karşı Suçlar, B. 4, US-A Yayıncılık, Ankara 2022, s. 484.; TEZCAN – ERDEM – ÖNOK, s. 1165, 1166. Bu görüşe benzer yönde yazarlar da kanunun sistematiği sebebiyle mağdurun gerçek kişi olarak kabul edilemeyeceğini düşünmektedir.

[242] **YALÇIN,** Türkân – **KÖPRÜLÜ,** Timuçin, Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları, B. 9, Savaş Yay., Ankara 2022, s. 156.

[243] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 484.

C. SUÇUN UNSURLARI

1. Maddi Unsur

a. Hareket

Fiil genelde hareket, netice ve bu iki terim arasında neden sonuç ilişkisini ifade eden nedensellik bağından ibarettir[244]. Bazı suçlar neticesiz suç (salt hareket suçu) olduğu için netice, fiilin zorunlu bir unsuru değildir[245]. Bununla beraber, hareketsiz suç olmayacağından hareket suçun zorunlu unsurudur. Hareket ise vücudun algılanabilir bir devinimi olarak ifade edilebilir[246].

Düzenlemeye göre anılan suçun oluşabilmesi için gereken fiil, bir bilişim sistemine hukuka aykırı şekilde girmek veya orada kalmaktır[247]. Suçun icrası birden fazla alternatif hareketle gerçekleştirilebileceğinden, suç, hareket unsuru bakımından seçimlik hareketlidir. Seçimlik hareketli suçlarda seçimlik hareketlerin hepsi yapılmış olsa dahi tek bir suç oluşacağından, bir bilişim sistemine girilerek o sistemde bir müddet kalınması halinde tek bir suçun varlığından söz edilecektir.

Kanunun ilk halinde fiil, "hukuka aykırı olarak girme *ve* orada kalmaya devam etme" olmak üzere birden fazla hareketli bir suç olarak düzenlenmişti. Daha sonra 6698

[244] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 168.

[245] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 168.

[246] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 168.

[247] DÜLGER, s. 251.

sayılı KVKK'nın 30. maddesinde yapılan değişiklikte *"ve"* ibaresi *"veya"* ile değiştirilerek hüküm 2003 tarihli TCK ön tasarısındaki düzenlenen haline geri getirilmiştir. Bu çerçevede, suçun meydana gelebilmesi bakımından hukuka aykırı girme ve orada kalma hareketleri bir bütün halinde aranmamakta, bunların bir tanesinin gerçekleşmesiyle suç meydana gelmiş bulunmaktadır. Ancak değişiklikten sonra dahi Yargıtay 8. ve 15. CD., pek çok kararında söz konusu suçu *"bilişim sistemine girme ve orada kalma suçu"* şeklinde hatalı nitelendirmektedir[248].

Suçun maddi unsuru dikkate alındığında, öğretide madde başlığının *"Bilişim sistemine girme"* olmasının suçun başlığının madde içeriğini karşılamada yeterli olmadığına yönelik eleştirilere[249] yol açmıştır. Özellikle maddeye 4. fıkra eklenmesiyle birlikte, maddenin başlığı kapsayıcı olmaktan daha da uzaklaşmıştır. Nitekim 6698 sayılı Kanunla TCK'ya eklenen bu suç, bilişim sistemine girilmeksizin sistemdeki veri akışının teknik araçlarla izlenmesi fiiliyle meydana gelmektedir. Kanaatimce, olması gereken 6698 sayılı Kanunla suç başlığının *"Bilişim sistemine girme veya sistemde kalma"* şeklinde değiştirilmesi ve bilişim sistemine girilmeksizin sistemdeki veri akışının teknik araçlarla izlenmesi suçunun farklı bir maddede münferit olarak düzenlenmesiydi.

Suç neticesiz bir suçtur[250]. Hükmün gerekçesinde de "*Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir."* denilerek ayrıca bir

---

[248] 15. CD., E. 2017/3543, K. 2018/7723, T. 07.11.2018. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023); 15. CD., E. 2017/33739, K. 2019/7428, T. 02.07.2019. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023); 8. CD., E. 2017/13047, K. 2019/5782, T. 29.04.2019. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023)

[249] ÖZBEK – DOĞAN – BACAKSIZ, s. 985.

[250] Aynı yönde bkz. KARAGÜLMEZ**,** s. 205.

neticenin gerçekleşmesinin aranmadığı vurgulanmıştır. Bu bakımdan seçimlik hareketlerden birinin gerçekleşmesiyle suç tamamlanacaktır[251].

Suç normuna bakıldığında, bilişim sistemine girme veya sistemde kalma neticesinde bir zararın ortaya çıkması aranmadığından, suç *'tehlike suçu'* olarak kabul edilmelidir[252].

aa. Bilişim Sistemine Girmek

Kanun metinde düzenlenen ilk hareket, bilişim sistemine girmektir. Girmek eylemi, TDK'nın güncel sözlüğünde *"Dışarıdan içeriye geçmek, erişmek, ulaşmak"* şeklinde tanımlanmıştır.

Öğretide, metinde yer alan *'girme'* fiili yerine *'erişme'* fiilinin tercih edilmesinin daha doğru olacağına yönelik bir görüş[253] mevcuttur. Kanaatimce de *girmek* fiili daha çok fiziksel bir yer değiştirmeyi çağrıştırmaktadır. Bunun yerine *erişmek* ifadesinin tercih edilmesi hem bilişim alanında bu ifadenin daha çok kullanılması, hem de uluslararası sözleşmelerle uyum sağlanması bakımından daha doğru olurdu. Gerçekten, AKSSS'nin 2. maddesinde de Türkçe'de erişme fiiline tekabül eden İngilizce *"access"* kelimesine yer verilmiştir.

[251] ERDAĞ, s. 283.

[252] TAŞKIN, Bilişim Suçları, s. 26.; MAHMUTOĞLU, *"Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi"*, s. 861.

[253] AKBULUT, Bilişim Alanında Suçlar, s. 25.; ÖZBEK – DOĞAN – BACAKSIZ, s. 986.; DÜLGER, s. 273, 274.; ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu"*, s. 1374.; ORTA, s. 113.

Bilişim sistemine girmek, sistemin yazılımının[254] tamamına veya bir bölümüne ulaşmak, içeriğine dahil olmak anlamı taşır[255]. Yargıtay 8. CD., yerleşik uygulamasında bilişim sistemine girme fiilini, *"bilişim sisteminde bulunan verilerin bir kısmına yahut tamamına, fiziken veya uzaktan başka bir cihaz yoluyla erişim sağlamak"* olarak tanımlamaktadır[256].

Yargıtay'ın yerleşik içtihadı, *girme* hareketinin *"bir kimsenin bilgisayarının açılarak içindeki verilere erişebilme imkânı sağlanması veya bir ağ, program veya yazılım yardımıyla bilişim sisteminde oturum açılması yoluyla olabileceği"* şeklindedir[257]. Yine Yargıtay, girme fiili açısından iletişimin kablolu veya kablosuz

[254] Bu çerçevede, bilgisayarın fiziki bileşenini oluşturan donanımlarının açılarak bilgisayarın içine fiziken girilmesi, yahut yalnızca bilişim sistemiyle donatılmış bir odaya adım atılması bilişim sistemine girme hareketini oluşturmaz.

[255] **AKSOY RETORNAZ**, Eylem, *"Ceza Hukuku Perspektifinden Blokzincir"*, Gelişen Teknolojiler ve Hukuk I - Blokzincir içinde (Ed. Eylem Aksoy Retornaz – Osman Gazi Güçlütürk), On İki Levha Yay., İstanbul 2020, s. 306.; ERDEM – TEZCAN – ÖNOK, s. 1167.; AKBULUT, Bilişim Alanında Suçlar, s. 27.; BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 238.

[256] Bkz. E. 2017/21566, K. 2020/13171, T. 11.6.2020. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023); E. 2019/26683, K. 2022/6848, T. 10.5.2022. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023); E. 2014/19342, K. 2015/2322, T. 3.2.2015. https://karararama.yargitay.gov.tr/ (E.T. 06.09.2023).

[257] 8. CD., E. 2014/21961, K. 2015/12125, T. 18.2.2015. https://karararama.yargitay.gov.tr/ (E.T. 07.09.2023); 8. CD., E. 2017/7105, K. 2017/13811, T. 6.12.2017. https://karararama.yargitay.gov.tr/ (E.T. 07.09.2023); 8. CD., E. 2018/1078, K. 2018/2485, T. 8.3.2018. https://karararama.yargitay.gov.tr/ https://karararama.yargitay.gov.tr/ (E.T. 07.09.2023).

olması, mesafenin yakın veya uzak olması gibi durumların önemli olmadığını belirtmektedir[258].

Bilişim sistemine girme hareketi, çeşitli *modus operandiler* ile gerçekleşebilir. Oltalama gibi sosyal mühendislik teknikleri kullanılarak veya şifre kırıcı saldırılar aracılığıyla bilişim sistemine yetkisiz erişmek mümkündür. Yine, sistemi kullanmaya yetkili kişilere ait erişim kodları (şifre, parmak izi vs) elde edilerek sistemde oturum açılabilecektir[259].

Bunun dışında, truva atları, kurtçuklar (worms), mantık bombaları gibi zararlı yazılımlar aracılığıyla sisteme erişim sağlanabilmektedir. Şüphesiz ki bilişim alanında yaşanan gelişmeler arttıkça bu gelişimleri kötüye kullanmayı amaçlayan kişiler ve bunların sisteme müdahale ederken başvurduğu teknikler de artacağı için, zararlı yazılımların sayılarak tüketilmesi mümkün değildir. Yargıtay 8. CD de, sisteme hukuka aykırı erişim olanağı veren yazılımları örnek olarak saymış[260], bunları sınırlamamıştır.

Zararlı yazılımların nihai amacının sisteme ve verilere müdahale etmek, bozmak, değiştirmek olduğu unutulmamalıdır. Bu çerçevede, zararlı yazılımlar aracılığıyla yalnızca sisteme giriş sağlanmışsa *"Bilişim sistemine girme veya sistemde kalma suçu"* oluşacak; buna karşılık sisteme veya verilere müdahale edilmişse şartlara göre TCK m. 244'te düzenlenen suçtan bahsedilebilecektir.

---

[258] 8. CD., E. 2018/1078, K. 2018/2485, T. 08.03.2018. https://karararama.yargitay.gov.tr/ (E.T. 08.09.2023)

[259] KETİZMEN, s. 103.

[260] *"Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi, kullanılarak veya sistemin açık kapıları zorlanarak giriş yapılabilir."* 8. CD., E. 2018/1078, K. 2018/2485, T. 8.3.2018. https://karararama.yargitay.gov.tr/ (E.T. 12.09.2023)

Yalnızca spam gönderme, bilişim sistemine girme niteliği taşımaz[261]. Konuya ilişkin olarak Yargıtay 8. CD'nin *"bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden bu durumun girme kapsamında düşünülemeyeceği"* yönünde yerleşik içtihadı bulunmaktadır. Ancak, gönderilen postalar içinde bilişim sistemine erişebilme fonksiyonunda bir program olması halinde suçunun icrai hareketlerine başlandığı kabul edilmelidir. Bu bağlamda, mağdurun e-postadaki linke tıklaması ve failin mağdurun bilişim sistemine erişmesi halinde suç tamamlanacak; mağdurun linke tıklamaması halinde suç teşebbüs aşamasında kalacaktır[262].

Yine yargıtaya göre, mağdurun şahsi bilgisayarındaki iletişim sistemine (linux, windows) bir başkasının girmesi halinde de bu suç oluşur[263].

Hükümde *"bir bilişim sisteminin bütününe veya bir kısmına"* ifadesi kullanıldığından, hukuka aykırı şekilde bilişim sistemine ait herhangi parçalardan birine, örneğin disket, CD ve USB bellek gibi araçlara girmek de bu suça vücut verir[264].

bb. Bilişim Sisteminde Kalmak

---

[261] **MALKOÇ**, İsmail, Açıklamalı Türk Ceza Kanunu, C. 4, Sözkesen Matbaacılık, Ankara 2013, s. 3820.; KURT, s. 155.; MAHMUTOĞLU, *"Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi",* s. 861.

[262] MAHMUTOĞLU, *"Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi",* s. 861.

[263] Yargıtay 8. CD., E. 2018/1078, K. 2018/2485, T. 8.3.2018. https://karararama.yargitay.gov.tr/ (E.T. 19.09.2023); 8. CD., E. 2016/12839, K. 2017/11114, T. 11.10.2017. https://karararama.yargitay.gov.tr/ (E.T. 19.09.2023)

[264] KARAKEHYA**,** s. 14, 15.; KURT, s. 156.

Kanun metninde düzenlenen ikinci seçimlik hareket ise bilişim sisteminde kalmaktır. Bilişim sisteminde kalmak, kısaca sistemden çıkmama durumudur[265].

Bilişim sisteminde kalma hareketinin tipikliği farklı çeşitlerde ortaya çıkabilmektedir. Bilişim sistemine hukuka aykırı girilerek orada kalınabileceği gibi, hukuka aykırı şekilde erişilmeksizin de sistemde kalınabilecektir. Bu durum iki şekilde ortaya çıkabilir. İlk ihtimal bilişim sisteminin sahibinin rızası ile hukuka uygun bir şekilde sisteme girme fakat sahibinin rızasının kapsadığı süreyi aşarak sistemden çıkmamasıdır. İkincisi ise istemsiz olarak sisteme girildikten sonra bunun fark edilmesine rağmen sistemde kalmaya devam etme şeklinde gerçekleşebilir.

Madde metninde *"kalmaya devam etme"* şeklindeki ifade, bu sürecin ne kadar sürmesi gerektiğine yönelik bir belirsizlik oluşturmaktadır. Öğretideki baskın görüş ve Yargıtay'ın uygulaması[266], suçun oluşabilmesi için kalmaya devam etme hareketinin ne kadar sürmesi gerektiğinin somut olayın özelliklerine göre hâkim tarafından değerlendirilmesi yönündedir[267]. Buna göre, bilişim sisteminde kalma fiili, failin ciddiliğini ortaya koyacak ölçüde bir süreye tekabül etmelidir[268].

Öte yandan bir başka görüş, madde metninde herhangi bir süre ifadesine yer verilmediğinden, sistemde kalınan sürenin bir işlem yapmaya elverişli olup olmadığı gibi koşullara bakılmaksızın sistemde hukuka aykırı olarak milisaniyelik kalmanın dahi bu suçu oluşturduğu şeklindedir[269]. Ben de bu görüşe katılıyorum. Buna göre ilk olarak

---

[265] KETİZMEN, s. 107.

[266] *"Bilişim sisteminde kalınan sürenin suçun oluşumu için yeterli olup olmadığı somut olaya göre hâkim tarafından belirlenmesi gerekmektedir."* CGK., E. 2019/239, K. 2021/325, T. 1.7.2021. https://www.lexpera.com.tr/ (E.T. 20.09.2023)

[267] İHTİYAROĞLU, s. 423.; TAŞKIN, Bilişim Suçları, s. 20.

[268] YILMAZ, Türk Ceza Hukuku Sisteminde Siber Suçlar, s. 197.

[269] ÖZSOY, s. 307, 308.

fail, sözgelimi sehven sisteme girmiş, bunu fark ettikten sonra sistemden hemen çıkabilecek olmasına rağmen çıkmayarak az bir süre dahi kalmış olsa dahi suç oluşacaktır. İkinci olarak fail, kendisine sistemde kalması için izin verilen süreyi bilerek ve isteyerek aştıysa, sistemden çıkabilecek olmasına rağmen çıkmadıysa, bu süre aşımı az da olsa, yine de suçun meydana geldiğinin kabulü gerekir.

b. Hukuka Uygunluk Nedenleri

Hukuka aykırılık, genel bir ifadeyle hukuka (hakka) karşı gelme, onunla çatışma halinde olma demektir[270]. İşlenen bir fiilin suç teşkil edebilmesi için, hukuk düzenine uygun bulunmaması gerekir. "Bilişim sistemine girme" veya "sistemde kalma" hareketleri hukuka uygunsa, suç da meydana gelmemiş demektir. Bazen hükmün tanımındakine uygun eylem gerçekleştirilse bile, kanun koyucu çeşitli sebeplerle bu eylemi hukuka aykırı olmaktan çıkartmıştır ki bu durumlara hukuka uygunluk sebepleri denir. Bu minvalde, *"Kanunun hükmünü icra (TCK 24/1)", "Yetkili merciin hukuka uygun olan emrini yerine getirme (TCK 24/2)", "Meşru savunma (TCK 25/1)", "Zorunluluk hali (TCK 25/2)", "Hakkın icrası (TCK 26/1)"* ve *"İlgili kişi veya hak sahibinin rızası (TCK 26/2)"* genel olarak hukuka uygunluk sebepledir.

Her hukuka uygunluk sebebi her suçla bağdaşmayabilir. Nitekim meşru müdafaa ve zorunluluk hali bu suçla bağdaşmaz.

Hukuka uygunluk sebeplerinden olan ilgilinin rızası ise bu suç için geçerli olabilecektir. Gerçekten, bilişim sistemi üzerinde izin verme konusunda yetkili olan

[270] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Genel Hükümler, B. 15, Seçkin Yay., Ankara 2022, s. 265.

kişinin geçerli rızası[271] dahilinde sisteme giriş yapan kişi, hukuka uygun davranmış olacaktır. Bu çerçevede, öğretide *"beyaz şapkalı bilişim korsanı"* olarak adlandırılan bilişim güvenliği uzmanlarının bir kişi veya kurumla yaptığı anlaşma çerçevesinde, bu kişi ve kurumların sahip olduğu sistemin zafiyetini test etmek için güvenlik duvarına saldırı düzenleyerek sisteme giriş yapması eylemi de hukuka uygundur[272].

Belirtmek gerekir ki, rıza değerlendirilirken rızanın kapsamı ve kim tarafından verildiği çok önemlidir. Rıza, bilişim sistemi üzerinde hak sahibi olan kişi tarafından verilmelidir[273].

Bilişim sistemi üzerinde hak sahibi olan kişi tarafından, bir kişiye sistemin bir bölümüne erişim yetkisi tanındığı olaylarda kişilerin bilişim sistemine erişimlerinin münferit olarak incelenmesi gerekmektedir. Eğer bilişim sisteminden yararlanmaya yetkili olan kişi, bir başkasına giriş izni vermişse eylem hukuka aykırı olmayacaktır[274]. Nitekim Yargıtay 8. CD., önüne gelen bir uyuşmazlıkta[275] *"tanığın katılan şirkete ait siteye bedeli karşılığında abone olduğu, sanığın tanıktan aldığı kullanıcı adı ve parola bilgileriyle tanığın bilgisayarından sisteme giriş yaptığı ve site içeriğindeki bazı bilgileri kopyaladığı"* olayda; sisteme giriş şeklinin yasal yollarla gerçekleştiği, bu

---

[271] *"Mağdurun rızasının varlığı çok dikkatli araştırılması gereken bir durumdur. Kişinin rızasının hata, hile ve ikrah ile sakatlanmamış bulunması gerekmektedir."* KURT, s. 157.

[272] KAYAER, s. 103.; Avrupa Siber Suç Sözleşmesi Açıklayıcı Raporunun 47. Paragrafında konuyla ilgili *"..Sistemin ya da bir parçasının sahibi ya da başka hak sahiplerinin izniyle yapılan erişimin (örneğin ilgili bilgisayar sisteminin izinli olarak test edilmesi ya da korunması amacıyla) suç olarak tanımlanamayacağı…"* ifadelerine yer verilmiştir. Rapor için bkz. https://rm.coe.int/16800cce5b (E.T. 1.10.2023)

[273] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 159.

[274] TAŞKIN, Bilişim Suçları, s. 27.

[275] 8. CD., E. 2014/35223, K. 2015/19051, T. 15.06.2015 https://kararara ma.yargitay.gov.tr (E.T. 1.10.2023)

doğrultuda maddede yer alan hukuka aykırılık şartının gerçekleşmediği gerekçesiyle suçun oluşmadığına hükmetmiştir.

Verilen rızanın sınırının aşıldığı takdirde, sözgelimi ilgili tarafından başka bir kullanım amacı için ödünç verilen bilgisayarı alan failin, bilgisayar üzerinden ilgilinin e-posta hesabına girmesi durumunda, verilen rızanın kapsamı dışına çıkıldığından suç oluşacaktır.

Hukuka uygunluk sebeplerinden kanun hükmünü yerine getirme hali bu suçla bağdaşmaktadır. Bir merci tarafından kanun hükmünün yerine getirilmesi doğrultusunda bilişim sistemine girilmesi veya bu sistemde kalınması halinde fiil hukuka aykırı olmaktan çıkacaktır. Kanun hükmünü yerine getirme durumuna örnek olarak, bir suç şüphesiyle CMK'da düzenlenen *"Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma (m. 134[276])"* koruma tedbirinin gerçekleştirilmesine yönelik yetkili bir hâkim veya savcı kararının olması gösterilebilir. Bu halde bu işlemi yapan görevlinin fiili suç teşkil etmeyecektir.

Sistem sahibinin belirli bir kişi veya kişilere giriş izni vermediği, herkesin dilediğince girebileceği aleni sistemlere girilmesi hukuka aykırı olmadığından suç oluşturmayacaktır. Ancak sistem sahibinin, bilişim sisteminin bir kısım ağlarına girmesine yahut birtakım verileri görmesine izin verdiği durumlarda, kendisine verilen iznin kapsam alanı dışına erişim sağlandığından suçun meydana geldiğinin kabulü

[276] CMK m. 134/1: *"Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir."*

gerekir[277]. Bu noktada, herkesin görüntüleyebildiği fakat her kullanıcının belirlediği şifrelerle korunan kişisel kullanıcı hesabına erişim sağlayabildiği sistemlerde (Twitter, Facebook, İnstagram vs), bir başka kişinin hesabına hukuka aykırı olarak erişim sağlanması da bu kapsamda suç sayılacaktır[278].

Rızanın süresi de çok önemlidir. Bilişim güvenliği uzmanı örneğinde, bilişim güvenliği uzmanının kişi veya kurumla yaptığı anlaşmanın herhangi bir şekilde son bulması halinde artık geçerli rıza ortadan kalkmış demektir. Bu çerçevede bu kişilerce, önceden iş yaptığı kişi veya kurumların sistemine giriş yapılması durumunda hukuka uygunluk nedeni yoktur. Buna ilişkin olarak Yargıtay 11. CD, sanığın katılan şirkette çalıştığı esnada kendisine görevi nedeniyle verilen şirketin bilişim sistemine ait internet şifresini iş yerinden ayrıldıktan sonra da kullanarak sisteme giriş yaptığı bir uyuşmazlıkta bilişim sistemine hukuka aykırı olarak girme fiilinin gerçekleştiğine karar vermiştir[279].

Rıza açıkça veya örtülü olarak verilmiş olabilir; yeter ki eylem sırasında mevcut olsun. Zira eylem gerçekleştirildikten sonra verilen rızanın hukuken geçerliliği yoktur.

[277] ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu"*, s. 1408.

[278] KETİZMEN, s. 104.

[279] E. 2009/22385, K. 2012/3683, T. 19.03.2012. https://karararama.yargitay.gov.tr/ (E.T. 10.10.2023)

2. Manevi Unsur

Suç kastla işlenebilir. Kast, failin yetkili olmadığını bildiği halde bilerek ve isteyerek bir bilişim sistemine girmesi veya orada kalması iradesidir[280].

Madde metninde yer alan *"hukuka aykırı olarak girme veya orada kalmaya devam etme"* ifadesinin ayrıca incelenmesi gerekmektedir. Bazı suçlarda yer alan bu ifadeden ne anlaşılması gerektiğine ilişkin çeşitli görüşler bulunmaktadır. Türk hukuku öğretisinde genel kabul gören görüşe göre kanun koyucu, bir suçun düzenlemesine *"hukuka aykırılık"* unsurunu ekleyerek o suça ilişkin fiilin yalnızca hukuka aykırı olduğunu bilinerek ve istenerek, yani doğrudan kastla gerçekleştirilebileceğini vurgulamaktadır[281]. Yargıtay CGK'nın da özel hukuka aykırılık durumu için aynı doğrultuda değerlendirme yaptığı görülmektedir: *"5237 sayılı Kanunda bazı suç tanımlarında 'hukuka aykırı olarak', 'hukuka aykırı başka bir davranışla', 'hukuka aykırı diğer davranışlarla', 'hukuka aykırı yolla', 'hukuka aykırı yollarla' gibi ifadelere yer verilmiştir. Bu ifadelerin geçtiği suçlarda failin, işlediği fiilin hukuka aykırı olduğunu bilmesi, yani bu konuda doğrudan kastla hareket etmesi gerekmektedir."*[282]. Bu sebeple suç olası kastla işlenemeyecek, yalnızca doğrudan kastla işlenebilecektir[283].

---

[280] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 486.; ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu"*, s. 1404.

[281] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Genel Hükümler, s. 167.; **DÖNMEZER**, Sulhi – **ERMAN**, Sahir, Nazarî ve Tatbikî Ceza Hukuku, C. 2, B. 15, Der Yay., İstanbul 2021, s. 251, 252.; DÜLGER, s. 297. YENİDÜNYA – DEĞİRMENCİ, s. 74.

[282] CGK., E. 2012/1514, K. 2014/312, T. 10.6.2014. https://karararama.yargitay.gov.tr/ (E.T. 12.10.2023)

[283] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 902.; KAYAER, s. 116.; Suçun olası kastla işlenebileceği yönündeki aksi görüş için bkz. TEZCAN – ERDEM – ÖNOK, s. 1172.; MAHMUTOĞLU, *"Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar Ve Karşılaşılan*

Madde metninde suç için özel bir kastın varlığı aranmamıştır. Yargıtay CGK da, bir kararında[284] *"Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir."* şeklindeki açıklamalarıyla sisteme giriş niyetinin önemli olmadığına dikkat çekmiştir.

Anlatılanların ışığında, failin bilişim sistemine girerken veya sistemde kalırken güttüğü amaç veya saik çok çeşitli olabilir. Suçun oluşumu bakımından hangi amaç veya saikle hareket ettiğinin önemi bulunmamaktadır. Örneğin failin kendi firmasının reklamını yapmak, başarma hazzını tatmak veya bilişim becerisini göstermek için sisteme girmesi halinde de suç oluşacaktır[285].

Kanunda suçun taksirli şekline yer verilmediğinden, suçun taksirle işlenebilmesi mümkün değildir. Bu takdirde, söz gelimi, internette gezinirken ihmalkâr veya dikkatsiz davranıp bir bilişim sistemine erişen kişiler bakımından cezai sorumluluk doğmaz[286]. Öte yandan, tesadüfen veya sehven erişim sağlandıktan sonra bunun fark edilmesine rağmen sistemde kalınmaya devam edildiği takdirde, suç oluşacaktır. Ancak burada suç, kasten sistemde kalma hareketinin gerçekleşmesi neticesinde tamamlanacaktır[287].

Suçun yalnızca kasten işlenebilir olması, AKSSS'de *"Yetkisiz erişim"* suçunun düzenlendiği 2. maddeyle de paralellik arz eder[288]. Nitekim bu maddede taraf devletlere

---

Sorunların Yargı Kararları Işığında Değerlendirilmesi", s. 862.; ÖZBEK – DOĞAN – BACAKSIZ, s. 991.; YAŞAR – GÖKCAN – ARTUÇ, s. 7295.

[284] Yargıtay CGK, E. 2019/239, K. 2021/325, T. 01.07.2021. https://karararama.yargitay.gov.tr/ (E.T. 21.10.2023)

[285] PARLAR – ÖZTÜRK, s. 27.; KURT, s. 151.

[286] KARAKEHYA, s. 201.

[287] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 902.

[288] ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu"*, s. 1405.

"yetkisiz erişim"in kasten gerçekleşmesi halinin suç olarak düzenlenmesi yükümlülüğü yüklenmiştir.

Suçun neticesi sebebiyle ağırlaşmış hali (3. fıkra) bakımından ise, suçun taksirle işlenmesi mümkün hatta gereklidir. Bu konuda ayrıntılı açıklama aşağıda yapılacaktır.

D. SUÇA ETKİ EDEN SEBEPLER

1. Daha Az Cezayı Gerektiren Nitelikli Hal

Maddenin 2. fıkrasında, 1. fıkradaki suçun "bedeli karşılığı yararlanılabilen sistemlere" karşı işlenmesi, daha az cezayı gerektiren hal olarak düzenlenmiştir. Madde gerekçesinde "bedeli karşılığında yararlanılabilen sistemlerden" ne anlaşılması gerektiğine ilişkin bir açıklama mevcut değildir. Kanaatimce, suç ve cezalarda belirlilik ilkesi ve kıyas yasağı doğrultusunda bu tür sistemlerin kanun koyucu tarafından kapsamının çizilmesi gerekmektedir. Bu husus, somut uyuşmazlıkta bir sistemin bedeli karşılığı yararlanılabilen sistem olup olmadığına ilişkin kıyasa mahal vermemek adına elzemdir.

Bedeli karşılığı yararlanılabilen sistemlerin kapsamı bilimsel öğreti ve içtihat doğrultusunda çizilmelidir. Bu sistemlerden ilk olarak belirli bir bedel karşılığında hizmet veren web sayfaları anlaşılmalıdır[289]. Örneğin internette ücretli olarak üyelik alınabilen gazete, dergi, oyun aboneliği gibi siteler bir bedel mukabilinde hizmet veren ve yararlanılabilen sistemlerdir.

[289] KARAGÜLMEZ, s. 209.

Buradaki bedel kavramı yalnızca para olarak anlaşılmamalıdır. Bedel kavramının TDK çevrimiçi sözlüğünde *'bir şeyin yerini tutabilen karşılık'* anlamına geldiği göz önünde bulundurulacak olursa, sözgelimi abonelik esası ile çalışan bir online dergi sitesi, kendilerine belli bir yazı gönderme karşılığında dergiye abone olabilmeyi şart koştuysa, bu derginin de bedeli karşılığı yararlanabilen bir sistem olduğunun kabulü gerekir[290].

Bedeli karşılığında yararlanılabilen sistemlerden ikinci olarak bilgisayar, akıllı cep telefonu gibi bilişim sistemlerine ücretli olarak indirilip kullanılabilen çeşitli uygulamalar anlaşılmalıdır. Sözgelimi, bir akıllı cep telefonuna bir ücret karşılığında indirilebilen müzik programı veya yazılımı, yine bu sistemlerden sayılacaktır.

Belli bir bedel karşılığı bilişim sisteminin kullanımının kiralandığı internet kafe gibi yerlerin bu kapsamda olup olmadığı öğretide tartışmalıdır. Birtakım yazarlar, bir bedel karşılığı bilişim sistemlerinin kiralandığı internet kafelerin de bu kapsamda olduğunu düşünmektedir[291].

Öte yandan daha çok taraftar bulan diğer görüşe göre bedeli karşılığında yararlanılabilen sistemlerden, bilişim sisteminin bedel aracılığıyla fiziken kullanıldığı yerler değil, bu sistem içindeki elektronik biçimde sunulan ücretli hizmetler anlaşılmalı, bu sebeple de internet kafe vb. yerlerin bu kapsamda olmadığı sonucuna varılmalıdır[292].

Bu sistemlerin kapsamı hakkında değinilmesi gereken son husus, otomatların bu fıkrada bahsedilen sistemlerden olmadığıdır. Çünkü otomatlar aracılığıyla bir bedel

---

[290] KARAGÜLMEZ, s. 210.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 148.; DÜLGER, s. 284.

[291] DÜLGER, s. 283.; YAŞAR – GÖKCAN – ARTUÇ, s. 7299.

[292] KARAGÜLMEZ, s. 210; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 149, KETİZMEN, s. 110.

mukabilinde sunulan hizmetlerden bedel ödenmeden fayda sağlanması eylemi, TCK m. 163'te ayrıca cezaya bağlanmıştır[293].

Öğretide bedeli karşılığı yararlanılabilen sistemler bakımından cezayı hafifleten halin düzenlenmesinin isabetsiz olduğunu düşünen bir görüş vardır. Bu görüşe göre, bedeli mukabilinde yararlanılabilen sistemlere yetkisiz erişim sağlandığında, 1. fıkrada düzenlenen suçun hukuki değeri olan bilişim sistemlerinin güvenliği yanı sıra, ayrıca sistem sahibinin malvarlığının korunmasına yönelik hukuksal menfaat de ihlal edilmiş olacağından, bunun cezayı hafifleten değil, tam tersi cezayı ağırlaştıran nitelikli hal şeklinde düzenlenmesi gerekirdi[294].

2. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

TCK m. 243/3'te suçun suçun neticesi sebebiyle ağırlaşmış haline yer verilmiştir. Nitekim madde gerekçesinde de bu fıkranın, suçun neticesi sebebiyle ağırlaşmış hali olduğu açıkça belirtilmiştir.

Düzenlemeye göre, 1. fıkradaki fiil nedeniyle sistemdeki verilerin "bozulması" yahut "değişmesi" halinde, faile suçun temel şeklinde öngörülen cezadan daha fazla bir ceza verilecektir. Hükmün gerekçesinde, bu fıkrada geçen veri ifadesinin sistem içerisindeki bütün soyut unsurları kapsadığı ifade edilmektedir.

Bu fıkra, esasen Fransız Ceza Kanunu'nun 323-1. maddesinin 2. cümlesine çok benzemektedir: *"Fiil, sistemdeki bir verinin yok olmasına yahut değişmesine veya*

[293] DÜLGER, s. 283.; KARAGÜLMEZ, s. 209; ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1398.; TAŞKIN, Bilişim Suçları, s. 35.

[294] Görüş için bkz. DÜLGER, s. 285; ERDOĞAN, *"Bilişim Sistemine Girme ve Kalma Suçu",* s. 1400.

sistemin işleyişinde herhangi bir değişikliğe neden olursa, verilecek ceza üç yıl hapis ve 45.000 Euro para cezasıdır.”.

TCK m. 243/3’ün uygulama alanı bulabilmesi için, failin hukuka aykırı olarak sisteme girmesi yahut sistemde kalması fiiline bağlı olarak *“verilerin yok olması”* veya *“verilerin değişmesi”* neticelerinden herhangi birinin gerçekleşmesi yeterlidir[295]. İkisinin birlikte gerçekleşmesi önem arz etmemektedir.

Neticesi sebebiyle ağırlaşmış bu suçun varlığından söz edebilmek için failin kastının verileri yok etmeye veya değiştirmeye yönelik olmaması gerekmektedir ki; Yargıtay’ın uygulaması da bu yöndedir[296]: *“Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.”*. Gerçekten de neticesi sebebiyle ağırlaşmış suçun doğası gereği, verilerin yok olması veya değişmesi, hukuka aykırı olarak sisteme girmenin neticesinde, fakat buna yönelik kast olmaksızın meydana gelmelidir. Zira verilerin yok olması veya değişmesi kastıyla hareket eden fail bakımından bu suç değil, TCK m. 244/2 de düzenlenen suç meydana gelecektir.

Ancak belirtmek gerekir ki bu hüküm bir objektif sorumluluk hali de değildir[297]. TCK m. 23’te düzenlenen neticesi sebebiyle ağırlaşmış suçun genel esasları, bu fıkra için de geçerlidir. Buna göre, failin ağırlaşan neticeden sorumlu tutulabilmesi için en azından bu sonucun gerçekleşmesinde taksirle hareket etmiş olması gerekmektedir[298].

---

[295] KARAGÜLMEZ**,** s. 212.; DÜLGER, s. 280.

[296] CGK, E. 2019/239, K. 2021/325, T. 01.07.2021. https://karararama.yargitay.gov.tr/ (E.T. 7.11.2023)

[297] DEĞİRMENCİ, s. 204.

[298] Karşı yönde bkz. ÖZBEK – DOĞAN – BACAKSIZ, s. 991. Yazarlar bu fıkradaki düzenlemenin ayrı bir suç olduğunu ve madde metninde suçun taksirli hali düzenlenmediğinden, suçun taksirle işlenmesinin mümkün olmadığını savunmaktadır.

Bu kapsamda, fail bilişim sistemine hukuka aykırı olarak kasten girmiş[299] veya orada kalmış, bunun neticesinde veriler yok olmuş veya değişmişse; gerçekleşen bu zarar faile taksir, bilinçli taksir veya olası kasttan herhangi biriyle isnat edilebilmelidir.

E. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

1. Teşebbüs

TCK'nın 35. maddesinde teşebbüs, kişinin işlemeyi kastettiği bir suçun icrasına doğrudan doğruya elverişli hareketlerle başlayıp, elinde olmayan sebeplerle tamamlayamaması durumu olarak tanımlanmıştır. Bu durumda faile daha az ceza verilecektir.

Suç, teşebbüse elverişli bir nitelik arz eder. Hukuka aykırı olarak sisteme girmeye çalışmak veya hukuka uygun olarak erişilmiş bir sistemde hukuka uygunluk hali ortadan kalktıktan sonra sistemde kalmaya niyetlenip bunu başaramamak teşebbüs halidir[300]. Yargıtay 8. ve 15. Ceza Dairelerinin yerleşik içtihadı da suçun teşebbüse elverişli olduğuna yöneliktir[301].

---

[299] Failin sisteme taksir veya bilinçli taksirle girmesi neticesinde veriler yok olmuş veya değişmişse TCK m. 243/3'ten bahsedilemez. Nitekim burada suçun temel hali gerçekleşmemiştir ve temel hali gerçekleşmeyen suçun neticesi sebebiyle ağırlaşmış halinin gerçekleşmesi mümkün değildir. KAYAER, s. 107.

[300] ERDAĞ, s. 283. Aynı görüşteki diğer yazarlar için bkz. DÜLGER, s. 313.; KARAKEHYA, s. 19.; AKARSLAN, s. 46.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 87.

[301] 8. CD., E. 2016/11922, K. 2017/6655, T. 07.06.2017. https://karararama.yargitay.gov.tr/ (E.T. 22.11.2023); 15. CD., E. 2012/13233, K. 2014/795, T. 21.1.2014. https://karararama.yargitay.gov.tr/ (E.T. 22.11.2023)

Fail, bilişim sistemine girmek için icra hareketlerine başlamış ancak örneğin elektrik veya internet kesikliği gibi herhangi bir sebeple iletişim kopması yaşadığı için sisteme erişememişse, *"bilişim sistemine girme"* hareketi teşebbüs aşamasında kalmıştır[302].

Öte yandan, failin sistem sahibinin rızası dahilinde sisteme girmesi ancak rızanın ortadan kalkmasına veya süresinin dolmasına rağmen sistemde hukuka aykırı olarak kalmaya niyetlenmesi ve buna yönelik icrai hareketlere başlaması (örneğin sistemde kalabilmek için sistemin şifresini değiştirmeye çalışması) fakat elinde olmayan sebeplerle bunu gerçekleştirememesi halinde *"bilişim sisteminde kalma"* hareketi[303] bakımından teşebbüsten bahsedilecektir.

Fail sisteme hukuka aykırı giriş yaptıktan sonra diğer seçimli hareket olan sistemde kalmaya devam etmeyi gerçekleştirememişse, seçimlik hareketlerden biri gerçekleşmiş olacağından bu durumda suça teşebbüs söz konusu olmayacaktır[304]; zira suç tamamlanmıştır.

Belirtmek gerekir ki, failin bir kişinin bilişim sistemine yetkisiz olarak erişebilmek için zararlı bir yazılım, şifre veya herhangi bir program üretmesi, ancak daha sonra pişman olup amaçladığı suçu işlememesi durumunda teşebbüsten bahsedilemeyecektir. Ancak fail, TCK m. 245/A'da belirtilen cihaz ve programları ürettiği için bu maddedeki suçtan sorumlu olacaktır. Zira TCK'da bu husus şu şekilde vurgulanmıştır: *"Fail, suçun icra hareketlerinden gönüllü vazgeçer veya kendi*

[302] KARAGÜLMEZ, s. 46.

[303] Öğretide birtakım yazarlar, sistemde kalma hareketinin teşebbüse elverişli olmadığını savunmaktadır. Ancak ben bu görüşe verilen örnekte sistemde kalma hareketinin teşebbüs aşamasında kaldığını düşünerek katılmıyorum. Aksi görüş için bkz. TEZCAN – ERDEM – ÖNOK, s. 1176.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 87.; ÖZBEK – DOĞAN – BACAKSIZ, s. 991.

[304] DÜLGER, s. 313.; TEZCAN – ERDEM – ÖNOK, s. 1175.

çabalarıyla suçun tamamlanmasını veya neticenin gerçekleşmesini önlerse, teşebbüsten dolayı cezalandırılmaz; fakat tamam olan kısım esasen bir suç oluşturduğu takdirde, sadece o suça ait ceza ile cezalandırılır. (m. 36)"

2. fıkrada düzenlenilen suçun neticesi sebebiyle ağırlaşmış haline teşebbüsün mümkün olup olmayacağı bakımından öğretide baskın görüş, neticesi sebebiyle ağırlaşmış suçların teşebbüse elverişli olmadığıdır[305].

2. İştirak

İştirak, bir suçun işlenebilmesi için gerekli olan kişi sayısından bir ya da birden fazla kişinin o suçu işlemesi halinde, işlenen suç açısından cezai sorumluluğunun esasını belirleyen ceza hukuku kurumudur[306].

Suç, iştirak bakımından bir özellik taşımamaktadır. Bu kapsamda suça iştirak değerlendirilirken TCK'nın 37. maddesi, 38. maddesi, 39. maddesi ve 40. maddesi dikkate alınacaktır.

Bir bilişim sistemine hukuka aykırı girebilmek için bilişim alanında uzman biriyle anlaşarak onu sisteme girme konusunda ikna eden kişinin, TCK m. 38 hükmünce azmettiren sıfatıyla cezai sorumluluğu gündeme gelecektir[307]. Buna karşılık TCK m. 243'teki suçun işlenmesi için bir kimseye ihtiyacı olan program ve yazılımların

[305] **DOĞAN**, Koray, Neticesi Sebebiyle Ağırlaşmış Suçlar, Adalet Yay., Ankara 2011, s. 236.

[306] **ÖZEN**, Mustafa, *"5237 Sayılı Türk Ceza Kanunu'nun İştirak Kurumuna Bakışı"*, TBB Dergisi, S. 70, 2007, s. 239.

[307] APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 57.

verilmesi halinde, bu fiil TCK m. 245/A'da düzenlenen suçu oluşturduğundan, faile ayrıca bilişim sistemine girme suçuna iştirakten ceza verilmeyecektir.

3. İçtima

Ceza hukukunun temel ilkelerinden biri de *"kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır (quot crimina, tot poenae)"* ilkesidir. Suçların içtimaı kurumu ise bu ilkenin istisnasıdır. Suçların içtimaında bir veya birden çok fiille kanunun aynı veya farklı hükümlerini ihlal eden fail, çeşitli sebeplerle tek bir suçtan sorumlu tutularak cezalandırılmaktadır[308]. Suçların içtimaının çeşitleri Kanun'da; *"Bileşik suç*[309] *(m. 42)", "Zincirleme suç (m. 43)"* ve *"Fikri içtima (m. 44)"* olarak düzenlenmiştir.

Zincirleme suç, Kanun'un 43. maddesinde *"bir suç işleme kararının icrası kapsamında, değişik zamanlarda bir kişiye karşı aynı suçun birden fazla işlenmesi durumu"* olarak ifade edilmiştir. 43. maddenin 1. fıkrasının son cümlesine *"5377 sayılı Türk Ceza Kanununda Değişiklik Yapılmasına Dair Kanun*[310]*"* adlı Kanun'un 6. maddesiyle, *"mağduru belli bir kişi olmayan suçlarda da bu fıkra uygulanır"* ifadesi eklenmiştir. Eklenen bu hükmün gerekçesinde ise toplumu oluşturan herkesin mağdur olduğu suçlarda da zincirleme suç hükümlerinin uygulanacağı belirtilmiştir.

---

[308] HAFIZOĞULLARI – ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 353, 354.

[309] Bileşik suç, Kanun'da, *"biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan suç"* şeklinde tanımlanmıştır.

[310] R.G., 08.07.2005 T., 25869 S.

İlgili suç, *"Topluma Karşı Suçlar"* başlığı altında düzenlenmiştir ve 43. maddeye eklenen bu cümleyle, suç, zincirleme suç hükümlerinin uygulanmasına elverişli hale gelmiştir.

Ancak suçun *"Topluma Karşı Suçlar"* başlığı altında düzenlenmesi sebebiyle, zincirleme suç hükümlerinin uygulanabilmesi açısından birden fazla kez girilen sistemin aynı kişiye ait bir sistem mi olması gerektiği konusu tartışmalıdır. Suçun mağdurunun gerçek kişi olduğunu düşünen görüşe ve karşı yönde suçun mağdurunun toplum ve kamu idaresi olduğunu düşünen bir başka yaklaşıma yukarıda ayrıntısıyla yer verilmişti. Bu noktada, suçun mağdurunun gerçek kişi olduğu düşüncesinde birden fazla kez girilen sistemin aynı kişiye ait olması gerekmektedir. Keza 43. maddenin 1. fıkrasından anlaşılan da budur. Zira bu görüşe paralel olarak Ankara Bölge Adliye Mahkemesi, konuya ilişkin önüne gelen bir uyuşmazlıkta *"Dosyanın bir bütün halinde incelenmesinde, sanığın birden fazla kez aynı kast altında katılanın yetkilisi olduğu ve F2 Bilişim Sistemleri Ltd. Şti'nin internet sitesine girerek kendi savunmasına göre orada tespit ettiği güvenlik açıklarını firma yetkililerine göstermek amacıyla veri yerleştiği ve verileri bozduğu iddia edilmiş ise de, sanığın katılana ait bilişim sistemine izinsiz girdiği, ancak veri yerleştirdiğine ve verileri bozduğuna dair delil bulunmadığından, sanığın eyleminin TCK'nın 244/2 maddesinde belirtilen bilişim sistemine izinsiz girerek veri yerleştirme ve bozma suçunu değil, sadece bilişim sistemine hukuka aykırı olarak girme suçunu oluşturduğu ve sanığın aynı suç işleme kararını icrası kapsamında değişik zamanlarda aynı mağdura karşı aynı suçu birden fazla kez işlediği, bu nedenle de hakkında zincirleme suç hükümlerinin uygulanması gerektiği…"* şeklinde karar vermiştir[311].

[311] İHTİYAROĞLU, s. 433.; Ankara BAM 8. CD., E. 2017/207, K. 2018/439, T. 17.4.2018. https://www.lexpera.com.tr (E.T. 12.12.2023)

Öte yandan, suçun mağdurunun toplum ve kamu idaresi olduğu, yani belli bir kişi olmadığı görüşü kabul edilecek olursa -ki kanun sistematiğinden bu anlaşılmaktadır-, birden fazla kez girilen veya kalınan sistemin aynı kişiye ait olmasına gerek yoktur. Nitekim suçun mağduru belli bir kişi olmadığından, bilişim sisteminin kime ait olduğunun da önemi yoktur. Dolayısıyla fail kimin sistemine girmiş veya orada kalmış olursa olsun, bir suç işleme kararının icrası kapsamında farklı zaman aralıklarında birden fazla kez giriş yapmış veya orada kalmışsa 43. maddenin 2. fıkrası gereğince zincirleme suç hükümleri uygulanacaktır.

Bilişim sistemine hukuka aykırı olarak giren kişi, bilişim sisteminin işleyişini engellemiş veya bozmuşsa yahut verileri yok etmiş veya değiştirmişse; yani kişi hem TCK m. 243/1'te hem de TCK m. 244/1 veya 244/2'de düzenlenen normu ihlal etmişse hangi hükmün uygulanacağı gündeme gelmektedir.

Bir görüşe göre, bilişim sistemine girilmek suretiyle işlenen, TCK m. 244 de dahil olmak üzere tüm suçlarla *"Bilişim sistemine girme veya sistemde kalma"* suçu arasındaki ilişki, fikri içtima ilişkisidir[312]. Fikri içtimaın düzenlendiği 44. maddeye göre *"İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır."*. Dolayısıyla, bilişim sistemine girilerek veya orada kalınarak işlenen diğer suçlarda fikri içtima hükümleri uygulanacak ve en ağır cezayı gerektiren suçtan ceza verilecektir. Ben bu görüşe katılmıyorum. Zira fikri içtimaın yapısı gereği, birden fazla farklı suçun oluşması, tek bir hareketle gerçekleşmelidir. Bilişim sistemine girme hareketinden sonra sözgelimi sistemin işleyişinin engellenmesi halinde iki farklı hareket söz konusudur ve fikri içtima hükümlerinin uygulanması mümkün değildir.

[312] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 997.; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 171; AKBULUT, Bilişim Alanında Suçlar, s. 49.

Bir diğer görüşe göre burada geçitli suç ilişkisi mevcuttur[313]. Geçitli suç kavramı, failin bir suçu işleyebilmek için aynı hukuksal menfaati koruyan bir başka suçtan geçmek zorunda olduğu suç için kullanılmaktadır[314]. Bu görüşe göre, TCK m. 244'te yer alan suçlardan birini işleyebilmek için mutlaka bilişim sistemine yetkisiz erişim gerektiğinden, bu iki suç arasında geçitli suç ilişkisi bulunmakta olup faile ayrıca yetkisiz erişim suçundan ceza verilmez. Ne var ki bu ön kabul, her durumda geçerli olamayabilecektir. Zira TCK m. 244'te yer alan, söz gelimi bilişim sisteminin işleyişini engelleme suçunu işleyebilmek için her durumda bilişim sistemine girmek gerekmez. Bilişim sistemine girmeden de örneğin DDoS saldırıları aracılığıyla sisteme erişim engellenebilir. Dolayısıyla mutlak bir geçit suç ilişkisinden bahsetmek mümkün değildir. Her olay ayrı ayrı değerlendirilmelidir.

Yargıtay 8. CD. önüne gelen uyuşmazlıklarda, katılanın elektronik e-posta adresinin şifresini kırıp sisteme yetkisiz erişen fail hakkında, şifrenin değiştirilmemesi halinde TCK m. 243/1'den, şifresinin değiştirilmesi halinde ise TCK m. 244/2'den hüküm kurulması gerektiğine karar vermektedir[315]. Ancak Yargıtay burada fikri içtima

---

[313] ÖZBEK – DOĞAN – BACAKSIZ, s. 992.; ARTUK – GÖKCEN – YENİDÜNYA, Ceza Hukuku Özel Hükümler, B. 13, Adalet Yay., Ankara 2013, s. 851.; YAZICIOĞLU, *"Hukukumuzda TCK'nun 243. Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, s. 86.; **DEMİRCİ**, Ömer, Bilişim Suçları ve Soruşturma Yöntemleri, Seçkin Yay., Ankara 2022, s. 64, 65.; **DEMİRCAN**, Tunç, Bilişim Alanında Suçlar, Legal Yay., İstanbul 2016, s. 79.

[314] **SARITAŞ**, Erkan, *"Cezalandırılmayan Önceki Hareketler"*, İÜHFM, S. 80, C. 2, 2022, s. 645.

[315] "*Katılana ait elektronik posta adresinin şifresini kırarak, erişilmez kıldığından bahisle açılan davada … katılanın mail adresinin şifresinin kim tarafından değiştirildiğinin e- posta adresinin bağlı olduğu firmadan sorulması, şifre değiştirildiğinin tespiti halinde TCK.nun 244/2, aksi halde aynı yasanın 243. maddesi kapsamında değerlendirilmesi gerektiğinin gözetilmemesi…".* 8. CD., E. 2016/7582, K. 2016/10690, T. 23.11.2016. https://kararara ma.yargitay.gov.tr/ (E.T. 12.1.2024) Benzer yönde 8. C.D. 2015/11993 E., 2016/3544 K., T. 17.03.2016. https://kararara ma.yargitay.gov.tr/ (E.T. 12.1.2024)

hükümlerinin mi yoksa geçitli suç ilişkisinin mi uygulanması gerektiğini belirtmemiştir. Ancak hangi görüşü kabul etmiş olursa olsun, bilişim sistemine yetkisiz erişilerek 244. maddedeki suçlardan birinin işlenmesi halinde Yargıtay, gerçek içtima hükümlerini uygulamamakta, iki suçtan hüküm kurmamaktadır.

F. YAPTIRIM, ZAMANAŞIMI, GÖREVLİ VE YETKİLİ MAHKEME

Suçun temel halinin cezası bir yıla kadar hapis veya adli para cezası olarak seçimlik belirlenmiştir. Dikkat edilirse cezalar seçimlik şekilde düzenlenmiştir, her iki cezanın birlikte verilmesi mümkün değildir. Hâkim, adli para cezası veya hapis cezasından birini TCK'nın 61. maddesinin 1. fıkrasını da göz önünde bulundurarak takdir edecektir[316].

Cezanın niceliği değerlendirildiğinde, suçun temel halinin cezasının caydırıcılık düzeyinin yeterli olduğunu söylemek çok zordur. Gerçekten de suç için öngörülen bir yıllık hapis cezası veya adli para cezası, günümüzdeki pek çok faaliyetin bilişime entegre olduğu ve bu sistemlere yalnızca erişimin dahi kamu esenliğine ciddi zarar verebileceği göz önünde bulundurulunca yetersiz kalmaktadır. Oysaki insanları suç işlemekten alıkoyma özelliğine sahip olan cezaların, suçun kamu düzenine verdiği zararla ve insanları suça teşvik eden sebeplerle orantılı olmaları gerekir[317]. Aksi halde ciddi suçlara hafif cezaların verilmesi sorunuyla karşı karşıya kalınır[318]. Bu sorun ise

[316] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 487.

[317] **BECCARIA**, Cesare, Suçlar ve Cezalar Hakkında (Çev. Sami Selçuk), B. 6, İmge Yay., Ankara 2016, s. 45.

[318] BECCARIA, s. 47.

yalnızca toplumdaki adalet duygusunun zedelenmesine yol açmakla kalmaz, cezaların caydırıcılığını da azaltır.

Suçun bedeli karşılığında yararlanılabilen sistemlere karşı işlenmesi halinde, ceza yarısına kadar indirilecektir.

Suçun neticesi sebebiyle ağırlaşmış hali gerçekleşirse, yani yetkisiz erişim sonucu veriler değişir veya yok olursa, faile altı aydan iki yıla kadar hapis cezası verilmesi öngörülmüştür.

Failin bedeli karşılığı yararlanabilen sistemlere girmesi neticesinde sistemde yer alan bazı verilerin yok olmasına veya değişmesine neden olduğu takdirde cezai yaptırımın ne olacağı hususu tartışmalıdır. Öğretide bir görüşe göre, suçun neticesi sebebiyle ağırlaşmış halinin düzenlendiği 3. fıkrada *"bu fiil nedeniyle"* ifadesi yer almış ve maddenin 1. ve 2. fıkrasını kapsayıcı bir ifade kullanılmıştır. Bu sebeple bedeli karşılığı yararlanılabilen sistemlere girilmesi halinde sistemdeki verilerin yok olması veya değişmesi halinde yalnızca 3. fıkradaki hüküm uygulanmalı[319], 2. fıkradaki indirim yapılmamalıdır.

Öğretideki bir diğer yaklaşım ve Yargıtay 8. C.D.'nin yerleşik uygulamasına göre ise, fail hem m. 243/2 hem de m. 243/3'ten yargılanmalıdır[320]. Yani ceza önce 3. fıkraya göre belirlenecek, sonra 2. fıkra uyarınca indirim yapılacaktır[321]. Bu yaklaşım, TCK m. 61/4'teki *"Bir suçun temel şekline nazaran daha ağır veya daha az cezayı gerektiren birden fazla nitelikli hallerin gerçekleşmesi durumunda; temel cezada önce artırma sonra indirme yapılır."* düzenlemesini esas almaktadır.

[319] YAŞAR – GÖKCAN – ARTUÇ, s. 7301.

[320] ÖZSOY, s. 311.

[321] ÖZSOY, s. 311.

Ancak belirtmek gerekir ki, ikinci yaklaşım tarzı daha adaletli gibi gözükse de Kanun'un düzenleniş biçimiyle pek uyuşmamaktadır[322]. Zira 61. maddenin 4. fıkrası, suçun temel şekline nazaran daha fazla veya daha az cezayı gerektiren nitelikli haller için düzenlenmiştir. Oysaki 243. maddenin 3. fıkrasında daha fazla cezayı gerektiren, yani cezada artırıma sebep olan nitelikli bir hal değil, neticesi sebebiyle ağırlaşmış bir suç düzenlenmiştir. Bu iki kurum her ne kadar benzermiş gibi gözükse de nitelikli haller fiilin haksızlık içeriğini artıran veya azaltan durumları belirlerken, neticesi sebebiyle ağırlaşan haller suçun netice unsuruna ilişkindir[323]. Bir örnek verilecek olursa, kasten yaralama suçu Kanun'un 86. maddesinde suç olarak düzenlenmiştir. Bununla beraber "*kasten yaralama suçunun üstsoya, altsoya, eşe, boşandığı eşe veya kardeşe karşı"* işlenmesi halinde verilecek cezada artırıma gidilecektir (TCK m. 86/3-a). Kanun koyucu bu kişilere karşı işlenen kasten yaralama fiilinin haksızlık olgusunu, suçun temel şekline nazaran daha ağır olarak belirlemiş, suçun nitelikli halini düzenlemiştir. Buna karşılık *"Kasten yaralama fiili sonucunda ölüm meydana gelmesi"* neticesi sebebiyle ağırlaşan bir suç olarak düzenlenmiştir (TCK m. 87/4). Zira burada kasten yaralama fiilinin netice unsuruna sirayet eden bir durum söz konusudur.

Özetle, bedeli karşılığı yararlanılabilen sistemlere hukuka aykırı olarak giren kişinin bu fiili neticesinde sistemdeki bazı veriler değişmiş veya yok olmuşsa, TCK'nın 61. maddenin 4. fıkrasının uygulanma alanı mümkün olmamalıdır. Keza kanun lafzı bakımından da 3. fıkrada yer alan *"bu fiil nedeniyle"* ifadesiyle 1. ve 2. fıkraya atıf yapıldığı kabul edilmelidir. Dolayısıyla 2. ve 3. fıkranın birlikte gerçekleşmesi halinde, fail yalnızca 3. fıkradaki suçtan sorumlu tutulmalı ve cezasında 2. fıkrada belirtilen indirim yapılmamalıdır.

---

[322] KARAGÜLMEZ, s. 214.

[323] KOCA – ÜZÜLMEZ, Ceza Hukuku Genel Hükümler, s. 146.

Her üç fıkrada düzenlenen suç da şikâyete bağlı suçlardan değildir, suçun re'sen takibi gerekir.

Ceza hukukunda, devletin yetkili organlarının suçu zamanında kovuşturmaması, suçu kovuşturma hakkını ortadan kaldırır[324]. Bu kuruma dava zamanaşımı denir. Kanunda *"Bilişim sistemine girme veya sistemde kalma suçu"* için özel bir zamanaşımı süresi öngörülmemiştir. Bu kapsamda TCK'nın 66. maddesinde düzenlenen "genel dava zamanaşımı süreleri" uyarınca ilgili suç için dava zamanaşımı süresi sekiz yıldır. Bir başka deyişle, sekiz yılın geçmesiyle birlikte artık bu suç bakımından kamu davası açılamayacak, eğer açıldıysa düşme kararı verilecektir. Belirtmek gerekir ki *"sistemde kalmaya devam etme"* hareketi devamlılık gösterdiğinden, temadinin kesintiye uğradığı zaman diliminden itibaren dava zamanaşımı süresinin hesaplanması gerekmektedir[325].

Yetkili mahkeme suçun işlendiği yerdeki mahkemedir. Uygulamada Yargıtay, suçun işlendiği yeri, failin sisteme girdiği anda bulunduğu yer olarak kabul etmektedir[326]. Ancak belirtmek gerekir ki, 7331 sayılı *"Ceza Muhakemesi Kanunu ve Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun"*un 10. maddesiyle CMK'nın 12. maddesinin 6. fıkrasına bilişim suçları bakımından önemli bir madde eklenmiştir. Buna göre, *"Bilişim sistemlerinin, banka veya kredi kurumlarının ya da banka veya kredi kartlarının araç olarak kullanılması suretiyle işlenen suçlarda mağdurun yerleşim yeri mahkemeleri de yetkilidir."*. Bu doğrultuda, mağdurun yerleşim yerindeki mahkeme de yetkili mahkemedir.

---

[324] **TANER**, Fahri Gökçen, Ceza Hukukunda Zamanaşımı, Seçkin Yay., Ankara 2008, s. 51.; TOROSLU – TOROSLU, s. 504.; HAFIZOĞULLARI – ÖZEN, Ceza Hukuku Genel Hükümler, s. 515, 516.

[325] DÜLGER, s. 279.

[326] **ÖNDİN**, Hasan Burak, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, Terazi Hukuk Dergisi, C. 15, S. 162, 2020, s. 332.

Görevli mahkeme, 5235 sayılı "*Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun"*un 11. maddesi uyarınca asliye ceza mahkemesidir. Belirtmek gerekir ki, 30.11.2021 tarihli ve 31675 sayılı Resmî Gazete'de yayınlanan 1229 sayılı HSK Birinci Dairesinin Kararı neticesinde asliye ceza ve ağır ceza mahkemeleri bünyesinde bilişim ihtisas mahkemeleri kurulmuş olup bu suç bakımından bilişim ihtisas mahkemeleri görevlendirilmiştir. Bu karara göre, 15.12.2021 tarihi itibarıyla gelecek olan yeni dava ve işler bu mahkemeye tevzi edilecektir.

II. BİLİŞİM SİSTEMİNE GİRMEKSİZİN TEKNİK ARAÇLARLA VERİ NAKİLLERİNİ İZLEME SUÇU (TCK m. 243/4)

A. GENEL BİLGİLER

Bilişim teknolojisi alanında yaşanan gelişmeler, sisteme erişim sağlanmadan da sistem dahilindeki verilere ulaşılabilmesine olanak sağlamıştır[327].

TCK'nın *"Bilişim sistemine girme suçu"* başlıklı 243. maddesine 6698 sayılı KVKK ile 4. fıkra eklenmiş, bu düzenlemeyle *"bilişim sistemine girmeksizin sistemin içindeki veya diğer sistemlerle olan veri akışını teknik araçlarla izlemek fiili"* suç haline getirilmiştir. Bu kapsamda AKSSS'nin 3. maddesinde düzenlenmiş olan *"Yasadışı araya girme suçu"* kanuna yansıtılmış, sözleşmenin taraf devletlere yüklediği sorumluluk yerine getirilmiştir.

Madde başlığı *"Bilişim Sistemine Girme"* olduğundan, sisteme girmeksizin teknik araçlarla izleme fiilinin bu başlık altında düzenlenmesi kanunun sistematiği açısından doğru olmamıştır. Kanaatimce suç, başlı başına ayrı bir başlık altında düzenlenmeliydi[328]. Zira taraf olduğumuz AKSSS'nin 3. maddesinde de *"Yasadışı araya girme"* adıyla bağımsız bir suç tipi olarak düzenlenmiştir.

---

[327] TEZCAN – ERDEM – ÖNOK, s. 1177.

[328] Suçun düzenlendiği yerin isabetli olmadığını ve ayrı bir başlık altında incelenmesi gerektiğini düşünen yazarlar için bkz. DÜLGER**,** s. 249; GÜL**,** s. 91.; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 895.; İHTİYAROĞLU, s. 436.; **ÖNDİN**, Hasan Burak, *"Türk Hukukunda Doğrudan Bilişim Suçları"*, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir 2017, s. 47.

B. SUÇA İLİŞKİN ÖN AÇIKLAMALAR

1. Suçun Hukuki Konusu

Bu suçla bilişim sistemi değil içindeki veriler hedef alınmaktadır. Bu minvalde korunan hukuksal değer sistemin güvenliği değil verilerin güvenliğidir[329]. Nitekim sistemdeki verilerin nakli sırasında, bir başkasının verileri teknik araçlarla izlemesi, verilerin kaynak ve içeriğinin öğrenilmesi tehlikesini doğurmakta ve bu tehlike de verilerin mahremiyetine tehdit oluşturmaktadır[330].

Öğretide birtakım yazarlar suçla korunan hukuki değerin kişisel verilerin güvenliği olduğunu düşünmektedir[331]. Ancak belirtmek gerekir ki, sistemin içerisindeki her veri kişisel veri değildir. Bu sebeple suçun düzenlenmesiyle kişisel verilerin güvenliğini korunduğuna ilişkin görüş, suçun kapsamını sınırlandırmaktadır.

2. Maddi Konu

Suçun konusunu, izlemenin gerçekleştiği bilişim sistemlerinin kendi içindeki veya diğer bilişim sistemleriyle ağlar aracılığıyla aktarımı halindeki veriler oluşturmaktadır[332].

---

[329] DÜLGER, s. 326.

[330] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 908.

[331] ÖZBEK – DOĞAN – BACAKSIZ, s. 988.

[332] AKBULUT, Bilişim Alanında Suçlar, s. 160.; DÜLGER, s. 327.; BAYRAKTAR – EVİK – KANGAL – YILDIZ – EVİK – AKSOY RETORNAZ – MEMİŞ KARTAL – BOSTANCI BOZBAYINDIR – EROĞLU – AYTEKİN İNCEOĞLU, s. 236.

Dikkat edilmelidir ki, sistem içerisindeki statik yani durağan veriler bu suçun konusunu oluşturmayacaktır. Zira suçun düzenlenmesindeki amaç ve kanunun lafzı dikkate alındığında, suçun konusu yalnızca nakil halindeki verilerdir[333].

Verilerin bilişim sistemlerinin kendi içerisinde veya bir başka bilişim sistemlerine aktarımı USB bellek, CD veya sistemler arası ağlar aracılığıyla olabilmektedir[334]. Veri naklini sağlayan bağlantının kablolu veya kablosuz olması yahut intranet, WLAN, VPN gibi özel ağlar olması önemli değildir[335]. AKSSS'de ve Alman Ceza Kanunu'nun teknik araçla veri iletimini izleme suçunu düzenleyen 202/b maddesinde[336] ayrıca *"elektromanyetik dalgalardan"* söz edilmişken TCK m. 243/4'te bu ifadeye yer verilmemiştir. Kanaatimce, elektromanyetik dalgalar vasıtasıyla yapılan veri aktarımının da bu çerçevede olduğu kabul edilmelidir[337]. Bu kapsamda sıklıkla kullanılan bluetooth strandardı[338] aracılığıyla gerçekleşen veri nakilleri de suçun konusu kapsamındadır.

---

[333] DÜLGER, s. 327.; TEZCAN – ERDEM – ÖNOK, s. 1178.

[334] TEZCAN – ERDEM – ÖNOK, s. 1178.; KAYAER, s. 109.

[335] DÜLGER, s. 328.

[336] Alman Ceza Kanunu, Madde 202b *"Teknik araçlar kullanarak, kamusal olmayan veri iletişimlerinden veya bir bilgi işlem sisteminin elektromanyetik dalgalarından yetkisiz olarak kendisi ya da bir başkası için verileri (m. 202a/2) yakalayan (ele geçiren) kişi, fiil başka hükümlerle daha ağır cezaya bağlanmamışsa, iki yıla kadar hapis veya (adli) para cezası ile cezalandırılır."* Tercüme edip aktaran: ERDAĞ, s. 286.

[337] AKBULUT, Bilişim Alanında Suçlar, s. 59.

[338] Bluetooth, sabit veya taşınabilir cihazlar arasında kısa mesafelerde veri aktarımı yapmaya veya kişisel alan ağları (PAN) kurmaya yarayan ve bunu yaparken elektromanyetik dalgaları kullanan kablosuz bağlantı standardıdır. Bkz. https://tr.wikipedia.org/wiki/Bluetooth (E.T. 20.1.2024)

3. Fail

Bu suçun faili herkes olabilecektir, maddede faile ilişkin bir özellik bulunmamaktadır.

4. Mağdur

Suçun mağduru bakımından öğretide *"Bilişim sistemine girme veya sistemde kalma suçu"*nda olduğu gibi görüş ayrılığı vardır. Suçun mağdurunun yalnızca nakledilen veriler üzerinde tasarruf yetkisi olan gerçek kişiler olabileceğini savunan görüş, gerçek kişilerin yanı sıra menfaati zedelenen tüzel kişilerin de mağdur olabileceğini savunan görüş ve son olarak suçun düzenleniş yerinin *"Topluma Karşı Suçlar"* olması sebebiyle suçun mağdurunun kamu idaresi olduğunu savunan yazarlar bulunmaktadır.

C. SUÇUN UNSURLARI

1. Maddi Unsur

a. Hareket

Suçun hareket unsuru, sisteme girmeksizin nakil halindeki verileri izlemektir. Madde metninde de belirtildiği üzere veri nakillerinin izlenmesi, bilişim sistemine

erişilmeksizin yapılmalıdır. Nitekim 6698 sayılı Kanun'a ilişkin Adalet Alt Komisyon Raporu'nda, verilerin izlenmesi eyleminden *"Bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesi"* eyleminin anlaşılması gerektiği ifade edilmektedir. Bu doğrultuda bilişim sistemine hukuka aykırı girilerek veya orada kalınarak nakil halindeki verilerin izlenmesi, *"Bilişim sistemine girme veya sistemde kalma suçunu"* oluşturacaktır.

İzlemenin teknik araçlar vasıtasıyla yapılması gerekmektedir[339]. Teknik araçlar olmadan, sözgelimi veri aktarımını çıplak gözle izlemek bu suçu oluşturmaz[340]. Teknik araç kavramının açıklamasına kanunun hiçbir yerinde yer verilmemiştir. Oysaki, oldukça muğlak olan bu ifadenin kanunilik ilkesi bakımından açıklıkla tanımlanması ve kapsamının çizilmesi gerekirdi. Öğretide teknik araç, insanın görme ve işitme duyusunun, algılama yeteneğinin sınırlarını aşmaya yardımcı olan her türlü teknolojik alet olarak tanımlanmıştır[341].

Suçun tamamlanabilmesi için veri nakillerini izlemek yeterli olup ayrıca veri içindeki bilgilerin öğrenilmiş olması yahut kaydedilmiş olması gerekmez[342]. Yine, izlenen veri aktarımının tamamlanmamış olması da suçun oluşması bakımından önemli değildir[343].

---

[339] KABADAYI, s. 118.

[340] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 910.

[341] ÖNDİN, *"Türk Hukukunda Doğrudan Bilişim Suçları",* s. 48.

[342] TEZCAN – ERDEM – ÖNOK, s. 1179.

[343] APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 149.

Bilişim sisteminin kendi içindeki veya bir başka sistemle olan veri akışının izlenmesine bilişim terminolojisinde *'sniffing'*, bu işlemi gerçekleştiren yazılımlara ise *'sniffer'* adı verilmektedir[344].

Suçun tamamlanması, teknik araçlarla izleme hareketiyle gerçekleşmekte olup ayrıca bir neticenin doğması önemli değildir. Bu bakımdan suç, sırf hareket suçu yani neticesiz suçtur.

b. Hukuka Uygunluk Nedenleri

Suçun oluşması için fiilin hukuk düzeniyle çatışması, bir başka deyişle hukuka aykırı olması gerekir. İzlemenin hukuka uygun olduğu hallerde suç oluşmaz. Verilerin naklinin herkesin dilediğince izleyebileceği şekilde umuma açık olması halinde, izleme fiili hukuka uygundur. Örneğin bilişim sistemleri aracılığıyla çevrimiçi yapılan derslerde hocanın bilgisayarın ekran görüntüsünü öğrencileriyle paylaşması ve öğrencilerin de bu bilgisayar içinde gerçekleşen veri nakillerini telefonları aracılığıyla izlemesi suç olarak sayılamayacaktır.

Nakledilen verilere ilişkin tasarruf hakkına sahip kişinin geçerli bir rızası olması halinde fiil hukuka uygun hale gelecektir[345].

Hukuka uygunluk sebeplerinden kanun hükmünün yerine getirilmesi de bu suçla bağdaşabilir. Kolluk başta olmak üzere çeşitli kamu görevlilerinin (asker, MİT

[344] **ÖZTEKİN**, Alp, Bilişim Sistemine Girme Suçu (TCK m. 243), Seçkin Yay., Ankara 2023, s. 102.; YILMAZ, Türk Ceza Hukuku Sisteminde Siber Suçlar, s. 202.

[345] KABADAYI, s. 123.

personeli[346]) şartları gerçekleştiği takdirde CMK'da düzenlenmiş olan "*Teknik araçlarla izleme (m. 140)"* koruma tedbirinin icrası, hukuka uygun sayılacaktır. Yine, CMK'daki bir başka koruma tedbiri olan *"İletişimin tespiti, dinlenmesi, kayda alınması (m. 135)"* icrası kapsamında yapılan teknik araçlarla izleme, bu suç bakımından şartları gerçekleştiği takdirde hukuka uygunluk nedeni oluşturacaktır[347].

2. Manevi Unsur

Suç ancak kasten işlenebilir. Suçun taksirli haline kanunda yer verilmemiştir.

Maddedeki düzenleme bakımından bilişim sistemine girme veya orada kalma suçunda olduğu gibi özel hukuka aykırılığa yer verildiğinden, suç olası kast ile işlenemez[348].

---

[346] MİT Kanunu'nun 6/g maddesinde MİT'in bu konudaki yetkisi şu şekilde düzenlenmiştir: *"Telekomünikasyon kanallarından geçen dış istihbarat, millî savunma, terörizm ve uluslararası suçlar ile siber güvenlikle ilgili verileri toplayabilir."*

[347] GÜL, s. 110.

[348] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 910.

D. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

1. Teşebbüs

Failin veri nakillerini izlemeye yönelik elverişli icra hareketlerine doğrudan doğruya başlaması ancak elinde olmayan nedenlerle bu hareketlerin yarıda kalması ve izlemenin gerçekleşememesi halinde suça teşebbüsten bahsedilecektir[349].

Belirtmek gerekir ki suç neticesiz bir suç olduğundan, veri izlemeye başlayan failin elinde olmayan nedenle bunu devam ettirememesi halinde suç tamamlanmış olacağından teşebbüs söz konusu olmayacaktır.

Veri izlemek için teknik araç temin edilmesi suça hazırlık hareketi olup icra hareketleri olarak nitelendirilemez. Kural olarak hazırlık hareketleri cezalandırılmasa da, TCK'nın 245/A maddesi kapsamında bu cihazların temin edilmesi ayrıca suç olarak düzenlenmiştir[350].

2. İştirak

Suç, iştirak bakımından bir özellik taşımamaktadır. Bu çerçevede iştirak değerlendirilirken TCK m. 37, 38 ve 39'daki düzenlemeler dikkate alınacaktır.

[349] DÜLGER, s. 332.; İHTİYAROĞLU, s. 430.

[350] APAYDIN, *"Bilişim Sistemine Girme, Engelleme ve Bozma Suçları"*, s. 150, 151.

3. İçtima

Failin bir suç işleme kararı vererek birbirinden farklı zamanlarda bir bilişim sisteminin kendi içerisinde veya aynı iki bilişim sistemini arasında gerçekleşen veri nakillerini teknik araçlarla izlemesi halinde zincirleme suç hükümleri uygulanacaktır.

MIM saldırıları[351] *(Man-in-the-middle attack)* olarak bilinen, iki kişi arasında bilişim sistemleri vasıtasıyla gerçekleştirilen iletişimin izlenmesi eylemi hem bu suçu hem de TCK m. 132/1'in ilk cümlesinde düzenlenen[352] *"Haberleşmenin Gizliliğini İhlal"* suçunu oluşturur. Tek fiille birden fazla suç oluştuğundan, fikri içtima hükümleri gereğince faile daha ağır cezayı öngören *"Haberleşmenin Gizliliğini İhlal"* suçundan hüküm kurulacaktır.

Fail, teknik araçlarla veri akışını izlerken ayrıca sisteme girmişse *"Bilişim sistemine girme veya sistemde kalma (TCK m. 243)"*, sistemdeki verilerin naklini engellemişse *"Verileri yok etme veya değiştirme (TCK m. 244/2)"* , bu veriler aynı zamanda haberleşme niteliğindeyse ve fail bu içeriğe vakıf olmuşsa *"Haberleşmenin gizliliğinin ihlali (TCK m. 132)"*, haberleşmeyi engellemişse *"Haberleşmenin engellenmesi (TCK m. 124)"*, kişisel verileri ele geçirmişse *"Verileri hukuka aykırı olarak verme veya ele geçirme (TCK m. 136)"* suçlarından birinden sorumlu olacaktır[353].

---

[351] Bu saldırılarda saldırgan iki kişi arasında devam eden bir iletişimi kontrol etmektedir. Ayrıntılı bilgi için bkz. MARION – TWEDE, s. 216.

[352] TCK m. 132/1, ilk cümle: *"Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."*

[353] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 911.

E. YAPTIRIM, ZAMANAŞIMI, GÖREVLİ VE YETKİLİ MAHKEME

Suç için öngörülen ceza, bir yıldan üç yıla kadar hapis cezasıdır. Suçun soruşturulması ve kovuşturulması re'sen yapılacaktır.

Bu suç bakımından özel bir düzenleme olmadığından, TCK'nın 66. maddesinde düzenlenen "genel dava zamanaşımı süreleri" uyarınca *"Veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçu"*nun dava zamanaşımı süresi sekiz yıl olacaktır. Suç kesintisiz bir suç olup failin veri nakillerini izlemeye devam ettiği müddetçe temadi eder[354]. Bu bakımdan dava zamanaşımı, temadinin sona erdiği tarihten itibaren başlar[355]. Bu bakımdan CMK'nın 12. maddesi uyarınca kesintinin gerçekleştiği yer, suçun işlendiği yer olup bu yer mahkemesi kovuşturma yapmaya yetkilidir.

Görevli mahkeme ise 5235 sayılı *"Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun"*un 11. maddesi uyarınca asliye ceza mahkemesidir. Ancak HSK Birinci Dairesinin Kararı dolayısıyla bu suç bakımından da 15.12.2021 tarihi itibariyle faaliyete geçen bilişim ihtisas mahkemeleri görevlidir.

[354] KABADAYI, s. 122.; ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 332.

[355] APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 153.

ÜÇÜNCÜ BÖLÜM

SİSTEMİ ENGELLEME, BOZMA; VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇU (TCK m. 244)

I. GENEL BİLGİLER

244. maddede *"Sistemi engelleme, bozma; verileri yok etme veya değiştirme suçu"* düzenlenmiştir. Buna göre:*"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."*

Maddenin 1. ve 2. fıkralarında üç ayrı suçun düzenlendiği görülmektedir. Buna karşılık 3. ve 4. fıkrada ise suçun nitelikli hallerine yer verilmiştir.

765 sayılı ETCK'nın 525/b maddesinde, bu suça benzer bir suç bulunmaktaydı. 244. maddenin ilk iki fıkrasındaki suçlar, 765 sayılı ETCK'nın 525/b maddesinin 1. fıkrasında bazı farkları olmakla beraber aynı cezayla cezalandırılan tek suç olarak

düzenlenmişti[356]. TCK 244. maddesinde, ETCK'dan farklı olarak *"verileri erişilmez kılmak, sisteme veri yerleştirmek ve var olan verileri başka bir yere göndermek"* hareketleri de suç olarak düzenlenmiş; *"sisteme zarar vermek"* ifadesine metinde yer verilmemiştir[357].

Maddenin 1. fıkrasında yer alan *"Bilişim sistemini engelleme veya bozma suçu"*nun AKSSS'nin *"Sistem engellemeleri"* başlıklı 5. maddesine karşılık geldiği söylenebilir. Buna göre *"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 bilerek ve isteyerek engellenmesi durumunu kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir."*

Maddenin 2. fıkrasında yer alan *"Bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin bir başka kişiye gönderilmesi suçu"* ise Sözleşmenin *"Veriye müdahale"* başlıklı 4. maddesine tekabül etmektedir. Buna göre *"Taraflardan biri bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilmez kılınması fiillerinin bilerek ve istenerek gerçekleştirilmesi halini kendi ulusal mevzuatı kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer tedbirleri kabul edecektir. (2) Taraflar yukarıda paragraf 1'de*

---

[356] **AKBULUT**, Berrin, *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"*, SÜHFD, C. 24, S. 2, 2016, s. 10.

[357] **MUCUK**, Melike Hafsa, *"Bilişim sistemine girme (TCK 243) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK 244) suçları"*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2022, s. 94.

tanımlanan fiili söz konusu fiilin ciddi zararla sonuçlanması şartına bağlanma hakkını saklı tutabilir."

Karşılaştırmalı hukukta, Alman Ceza Kanunu, *"Mala zarar verme (m. 303 Sachbeschädigung)"* başlığı altında yaptırıma bağlanan 303a ve 303b maddeleriyle TCK m. 244'e yakın düzenlemeler içermektedir [358].

İtalyan Ceza Kanunu'nunda da Almanya'dakine benzer şekilde, ilgili suç, malvarlığı aleyhine suçlar kısmında düzenlenmiştir. Kanun'un 635-bis ve 635-ter maddesinde *"Bilgisayarlar ve Enformatik Sistemlere Zarar Verilmesi Suçu"* başlığı altında bilişim sistemlerine ve telematik sistemlere, bunların programlarına veya bunlar içindeki verilere zarar verilmesi, bozulması, tamamen ya da kısmen kullanılamaz hale gelmesi hareketleri cezalandırılmıştır. Bu hususa ilişkin İtalyan öğretisinde, bilişim sistemlerindeki verilerin ve programların, yazılımların veya gayri maddi malların korunması gerekliliğinin bilgisayar mallarının bütünlüğünün korunmasına yönelik bir unsur olduğu ve mal bütünlüğünün korunmasından ayrı düşünülemeyeceği belirtilmiştir[359].

Görüldüğü üzere İtalyan ve Alman kanun koyucu, bilişim sistemlerini ve sistemdeki verileri malvarlığı değeri olarak ele almış ve bunlara verilecek zararların cezasını malvarlığı aleyhine suçlar başlığında düzenlemiştir.

---

[358] ERDAĞ, s. 291. Alman Ceza Kanunu, Madde 303/a*"(1) Hukuka aykırı olarak (202a maddesi ikinci fıkrası anlamındaki) verileri silen, gizleyen, kullanılmaz hale getiren veya değiştiren kişi, iki yıla kadar hapis veya (adli) para cezası ile cezalandırılır. (2) Bu suça teşebbüs cezalandırılır. (3) Birinci fıkrada tanımlanmış bulunan suça hazırlık hareketleri hakkında, 202c maddesi, gereğince uygulanır."* Tercüme edip aktaran: ERDAĞ, s. 292.

[359] CAPPELLINI, s. 812.

II. SUÇA İLİŞKİN ÖN AÇIKLAMALAR

A. SUÇUN HUKUKİ KONUSU

Maddenin 1. fıkrasında düzenlenen *"Bilişim sisteminin işleyişinin engellenmesi veya bozulması suçu"*'nun koruduğu hukuki değer konusunda öğretide bir görüş birliği yoktur. Suçla korunmak istenen değere ilişkin bilişim sisteminin güvenliği, zilyetlik ve mülkiyet hakkı[360], bilişim sistemi üzerinde tasarruf yetkisi olan kişinin sistemi herhangi bir engel olmaksızın kullanmasına ilişkin çıkarı[361], yalnızca mülkiyet veya malvarlığı hakkı[362], kişinin sahip olduğu malvarlığı değeri ve bilişim sistemlerine duyulan güven[363], bilişim sisteminin işleyişinin kişinin toplumla kişisel, ekonomik, sosyal etkileşimini sağlayan değer[364], bilişim ortamının korunması ve güvenilir şekilde işlenmesine ilişkin ferdi-kamusal yarar[365] şeklinde görüşler bulunmaktadır.

Maddenin 2. fıkrasında düzenlenen suçla korunan hukuki değer irdelenirken, bu suçta bilişim sistemine değil içindeki verilere yönelik bir ihlal olduğu göz önünde bulundurulmalıdır. Hal böyle olunca, korunan hukuksal değer, verilerin üzerinde tasarruf yetkisi olan kişilerin verileri dilediği gibi, engel veya müdahale olmaksızın

[360] ÖZBEK – DOĞAN – BACAKSIZ, s. 989.

[361] DÜLGER, s. 336.; DEMİRCAN, s. 103.

[362] KURT, s. 162.; TEZCAN – ERDEM – ÖNOK, s. 1182.; YAŞAR – GÖKCAN – ARTUÇ, s. 7307.

[363] GÜL, s. 131.

[364] KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 91.

[365] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 490.

kullanabilmesine ilişkin çıkardır[366]. AKSSS Açıklayıcı Raporunda, 4. maddede düzenlenen *"Veriye müdahale"* suçuyla korunmak istenen değerin, "*Mala zarar verme suçu"* ile korunmak istenen değere benzer bir nitelik arz ettiği ifade edilmiştir[367]. Bu benzetmenin ardından, suçun koruduğu değerin bilgisayar verileri ve programlarının düzgün işleyişi ve bütünlüğü olduğu[368] belirtilmiştir.

Yargıtay, eski tarihli kararlarında AKSSS açıklayıcı raporuna paralel şekilde 1. ve 2. fıkradaki suçların klasik *"Mala zarar verme suçu"*nun özel bir şekli olduğu görüşündedir[369]. Buna karşılık yeni tarihli kararlarında, 244. maddedeki düzenleme ile *"bilişim sistemlerinin doğru ve işlevine uygun şekilde faaliyetine devam etmesinin amaçlandığını"*[370] belirtmektedir.

Yargıtay'ın içtihadına paralel olarak suçla korunmak istenen değerin *"Mala zarar verme suçu"*yla korunan hukuki değere benzediğini düşünen ve buradan yola

[366] ARTUK – GÖKCEN – YENİDÜNYA, s. 853, 854.; DÜLGER, s. 326.; AKBULUT, Bilişim Alanında Suçlar, s. 77.

[367] Bkz. Açıklayıcı Rapor 60. paragraf: *"The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage."* https://rm.coe.int/16800cce5b (E.T. 13.02.2024)

[368] İtalyan öğretisinde de baskın görüş, TCK m. 244'e paralel bir düzenleme olan 635-bis ve 635-ter maddelerinin koruduğu değerin veri, program ve bilgi sistemlerinin bütünlüğü ve güvenliği olduğu yönündedir. Bkz. CAPPELLINI, s. 825.

[369] CGK., E. 2009/193, K. 2009/268, T. 17.11.2009.; 8. CD., E. 2015/14782, K. 2016/4928, T. 12.4.2016; 11. CD., E. 2009/1616, K. 2009/11328, T. 07.10.2009. https://karararama.yargitay.gov.tr (E.T. 20.02.2024)

[370] 8. CD., E. 2019/9478, K. 2020/15892, T. 23.9.2020. https://karararama.yargitay.gov.tr (E.T. 20.02.2024)

çıkarak öğretide, suçla korunan hukuki değerin mülkiyet hakkı veya malvarlığı hakkı olduğuna ilişkin görüş çoğu yazar tarafından kabul görmektedir[371].

Yukarıda verilen işçiye tahsis edilen bilişim sistemi örneğindeki gibi sistemin engellenmesi veya bozulması fiilinden her zaman malikin zarar görmediği, zilyetlik sıfatına sahip olan kişilerin mağdur olduğu göz önünde bulundurulduğunda, ben suçun hukuki konusunun mülkiyet veya malvarlığı hakkı olduğu görüşüne katılmıyorum. Kaldı ki suç, bilişim sistemlerinin günümüzde toplumun ayrılmaz bir parçası haline gelmesi ve birey menfaatinin ötesinde anlam ifade etmesiyle, *"Kişilere Karşı Suçlar"* kısmının *"Malvarlığına Karşı Suçlar"* bölümü altında değil, *"Topluma Karşı Suçlar"* kısmında düzenlenmiştir[372]. Gerçekten, Alman Ceza Kanunu, Fransız Ceza Kanunu ve İtalyan Ceza Kanunu gibi Türk Ceza Kanunu'na ilham kaynağı olan Kanunlarda bu suç *"Malvarlığına Karşı Suçlar"* başlığı altında yer almışken[373], kanun koyucumuzun suçu *"Malvarlığına Karşı Suçlar"* başlığı altında düzenlememesi de suçla korunan hukuki değerin malvarlığı olmamasına ilişkin bir tercihidir. Bu itibarla, kanaatimce korunmak istenen değer malvarlığı veya mülkiyet hakkından ziyade, toplumun bilişim sistemlerinin ve içindeki verilerin düzgün işleyişine ilişkin çıkarıdır[374].

[371] TEZCAN – ERDEM – ÖNOK, s. 1182.; KURT, s. 161.; YAŞAR – GÖKCAN – ARTUÇ, s. 7307.

[372]HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 490.; KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu",* s. 91.

[373] KETİZMEN, s. 120.

[374] Aynı yönde bkz. HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar s. 490.; ORTA, s. 116.

B. SUÇUN MADDİ KONUSU

Suçun konusu 1. fıkradaki suç açısından bilişim sistemidir. Maddenin gerekçe metninde *"Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır."* şeklindeki ifadeyle bilişim sisteminin yazılım ve donanım unsurlarının suçun konusu olduğu belirtilmiştir. Suçun konusu yalnızca hareketin yöneldiği bir insan veya bir eşya olabileceğinden öğretide 1. fıkradaki suçun konusunun bilişim sisteminin işleyişi olduğu görüşüne[375], bilişim sisteminin işleyişi maddi bir varlık olmadığından katılmak mümkün değildir.

Maddenin 2. fıkrasında *"bilişim sisteminin içindeki veriler"* ifadesine yer verildiğinden, öğretide bilişim sisteminin içinde yer almayan verilerin suçun konusunu oluşturmayacağına ilişkin bir görüş bulunmaktadır[376]. Kanaatimce de kıyas yasağı gereği; CD, flash bellek, disket gibi sisteme bağlı bir faaliyet göstermeyen ve münhasıran bilişim sistemi olarak nitelendirilemeyecek veri saklama aletlerinin içinde yer alan veriler, suçun konusunu oluşturmamalıdır.

C. FAİL

Suçun faili herhangi bir kişi olabilir. Bu açıdan suç, özgü suç değildir.

---

[375] Görüş için bkz. AKBULUT, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme, s. 24.

[376] **KOCA**, Mahmut, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, (9-10 Ekim 2008) Bilişim Hukuku Konferansı, Yargıtay Başkanlığı Yayını, Ankara 2008, s. 94.; TEZCAN – ERDEM – ÖNOK, s. 1183. Aksi görüş için bkz. AKBULUT, Bilişim Alanında Suçlar, s. 85.

Suçun failinin tespiti her zaman kolay olmamaktadır. Bu noktada öncelikle, failin hareketinin bilişim sistemine mi yoksa verilere mi yöneldiğini tespit etmek gerekir. Daha sonra ise, sistem ve veriler üzerindeki mülkiyet, kullanım veya tasarruf yetkisinin kime ait olduğunun araştırılması gerekmektedir[377]. Yargıtay 11. CD de bir kararında[378] sistemi ve içindeki verileri kullanma yetkisine sahip olan kişinin verilere zarar vermesinin bu suçu oluşturmadığını şu şekilde ifade etmiştir: *"Sisteme veri yerleştirme suçunun oluşması için; hukuka aykırı olarak girilen sisteme, veri sağlayıcısı tarafından izin verilmeyen şekilde veri girişi yapmak ya da veri taşıma araçları ile yükleme yapmak gerekir. Fail ise açıklandığı gibi veriler üzerinde tasarruf yetkisine sahip olmayan, sisteme hukuka aykırı giren kişidir. Somut olayda; şirketin yetkili temsilcisi olan sanığın katılan kurum ile yapılan sözleşmeye istinaden kurumun verdiği şifreyle sisteme hukuka uygun şekilde girerek, e-bildirge içeriğine doğru olmayan verileri yerleştirmesi sonucu kuruma elektronik ortamda gerçek olmayan bir beyanı iletmekten ibaret eyleminde atılı suçun açıklandığı üzere unsurları itibariyle oluşmadığı anlaşılmıştır."*

Buna karşılık sistemin sahibi olan bir kişi, sistemi kullanma hakkına sahip bir kimsenin tasarrufunda bulunan verilere zarar vermişse, 2. fıkrada düzenlenen suçun faili olduğu kabul edilmelidir[379].

---

[377] Yargıtay 11. CD., E. 2018/6275, K. 2021/2806, T. 18.3.2021: *"Sistemdeki verilere müdahale niteliğindeki bu eylemleri gerçekleştiren kişiyi (faili) tespit için ise; mülkiyet, tasarruf ve kullanım yetkisine bakmak gerekecektir."* www.kazanci.com.tr (E.T. 1.02.2024)

[378] 11. CD., E. 2018/6275, K. 2021/2806, T. 18.3.2021. https://karararama.yargitay.gov.tr (E.T. 10.02.2024)

[379] AKBULUT, *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"*, s. 19.; **GEÇMEZ**, İrem, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244), Seçkin Yay., Ankara 2020, s. 123.

Son olarak, failin başka bir kişiye ait bir bilişim sisteminde bulunan ancak failin kendisinin tasarruf alanında olan verilere zarar vermesi halinde 2. fıkradaki suç oluşmayacaktır. Nitekim 2. fıkradaki suçun konusu bilişim sistemi değil fakat veriler olduğundan, kişinin kendi tasarrufunda olan, dilediğince tasarruf edebileceği verilere zarar vermesi halinde bilişim sistemi bir başkasına aitse bile suç teşkil etmeyecektir.

D. MAĞDUR

Mağdurun toplum değil, gerçek kişi olduğu görüşü kabul edilecek olursa *"Sistemi engelleme veya bozma suçu"* açısından mağdur, sistem üzerinde tasarruf yetkisi olan kişidir[380]. Verilere müdahaleyi cezalandıran 2. fıkradaki suç açısından ise mağdur, veriler üzerinde hak sahibi olan kişilerdir.

Dikkat edilirse, her zaman sistem veya verinin sahibi bu suçun mağduru olmayabilecektir. Örneğin bir iş yerinde iş sözleşmesi boyunca işçiye tahsis edilmiş olan bilgisayardaki sisteme zarar verilmesi halinde suçun mağduru bilgisayarın maliki olan işyeri değil, bilgisayarı kullanma ödüncü alan işçi olacaktır. Bu bakımdan sistemin veya verilerin üzerinde herhangi bir şekilde tasarruf yetkisi olan kişiler mağdur olabilecekken, sistem veya verinin sahibi her zaman mağdur olarak nitelendirilemeyecektir. Kısacası verilerin zarar görmemesini isteme hakkı veya sistemin aksamadan çalışmasındaki yarar kime aitse suçun mağduru da odur[381].

---

[380] **YILMAZ**, Sacit, *"5237 Sayılı Tck'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar"*, TBB Dergisi, 2011, S. 92, s. 70.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 265.

[381] AKBULUT, Bilişim Alanında Suçlar, s. 81.

Tüzel kişilerin bu suçun mağduru olup olamayacağı konusunda öğretide tartışma bulunmaktadır. Yargıtay, 2022 tarihli bir kararında[382] *"Bilişim sistemindeki verileri bozma yok etme, erişilmez kılma suçundan suçunun mağduru ... Bankası A.Ş'ye..."* şeklindeki ifadeleriyle suçun mağdurunun tüzel kişi olabileceği görüşünü benimsediği görülmektedir.

[382] 8. CD., E. 2022/1413, K. 2022/7668, T. 24.05.2022. https://karararama.yargitay.gov.tr (E.T. 13.02.2024)

III. SUÇUN UNSURLARI

A. MADDİ UNSUR

1. Hareket

a. Bilişim Sisteminin İşleyişinin Engellenmesi veya Bozulması

1. fıkrada düzenlenen suçun oluşması için sistemin işleyişinin "engellenmesi" veya "bozulması" gerekmektedir. Bu kapsamda TCK m. 244/1 bakımından fiil iki farklı seçimlik hareketten ibarettir[383]. Bu hareketlerin birinin gerçekleşmesiyle suç oluşacaktır.

TDK çevrimiçi sözlüğünde "engellemek" kelimesi *"bir şeyin gerçekleşmesini veya yapılmasını önlemek"* olarak ifade edilmiştir. Bu kapsamda *"bilişim sisteminin işleyişinin engellenmesi"*, sistemin normal şartlarda yerine getirdiği işlevlerin gerçekleştirilememesi olarak tanımlanabilir.

Yargıtay 11. C.D., bilişim sisteminin işleyişinin engellenmesini *"...bilişim sisteminin verimli çalışmasının önlenmesi, icra ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi..."* olarak tanımlamıştır. Buna paralel olarak öğretide bilişim sisteminin işleyişinin engellenmesine veri işleme hızının düşmesi, istenilen performansta çalışmaması veya

[383] Öğretide bilişim sistemlerinin engellenmesinin veya bozulmasının hareket değil netice olduğu, bu kapsamda suçun serbest hareketle işlenebileceğini düşünen yazarlar bulunmaktadır. Bkz. KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 915.; AKBULUT, Bilişim Alanında Suçlar, s. 85, 86.

veri alışverişinin yavaşlaması gibi örnekler verilmiştir[384]. İfade etmeliyim ki, ben Yargıtay'ın görüşüne ve buna paralel olarak öğretide verilen örneklere katılmıyorum. Nitekim sistemdeki veri akışının yavaşlatılması veya sınırlandırılması, sistemin işleyişini engelleme kapsamında sayılamaz. Çünkü burada sistemin görevlerini eda etmesini önlemekten ziyade, sistemde gerçekleşen olağan dönemdeki akışın hızını yavaşlatmak veya bu akışı zorlaştırmak söz konusudur. Gerçekten, sistemi engellemeksizin sistemdeki veri alışverişinin yavaşlatılması, sistemin eskisi kadar hızlı çalışmamasının sağlanması fiilleri *"engelleme"* veya *"bozma"* kapsamına girmediğinden kıyas yasağı gereğince cezalandırılamamalıdır[385]. TDK'nın *engelleme* ifadesinin tanımından çıkarılacak sonuç da budur. Kanaatimce, madde metnine *"bilişim sisteminin işleyişinin yavaşlatılması"* hareketi de eklenerek kıyas ihtimalinin önüne geçilmesi gerekirdi.

Sistemin işleyişinin engellenmesi, çoğunlukla DDoS atakları aracılığıyla gerçekleştirilmektedir. Yine yoğun spam (istenmeyen e-posta) bombardımanları da sistemin işleyişinin engellenebileceği bir diğer sisteme ve verilere müdahale tekniğidir.

Bilişim sistemi hiç kullanılmadan da sistemin engellenmesi mümkündür. Örneğin, iç ağda (intranet) bilgisayarları birbirine bağlayan kablolar kesilmek suretiyle sistem engellenebilecektir[386].

---

[384] KURT, s. 164.; DÜLGER, s. 342.

[385] Öğretide AKBULUT, kanun koyucunun *"bilişim sisteminin işleyişini engelleme"* ifadesinin kapsamını çok geniş tuttuğunu ve sistemin bozulması dışında sistemin verimliliğini engelleyen, yavaşlatılma da dahil her türlü müdahalenin bu kapsama girdiğini düşünmektedir. AKBULUT, Bilişim Alanında Suçlar, s. 86. Benzer yönde bkz. MAHMUTOĞLU, *"Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi",* s. 866, 867.

[386] ARTUK – GÖKCEN – YENİDÜNYA, s. 849.

Sözlükte "bozmak" kavramı ise *"bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek"* şeklinde tanımlanmıştır[387]. Bu halde sistem tamamıyla çalışamaz hale gelmekte, bir başka deyişle çökmektedir. Bozulan sistem kendisine verilen komutlara cevap vermemekte, veri alışverişi gerçekleştirmemekte, işlevlerini kalıcı olarak yerine getiremez duruma gelmektedir[388].

Yargıtay 11. C.D., bilişim sisteminin bozulmasını *"...bilişim sistemine dahil olan mekanik parçanın veya bir yazılım programının esasen yapması gereken özgülendiği işlevi yapamayacak hale getirilmesi ile birlikte sistemin engellenmesi halinin en üst noktası olan durma noktasından daha ileri olarak sistemin çökertilmesi, zarara uğratılması, işlemez hale getirilmesi, hatta, fiziki olarak dahi zarar verilmesi anlaşılmalıdır."*[389] şeklinde tanımlamışsa da kanaatimce bu tanım da doğru olmamıştır[390]. Nitekim bilişim sistemine veya sisteme dahil olan parçalara fiziksel müdahalenin bilişim suçu olarak değerlendirilebilmesi, *"Mala Zarar Verme Suçu (TCK m. 151)"* karşısında mümkün olmamalıdır. Her ne kadar madde gerekçesinde de *"sistemin fiziki varlığı ve işlemesini sağlayan bütün diğer unsurların"* suçun konusu olduğu belirtilmişse de suçun düzenlendiği yer dikkate alındığında yalnızca soyut unsurlara ilişkin müdahalelerin cezalandırıldığı sonucu çıkarılmalıdır[391]. Diğer bir deyişle, fail sistemin donanımını fiziki saldırılarla tahrip etmesi neticesinde sistemin

[387] https://sozluk.gov.tr/ (E.T. 22.02.2024)

[388] YILMAZ, *"5237 Sayılı Tck'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar"*, s. 72.; AKBULUT, *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"*, s. 30, 31.

[389] 11. C.D., E. 2014/7245, K. 2014/5492, T. 24.03.2014. www.kazanci.com.tr (E.T. 22.02.2024)

[390] Benzer yönde DÜLGER, s. 339, 340.

[391] KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 93.

işleyişi engellendiyse yahut bozulduysa, "*Mala Zarar Verme Suçu* (TCK m. 151)" oluşturduğunun kabulü gerekir[392].

Sistemin işleyişinin engellenmesi ve bozulması arasındaki fark, engelleme durumunda müdahale bittiği veya yapılan müdahalenin sona erdiği anda sistemin tekrar işlevlerini yerine getirebilmesi söz konusuyken; bozma durumunda sistemin fonksiyonları müdahale sona erse dahi sistem kalıcı olarak çalışmaz hale gelmiş olmaktadır.

Öte yandan, sistemin işleyişinin bozulması kalıcı olduğundan, sistemin işleyişini engellemeye kıyasla daha ağır sonuçlar doğuracaktır. Bu doğrultuda engelleme ve bozma hareketlerinin cezasının aynı olması kanaatimce hatalı olmuştur. Bu kapsamda, sistemin işleyişinin yavaşlatılması, engellenmesi ve bozulması olarak üç ayrı suç düzenlenmeli ve sırasıyla kademeli olarak cezanın artırılması gerekirdi.

[392] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 491.; ERDAĞ, s. 289, 290.; TEZCAN – ERDEM – ÖNOK, s. 1184.; Aksi yönde bkz. AKBULUT, Bilişim Alanında Suçlar, s. 87, 88. Yazar hükmün gerekçesine paralel olarak, bilişim sisteminin donanımına verilecek fiziki tahribatların ve zararların TCK m. 244/1 kapsamında değerlendirilebileceğini düşünmektedir.

b. Verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme

Maddenin 2. fıkrasında, verileri hedef alan suç teşkil eden fiiller sayılmıştır. Sayılan fiiller seçimlik hareketli olup bir tanesinin gerçekleşmesiyle suç meydana gelmiş sayılır.

"Verilerin bozulması", kısaca verinin kullanılamayacak hale getirilmesidir. Bozma, verilerin içeriğinin bozulması olabileceği gibi veriye ulaşmayı sağlayan veri anahtar kodlarının bozulması şeklinde de olabilir. Bu durumda, ne yapılırsa yapılsın veriden amaçlanan veya planlanan fayda elde edilememektedir[393]. Bilgisayar virüsleri, verilerin bozulmasına yol açan en etkili kötücül yazılımlardan biridir.

"Verilerin yok edilmesi", verinin tekrar elde edilemeyecek biçimde ortadan kaldırılması anlamına gelir[394]. Verinin silinmesi eyleminin verinin yok edilmesi anlamına gelip gelmediği hususunda öğretide bir görüş ayrılığı mevcuttur.

Birtakım yazarlara göre verilerin silinmesi, silinen verilerin bulunduğu yerde ortadan kaldırılması ve veri sahibinin verisini bıraktığı yerde bulamaması sebebiyle verilerin yok edilmesi kapsamında sayılacaktır[395]. Buna göre bilişim sistemlerinde verileri bir daha ulaşılamayacak şekilde yok etmek her durumda mümkün

---

[393] YAŞAR – GÖKCAN – ARTUÇ, s. 7311.

[394] KURT, s. 168. Karşı yönde bkz. KETİZMEN, s. 138. Yazar, verilerin hak sahibinin büyük güçlüklerle verilere ulaşabileceği şekilde tasarrufundan çıkarılmasını da verilerin yok edilmesi kapsamında geniş yorumlamaktadır.

[395] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 263.; KETİZMEN, s. 139.; APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 270.; KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 94.; AKBULUT, Bilişim Alanında Suçlar, s. 93.

olmadığından, kanun koyucunun burada kastettiği mantıksal olarak yok etme yani silme eylemidir[396]. Ancak bu noktada, geri dönüşüm kutusunda bulunabilecek şekilde veriyi silme fiilinin 'yok edilme' kapsamında olmadığını vurgulamak gerekir. Gerçekten, verinin sistemin hiçbir yerinde bulunamayacak şekilde silinmesi gerekmektedir.

Diğer birtakım yazarlara göre burada verilerin tamamen ortadan kaldırılmış olmaması, yalnızca o veriye ulaşımı gerçekleştiren anahtar veriler değiştirilmesi gerekçesiyle verileri silme eylemiyle verilerin yok edilmesi eşdeğer anlamda değildir[397].

"Verilerin değiştirilmesi", veriyi başka bir biçime sokmak, var olduğu konumdan başka bir konuma taşımak, farklı bir duruma veya görünüme getirmek, yeni bir içerik kazandırmak olarak ifade edilebilir[398]. Verilerin değiştirilmesi, verilerin içeriğinin değiştirilmesi şeklinde olabileceği gibi bir bu verilere ulaşmayı sağlayan anahtar kodların değiştirilmesi şeklinde de olabilir. Nitekim Yargıtay'ın istikrarlı içtihadı, kullanıcının sosyal medya hesaplarına ulaşmasına yarayan şifresinin değiştirilmesinin *"verilerin değiştirilmesi"* kapsamında olduğuna yöneliktir[399].

---

[396] DÜLGER, s. 138.

[397] KURT, s. 168.

[398] YAZICIOĞLU, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, s. 262.; KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 95.; **GERÇEKER**, Hasan, Yorumlu & Uygulamalı Türk Ceza Kanunu (2 Cilt), B. 6, Seçkin Yay., Ankara 2022, s. 2208.

[399] 8. CD. E. 2018/8369, K. 2019/5454, T. 16.4.2019; *"...somut olayda Facebook şifresini değiştirmek suretiyle katılanın erişimini engelleyen sanığın eyleminin anılan Kanun'un 244/2. maddesinde düzenlenen bir bilişim sistemindeki verileri değiştirme suçunu oluşturduğu..."* Benzer yönde bkz. 12. CD., E. 2014/18179, K. 2015/564, T. 19.1.2015.; 12. CD., E. 2014/18179, K. 2015/564, T. 19.01.2015. https://kararara ma.yargitay.gov.tr/ (E.T. 25.02.2024)

CGK, önüne gelen bir uyuşmazlıkta, bir üniversite öğrencisinin başarısız olduğu sınav sonucu notlarının sisteme girilerek başarılı olacak şekilde değiştirilmesi eylemini verilerin değiştirilmesi olarak nitelendirmiştir[400].

"Verilerin erişilmez kılınması", verilerin üzerinde tasarruf yetkisi olan kişinin dilediği zaman ve yerde verilerine ulaşabilme imkanının yok edilmesi anlamına gelmektedir[401]. Buna göre veri bozulmamış yahut yok edilmemiştir ancak verilere ulaşım bir şekilde önlenmektedir[402]. Kanun koyucu madde metninde sürekli bir erişim engelinden bahsetmediğinden, verilere ulaşımın engellenmesinin geçici veya sürekli olması arasında fark bulunmamaktadır. Fidye yazılımlar kullanılarak verilerin şifrelenmesi ve belirli bir ücret ödene dek kullanıcının verilere ulaşmasının engellenmesi, verilerin erişilmez kılınmasına örnek gösterilebilir.

"Sisteme veri yerleştirilmesi", sistem üzerinde tasarruf yetkisi olan kişinin rızası alınmaksızın sisteme yeni verilerin eklenmesidir[403]. Bu veriler kötücül yazılım olabileceği gibi, zararsız yazılım da olabilir. Yani örneğin sisteme, hak sahibi olan kişinin haberi olmadan bir truva atı yerleştirilmesi ile tamamen eğlence amacı güden zararsız bir oyun yazılımının yerleştirilmesi arasında hareketin gerçekleşmesi açısından fark yoktur. Kanun koyucunun bu noktada bir ayrım gözetmediğine dikkat etmek gerekir.

"*Verilerin başka bir yere gönderilmesi*" ise bir bilişim sistemi içindeki verilerin başka bir bilişim sistemine ya da veri taşıma cihazına aktarılması, kaydedilmesi yahut

---

[400] CGK., E. 2007/44, K. 2007/200, T. 09.10.2007. https://karararama.yargitay.gov.tr/ (E.T. 25.02.2024)

[401] DÜLGER, s. 347.

[402] GERÇEKER, s. 1073.; ÖZBEK – DOĞAN – BACAKSIZ, s. 1003.; DÜLGER, s. 347.

[403] APAYDIN, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, s. 275.

kopyalanmasıdır[404]. Nitekim Yargıtay da önüne gelen bir uyuşmazlıkta bilişim sistemindeki verilerin CD'ye aktarılmasını bu kapsamda değerlendirmiştir[405]. Yine, verilerin internet üzerinden veya bluetooth gibi kısa mesafelerde veri aktarımı yapmaya yarayan kablosuz ağ standartları üzerinden de gönderimi sağlanabilir.

2. Hukuka Uygunluk Nedenleri

Hukuka uygunluk nedenlerinden ilgilinin rızası bu suçla bağdaşır niteliktedir. Sistem ve veriler üzerinde hak sahibi olan kişinin rızası dahilinde "sistemin işleyişinin engellenmesi, bozulması, verilerin bozulması, erişilmez kılınması, değiştirilmesi" veya maddede yazılan diğer fiillerin gerçekleştirilmesi suç oluşturmayacaktır. Örneğin *'format atma'* olarak bilinen, herhangi bir bilginin depolandığı ortamdan tamamen kaldırılmasını sağlayan işlemi ilgilinin rızası çerçevesinde gerçekleştiren kişi hukuka uygunluk kapsamında hareket etmiş olur. Dikkat edilmesi gereken husus şudur ki, kimi zaman veriler üzerinde tasarruf yetkisine sahip kişi ile sistem üzerinde tasarruf yetkisine sahip kişi aynı olmayabilir. Bu durumda sistem üzerinde tasarruf yetkisine sahip olan kişi, üzerinde hak sahibi olmadığı "verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması" gibi eylemlere geçerli bir rıza gösteremez.

Görevin ifası ve kanun hükmünün icrası kapsamında hareket edilmesi de bu suçla bağdaşan bir diğer hukuka uygunluk nedenidir. 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele*

[404] KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 95.

[405] 8. CD, E. 2013/3173, K. 2014/18506, T. 14.07.2014. (APAYDIN, Bilişim Suçları ve Bilişim Ceza Hukuku, s. 305, 306.)

Edilmesi Hakkında Kanun" çerçevesinde mahkeme kararıyla bir siteye erişiminin engellenmesi hukuka uygunluk nedenidir[406].

B. MANEVİ UNSUR

Suçun manevi unsuru kasttır. Suçun taksirli hali kanunda düzenlenmediğinden, taksirle işlenebilmesi mümkün değildir.

765 sayılı ETCK m. 525/b fıkrasının 1. cümlesinde sisteme veya verilere müdahale eden failde başkasına zarar verme veya kendine yarar sağlama maksadı aranmaktaydı. Bir başka deyişle, suçun gerçekleşmiş sayılması için genel kast yeterli olmayıp özel kasta[407] ihtiyaç duyulmaktaydı. Öğretide çokça eleştirilen bu duruma 5237 sayılı Kanun'da yer verilmemiştir. Yani suçun işlenebilmesi için genel kast yeterli olup failde özel bir saikin varlığı gerekmez. Bu itibarla, failin bilişim sisteminin "işleyişini engellediğini" veya "bozduğunu" ya da sistemdeki verileri "değiştirdiğini", "yok ettiğini", "bozduğunu", "erişilmez kıldığını", sisteme "veri yerleştirdiğini" veya "sistemdeki verileri başka yere gönderdiğini" bilmesi ve bunu istemesi yeterlidir.

Özel bir kastın varlığı aranmadığından, suçun olası kastla işlenebilmesi mümkündür[408].

---

[406] AKARSLAN, s. 50.

[407] Kanunun suçun oluşması için fiilin bilinçli ve iradi, yani kasten gerçekleştirilmesinden başka failin özel bir amaçla hareket etmesinin zorunlu olduğu hallerde özel kast söz konusudur.

[408] ARTUK – GÖKCEN – YENİDÜNYA, s. 850.

IV. SUÇA ETKİ EDEN NEDENLER

A. ÜÇÜNCÜ FIKRADA DÜZENLENEN NİTELİKLİ HAL

Maddenin 3. fıkrasında, *"1. ve 2. fıkrada yer alan fiillerin bir banka kurumuna veya bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde cezanın yarı oranında artırılacağı"* düzenlenerek suçun nitelikli haline yer verilmiştir.

Kamu kurum ve kuruluşları ifadesinden merkezi idare, yerel yönetimler ve hizmet yerinden yönetim kuruluşları da dahil olmak üzere tüzel kişiliği olsun veya olmasın tüm idari kuruluşlar anlaşılmalıdır[409].

Kredi kurumu, TCK'nın 158. maddesinin 1/j fıkrasında bahsedilmiş ve bu maddenin gerekçesinde "*Banka olmamasına karşın, kanunen borç para vermeye yetkili kılınan kurumlar"* şeklinde tanımlanmıştır.

Öte taraftan Bankacılık Kanunu'nda[410], "Banka" kavramından ise *"mevduat bankaları, katılım bankaları ile kalkınma ve yatırım bankaları anlaşılacağı (m.3)"* belirtilmiştir.

Bu nitelikli hale yer verilmesindeki esas neden, kamu veya banka kurumlarının bilişim sistemleri aracılığıyla yerine getirdiği bankacılık veya kamu hizmetlerini aksatılmasının yol açtığı yıkıcı sonuçlardır. Gerçekten, kurumların bilişim sistemleri altyapılarına gerçekleştirilen saldırılar, toplumu oluşturan fertlerin bu kurumların itibarlarına ve bilişim sistemlerin güvenliğine ilişkin itimadının sarsılmasına sebep olmaktadır.

---

[409] AKBULUT, Bilişim Alanında Suçlar, s. 102.

[410] R.G., 1.11.2005 T., 25983 S.

Kanun koyucunun esasen burada "hacktivizm" faaliyetlerini önlemeye çalıştığı söylenebilir. Nitekim çoğunlukla bu kurumların internet siteleri, hacktivistler tarafından toplumsal sorunlara dikkat çekmek, bu kurumların belirli bir tutumunu eleştirmek amacıyla güvenilirliğini sarsmak amacıyla hedef alınmaktadır.

Öğretide, nitelikli halin yalnızca kamu kurumları, bankalar ve kredi kurumlarıyla sınırlandırılması eleştirilmekte ve özel kurumların da menfaatlerinin aynı çerçevede korunması gerektiği belirtilmektedir[411]. Ben de bu görüşe katılıyorum. Hacktivistler tarafından sıklıkla özel nitelikteki kuruluşlar, şirketler de hedef alınmaktadır. Örneğin THY'deki işçi greve destek vermek amacıyla 2012 senesinde şirketin internet sitesine yoğun saldırılar gerçekleştirilmiştir. THY'nin toplumun nezdinde itibarı ve seçkin havacılık kurumlarından biri olması göz önünde bulundurulduğunda, bu şirketi hedef alan siber saldırıların tıpkı kamu kurumları, banka ve kredi kurumlarına yapılan saldırılar kadar infial yarattığı açıktır.

B. DÖRDÜNCÜ FIKRADA DÜZENLENEN NİTELİKLİ HAL

Maddenin 4. fıkrasına göre *"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 adli para cezasına hükmolunur."*

Öğretide, bu fıkranın bağımsız bir suç mu yoksa 1. ve 2. fıkralarda düzenlenen suçların ağırlatıcı sebebi mi olduğu yönünde bir görüş ayrılığı bulunmaktadır.

[411] AKBULUT, *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"*, s. 41.

Bir görüşe göre, bu fıkrayla TCK m. 244/1 ve 244/2'den bağımsız ve müstakil bir suç düzenlenmiştir[412]. Bu görüşe göre, bu bağımsız suç bileşik bir suçtur ve birinci ve ikinci fıkrada düzenlenen suçlar, bu suçun unsuru haline gelmiştir. Esasen Yargıtay da pek çok kararında, 244. maddenin 4. fıkrasından *"Bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama suçu"* şeklinde bahsetmiştir[413].

Bir diğer görüşe göre ise bu fıkra *"Sistemi engelleme veya bozma (244/1)"* ve *"Verileri yok etme veya değiştirme (244/2)"* suçunun nitelikli halini oluşturmaktadır[414]. Zira suçun nitelikli halinin düzenlendiği durumlarda, suçun temel şekliyle nitelikli hali arasında bir bağlılık devam eder. Gerçekten, 4. fıkrada geçen "*Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle"* ifadesi de esasında bu normun bağımsız olmadığını, temel suç tipine bağlılığın devam edildiğini ortaya koymaktadır[415].

Kanun yapma tekniği ve hükmün lafzı gereğince, 4. fıkra, suçun nitelikli hali olarak incelenecektir.

Nitelikli halin gerçekleşebilmesi için ilk koşul, ya *"bilişim sisteminin işleyişinin engellenmesi veya bozulması"* (1. fıkra) ya da *"bilişim sistemi içerisindeki verilerin bozulması, yok edilmesi, değiştirilmesi, sisteme veri yerleştirilmesi veya var olan*

---

[412] ARTUK – GÖKCEN – YENİDÜNYA, s. 859.; AKBULUT, Bilişim Alanında Suçlar, s. 112.; HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 496.; DÜLGER, s. 364.; **AÇIKGÖZ**, Emre İkbâl, Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4), Adalet Yay., Ankara 2020, s. 62.

[413] 8. C.D., E. 2021/3799, K. 2023/8515, T. 7.11.2023. www.kazanci.com.tr (E.T. 28.02.2024); 8. C.D., E. 2021/3477, K. 2023/8513, T. 7.11.2023. www.kazanci.com.tr (E.T. 28.02.2024); 8. C.D., E. 2020/11290, K. 2023/520, T. 14.2.2023. www.kazanci.com.tr (E.T. 28.02.2024).

[414] ÖZBEK – DOĞAN – BACAKSIZ, s. 1005.

[415] ÖZBEK – DOĞAN – BACAKSIZ, s. 1005.

verilerin başka bir yere gönderilmesi" (2. fıkra) fiillerinden birinin işlenmesi gerekmektedir.

İkinci olarak, gerçekleştirilen bu eylem dolayısıyla kendisi ya da üçüncü bir kişi lehine haksız bir çıkar elde edilmiş olmalıdır. Belirtmek gerekir ki, hukuken tasvip edilmeyen maddi ve manevi her türlü çıkar, haksız çıkar teşkil eder[416].

Son olarak, gerçekleştirilen bu eylemin bir başka suçu oluşturmaması gerekir. Yargıtay, *"başka bir suç oluşturmaması halinde"* ifadesinden, bu fıkradaki düzenlemenin tali norm niteliğinde olduğu, dolayısıyla bilişim sistemleri aracılığıyla haksız çıkar sağlanması halinde öncelikle kanunda düzenlenen diğer suçların (dolandırıcılık, hırsızlık vs) gerçekleşip gerçekleşmediğinin değerlendirilmesi gerektiği, şayet gerçekleştirilmediyse m. 244/4'teki düzenlemeye gidilebileceğini sonucunu çıkarmaktadır[417].

[416] MALKOÇ, s. 3835.; KOCA, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, s. 95.; Karşı yönde bkz. TEZCAN – ERDEM – ÖNOK, s. 1186. Yazarlar haksız çıkar ifadesinden her türlü menfaatin değil, yalnızca maddi menfaatin çıkarılması gerektiğini savunmaktadır.

[417] 8. CD., E. 2019/9478, K. 2020/15892, T. 23.9.2020. www.kazanci.com.tr (E.T. 28.02.2024) 13. CD., E. 2014/18554, K. 2015/1620, T. 22.1.2015. www.kazanci.com.tr (E.T. 28.02.2024)

V. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

A. TEŞEBBÜS

Öğretide TCK m. 244'te düzenlenen suça teşebbüs edilemeyeceğine ilişkin görüşler olmakla birlikte[418], baskın olan görüş suçun teşebbüse elverişli olduğu yönündedir. Gerçekten, bir bilişim sistemine veya içerdiği verilere zarar verilmesi amacıyla sisteme bir virüsün yüklenmesi ve bu yazılım harekete geçmeden sistemin sahibi tarafından fark edilip önlenmesi durumunda suça teşebbüs edilmiş olacaktır[419].

1. ve 2. fıkrada düzenlenen suç tipleri seçimlik hareketli oldukları için, sözgelimi failin suç tipinde yer alan hareketlerden iki tanesini yapması sonucunda hareketlerden birinin teşebbüs aşamasında kalması, diğerinin ise netice meydana getirmesi halinde suç tamamlanmış sayılacaktır[420].

B. İŞTİRAK

Suça iştirak bakımından özel bir durum söz konusu değildir. Bu çerçevede TCK'nın iştirake ilişkin genel hükümleri dikkate alınacaktır.

---

[418] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 492-494.

[419] DÜLGER, s. 359.

[420] DÜLGER, s. 359.

C. İÇTİMA

TCK m. 244'te düzenlenen suç, zincirleme suç şeklinde işlenebilir. Buna göre, failin farklı zamanlarda bir bilişim sisteminin işleyişini engellemesi veya sistemdeki verileri değiştirmesi halinde zincirleme suç hükümleri uygulanacaktır. Bilişim sistemine kalma suçunda değinilen zincirleme suça ilişkin tartışma burada da geçerlidir. Bu suçun mağdurunun gerçek kişi olduğu kabul edilirse, zincirleme suç hükümleri yalnızca gerçek kişi mağdura karşı bir suçun icrası kapsamında birden fazla kez 244. maddedeki suçun işlenmesi halinde uygulanabilecektir. Mağdurun kamu idaresi veya toplum olduğu görüşünde ise suç kime karşı işlenirse işlensin, bir suçun icrası kapsamında farklı zaman aralıklarında işlendiği müddetçe zincirleme suç hükümleri uygulanabilecektir.

Belirtmek gerekir ki Yargıtay ilk görüşe paralel bir içtihat geliştirmiştir. Örneğin Yargıtay, bir kararında sanığın müştekiye ait facebook hesabıyla e-posta hesaplarının her ikisinin de şifresini kırarak hesaplarına erişip şifreyi değiştirmesi ve dolayısıyla sistemi erişilmez kılması eylemlerine, facebook ve e-mail farklı bilişim sistemleri olsa dahi mağdur aynı olduğundan, zincirleme suç hükümlerinin uygulanması gerektiğini belirtmiştir[421]. Bu karardan çıkarılacak bir diğer sonuç da, Yargıtay nazarında bilişim sistemlerinin farklı olması, mağdur aynı olduğu müddetçe zincirleme suç hükümlerinin uygulanmasına engel değildir.

Bilişim sisteminin işleyişini engelleyici hareketle *"Haberleşmenin engellenmesi suçu (TCK m. 124)"* işlenmesi de mümkündür. Bu kapsamda tek fiille birden fazla suç işlendiğinden, fikri içtima hükümleri uygulanmalı ve daha ağır yaptırıma bağlanmış olan 244. maddeden hüküm kurulacaktır.

[421] 12. CD., E. 2015/7239, K. 2016/7863, T. 4.5.2016. https://karararama.yargitay.gov.tr/ (E.T. 1.3.2024)

VI. YAPTIRIM, ZAMANAŞIMI, GÖREVLİ VE YETKİLİ MAHKEME

Bu suç bakımından bilişim sistemine girme suçundan farklı olarak, seçimlik adli para cezası öngörülmemiştir[422].

1. fıkrada düzenlenen suçun cezası bir yıldan beş yıla kadar hapis cezası; 2. fıkrada düzenlenen suçun cezası ise altı aydan üç yıla kadar hapis cezasıdır. 3. fıkrada düzenlenen nitelikli hal bakımından yani 1. ve 2. fıkradaki fiillerin *"bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi"* halinde verilecek ceza yarı oranında artırılacaktır. 4. fıkradaki nitelikli hal bakımından ise ceza, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasıdır. Bu cezalar seçimlik değildir. Hâkim, iki cezaya birden hükmetmek zorundadır.

1. ve 2. fıkrada düzenlenen suç bakımından dava zamanaşımı süresi sekiz yıldır.

TCK'nın 66. maddesinin 3. fıkrası hükmünce, dava zamanaşımının hesaplanmasında suçun nitelikli hali göz önünde bulundurulacaktır. Bu minvalde 3. ve 4. fıkradaki nitelikli hale ilişkin dava zamanaşımı hesaplamasında bu husus göz önünde bulundurulmalıdır. Bu kapsamda 1. fıkradaki fiilin *"bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi"* halinde cezanın üst sınırı dört yıl altı ay olduğundan, suça ilişkin dava zamanaşımı sekiz yıl olacaktır. Buna karşın 2. fıkradaki fiilin *"bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi"* halindeyse cezanın üst sınırı yedi yıl altı aydır ve dava zamanaşımı süresi on beş yıl olarak hesaplanmalıdır.

[422] HAFIZOĞULLARI – ÖZEN, Topluma Karşı Suçlar, s. 495.

4. fıkradaki nitelikli hal bakımından verilebilecek hapis cezasının üst sınırı altı yıl olduğundan, 66. maddede düzenlenen *"Genel dava zamanaşımı süreleri"* uyarınca, dava zamanaşımı süresi on beş yıldır.

Yetkili mahkeme, suçun işlendiği yerdeki mahkeme veya mağdurun yerleşim yerindeki mahkemedir.

Görevli mahkeme ise asliye ceza mahkemesidir. Ancak 25.11.2021 tarihi itibarıyla, HSK Birinci Dairesinin kararı çerçevesinde asliye ceza ve ağır ceza mahkemeleri bünyesinde belirlenen bilişim ihtisas mahkemeleri bu suça ilişkin davalara bakacaktır.

DÖRDÜNCÜ BÖLÜM

YASAK CİHAZ VEYA PROGRAMLAR SUÇU (TCK m. 245/A)

I. GENEL BİLGİLER

Gelişen bilişim teknolojisiyle birlikte teknolojik sistemlere zarar vermeye yönelik faaliyetler artmış, buna paralel olarak bu sistemlerin güvenlik duvarlarını rahatlıkla aşabilen cihaz, yazılım ve programlar üretilmeye başlanmıştır. Bu cihazların üretiminin ve kolaylıkla tedavül edilebilmesinin bilişim sistemlerine ve verilerin güvenliğine ciddi düzeyde tehdit oluşturduğu açıktır. İşte bu tehdidi bertaraf etmek isteyen kanun koyucu, bilişim sistemlerine ve verilere karşı suçlara giden yolu daha en başından, hazırlık hareketi sürecinde yasaklamak istemiştir. Esasen hazırlık hareketlerinin cezalandırılmaması kural olsa da Kanun'da sayılan istisnai durumlarda hazırlık hareketlerinin suç olarak kabul edilmiştir[423].

Maddeye göre, *"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."*

[423] **TAŞKIN**, Şaban Cankat, *"Ceza Hukukunda Cezalandırılabilirliğin Ön Alana Kaydırılması ve Hazırlık Hareketlerinin Cezalandırılması Sorununun Yasak Cihaz veya Programlar Suçu Özelinde İngiliz Ceza Hukuku, Kanada Ceza Hukuku ve Avrupa Konseyi Siber Suç Sözleşmesindeki Düzenlemelerle"*, Ceza Hukuku Dergisi, C. 19, S. 55, 2024, s. 256, 257.

Öğretide maddenin başlığı eleştirilmiştir. Gerçekten, *"yasak cihaz veya programlar suçu"* başlığıyla, suçun içeriği hakkında bir bilgi verilmemekte, yalnızca suçun maddi konusunu ön plana çıkarılmaktadır[424]. Öte yandan başlıkta yalnızca cihaz veya programa yer verilmesi, madde içinde bunlardan başka sayılan şifre veya sair güvenlik kodlarını açısından kapsayıcı olmamaktadır. Bu bakımdan öğretide, suçun başlığının, hareket unsuru ön plana çıkarılmak suretiyle *"suçta kullanılacak cihaz, program, şifre ve sair güvenlik kodunun üretilmesi, yayılması veya bulundurulması"* olması gerektiği savunulmaktadır[425].

Maddenin AKSSS'nin 6. maddesine paralellik arz ettiği açıktır. Zira Sözleşme'nin *"Cihazların kötüye kullanımı"* başlıklı 6. maddesinde akit devletlerden her birine *"Kasten ve haksız olarak yetkisiz erişim, yasadışı araya girme, veri engelleme ve sistemi engelleme suçlarından herhangi birinin işlenmesi amaçlı uyarlanmış veya tasarlanmış bir bilgisayar programı, donanım, bilgisayar şifresi, giriş kodu veya benzer verinin üretilmesi, satışı, kullanım için tedariği, ithali, dağıtılması veya elde edilebilir hale getirilmesi"* fiillerini suç olarak düzenleme yükümlülüğü getirilmiştir.

AKSSS açıklayıcı raporunda[426], bilişim sistemlerine ve verilere karşı suçlarının işlenebilmesi için faillerin *"erişim araçlarına"* ihtiyaç duyması ve bu gereksinimin de

---

[424] **YANAR**, Yasin, *"Ceza Hukuku ve Bilişim Hukuku Bağlamında TCK md. 245/A Yasak Cihaz veya Programlar Suçu",* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2019, s. 57.

[425] **KARAKURT EREN**, Ahu, *"Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre Ya Da Güvenlik Kodlarının Üretilmesi, Yayılması veya Bulundurulması Suçu",* TAAD, S. 43, Y. 11, 2020, s. 222, 223.; DÜLGER, s. 502.; ÖZBEK – DOĞAN – BACAKSIZ, s. 1057.

[426] Avrupa Konseyi Siber Suçlar Sözleşmesi Açıklayıcı Raporu, 71. paragraf.

güvenlik duvarlarını aşabilecek cihaz, donanım ve kodlar için bir karaborsa oluşturacağı vurgulanarak 6. maddede düzenlenen suçla bu karaborsanın oluşumunu engellemek istenildiği belirtilmiştir.

Karşılaştırmalı hukukta, Alman Ceza Kanunu'nun 202c hükmüyle veri casusluğu veya verilerin ele geçirilmesi suçunu işlemek için suç aletleri (program, cihaz, şifre vs) bulundurma ve tedavüle sokma suçu düzenlenmiştir[427]. Aynı Kanun'un verilerin değiştirilmesi suçunu düzenleyen 303a ve bilgisayar sabotajı suçunu düzenleyen 303b hükümlerinin 3. paragraflarında 202c maddesine atıf yapılmış, bu suçlar için de suç aletleri bulundurma ve tedavüle sokma eylemleri cezalandırılmıştır[428]. Yine aynı Kanun'un 263a/3 hükmüne bilgisayar dolandırıcılığı suçu için benzer bir hüküm düzenlenmiştir. Görüldüğü üzere, Alman Ceza Kanunu'nun muhtelif yerlerinde bilişim suçlarının işlenebilmesi için programların üretilmesi ve tedavüle sokulması cezalandırılmaktayken TCK'nın 245/A hükmü bu ihtiyacı tek başına karşılamaktadır[429].

İtalyan Ceza Kanunu'nda ise benzer bir hüküm, 615-quinquies maddesinde düzenlenmiş bulunmaktadır[430]. Bu maddenin TCK düzenlemesinden farklı yönü ise, TCK'daki düzenlemede hem bilişim sistemlerine ve sistemdeki verilere müdahale etmek için hem de bilişim sisteminin araç olarak kullanılması suretiyle işlenen diğer

---

[427] **ÜNAL**, Osman Gazi, *"Cezalandırılabilirliğin Ön Alana Kaydırılması Bağlamında, Yasak Cihaz veya Programlar Suçu (TCK M. 245/A)"*, AHBVÜD, C. 26, S. 2, 2022, s. 602.

[428] ÜNAL, s. 604, 605.

[429] ÜNAL, s. 605.

[430] *"Her kim, bir bilgisayar veya telekomünikasyon sistemine, bu sistemde bulunan veya bu sistemle ilgili bilgi, veri veya programlara hukuka aykırı olarak zarar vermek veya işleyişinin tamamen veya kısmen kesintiye uğramasını veya değiştirilmesini sağlamak amacıyla, hukuka aykırı olarak bilgisayar ekipmanı, cihazı veya programı temin eder, bulundurur, üretir, çoğaltır, ithal eder, yayar, iletir, teslim eder veya başka bir şekilde başkalarının kullanımına sunar veya kurarsa, iki yıla kadar hapis ve (günlük) 10 Euro'ya kadar para cezası ile cezalandırılır."*

suçların işlenmesi için cihaz, program, şifre vs üretilmesi ve tedavüle sokulması cezalandırılmışken; İtalyan Ceza Kanunu'ndaki düzenlemede AKSSS m. 6'ya paralel olarak yalnızca bilişim sistemlerine ve sistemdeki verilere müdahale etmek için bu tür suç aletlerinin üretimi ve tedavüle sokulması yaptırıma bağlanmıştır.

II. SUÇA İLİŞKİN ÖN AÇIKLAMALAR

A. SUÇUN HUKUKİ KONUSU

Bu suçla birlikte korunan hukuki değer toplumun bilişim sistemlerine duyduğu güvendir[431]. Çünkü suç olarak kabul edilen cihaz ve programların karaborsasının oluşturulması kamunun bilişim sistemlerinin güvenli olduğuna ve hukuka aykırı çıkar doğrultusunda kötüye kullanılamayacağına ilişkin güvenini sarsmaktadır.

Kanaatimce suç bir *"reato ostacolo"* yani *"engelleme suçu"*dur. Bu bağlamda, kanun koyucu bilişim sistemine ve verilere karşı suçların işlenmesini büyük ölçüde kolaylaştıran *"Cihaz ve programların üretimi ve tedavüle sokulmasını"* suç olarak düzenleyerek, bilişim sistemine ve verilere karşı suçların işlenmesinin önüne geçmeyi amaçlamaktadır.

B. SUÇUN MADDİ KONUSU

Suçun maddi konusunu *"Bilişim Alanında Suçlar"* bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar için oluşturulan cihaz, bilgisayar programı, şifre veya sair güvenlik kodu oluşturur[432].

---

[431] **KAYA**, İslam Safa – **ÇAKIR**, Adem, *"Yasak Cihaz veya Programlar Suçu"*, C. 19, S. 38, 2020, s. 42.; KOCA – ÜZÜLMEZ, Ceza Hukuku Özel Hükümler, s. 959.

[432] KOCA – ÜZÜLMEZ, Ceza Hukuku Özel Hükümler, s. 960.

"Bilgisayar programları" kavramından anlaşılması gereken her türlü yazılım dahil olmak üzere bilgisayar içinde komutları ve özel fonksiyonları yerine getirmek üzere tasarlanmış veriler bütünüdür. Örneğin verilere zarar vermek amacıyla oluşturulan truva atı yazılımları, bu madde kapsamında suç olarak kabul edilen bilgisayar programlarına örnektir.

"Cihaz" ise bilişim sistemine eklenebilen ve çıkarılabilen; bilişim suçlarının işlenmesine elverişli olan fiziki parçaları ifade etmektedir[433]. Örneğin bilişim sisteminin işleyişine müdahale etmek için DDoS saldırılarında araç olarak kullanılacak bilgisayarları zombi bilgisayarlara dönüştürebilmek için üretilen cihazlar madde kapsamında yasaklı cihazlardandır.

"Şifre", iddia edilen kullanıcı olduğunu ispatlamak veya herkes tarafından erişilemeyen yerlere erişebilmek için kullanılan harf, sembol ve rakamlardan oluşan dijital karakter dizisidir[434]. Şifre kırıcı saldırılarda saldırganın mağdurun şifresini kırabilmek için önceden elde ettiği bir dizi şifrelerden ibaret olan ve *"gökkuşağı tablosu"* olarak adlandırılan parola dizisi bu madde kapsamında yasaklı şifre olarak kabul edilebilir.

"Sair güvenlik kodu" ise, güvenliği sağlamak için oluşturulmuş ilave kodlardır[435]. Ses, parmak izi, avuç içi tanıma özelliklerini barındıran güvenlik unsurları buna örnektir[436].

[433] ÖZBEK – DOĞAN – BACAKSIZ, s. 1057, 1058.

[434] AKBULUT, Bilişim Alanında Suçlar, s. 245.; DÜLGER, s. 505.

[435] AKBULUT, Bilişim Alanında Suçlar, s. 245.

[436] DÜLGER, s. 505.

C. MAĞDUR

Suçun mağduru toplumdur. Çünkü bu suçun işlenmesiyle henüz herhangi bir kişinin bilişim sistemlerine veya verilerine yönelik somut bir ihlal söz konusu değildir[437].

D. FAİL

Suçun faili herkes olabilir, bu açıdan suç özgü bir suç değildir.

Suçun konusunu oluşturan cihazları satma veya başkalarına verme fiilleri açısından bunu gerçekleştiren failin karşısında bu cihazları satın alan veya kabul eden failler bulunur. Bu bakımdan suç, çok failli suç özelliği gösterir[438].

[437] **APAYDIN**, Cengiz, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, Terazi Hukuk Dergisi, C. 15, S. 163, 2020, s. 564.; AKBULUT, Bilişim Alanında Suçlar, s. 243.

[438] KOCA – ÜZÜLMEZ, Ceza Hukuku Özel Hükümler, s. 960.

III. SUÇUN UNSURLARI

A. MADDİ UNSUR

1. Hareket

Suç, seçimlik hareketli bir suç olup bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun "imal edilmesi", "ithal edilmesi", "sevk edilmesi", "nakledilmesi", "depolanması", "kabul edilmesi", "satılması", "satışa arz edilmesi", "satın alınması", "başkalarına verilmesi" veya "bulundurulması" hareketlerinden birinin yapılmasıyla meydana gelir.

"İmal etmek", maddede bahsedilen bilgisayar programı, cihaz, sair güvenlik kodu yahut şifrenin üretilmesini ifade eder. "*İthal etmek"*, bu tür bir cihazın, programın, şifre yahut güvenlik kodunun yurtdışından Türkiye sınırları içine sokulmasıdır.

"Sevk etmek", suçun konusunu oluşturan bilgisayar programı, cihaz, sair güvenlik kodu yahut şifrenin bir mekândan bir başka mekâna aracı vasıtasıyla gönderilmesidir[439]. *Nakletmek* ise suçun konusunu oluşturan cihaz, bilgisayar programı, şifre yahut sair güvenlik kodunun bir mekândan başka bir mekâna fail aracılığıyla iletilmesi olup, ağlar üzerinden gönderim de nakil işlemidir[440].

"Depolamak", bilişim suçlarını işlemeye yarayan bir bilgisayar programı, cihaz, sair güvenlik kodu yahut şifrenin dilendiği zaman erişilebilecek bir yerde

[439] APAYDIN, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, s. 565.

[440] APAYDIN, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, s. 566.

saklanmasıdır[441]. Kanaatimce, bu tür bir bilgisayar programı, cihaz, sair güvenlik kodu yahut şifrenin bilgisayara yüklenmesi (download) eylemini, *"depolanma"* kapsamında düşünmek gerekecektir. Zira internetteki veri arşivinin devasa boyutta olduğu ve her türlü içeriğe ilişkin denetlemenin yapılmasının neredeyse imkânsız olduğu göz önünde bulundurulacak olursa, bu tür program ve yazılımların internetten bulunarak bilgisayara yüklenmesi çok yaygındır. Bu şekilde yüklenen programlar bilgisayarda depolanmış olmaktadır. Bu sebeple, kanun koyucunun *"yükleme, indirme (download)"* eylemini maddede bizatihi saymamış olmasının önemi yoktur.

"Kabul etmek ve başkalarına vermek", suçun konusunu oluşturan bilgisayar programının, cihazın, sair güvenlik kodu yahut şifrenin bedel olmaksızın tasarruf alanına sokulması/tasarruf alanından çıkarılmasıdır[442]. "*Satmak ve satın almak"* ise, yukarıdaki fiillerden farklı olarak bir bedel karşılığında suçun konusu olan programın, cihazın, sair güvenlik kodunun yahut şifrenin alıcıya verilmesi/alıcı tarafından alınmasıdır.[443] Buna karşılık "*satışa arz etmek"* ise satma iradesinin ortaya konulduğu herhangi bir davranışı ifade eder.

2. Hukuka Uygunluk Nedenleri

Bu madde kapsamına giren cihaz, program, şifre veya sair güvenlik kodlarının kanunun verdiği yetkiye dayanılarak üretilmesi, ithal edilmesi veya bulundurulması vb.

[441] APAYDIN, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, s. 566.

[442] ÖZBEK – DOĞAN – BACAKSIZ, s. 1061.

[443] KAYA – ÇAKIR, s. 46.

hukuka uygun olduğundan, suç oluşmayacaktır. Gerçekten, suçla mücadele kapsamında kolluk güçleri ve adli bilişim laboratuvarlarında bu tür cihazlar bulunmaktadır[444].

Yetkili merci tarafından bir bilişim sistemi için CMK m. 134 kapsamında "*Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve elkoyma*" koruma tedbiri uygulanabilir. Bu bağlamda, sistemde bulunan şifrelerin çözülmesi için kolluk güçleri için özel program, cihaz veya şifrelerin üretilmesi ve bulundurulması halinde bu suç oluşmaz[445].

Yine, bir kurum bünyesinde çalışan bilişim uzmanlarının sistemi test etmek amacıyla bu tür cihaz ve programları oluşturması durumunda da kurumun rızası gündeme gelecek ve fiil suç teşkil etmeyecektir[446].

B. MANEVİ UNSUR

Suç, kasten işlenebilen bir suçtur. Suçun taksirli hali kanunda düzenlenmediğinden, taksirle işlenebilmesi mümkün değildir.

Bu bağlamda örneğin, içinde virüs barındıran programını, programı yeterince incelemediği için niteliğini bilmeden depolayan kişi bu suçu işlemiş olmaz.

Suçun oluşabilmesi için özel kastın varlığı gerekir. Nitekim madde metninde *"suçun konusunu oluşturan program, cihaz veya yazılımların münhasıran bilişim*

---

[444] DÜLGER, s. 507.

[445] ÖZBEK – DOĞAN – BACAKSIZ, s. 1062.

[446] TAŞKIN, *"Ceza Hukukunda Cezalandırılabilirliğin Ön Alana Kaydırılması ve Hazırlık Hareketlerinin Cezalandırılması Sorununun Yasak Cihaz veya Programlar Suçu Özelinde İngiliz Ceza Hukuku, Kanada Ceza Hukuku ve Avrupa Konseyi Siber Suç Sözleşmesindeki Düzenlemelerle",* s. 264.

alanında suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması" gerektiği belirtilmiştir. O halde, suçun konusunu oluşturan program, şifre, cihaz veya güvenlik kodu üretiminin bilişim suçunu işlemek maksadıyla üretildiği veya tedavüle sokulduğu ispat edilemedikçe failin kastından söz edilemez[447].

[447] PARLAR – ÖZTÜRK, s. 274.; APAYDIN, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, s. 565.

IV. SUÇUN ORTAYA ÇIKIŞ BİÇİMLERİ

1. Teşebbüs

Suç, sırf hareket suçudur. Herhangi bir neticenin ortaya çıkması aranmaz, hareketin yapılmasıyla suç da meydana gelmiş olur. Ancak hareketin parçalara bölünebilmesi halinde suça teşebbüs mümkündür. Örneğin cihaz, program, şifre ve kodun üretimine başlanmasına rağmen, kolluk görevlilerinin yaptığı baskınla üretim ve imal sürecinin tamamlanamaması halinde suça teşebbüs edilmiş olur[448].

2. İştirak

Maddede düzenlenen bu suç için iştirak hükümlerinin uygulanmasında herhangi bir özel durum yoktur. TCK'nın iştirake ilişkin genel hükümleri uygulanacaktır.

Satma veya başkalarına verme fiilleri açısından bunu gerçekleştiren failin karşısında bu cihaz, program yahut yazılımı satın alan veya kabul eden failler bulunur. Bu hareketler çok failli suç özelliğini taşıdığından suça iştirak olarak nitelendirilemez[449]. Zira burada satın alan ve satan; veren ve kabul eden, hepsi faildir.

[448] AKBULUT, Bilişim Alanında Suçlar, s. 253.; DÜLGER, s. 507.

[449] DÜLGER, s. 508.

3. İçtima

TCK m. 245/A'da düzenlenen suç tipi, işlenmesi planlanan bilişim suçları bakımından hazırlık hareketlerini cezalandırmaktadır. Dolayısıyla, amaç suçu işlemek için bu cihaz, program veya yazılımları üreten, tedavüle sokan kişiler hem bu suçu hem de amaç suçu işlemesi (örneğin bilişim sistemine yetkisiz erişim) halinde hem bu suçtan hem de amaç suçtan sorumlu tutulurlar[450]. Gerçekten, kanunda açıkça *"bileşik suç"* olarak öngörülmemiş ve *"araç – amaç suç ilişkisi"* bağlamında işlenen suçlarda, faile her iki suç için münhasıran ceza verilir[451].

Suçun konusunu oluşturan cihaz, program veya yazılımlardan çok sayıda üretilmesi, kabul edilmesi veya satın alınması halinde tek suç oluşacaktır. Ancak bu hareketlerin değişik zaman aralığında gerçekleşmiş olması halinde, sözgelimi failin 10 adet cihazı üretip sattıktan 1 yıl sonra, tekrar 10 program üretip satmışsa *"Zincirleme suç (TCK m. 43)"* hükümleri uygulanacaktır[452].

V. YAPTIRIM, ZAMANAŞIMI, YETKİLİ VE GÖREVLİ MAHKEME

Bu suç bakımından bir yıldan üç yıla kadar hapis cezası ve beş bin güne kadar adli para cezası öngörülmüştür. Bu cezalar seçimlik ceza olmayıp, cezalandırılabilirlik koşulu gerçekleştiği takdirde hâkimin her iki cezaya birden hükmetmesi gerekmektedir[453].

---

[450] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 962.; DÜLGER, s. 508.

[451] **AKSOY İPEKÇİOĞLU**, Pervin, *"Türk Ceza Kanunu'nda Bileşik Suç"*, AÜHFD, S. 61, C. 1, 2021, s. 65.

[452] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 962.

[453] DÜLGER, s. 508.

Kanun'da öngörülen yaptırım açısından bir orantısızlık söz konusudur. Şöyle ki; TCK 245/A'da düzenlenen suç, bilişim suçlarının hazırlık hareketlerinin cezalandırıldığı bir suçtur. Bu nedenle mantıken esas suç olan bilişim suçları için öngörülen cezalardan daha hafif bir yaptırıma tabi tutulması beklenir. Ancak, TCK'nın 243. maddesinde yer alan "Bilişim sistemine girme veya sistemde kalma" suçunun cezası, bir yıla kadar hapis veya adli para cezası olarak belirlenmiştir. Hazırlık hareketi niteliğindeki program, cihaz, şifre vb. üretimi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezasına tabi iken, asıl suç olan bilişim sistemine girme veya sistemde kalma fiilinin bir yıla kadar hapis veya adli para cezası ile cezalandırılması, açık bir orantısızlık teşkil etmektedir.

Bu suça ilişkin dava zamanaşımı süresi, TCK'nın 66. maddesi uyarınca sekiz yıldır.

Suç, şikâyete tabi bir suç değildir. Bu noktada soruşturma ve kovuşturma re'sen yapılır. Bu suç bakımından da bilişim ihtisas mahkemeleri görevlendirilmiştir. Suç bir neticesiz suç olduğundan, yani hareketin yapılmasıyla meydana geldiğinden, yetkili mahkeme hareketin kısmen veya tamamen gerçekleştiği yer mahkemesidir. Her ne kadar bilişim suçları bakımından mağdurun yerleşim yerindeki mahkeme yetkili kılınsa da 245/A'da düzenlenen suç bakımından belirli bir kişinin menfaati ihlal edilmediğinden, bu hükmün uygulanabilmesi mümkün değildir.

SONUÇ

Bilişim sistemine ve verilere karşı suçlar son yüzyılda meydana çıkmış olmasına karşın, geleneksel suçlardan çok daha basit şekilde işlenebilme özelliği sayesinde günümüz dünyasında uluslararası alanda üst düzey tehdit oluşturan suçlardır. Pek çok ülke, bu suçlarla mücadele konusunda hala verimli bir altyapı oluşturabilmiş değildir. Esasen, yargılama makamları dahi her gün güncellenen bilişim terimlerine ayak uydurabilecek bilgi ve birikime sahip olmayabilmektedir.

Türkiye'nin ceza mevzuatında ilk kez 1991 yılında yapılan değişiklikle düzenleme bulan *"Bilişim Alanında Suçlar"*, 2005 tarihli Türk Ceza Kanunu'nda suç tipleri genişletilmek suretiyle tekrar yer almıştır. Gerçekten, sürekli yeni türleri ortaya çıkan bilişim sistemine ve sistemdeki verilere müdahalelerle etkin mücadele bakımından kanun koyucu, zamanla ortaya çıkan yeni antisosyal fiilleri suç olarak düzenlemek zorunda kalmıştır. Örneğin, *"Bilişim Sistemine Girme"* (TCK m. 243) suçu, 1991 yılındaki düzenlemelerde yer almayan, 2005 tarihli yeni TCK ile düzenlenmiş bir suçtur. Bundan önce bilişim sistemine girme hareketi tek başına cezalandırılmıyor, *"sisteme girerek programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirme"* fiili cezalandırılıyordu. Veriler ele geçirilmeden de *"Bilişim sistemine girme veya kalma"* hareketlerinin suç olarak düzenlenmesinde 765 sayılı ETCK döneminde öğretide yapılan eleştiriler ve 2001 tarihli AKSSS etkili olmuştur. Bununla birlikte, bilişim sistemine girme veya sistemde kalma suçunun düzenlendiği 243. maddeye, 24.3.2016 tarihli KVKK ile 4. fıkra eklenmiş ve bu fıkrada teknik araçlarla veri naklini izleme suçu düzenlenmiştir. Bu itibarla, *"Bilişim Sistemine Girme"* suçu başlığı altında sisteme girme, sistemde kalma ve sisteme girmeksizin teknik araçlarla veri nakillerini izleme olmak üzere üç seçimlik hareketten oluşan bir suç düzenlenmiştir. Teknik araçlarla veri nakillerini izleme gerek AKSSS'de, gerekse

Alman ve İtalyan Ceza Kanununda farklı başlıklar altında ayrı bir suç tipi olarak düzenlenmişken; üstelik bu suçu bilişim sistemine girme suçundan ayıran en büyük unsurun sisteme girilmeden veri nakillerinin teknik araçlarla izlenmesiyken, suçun *"Bilişim sistemine girme veya sistemde kalma"* suçuyla birlikte düzenlenmesi teknik açıdan doğru olmamıştır. Yine TCK 243. maddede düzenlenen bir diğer seçimlik hareket olan "*sistemde kalma"* hareketine başlıkta yer verilmemesiyle madde içeriğini kapsayıcılıktan uzaklaşılmıştır. Bu bakımdan madde başlığının *"Bilişim sistemine girme veya sistemde kalma"* olarak değiştirilmesi ve *"Bilişim sistemine girmeksizin veri nakillerinin teknik araçlarla izlenmesi"* suçunun farklı bir başlık altında düzenlenmesi kanaatimce kanun tekniği açısından daha doğru olacaktır.

Kanunumuzun 244. maddesinde, *"Bilişim sistemini engelleme, bozma; verileri yok etme veya değiştirme suçu"* düzenlenmiştir. Bu suç 765 sayılı ETCK'nın 525/b maddesindeki suça benzemekle beraber, 525/b fıkrasında düzenlenen suçta başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadı aranmaktaydı. Oysaki AKSSS'nin bilişim sistemine ve sistemdeki verilere karşı suçlar bakımından taraf devletlere getirdiği yükümlülük, fiillerin hukuka aykırı ve kasten olması halinde cezalandırılması gerektiğidir. Yani bir ETCK'nın 525/b maddesinde aranan özel saikten sözleşmede bahsedilmemiştir. Bu bakımdan madde AKSSS ile uyumlulaştırılarak 5237 sayılı TCK'nın 244. maddesinde tekrar düzenlenmiş, suçun cezası aynı bırakılmış ve fakat suçun unsurlarında birtakım değişikliklere gidilmiş, suç genel kastla işlenebilen bir suç haline getirilmiştir.

Yine, bilişim suçlarında kullanılan cihazların üretilmesi ve tedavüle sokulmasını cezalandıran *"Yasak Cihaz veya Programlar*" suçu, ilk defa 24/3/2016 tarihli ve 6698 sayılı KVKK ile TCK'nın 245/A maddesinde düzenlenmiştir. Bu suçla birlikte, bilişim sistemlerine ve sistemdeki verilere karşı suçlara giden yolculuk daha en başından cezalandırılmıştır. Zira Türkiye'nin taraf olduğu AKSSS'nin yükümlülüklerini yerine

getirmek ve Sözleşmeyle Kanunumuzun uyumlulaştırılması bakımından bu düzenleme yerinde olmuştur. Ancak yükümlülük bakımından AKSSS'de yer verilen "elektromanyetik dalgalar" ifadesine, Kanun'daki madde metninde de yer verilmesi gerekirdi. Bunun yanı sıra, suçta ve cezada kanunilik ilkesi göz önünde bulundurularak madde metninde yer alan teknik araç kavramının kapsam ve sınırlarının çizilmesi doğru olacaktır.

Bilişim sistemine ve sistemin içindeki verilere karşı suçların pek çoğunun cezasının üst sınırı beş yılı geçmemektedir. Halbuki günümüzde bilişim sistemleriyle bütünleşmiş olan yaşam faaliyetlerinde, bilişim sistemlerine yapılan en ufak bir müdahalenin dahi pek çok önemli hizmette aksama, pek çoğu bilişim sistemlerinde tutulan hayati verilerin kaybı sonucu doğurabileceği göz önünde bulundurulduğunda, bu derecedeki hapis cezasının caydırıcılıktan uzak ve zararı karşılamaktan yoksun olduğu görülmektedir. Üstelik bilişim dünyasının karmaşık ve suçları karanlıkta bırakmaya elverişli yapısı, failleri bu suçları işleme konusunda daha da cesaretlendirmektedir.

Son yıllarda asliye ve ağır ceza mahkemesi bünyesinde bilişim mahkemeleri kurulmasına ve bilişim sistemlerine ve sistemdeki verilere karşı suçların da içinde bulunduğu bilişim suçlarının bu mahkemelerde yargılanmasının kararlaştırılmasına rağmen, halen daha uygulamada hâkim ve savcılar bilişim sistemlerine özgü terimler konusunda yeteri bilgi ve birikime sahip değildir. Özellikle eğitim dönemlerinde hâkim ve savcılara zorunlu bilişim eğitimlerinin verilmesi bu suçlarla etkin mücadele bakımından hayatidir.

KAYNAKÇA

AÇIKGÖZ Emre İkbâl, Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4), Adalet Yay., Ankara 2020.

ADALET BAKANLIĞI, 2021 Adli İstatistik Raporu. İnternet Erişim: https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022140538 2021HİZMETEÖZELKİTAP.pdf (E.T. 20.08.2023)

AKARSLAN Hüseyin, Bilişim Suçları, Seçkin Yay., B. 2, Ankara 2015.

AKBULUT Berrin, Bilişim Alanında Suçlar, Adalet Yay., Ankara 2017.

AKBULUT Berrin, *"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"*, SÜHFD, C. 24, S. 2, 2016, ss. 7-55.

AKDEMİR Naci (Ed.) – **TUNCER** Can Ozan (Ed.), Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım, Pegem Akademi Yay., Ankara 2021.

AKTAŞ Duygu Şimşek, Bilişim Teknolojilerindeki Gelişmelerin Anayasal Fonksiyonlar Üzerindeki Dönüştürücü Etkisi, On İki Levha Yay., İstanbul 2020.

AKSOY İPEKÇİOĞLU Pervin, *"Türk Ceza Kanunu'nda Bileşik Suç",* AÜHFD, S. 61, C. 1, 2021, ss. 43-67.

AKSOY RETORNAZ Eylem, *"Ceza Hukuku Perspektifinden Blokzincir"*, Gelişen Teknolojiler ve Hukuk I - Blokzincir içinde (Ed. Eylem Aksoy Retornaz – Osman Gazi Güçlütürk), On İki Levha Yay., İstanbul 2020, ss. 377-408.

AMATO Astolfo di – **FUCITO**, Federico, Criminal Law in Italy, B. 4, Wolters Kluver Publishing, United Kingdom 2020.

APAYDIN Cengiz, Bilişim Suçları ve Bilişim Ceza Hukuku, Acar Matbaacılık, İstanbul 2017.

APAYDIN Cengiz, *"Yasak Cihaz veya Program Oluşturma, Bulundurma, Taşıma veya Satma Suçu"*, Terazi Hukuk Dergisi, C. 15, S. 163, 2020, ss. 563-571.

APAYDIN Cengiz, Bilişim Sistemine Girme, Engelleme ve Bozma Suçları, Seçin Yay., Ankara 2023.

ARTUK Mehmet Emin – **GÖKCEN** Ahmet – **YENİDÜNYA** Ahmet Caner, Türk Ceza Hukuku Özel Hükümler, B. 13, Adalet Yay., Ankara 2013.

BAŞ Eylem, Ceza Hukukunda Fail ve Mağdur, Seçkin Yay., Ankara 2021.

BAYRAKTAR Köksal – **EVİK** Vesile Sonay – **KANGAL** Zeynel Temel – **YILDIZ** Ali Kemal – **EVİK** Ali Hakan – **AKSOY RETORNAZ** Eylem – **MEMİŞ KARTAL** Pınar – **BOSTANCI BOZBAYINDIR** Gülşah – **EROĞLU** Fulya – **AYTEKİN İNCEOĞLU** Asuman, Ekonomi, Sanayi ve Ticarete İlişkin Suçlar – Bilişim Alanında Suçlar, On İki Levha Yay., İstanbul 2021.

BECCARIA Cesare, Suçlar ve Cezalar Hakkında (Çev. Sami Selçuk), B. 6, İmge Yay., Ankara 2016.

BOZDOĞAN AKBULUT Berrin, *"Bilişim Suçları"*, SÜHFD, C. 8, S. 1-2, 2000, ss. 545-555.

CANBEK Gürol – **SAĞIROĞLU** Şeref, *"Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma"*, Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, C. 22, S. 1, 2007, ss. 121-136.

CAPPELLINI Alberto, *"I Dellitti Contro L'integrità Dei Dati, Dei Programmi e Dei Sistemi Informatici"*, Cybercrime içinde (Ed. Alberto Cadoppi – Stefano Canestrari – Adelmo Manna – Michele Papa), B. 2, Wolters Kluver Italia, Italy 2023, ss. 809-875.

CLOUGH Paul – **MUNGO** Bryan, Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals, Random House, New York 2013.

CLOUGH Jonathan, *"A World Of Difference: The Budapest Convention On Cybercrıme And The Challenges Of Harmonisation"*, Monash University Law Review, Vol. 40, No. 3, ss. 698-736.

ÇAKIR Hüseyin (Ed.) – **KILIÇ** Mehmet Serkan (Ed.), Güncel Tehdit: Siber Suçlar, Seçkin Yay., Ankara 2014.

ÇAKIR Hüseyin (Ed.) – **KILIÇ** Mehmet Serkan (Ed.), Adli Bilişim ve Elektronik Deliller, Seçkin Yay., Ankara 2014.

DEĞER COŞKUNFIRAT Nesil, *"Asperger Syndrome: An Anesthetic Point of View: Review"*, Türkiye Klinikleri Anesteziyoloji Reanimasyon Dergisi, C. 12, S. 3, ss. 148-153.

DEĞİRMENCİ Olgun, *"2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi"*, TBB Dergisi, S. 58, 2005, ss. 195-208.

DEMİRCAN Tunç, Bilişim Alanında Suçlar, Legal Yay., İstanbul 2016.

DEMİRCİ Ömer, Bilişim Suçları ve Soruşturma Yöntemleri, Seçkin Yay., Ankara 2022.

DEMİRKIRAN Pınar, *"Hacktivzm"*, Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Bilimi içinde (Der. Ali Rıza Keleş), Alternatif Bilişim Yay., İstanbul 2023, ss. 27-33.

DOĞAN Koray, Neticesi Sebebiyle Ağırlaşmış Suçlar, Adalet Yay., Ankara 2011.

DÖNMEZER Sulhi – **ERMAN** Sahir, Nazarî ve Tatbikî Ceza Hukuku, C. 2, B. 15, Der Yay., İstanbul 2021.

DÜLGER Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, B. 10, Seçkin Yay., Ankara 2023.

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, C. 19, S. 62, ss. 101-131.

EMNİYET GENEL MÜDÜRLÜĞÜ, Kaçakçılık ve Organize Suçlarla Mücadele 2018 Raporu, Eflal Matbaacılık, Ankara 2019.

ERBSCHOLE Michael, Trojans, Worms, And Spyware: A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth-Heinemann, USA 2005.

ERDAĞ Ali İhsan, *"Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)"*, GÜHFD, C. 14, S. 2, 2010, ss. 275-303.

ERDOĞAN Yavuz, Türk Ceza Kanunu'nda Bilişim Suçları, B. 1, Legal Yay., İstanbul 2012.

ERDOĞAN Yavuz, *"Bilişim Sistemine Girme ve Kalma Suçu",* Dokuz Eylül Hukuk Fakültesi Dergisi, C. 12, Özel Sayı, 2010, ss. 1363-1433.

ERGÜN İsmail, Siber Suçların Cezalandırılması ve Türkiye'de Durum, B. 1, Adalet Yay., Ankara 2008.

ERMEYDAN Damla, Türk Ceza Hukukunda Bilişim Suçları, B. 2, Seçkin Yay., Ankara 2023.

FİDAN Serdal – **ULUDAĞ** Buket Cansu, *"Rutin Aktiviteler Teorisi Bağlamında Dijitalleşen Dünyada Siber Suç Mağdurları"*, HABITUS Toplumbilim Dergisi, S. 4, 2023, ss. 175-210.

GEÇMEZ İrem, Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (TCK m. 244), Seçkin Yay., Ankara 2020.

GERÇEKER Hasan, Yorumlu & Uygulamalı Türk Ceza Kanunu (2 Cilt), B. 6, Seçkin Yay., Ankara 2022.

GERKCE Marko, *"Siber Suç Sözleşmesi ile 10 Yıl: Avrupa Konseyi'nin İnternet Bağlantılı Suçlara Karşı Mücadele Belgesinin Başarıları ve Kusurları"* (Çev. Kerem Öz), Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), Seçkin Yay., Ankara 2013, ss. 103-120.

GIBONEY Justin Scott – **SCHUETZLER** Ryan M. – **GRIMES** G. Mark, *"Know your enemy: Conversational agents for security, education, training, and awareness at scale"*, Computer&Security Journal, Vol. 129, No. 2, 2023. İnternet Erişim: https://doi.org/10.1016/j.cose.2023.103207 (E.T. 27.09.2023)

GÜL Ahmet, Doğrudan – Dolaylı Bilişim Suçları, B. 3, Seçkin Yay., Ankara 2021.

HAFIZOĞULLARI Zeki – **GÜNGÖR** Devrim, *"Türk Ceza Hukukunda Suçların Tasnifi"*, TBB Dergisi, S. 69, 2007, ss. 21-50.

HAFIZOĞULLARI Zeki – **ÖZEN** Muharrem, Türk Ceza Hukuku Genel Hükümler, B. 13, US-A Yay., Ankara 2021.

HAFIZOĞULLARI Zeki – **ÖZEN** Muharrem, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, B. 4, US-A Yayıncılık, Ankara 2022.

HEKİM Hakan, *"Oltalama (Phishing) Saldırıları"*, Siber Suçlar: Tehditler, Farkındalık ve Mücadele içinde (Ed. Fatih Tombul – Murat Güneştaş – Oğuzhan Başıbüyük), Global Politika ve Strateji Yay., Ankara 2015, ss. 57-83.

HILL Josua B. – **MARION** Nancy E., Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century, Praeger, USA 2016.

HOLT Thomas J. – **BOSSLER** Adam M., Cybercrime in Progress: Theory and prevention of technology-enabled offenses, Routledge, New York 2016.

JORDAN Tim – **TAYLOR** Paul, *"A sociology of hackers",* Sociological Review, C. 46, S. 4, 1998, ss. 757-780.

İÇEL Kayıhan *"Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri"*, İÜHFM, C. 59, S. 1, 2001, ss. 3-10.

İHTİYAROĞLU Uğur, *"Bilişim Sistemine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi"*, HÜHFD, C. 10, S. 2, 2020, ss. 406-440.

İKİNCİ Özlem, *"30 Tonluk Hayal Artık Cepte: Bilgisayar"*, TÜBİTAK Bilim ve Teknik Dergisi, S. 508, 2010, ss. 20-29.

KABADAYI Sami, *"Bilişim Sistemine Girme Suçu (TCK m. 243)"*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2021.

KARAKEHYA Hakan, *"Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu",* TBB Dergisi, S. 81, 2009, ss. 1-24.

KARAKURT EREN Ahu, *"Bilişim Alanında Suçların veya Bilişim Sistemlerinin Araç Olarak Kullanıldığı Diğer Suçların İşlenmesi Amacıyla Cihaz, Program, Şifre Ya Da Güvenlik Kodlarının Üretilmesi, Yayılması veya Bulundurulması Suçu",* TAAD, S. 43, Y. 11, 2020, ss. 219-261.

KARAGÖZ Mehmet Can, Bilişim Sistemleri Teorisine Giriş ile Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu, On İki Levha Yay., İstanbul 2020.

KARAGÜLMEZ Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, B. 5, Seçkin Yay., Ankara 2014.

KAYA İslam Safa – **ÇAKIR** Adem, *"Yasak Cihaz veya Programlar Suçu"*, C. 19, S. 38, 2020, ss. 32-55.

KAYAER Nebahat, *"Türk Hukukunda Bilişim Sistemine Girme Suçu (TCK m. 243)"*, CHD, C. 14, S. 39, ss. 83-128.

KETİZMEN Muammer, Türk Ceza Hukukunda Bilişim Suçları, Adalet Yay., Ankara 2008.

KIRWAN Gráinne – **POWER** Andrew, Cybercrime: The Psycologhy of Online Offenders, Cambridge University Press, Cambridge 2013.

KİŞİSEL VERİLERİ KORUMA KURUMU, 6698 Sayılı Kanun'da Yer Alan Temel Kavramlar Kitapçığı. İnternet Erişim: https://www.kvkk.gov.tr/Icerik/4187/6698-Sayili-Kanun'da-Yer-Alan-Temel-Kavramlar (E.T. 14.04.2023)

KOCA Mahmut, *"Hukukumuzda TCK'nun 244.Maddesi Kapsamında Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu"*, (9-10 Ekim 2008) Bilişim Hukuku Konferansı içinde, Yargıtay Başkanlığı Yayını, Ankara 2008, ss. 89-99.

KOCA Mahmut – **ÜZÜLMEZ** İlhan, Türk Ceza Hukuku Genel Hükümler, B. 15, Seçkin Yay., Ankara 2022.

KOCA Mahmut – **ÜZÜLMEZ** İlhan, Türk Ceza Hukuku Özel Hükümler, B. 7, Adalet Yay., Ankara 2020.

KRANENBARG Marleen Weulen, *"Cyber-Dependent Crime Versus Traditional Crime: Empirical Evidence for Clusters of Offenses and Related Motives"*, Cybercrime in context the human factor in victimization, offending, and policing içinde (Ed. Marleen Weulen Kranenbarg - Rutger Leukfeldt), Springer Nature, Switzerland 2021, ss. 195-215.

KURT Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yay., Ankara 2005.

MAHMUTOĞLU Fatih Selami, *"Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu"*, İÜHFM, C. 59, S. 1-2, 2001, ss. 39-49.

MAHMUTOĞLU Fatih Selami, *"Türk Ceza Kanunu'nda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi"*, İÜHFM, C. LXXI, S. 1, 2013, ss. 855-889.

MALKOÇ İsmail, Açıklamalı Türk Ceza Kanunu, C. 4, Sözkesen Matbaacılık, Ankara 2013.

MARION Nancy E. – **TWEDE** Johnson, Cybercrime: An Encyclopedia of Digital Crime, ABC-CLIO, California 2020.

MUCUK Melike Hafsa, *"Bilişim sistemine girme (TCK 243) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK 244) suçları"*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2022.

NATIONAL CYBER CRIME UNIT, Pathways Into Cyber Crime Report, 2017. İnternet Erişim: https://nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file (E.T. 20.08.2023)

OKUYUCU ERGÜN Güneş, Banka veya Kredi Kartlarının Kötüye Kullanılması, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 19, S. 2, 2013, ss. 1065-1086.

OORSCHOT Paul C. Van, Siber Güvenliğe Giriş: Bilgisayar Güvenliği ve İnternet (Çev. Kemal Bıçakçı), Palme Yay., Ankara 2022.

ORUNSOLU A. A. – **SODIYA** A. S. – **AKINWALE** A. T., *"A predictive model for phishing detection",* Journal of King Saud University – Computer and Information Sciences, Vol. 34, 2022, ss. 232-247.

ORTA Mesut, Bilişim Suçları ve Elektronik Delillerin Toplanması, Muhafazası, Değerlendirilmesi, Sunulması (Adli Bilişim), Yetkin Yay., Ankara 2015.

ÖNDİN Hasan Burak, *"Türk Hukukunda Doğrudan Bilişim Suçları"*, Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir 2017.

ÖNDİN Hasan Burak, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, Terazi Hukuk Dergisi, C. 15, S. 162, 2020, ss. 320-337.

ÖNOK Murat, *"Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği"*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, C. 19, S. 2, 2013, ss. 1229-1270.

ÖZBEK Veli Özer – **DOĞAN** Koray – **BACAKSIZ** Pınar, Türk Ceza Hukuku Özel Hükümler, B. 17, Seçkin Yay., Ankara 2022.

ÖZEN Muharrem – **BAŞTÜRK** İhsan, Temel Hak ve Özgürlükler Bağlamında Bilişim - İnternet ve Ceza Hukuku, Adalet Yay., Ankara 2021.

ÖZEN Mustafa, *"5237 Sayılı Türk Ceza Kanunu'nun İştirak Kurumuna Bakışı"*, TBB Dergisi, S. 70, 2007, ss. 239-253.

ÖZGENÇ İzzet, Türk Ceza Hukuku Genel Hükümler, B. 19, Seçkin Yay., Ankara 2023.

ÖZKUL Davut, *"Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi"*, Sayıştay Dergisi, Ocak-Şubat 2002, C. 13, S. 44-45, ss. 11-34.

ÖZOCAK Gürkan, *"DDoS Saldırısı ve Failin Cezai Sorumluluğu",* Ankara 29. Ulusal Bilişim Kurultayı Bildiriler Kitabı içinde, Ankara 2012, ss. 23–29.

ÖZÇELİK İlker – **BROOKS** Richard, Distributed Denial of Service Attacks: Real-world Detection and Mitigation, CRC Press, 2020.

ÖZSOY Nevzat, *"Yargıtay Kararları Işığında Doğrudan Bilişim Suçları (TCK. 243 ve 244)"*, Yaşar Hukuk Dergisi, C. 1, S. 2, 2019, ss. 295-352.

ÖZTEKİN Alp, Bilişim Sistemine Girme Suçu (TCK m. 243), Seçkin Yay., Ankara 2023.

PARLAR Ali **– ÖZTÜRK** Mustafa, Doğrudan ve Dolaylı Bilişim Suçları, Aristo Yay., İstanbul 2020.

PICOTTI Lorenzo, *"Sistemica dei reati informatici, technice di formulazione legislativa e beni giurdici tutelati"*, Il Diritto Penale Dell'Informatica Nell'epoca di Internet içinde (Ed. Lorenzo Picotti), CEDAM, Padova 2004, ss. 22-94.

PICOTTI Lorenzo, *"Diritto Penale, technologie informatiche ed intelligenza artificiale: una visione d'insieme"*, Cybercrime içinde (Ed. Alberto Cadoppi – Stefano Canestrari –Adelmo Manna – Michele Papa), B. 2, Wolters Kluver Italia, Italy 2023, ss. 32-98.

POLYZOIDOU Vagia, *"Combatting the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime",* EU Internet Law in the Digital Single Market içinde (Ed. Tatiana Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou Merdi), Springer Nature, Switzerland 2021, ss. 355- 375.

SARITAŞ Erkan, *"Cezalandırılmayan Önceki Hareketler"*, İÜHFM, S. 80, C. 2, 2022, ss. 615-654.

SCHJØLBERG Stein, *"The History of Global Harmonization on Cybercrime Legislation - The Road to Geneva",* 2008.

https://www.cybercrimelaw.net/documents/cybercrime_history.pdf (E.T. 3.1.2024)

SCHJØLBERG Stein – **HUBBARD** Amanda M., *"Harmonizing National Legal Approaches on Cybercrime",* WSIS Thematic Meeting on Cybersecurity, International Telocommunication Union, 2005. İnternet Erişim: https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf (E.T. 5.1.2024)

SELZER Nicole – **OELRICH** Sebastian, *"Saint or Satan? Moral Development and Dark Triad Infuences on Cybercriminal Intent"*, Cybercrime in context the human factor in victimization, offending, and policing içinde (Ed. Marleen Weulen Kranenbarg - Rutger Leukfeldt), Springer Nature, Switzerland 2021, ss. 175-194.

SEMİZ Murat, Bilişim Suçları ve Soruşturma Yöntemleri, B. 3, Adalet Yay., Ankara 2022.

SIEBER Ulrich, *"Bilgisayar Suçluluğu" (Çev. Yener Ünver),* Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), Seçkin Yay., Ankara 2013, ss. 13-59.

SIEBER Ulrich, *"Bilişim Suçları"* (Çev. Feridun Yenisey ve Damla Zaimoğlu), Bilişim Teknolojisi ile Globalleşen Dünyadaki Tehlikelerin Önlenmesi ve Ceza Hukuku içinde (Ed. Feridun Yenisey, Salih Oktar, Zehra Başer Doğan), Seçkin Yay., Ankara 2021, ss. 259-302.

TANER Fahri Gökçen, Ceza Hukukunda Zamanaşımı, Seçkin Yay., Ankara 2008.

TAŞKIN Şaban Cankat, *"Ceza Hukukunda Cezalandırılabilirliğin Ön Alana Kaydırılması ve Hazırlık Hareketlerinin Cezalandırılması Sorununun Yasak Cihaz veya Programlar Suçu Özelinde İngiliz Ceza Hukuku, Kanada Ceza Hukuku ve Avrupa Konseyi Siber Suç Sözleşmesindeki Düzenlemelerle"*, Ceza Hukuku Dergisi, C. 19, S. 55, 2024, ss. 251-270.

TAŞKIN Şaban Cankat, Bilişim Suçları, Beta Yay., Bursa 2008.

TAYLOR Paul A., Hackers: Crime in the Digital Sublime, Routledge, London 1999.

TEPE İlker, *"Yeni Bir Temel Hak Olarak 'Bilişim Teknolojisi Sistemlerinin Gizliliği ve Bütünlüğünün Korunması Hakkı' – Alman Federal Mahkemesi'nin 'Online Arama' Kararının Sistematik Analizi"*, Karşılaştırmalı Güncel Ceza Hukuku Serisi [13] – İnternet Hukuku içinde (Ed. Yener Ünver), Seçkin Yay., Ankara 2013, ss. 387-415.

TEZCAN Durmuş – **ERDEM** Mustafa Ruhan – **ÖNOK** Rıfat Murat, Teorik ve Pratik Ceza Özel Hukuku, B. 20, Seçkin Yay., 2022.

TIEDEMANN Klaus, *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünden İncelenmesi"* (Çev. Feridun Yenisey), İÜHFM, C. 41, S. 1-2, 1975, ss. 319-332.

TOROSLU Nevzat – **TOROSLU** Haluk, Ceza Hukuku Genel Hükümler, B. 26, Savaş Yay., Ankara 2021.

TURAN Metin, Bilişim Hukuku, B. 7, Seçkin Yay., Ankara 2023.

ÜNAL Osman Gazi, *"Cezalandırılabilirliğin Ön Alana Kaydırılması Bağlamında, Yasak Cihaz veya Programlar Suçu (TCK M. 245/A)"*, AHBVÜD, C. 26, S. 2, 2022, ss. 589-646.

ÜNVER Yener, *"Türk Ceza Kanunu'nun ve Ceza Kanunu Tasarısının İnternet Açısından Değerlendirilmesi"*, İÜHFM İnternet Özel Bölümü, C. LIX, S. 1-2, 2001, ss. 51-153.

VIANO Emilio C., *"Cybercrime: Definition, Typology, and Criminalization",* Cybercrime, Organized Crime, and Societal Responses içinde (Ed. Emilio C. Viano), Springer Nature, Switzerland 2017, ss. 3-22.

VINCENT Nicole A., *"Victims of cybercrime: Definitions and challenges"*, Cybercrime and It's Victims içinde (Ed. Elena Martellozo – Emma A. Jane), B. 1, Routledge, New York 2017, ss. 27-42.

WILHELM Thomas, Professional Penatration Testing, B. 2, Elsevier Nature, USA 2013.

YALÇIN Türkân – **KÖPRÜLÜ** Timuçin, Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları, B. 9, Savaş Yay., Ankara 2022.

YANAR Yasin, *"Ceza Hukuku ve Bilişim Hukuku Bağlamında TCK Md. 245/A Yasak Cihaz veya Programlar Suçu",* Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Lisansüstü Programlar Enstitüsü, İstanbul 2019.

YAŞAR Osman – **GÖKCAN** Hasan Tahsin – **ARTUÇ** Mustafa, Yorumlu – Uygulamalı Türk Ceza Kanunu, C. 5, B. 2, Adalet Yay., Ankara 2014.

YAZICIOĞLU Yılmaz, Kriminolojik, Sosyolojik ve Hukuki Boyutları ile Bilgisayar Suçları, Alfa Yay., İstanbul 1997.

YAZICIOĞLU Yılmaz, *"Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı",* Uluslararası İnternet Hukuku Sempozyumu (21-22 Mayıs 2001) içinde, Dokuz Eylül Üniversitesi Yayını, İzmir 2002, ss. 451-470.

YAZICIOĞLU Yılmaz, *"Hukukumuzda TCK 243.Madde Kapsamında Bilişim Sistemine Girme Eylemi"*, Bilişim Hukuku Konferansı (9-10 Ekim 2008) içinde, Yargıtay Başkanlığı Yay., Ankara 2008, ss. 69-87.

YELDAN Didem, Siber Suçlar, Seçkin Yay., Ankara 2022.

YENİDÜNYA Caner – **DEĞİRMENCİ** Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yay., İstanbul 2003.

YETİM Servet, *"Bilişim Suçları ve Etkin Mücadele Yöntemleri"*, Terazi Hukuk Dergisi, C. 9, S. 95, 2014, ss. 80-86.

YILMAZ Sacit, *"5237 Sayılı Tck'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar"*, TBB Dergisi, 2011, S. 92., ss. 62-100.

YILMAZ Sacit, Türk Ceza Hukuku Sisteminde Siber Suçlar, B. 2, Adalet Yay., Ankara 2023.

ÖZET

Dört bölüm altında ele alınan çalışmanın konusunu 5237 sayılı TCK'da düzenlenen bilişim sistemine ve bilişim sistemindeki verilere karşı suçlar oluşturmaktadır. Birinci bölümde, konu genel kapsamda incelenmiştir. Bu çerçevede konuyla ilgili kavramlar, bilişim sistemlerine ve sistemdeki verilere karşı suçların işlenme şekilleri ve bu suçların genel özellikleri, bu suçların fail ve mağdurlarına ilişkin açıklamalar yapılmıştır.

Tezin ikinci bölümünde bilişim sistemine girme veya sistemde kalma, sisteme girmeksizin veri nakillerini teknik araçlarla izleme suçları (TCK m. 243), üçüncü bölümünde bilişim sistemini engelleme veya bozma; verileri yok etme veya değiştirme suçları (TCK m. 244), son bölümde ise yasak cihaz veya programlar suçu (TCK m. 245/A) unsurlarıyla birlikte incelenmiştir.

Anahtar kelimeler: Bilişim, veri, bilişim sistemi, bilişim suçları, AKSSS, bilişim alanında suçlar, veri nakli, oltalama, sistemi engelleme, DDoS atağı.

ABSTRACT

The subject of the study, which is handled under four chapters, is the crimes against the information system and the data in the information system regulated in the Turkish Penal Code No. 5237. In the first part, the subject is examined in general. In this framework, the concepts related to the subject, the ways of committing crimes against information systems and data in the system, the general characteristics of these crimes, and the perpetrators and victims of these crimes are explained.

In the second part of the thesis, the crimes of accessing a data processing system, monitoring data transmissions through technical means without entering the system (Article 243 of the Turkish Penal Code); in the third part, the crimes of preventing the functioning of a system and deletion, alteration or corrupting of data (Article 244 of the Turkish Penal Code); and in the last part, the crime of prohibited devices or programs (Article 245/A of the Turkish Penal Code) are examined together with their elements.

Key words: IT, data, information system, cyber crimes, Council of Europe Convention on Cybercrime, crimes in the field of IT, data transfer, phishing, system blocking, DDoS attack.