T.C.
HASAN KALYONCU ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU TEZLİ YÜKSEK LİSANS PROGRAMI

BİLİŞİM SİSTEMİNE GİRME, SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

YÜKSEK LİSANS TEZİ

HAZIRLAYAN
SANİYE TUBA TOPYILDIZ SUBAŞI

GAZİANTEP - 2022

T.C.
HASAN KALYONCU ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI
KAMU HUKUKU TEZLİ YÜKSEK LİSANS PROGRAMI

BİLİŞİM SİSTEMİNE GİRME, SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

YÜKSEK LİSANS TEZİ

HAZIRLAYAN
SANİYE TUBA TOPYILDIZ SUBAŞI

TEZ DANIŞMANI
DR. ÖĞR. ÜYESİ ALİ TANJU SARIGÜL

GAZİANTEP - 2022

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÜKSEK LİSANS KABUL VE ONAY FORMU

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Kamu Hukuku Anabilim Dalı **Kamu Hukuku** Tezli Yüksek Lisans Programı öğrencisi **Saniye Tuba Subaşı** tarafından hazırlanan **"**Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları**"** başlıklı tez, 26/10/2022 tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Görevi	**Unvanı, Adı ve Soyadı** **Kurumu/Üniversitesi**	**İmzası:**
Tez Danışmanı	Dr. Öğr. Üyesi Ali Tanju Sarıgül Hasan Kalyoncu Üniversitesi	
Jüri Başkanı	Doç. Dr. Ahmet Bozdağ Gaziantep Üniversitesi	
Jüri Üyesi	Dr. Öğr. Üyesi Hakan Gündüz Hasan Kalyoncu Üniversitesi	

Bu tez Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

Enstitü Müdürü

Prof. Dr. Mahmut Serhat Yenice

TEZ ETİK VE BİLDİRİM SAYFASI

Yüksek Lisans Tezi olarak sunduğum “Bilişim Sistemine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları” başlıklı çalışmanın tarafımca, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bunlara atıf yapılarak yararlanmış olduğumu belirtir ve onurumla doğrularım. 26/10/2022

Saniye Tuba TOPYILDIZ SUBAŞI

ÖNSÖZ

Bu tez çalışmasının hazırlanması sürecinde tecrübelerini, desteğini, görüşlerini ve değerli zamanını esirgemeyen çok kıymetli tez danışmanım Dr. Öğr. Üyesi ALİ TANJU SARIGÜL'e;

Çalışmalarım sırasında yardım ve desteklerini esirgemeyen değerli eşim Av. Murat SUBAŞI'na;

Hayatımın her anında desteklerini ve güvenlerini hissettiğim ve çalışmam boyunca manevi destekleriyle yanımda olan annem Lütfiye TOPYILDIZ, babam Hüseyin TOPYILDIZ ve kardeşlerime;

Sonsuz teşekkürler.

ÖZET

Günümüzde bilgi teknolojilerinin büyük bir hızla yaygınlaşmasının bilişim suçlarını artırdığı söylenebilir. Teknolojinin evrimi, akıllı teknolojinin erişilebilirliği artırması ve klasik suç tiplerine göre daha kolay daha hızlı suç işlenebilmesi bilişim suçlarının sayısını ve suç çeşitlerini artırmıştır. Bilişim suçlarıyla etkin bir mücadele için çağımızın gelişimlerine uyum sağlayabilecek daha kapsamlı maddi ceza hukuku normlarının düzenlenmesi gerekmektedir.

Bilişim sistemine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları başlıklı tez çalışmamız üç ana bölümden oluşmaktadır. Birinci bölümde bilişim suçlarının daha doğru anlaşılması amacıyla teknik kavramlar açıklanmış ve bilişim suçları işlenirken kullanılan yöntemler hakkında bilgi verilmiştir. İkinci bölümde uluslararası örgütlerin bilişim suçlarıyla mücadele kapsamında aldıkları önlemler ile bazı ülkelerin bilişim suçlarına ilişkin iç hukuk düzenlemeleri incelenmiştir. Son bölümde ise çalışma konumuzu oluşturan suç eylemleri Türk Ceza Kanunu'ndaki düzenlemeler kapsamında suçun unsurları da dikkate alınarak detaylı olarak açıklanmıştır.

Anahtar Kelimeler: Bilişim, İnternet, Bilişim Suçları, Türk Ceza Hukuku.

ABSTRACT

Nowadays, it can be said that the rapid spread of information technologies has increased cyber crimes. The evolution of technology, the increase in accessibility of smart technology and the ability to commit crimes more easily and faster than classical crime types have increased the number of cyber crime and the types of crimes. For an effective fight against cyber crimes, more comprehensive substantive criminal law norms that can adapt to the developments of our century should be regulated.

Our thesis consists of three main parts: Crimes of entering the information system, blocking the system, corrupting, destroying or changing the data. In the first part, technical terms and concepts are explained in order to understand informatics crimes more accurately and information about the methods used in committing cyber crimes is given. In the second part, the measures taken by international organizations within the scope of combating cyber crimes and the domestic legal regulations of some countries regarding cyber crimes are examined. In the last part, the criminal acts, which constitute our study subject, are explained in detail, taking into account the elements of the crime within the scope of the regulations in the Turkish Penal Code.

Keywords: Informatics, Internet, Cyber Crimes, Turkish Criminal Law.

İÇİNDEKİLER

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR

ABD	:	Amerika Birleşik Devletleri
AKSS	:	Avrupa Konseyi Siber Suç Sözleşmesi
ARPA	:	Advanced Research Projects Agency – Gelişmiş Savunma Araştırmaları Projeleri Birimi
ARPANET	:	The Advanced Research Projects Agency Network – Gelişmiş Araştırma Projeleri Dairesi Ağı
ATM	:	Automatic Teller Machine – Otomatik Vezne Makinesi
bkz.	:	bakınız
BM	:	Birleşmiş Milletler
C.	:	Cilt
CCI	:	Commonwealth Cybercrime Initiative – İngiliz Milletler Topluluğu Bilişim Suçları Girişimi
CCP	:	Cybercrime Collaboration Services – Siber Suç İşbirliği Hizmetleri
CD	:	Compact Disc – Yoğun Disk
CFAA	:	Computer Fraud and Abuse Act - Bilgisayar Sahtekârlığı ve Kötüye Kullanılması Yasası
DDoS	:	Distributed Denial of Services – Dağıtık Hizmet Reddi
DOS	:	Disk Operating System – Disk İşletim Sistemi
ENIAC	:	Electronic Numerical Integrator And Computer Elektronik Sayısal Entegreli Hesaplayıcı
FCK	:	Fransız Ceza Kanunu
FCKT	:	Fransız Ceza Kanunu Tasarısı
G7	:	Group of Seven – Yediler Grubu
G8	:	Group of Eight – Sekizler Grubu
HSK	:	Hakimler Savcılar Kurulu
INTERPOL	:	International Criminal Police Organization – Uluslararası Kriminal Polis Teşkilatı
IP	:	İnternet Protocol – İnternet Protokolü
KİT	:	Kamu İktisadi Teşebbüsleri
KYOK	:	Kovuşturmaya Yer Olmadığına Dair Karar

LCD	:	Liquid Crystal Display – Sıvı Kristal Ekran
LED	:	Light Emitting Diode – Işık Yayan Diyot
m.	:	Madde
OAS	:	Organization of American Stares – Amerikan Devletleri Örgütü
ODTÜ	:	Ortadoğu Teknik Üniversitesi
OECD	:	Organisation for Economic Co-operation and Development – Ekonomik Kalkınma ve İşbirliği Örgütü
RAM	:	Random Access Memory – Rastgele Erişim Belleği
ROM	:	Read Only Memory – Salt Okunur Bellek
s.	:	sayfa
S.	:	Sayı
SBE	:	Sosyal Bilimler Enstitüsü
Spam	:	Spiced Pork And Ham
TBBD	:	Türkiye Barolar Birliği Dergisi
TBBM	:	Türkiye Büyük Millet Meclisi
TCK	:	Türk Ceza Kanunu
TCKÖ	:	Türk Ceza Kanunu Ön Tasarısı
TCP	:	Transmission Control Protocol – İletişim Kontrol Protokolü
TDK	:	Türk Dil Kurumu
TÜBİTAK	:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UNODC	:	United Nations Office on Drugs and Crime – Birleşmiş Milletler Uyuşturucu ve Suç Ofisi
USB	:	Universal Serial Bus – Evrensel Seri Yolu
Y.	:	Yıl
yy.	:	Yüzyıl

GİRİŞ

Bilgi teknolojileri dünyada önlenemeyen bir salgın gibi büyümekte her saniye şaşırtıcı gelişmeler göstermektedir. Teknoloji çağı veya dijital çağ olarak da adlandırılan bu dönemde teknolojik atılımlar toplumda iletişim, ulaşım, sağlık, eğlence gibi birçok alanda fayda sağladığı gibi kötü niyetli kişiler tarafından kullanıldığında hukuki problemleri de beraberinde getirmektedir. Günümüzde hayatın ayrılmaz bir parçası haline gelen bilişim teknolojileri bir süre sonra kötüye kullanılarak bilişim suçlarını da doğurmuştur. Geleneksel suçların da adeta gelişen teknolojiye uyum sağlayarak yerlerini bilişim suçlarına bırakmaya başladıkları görülmektedir.

Bilişim suçlarının faillerinin klasik suç tiplerindeki faillerden farklı olarak teknik donanıma sahip kişiler oldukları söylenebilir. Kendine özgü yöntemlerle işlenen bu suçların en yaygın görülen işlenme şekilleri; truva atları, bukalemunlar, tavşanlar, salam tekniği, istem dışı alınan elektronik postalar (e-posta), mantık bombaları, ağ solucanları, sistem güvenliğinin kırılıp içeri girilmesi (hacking), bilgisayar virüsleri ve phishing saldırılarıdır.

Bilişim alanında işlenen suçların küresel nitelikte ve fiziki hareket gerektirmeyen suçlar oldukları söylenebilir. Suç işleyen kişinin bilgisayara sahip olması ve bir ağa bağlanması bulunduğu yerden ayrılmadan dünyanın başka bir yerinde yalnızca bir tuşa basarak bilişim suçu işlemesi için yeterli olacaktır. Bu durum bilişim suçlarını zamansız ve mekânsız suçlar haline getirmektedir. Bilişim suçlarının yarattığı tehlikelerin ciddi boyutlara ulaşması, uluslararası kuruluşları endişelendirmeye başlamıştır. Özellikle de küresel ekonomiye oldukça büyük zararlar verilmesi, bu kuruluşların bilişim alanında suçlarla mücadelede uygulama birliği sağlayacak uluslararası bir düzenleme ihtiyaçlarını doğurmuştur. Bilişim suç ve suç tehditleriyle mücadelede en etkili yol uluslararası iş birliğinin sağlanması olacaktır. Bu kapsamda Birleşmiş Milletler, G8(Sekizler Grubu), İngiliz Milletler Topluluğu, İnterpol, Ekonomik İşbirliği ve Kalkınma Örgütü (OECD), Avrupa Konseyi gibi çeşitli kuruluşların çalışmaları olduğu ve bilişim suçlarıyla mücadelede etkili olabilecek düzenlemeler yaptıkları görülmektedir. Bu düzenlemelerden en önemlisinin 2001 yılında Avrupa Konseyi tarafından hazırlanan Avrupa Konseyi Siber Suç Sözleşmesi (AKSS) olduğu söylenebilir. Bu sözleşmeyle ülkelerin, bilişim suçlarıyla mücadelede iç hukuklarında sözleşmeyle uyumlu maddi ceza hukuku hükümlerine yer vermeleri sağlanarak uluslararası iş birliğinin pekiştirilmesi amaçlanmıştır. Günümüzde bilişim suçlarına dair en kapsamlı düzenlemeleri içeren ve en fazla ülke tarafından kabul gören uluslararası düzenlemenin AKSS olduğu görülmektedir.

Dünya genelinde bilişim suçlarının yarattığı ciddi tehditlerle başa çıkmaya çalışan ülkelerin, kendi iç hukuklarında da suç işlemeyi caydırıcı etkili önlemler alarak düzenlemeler yapma çabasında oldukları görülür. Anglo-Sakson hukuk sistemini benimseyen İngiltere, Amerika gibi ülkelerin bilişim suçlarını ceza kanunlarından bağımsız, ayrı bir kanun olarak düzenledikleri görülmektedir. Türk hukuk mevzuatında bilişim suçları Almanya'da olduğu gibi ayrı bir kanunla düzenlenmemiş mevcut ceza kanunları içerisinde bilişim suçlarına yer verilmiştir.

Mevzuatımızda bilişim alanında suçlar 5237 sayılı Türk Ceza Kanunu'nun onuncu bölümünde yer almaktadır. Çalışma konumuzu oluşturan bilişim sistemlerine girme, kalma, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçları da bilişim alanında suçlar başlıklı bu bölümde 243. ve 244. maddelerde düzenlenmiştir.

Tez çalışmamız üç ana bölümden oluşmaktadır. Birinci bölümde bilişim alanında işlenen suçları kavrayabilmek adına bilişim sistemi ve suçlarına ilişkin bilişim, bilgisayar, bilişim sistemi, internet gibi temel terimlerle, bilişim suçlarının yaygın işleniş yöntemleri ele alınmıştır. İkinci bölümde uluslararası örgütlerin bilişim suçlarına yaklaşımı, bu suçlarla mücadelede kullandıkları yöntemler, uluslararası sözleşmelerle korunmaya çalışılan bilişim güvenliğine dair incelemelerde bulunulmuştur. Ayrıca mukayeseli hukukta diğer ülkelerin bilişim alanında yaptıkları çalışmalara da yer verilmiştir. Son olarak üçüncü bölümde 5237 sayılı Kanun'da düzenlenen bilişim sistemlerine girme, sistemi engelleme, verileri bozma, yok etme veya değiştirme suçları unsurları da dikkate alınarak incelenmeye çalışılmıştır.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİ VE BİLİŞİM SUÇLARIYLA İLGİLİ TEMEL KAVRAMLAR

1.1. Temel Kavramlar

1.1.1. Bilişim ve Bilişim Sistemi Kavramı

Teknolojinin gelişmesiyle birlikte bilgisayarların toplum hayatında yaygınlaşarak önemli bir yer edinmesi dilimize yeni kavramların girmesine yol açmıştır. Bilişim kavramı da bunlardan biri olarak karşımıza çıkmaktadır.

Bilişim kavramı henüz dilimizde yokken yerine, Fransızca'da kullanılan "informatique" kelimesinin Türkçe tercümesi olan "enformasyon" kavramının kullanıldığı bilinmektedir.[1] Dilimizde ilk defa 1970 yılında kullanılan bilişim sözcüğü Prof. Dr. Aydın Köksal'ın bilmek eyleminin kökeninden türettiği bir kavramdır.[2]

Bilişim kavramı Türk Dil Kurumu sözlüğünde; *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi, enformatik."* olarak açıklanmıştır.[3]

Doktrinde birçok yazarın bilişim kavramı için farklı tanımlamalar yaptıkları görülmektedir.

Akbulut, ilk zamanlarda bilginin muhafazası ve erişim kolaylığı amacıyla kullanılan bilişim kavramının daha sonra bilginin yönetimi ve işlenmesi için kullanılan bir alan olduğunu günümüzde ise yaygın kullanılan bilgisayar ve bilgisayarlara bağlı sistemler aracılığıyla bilginin işlenmesi kavramını karşıladığını ifade etmektedir.[4]

Artuk/Gökcen/Yenidünya bilişimi özünde verilerin saklanması elektronik ortamda işlenerek veri iletişim araçlarıyla aktarılması olarak açıklamıştır.[5]

---

[1] Değirmenci, Olgun, "Bilişim Suçları", (Marmara Üniversitesi Sosyal Bilimler Enstitüsü Hukuk Anabilim Dalı Kamu Hukuku Bilim Dalı Yayımlanmamış Yüksek Lisans Tezi), İstanbul, 2002, s. 10.

[2] Erdoğan, Yavuz, Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle), İstanbul, Legal Yayıncılık, 2012, s. 49.

[3] https://sozluk.gov.tr/ (Erişim Tarihi: 16.10.2021).

[4] Akbulut, Berrin, Bilişim Alanında Suçlar, Ankara, Adalet Yayınevi, Kasım 2017, s. 13.

[5] *"Bilişim, insanların, teknik, ekonomik, sosyal, kültürel, hukuksal veya benzeri alanlarda sahip oldukları verinin saklanması, saklanan bu verinin elektronik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılmasıdır."* Artuk, Mehmet Emin/Gökcen, Ahmet/Yenidünya, Ahmet Caner, Ceza Hukuku Özel Hükümler, Ankara, Adalet Yayınevi, 2014, s. 753.

Bilişimi bir bilim dalı olarak ifade eden Değirmenci'ye göre, verilerin otomatik olarak, işlenmesi, saklanması, düzenlenmesi, değerlendirilmesi ve aktarılmasıdır.[6]

Yazıcıoğlu'nun bilişimi tanımlarken bilginin özellikle bilgisayarlardan yararlanılarak işlenmesi, saklanması ve iletilmesini vurguladığı görülmektedir.[7]

Erdoğan bilişimin sürekli güncellenen teknik bir bilim dalı olduğunu tanımlamada eksik bırakılan bir hususun bilişim suçlarında kanunilik ilkesine zarar vereceğini belirterek bilişim tanımı yapmaktan kaçınmış ancak kavramın temelini oluşturan verilerin işlenmesi, saklanması ve aktarılması olmak üzere üç unsurunun bulunduğunu ifade etmiştir.[8]

Kurt'un tanımında verilerin işlenme, saklanma aktarılma süreçlerinin bilişim temelli ve otomatik olduğu vurgusunun yapıldığı görülmektedir.[9]

Bilişim başka bir tanımda *"Bilginin ve iletişim yapısı ve özellikleri; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, süreçleri ve etkinlikleri*"[10] biçiminde ifade edilmiştir.

Yargıtay bir kararında bilişimi "bilginin otomasyona tabi tutulması sonucunda işlenmesi" olarak ifade etmiştir.[11]

Dülger ise bilişimi; *"Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayarlar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."*[12] şeklinde tanımlamıştır. Bu tanımlamada doktrindeki diğer tanımlarda bulunmayan işlemlere yer verildiği ayrıca özellikle de bilgisayar vurgusu yapıldığı görülmektedir. Doktrindeki bu tanımlar incelendiğinde; bilginin bilgisayarlar aracılığıyla işlenmesi ve aktarılmasının ortak yön

---

[6] "*Bilişim; teknik, ekonomik, sosyal, hukuki alandaki verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır*." Değirmenci, Bilişim Suçları, s. 10.

[7] "*Bilişim bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır*." Yazıcıoğlu, Recep Yılmaz, Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle, İstanbul, Alfa Yayınları, 1997, s. 131.

[8] Erdoğan, Bilişim Suçları, s. 8.

[9] *"Bilişim, her alandaki üretilmiş bilgileri içeren verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili bir bilim dalıdır."* Kurt, Levent, Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Ankara, Seçkin Yayıncılık, 2005, s. 25.

[10] Aydın, D. Emin, Bilişim Suçları ve Hukukuna Giriş, Ankara, Doruk Yayınevi, Eylül 1992, s. 3.

[11] "Bilişim sözcüğü ise, bilginin otomasyona tabi tutulması sonucunda işlenmesini, başka deyişle, verinin saklanması, organize edilmesi, değerlendirilmesi, nakledilmesi, çoğaltılmasını da kapsamaktadır." Yargıtay Ceza Genel Kurulu E. 2007/6-136 K. 2007/150 T. 19.06.2007, (https://legalbank.net/arama/mahkeme-kararlari).

[12] Dülger, Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Ankara, Seçkin Yayıncılık, 2020, s. 68.

olduğu görülmektedir. Bilişim temelde bilgiyi var eden, saklayan, bu bilgiyi geliştirip sunan elektronik bir sistemin davranış ve yapısının incelenmesi esasında bir bilgi bilimidir.

Bazı yazarların bilişim kavramıyla bilgisayar kavramını karşılaştırdıkları görülmektedir. Bilgisayarların veri işleme görevi yapması ancak veri iletimi sağlayamaması sebebiyle bilişim kavramının bilgisayar kavramını içine alan daha geniş bir ifade olduğunu değerlendirenler[13] olduğu gibi bilim dalı ile makinenin iki farklı ifade olduğunu, içeriklerinin karşılaştırılmaması gerektiğini, bu sebeple yerinde bir karşılaştırma olmadığını[14] belirten yazarlar da bulunmaktadır.

Bilişim kavramının Türk hukukuna girişi 1989 tarihli Türk Ceza Kanunu ön tasarısının (TCKÖ) gerekçesinde bilişim alanının tanımlanması ile olmuştur.[15] Daha sonra 765 sayılı Kanun'a değişiklik getiren 06.06.1991 tarihinde TBMM tarafından kabul edilerek, 14.06.1991 tarihinde Resmi Gazete'de yayımlanıp yürürlüğe giren düzenlemede de aynı tanıma yer verildiği görülür. Bu düzenleme ile TCK'ya bilişim alanında suçlar başlığını taşıyan yeni bir bölüm eklemesi yapılmış ancak madde metinlerinde bilişim kavramı tercih edilmeyerek "*bilgileri otomatik olarak işleme tabi tutmuş olan bir sistem*" ifadesi kullanılmıştır. 1997'de düzenlenen TCKÖ'de bilişim alanı tanımında değişiklik yapılarak verileri toplayıp, yerleştirme işlemleri ile manyetik sistemler ifadelerine yer verildiği görülür.[16] 2003 yılındaki son tasarıda da bilişim alanı tanımı yeniden yapılmamış bir önceki tasarı ile aynı paralellikte düzenlenmiştir.

Türk hukukuna 1991 değişiklikleriyle giren 765 sayılı Türk Ceza Kanunu'na ilave edilen on birinci bab başlığından sonra gelmek üzere eklenen 525/a, b, c maddelerinde bilişim sistemi teriminin kullanılmayarak *"Bilgileri otomatik olarak işleme tabi tutmuş bir sistem"* ifadesine yer verildiği görülmektedir. Bilişim alanı ifadesinin kullanıldığı ancak bilişim sistemi kavramına yer verilmediği kullanılan "bilgileri otomatik işleme tabi tutan sistem" tabiriyle de bilişim sistemi kavramının karşılanmak istenildiği değerlendirilmektedir.

5237 sayılı TCK'da bilişim alanı ve bilişim sistemi ayrımı bulunmaktadır Kanun koyucunun ilgili düzenlemede bölüm başlığı olarak "bilişim alanı" ifadesine yer verdiği ancak madde içeriklerinde bilişim sistemi kavramının kullanıldığı görülmektedir. Bilişim alanı, bilişim sistemlerini de içeren daha teknik ve daha geniş kapsamlı bir kavram olarak karşımıza çıkmaktadır. Kanun koyucu 5237 sayılı Kanun'un 243. maddesinin gerekçesinde bilişim

---

[13] Yenidünya, Ahmet Caner/Değirmenci, Olgun, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, 1.bs., İstanbul, Legal Yayıncılık, 2003, s. 30.

[14] Dülger, Bilişim Suçları, s. 67.

[15] Bilişim alanı "...bilgileri depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden oluşan alan.." şeklinde tanımlanmıştır. Dülger, Bilişim Suçları, s. 69.

[16] "...verileri toplayıp yerleştirdikten sonra bunları otomatik olarak işleme tabi tutma imkânı veren manyetik sistemler…" Yenidünya/Değirmenci, Bilişim Suçları, s. 28.

sistemini, verileri yahut bilgileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma imkânı verebilen elektronik manyetik sistem olarak tanımlamıştır.[17] Her ne kadar bilişim sistemi denildiğinde sadece bilgisayarlar akla gelse de bilişim sistemi kavramının yalnızca bilgisayarları karşılamadığı, bilgisayarın bu sistemde kullanılan araçlardan sadece bir tanesi olduğu yani bilişim sisteminin daha kapsayıcı olduğu söylenebilir. Bilişim sistemleri genellikle verileri yönetmeye ve işlemeye yardımcı olmak için bilgisayarları içerirken, mutlaka bilgisayarların varlığı gerekmez. Bilişim teknolojisinin her gün gelişip ilerlemesiyle bilişim sistemleri hayatımızın neredeyse her alanında karşımıza çıkmaya başlamıştır. Banka kartları, ATM cihazları, e-imzalar, online para transferleri bilgisayar haricindeki bilişim sistemlerine örnek verilebilir.

1.1.2. Bilgisayar

Bilgisayar, kullanıcı tarafından sağlanan bir dizi talimatı kullanarak aritmetik ve mantıksal işlemleri otomatik olarak gerçekleştiren programlanabilir bir elektronik cihazdır.[18] Bilgi toplama, saklama, kullanıcı talimatlarına göre işleme ve ardından sonuca ulaştırma işlevini yerine getirir. İlk olarak on altıncı yüzyılda hesap yapan bir kişi için kullanılan bu kelimenin günümüzdeki kullanımı genellikle elektrikle çalışan programlanabilir dijital cihazları tanımlamakta dilimizde “elektronik beyin” olarak da adlandırılmaktadır.[19] "Enformatik", “sibernetik”, "kompüter" gibi kelimelere karşılık gelen bilgisayar aslında bilgileri işleyen bir makinedir.[20] Ancak bu ifade bilgisayarın gerçek niteliğini ortaya çıkarabilmek, bilgisayar ile hesap makinelerinin farkını yansıtabilmek adına yeterli değildir.[21] Bilgisayarın her şeyden önce bilişim özelliğine sahip olması gereklidir. Bu bilgisayarın her türlü bilgiyi işleyip saklayabilmesi, başka bir yere aktarıp değiştirilebilmesi, her çeşit problem üzerinde çalışabilmesi yani genel amaçlı kullanılabilmesi anlamına gelmektedir.[22] Bilgisayarı günümüz ev aletlerinden ayıran temel özellik bilgisayarın genel amaçlı kullanılabilmesidir. Evlerde bulunan buzdolabı, çamaşır makinesi, bulaşık makinesi gibi cihazlar da programlanabilme özelliğine sahiptir. Ama bu programlamayla yalnızca daha önce hazırlanmış programlar

[17] https://legalbank.net/belge/turk-ceza-kanunu-gerekceler/2677276/TCK (Erişim Tarihi: 25.12.2021).
[18] https://tr.wikipedia.org/wiki/Bilgisayar (Erişim Tarihi: 05/09/2022).
[19] Ansiklopedik Kişisel Bilgisayar Kılavuzu, PC World, Ocak 1995 s. 1-9.
[20] Erem, Faruk, “Bilgisayar Suçları ve Türk Ceza Kanunu”, Türkiye Barolar Birliği Dergisi, C.5, S.2 (Mayıs 1993), s. 179.
[21] Yazıcıoğlu, Bilgisayar Suçları, s. 170.
[22] Taşdemir, Kubilay, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları, Ankara, Ütopyagrafik, 2009, s. 244.

seçilebilecektir. Bilişim özelliğine sahip bilgisayar üzerinde ise kullanıcı bilgiyi dilediği gibi işleyip değiştirebilmekte, başka yere aktarabilmektedir.

Bilgisayar donanımsal özelliklerine göre; *"İnsanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler"*[23] şeklinde tanımlanabilir.

Bilgisayarın birçok fonksiyonunun bulunması ve gelişen teknoloji karşısında sabit bir bilgisayar tanımı yapılması yerine durum ve özelliklerini belirten tanımların daha isabetli olacağı, günümüz koşullarında hangi tanım yapılırsa yapılsın bu tanımı tam karşılayamayacağı yönünde görüşlerde bulunmaktadır.[24]

Yirminci yüzyılda icat edilen bilgisayarın çok uzun bir geçmişi olmamasına rağmen son yıllarda büyük bir gelişim gösterdiği görülmektedir. Bilgisayarların toplumsal ve ekonomik hayatta etkinliği oldukça fazladır. Bilgisayar özelliklerinin zaman içerisinde gösterdiği değişim ve gelişim süreçleri genellikle bilgisayar nesli olarak adlandırılmaktadır. Günümüzde kullandığımız sistemler beşinci nesil bilgisayarları oluşturmaktadır[25]

Birinci nesil 1944'ten 1958'e kadar olan dönemdir.[26] Bu dönem, bilgisayarların kullanımı için makine dilinin geliştirildiği bir süreçtir. Devre için vakum tüplerinin kullanıldığı, hafıza amacıyla manyetik tamburların hayata geçirildiği bir dönemdir. Bu nesil makinelerin oldukça karmaşık, büyük ve pahalı oldukları görülür. Ayrıca bilgisayarlar hızlı ısınmakta ve fazla enerji harcamaktadır. Çoğunlukla toplu işletim sistemleri üzerine inşa edilmişlerdir. ABD ordusu tarafından 1946 yılında genel kullanım amaçlı geliştirilen ENIAC[27] adlı ilk elektronik bilgisayar bu dönemdedir.[28]

1957 ile 1963 yılları, ikinci nesil bilgisayarlar olarak anılmaktadır. Burada vakum tüplerinden transistörlere geçiş yapılmıştır. Böylece bilgisayarlar daha küçük, daha hızlı ve daha enerji verimli hale getirilmiştir. Bu yıllardaki bilgisayarların en önemli özelliği programlanma özelliğidir.[29] Önceleri yapılan her şey bilgisayarın yapısına bağlıyken bu

---

[23] Değirmenci, Bilişim Suçları, s. 10.
[24] Akbulut Bozdoğan, Berrin, "Bilişim Suçları", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, C.8, S.1-2, (Haziran 2000), s. 546.
[25] Karahoca, Dilek/Karahoca, Adem, Yönetim Bilişim Sistemleri ve Uygulamaları, İstanbul, Beta Yayınları, 1998, s. 3.
[26] Keser, Hafize, "Bilgisayarın Evrimi", Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, C.24, S.2 (1991), s. 415.
[27]İngilizce Electronic Numerical Integrator And Computer (ENIAC) kelimesinin kısaltmasıdır. Türkçe'ye elektronik sayısal entegreli hesaplayıcı olarak çevrilmiştir. https://tr.wikipedia.org/wiki/ENIAC (Erişim Tarihi: 05/09/2022).
[28] https://tr.wikipedia.org/wiki/Bilgisayar# (Erişim Tarihi: 05/01/2022).
[29] Yazıcıoğlu, Bilgisayar Suçları, s. 19.

dönemde bilgisayardan bağımsız programlamaların ortaya çıktığı görülmektedir.

Üçüncü nesil olarak adlandırılan 1964 ile 1971 yılları arası dönemde transistörlerin yerini tümleşik devrelerin aldığı görülmektedir. Tek bir tümleşik devre hem bilgisayarın gücünü artırırken aynı zamanda maliyeti de düşüren birçok transistörden oluşmaktadır.[30] Donanım ile yazılım bu dönemde birleştirilmeye çalışılmıştır. Bu bilgisayarlar öncekilerden daha hızlı, daha küçük, daha güvenilir ve daha ucuzdur. [31]

Mikroişlemcilerin icadı, dördüncü nesil bilgisayarları beraberinde getirmiştir. 1971 ile 1980 yılları dördüncü nesil bilgisayarların egemenliği altına girilerek sistem yazılımları C, C++ ve Java, bu nesil bilgisayarlarda kullanılan geliştirilen programlama dilleri olarak ilk defa karşımıza çıkmıştır.[32] Ayrıca bu dönem, ev kullanımı için bilgisayarın da üretilmeye başlandığı dönemdir.

Son olarak beşinci nesil bilgisayarlar 1980 yılından beri kullanılmakta ve günümüzde de kullanılmaya devam edilmektedir. Beşinci nesil bilgisayarlar dünyanın bugünü ve geleceği olarak düşünülür. En yeni ve gelişmiş bilgisayar nesli olan beşinci nesil bilgisayarların belirleyici yönü yapay zeka teknolojisi olarak karşımıza çıkmaktadır.

1.1.2.1. Donanım

1940'larda icat edilen bilgisayarlar çalışabilmek için hem donanıma hem de yazılıma ihtiyaç duyan oldukça karmaşık makinelerdir. Yirminci yüzyılın ortalarında, bilgisayarlaşma ve veri paylaşımı çağında bilgisayar bileşenlerinin nasıl etkileşime girdiğini anlayabilmek ve bu terimler arasında ayrım yapabilmek her birey için gereklidir.

Donanım, veri işlemek için kullanılan bilgisayar sisteminin fiziksel bileşenlerini ifade eden bir terimdir.[33] Bu tür bileşenler, bir bilgisayar sistemi içindeki işlevsel kullanımlarına göre sınıflandırılır. Donanım; mikroişlemci, anakart, güç kaynağı gibi unsurları içeren bilgisayarın içindeki tüm bileşenlerden oluşmaktadır. Bilgisayarı açmadan insan gözüyle görülebilen diğer donanım bileşenlerine monitör, klavye, fare, yazıcı, CD sürücüsü örnek gösterilebilir

Birincil öneme sahip üç ana donanım bileşeni bulunmaktadır. Bunlar; merkezi işlem birimi (central process unit), ROM (salt okunur bellek) ve RAM (rastgele erişim belleği)'dir.[34]

Merkezi işlem birimi yazılım talimatlarının yorumlanması, yürütülmesi için gerekli olan

[30] Keser, "Bilgisayarın Evrimi", s. 417.
[31] Yazıcıoğlu, Bilgisayar Suçları s. 20.
[32] Keser, "Bilgisayarın Evrimi", s. 418-419.
[33] Ansiklopedik Kişisel Bilgisayar Kılavuzu, s. 17.
[34] Karahoca/Karahoca, Yönetim Bilişim Sistemleri, s. 6.

tüm sistemin anahtar bileşeni, beynidir ve tüm hesaplamalar burada yapılmaktadır.[35] Merkezi işlem biriminin dört ana işlevi gerçekleştirmekle görevli olduğu söylenebilir. Tüm bilgisayar programlarının performansını yönlendiren talimatları alma, bu talimatları deşifre etme, daha sonra bunları pratik uygulamaya dönüştürme ve son olarak geri bildirim alarak gerçekleştirilen etkinlikleri gerektiğinde çıkarabilmek için bilgisayar belleğinde saklamakla görevlidir.[36] Çip adıyla adlandırılan bilgisayarın içinde bulunan merkezi işlem birimi, bilgisayardaki aritmetik ile mantıksal işlemleri yapmakta olup, aygıtın kendisi dahi bazı olaylarda delil olarak kullanabilmektedir.[37]

ROM (Salt Okunur Bellek), yalnızca bilgisayarlarda değil, aynı zamanda bir dizi başka elektronik aygıtta da kullanılan yerleşik, kalıcı bir veri depolama biçimidir. Kolayca değiştirilememesi veya yeniden programlanamaması nedeniyle bilgisayarın aniden kapanması veya yeniden başlatılması durumunda veri kaybına uğramamayı sağlar. [38]

RAM (Rastgele Erişim Belleği), sistem çalışma hızını en üst düzeye çıkarmak için sık çalıştırılan uygulamaların program talimatlarını ezberlemekten sorumlu olan başka bir veri depolama biçimi olan RAM verilerin nerede depolandığına bakılmaksızın aynı zaman diliminde yazılmasını veya okunmasını mümkün kılmaktır.[39] ROM'dan farkı yazılabilen, silinebilen, geçici hafızalı olmasıdır.

Bu üç bileşenin bağlı olduğu donanım ise anakart olarak tanımlanmaktadır. Bu kart, bilgisayarın çıkış ve giriş aygıtları dışında neredeyse tüm parçalarını bir arada tutmaktadır. Bir bilgisayar kasasında bulunan en önemli ve en büyük devre kartı anakarttır. Kendisine bağlı tüm donanımlara güç tahsis eden anakart ayrıca cihazların birbirleriyle iletişim kurmasını sağlamaktadır.

Diğer bir donanım ise monitördür. Monitör, bir bilgisayarın görüntüleme birimi olarak tanımlanabilir. Metinler ve resimler gibi işlenmiş tüm veriler doğrudan monitörde görüntülenir. Monitör ayrıca bir kutu içerisinde ekran devresi içermektedir. Görsel görüntüleme birimi olarak da adlandırılan monitörlerin farklı türleri de bulunmaktadır. CRT monitör, LCD ekran, LED monitör ve plazma monitörü bunlara örnek gösterilebilir.

Klavye veya diğer adıyla tuş takımı, donanımın başka bir unsurudur. Klavyenin, bilgisayarın en önemli giriş aygıtlarından biri olduğu söylenebilir. Klavye, kullanıcının metin,

---

[35] Değirmenci, Bilişim Suçları, s. 11.
[36] https://tr.wikipedia.org/wiki/Merkez%C3%AE_i%C5%9Flem_birimi (Erişim Tarihi: 30.08.2022).
[37] Berber, Leyla Keser, Adli Bilişim (Computer Forensic), Ankara, Yetkin Yayınları, 2004, s. 54-55.
[38] http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/06/bellek-turleri (Erişim Tarihi: 22.04.2022).
[39] https://tr.wikipedia.org/wiki/RAM (Erişim Tarihi: 30.08.2022).

karakter ve diğer komutlarının doğrudan bir bilgisayara, tablete, masaüstüne veya diğer cihazlara girmesine izin verecek şekilde tasarlanmıştır. Klavyeler ayrıca karakterleri, sayıları girmek ve diğer birçok işlevi gerçekleştirmek için kullanılabilecek farklı tuş takımlarını da içermektedir. Klavyeler tarafından gerçekleştirilebilen bazı işlevler arasında yapıştır, kopyala, gir ve sil eylemleri yer almaktadır.

Diğer donanım unsuru olan fare, küçük bir el cihazı olarak tanımlanabilir. Bu cihaz, bilgisayar ekranında bulunan imleci kontrol etmek veya hareket ettirmek için tasarlanmıştır. Bir fare temel olarak kullanıcının bilgisayarın ekranında bulunan herhangi bir nesneyi seçmesine veya işaret etmesine yardımcı olmaktadır. Bu cihaz, imleci kontrol etmek için düzgün hareket sağlamak için genellikle düz bir yüzeye yerleştirilerek kullanılmaktadır.

1.1.2.2. Yazılım

Bilgisayarların yalnızca donanımsal parçalarıyla kendi başına herhangi bir işlem yapabilmeleri mümkün değildir. Bu nedenle bilgisayarın bir problemi çözebilmesi için gerçekleştirmesi gereken anlaşılabilir dilde yazılmış talimat dizisinin belirlenmesi gereklidir. Yazılım, bilgisayar tarafından verileri işleme faaliyetini kontrol edebilmek için oluşturulan ve bilgisayarın tam olarak yapmasını istediği şeyi gerçekleştirmesini sağlayan talimat dizileri, komutlardır.[40] Yazılım bir programlar topluluğunu ifade eder ve amacı donanımı harekete geçirmektir.[41] Yazılım kavramının mevzuatımızda 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanunu'nun 3. maddesinde de tanımladığı görülmektedir.[42]

Belirli bir sorunu çözen veya belirli bir iş türünü gerçekleştiren bir grup program olarak tanımlanan yazılımlar bir kelime işlem paketi, metin düzenleme, metin biçimlendirme, grafik çizme, yazım denetimi gibi programlar içerebilmektedir.[43] Dolayısıyla, çok amaçlı bilgisayar sistemlerinin, gerçekleştirebileceği her tür iş için bir tane olmak üzere birkaç yazılım paketine sahip olması gereklidir. Sistem yani işletim yazılımı, bir bilgisayar sisteminin işleyişini kontrol etmek ve işleme kapasitesini genişletmek için tasarlanmış bir veya daha fazla program kümesi

---

[40] Dülger, Bilişim Suçları, s. 62.
[41] Esen, Hüseyin Öner, İşletme Yönetiminde Sistem Yaklaşımı, 3. bs., İstanbul, Alfa Yayınları, 1998, s. 10.
[42] 4691 sayılı Teknoloji Geliştirme Bölgeleri Kanunu'nun 3/1-l bendinde yazılım "*Bir bilgisayar, iletişim cihazı veya bilgi teknolojilerine dayalı bir diğer cihazın çalışmasını ve kendisine verilen verilerle ilgili gereken işlemleri yapmasını sağlayan komutlar dizisinin veya programların ve bunların kod listesini, işletim ve kullanım kılavuzlarını da içeren belgelerin, belli bir sistematik içinde, tasarlama, geliştirme şeklindeki ürün ve hizmetlerin tümü ile bu ürün ya da mal ve hizmetlerin lisanslama, kiralama ve tüm hakları ile devretme gibi teslim şekillerinin tümü"* şeklinde tanımlanmıştır. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4691.pdf (Erişim Tarihi: 28.08.2022).
[43] https://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1m (Erişim Tarihi: 28.04.2022).

olarak tanımlanır.[44] Genel olarak bir bilgisayarın sistem yazılımının, diğer uygulama yazılımlarının geliştirilmesi ve yürütülmesini destekleme, çeşitli donanım kaynaklarının etkin kullanımını izleme, yazıcı, disk gibi çevresel aygıtlarla iletişim kurarak bunların çalışmasını kontrol etme gibi işlevleri bulunmaktadır.[45]

Sistem yazılımının, bilgisayar sisteminin çalışmasını daha verimli ve etkili hale getirdiği söylenebilir. Donanım bileşenlerinin birlikte çalışmasına yardımcı olarak uygulama yazılımının geliştirilmesi ve yürütülmesi için destek sağlayacaktır.

Uygulama yazılımları sistem yazılımlarıyla aynı özellikleri gösteren yazılım türüdür. Uygulama yazılımlarını sistem yazılımlarında ayıran en önemli özellik belirli bir işlevi yerine getirme görevine özgülenmeleridir.

1.1.2.3. İnternet

İnternet; dünya üzerindeki milyonlarca ağın ve bilgisayarın birbirine bağlanmasına olanak sağlayan yayılmış bir uluslararası ağ sistemidir.[46] Günümüzde bilgiye ulaşmanın en kolay yolu olarak görülen internetin Türkçe kelime anlamı ise "genel ağ"dır.[47]

Daha teknik ifade etmek gerekirse internet mevcut ağların ve bilgisayarların internetin çalışmasına olanak sağlayan TCP/IP[48] (Transmission Control Protocol/Internet Protocol) adında bir protokolle birbiriyle bağlantı kurması sonucu oluşan ağlar bütününe verilen addır. İnternete bağlanabilen tüm ağlar bu protokolleri kullanmak zorundadır. TCP bilgisayarlar arasındaki iletişimin veri kaybına uğramaksızın küçük paketler halinde gerçekleştirilmesine yarayan, IP ise ağ adresleme sistemini belirten protokoldür.[49]

İnternetin tarihçesine bakacak olursak internet; kesin bir tarih verilmemekle birlikte yirminci yüzyılın ortalarında ilk olarak askeri alanda kendisini göstermiştir. 1969 yılında Amerika Birleşik Devletleri savaş halinde haberleşme ağlarının devamını sağlamak ve bilgisayarların güvenli bir ağla birbirlerine bağlanabilmesi amacıyla ARPA (Advanced Research Projects Agency) kurumu aracılığıyla ARPANET ağını kurmuştur.[50] Askeri amaçlı

---

[44] Akbulut, Bilişim Alanında Suçlar, s. 12.
[45] Kurt, Bilişim Suçları, s. 34.
[46] Erkan Boğaç/Songür Murat, Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü, Ankara, Hacette-Taş Yayınevi, 1999, s. 282.
[47] www.tdk.gov.tr. (Erişim Tarihi:18/11/2021).
[48] İngilizce "Transmission Control Protocol" ve "Internet Protocol" kelimelerinin baş harflerinin kısaltılmasıyla oluşan TCP/IP "İletim Kontrol Protokolü" ve "İnternet Protokolü" olarak Türkçe'ye çevrilmektedir.
[49] Sınar, Hasan, İnternet ve Ceza Hukuku, İstanbul, Beta Yayıncılık, 1.bs., 2001, s. 24.
[50] Akbulut, Bilişim Alanında Suçlar, s. 19; Orta Doğu Teknik Üniversitesi Bilgi İşlem Daire Başkanlığı "İnternet Tarihi" http://www.internetarsivi.metu.edu.tr/tarihce.php (Erişim Tarihi:18/11/2021).

kullanılan bu ağa daha sonra farklı kuruluşların bağlanmasıyla katılımcı sayısı çoğalmış ve ARPANET protokolündeki yük artmıştır.[51] Bu nedenle farklı özellikteki bilgisayarların aralarında bağlantı kurmasını sağlayan ve yine yerel ağların da birbirleriyle bağlantısını oluşturan TCP/IP gibi protokoller geliştirilmiştir.[52]

Ülkemizde internet bağlantısı ilk olarak 12.04.1993'te Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'nun (TÜBİTAK) desteklediği bir proje sonucu Orta Doğu Teknik Üniversitesi (ODTÜ) tarafından gerçekleştirilmiştir.[53]

Günümüzde insanların olmazsa olmazı haline gelen internet yaşamın her alanında kendisini göstermektedir. İnsanların görüntülü konuşması, bankacılık işlemleri, basit ve ucuz haberleşmenin sağlanması dosya, görüntü paylaşabilmesi internet sayesinde olmaktadır. Ancak internetin her ne kadar iyi ve yararlı yönleri kullanılmışsa da zamanla hemen hemen her şeyin internet üzerinden yapılabilmesi kötü amaçlı kullanıma da zemin hazırlamıştır. İşte bu kötü niyetli kullanım neticesinde bir sonraki başlıkta da değineceğimiz üzere bilişim suçları ortaya çıkmıştır.

1.2. Bilişim Suçları ve Tarihsel Gelişimde İşleniş Yöntemleri

1.2.1. Genel Olarak Bilişim Suçları ve Özellikleri

İnsanın doğası gereği ilk çağlardan beri yenilikçi ve yaratıcı olduğu görülmektedir. Farklı ihtiyaçlar yeni cihazların, araçların ve teknolojilerin ortaya çıkmasına neden olmuştur. Teknoloji aynı zamanda insanın işini kolaylaştırmak için yaptığı bir keşiftir. Teknolojideki ilerleme bir yandan faydalı olsa da diğer yandan teknolojinin bazı yıkıcı etkileri de bulunmaktadır. Bilişim suçlarının da bu teknolojik gelişmelerin olumsuz bir yönü olduğu söylenebilir. Teknolojinin sürekli değişip gelişmesiyle bilişim suçlarının farklı işlenme yöntemleri ortaya çıkmakta bunun neticesinde de bilişim suçları teriminin uluslararası alanda ortak bir tanımı yapılamamaktadır.

Mukayeseli hukukta bilişim suçlarını karşılayan genel bir kavram kullanılmadığı görülmektedir. İlk olarak Amerika'da işlendiği bilinen bilişim suçlarının Amerikan doktrininde "computer crime" şeklinde adlandırılmasıyla uluslararasındaki yaygın kullanıma yön verdiği

[51] Akbulut, Bilişim Alanında Suçlar, s. 19.
[52] Yenidünya/Değirmenci, Bilişim Suçları, s. 40-42.
[53] Sınar, İnternet ve Ceza Hukuku, s. 111.

söylenebilir.[54] Her ne kadar yaygın kullanımı "computer crime" olsa da birçok ülkenin kavramı karşılayacak başka ifadeler de kullandıkları görülmektedir.[55]

Ülkemizde de ilk zamanlar bilişim suçları kavramının hangi terim ile ifade edilebileceği sorunu yaşanmıştır. İnternet suçu, siber suç, bilgisayar suçu, ileri teknoloji suçu gibi kavramların bilişim suçu yerine kullanıldıkları görülmektedir.[56] Ancak bu kavramların hiçbirinin suçun tanımına tam olarak uyduğu söylenemeyecektir. Bilişim alanında suçların ülkemizde ortaya çıktığı ilk zamanlarda bilgisayar suçları tabiri kullanılmış, ancak bilgisayarın suç işlemede kullanılan sadece bir araç olması bu sebeple kullanılan kavramın doğru olmadığı belirtilerek eleştirilmiştir.[57] Günümüzde ise bilişim suçunun dışında siber suç ifadesinin de yaygın kullanıldığı görülür. Türkçe sözlüklerde tam olarak karşılığı bulunmayan bu kelimenin sanal suç kavramının karşılığı olduğu, ifade edilmek istenen kavramı tam olarak karşılayamadığı ve gerçek işlenen suçların sanal bir ifadeyle belirtilmemesi gerektiği sebepleriyle eleştirilere maruz kalmıştır.[58]

Doktrindeki bu kavram belirsizliği, kanuni düzenlemelerde de kullanılan ve genel kabul gören bilişim suçları kavramının tercih edilmesiyle çözülmüştür. Bizim kanaatimize göre de bilişim suçu doğru ve kapsayıcı ortak bir kavramdır ancak ülkemizde kolluk birimlerinde bilişim suçu yerine siber suç kavramının tercih edildiği görülmekte ve sebebi anlaşılamamaktadır. AKSS'de de siber suç kavramı kullanılmış, ancak tanımı yapılmayarak suçu oluşturan eylemlerin tek tek sayılması suretiyle kavram açıklanmaya çalışılmıştır.

Doktrinde bilişim suçlarının kavram karışıklığının tanımına da yansıdığı ve görüş birliğinin sağlanamadığı dikkat çekmektedir. Yazarların bazılarının suçu oluşturan eylemlere önem ve öncelik vererek tanımlamalar yaptıkları, bir kısmının suçla korunan hukuki değeri esas alarak dar veya geniş yorumlamalarda bulundukları görülmektedir. Neticeten tüm bu yazarların esas aldığı değerler de dikkate alınarak bilişim suçlarının altı farklı kıstas temelinde tanımlanabileceğinde uzlaşılmıştır.[59]

---

[54] Yazıcıoğlu, Bilgisayar Suçları, s. 125.

[55] Alman Hukuku'nda "computer kriminalität" terimi kullanılmakta, Fransız Hukuku'nda bilişim alanı "Le droit pénal informatique", bilişim suçları "la fraude informatique", bilişim suçluluğu "la criminalité informatique" kavramlarıyla karşılanmakta ve İtalyan Hukuku'nda ise ilk zamanlar "dolo informatico" (enformatik cürmü), "I reati elettronici" (elektronik suçlar) veya "I reati commessi con I'uso del computer" (bilgisayar kullanımı vasıtasıyla işlenen suçlar) gibi kavramlar 23 Aralık 1993 tarih ve 547 sayılı "Bilişim Suçluluğu Alanında Ceza ve Ceza Usul Kanunlarında Değişiklik Yapılmasına Dair Kanun" dan itibaren de "bilişim suçluluğu" (la criminalitá informatica) kavramının kullanıldığı görülmektedir. Yazıcıoğlu, Bilgisayar Suçları, s. 126-129.

[56] Sınar, İnternet ve Ceza Hukuku, s. 129; Tanılır, Mehmet Niyazi, İnternet Suçları ve Bireysel Mahremiyet, Ankara, Liberte Yayınları, 2002, s. 13.

[57] Değirmenci, Bilişim Suçları, s. 55.

[58] Dülger, Bilişim Suçları, s. 72.

[59] Akbulut Bozdoğan, "Bilişim Suçları", s. 550-551.

Bilişim suçunu oluşturan eylemlere önem vererek tanımlayan Kurt'a göre, bilişim sistemlerindeki verilerin hukuka aykırı işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi bilişim suçunu oluşturacaktır.[60] Aydın'ın tanımına göre ise; verilere hukuka aykırı erişilmesi, verilerin hukuksuz değiştirilmesi, silinmesi, kayıtlara girilmesi veya girme hazırlıklarının yapılması eylemleri bilişim suçunu oluşturacaktır.[61]

Bazı yazarların ise bilişim suçu oluşturacak eylemleri belirtmeyerek eylemin yöneldiği alana önem veren tanımlamalar yaptıkları görülür. İçel "bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik eylemler" in bilişim suçu oluşturacağını belirtmiştir.[62]

Bilişim suçunu dar ve geniş anlamda iki farklı biçimde tanımlayan yazarlar da bulunmaktadır. Erdoğan'ın dar anlamdaki tanımında yalnızca bilişim alanında işlenebilen suçlara yer verdiği geniş anlamdaki tanımında ise bilişim sistem veya araçlarının suç işlerken kullanılması durumuyla suçun kapsamını genişlettiği görülür.[63]

Dülger ise dar anlamda "*verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenliğine ya da bütünlüğüne karşı işlenen suçlar"*, geniş anlamda *"bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suç"* biçiminde iki farklı tanımlama yaparak bilişim suçları ifadesinden kastının dar anlamda suçlar olduğunu ifade etmektedir.[64] Akbulut'un görüşünün Dülger'e benzer olduğu bilişim teknolojilerinin neticesi olarak oluşan bilişim sistemine girme, sisteme ve verilere müdahale gibi suçların dar anlamda bilişim suçlarını, kanunda mevcut hırsızlık, dolandırıcılık gibi klasik suç tiplerinin bilişim araçlarıyla işlenmesinin de geniş anlamı kapsadığını ifade etmiştir.[65]

Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu Paris Toplantısı'nda bilişim suçlarını *"Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* olarak tanımladığı görülmektedir.[66] Bu topluluğun ayrıca bir tavsiye kararında bilişim suçlarını beşe ayırarak

---

[60] Kurt, Bilişim Suçları, s. 53.
[61] Aydın, Bilişim Suçları, s. 27.
[62] İçel, Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri" İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 59, S. 1-2, (2001), s. 3.
[63] Dar anlamda bilişim suçları "*bilişim sisteminin kendisinin ya da bilişim sistemi içerisinde bulunan verilerin hedef alındığı ve bilişim teknolojilerinin kullanılması suretiyle ya da bilişim araçlarına doğrudan fiziki müdahaleyle işlenen suçlardır",* geniş anlamda bilişim suçları ise *"herhangi bir şekilde suçun icrasında bilişim sistem ya da araçlarının kullanıldığı ya da bilişim sistemlerinin veya içindeki verilerin hedef alındığı suçlardır"* Erdoğan, Bilişim Suçları, s. 234.
[64] Dülger, Bilişim Suçları, s.75-76.
[65] Akbulut, Bilişim Alanında Suçlar, s. 69-70.
[66] Erdoğan, Bilişim Suçları, s. 49.

tasnif ettiği verilere girme, bunları bozma, silme veya yok etme eylemlerinin hukuka aykırı girilen sistemlerde verilerin aktarımını sağlamak için, dolandırıcılık amacıyla ve bilişim sisteminin çalışmasını engellemek suretiyle işlenmesini, bilgisayar programlarından haksız çıkar elde edilmesini, güvenlik önlemleriyle korunan bir bilişim sistemine hukuka aykırı olarak güvenlik duvarının aşılarak girilmesi eylemlerini bu kapsamda değerlendirdikleri görülmektedir.[67]

Tüm bu tanımlamalar doğrultusunda kanaatimizce bilişim suçları kavramı temelde iki farklı şekilde tanımlanabilecek bunların ilkini bilişim sistemleri ve/veya verileri hedef alan eylemler oluştururken ikinci tanımlama bilişim sistemlerinin araç olarak kullanılması suretiyle gerçekleşen suçları kapsadığı söylenebilecektir.

Teknolojik yeniliklerin yararlarının yanında kötü niyetli kişilerce kullanılmasının yol açtığı zararların en iyi örneği olan bilişim suçlarının tarihi on dokuzuncu yüzyılda telgraf sistemleriyle işlenen dolandırıcılıklara dayandırılabilir.[68] Bu dönemde suç işleyen kişilerin bazı dolandırıcılık eylemlerinde telgraf sistemlerini kullanmasıyla günümüzdeki bilişim suçları arasında ilişki kurmayı sağlayacak bir benzerlik dikkat çekmektedir.

Tarihte gerçek anlamda bilişim suçu olarak değerlendirilen ilk olay bir Amerikan gazetesinde 1966 yılında yayımlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlığını taşıyan haber olarak kabul edilmektedir.[69] Bilgisayarların ana vatanı olarak görülen Amerika'da bilişim suçlarıyla mücadeleye de diğer ülkelerden önce başlandığı görülmektedir. Avrupa ülkelerinin ise bu suçlara ilgi göstermesi neredeyse 1970'li yılları bulmuştur. Evlerde bilgisayar kullanımının yaygınlaştığı 1980'li yıllarda bilişim suçlarının nitelik değiştirerek sadece malvarlığı amacıyla haksız bir menfaat elde etmek amacıyla değil başka menfaatler içinde işlenebileceği ortaya çıkmıştır.[70]

1990'lı yıllarda internet ağlarının yaygınlaşması bilişim suçlarının artmasına ve yeni suç şekillerinin oluşmasına sebep olmuştur. Günümüzde de hala kullanılan ve truva atı, ağ solucanı gibi sistemlere zarar veren yazılımların ilk defa bu dönemde ortaya çıktıları bilinmektedir.

1.2.2. Bilişim Suçları İşlenirken Sık Kullanılan Yöntemler

1.2.2.1. Truva Atı

[67] Özel, Cevat, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, C. 75, S.7-8-9 (Eylül 2001), s. 858.
[68] Dülger, Bilişim Suçları, s. 94.
[69] Akbulut, Bilişim Alanında Suçlar, s. 51.
[70] Akbulut, Bilişim Alanında Suçlar, s. 52.

Truva atları; kendi kendilerine çoğalabilme özellikleri olmadığı için teknik olarak virüs olmayan, ücretsiz yardımcı bir programmış gibi yararlı görünen ancak aslında bir tür kötü amaçlı ve sisteme zarar veren yazılımlardır.[71] Tarihte ki Truva atı efsanesiyle benzer yönlerinin olması nedeniyle bu şekilde adlandırılmıştır.[72]

Truva atları meşru bir program kılığında bilgisayara indirilen bir tür kötü amaçlı yazılımlardır. Tek amacı, dosyaları silerek veya bozarak disk biçimlendirmesiyle veya büyük miktarda bilgisayar kaynağı kullanarak bilgisayarın ya da ağların çalışmasını engellemektir. Bilgisayar ayarlarının beklenmedik bir şekilde değiştirilmesi gibi olağan dışı etkinliklerin gerçekleşmesi bir sistemde truva atı yazılımının varlığının en belirgin belirtilerindendir. Bilgisayar virüslerinin aksine bir truva atı yazılımının kendi kendine oluşmaması nedeniyle çalışması için bir kullanıcının yazılımın sunucu tarafını indirmesi gerekmektedir.

Truva atı yazılımı en yaygın meşru görünen e-postalar ve e-postalara eklenen dosyalar, ücretsiz yazılım imkânı sağlayan web siteleri aracılığıyla yayılırlar. Gelen kutusundaki mail kişilerce açıldığında ya da eklenen dosya bilgisayara indirildiğinde truva atı sunucusu yüklenir ve artık cihaz her açıldığında otomatik olarak yazılım çalışmaya başlar.[73] Bilişim suçu faillerinin truva atı yazılımını bulaştırmada kullandıkları diğer bir yolda sosyal mühendislik[74] taktikleri uygulayarak kullanıcıların kötü amaçlı uygulamayı indirmesini sağlamak ve kullandıkları cihazlara truva atı bulaştırmaktır. Böylece truva atı yazılımı, bulaştığı bilgisayarlarda sistemdeki yazılım açıklarını tespit edip bunlardan yararlanarak sistemin tamamında hâkimiyet kurup failin tüm komutlarını yerine getirmektedir.[75] Kötü amaçlı dosya, başlık reklamlarında, açılır reklamlarda veya web sitelerindeki bağlantılarda gizlenebilir. Örneğin; 2019 yılında ortaya çıkan "*AZORult*" adlı bir program ile internette sık kullanılan web siteleri taklit edilerek benzer web siteleri oluşturulduğu böylece sahte web sitesini gerçeğiyle karıştırarak siteye giren kullanıcıların bilgisayarına truva atı yazılımları

---

[71] Canbek, Gürol/Sağıroğlu, Şeref, "Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma", Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi C. 22, S. 1 (2007), s. 125.
[72] Aydın, Bilişim Suçları, s. 48.
[73] Dülger, Bilişim Suçları, s. 104.
[74] "Sosyal mühendislik, yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir." Arslan, Mehmet Emin, "Siber Güvenlik ve Siber Saldırı Türleri",(Çevrimiçi) https://www.academia.edu/31827545/S%C4%B0BER_G%C3%9CVENL%C4%B0K_VE_S%C4%B0BER_SALDIRI_T%C3%9CRLER%C4%B0_CYBER_SECURITY_AND_CYBER_ATTACK_TYPES_03_05_2016, (Erişim Tarihi:20.08.2022), s. 5.
[75] Değirmenci, Bilişim Suçları, s. 79.

yerleştirildiği tespit edilmiştir.[76] Kullanıcıların kripto hesap bilgileri de dahil olmak üzere bir çok veriyi elde etmeye imkânı sağlayan bu yöntem ile Türkiye'de 2020 yılı içinde toplamda 12.748 sistem kullanıcısı hedef alınmıştır.[77]

Kötü amaçlı bir yazılım türü olan truva atları bulaştığı bir bilgisayarı zombi bilgisayara[78] dönüştürerek bu bilgisayar aracılığıyla diğer bilgisayarlara zararlı yazılımın aktarımını sağlayarak kullanıcının haberi olmadan uzaktan kontrol sağlayabilecektir.[79] Truva atı virüsleri direkt olarak bilgisayarın işletim sistemini hedef alır ve bilgisayara hangi program aracılığıyla girmiş ise o program açılana kadar bilgisayarda aktif rol alamaz. Kötü amaçlı yazılımların ortak özellikleri dosya silme, bilgisayarı yavaşlatma veya sabit sürücüyü tamamen silme gibi bir bilgi işlem aygıtı üzerinde kasıtlı olarak zarar verici eylemler gerçekleştirmeleridir.[80]

Faillerin farklı eylemler ve farklı saldırı yöntemleri gerçekleştirmek için kullandıkları truva atı türleri bulunmaktadır. Kullanılan en yaygın truva atı türleri; arka kapı truva atı, bankacı truva atı, dağıtılmış hizmet reddi (DDoS) truva atı, indirici truva atı, exploit truva atı ve sahte antivirüs truva atı olarak karşımıza çıkmaktadır.[81]

Günümüzde mobil bankacılık faaliyetlerinin sık kullanılması bilişim suçu işleyen kişilerin dikkatini çekerek dünya genelinde bankacılık truva atı kötücül yazılımlarıyla daha çok karşılaşılmasına sebep olmuştur. 2021 yılında Kore'de ortaya çıkan "*Fakecalls*" isimli bir yazılım bilinen bankaların uygulamalarını taklit ederek kişilerin gerçek bankanın uygulamasıyla karıştırıp uygulamayı telefonlarına yüklemesini hedeflemektedir. Uygulamada dikkat çeken nokta gerçek bankanın müşteri hizmetleri numarasına yer verilmesidir. Daha önceki bankacı truva atlarında olmayan özelliği kişilerin müşteri hizmetlerini aramaları durumunda telefonda gerçek müşteri hizmetlerinin numarası görünmesine rağmen görüşmeyi kesip kendilerine yönlendirebilmeleri ve bankanın müşteri temsilcisi gibi görüşme sağlayıp

---

[76]https://www.indyturk.com/node/134161/haber/t%C3%BCrkiyedeki-internet-kullan%C4%B1c%C4%B1lar%C4%B1na-da-sald%C4%B1ran-truva-at%C4%B1-tespit-edildi%E2%80%A6-23 (Erişim Tarihi:20.08.2022).

[77]https://www.indyturk.com/node/134161/haber/t%C3%BCrkiyedeki-internet-kullan%C4%B1c%C4%B1lar%C4%B1na-da-sald%C4%B1ran-truva-at%C4%B1-tespit-edildi%E2%80%A6-23 (Erişim Tarihi:20.08.2022).

[78] Zombi (köle) bilgisayar, 13/07/2014 tarihli 29059 sayılı Resmi Gazete'de yayımlanarak yürürlüğe giren Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği tanımlar ve kısaltmalar başlıklı 3. maddede köle bilgisayar kavramıyla; "*herhangi bir amaçla kullanılmak üzere, zararlı yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayar*" şeklinde tanımlanmıştır. https://www.mevzuat.gov.tr/File/GeneratePdf?mevzuatNo=19880&mevzuatTur=KurumVeKurulusYonetmeligi&mevzuatTertip=5, (Erişim Tarihi:22.09.2022).

[79] Goodman, Marc, Cybercrime, Cybercrimes: A Multidisciplinary Analysis, Ed., Sumit Ghosh, Elliot Turrini, Berlin, Springer, 2010, s. 57.

[80] Canbek/Sağıroğlu, "Kötücül ve Casus Yazılımlar", s. 123.

[81] Hoşcan, Yaşar, Yönetim Bilgi Sistemi, 2.bs., Ankara, Anadolu Üniversitesi Yayınları, 2003, s. 29.

bankacılık bilgilerine rahatlıkla ulaşabilmeleridir.[82]

1.2.2.2. Ağ Solucanları

Bağımsız olarak çoğalma ve ağlar arasında yayılmak için seyahat edebilme özelliklerine sahip ağ solucanları, önemli dosyaları yok ederek, bilgisayarı yavaşlatarak ve hatta bilgisayarın çalışmasını tamamen durdurarak tüm veri dizilerine zarar verme becerisine sahiptir.[83] Bu solucanlar aynı ağ üzerinde bulaşacak başka bilgisayar kalmayana kadar yayılmaya devam ettiğinden çok sayıda ağ kullanan işletmeler için daha fazla tehlikelidir.[84] Sisteme bir kez eriştikten sonra kendi başına ilerleyerek çok sayıda çoğalma sağlayabilen bu solucanlar oldukça hızlı yayılma gücüne sahiptir. Taşıyıcı bir programa veya bir dosyaya ihtiyaç duymayan solucanlar sistemde açtıkları bir tünel vasıtasıyla bilgisayar korsanlarının bilgisayar üzerinde rahatlıkla denetim kurmasına yardımcı olurlar.

Tarihte bilinen ilk ağ solucanı ABD'de 1988 yılında görülen bilgisayarda önlenemez bir çoğalmayla belleği doldurmak dışında zarar verici bir unsuru bulunmayan morris solucanı veya diğer adıyla internet solucanıdır.[85] İlk kez 2003 yılında ortaya çıkan o zamandan itibaren internete bağlı milyonlarca bilgisayara bulaşan en ünlü ve tehlikeli ağ solucanı türü olan sobig solucanı ise e-posta yoluyla yayılarak kendini çoğaltabilmektedir.[86]

1.2.2.3. Mantık Bombaları

Truva atı yazılımlarıyla benzer yönler taşıyan mantık bombaları önceden belirlenmiş bazı durumların gerçekleşmesiyle aktif hale gelerek zararlı yazılım işlevlerini başlatırlar ve yerleştikleri sistemde yıkıcı özellikte hareket ederler. Bu yazılımlar truva atının bir türü olarak değerlendirilse de truva atı yazılımları bulaştıkları sistemlerde kendisini her zaman gizli tutma çabasındayken mantık bombaları üretilirken ayarlanan, önceden belirli kodlanmış koşulun gerçeklemesiyle sisteme zarar vermeye başlar ve ortaya çıkarlar.[87] Mantık bombası, ya yazılımda mevcut dosyaya eklenir ya da var olanı değiştirerek istenen sonucu gerçekleştirir.[88]

---

[82] https://www.kaspersky.com.tr/blog/fakecalls-banking-trojan/10619/ (Erişim Tarihi:20.08.2022).
[83] Goodman, Cybercrime, s. 52.
[84] Hoşcan, Yönetim Bilgi Sistemi, s. 35.
[85] Dülger, Bilişim Suçları, s. 97.
[86] Goodman, Cybercrime, s. 55.
[87] Değirmenci, Bilişim Suçları, s. 101; Dülger, Bilişim Suçları, s. 111.
[88] Aydın, Bilişim Suçları, s. 3.

Mantık bombalarının en bilinen örneği olan 1999 tarihinde gerçekleşen Çernobil virüsü ile her ayın 26'sında bilgisayarların anakartına ve hard diskine zarar verilerek bilgisayar sabotajı gerçekleştirilmiş Türkiye'nin de aralarında bulunduğu pek çok ülke yazılımdan olumsuz etkilenmiştir.[89]

1.2.2.4. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

"*Hacking*" eylemi "*hacker*" denilen kişilerce gerçekleştirilir. "*Hacker*" bilişim sistemlerinin işleyiş sistemlerini merak eden ve sisteme müdahale eden kişiye verilen isim olarak karşımıza çıkarken "*cracker*" ise bu sisteme müdahale edenler arasında üst seviyede teknik bilgi ve donanıma sahip, tecrübeli, bu işte ileri düzeydeki kötü niyetli hukuki bir yarar sağlayan kişiler olarak tanımlanmaktadır.[90] Bilişim korsanı olarak adlandırılan bu kişiler bilişim sistemlerinin güvenlik duvarlarını aşarak sisteme sızabilmektedir. Amaçlarına göre üç temel hacker sınıflandırılması yapılmaktadır. Beyaz şapkalı hackerların sistemlerdeki güvenlik açıklarını tespit ederek kapatmaya çalıştıkları yani saldırılara karşı sistemleri koruduğu, siyah şapkalı hackerların sistemlere sızarak kişisel kazanç elde ettikleri, gri şapkalı hackerların ise sistemdeki zayıflıkları tespit ederek sistem sahibine göstermeyi amaçladıkları görülmektedir.[91]

1.2.2.5. İstem Dışı Alınan Elektronik Postalar (Spam)

Son zamanlarda istenmeyen elektronik postalar herkes için önemli bir sorun haline gelmiştir. "Spam" sözcüğü Amerika Birleşik Devletleri'nde Hormel Foods Corporation firmasınca üretilen gıdalara verilen "Spiced Pork And Ham" kelimelerinin baş harflerinin kısaltılmasıdır.[92] Dilimizde spam ifadesine denk bir Türkçe karşılık bulunamadığı görülmektedir.

Spam bir bülten veya haber grubu üzerinden ticari amaç taşımayan, bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklam olarak tanımlanabilir.[93] Spamlar genellikle e-posta yoluyla alıcılara gönderilmektedir. Spam göndericilerinin beslenme kaynağı spam gönderilecek e-posta adresleridir. Spam göndericisi ne kadar çok e-posta adresine

---

[89] Akbulut, Bilişim Alanında Suçlar, s. 77.
[90] Dülger, Bilişim Suçları, s.106.
[91] https://www.techtarget.com/searchsecurity/definition/hacker (Erişim Tarihi: 13.08.2022).
[92] Memiş, Tekin, "Hukuki Açıdan Kitlelere E-Posta Gönderilmesi", Erzincan Üniversitesi Hukuk Fakültesi Dergisi, C.5, S. 1-4 (2001), s. 432.
[93] Memiş, "Hukuki Açıdan Kitlelere E-Posta Gönderilmesi", s. 432.

sahipse o kadar çok kişiye ulaşabilir. Bu sebeple e-posta adresleri çeşitli yollarla alınıp satılabilen ticari değere dönüşmüştür. Spam göndericileri çeşitli yollarla e-posta adreslerini ele geçirebilmektedirler. E-posta yoluyla ücretsiz sitelere üye olunması, bazı spam göndericilerinin bu iş için satılan e-posta CD'lerini satın alması,[94] web sitelerinde dolaşıp e-posta toplayan robot yazılımlar[95] sayesinde e-postalar spam göndericilerine ulaştırılmaktadır.

Spam sorununun dünyada hızla artması ve gelişen bilişim teknolojilerinin verdiği zararla mücadele için ilk olarak ABD (federal düzeyde) ve Avusturya devamında da diğer birçok devlet spam konusunda kanunlarında düzenlemeler yapmak mecburiyetinde kalmıştır. Avusturya Telekomünikasyon Kanunu 101'inci maddesinde, spamın açık bir hükümle yasaklandığı görülür.[96] Türk Ceza Kanunu'nda istem dışı alınan elektronik postaları yasaklayan özel bir hüküm bulunmamaktadır. Ancak gönderilen istenmeyen elektronik postaların içeriğinde ceza mevzuatımızda suç kabul edilen bir eylem mevcut ise cezalandırılma koşulu sağlanacaktır. İçeriği reklam niteliğinde olan bir e-postanın kişilere gönderilebilmesinin yasal olabilmesi için e-posta sahibi kişinin rızasının alınmış olması gerekir.[97]

1.2.2.6. Salam Tekniği

Salam tekniği genellikle bankacılık alanında sıklıkla kullanılan bir yöntemdir. Fail bu tekniği kullanarak bilişim sistemleri ile hesaplanan bankacılık sektöründeki değerlerin çarpımları neticesinde bulunan çok basamaklı değerlerin virgülden sonra bir veya iki rakamını başka hesaba aktararak yuvarlar.[98] Yuvarlama sonucu çıkan rakam, failin belirlediği başka, üçüncü bir hesaba gönderilir. Bu sayede hesaplarda banka çalışanlarının ya da hesap sahiplerinin dahi fark edemeyeceği küçük değişiklikler olur. Bu yöntemle fail kendisine veya üçüncü bir kişi yararına hukuka aykırı olarak yarar sağlar. Bu teknik uygulanırken truva atı yazılımları da aracı olarak kullanılabilir.

Bu yöntemle çok sayıda hesaptan tek başına değersiz görünen çok az miktar alternatif başka bir hesaba aktarılarak toplamda yüklü miktarların toplanması amaçlanmaktadır.

---

[94] https://keremkoseoglu.wordpress.com/2005/04/30/e-posta-adresini-spammerlardan-saklayin/ (Erişim Tarihi: 13.08.2022).
[95] https://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar (Erişim Tarihi: 13.08.2022).
[96] Memiş, "Hukuki Açıdan Kitlelere E-Posta Gönderilmesi", s. 439.
[97] Ticari elektronik iletiler, alıcılara ancak önceden onayları alınmak kaydıyla gönderilebilir. Bu kurala aykırı davranılması durumunda Elektronik Ticaretin Düzenlenmesi Hakkında Kanun'un 12. maddesi gereğince bin Türk lirasından beş bin Türk lirasına kadar idari para cezası verilmektedir.
[98] Değirmenci, Bilişim Suçları, s. 84.

1.2.2.7. Bilgisayar Virüsleri

Günümüzde farklı şekillerde karşımıza çıkan bilgisayar virüslerinin en temel özelliği kendi kendini çoğaltma, kopyalama özelliğinin mevcut olmasıdır. Bilişim virüslerinin kopyalarını çeşitli yöntemler kullanarak diğer bilişim sistemlerine ulaştırması yazılımlara, dosyalara, sistemlere kendisini kopyalama işlemi virüs bulaşması olarak adlandırılmaktadır.[99]

Bu yazılımlara virüs denmesinin sebebi biyolojik virüsler gibi sisteme kendiliğinden bulaşıp, çoğalarak sistemi hasta etmesidir.[100]

Virüslerin aktif hale gelebilmesi için çalıştırılabilen programlara bulaşması gerekir. Bir bilgisayara virüs bulaşırsa o bilgisayarda virüsün bulaştığı program her çalıştırıldığında, virüste bilgisayar belleğine taşınacaktır. Çünkü virüsün amacı belleğe taşınarak bulunduğu sürücünün hafızasına bulaşmaktır. Virüs bir kez bilgisayara yerleştikten sonra sistemin her açılışında kendisini belleğe yüklemekte ve çalıştırılan her programa bulaşabilmektedir.

Bilişim virüsleri kendi içerisinde farklı türlere ayrılır. Bunlardan bazıları; sabit diske zarar verenler, genel amaçlı virüsler, kabuk tipi virüsler, kütük tipi virüsler, işletim sistemi virüsleri, komut işlemcisi virüsleri, özgün kaynak program virüsleri, çok amaçlı virüsler, bellekte duran virüslerdir.[101]

Bilgisayar virüslerinden korunmak, virüsü tespit ederek etkisiz hale getirmek için anti virüs programları kullanılmaktadır. Ancak bir anti virüs programının tüm virüs çeşitlerini engellediği söylenemez. Bu nedenle programın sık sık güncellenmesi yeni gelişen virüslere karşı güçlendirilmesi gerekmektedir.

1.2.2.8. Tavşanlar

Bilişim sistemlerinde sistem kaynaklarının süratle aralıksız çalışarak gereksiz işler yapması ve neticesinde de kaynakların azalarak tükenmesine neden olan zararlı bir yazılımdır. İsmini aldığı hayvan türü tavşan gibi hızla çoğalması ve kolonileşmesi en belirgin özelliğidir.

Oluşturduğu kolonide önce bir yavru koloni üreterek geliştirir, yavru koloni gelişimini tamamladığında yeni bir yavru koloni daha geliştirir ve bu şekilde bir döngüyle devam eder. Amaçlanan çok kullanıcılı sistemlerde ana sistemin bilgi işleme gücünü kaybettirip sistem kaynaklarını yok etmesini sağlamaktır.

---

[99] Akbulut, Bilişim Alanında Suçlar, s. 77.
[100] Yazıcıoğlu, Bilgisayar Suçları, s. 170.
[101] Akbulut, Bilişim Alanında Suçlar, s. 77.

Kullanıcı veri kütüklerinin sonuna eklenmeyen, asalak özelliklere sahip olmayan, kendi kendilerine yetebilip parazitlik özelliği yapmayan tavşanlar bu özellikleriyle bilişim virüslerinden ayrılmaktadır.[102] Tavşanlar, virüslerin yaptığı gibi bilgisayarların ana programlarını kullanılmaz hale getiremeyecek ve solucanlar gibi bilgisayar ağlarına ve sistemlere özel yetenekleriyle yetkisiz giremeyeceklerdir.[103]

1.2.2.9. Bukalemunlar

Truva atı programıyla oldukça benzer özellikler gösteren bukalemunlar bazı hile ve aldatma yollarıyla alışılmış, güvenilir bir programmış gibi davranarak sistemin içine girerler. Bu program kendisini saklamakta oldukça başarılı olduğundan bukalemun ismi verilmiştir.[104] Bukalemunlar bilgisayar ağlarına giriş iletilerini taklit edecek biçimde programlanmışlardır. Böylece sisteme giren başka kullanıcıların isimleri ile şifreleri gizli bir dosyada kayıt altına alınır ve daha sonra monitörde sistemin bakım için geçici bir süre kapatılacağına ilişkin uyarı mesajı verilir.[105] Bukalemunun yaratıcısı bu mesaj sonrası sistemin kapanmasıyla kendi yasa dışı amaçları için programlara dilediği gibi girip çıkarak istediği her eylemi gerçekleştirebilir.

1.2.2.10. Phishing Saldırıları

Phishing, bilişim tarihinin en eski ve en etkili saldırı türlerinden biridir. Günümüzde de oldukça popüler olan phishing, password (şifre) ile fishing (balık tutmak) kelimelerinin birleştirilmesiyle oluşmuş Türkçe karşılığı yemleme, oltalama olan bir saldırı çeşididir.

Phishing, genel olarak bir kişinin parolasını, banka hesabını veya kredi kartı bilgilerini öğrenmek amacıyla kullanılır. Fail tarafından resmi bir kurumdan geliyormuş gibi hazırlanan iletilerle mağdurların sahte internet sitelerine girmeleri hedeflenir. Bunun aracılığıyla kullanıcılardan kimlik bilgileri, kredi kartı numarası veya şifresi gibi bilgilerinin girilmesi talep edilerek kötü niyetli üçüncü şahıslarca bu bilgiler ele geçirilmeye çalışılır. Phishing saldırıları en çok telefon mesajı, e-posta veya sosyal ağlar vasıtasıyla gönderilen linkler vasıtasıyla gerçekleştirilmektedir. Son zamanlarda avukatları hedef alan bir oltalama saldırısı dikkat çekmektedir. Türkiye Barolar Birliğince oluşturulan UHAP internet sitesinin linkine oldukça

[102] Aydın, Bilişim Suçları, s. 53.
[103] Canbek/Sağıroğlu, "Kötücül ve Casus Yazılımlar", s. 132.
[104] Dülger, Bilişim Suçları, s. 111.
[105] Aydın, Bilişim Suçları, s. 51.

benzeyen bir web adresi kullanan bilişim suçu failleri avukatlara gönderdikleri mesaj ve maillerde UHAP şifrelerini güncellemelerini isteyerek mailin sonundaki yönlendirme linkine tıklamalarını sağlayarak şifre ve kişisel bilgilerini elde etmeye çalışmışlardır. Yine oldukça yaygın kullanılan sosyal medya hesaplarına gönderilen ve kişinin hakkında şikâyet olduğu, içeriğinin kötü olduğuna dair mesajlar ve sahte şikâyete dair ekran görüntüleriyle şikâyetin kaldırılması için gönderilen linke girilmesi istenilmektedir. Hakkındaki kötü içerikleri kaldırmak isteyerek yönlendirilen linke giriş yapan kişinin sosyal medya hesapları hackerlar tarafından ele geçirilip, erişimlerinin engellendiği görülür. Bu gibi saldırıları gerçekleştiren bilişim korsanları 5237 sayılı TCK kapsamında suç oluşturan eyleme göre cezalandırılabilmektedir. Günümüzde gittikçe yaygınlaşan phishing saldırılarının mağduru olmamak için dikkat edilmesi gereken en temel unsur gönderilen bağlantı linklerindeki adresleri kontrol etmek olacaktır. Site içeriklerini neredeyse birebir kopyalayan failler web adreslerini gerçek adrese oldukça benzetseler de dikkatli kullanıcılar tarafından fark edilebilmektedir. Yine yönlendirilen link aracılığıyla istenilen kullanıcı adı ve şifre bilgilerinin girilmemesi bu noktada oldukça önemlidir.

İKİNCİ BÖLÜM

ULUSLARARASI ALANDA BİLİŞİM SUÇLARINA İLİŞKİN ÇALIŞMALAR VE KARŞILAŞTIRMALI HUKUKTA BİLİŞİM SUÇLARI

2.1. Uluslararası Alanda Bilişim Suçlarına İlişkin Çalışmalar

Teknolojinin gelişmesi, bilgisayarların, akıllı telefonların, tabletlerin hayatımızın hemen hemen her alanına girmesi, hayatımızı kolaylaştırıp daha hızlı, daha kolay sonuca ulaşma imkânı sağlamıştır. Ancak bu gelişmeler kötü niyetli kişiler tarafından dijital ortamların güvenilirliğini sarsacak şekilde kullanılmaktadır. Bilişim teknolojilerinin sürekli güncellenmesi ülkelerin bilişim suçları ile iç hukuk kapsamında mücadelelerinin zamanla yetersiz kalmasına sebep olarak bu mücadelenin uluslararası, sınır ötesi bir boyutta yapılması ihtiyacını doğurmuştur. "Uluslararası boyut", "ulus ötesi boyut" veya "küresel boyut" gibi kullanılan tüm ifadelerden de anlaşılacağı üzere bilişim suçları evrensel olarak algılanmaktadır. Devletler bilişim suçlarıyla mücadele etmek amacıyla maddi ceza ve usul hukuklarına kurallar getirmektedir. Her ülkenin kendi iç hukukunda bilişim suçlarına karşı aldığı önlemler elbette kritik öneme sahip olacaktır ancak dünya çapındaki bu zorluğun üstesinden gelmek için yeterli olmayacağı değerlendirilmektedir. Bilişim alanında işlenen suçlarla mücadelenin etkili olabilmesi için devletlerin tek başına hareket etmeyerek ortak bir yönde ilerlemeleri gereklidir. Uluslararası örgütlerin ülkeleri için büyük bir tehdit olarak gördüğü bilişim suçlarının bir nebze de olsa önüne geçebilmek adına bazı çalışmalar yaptığı bunların sonucunda da aldıkları tavsiye kararlarını ve suçlarla mücadele kapsamında ilkeleri yayınlayarak tüm dünya ile paylaştıkları görülmektedir. Dünya için oldukça tehlike teşkil eden bilişim suçları, çok uluslu topluluklar tarafından da dikkate alınmış, bu kapsamda bilişim suçları ile mücadele edebilmek için iş birlikleri düzenlenmiştir.

2.1.1. Ekonomik İşbirliği ve Kalkınma Örgütü (OECD)

14 Aralık 1960 tarihli Paris Sözleşmesi'ne istinaden, 1961 yılında kurulan Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) ile üye ülkeler arasında iş birliğinin güçlendirilmesi, ekonomi politikalarının genişlemesi, işsizliğin yok olması, küresel sorunlara çözüm bulunması amaçlanmaktadır. Üyesi bulunan otuz sekiz ülkeden otuzu Dünya Bankası tarafından yüksek

gelirli ülkeler listesinde gösterilmiştir.[106] OECD üyesi ülkeler, ekonomik ve sosyal politikaları tartışmak, geliştirmek ve mevcut durumu iyileştirmek amacıyla deneyimlerini paylaşarak küreselleşen dünyada ortak sorunlara yerel ve uluslararası çözümler sunmaktadır.

1983 yılında OECD bünyesinde uzman bir komite kurulmuştur. Bilişim ve ceza hukuku arasındaki ilişkiyi tartışmak üzere görevlendirilen bu komitenin 1983 ve 1985 yılları arasında Avrupa ülkelerinin bilişim suçlarına ilişkin ceza mevzuatlarını uyumlu hale getirmek için çalıştığı bilinmektedir.[107] Bu sayede bilişim suçlarının uluslararası alanda ceza kanunlarındaki uyumlaştırma sürecinin de ilk defa OECD ülkelerinde başladığı görülür.[108] Komitenin hazırladığı ilk rapor olan "*Computer-Related Crime: Analysis of Legal Policy*" ile bilgisayar aracılığıyla gerçekleştirilen suçlar karşısında ülkelere uygulayacakları cezai müeyyidelere yönelik önerilerde bulunulmuştur.[109] Raporda bilişim suçlarına ilişkin;

1- Bilgisayar verilerinin veya bilgisayar programlarının hukuka aykırı bir şekilde aktarılması amacıyla kasıtlı olarak girilmesi, değiştirilmesi, silinmesi veya bastırılması,

2- Bilgisayar verilerinde veya bilgisayar programlarında sahtecilik yapılması,

3- Bir bilgisayarın veya telekomünikasyon sisteminin işleyişini engellemek amacıyla kasten programlarında veya bilgisayar sistemlerinde değişiklik yapılması,

4- Korunan bir bilgisayar programının üzerinde hak sahibi olan kişinin hakkının ihlali ve telif haklarına aykırı olarak programı ticari olarak sömürülmesi,

5- Bilgisayar veya telekomünikasyon sisteminin yetkisiz kişilerce kötü niyetli olarak zarara uğratılması durumlarıyla karşılaşan üye ülkelere failleri cezalandırmaları tavsiye edilmiştir.[110]

1986 tarihli bu rapor Avrupa Konseyi tarafından da referans alınmıştır.

26 Kasım 1992 tarihinde komite tarafından üye ülkelere tavsiye niteliğinde Bilgi Sistemleri Güvenliği Tavsiye Yönergesi hazırlanmıştır. Kamu ve özel sektörü ilgilendiren bu raporun bilgi sistemlerinin güvenliğine ilişkin ülkeler arası karşılıklı yardımlaşma gibi bilgi sistemlerinde minimum standartların uygulanması konusu üzerinde ayrıca durduğu görülmektedir. "Bilişim Sistemleri Güvenliği İçin OECD İlkeleri" isimli bu yönerge 2002 yılında yenilenmiştir.[111]

---

[106] https://tr.wikipedia.org/wiki/OECD (Erişim Tarihi: 03.02.2022).
[107] Goodman, Cybercrime, s. 326.
[108] Değirmenci, Olgun, "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", Legal Hukuk Dergisi, C. 1, S. 11 (2003) s. 2751.
[109]https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm (ErişimTarihi:24.02.2022).
[110] Goodman, Cybercrime, s. 327.
[111] Detaylı bilgi için bkz: https://www.oecd.org/sti/ieconomy/32493366.PDF (Erişim Tarihi: 24.02.2022).

2.1.2. Birleşmiş Milletler

Birleşmiş Milletler bilişim teknolojilerinin dünyada yaygınlaşması ve gelişmesiyle birlikte bilişim suçlarının önlenmesi amacıyla uluslararası alanda etkili çalışmalar yapma ihtiyacı hissetmiş ve çözüm arayışlarına girmiştir. Bu kapsamda 1985 yılında yapılan ilk faaliyet "*7. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresi*" dir. Kongrenin hemen ardından ortaya çıkan Milan Eylem Planı'nın 42'nci ile 44'üncü paragrafları arasında klasik mağdur tiplerinin dışında yeni mağdur şekillerinin meydana geldiği, bilgisayar suçlarının buna örnek oluşturan mağduriyetlerden olduğu tartışılmıştır. Aslında bu eylem planının arka planında açıklanan tavsiye kararlarına uygun olarak hukuki güvenliği sağlamak için ülkelere harekete geçme çağrısında bulunulduğu söylenebilir. 1985 yılındaki çalışmanın ardından Birleşmiş Milletler, bilişim suçlarının ortaya çıkardığı uluslararası yasal zorluklarla mücadele amacıyla Havana'da 1990 yılında "*BM 8. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresi*" düzenlemiştir. Kongre sonrası yayımlanan raporda üye devletlere mevzuatlarındaki ceza kanunlarını gelişen teknolojik suçlarla uyumlaştırıp gerektiğinde yeni kanunlar ve prosedürler oluşturarak bilişim suçlarıyla mücadele çabalarını artırmaları tavsiye edilmiştir.[112]

Birleşmiş Milletler bünyesinde 1997'de Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) kurulmuş, bu oluşum ulusal yapılarla koalisyon kurup faaliyetlerini destekleyerek bilişim suçlarına karşı eylemliliği hedeflemiştir.[113] Bilişim suçlarına ilişkin verileri toplama, araştırma ve analiz konularında teknik yardım sağlamak uzmanlık alanları içinde sayılabilir.

Birleşmiş Milletler'in bilişim suçlarına oldukça önem verdiği görülmektedir. Uluslararası alanda maddi hukukun uyumlaştırılması ve yargısal bir temelin oluşturulması da dahil olmak üzere başka faaliyetlerin de üstlenilebileceğini belirtmiştir. BM her ülkenin farklı hukuk sistemlerinin uyumlu hale getirilerek ortak bir çerçeve oluşturulması, uluslararası iş birliği ve karşılıklı yardımlaşmalarla karşılaşılan sorunların üstesinden gelmek için birleşik, yasal olarak bağlayıcı bir belgenin önemini vurgulamaktadır.[114] İtalya'da 14 Aralık 2000 tarihinde düzenlenen *"Sınırlar Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi Sempozyumu'*nda üye devletlerin belirlenen eylemlerle karşılaşması durumunda iç hukuklarında cezai müeyyideye yer vermeleri tavsiye edilmiştir. Müeyyideye tabi eylemleri de bilişim sistemlerine yetkisiz giriş, bilişim sistemlerindeki verilerin yok edilmesi veya

[112]https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf (Erişim Tarihi: 07.03.2022).
[113] https://www.unodc.org/unodc/en/cybercrime/index.html (Erişim Tarihi: 09.03.2022).
[114] Goodman, Cybercrime, s. 327.

değiştirilmesi, bilişim ya da bilişim sistemlerinin hukuka uygun kullanımının engellenmesi, gayri fiziki ekonomik değer taşıyan objelerin çalınması, aldatma yoluyla değer elde edilmesi şeklinde belirlemiştir.[115]

Birleşmiş Milletler Genel Kurulu'nun 45/121 (1990) sayılı kararı bilgisayar suçlarına ilişkin olup, bu karara dayanılarak 1994 yılında "*Uluslararası Suç Politikası İncelemesi: Bilgisayarla İlgili Suçların Önlenmesi ve Kontrolüne İlişkin Birleşmiş Milletler El Kitabı"* yayımlanmış ve bununla bilgisayarla ilgili suçlar sorununa dair uygun bir açıklama yapılarak üye ülkelere daha fazla uluslararası iş birliği yapmaları çağrısında bulunulmuştur.[116]

Birleşmiş Milletler'in bilişim suçları konusunda uluslararası geçerli bir sistem oluşturma fikrinin yalnızca bir ön fikir olarak kaldığı, uygulamada yeterince başarılı olamadığı söylenebilir. BM'nin üye ülke sayısının fazlalığı ve üye ülkelerin farklı hukuk sistemlerinin bulunması herkes için geçerli bir anlaşma yapılmasına engel olmaktadır.

2.1.3. Sekizli Grup (G8)

1975 yılından beri her yıl ekonomi grup toplantıları düzenleyen sekizli grup önceleri Fransa, Almanya, İtalya, ABD, Birleşik Krallık ve Japonya'dan oluşmaktaydı. Daha sonra 1976 yılında Kanada'nın ve 1997 yılında Rusya'nın katılımıyla G8 olarak anılmaya başlamıştır. Bu topluluğun, bilişim suçlarının küresel boyuta ulaşması ve bilişim suçu mağdurlarının oldukça büyük ekonomik zararlar görme tehlikesinin doğmasıyla bilişim suçlarıyla mücadelede uluslararası iş birliği konusunu gündeme getirerek çalışmalar yaptıkları görülmektedir. 1990'lı yılların ortalarından bu yana, bilişim suçlarıyla ilgili çalışma gruplarının eylem planları hazırladıkları görülmektedir.

1995'te Kanada'da toplanan, Halifax Zirvesi'nde topluluğa üye devletlerin ciddi suçlardan elde edilen gelirlerin aklanmasının engellenmesi amacıyla etkili önlemler alınması ayrıca uluslararası organize suçlarla mücadelede üyelerin taahhütlerini yerine getirmesi gerektiği ifade edilmiştir. Bu ifade dolaylı olarak bilişim suçlarıyla mücadeleyi kastetmektedir. Ayrıca bir "Lyon Grubu" yani "Organize Suçlar Kıdemli Uzmanlar Grubu" nun oluşturulması kararı alınmıştır. Lyon grubu Fransa'da aynı yıl bir toplantı gerçekleştirmiş ve toplantı sonunda 40 maddelik "*Uluslararası Organize Suçlarla Verimli Bir Şekilde Mücadele Etmek İçin*

[115] Eker, Umut, "Türk Ceza Hukuku'nda Bilişim Suçları Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu", Türkiye Barolar Birliği Dergisi, C. 19, S. 62 (Ocak 2006), s. 110.

[116] Önok, Rıfat 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. 1238-1239.

Tavsiyeler" raporunu yayımlamıştır. Bu raporla üye ülkelere bilişim suçlarına ilişkin iç hukuklarında cezai müeyyide düzenlemeleri konusunda çağrıda bulunulmuştur. Ayrıca tavsiye kararında üye devletlerin bilişim suçlarına ilişkin uluslararası iş birliklerini artırmaları gereksinimi de açıklanmıştır. Japonya'da düzenlenen Okinava Zirvesi'nde "*Okinava Küresel Bilgi Toplumu Bildirisi"* açıklanmış, bu bildiriyle uluslararası iş birliği ve bilişim suçlarında uyumlaştırılma ilkesi benimsenerek G8 üyesi ülkelere Avrupa Konseyi Siber Suçlar Sözleşmesi'ne taraf olmaları yönünde tavsiyelerde bulunulmuştur.[117]

1997'de Rusya'nın üyeliğinden önce G7 bünyesinde "İleri Teknoloji Suçları Alt Komisyonu" kurulmuştur. Bu alt komisyonla amaçlanan soruşturma, kovuşturma işlemlerini kolaylaştırmak ayrıca bilişim suçlarına ilişkin dijital delillerin ele geçirilip güvenle saklanabilmesini sağlamaktır. Bu amaca uygun olarak 7 gün 24 saat hizmet veren bir bilişim suçları ağı, iletişim grubu kurulmuştur.

Washington' da toplanan G8 iç ve dışişleri bakanları "İleri Teknoloji Suçları"'nı tartışmış sonuçta "*10 Prensip ve 10 Noktada Eylem Planı*" üzerine mutabakat sağlanmıştır.

"Buna göre;

a-) Telekomünikasyon ve bilgisayar sistemlerine yapılan ihlallerin cezai müeyyide ile karşılanması hususunda üye ülkelerin hukuk sistemlerinin gözden geçirilmesi ve ileri teknoloji suçlarının araştırılmasının geliştirilmesine yardımcı olmak,

b-) İleri teknoloji suçlarıyla artan hususların karşılıklı yardım anlaşmalarının ve düzenlemelerin yapılması sırasında göz önünde bulundurulması,

c-) Ülkesel bazda yerleri tespit edilemeyen verilerin bilgisayar yolu ile araştırılması ve sınırlar ötesi araştırma; karşılıklı yardım için yerine getirilmesi önerilen delillerin muhafaza edilmesi hususlarında, uygulanabilir çözümlerin geliştirilmesi ve incelenmesinin devam edilmesi,

d-) Kritik delillerin saklanması ve korunması yoluyla ileri teknoloji suçlarıyla savaşma hususunda sarf edilen çabanın azaltılmaması için özel sektörle birlikte çalışarak yeni teknolojilerin sağlanması."[118] ilkeleri bildirilmiştir.

Sekizli gruptaki üye ülkelerin bilişim alanındaki suçlarla mücadele ve önlem almaya yönelik bu çalışmalarının temelinde bilişim suçlarının ileri zamanlarda gittikçe artarak daha önemli neticelere sebep olabileceği ve üye ülkelerin de bu durumdan dünyada en çok etkilenecek ülkeler olacağı yönündeki düşünceleri yer almaktadır.

2.1.4. Amerikan Devletleri Örgütü

[117] https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html (Erişim Tarihi: 11.03.2022).
[118] Yaycı, Esra, "Bilişim Suçları", (Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuk Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi), Ankara, 2007, s. 38-39.

Otuz beş üye devlete sahip Amerikan Devletleri Örgütü (OAS)'nün de diğer uluslararası kuruluşlar gibi bilişim suçları konusunda oldukça endişeli oldukları görülür. Amerikan Devletleri Örgütü, Adalet Bakanları veya Amerika Kıtası Bakanları ya da Başsavcılar aracılığıyla düzenlenmiş sağlam bir yasal çerçevenin bilişim suçlarıyla mücadelede merkezi bir rol aldığını uzun zamandır kabul etmektedir. Topluluk üye devletlerine uluslararası iş birliğini mümkün kılma amacıyla bilişim suçları kanunlarını uyumlu hale getirme önerisinde bulunmuştur. Bu kapsamda örgüt üyelerine 1999 yılında bilişim suçları konusunda Devlet Uzmanları Grubu'nun (Uzmanlar Grubu) oluşturulmasını tavsiye etmiştir. Uzmanlar Grubu, bilişim suçlarını analiz etme, yerel bilişim suç kanunlarını inceleme ve bilişim suçlarıyla mücadelede Amerikalılar arasında sistemde iş birliği yapma amaçlarını taşır. Topluluğun 2003 yılında dördüncü genel kurulda "*Bilişim Güvenliğine Yönelik Tehditlere Karşı Mücadelede Amerikan Ülkeleri Stratejis*i" konulu kararı imzalayarak bilişim suçu tehditlerine karşı ortak bir mücadele stratejisi belirledikleri görülmektedir.

2.1.5. İngiliz Milletler Topluluğu (Commonwealth)

Geçmişte Britanya İmparatorluğu'na ait otuz yedi ülke ile günümüzde Birleşik Krallık'ın parçası olan on altı ülkenin oluşturduğu uluslararası bir topluluk olan İngiliz Milletler Topluluğu genelde Milletler Topluluğu adıyla ifade edilmektedir.[119]

Milletler Topluluğu Sekreterliği Ekim 2002'de "*Bilgisayar ve Bilgisayarla İlgili Suçlara İlişkin Model Kanunu*" hazırlamıştır. Bu Kanun topluluğun bilişim alanında suçlara ilişkin en mühim düzenlemesidir. Milletler topluluğu elli üç üye ülkesiyle Model Kanun'la geniş bir etkiye sahiptir. Bilgisayar ve Bilgisayarla İlgili Suçlara İlişkin Model Kanun, Avrupa Konseyi Siber Suç Sözleşmesi'nin esasını oluşturan yasa dışı erişim, verilere müdahale etme, bilgisayar sistemlerine müdahale etme, verilere yasa dışı müdahale, yasa dışı veriler ve çocuk pornografisi suçlarını kapsamaktadır.[120]

Bilgisayar ve Bilgisayarla İlgili Suçlara İlişkin Model Kanun ile Avrupa Konseyi Siber Suç Sözleşmesi kıyaslandığında, verilere müdahale, bilgisayar sistemlerine müdahale ve yasa dışı aygıtların kullanılması suçlarına ilişkin cezai sorumluluğun Model Kanun'da daha geniş

[119] https://tr.wikipedia.org/wiki/%C4%B0ngiliz_Milletler_Toplulu%C4%9Fu (Erişim Tarihi: 14.03.2022).
[120]https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf (Erişim Tarihi: 17.03.2022).

düzenlendiği görülür.

Milletler Topluluğu, bünyesinde oluşturduğu "Bilişim Suçları Girişimi" (Commonwealth Cybercrime Initiative- CCI) teşkilatlanmasıyla bilişim ve bilişim sistemlerinin güvenliklerine ilişkin üye devletlere hizmet etmektedir.[121]

2.1.6. İnterpol

Birleşmiş Milletlerden sonra gelen, dünyanın ikinci büyük uluslararası örgütü olarak 1923 yılında Uluslararası Kriminal Polis Teşkilatı kurulmuştur. Günümüzde 190 üyesi bulunan İnterpol, bilişim suçlarıyla uluslararası mücadelede profesyonel çabalar göstermektedir. Teşkilatın siber güvenlik koruması ve siber suçları önleme alanına oldukça önem verdiği görülmektedir. İnterpol, üye devletlere yönelik bilişim suç tehditlerini minimuma indirmek amacıyla kolluk kuvvetleriyle eş güdümlü operasyonlar gerçekleştirme, verilerin güvenli paylaşım platformlarını oluşturma, eğitim ve analiz gibi faaliyetlerde bulunmaktadır.[122]

İnterpol bünyesinde Siber Suç İşbirliği Operasyonu (CCP) kurulmuştur. Bu operasyonla hedeflenen platforma üye ülkelerin bilişim suçu tehditlerini ve suç eğilimlerini görerek mücadeleye daha iyi odaklanmaları, tekrarlanan bilişim suçu tehditlerine karşı daha az çaba göstermelerini sağlamaktır. Platforma erişim kısıtlı olup bu durum üyelerin güvenli bir ortamda bilişim suçlarına ilişkin istihbarat paylaşmasına olanak sağlamaktadır.

2.1.7. Avrupa Konseyi

2.1.7.1. Bilişim Suçlarına İlişin Avrupa Konseyi Çalışmaları

Avrupa Konseyi; 1949 yılında kurulmuş, demokrasi, insan haklarına saygı ve hukukun üstünlüğünü Avrupa çapındaki hükümetler arasında savunan, bünyesinde Avrupa İnsan Hakları Mahkemesi'ni barındıran bir kuruluştur. Avrupa Konseyi'nce yürütülen çalışmalar neticesinde sözleşme ve protokoller hazırlanarak Konseye üye devletlerin iç hukuklarında mevzuatlarını uyumlu hale getirmesi, genel çerçevede Avrupa'da ortak bir hukuk düzeni kurulması hedeflenmektedir. 13 Nisan 1950'de Türkiye Avrupa Konseyi üyesi olmuştur.

---

[121] CCI'a ilişkin haberler için bkz: https://thecommonwealth.org/news/commonwealth-cybercrime-experts-barbados-call-robust-cybersecurity (Erişim Tarihi: 17.03.2022).
[122] https://www.interpol.int/Crimes/Cybercrime (Erişim Tarihi: 17.03.2022).

Elektronik bilgi bankaları tarafından işlenen verilerin kişilerin özel hayatının korunması kapsamında işlenebilmesi amacıyla 1970'li yıllarda Avrupa Konseyi Bakanlar Komitesi iki adet tavsiye kararı almıştır.[123] Dünyada büyük bir hızla gelişen haberleşme sistemleri kişilerin özel hayatına ilişkin verilerin muhafazasına dair Avrupa Konseyi üyesi ülkeler arasında uluslararası bir sözleşme ihtiyacı doğurmuştur. 28 Ocak 1981'de "*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına İlişkin 108 Sayılı Sözleşme*" hem Avrupa Konseyi'ne üye devletler hem de Türkiye tarafından imza altına alınmıştır. Bu sözleşme ile sözleşmeye taraf devletlerin iç hukuk düzenlemelerinin uyumlaştırılması ve veri akış serbestisi sağlanması amaçlanmıştır.[124]

Avrupa Konseyi'nin, bilişim suçlarının ülkeler üzerindeki uluslararası kaygısıyla 1980'lerin başından beri mücadele çabasında olduğu görülmektedir. Bilişim suçlarına ilişkin ilk çalışmalarını, bünyesinde kurulan Uzmanlar Komitesi vasıtasıyla yürütmüştür. 1985-1989 tarihleri arasında faaliyet gösteren komite, üye ülkelere karşılaştıkları eylemlerden hangilerinin iç hukuklarında bilişim suçu kapsamında değerlendirilerek müeyyideye bağlanması gerektiği konularında yol göstericidir.[125]

OECD'nin 1986 yılında düzenlediği "*Computer –Related Crime - Analysis of Legal Policy*" adlı raporu Avrupa Konseyi Uzmanlar Komitesi'nce esas alınarak yeni bir rapor düzenlenmiştir. Raporda, OECD'nin hazırladığı raporda belirtilen üye ülkelerin iç hukuklarında müeyyideye bağlanması tavsiye edilen ihlallerin Avrupa Konseyi'nce de benimsendiği ayrıca bilişim suçlarına ilişkin bu raporda yer almayan başka suç tiplerinin de kabul edildiği görülmektedir.

Avrupa Konseyi 1989 ve 1995 yıllarında bilişim suçlarının zorluklarıyla mücadele amacıyla hükümetlere kanunlarında yenilikler getirmelerini teşvik eden iki tavsiye kararı yayımlamıştır. Avrupa Konseyi Uzmanlar Komitesi, Avrupa Suç Sorunları Komitesi ile birlikte 13 Eylül 1989'da kabul edilen 89(9) sayılı Tavsiye Kararı'nı hazırlamıştır. Bu tavsiyede bilişim suçlarının yeni ortaya çıkan zorluklarına hızlı ve yeterli yanıt verilmesinin önemi vurgulanarak, kanunların ve uygulamaların uyumlaştırılması ile uluslararası yasal iş birliğinin geliştirilmesi gerekliliğinden bahsedilmiştir.[126] Ayrıca, bilgisayarla ilgili belirli eylemlerin suç haline getirilmesinde uluslararası mutabakata duyulan ihtiyacın altı çizilmiştir. 1995 yılında, Avrupa Konseyi bilişim suçlarıyla ilgili ikinci R (95)13 sayılı Tavsiye Kararı'nı kabul etmiştir. Bu rapor

[123] Değirmenci, "Bilişim Suçları Alanında Yapılan Çalışmalar", s. 2751.
[124] Sarıusta, Kader,"Kişisel Verilerin Ceza Hukuku Yoluyla Korunması", (Gaziantep Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana bilim Dalı Yayımlanmamış Yüksek Lisans Tezi), Gaziantep, 2018, s.62.
[125] Dülger, Bilişim Suçları, s. 199.
[126] https://rm.coe.int/09000016804f1094 (Erişim Tarihi: 20.03.2022).

konseye üye devletlere bilgi teknolojisi alanında rehberlik edebilecek esas olarak ceza muhakemesi hukuku meseleleri olan arama ve el koyma, teknik gözetim gibi ayrıntılı ilkeler sunmuştur.[127]

2.1.7.2. Avrupa Konseyi Siber Suç Sözleşmesi

Avrupa Konseyi Avrupa Suç Sorunları Komitesi tarafından 4 Şubat 1997'de Siber-Uzay Suçları Uzmanlar Komitesi kurulmuştur.[128] Konsey, yeni oluşturulan bu komiteden 89(9) ve (95)13 Tavsiye Kararları doğrultusunda bilgi teknolojisi ile bağlantılı ceza hukuku sorunlarını incelemesini istemiştir. Komitenin çalışmaları küresel bilişim suçlarıyla mücadelede ileriye doğru en temel adımları oluşturmaktadır.

23 Kasım 2001'de, Avrupa Konseyi'ne üye ülkelerle üye olmayan dört ülke; Kanada, Japonya, Güney Afrika ve Amerika Birleşik Devletleri'nin katılımıyla Macaristan'ın başkenti Budapeşte'de düzenlenen bir toplantıda bilişim suçlarına ilişkin ilk bağlayıcı, çok taraflı sözleşme imzaya açılmıştır. Otuz bir ülke tarafından imzaya açıldığı gün kabul edilen bu sözleşmeyi imzalayarak taraf olan devletlerin sözleşmedeki genel ilkeler doğrultusunda kendi iç hukuk mevzuatlarında düzenleme yapmaları gerekmektedir. Tüm bu prosedürler tamamlandıktan sonra 1 Temmuz 2004 tarihinde Avrupa Konseyi Siber Suç Sözleşmesi yürürlüğe girmiştir. Türkiye 2010'da sözleşmeyi imzalamış, ancak TBMM Dışişleri Komisyonu sözleşmeye dair raporu imzadan neredeyse iki sene sonra 20.12.2012 tarihinde TBMM'ye sunmuştur. Sözleşmede düzenlenen genel ilkelerin iç hukukumuzdaki düzenlemelerinin yapılması 02.05.2014 tarihini bulmuş sonuç olarak "*Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun*" olarak Resmi Gazete'de yayımlanmasıyla bağlayıcılık kazanmıştır. Sözleşmenin bugüne kadar toplam elli altı ülke tarafından kabul edildiği genel ilke düzenlemelerinin yapılarak, yürürlüğe girdiği ve bağlayıcılığı bulunduğu bilinmektedir.[129]

Öncelikle sözleşmeyle hedeflenenin uygun mevzuatın kabul edilmesi ve uluslararası iş birliğinin teşvik edilmesi yoluyla toplumun bilişim suçlarına karşı korunmasını amaçlayan ortak bir suç politikası izlemek olduğu söylenebilir.[130] Sözleşmenin üç temel amacı bulunur.

---

[127]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 (Erişim Tarihi: 20.03.2022).
[128] İçel, "Avrupa Siber Suç Politikasının Ana İlkeleri", s. 5.
[129] Dülger, Bilişim Suçları, s. 200.
[130] Erdoğan, Yavuz, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri, İstanbul, Legal Yayıncılık, 2018, s. 26.

Bunlar; *"(1) Siber suçlar alanında ülkelerin maddi ceza hukuku bölümlerini uyumlu duruma getirmek, (2) Bu suçların ve bilgisayar kullanılarak işlenen diğer suçların soruşturulması ve kovuşturulması için ceza yargılaması hukuku alanında gerekli yerel yetkileri sağlamak, (3) Bu bağlamda hızlı ve etkin bir uluslararası iş birliği rejimi oluşturmak"*[131] olarak sıralanabilir.

Avrupa Siber Suç Sözleşmesi dört bölüme ayrılmış kırk sekiz maddeden oluşmaktadır. Birinci bölümde sözleşmede yer alan terimlerin kullanımı açıklanmıştır. İkinci bölümde ulusal düzeyde alınması gereken önlemlerin neler olduğu düzenlenmiş, üçüncü bölümde uluslararası iş birliklerine yer verilmiş ve dördüncü bölümde de son hükümlerle sözleşmenin uygulamasındaki usulü ve teknik hükümlere yer verilerek sözleşme tamamlanmıştır.

Sözleşmede kullanılan siber suç kavramının tanımı yapılmamış ancak siber suç kapsamında değerlendirilebilecek suçlar sözleşmenin ikinci bölümünde ikinci ile onuncu maddeleri arasında tek tek sayılmıştır. Taraf devletlerin sözleşmede yer alan maddi ceza hukukuna ilişkin düzenlemeleri iç hukuklarında uyumlaştırırken sözleşme hükümlerini tam tercümeyle kabul etmeleri mecburi olmamakta bu hususta düzenleme yapmaları yeterli görülmektedir.

Sözleşmenin maddi ceza hukukunu düzenleyen birinci kısmında yer verilen ilk başlığın "*Bilgisayar Veri ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Karşı Suçlar*" olduğu görülmektedir.[132] Bu başlığın içerisinde beş madde ile suçlar düzenlenmiştir. Bunlar; hukuka aykırı erişim, hukuka aykırı müdahale, verilere müdahale, bilişim sistemine müdahale ve cihazların kötüye kullanımı suçlarıdır. "*Bilgisayarlarla Bağlantılı Suçlar*" adlı ikinci başlıkta, bilgisayarla ilgili sahtecilik eylemleri ve bilgisayarla bağlantılı dolandırıcılık eylemleri düzenlenmiştir. Sözleşme'de çocuk pornografisi hususuna ayrıca önem verilmesi dolayısıyla "*İçerikle İlgili Suçlar*" başlığında bu suçlara ilişkin düzenlemelere yer verildiği görülmektedir. Son olarak dördüncü başlık ile telif hakları ve benzer hakların ihlali ile ilgili suçlar düzenlenmiştir.

Sözleşmede yer alan ve tez çalışmamızın konusunu ilgilendiren maddeler ileriki bölümlerde anlatılacağından bu başlıkta tekrar değinilmeyecektir.

2.2. Karşılaştırmalı Hukukta Bilişim Suçları

[131] İçel, "Avrupa Siber Suç Politikasının Ana İlkeleri", s. 6.
[132] ASSS'nin orijinal metni için bkz: Convention on Cybercrime; https://rm.coe.int/1680081561 (Erişim Tarihi: 05.05.2022).

2.2.1. Amerika

Bilişim teknolojilerinin dünyada ortaya çıktığı ve yayıldığı yer olarak kabul edebileceğimiz Amerika'da ülke ekonomisinde bilişim sektörlerinin yeri bir hayli fazla yer kaplamaktadır. Ekonomideki etkisinin bu denli büyük olması da beraberinde sistem güvenliklerinin sağlanması hususunda çeşitli önlemler alınması, çalışmalar yapılmasını gerektirmiştir. Amerika, bilişim sistemlerine yetkisiz olarak girişin müeyyideye bağlandığı ilk ülke unvanına sahiptir.[133] Dünyanın en büyük teknoloji şirketlerini barındıran Amerika'da internetin ve bilişim sistemlerinin güvenilirliği ekonomik istikrar ve güvenlik için oldukça önem arz etmektedir. Bu nedenle Amerika Birleşik Devletleri'nde hem federal hem de eyalet düzeylerinde bilişim suçlarını izlemek, tespit etmek, önlemek, hafifletmek için makul güvenlik tedbirleri düzenlemeleri yapılmıştır.[134] Bilişim suçlarıyla mücadeleye ciddi ölçüde önem veren Amerika uluslararası alanda da bu suçun tehditlerinin farkındalığıyla AKSS'nin imzaya açılmasıyla Avrupa Konseyi'ne üye ülkeler içerisinde olmamasına rağmen aynı gün imzalayarak taraf olmuş, iç hukuk düzenlemelerini de tamamlayarak bağlayıcılık kazandırmıştır.

Amerika'da ilk başlarda eyaletler düzeyinde başlayan bilişim suçları ve sistem güvenliğine ilişkin düzenlemeler daha sonraları federal düzeyde yapılmaya başlanmıştır. Amerika'nın bilişim suçlarına ilişkin düzenlemelere genellikle ayrı bir kanun olarak yer verdiği görülmektedir. "*Bilgisayar Sahtekârlığı ve Kötüye Kullanılması Yasası*" yani "*Computer Fraud and Abuse Act (CFAA)*" 1984 yılında tüm ülke çapında yürürlüğe giren ilk düzenleme olmuştur.[135] Bu Kanun'da bilgisayarlara yetkisiz erişimle ilgili eylemlerin düzenlendiği görülmektedir. Hükümet tarafından ulusal güvenlik amacıyla kısıtlanmış verileri elde etmek için yetkisiz olarak kasten bir bilgisayara erişilmesi, bir finans kurumundan, tüketici raporlama kurumundan, federal hükümetten veya korumalı bir bilgisayardan belirli bilgileri almak için yetkisiz olarak bir bilgisayara kasıtlı olarak erişilmesi ve bir devlet bilgisayarına kasten erişilerek bu bilgisayarın kullanımının etkilemesi bu düzenlemede yer alan eylemlerdendir.[136] Ayrıca dolandırıcılık ve hukuka aykırı yarar elde etmek için korunan bir bilgisayara bilerek erişilmesi, zararlı öğeleri bilerek iletmek veya korunan bir bilgisayara kasten erişerek tüzükte

[133] Erdoğan, Bilişim Suçları, s. 54.
[134] Dülger, Bilişim Suçları, s. 214.
[135] Yazıcıoğlu, Bilgisayar Suçları, s. 187.
[136] Brenner, Susan W., State Cybercrime Legislation in the United States of America: A Survey, Richmond Journal of Law And Technology, Volume7 Issue 3, (Çevrimiçi) https://core.ac.uk/download/pdf/232774633.pdf (Erişim Tarihi: 07.07.2022).

belirtilen zararlara neden olmak, bilgisayar parolalarında bilerek ticaret yapmak ve korunan bir bilgisayara zarar verme tehditlerini içeren gasp eylemleri de düzenlenmiştir.[137]

Eyalet düzeyinde bilişim suçlarına ilişkin yapılan düzenlemeler federal kanunlar çıkmadan var olmasına rağmen federal kanunlar eyaletlere göre daha sığ kalarak uyumlaştırılma yapılamamıştır.[138] Eyalet kanunları incelendiğinde de en fazla düzenlenen hususun bilgisayar sistemlerine izinsiz ve yetkisiz girişlerin meydana getirdiği zararlarla ilgili olduğu görülmektedir.[139]

1986 yılında bir başka federal kanun Elektronik Haberleşmenin Gizliliği Kanunu (Electronic Communications Privacy Law) düzenlenmiştir. Bu Kanun 1968 tarihli Federal Amerikan İletişim Kanunu'nu güncellemiştir. Söz konusu düzenlemenin e-posta, telefon görüşmeleri ve elektronik olarak saklanan veriler için iletişimin korunması amacıyla gerçekleştirildiği görülmektedir.[140]

1996 tarihli İletişim Ahlak Kanunu, Amerikan Telekomünikasyon Kanunu'nda değişiklikler yapan bir düzenleme olarak değerlendirilir. Bu düzenleme çocukların internet yoluyla pornografik içerikli yayınlara erişiminin önlenmesi amacıyla çeşitli sınırlamalar içermektedir.[141] Söz konusu Kanun'un yürürlüğe girmesiyle ifade özgürlüğünü ihlal ettiği düşüncesi, Kanun'da sınırlamaya tabi tutulan kavramların tam olarak açıklanmaması bu nedenlerle soyut ve geniş kalması kamuoyunda büyük tepkiler oluşturarak ACLU ve Janet Reno davası açılmasına sebep olmuştur.[142] Aynı yıl çocuk pornografisine dair "Çocuk Pornografisini Önleme Kanunu" düzenlenmiş, bu Kanun'da İletişim Ahlak Kanunu'nda olduğu gibi sivil toplum kuruluşları ve kamuoyu tarafından tepkiyle karşılanılmıştır. 1998 yılında da "Çocukların Online Yayınlardan Korunması Kanunu" yine çocukları koruma

---

[137] Brenner, State Cybercrime Legislation in the United States of America, (Erişim Tarihi: 07.07.2022).
[138] Yazıcıoğlu, Bilgisayar Suçları, s. 187.
[139] Brenner, State Cybercrime Legislation in the United States of America, (Erişim Tarihi: 07.07.2022).
[140] Çeken, Hüseyin, Amerika Birleşik Devletlerinde Siber Suçlar, (Çevrimiçi) http://archiv.jura.uni-saarland.de/turkish/HCeken.html (Erişim Tarihi: 07.04.2022).
[141] https://www.britannica.com/topic/Communications-Decency-Act, (Erişim Tarihi: 07.04.2022).
[142] Kanun'un lafzında yer alan "ahlaksız" kelimesi içi istenildiği gibi doldurulmaya oldukça müsait bir kelime olarak görülmüş aslında öğretici ve toplumu bilgilendirici nitelikte olan AIDS ile ilgili öğretici bilgiler, doğum kontrolü, cezaevlerindeki tecavüzler gibi konularında bu durumda ahlaki olmadıklarının rahatlıkla iddia edilebileceği savunulmuştur. Bu kapsamda ACLU önderliğinde açılan davada Kanun'un sakat olduğunu, Kanun'la ne tür eylemlerin suç haline getirildiğinin anlaşılamadığı, bu kavramın sınırlarının Kanun'da net bir şekilde çizilmediği öne sürülmüştür. Ayrıca Kanun'un sadece ifade özgürlüğünü ihlal etmekle kalmadığını, aynı zamanda yetişkinlerin kendi çocukları için neyin doğru neyin yanlış olduğuna kendilerinin karar verme yetkilerinin de ellerinden alındığı iddia edilmiştir. Bu kapsamda Philadelphia Bölge Mahkemesi'nin ACLU'nun iddia ettiği gerekçelerle, anayasaya aykırı olabileceği düşüncesiyle Kanun'un iptaline karar verdiği görülmektedir. Çeken, Hüseyin, Amerika Birleşik Devletleri'nde Siber Suçlar, (Çevrimiçi) http://archiv.jura.uni-saarland.de/turkish/HCeken.html (Erişim Tarihi: 07.04.2022).

amacıyla erişkinler nezdinde erişime açık pornografik, müstehcen sitelere çocukların kolaylıkla erişememesi amacıyla düzenlenmiştir.

1997'de "İnternette Kumarın Önlenmesi Kanunu", 1998'de kimlik bilgilerine hukuka aykırı ulaşım ve bilişim güvenliği uzmanlığıyla alakalı düzenlemeler yapılmıştır.

2.2.2. İtalya

İtalya Ceza Kanunu ve Ceza Usul Kanunu'nda 1993 tarihinde 547 sayılı Kanunla bilişim alanında işlenen çeşitli fiiller suç olarak düzenlenmiştir. İtalya'nın bilişim suçlarına ilişkin ayrı bir kanun düzenlemesi yoluna gitmediği var olan ceza ve usul kanunlarına ek maddeler ve düzenlemeler yapmayı tercih ettiği görülmektedir.[143]

Kanun'un 615-ter maddesinde bilgisayar veya telekomünikasyon sistemlerine yetkisiz erişim suçu düzenlenmiştir. Bu madde ile suç eylemlerini kamu hizmeti yapanların görevini kötüye kullanarak veya görev ihlali yoluyla işlemesi, özel bir meslek yapan dedektiflerce gerçekleştirilmesi durumlarında suçun cezasının ağırlaştırılması gerektiği belirtilmiştir.[144] Failin eylemi esnasında insanlara veya eşyalara şiddet uygulaması, suç oluşturan eylemin silahla gerçekleşmesi ve suç neticesinde bilişim sisteminin zarar görerek çalışmaması ya da tahrip olması durumlarında da temel ceza artırılacaktır.[145] Söz konusu Kanun'un 615-quater maddesi bilgisayar ve telekomünikasyona giriş kodlarının kanuna aykırı sahipliği ve yayılması eylemini düzenlemiştir. Buna göre, kanuna aykırı olarak, kendisine veya başkalarına menfaat sağlamak veya başkalarına zarar vermek amacıyla bilgisayar ve telekomünikasyon sistemlerine hukuka aykırı erişim için uygun kodları, anahtar kelimeleri veya diğer araçları tedarik eden, çoğaltan, yayan, ileten kişi hapis ve adli para cezası ile cezalandırılacaktır.[146] 615-quinquies maddesi ise bilişim sistemlerine zarar vermeyi veya bozmayı amaçlayan programların yayılması fiillerini düzenlemiştir. Bu madde ile hukuka aykırı olarak bu sistemlere zarar vermek, işleyişinin tamamen veya kısmen kesintiye uğramasını veya değiştirilmesini sağlamak veya sistemdeki verilere, programlara zarar vermek amacıyla kendisi veya başkaları tarafından hazırlanmış bir bilgisayar programını üreten, ileten, dağıtan kişilerin hapis ve adli para cezasıyla cezalandırılacağı hükme bağlanmıştır.[147]

---

[143] İtalya Ceza Kanunu'nda bilişim suçlarının 615.maddeye eklenen 615-ter, 615- quater, 615- quinquies ile 635. maddeye eklenen 635-bis ve 640. maddeye eklenen 640-ter ile hüküm altına alındığı görülmektedir.
[144] https://www.cybercrimelaw.net/Italy.html (Erişim Tarihi: 12.04.2022).
[145] https://www.cybercrimelaw.net/Italy.html (Erişim Tarihi: 12.04.2022).
[146] Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s.104.
[147] Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s.105.

Başkasının verilerini, bilgilerini, yazılımlarını tamamen veya kısmen yok etmek, bozmak, silmek, değiştirmek de İtalya Ceza Kanunu madde 635-bis'te suç olarak düzenlenmiştir. Elektronik ticaret hacmi dünyada oldukça büyük yer tutan İtalya bilişim sistemleri aracı kılınarak işlenen dolandırıcılık fiillerini de İtalyan Ceza Kanunu madde 640-ter ile suç haline getirmiştir.[148]

2.2.3. Almanya

Kıta Avrupası ülkelerinde bilişim suçları ve bu suçların sorumlularına dair ilk çalışma ve düzenlemelerin Almanya'da yapıldığı görülmektedir.[149] Alman Ceza Kanunu da aynı Türk Ceza Kanunu'ndaki gibi bilişim suçlarını ayrı bir kanun olarak düzenlememiş, kanun sistematiği içerisinde korunan hukuksal değer göz önüne alınarak bilişim suçu hangi suçla ilgiliyse o bölümde düzenlenmiştir. Kanun koyucu bilişim suçu olarak kabul edilen eylemleri ayrı bir kanun olarak düzenlememekte mevcut kanunlardaki hükümleri bu eylemler doğrultusunda yeniden düzenlemektedir.[150]

İnternetin süratli gelişimini dikkate alan Almanya, internet suçlarından dolayı kişilerin ceza hukuku bağlamında sorumluluklarını düzenlemek amacıyla çalışmalar gerçekleştirmiş, 1 Ağustos 1996'da Telekomünikasyon Kanunu ile 13 Haziran 1997 tarihinde Teleservisler Kanunu'nu da içeren Bilişim ve İletişim Servisleri Kanunu yürürlüğe girmiştir. Bu son düzenleme ile başkalarına ait verilere ulaşılmasına aracılık eden erişim sağlayıcıların cezai sorumluluğu olmadığı kabul edilmiştir.[151] Teleservisler Kanunu'nda internet kişilerinin sorumluluklarını genişleten düzenlemeler yapılmıştır. Pornografik ve şiddet içerikli yayınlar, hakaret, sövme, tehdit, fikri hakların ihlâli, suç işlemeye tahrik gibi suçların internet üzerinden oldukça kolay işlenebilme imkânlarının bulunması Almanya'nın internet süjeleri hakkında bir sorumluluk rejimi getirecek ceza hukuku yöntemlerine başvurmasını gerektirmiştir.[152]

Alman Ceza Kanunu'nda "*Verilere Yetkisiz Olarak Erişim İmkânı Sağlama*" madde başlığını taşıyan 202a maddesinin kanun koyucu tarafından "Sır Aleyhine İşlenen Suçlar" arasında düzenlendiği görülür. 2007'den önce bu suçun oluşabilmesi için verilere ulaşım ve

---

[148] Dülger, Bilişim Suçları, s. 225.
[149] Mahmutoğlu, Fatih Selami, "Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C. 59, S. 1-2, (2001), s. 43.
[150] Turhan, Oğuz, Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar), Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, Ankara, 2006, s. 83.
[151] Mahmutoğlu, "İnternet Süjelerinin Ceza Sorumluluğu", s. 45.
[152] Kangal, Zeynel Temel, "Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.59, S.1-2, (2001). s. 227.

erişim imkânı sağlanması şart iken, yani bir bilişim sistemine failin yalnızca girmesi değil sistemdeki verilere ulaşabilecek makul bir süre boyunca da kalması gerekliyken, 2007'de yapılan değişiklikler sonrasında bir sisteme, sistemdeki verilere ulaşmaksızın sadece girilmesi suçun oluşumu ve cezalandırılma için yeterli olacaktır.[153]

Alman Ceza Kanunu'nun 263a maddesinde ise "*kendisinin veya üçüncü kişinin malvarlığında hukuka aykırı bir artış sağlama amacıyla bilgisayarı hatalı bir sonuç verecek şekilde programlayan veya bir şekilde yetkisiz olarak bilgisayar programının işleyiş sürecine müdahale eden kişi 5 yıla kadar hapis veya adli para cezası ile cezalandırılır."*[154] biçiminde bilişim sistemlerinin kullanılmasıyla işlenen dolandırıcılık fiilleri suç olarak düzenlenmiştir. Bu suçun oluşabilmesi için failin kendisi veya üçüncü bir kişi yararına hukuka aykırı olarak ekonomik bir çıkar elde etme saikiyle hareket etmesi yani genel değil özel bir kastının mevcudiyeti gereklidir.

Hukuki değer taşıyan bir belgenin bilişim sistemleri aracılığıyla sahte olarak düzenlenmesi, üzerinde tahrifat yapılarak oluşturulması ve bu belgenin kullanılması durumlarını Alman Ceza Kanunu 269. ve 279. maddeleri bilişim sistemleri vasıtasıyla sahtekârlık eylemleri olarak düzenlemiştir.[155]

2.2.4. Fransa

Fransız kanun koyucunun bilişim suçlarına ilişkin ayrı bir kanun düzenlemesi yoluna gitmediği ilk başlarda FCK'daki hırsızlık, inancı kötüye kullanma ve dolandırıcılık gibi mal aleyhine işlenen bazı suç tiplerini interneti de içine alabilecek biçimde çeşitli düzenlemeler yaparak bilişim suçlarını karşılamaya çalıştığı görülmektedir.[156] Kanunda bilişim suçlarına ayrı bir bölüm düzenlenmemesi bu alanda işlenen suçlarda ceza hukukunun sağlayacağı korumada birtakım boşluklar oluşturmuş neticesinde Fransız kanunlarında çeşitli düzenlemeler yapılması ihtiyacı doğmuştur.

Fransız Ceza Kanunu'nda ayrı bir bilişim suçları düzenlemesi ilk defa 5 Ocak 1988'de yapılmıştır. "Bilişim sistemlerine hukuka aykırı yollarla girilmesi veya sistemde kalınması",

---

[153] Erdağ, Ali İhsan "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", Gazi Üniversitesi Hukuk Fakültesi Dergisi, C.14, S. 2 (2010), s. 287.

[154] Karagöz, Mehmet Can, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244)", (Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı Yayımlanmamış Yüksek Lisans Tezi), Antalya, 2019, s. 98.

[155] Değirmenci, Bilişim Suçları, s. 144.

[156] Şamlı, Rüya, Türk ve Dünya Hukukunda Bilişim Suçları, Akademik Bilişim'10 - XII. Akademik Bilişim Konferansı Bildirileri10 - 12 Şubat 2010 Muğla Üniversitesi, (Çevrimiçi) https://ab.org.tr/ab10/kitap/samli_AB10.pdf, (Erişim Tarihi: 14.04.2022), s. 101.

“sistemde bulunan verilerin tahribata uğratılması, değiştirilmesi, yok edilmesi veya verilerin yerine başka veriler yüklenmesi”, “sistemin işleyişinin engellenmesi ve bozulması”, “bilgisayar belgeleri üzerinde sahtekârlık yapılması ve sahte düzenlenen belgenin kasten kullanılması” olmak üzere beş yeni suç tipi düzenlenmiştir.[157]

Fransa Yeni Ceza Kanunu 1 Mart 1993’te yürürlüğe girmiştir. Bu yeni Kanun'un gerekçesinde "Bilgileri Otomatik Olarak İşleyen Sistemlere Karşı Saldırılar" başlıklı bölümünde modern ceza hukukunun bilgi tekniğinin gelişmesinin dikkate alınması gerekliliğinden bahsedilmiştir.[158] Fransız Ceza Kanunu bir kimsenin fotoğrafları ve sözlerinde rızası olmadan montaj yapılıp herhangi bir yolla yayılmasını, bir çocuğun resminin pornografik nitelikte kullanılıp her türlü araçla yayılmasını ve bir çocuk tarafından görülmesi muhtemel şiddet ve pornografik içerikli mesajların her türlü yolla yayılmasını suç olarak düzenlemiştir.[159] Suç eylemlerinde bahsi geçen her türlü yayılmanın interneti de kapsadığı değerlendirilmektedir. Fransız Ceza Kanunu’nda düzenlenen bilişim suçları; programa hile ile girmek, programda casusluk, sabotaj ve ekonomik hile olarak karşımıza çıkar.[160] Bu düzenlemeler malvarlığı aleyhine işlenen suçlar bölümünde bulunmaktadır.

765 sayılı TCK’da bilişim suçlarına ilişkin hükümlerin Yeni Fransız Ceza Kanunu’ndan esinlenilerek düzenlendiği görülmektedir. Bilişim sistemlerinin tamamına ve bir kısmına hukuka aykırı girme, bu erişim neticesinde sistemdeki verilerin tahribatı, değiştirilmesi veya sistemin işlevinin değiştirilmesi suçun cezasını artıran ağırlaştırıcı sebepler olarak düzenlenmiştir. Ayrıca bahsedilen düzenleme ile bilişim sistemleri vasıtasıyla dolandırıcılık suçlarının işlenmesi durumu da müeyyideye bağlanmıştır.

2.2.5. İngiltere

İngiltere, bilişim suçlarına Anglo Sakson hukuk sisteminin uyguladığı şekilde, ceza mevzuatının içerisinde yer vermeyerek bu suçları ayrı kanunlar biçiminde düzenlemeyi tercih etmiştir. 28 Ağustos 1990 tarihinde yürürlüğe giren Bilgisayarların Kötüye Kullanılması Kanunu bu suçları düzenleyen genel bir kanun olarak düşünülebilir. Bunun haricinde, Müstehcen Yayınlar Kanunu, Telekomünikasyon Kanunu, Çocuk Koruma Kanunu, Veri Koruma Kanunu, Dolandırıcılık Kanunu, Terörizm Kanunu, Polis ve Adalet Kanunu, Ağır

[157] Kurt, Bilişim Suçları, s. 103.
[158] Erem, “Bilgisayar Suçları”, s. 182.
[159] Kangal, “Fransa’da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu”, s. 228.
[160] Erem, “Bilgisayar Suçları”, s. 182.

Suçlar Kanunu gibi içeriğinde bilişim suçlarına dair düzenlemelere yer veren kanunlar da bulunmaktadır. 1990'da yürürlüğe giren Bilgisayarların Kötüye Kullanılması Kanunu suç tiplerinin düzenlendiği birinci bölüm, ceza muhakemesi hukuku hükümlerinden oluşan ikinci bölüm ve genel düzenlemelerin olduğu üçüncü bölüm olmak üzere üç bölümden oluşmaktadır.[161] Bilgisayardaki program ve verilere yetkisiz giriş, diğer suçların işlenmesini kolaylaştırmak veya yardımcı olmak amacıyla bilgisayara yetkisiz erişim, bilgisayardaki yazılım veya verilerin yetkisiz değiştirilmesi eylemlerinin birinci bölümdeki suç tipleri içinde düzenlendiği görülmektedir.[162]

Bilgisayarların Kötüye Kullanılması Kanunu yürürlüğe girmesiyle beraberinde birçok tartışmayı da gündeme getirmiştir. İnternetin ve bilişim sistemlerinin gelişimlerinin henüz çok başında olduğu, yapılan bu düzenlemelerin çok kısa zamanda eskiyeceği ve ihtiyaca karşılık veremeyeceğinden bahisle kanun kapsamının genişletilmesi yönünde kamuoyunca baskılar kurulmuştur.[163] Sonuç olarak bilgisayarların kötüye kullanıma ilişkin yeni suç tipleri Polis ve Adalet Kanunu ile Ağır Suçlar Kanunu'na eklenmiştir.

2.2.6. Japonya

Japonya'nın bilişim ve bilgi sistemleri teknolojisindeki gelişimlerle yakından ilgileniyor olması bu alandaki tehlikeleri sezerek önlem almasını sağlamıştır. 22 Haziran 1987'de "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun" yürürlüğe girerek bilişim suçları maddeleri mevzuata dahil edilmiştir. Japonya'nın kanuni düzenlemelerinde suçla korunan hukuksal değeri baz aldıkları görülmektedir.[164] Japon hukukunda bilişim suçları düzenlemelerine oldukça önem verilmiştir. Klasik suç tiplerinin bilişim sistemleriyle işlendiği durumlarda örneğin hırsızlık suçunun bilişim sistemleri vasıtasıyla işlenmesi durumunda kanunda mevcut hırsızlık suçu maddesine atıf yapmadan yeni bir suç tipi vasfında yaptırımı da içerecek şekilde maddeyi detaylandırma yoluna gittikleri görülür.[165] 03.02.2000 tarihinde yalnızca bilişim suçlarının düzenlendiği "Bilgisayarlara Yetkisiz Erişim Kanunu" yürürlüğe girmiştir. Bu Kanun'dan hemen sonra 13.02.2000'de ise "İnternete Haksız Girmenin Yasaklanması Hakkında Kanun" yürürlüğe girmiştir. Bilişimle ilişkili suçları Ceza Kanunu'nun

[161] Dülger, Bilişim Suçları, s. 222.
[162] Değirmenci, Bilişim Suçları, s. 140-14.
[163] Dülger, Murat Volkan, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", Türkiye Adalet Akademisi Dergisi, C. 8, S. 31 (2017), s. 170-171.
[164] Dülger, Bilişim Suçları, s. 227.
[165] Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 102.

ilgili maddelerinde düzenleme yoluna giden Japonya'nın sadece bilişim suçlarının düzenlendiği ayrı Kanunu'da bulunmaktadır. Bu düzenlemelerinin içeriklerinin oldukça zengin ve ayrıntılı olması Japon hukukunda bilişim suçlarına verilen önemi göstermektedir.

Bulunduğumuz yüzyılda teknolojinin sürekli gelişim içinde olması, bilişim teknolojilerinin çok geniş bir alana yayılması ülkelerin iç hukuklarında yeni düzenlemeler yapma ihtiyaçlarını doğurmuştur. Klasik suç tiplerinin dahi bilişim sistemleriyle işlenebilme imkânı bilişim suçu sayısını artırmış, bilişim suçlarıyla mücadele amacıyla devletlerin düzenlemelerini zorunlu kılmıştır. Bu kapsamda yukarıda değindiğimiz ülkelerde olduğu gibi Türk hukukunda da bilişim suçları hem 765 sayılı TCK'da hem de 5237 sayılı TCK'da düzenlenmiştir. Bir sonraki bölümde eski ve yeni düzenlemeler karşılaştırmalı olarak incelenerek, açıklanmaya çalışılacaktır.

ÜÇÜNCÜ BÖLÜM

5237 SAYILI TÜRK CEZA KANUNU'NDA BİLİŞİM SİSTEMİNE GİRME, SİSTEMİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI

3.1. Genel Olarak

Bilgi teknolojilerinde yaşanan hızlı gelişimlere ceza hukukumuzun uyumlaştırılması ihtiyacıyla Türkiye'nin üyesi bulunduğu uluslararası kuruluşların tavsiye kararlarının da bir neticesi olarak bilişim suçları alanında çalışmalar yapılmıştır.[166] Türk hukuk sisteminde bilişim alanında suçlar düzenlenirken Kıta Avrupası ülkelerindeki uygulamalarla benzer olarak bilişim suçları ayrı bir kanun olarak düzenlenmemiştir. Türk hukukunda bilişim suçlarına dair düzenlemelerin temelinde Türk Ceza Kanunu olduğu görülmektedir. Yürürlükte bulunan 5237 sayılı TCK'da bilişim suçlarına ayrı bir bölümde yer verilirken bilişim sistemleriyle işlenebilmesi muhtemel geleneksel suç tiplerine suç oluşturan eylemler eklenerek düzenleme alanının genişletildiği görülmektedir. Bilişim ve bilişim ilintili suç tiplerinin büyük çoğunluğu bu kanunda düzenlenmiştir. Ayrıca bazı özel kanunların da bilişim suçu kapsamında değerlendirilebilecek eylemleri yaptırım altına aldığı görülmektedir. Elektronik Haberleşme Kanunu, Fikir ve Sanat Eserleri Kanunu ve Kişisel Verilerin Korunması Kanunu'nda bilişim sistemleri suçlarıyla ilişkili bazı eylemlerin suç olarak yer aldıkları görülmektedir.

Türk hukukunda bilişim suçlarına yer verilen ilk çalışma 1989 tarihli Türk Ceza Kanunu ön tasarısı (TCKÖ) olmuştur. Bu tasarıda bilişim suçlarının "Topluma Karşı Suçlar" başlığı altında beş madde olarak düzenlendiği görülmektedir. Ancak 1989 tarihli kanun tasarısının kanunlaşma sürecinde yaşanan aksaklıklar sebebiyle bilişim suçlarının yaptırım altına alınması gecikmiştir. Bilişim suçları ilk defa 6 Haziran 1991'de kabul edilerek aynı yılın 14 Haziran günü Resmi Gazete'de yayımlanıp yürürlüğe giren 3756 Kanun numaralı *"765 Sayılı Türk Ceza Kanun'unun Bazı Maddelerinin Değiştirilmesine Dair Kanun*" la Türk hukukunda düzenlenmiştir. 1989 kanun tasarısında yer verilen bilişim suçlarına ilişkin bölümün bazı ufak değişikliklerle 3756 sayılı Kanun metninde de aynen düzenlendiği görülmektedir. Bu Kanun'un 20. maddesindeki düzenlemeyle Türk Ceza Kanunu'na on birinci bölüm eklenerek ilk defa

[166] Karakehya, Hakan, "Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu", Türkiye Barolar Birliği Dergisi, C.22, S.81, (Mart 2009), s. 6.

bilişim alanında suçlar başlığına yer verildiği görülmektedir. 765 sayılı Türk Ceza Kanunu'nun 525. maddesinden sonra gelmek üzere "On birinci Bab" başlığı altında 525/a, b, c, d maddelerinden oluşan "Bilişim Alanında Suçlar" eklenmiştir. Bu düzenlemelerde hemen hemen aynı dönemlerde ceza kanununda değişiklikler yapan Fransa'dan esinlenilerek, Fransız Ceza Kanunu Tasarısı (FCKT) 307. maddesinden ilham alınarak tasarı hazırlanmıştır.[167] Ancak düzenlemelerin birebir FCKT ile aynı olduğu söylenememektedir. FCKT'de mal aleyhine işlenen suçlar bölümü altında bilişim suçlarına yer verilirken 765 sayılı TCK'da "Cürümler" başlıklı ikinci kitap on birinci babında "Bilişim Alanında Suçlar" olarak yer aldığı görülmektedir.[168] Fransız tasarısında bilgi sistemine karşı suçlar bölüm başlığı altında programa hile ile girmek, programda casusluk, sabotaj ve ekonomik hile olmak üzere dört grup suç eylemlerinin bu kapsamda yaptırım altına alındığı görülmektedir.[169]

765 sayılı TCK'nın "Bilişim Alanında Suçlar" düzenlemesi şu şekildedir:

"*Madde 525/a-* *Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve bir milyon liradan on beş milyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir.

Madde 525/b- *Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beş milyon liradan elli milyon liraya kadar ağır para cezası verilir.*

Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyon liradan yirmi milyon liraya kadar ağır para cezası verilir.

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

1989 tarihli TCKÖ'de yer verilen hükümlerden bir kısmının kanun metninde olmadığı görülmektedir. Tasarıda bilişim suçlarına teşebbüs halinde failin suç tamamlanmış gibi tam

[167] Ketizmen, Muammer, Türk Ceza Hukukunda Bilişim Suçları, Ankara, Adalet Yayınevi, 2008, s. 67.
[168] Akbulut, Bilişim Alanında Suçlar, s. 97.
[169] Erem, "Bilgisayar Suçları", s. 182.

olarak cezalandırılacağına ilişkin hüküm düzenlenmiş ancak kanun metninde bu düzenlemeye yer verilmemiştir. Tüzel kişilerin bilişim suçlarından dolayı sorumluluğuna 765 sayılı TCK'da yer verilmemesi ise TCKÖ ile diğer bir farkını oluşturmaktadır. Tasarıda suç olarak yer verilen eylemler değişikliğe uğramaksızın kabul edilmişse de öngörülen cezalar bakımından da farklılıklar olduğu görülmektedir.

Doktrinde 765 sayılı TCK'da bilişim alanında suçlar bölümündeki maddelerde düzenlenen suçları gruplandırırken farklı sınıflandırmaları kabul eden yazarların olduğu görülmektedir. Bazı yazarlar madde metnindeki her bir fıkranın ayrı bir suç fiilini düzenlediğini ifade etmektedir.[170] Ancak bazı yazarların daha geniş bir sınıflandırma yaptığı görülmektedir. Bu sınıflandırmaya göre ise 525/a-1. maddesinde verilerin ele geçirilmesi suçu, 525/a-2. maddesinde başkasına zarar vermek için verileri kullanmak, nakletmek veya çoğaltma suçu, 525/b-1.maddesinde verilere ya da veri işleme zarar verme suçu, 525/b-2. maddesinde bilgisayar aracılığıyla hukuka aykırı yarar sağlama suçu, 525/c maddesinde veriler üzerinde sahtekârlık suçu olmak üzere beş başlık altında sınıflandırılmaktadır.[171]

765 sayılı TCK'da gerçekleştirilen 1991 değişikliklerine olumlu ve olumsuz birçok eleştiri yöneltilmiştir. Bilişim suçlarına ilişkin düzenlemelerin kanun sistematiğine uygun olmadığı, korunan hukuki değerleri farklı suç tiplerinin aynı bölümde yer almasının yanlış olduğu eleştiri konusu yapılmıştır. Kanun koyucunun hukuken korunan değerleri birbirinden farklı suç tiplerini tek bir başlık altında toplamasıyla, sistematik bir kaygıdan çok kanundaki boşluğu doldururken uygulamada kolaylık sağlamayı amaçladığı söylenebilir.[172] Teknolojinin büyük bir hızla gelişmesiyle bu kanuni hükümlerin yeterli olmayacağı ve ilerleyen günlerde yeni bir çalışmanın kaçınılmaz olduğuna yönelik eleştiriler de belirtilmiştir.[173] Bahse konu düzenlemelerde bilgisayar sistemlerine yetkisiz giriş eylemine yer verilmemesi bu hükümlerin yetersiz kaldığı eleştirisinin ana kaynağı olarak görülmektedir. Erem ise karşı bir görüşte olup 3756 sayılı Kanunla getirilen bilişim suçlarına yönelik düzenlemelerin oldukça ileri bir sistem ve düzenleme içerdiğini ifade etmektedir.[174] Kanun metninde "bilgileri otomatik işleme tabi

[170] Erem bilişim suçlarını üçlü bir ayrıma tabi tutarak m.525/a ele geçirme, 525/b yarar sağlamak, zarar vermek ve 525/c ile de bilgisayar sahteciliği suçları gruplandırmasını yapmıştır. Erem, "Bilgisayar Suçları", s. 183.
[171] Akbulut, Bilişim Alanında Suçlar, s. 100; Yazıcıoğlu da suçları sınıflandırırken beş tip suç ayrımı yaparak 525/a-1 maddesinde bilgisayarda yer alan bilgiyi öğrenme, sır aleyhine işlenen suçlar, 525/a-2 maddesinde sistemin içeriğini kullanma, nakletme, çoğaltma yani hukuka aykırı sistem içeriğini kullanma suçları, 525/b-1 maddesinde özel bir zarar suçlarının, 525/b-2 maddesinde bilgisayar aracılığıyla dolandırıcılık suçlarının ve 525/c maddesinde ise bilgisayar aracılığıyla sahtecilik suçlarının düzenlendiğini ifade etmektedir. Yazıcıoğlu, Bilgisayar Suçları, s. 242.
[172] Yazıcıoğlu, Bilgisayar Suçları, s. 230.
[173] Ersoy, Yüksel, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları" Ankara Üniversitesi SBF Dergisi, C.49, S.3 (1994) s. 164.
[174] Erem, "Bilgisayar Suçları", s. 178.

tutmuş sistem" ifadesine yer verilmesi de çeşitli yorumlara sebep olmaktadır. Kanun koyucunun bilgisayar kavramı yerine tercih ettiği bu kavramla cezalandırılma koşulunun alanını genişletmek istediği, kavramın yerinde kullanıldığı düzenlemeye yönelen olumlu eleştiriler arasında yer almaktadır.[175] Ancak ifadede kullanılan otomatik kavramının manyetik ve elektronik özelliğine sahip bilgisayarlar için isabetli olmadığını ifade eden görüşler de bulunmaktadır.[176]

5237 sayılı TCK'da bilişim suçları özel hükümlerin düzenlendiği ikinci kitap üçüncü kısımda "Topluma Karşı Suçlar" başlığı altındaki onuncu bölümünde "Bilişim Alanında Suçlar" başlığı altında yer almaktadır. Kanun koyucunun bilişim alanındaki suçları bu başlık altında beş madde ile düzenlediği görülmektedir. TCK'nın 243. maddesinde "*bilişim sistemine girme*", 244. maddesinde "*sistemi engelleme, bozma, verileri yok etme veya değiştirme*", 245. maddesinde "*banka veya kredi kartlarının kötüye kullanılması*", 245/A maddesinde "*yasak cihaz veya programlar*" suçlarına ve son olarak 246. maddesinde de "*tüzel kişiler hakkında güvenlik tedbiri uygulanması*" tedbirine yer verilmektedir.

5237 sayılı Türk Ceza Kanunu'nda 765 sayılı eski Türk Ceza Kanunu'nda olduğu gibi bilişim suçlarının kanun sistematiği içerisinde ayrı bir bölümde düzenlendiği, farklı olarak bilgileri otomatik olarak işleme tabi tutmuş sistem kavramı yerine bilişim sistemi kavramının tercih edildiği görülmektedir. Bu değişikliğin hukuk terminolojisinde birlik ve gelişen bir alanın standartlaştırılması adına oldukça yerinde olduğu değerlendirilmektedir.[177] İki kanun arasındaki bir diğer farklılık da bilişim sistemlerine girme suçunun daha önce 765 sayılı Kanun'da düzenlememiş olmasıdır. Her ne kadar bu suçun 765 sayılı Kanun'da 525/a-1. maddesinde düzenlenen "verilerin ele geçirilmesi" ve 525/a-2. maddesinde düzenlenen "başkasına zarar vermek üzere ele geçirilen verilerin kullanılması" suçlarının karşılığı olduğu düşünülse de bilişim sistemine girme suçunun oluşması için verilerin ele geçirilmesi şartının olmaması iki maddenin birbirine karşılık gelmediğini göstermektedir.[178] 5237 sayılı TCK'nın 243. maddesi ile bilişim sistemine girme eylemi ilk defa suç olarak düzenlenmiştir. 765 sayılı Kanun'da bilişim alanında suçlar bölümünde yer verilen, verilerin ele geçirilmesi suçu, başkasına zarar vermek için verileri kullanmak, nakletmek veya çoğaltmak suçu ve verilerde sahtekârlık suçlarının 5237 sayılı Kanun'da düzenlenmediği görülmektedir. Banka ve kredi

[175] Ersoy, Bilişim Suçları s. 165.
[176] Akbulut, Bilişim Alanında Suçlar, s. 104.
[177] Eker, "Türk Ceza Hukuku'nda Bilişim Suçları" s. 120.
[178] Erdoğan, Bilişim Suçları, s. 110.

kartlarının kötüye kullanılması suçu ise 5237 sayılı Kanun'da 245. maddesi ile ilk defa hükme bağlanmıştır.

3.2. Bilişim Sistemine Hukuka Aykırı Girme veya Sistemde Kalma Suçu

3.2.1. Genel Olarak

Bilişim sistemine girme veya sistemde kalmaya hukuka aykırı olarak devam etme eylemi ilk defa 1 Haziran 2005'te yürürlüğe giren 5237 sayılı TCK'nın 243. maddesi ile yaptırım altına alınmıştır. 765 sayılı TCK'nın 525/a maddesinde bilgileri otomatik işleme tabi tutmuş bir sistemden program, veri veya diğer herhangi bir unsurun hukuka aykırı ele geçirilmesi eylemi bazı yönleriyle 5237 sayılı TCK'nın 243. maddesine benzetilse de bilişim sistemlerine hukuka aykırı girme hükmünü tam olarak karşılayamadığı görülmektedir.[179]

5237 sayılı TCK'nın "Bilişim Alanında Suçlar" bölümü 243.maddesi "bilişim sistemine girme" kenar başlığında;

"(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

(4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."[180] şeklinde düzenlenmiştir.

Türk Ceza Kanunu'ndaki bilişim sistemine girme suçunun Avrupa Siber Suç Sözleşmesi ikinci bölüm 2. maddesinde yer alan hukuka aykırı erişim düzenlemesi ile aynı doğrultuda olduğu görülmektedir.[181]

TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme suçu dört fıkradan oluşmaktadır. Birinci fıkrada bilişim sistemlerine hukuka aykırı olarak girme veya orada kalma fiilinin suçun temel şekli olarak düzenlendiği, ikinci fıkra da daha az cezayı gerektiren bedel karşılığı yararlanılabilen sistemlerde suçun işlenmesi durumuna yer verildiği, üçüncü fıkrada

[179] Değirmenci, Olgun, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", Türkiye Barolar Birliği Dergisi, C. 18, S. 58 (Mayıs 2005), s. 204.
[180] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 19.04.2022).
[181] Kurt, Bilişim Suçları, s. 147.

ise suçun neticesi sebebiyle ağırlaşmış hali olan sistemdeki verilerin yok olması veya değişmesinin hükme bağlandığı görülmektedir. Son fıkra olan dördüncü fıkrada veri nakillerini teknik araçla takip suçu ise Avrupa Siber Suç Sözleşmesinin 3. maddesinde düzenlenen "yasa dışı araya girme" suçunun Türk hukukuna uyarlanmasıdır.[182] Madde metnine sonradan eklenen bu fıkranın, 24 Mart 2016'da kabul edilerek 7 Nisan 2016'da yürürlüğe giren 6698 sayılı Kanun'un 30. maddesiyle mevzuatımıza girdiği görülmektedir.

765 sayılı Kanun'a değişiklik getiren 3756 sayılı Kanun'la hukukumuza giren bilişim alanında suçlara yönelen ağır eleştiriler, 1997 yılında yeni bir ceza kanunu tasarısı hazırlayan komisyona da bilişim suçlarında değişikliklere ihtiyaç olduğunu düşündürmüştür. 1997 tarihli TCK tasarısının 347. maddesi ile batı hukukundaki değişiklikler özellikle Fransız Ceza Kanunu ana iskelet olarak kabul edilmiş ve bilişim sisteminin tamamına veya bir kısmına hukuka aykırı girme veya sistemde kalma suçu düzenlenmiştir.[183] Bilişim sistemlerine girme suçuna 1997 tarihli kanun tasarısından sonra 2000 ve 2003 tarihli ceza kanunu tasarılarında da öngörülen cezalarda farklılıklarla tekrar yer verilmiştir.

Bilişim sistemine girme kavramı "bilgisayar korsanlığı", " bilgisayara tecavüz", "kod kırma", "bilişim sistemlerine hukuka aykırı erişim" gibi terimlerle de tanımlanabilmektedir.[184] Kanun lafzında geçen bilişim sistemine girme eylemiyle aslında kastedilen sistemin donanımsal parçalara ayrılarak içine girilmesi manasına gelmemekte sistemin sanal alanının tümüne veya bir kısmına hukuka aykırı olarak erişim sağlama anlamında kullanılmaktadır.[185] Ayrıca suçun oluşması için sistemde bulunan verilere ulaşılması, ele geçirilmesi, verilerin içeriklerinin okunması şartı aranmamaktadır.[186] Verilerin ele geçirilip geçirilmediğine bakılmaksızın bir bilişim sistemine hukuka aykırı girmek veya sistemde kalmaya devam etmek, hukuka uygun olarak sisteme girip, hukuka aykırı sistemde kalmaya devam etmek fiilleri suçun cezalandırılması için yeterlidir. Failin bir bilişim sistemine hukuka aykırı giriş sağlayarak sistemde bulunan kişisel verileri ele geçirilmesi durumunda artık sisteme girme suçundan

---

[182] Dülger'e göre; Her ne kadar söz konusu fıkra kanun koyucu tarafından madde metnine ek olarak düzenlenmişse de veri akışını teknik araçlarla izleme suçu başlı başına ayrı bir suç oluşturmaktadır. Dülger, Bilişim Suçları, s. 237.

[183] "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve yüz milyon liradan üç yüz milyon liraya kadar ağır para cezası verilir." Akbulut, Bilişim Alanında Suçlar, s. 113.

[184] Erdoğan, Yavuz, "Bilişim Sistemine Girme ve Kalma Suçu", Prof. Dr. Burhan Ceyhan'a Armağan II, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. 12, Özel Sayı (2010), s. 1365; Akbulut, Bilişim Alanında Suçlar, s. 116.

[185] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1375.

[186] Yazıcıoğlu, Recep Yılmaz, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunun Değerlendirilmesi" Hukuk ve Adalet Eleştirel Hukuk Dergisi, Y. 1, S. 1 (Ocak-Mart 2004), s. 177.

bahsedilemeyecek Ceza Kanunu'nun 136. maddesinde yer alan "kişisel verileri ele geçirme ve yayma" suçu oluşacaktır.

24/03/2016 tarihinde kabul edilen 6698 sayılı Kanun'un 30. maddesi bilişim sistemine girme suçu açısından bazı değişiklikler getirmiştir. Bu değişiklikle 243. maddenin ilk fıkrasında yer alan "ve" bağlacı kaldırılarak yerine "veya" bağlacı kullanılmıştır. Yapılan bu değişikliğin öncesinde bilişim sistemlerine sadece hukuka aykırı olarak erişim sağlamak bu suçun cezalandırılması için yeterli görülmemekte aynı zamanda erişilen sistemde kalmaya bir zaman zarfı devam edilmesi şartıyla yaptırım altına alınmaktaydı.[187] Bu değişiklikle kanun koyucu tek bir fiili suçun oluşumunda yeterli görmeyerek çok hareketlilik, birden fazla hareket[188] şartı ararken "ve" bağlacının "veya" biçiminde değiştirilmesiyle suç seçimlik hareketli suç halini almıştır.[189]

3.2.2. Suçla Korunan Hukuki Değer

Bilişim sistemlerine hukuka aykırı girme veya sistemde kalmaya devam etme suçunun yaptırım altına alınmasıyla suçla korunmak istenen hukuki değere ilişkin doktrinde farklı görüşlerle karşılaşılmaktadır.

Bir görüşe göre, bu suçun koruduğu hukuksal değer karma nitelik taşımakta olup, bilişim sistemleri bireylerin şahsi, dokunulmaz alanlarını oluşturduğundan öncelikli olarak kişilerin özel yaşamının gizliliğinin, haberleşme hürriyetlerinin ve sırlarının masumiyetinin korunduğu, ikincil bir değer olarak da bilişim sistemlerinin güvenliğinin korunduğu savunulmuştur.[190]

Diğer görüşe göre ise bu düzenlemenin koruduğu birden fazla hukuki değer bulunmaktadır. Buna göre; maddenin Kanun'da "Topluma Karşı Suçlar" başlığı altında düzenlenmesi sebebiyle toplum düzenini koruduğu, bilişim sisteminin sahibinin izni dışında sisteme erişilmesi sebebiyle özel hayatın gizliliğini koruduğu ve bilişim sistemlerinin haberleşme amacıyla kullanılmasından dolayı da haberleşmenin gizliliğini koruduğunu ifade

---

[187] "Sanık ... adına kayıtlı 0 342 *** 75 95 numaralı hat tarafından kullanılan 78.164.61.188 numaralı IP ile 13.11.2009 tarihinde saat 13.49.39'da ... Organizasyon Danışmanlık adına kayıtlı 0 532 *** 01 71 numaralı hatta ilişkin Turkcell İletişim Hizmetleri AŞ'nin **bilişim sistemine giriş yapıldığı sabit ise de suç tarihi itibarıyla bilişim sistemine hukuka aykırı olarak girme suçunun oluşabilmesi için failin sadece bilişim sisteminin bir kısmına veya bütününe hukuka aykırı olarak girmesinin yeterli olmadığı**, ayrıca girdiğini fark etmesine rağmen makul bir süre orada kalmasının da gerektiği…" Yargıtay Ceza Genel Kurulu E. 2019/239 K. 2021/325 T. 01.07.2021, (https://legalbank.net/arama/mahkeme-kararlari).

[188] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1374.

[189] Dülger, Bilişim Suçları, s. 238.

[190] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 743-744.

etmektedir.[191] Ayrıca bu suçla, sisteme her yetkisiz girişin sistem sahibi ve kullanıcılarının maddi ya da manevi zarara uğratılma ihtimalini doğurmasından dolayı kullanıcı ve sistem sahibi menfaatlerinin ihlal edildiğini, bir sisteme yetkisiz girişin önlenmesiyle sonradan sistem aracılığıyla işlenecek suçların önüne geçilebileceğinden olası başka suçların işlenmesinin de engellenmesini sağlandığını ve son olarak da bilişim sistemlerinin güvenliği ve güvenilirliğinin korunduğunu düşünmektedir.[192]

Başka bir görüşte; bilişim sistemlerinin güvenliğinin sağlanması bu suç tipiyle korunan öncelikli yarar iken aynı zamanda sistem kullanıcılarının menfaatlerinin zarar görmemesi amacıyla özel hayatın gizliliğinin de dolaylı olarak korunduğu düşünülmektedir.[193]

Doktrinde bu suçla korunan hukuki değerin malvarlığı olduğunu savunan görüşler de mevcuttur.[194] Yine diğer bir görüşte ise; bu suçla korunan hukuki değer bilişim sistemlerinin güvenliği, sistemin dokunulmazlığı olmakla beraber sisteme hukuka aykırı girişlerin cezalandırılmasıyla bilişim sistemleri aracılığıyla ileride işlenebilecek diğer suçların da önüne geçilerek farklı türdeki birçok hakkı korumakta olduğu savunulmuştur.[195]

Diğer bir görüşe göre; bu suç tipiyle korunmak istenen hukuki değerin bilişim sistemlerinin güvenliği olduğu savunulmaktadır.[196] Çünkü bilişim sistemlerine hukuka aykırı girme veya sistemde kalmaya hukuksuz devam etme eylemi korunmaya değer birden fazla hukuksal değeri barındırmasına rağmen tüm bunların çatısında hepsini kapsayacak hukuki değer bireylerin menfaatlerine direkt bir zarar verilmese dahi müdahaleden uzak sistemin güvenli kullanımı hususudur. Bizim de katıldığımız bu görüşe göre, bilişim sistemine girme suçuyla korunması gereken günümüzde bireylerin sıklıkla kullanımına başvurduğu ve ilerleyen teknolojiyle beraber hayatın her alanında karşımıza çıkan bilişim sistemleriyle yapılan işlemlere güven duygusunun korunması gerektiği yönündedir.

3.2.3. Suçun Maddi Unsurları

3.2.3.1. Fail ve Mağdur

[191] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1370.
[192] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1371.
[193] Parlar, Ali/Öztürk, Mustafa, Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar, İstanbul, Aristo Yayınevi, 2020, s. 25-26.
[194] Ketizmen, Bilişim Suçları, s. 92.
[195] Yücel, Mustafa, "Bilişim Suçları", Ankara Barosu Dergisi, C.49, S.4 (1992), s. 509.
[196] Dülger, Bilişim Suçları, s. 246; Aynı görüşte Bkz: Akbulut, Bilişim Alanında Suçlar, s. 118.

Bilişim sistemlerine hukuka aykırı girme veya sistemde kalma suçu işleyen kişi yönünden bir özellik göstermemektedir. Kanun metninde "kimse" tabiri kullanıldığından fail bakımından ayrıca bir özellik aramamaktadır.[197] Bu suçun faili herkes olabilir.

Bilişim sistemleri henüz bu kadar yaygınlaşmadan önce teknolojik bilgiye sahip insan sayısının azlığı sebebiyle bilişim suçlarını işleyebilecek kişilerin mesleki faaliyetlerinden dolayı bu bilgiye sahip olabilecekleri bağlantısı kurulur ve bu suçlar beyaz yaka suçları olarak adlandırılırdı.[198] Ancak böyle bir sınırlama yapabilme imkânı artık bulunmamaktadır.[199] Her ne kadar önceleri belirli bir bilgi düzeyine sahip kişilerin bu suçun faili olabileceği değerlendirilmiş olsa da günümüz koşullarında internet kullanımının yaygınlaşmasıyla kolayca ulaşılabilecek birkaç program vasıtasıyla standart bilgisayar becerisine sahip kişilerce de kolaylıkla işlenebilen bir suç konumundadır.[200]

Bilişim sistemlerine karşı işlenen suçların failleri toplumda hacker, bilişim korsanı gibi özel isimlerle anılmakta ve çoğu zaman gerçekleştirdikleri eylemleri suç değilmişçesine halk arasında sempatik bulunmakta hatta bilişim sistemlerinin güvenliğine ilişkin yeniliklerin onlar sayesinde olduğu değerlendirilmektedir. Toplumda bu şekilde zararsız ve çocukça oldukları değerlendirilen bilişim korsanları aslında kayda değer büyük zararlara sebebiyet vermektedir.[201]

Bilişim suçları fail yönünden özellik gösteren bir yönü de tüzel kişilerin durumudur. Bilişim suçları gerçek kişiler tarafından işlenebilen suçlardır ancak tüzel kişilerin yararına haksız menfaat sağlanarak bu suçların işlenmesi durumunda 5237 sayılı TCK'nın 246. maddesi gereği haksız menfaat sağlayan tüzel kişiler hakkında bunlara özgü güvenlik tedbiri uygulanabilecektir.[202]

Uygulamada bilişim sistemi suçlarında failin tespiti amacıyla öncelikle IP adresinin belirlenmesi yoluna gidilmektedir. Ancak tek başına bu bilgiyle suçun failinin IP adresinin üzerine kayıtlı kişi olduğu kesin olarak söylenemeyecek, IP adresinin değişken bir özellik

---

[197] Erdoğan, Bilişim Suçları, s. 143; Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 749; Dülger, Bilişim Suçları, s. 249.

[198] "Beyaz yaka suçu, bir kimsenin sahip bulunduğu mesleğinden kaynaklanan sosyal statüsü ve kendisine duyulan güveni kötüye kullanarak işlediği suç teşkil eden eylemleri ifade etmektedir." Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 749.

[199] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 749.

[200] Yenidünya/Değirmenci, Bilişim Suçları, s. 57.

[201] Dandin, Ali Nazmi, "Risk Toplumunda Bilişim Suçları Ve Hukukun Etkinliği", (Afyon Kocatepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Ana Bilim Dalı Yayımlanmamış Yüksek Lisans Tezi), Afyonkarahisar, 2019, s. 75.

[202] Mahmutoğlu, Fatih Selami, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, C.71, S.1, (2013), s. 859.

göstermesi sebebiyle suçun fail tarafından işlendiğinin şüpheden uzak teknik verilerle tespiti de cezalandırma şartı için aranacaktır.[203]

Bilişim sistemlerine hukuka aykırı girme ve sistemde kalma suçu mağdur bakımından da ayrı bir özellik aramamıştır. Bu sebeple hukuka aykırı olarak bir bilişim sisteminin tümüne veya bir kısmına girilen, girildikten sonra kalınmaya devam edilen sisteminin hak sahibi ya da sistem kullanıcısı olan herkes bu suçta mağdur olabilir.[204] Bir bilişim sistemine erişim için gerekli yetkiye sahip olup bu yetkiyi doğrudan kullanabilen kişilerin sistemde hak sahibi kişi olduğu dolayısıyla mağdur sıfatını alabilecekleri söylenebilir. Ancak hak sahibince üçüncü kişilerin bilişim sistemine erişimine zımni veya açıkça rıza gösterilmiş ise bu suçun mağduru olamayacaktır.[205]

Bu suçta mağdurun kim olacağı hususunda doktrinde çeşitli görüşler yer almaktadır. Öncelikle tüzel kişilerin mağdur mu suçtan zarar gören mi olacağı hususunda görüş ayrılıkları yaşanmaktadır. Bazı yazarlara göre, bir suçun mağduru ancak gerçek kişiler olabileceğinden bilişim sistemleri suçları ile bir tüzel kişinin menfaati zarar görüyorsa suçtan zarar gören olarak kabul edilecektir.[206] Bir görüşe göre ise, bu suçun mağduru gerçek kişiler olabileceği gibi tüzel kişilerde suçun mağduru olabilecektir.[207] Bizim kanaatimize göre suçtan zarar gören ile suçun mağduru farklı kavramlardır. Bilişim sistemleri suçları ile bir tüzel kişinin menfaati zarar görüyorsa bu kişi suçtan zarar gören olarak kabul edilecektir. Yargıtay'ın da suçtan zarar gören kamu kurum kuruluşlarının kovuşturmadan haberdar edilerek davaya katılma olanağı sağlanması gerektiği yönündeki kararları bulunmaktadır.[208]

---

[203] İhtiyaroğlu, Uğur, "Bilişim Sistemlerine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi", Hacettepe Hukuk Fakültesi Dergisi, C.10, S. 2 (2020), s. 413.
"Sanığın suçlamayı kabul etmeyerek, kablosuz modem kullanıldığından hattının başkaları tarafından girilip kullanılmış olabileceğine ilişkin savunması karşısında; bildirilen **IP numaralarının** bağlı bulunduğu internet hattında **ne özellikte modem** kullanıldığı, **kablolu veya kablosuz** olup olmadığı, **şifreli** olup olmadığı, **modemden başka kullanıcıların internete bağlanılıp bağlanılmadığının** belirlenmesi açısından ilgili internet sağlayıcısından bilgi istenmesi ve sanığa ait bilgisayar getirtilip uzman bilirkişi tarafından **LOG kayıtları incelenerek** sonucuna göre, katılana ait mail adresinin erişilmez kılındığı takdirde TCK.nun 244/2. mail adresine girilmesi ancak; bu adrese erişimin engellenmemesi ve katılanın mail adresinde kalmaya devam ettiğinin tespiti halinde aynı yasanın 243/1. maddesi kapsamındaki suçun oluşacağı dikkate alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması,...BOZULMASINA.." Yargıtay 8. Ceza Dairesi E. 2016/12634 K. 2017/4967 T. 03.05.2017, (https://legalbank.net/arama/mahkeme-kararlari).
[204] Mahmutoğlu, "TCK'da Bilişim Alanında Suçlar", s. 859.
[205] Yaşar, Osman/Gökcan, Hasan Tahsin/Artuç, Mustafa, Yorumlu - Uygulamalı Türk Ceza Kanunu Cilt V, Ankara, Adalet Yayınevi, 2010, s. 6739.
[206] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 75; Mahmutoğlu, "TCK'da Bilişim Alanında Suçlar", s. 859; Dülger, Bilişim Suçları, s. 258.
[207] Erdoğan, Bilişim Suçları, s. 145.
[208]"…. şikayetçi T.C. Ölçme, Seçme ve Yerleştirme Merkezi (ÖSYM)'nin…. **Şikayetçi kurumun** davadan haberdar edilip delillerini sunma ve **davaya katılma olanağı sağlanarak** sanığın hukuki durumunun değerlendirilmesi gerektiği gözetilmeden, yargılamaya devamla hüküm kurulması …BOZULMASINA…"

Mukayeseli hukuk incelendiğinde; bazı ülkelerin maddi ceza hukuklarında bilişim sistemine erişim suçu düzenlemelerinde mağdura yönelik birtakım unsurlar arandığı görülmektedir. Mağdurun suça konu bilişim sisteminin güvenliğini özel olarak sağlaması şartı aranabilmektedir. Alman Ceza Kanunu'nun "özel hayat ve sır alanının ihlali" bölümünde verilere yetkisiz girişi düzenleyen 202a maddesinde[209] bilişim sistemine yetkisiz girişlere karşı sistemin mağdur tarafından özel olarak korunması suçun unsuru olarak aranmakta; Japonya'nın Bilgisayarlara Yetkisiz Erişim isimli Kanunu ise bu suçun oluşabilmesi için şifre ile erişilen bilişim sistemlerinin bulunması gerektiğini düzenlemektedir.[210] Türk hukukunda ise suçun oluşması için mağdura yönelik bir unsur aranmamaktadır. Mağdurun bilişim sistemine yönelik herhangi bir önlem alması, sistemin güvenlik yazılımlarıyla korunması suçun oluşmasında da faillerin cezalandırılmasında da etkili görülmemiştir.

3.2.3.2. Suçun Konusu

5237 sayılı TCK'nın 243. maddesinde yer alan her fıkra bakımından suçun konusunun ayrı değerlendirilmesi gereklidir. Maddenin 1. fıkrasında düzenlenen suç bakımından hukuka aykırı olarak yetkisiz girilen veya kalmaya devam edilen bilişim sistemi suçun konusudur. Yani bilgisayarın donanımsal özellikleri değil, soyut olan yazılım ve programlara ilişkin yanı suçun konusunu oluşturmaktadır.[211] Suça konu bilişim sistemine erişimin birtakım uygulamalar ve güvenlik tedbirleriyle sınırlandırılması yani bu sisteme yalnızca işlem yapma yetkisine sahip kişilerce erişilebilmesi, kullanılabilmesi gerekmektedir. Herkes tarafından talep edilen, istenilen her anda ulaşılabilen sistemlerin, halka açık internet siteleri gibi, bu suçun konusunu oluşturduğu söylenemeyecektir.[212]

Bilişim sistemine girme suçunun nitelikli halini düzenleyen 243. maddenin ikinci fıkrasında bedel karşılığında yararlanılan sistemler suçun konusu iken neticesi sebebiyle ağırlaşmış hal düzenlemesi içeren üçüncü fıkrada failin taksiri neticesinde sistemdeki verilerin yok olması, değişmesi eyleminde sistemdeki veriler suçun konusunu oluşturacaktır.

Yargıtay 8. Ceza Dairesi E. 2017/6844 K. 2017/11127 T. 11.10.2017, (https://legalbank.net/arama/mahkeme-kararlari).

[209] "Madde 202a- (1) Yetkisiz olarak, kendisine ait olmayan ve haksız erişimlere karşı özel olarak güvenlik altına alınmış bulunan verilere, giriş güvenliğini kırarak kendisi veya bir başkası için erişme imkanı sağlayan kişi, üç yıla kadar hapis veya (adli) para cezası ile cezalandırılır.
(2) Birinci fıkra anlamındaki veriler, sadece elektronik veya manyetik olarak ya da doğrudan algılanabilir olmayan başkaca herhangi bir şekilde saklanmış veya iletilen verilerdir." Erdağ, "Bilişim Alanında Suçlar", s. 286.

[210] Dülger, Bilişim Suçları, s. 258.

[211] Taşdemir, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması Dolandırıcılık Suçları, s. 255.

[212] Erdoğan, Bilişim Suçları, s. 1381.

Uygulamada TCK'nın 243. maddesi ikinci fıkrasında bedeli karşılığında yararlanılabilen bir bilişim sistemine girme suçunun konusu ile TCK'nın 163. maddesi ile düzenlenen karşılıksız yararlanma suçunun konularının birbirleriyle karıştırıldıkları görülmektedir. Otomatlarca sunulan hizmetler, ücretle yararlanılan telefon hatları ve frekanslar, elektromanyetik dalgalar aracılığıyla yapılan şifreli ve şifresiz yayınlar bilişim sistemine girme suçunun konusu olamayacaktır.[213] Bir bilişim sistemine ya da sistemin bir kısmı üzerine sisteme giriş yapıldığı durumlar suçun konusunu oluşturacaktır.

Suçun konusu olan bilişim sistemi kamu kuruluşlarına, bankalara, büyük şirketlere ait olabileceği gibi kendimize ait kişisel sistemimiz de olabilecektir.[214] TCK'da hukuka aykırı girilen bilişim sisteminin önem ve değerine göre bir yaptırım belirlenmemiştir. Hukuksuz girilen tüm sistemler, aynı suçun konusunu oluşturacaktır. Bazı yazarlar kanunda eksik bir düzenleme olduğunu bu durumun suçun daha çok cezayı gerektiren nitelikli bir hal olarak düzenlenmesi gerekliliğini belirtmişlerdir.[215] Biz de bilişim sistemlerine girme eyleminin yöneldiği bilişim sisteminin kişisel bir bilgisayar veya bulut sistemi olması ile devletin bir kamu kurumuna ait sistem olması ya da bir banka sistemi olması durumlarının yarattığı mağduriyetlerin birbirinden farklı olması nedeniyle aynı suçun konusu olmalarının kanundaki bir eksiklik olduğunu değerlendirmekteyiz.

3.2.3.3. Hareket

Bilişim sistemine girme suçunda kanun koyucunun düzenlediği hareket unsuru; hangi yolla olursa olsun bilişim sistemine girilmesi ya da girilen sistemde kalmaya devam edilmesidir. Seçimlik hareketli olarak düzenlenen bu suç tipindeki hareketlerden birinin yapılmasıyla suç gerçekleşmiş olacaktır.

2016'da yürürlüğe giren 6698 sayılı Kanun'dan önce doktrinde madde metnindeki hareketin seçimlik hareketli suç mu birden fazla hareketli suç mu olduğu tartışılmaktaydı. Bu tartışmanın dayanağını madde metni ile maddenin gerekçesinde bulunan farklılıklar oluşturmaktadır. Madde metninde geçen "ve" bağlacı gerekçede "veya" olarak bulunmakta bu durum maddelerin yorumlanmasında madde metni, başlık ve gerekçenin bir bütün olarak ele alınması göz önüne alındığında doktrindeki görüşleri ikiye bölmekteydi.[216] Salt madde metnine

[213] Dülger, Bilişim Suçları, s. 270.
[214] Erdoğan, Bilişim Suçları, s. 1396.
[215] Dülger, Bilişim Suçları, s. 258.; Erdoğan, Bilişim Suçları, s. 1400.
[216] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6743.

göre değerlendirildiğinde bilişim sistemine girip hemen çıkan kişiler sistemde kalma şartını sağlamadığı için cezalandırılma imkânı bulunmamaktaydı.[217]

Bu suçun oluşması için gerekli bilişim sistemine girme veya orada kalma eylemlerinin hangi hareketlerle yapılacağı kanunda sınırlandırılmadığından her türlü hareketle gerçekleşebilecek serbest hareketli bir suçtur.[218] Yine failin eylemiyle suçun oluşumu için bir sonucun gerçekleşmesi veya bir zararın oluşması aranmadığı için soyut tehlike suçudur.[219]

Bilişim sistemine girme suçunun oluşması için girme hareketi icrai niteliktedir. Failin sistemde kalmaya devam etmesi hem icrai hem de ihmali şekilde olabilir. Failin bilişim sistemine girmesinden sonra çeşitli yazılımlar vasıtasıyla sistemden dışarı atımı önlemek adına çeşitli işlemler yapması, hareketi icrai nitelikte yapacaktır.[220] Kanun koyucu fiilin icrai veya ihmali hareketle işlenmesinde suçun oluşumu ve cezalandırma açısından bir fark görmemiştir. Yargıtay'ın da bir kararında bilişim sistemlerine girme eylemini tanımladığı görülmektedir.[221]

Suçu oluşturan bilişim sistemine girme eylemi bilgisayarın donanım parçalarının açılarak fiziki olarak içerisine girilmesi yani bilgisayar kasasının veya ekranın sökülüp içine girilmesi gibi ya da bir bilişim sisteminin bulunduğu odaya girilip mekanizmasına müdahale edilmesi değildir. Burada kast edilen sistemin soyut alanı olan dijital alana girilmesidir.[222] Girmek teriminin burada suçun hareket unsurunu tam karşılayamadığından bahisle erişim kavramının kullanılması gerektiğini savunan görüşler vardır. Bu yazarlar; suç oluşturan eylemin sanal ortama yani işletim sistemleri, yazılımlar ve programlara yöneldiğini, girmek terimiyle fiziksel bir alana girme eylemi çağrıştırıldığından terminoloji açısından "erişim" kavramının

---

[217] Taşdemir, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması Dolandırıcılık Suçları, s. 257.
[218] Erdoğan, Bilişim Suçları, s. 1378.
[219] Özbek, Veli Özer/Kanbur, Mehmet Nihat/Doğan, Koray/Bacaksız, Pınar/Tepe, İlker, Türk Ceza Hukuku Özel Hükümler, Ankara, Seçkin Yayıncılık, 2011, s. 846.
[220] Dülger, Bilişim Suçları, s. 261; Taşdemir, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması Dolandırıcılık Suçları, s. 256.
[221] **"Bilişim sistemine girmek", bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir.** 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. Bilgisayar veri ve sistemlerine yapılan izinsiz giriş, aynı zamanda, "bilgisayara tecavüz", "kod kırma" ya da "bilgisayar korsanlığı" olarak da tanımlanmaktadır. Bu suç, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir. Girmede, iletişimin kablolu veya kablosuz olması ile mesafenin yakın ve uzak olması arasında da fark yoktur. Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez. Mağdurun kişisel bilgisayarına ait işletim sistemine, bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır." Y 8. CD E.2013/10402 K.2014/11836 T.07.05.2014, (https://legalbank.net/arama/mahkeme-kararlari).
[222] Erdoğan, Bilişim Suçları, s. 117; Dülger, Bilişim Suçları, s. 262.

kullanılmasının daha doğru olacağını savunmaktadır.[223] Kaldı ki kanun koyucunun "İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik" ve "İnternet Toplu Kullanım Sağlayıcılar Hakkındaki Yönetmelik"lerinde de "girmek" yerine "erişim" terimini kullanmasıyla doktrindeki çoğunluk görüşü desteklediği sonucuna ulaşılabilir. Bilişim sistemine girmek bir ağ vasıtasıyla sistemin içine girme olabileceği gibi kapalı bir sistemin düğmesine basarak oturum açmak şeklinde de olabileceği bu sebeple kanunda geçen "girmek" teriminin yerinde ve doğru kullanıldığı görüşünü savunan yazarlarda mevcuttur.[224]

Mukayeseli hukuk incelendiğinde bilişim sistemine girme kavramının "yetkisiz erişim", "hileyle erişim", "zorla erişim", gibi terimlerle karşılandığı görülmektedir. TCK'nın 243. maddesi 1. fıkrasında düzenlenen bilişim sistemine girme suçunun aslında Avrupa Konseyi Siber Suç Sözleşmesi'nin ikinci maddesinde yer alan hukuka aykırı erişim düzenlemesini karşıladığı görülmektedir.[225]

Bir bilişim sisteminin bütününe veya yalnızca bir kısmına hukuka aykırı girilmesi suçun oluşumu için bir farklılık yaratmaz. Her iki eylemde de suç tamamlanmıştır. Bilişim sistemleri içinde değerlendirilen veri taşıyıcısı, usb, cd gibi sistemin parçalarına girilmesi de bu suçu oluşturacaktır.[226]

Suçun oluşumu için bilişim sistemine girmeyi engelleyici programlara sahip, özel olarak korunan bir sistem olması şartı aranmaz. Fail haksız olarak elde ettiği sistem şifresiyle, casus yazılımlar aracılığıyla veya sistem güvenlik duvarını aşarak bilişim sistemine girebilecektir. Sistem sahibinin açık veya zımni rızası yani hukuki sınırların var olup olmadığı suçun oluşumunda kriterdir.[227] Hukuka uygun olarak girilen bir sistemde sistem sahibinin daha sonra

---

[223] Aynı görüşteki yazarlar için bkz: Artuk/Gökcen/Yenidünya, Ceza Hukuku, s. 741; Dülger, Bilişim Suçları, s.263; Erdoğan, Bilişim Suçları, s. 117; Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 843.

[224] Koca, Mahmut/Üzülmez, İlhan, Türk Ceza Hukuku Özel Hükümler, Ankara, Adalet Yayınevi, 2018, s. 854; Akbulut, Bilişim Alanında Suçlar, s. 129.

[225] AKSS Madde 2: "Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir." https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf (Erişim Tarihi: 16.05.2022).

[226] Karakehya, "Bilişim Sistemine Girme Suçu", s. 15.

[227] "Sanığın, katılan ile internette tanıştığı ve bir süre telefonda ve msn üzerinden görüntülü görüşerek arkadaşlık yürüttüğü, sanığın teklifi üzerine katılanın, kendisi, kızı ve sanık ile birlikte bir otelde yaklaşık 1 hafta süreyle tatil yaptıkları, arkadaşlıklarının bitmesi üzerine bilahare sanığın, katılanın kullandığı **elektronik posta adresine rızası dışında birçok kez girdiği** olayda, sanığın, bu şekildeki eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu oluşturduğu…" Yargıtay 12. Ceza Dairesi E. 2015/15933 K. 2016/277 T. 13.01.2016, (https://legalbank.net/arama/mahkeme-kararlari).

rıza göstermemesine rağmen hukuka aykırı olarak sistemde kalınmaya devam edilmesi durumunda da her ne kadar sisteme giriş hukuka uygunluk sebebine dayansa da sistemde rıza dışı kalınmaya devam edilmesi bu suçu oluşturacaktır.

Sisteme girilme veya sistemde hukuka aykırı kalınmaya devam edilmesi seçimlik hareketlerinden herhangi biri ya da her ikisi gerçekleştiğinde suç tamamlanır. Suçun oluşumu için bir başka bir neticenin varlığı aranmaz. Failin girdiği sistemdeki verileri ele geçirip geçirmemesi, herhangi bir bilgi edinip edinmemesinin hiçbir önemi bulunmamaktadır.[228]

3.2.4. Suçun Manevi Unsurları

Bilişim sistemlerine girme veya kalmaya devam etme suçu doğrudan kastla işlenebilen bir suçtur. Bu suçta failin verileri elde etme, tahrip etme, yok etme, sistemden yarar elde etme gibi özel bir kastının olması gerekli değildir, genel kastın varlığı yeterlidir.[229] Bu suçun oluşması için failin başkasına ait olduğunu bildiği ve giriş izninin olmadığı bir sistemin tamamına ya da bir kısmına kendi isteğiyle girmesi, kalmaya devam etmesi yani eyleminin haksızlık teşkil ettiğinin farkında olması gereklidir.[230] Failin suç işlerken sistemi merak etme, oyun oynama, sistem güvenliğini test etme gibi saiklerle hareket etmesi durumlarında da suç oluşacaktır.[231]

Kanun koyucu suçun taksirli halini düzenlememiştir. Bu nedenle dikkatsiz ve özensiz davranışlarıyla başka bir kişinin bilişim sistemine giren kişi durumu fark eder etmez bu sistemden ayrılırsa suç oluşmayacaktır.[232]

Bilişim sistemine girme veya kalma suçunun neticesi sebebiyle ağırlaşmış halinin düzenlendiği 243. maddenin 3. fıkrasında bilişim sisteminin tamamı veya bir kısmına hukuka aykırı girilmesi veya orada kalınması fiilleri sonucunda, sistemin içerdiği verilerin yok olması veya değişmesi haline yer verilmiştir. Bu kapsamda fail yalnızca bilişim sistemine girme veya

---

[228] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6744.
"Sanıkların sübut bulan bilişim sistemindeki mağdura özel kısma girip, hakları olmadığı halde sistemde kalmaya devam etme eylemlerinin TCK'nın 243/1. maddesinde tanımlanan **bilişim sistemine girme ve mağdura ait içeriği özel elektronik iletileri okuyup, tarafı olmadıkları haberleşme içeriklerini kaydetmeleri eylemlerinin** TCK'nın 132/1. maddesindeki **haberleşmenin gizliliğini ihlal suçlarını** oluşturacağı gözetilmeden, suç vasfında yanılgıya düşülerek, sanık …hakkında TCK'nın 136/1. maddesindeki verileri hukuka aykırı olarak verme veya ele geçirme ve sanık ... hakkında TCK'nın 134/1. maddesindeki özel hayatın gizliliğini ihlal suçundan mahkumiyet kararı verilmesi,.. BOZULMASINA…"Yargıtay 12. Ceza Dairesi E. 2014/15082 K. 2015/1624 T. 02.02.2015, (https://legalbank.net/arama/mahkeme-kararlari).
[229] Parlar/Öztürk, Doğrudan ve Dolaylı Bilişim Suçları, s. 28.
[230] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 857.
[231] Taşdemir, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması Dolandırıcılık Suçları, s. 260.
[232] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 856; Kurt, Bilişim Suçları, s. 151; Yaşar/ Gökçan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6745.

sistemde kalma kastıyla hareket ederken bu eylem neticesinde en azından taksirli hareketiyle bir zarar meydana getirecektir.[233] Fail girdiği veya kalmaya devam ettiği sistemde kasten sistemdeki verileri yok eder veya değiştirirse o zaman "sistemdeki verileri yok etme" suçu oluşacaktır.[234]

3.2.5. Hukuka Aykırılık

TCK'nın 243. maddesinde suç tipi düzenlenirken açıkça hukuka aykırılık unsuru ifade edilmiştir. Bundan dolayı bu maddede hukuka özel aykırılık hali bulunmaktadır. Bu durumda failin suç eylemlerine yönelik doğrudan kastının yanında gerçekleştirdiği eyleminin hukuka aykırı olduğunu bilip bilmediği, buna göre hareket etmeyi isteyip istemediği de dikkate alınacaktır.[235] Avrupa Konseyi Siber Suç Sözleşmesi'ne dair açıklayıcı raporda da bilişim suçlarının düzenlemelerinde suç tiplerinde hukuka aykırılık unsurlarının özel olarak açıkça belirtilmesi tavsiye edilmiştir.[236] Bu suçların yargılamasında bilişim sistemine girme eyleminin hukuka aykırı gerçekleştiğinin tespit edilmesiyle suçun artık oluştuğu kabul edilecektir. Yargıtay da bir kararında hukuka uygun olarak yasal yollarla bilişim sistemine giriş sağlanması durumunda suçun unsurlarının oluşmadığı yönünde karar vermiştir.[237]

Bir başkasının bilişim sistemine girmesine rıza gösteren sistem sahibi eylemi hukuka uygun hale getirdiği için suç oluşmayacaktır. Burada önemli olan sisteme girilmeden önce ya da sisteme girilirken rızanın olmasıdır.[238] Sisteme hukuka aykırı giriş yapıldıktan sonra sistem sahibinin rızasının alınması sistemde kalmaya devam etme eyleminin oluşmasına engel olabilecek ancak bilişim sistemine hukuka aykırı girme eylemi tamamlanmış olacaktır.

Bir kişinin yerine getirdiği görevi dolayısıyla veya hukuki bir ilişkiye dayanılarak kendisine bilişim sistemine girme yetkisi verildiğinde bu kişinin görevi süresince ya da hukuki

---

[233] Çetin, Muhammet Sefa, "Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu (TCK M. 243)", Türkiye Adalet Akademisi Dergisi, C. 12, S. 45 (Ocak 2021), s. 11.

[234] Dülger'e göre failin bilişim sistemine yetkisiz olarak girip, sistemde kalmaya devam ederken sistemdeki verileri kasten yok etmesi, değiştirmesi durumunda hem 243/3 hem de 244/2. maddeleri ihlal edilmiş olacaktır. Dülger, Bilişim Suçları, s. 267.

[235] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 759.

[236] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 760.

[237] Aşamalarda tanık olarak dinlenen .'nun, katılan şirkete ait siteye yıllık ücretini yatırarak abone olduğu, sanığın tanıktan aldığı kullanıcı adı ve şifre bilgileri ile, tanığın bilgisayarından doğrudan ve TeamViewer isimli program aracılığıyla uzaktan bağlantı yoluyla katılan şirkete ait web sitesine yasal yollardan giriş yaparak, site içeriğindeki bazı bilgileri kopyaladığı, **kopyalanan bu bilgilerin sanığın çalıştığı şirkete ait internet sitesine konulduğuna dair bilgi olmadığı, dolayısıyla katılan şirkete ait siteye yasal olmayan yollardan giriş yapılmadığı**, olayın hukuki nitelikte bulunduğu, TCK.nun 243. maddesinde tanımlanan suçun yasal unsurlarının oluşmadığı gözetilmeden, sanığın beraatı yerine mahkumiyetine karar verilmesi,.. BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2014/35223 K. 2015/19051 T. 15.06.2015, (https://legalbank.net/arama/mahkeme-kararlari).

[238] Dülger, Bilişim Suçları, s. 291.

ilişki sonlanıncaya kadar bu sistemlere girmesi hukuka uygun olacaktır. Ancak görevinden ayrılan, görevine son verilen, aralarındaki hukuki ilişki son bulan veya sisteme giriş yetkisi kendisinden alınan bir kişinin daha önceden elinde bulundurduğu şifreler ile sisteme giriş yapması durumunda hukuka uygunluk sebepleri ortadan kalktığı için artık bilişim sistemine girme suçunun oluştuğundan bahsedilebilecektir. Yargıtay da çalıştığı şirketten ayrılan sanığın görevi sırasında kullandığı internet şifresini şirketten ayrıldıktan sonra kullanarak şirketin bilişim sistemine girme eyleminin TCK'nın 243/1. maddesindeki suçu oluşturduğunu kabul etmiştir.[239]

3.2.6. Suçun Neticesi Sebebiyle Ağırlaşmış Hali

Failin bir bilişim sistemine hukuka aykırı olarak girme veya kalmaya devam etme eylemi nedeniyle sistemdeki bilgiler, veriler yok olursa, tahribata uğrarsa, değişirse bu durum suçun neticesi sebebiyle ağırlaşmış halini oluşturur. Bu fıkrada dikkat edilmesi gereken durum failin kastıdır. Failin bu durumda kastı sistemdeki veri içeriklerinin değişmesi veya verileri yok etmek değildir. Fail bilişim sistemine hukuka aykırı erişim sağlama veya sistemde kalma çabasındayken dikkatsizliği, özensizliği, bilgisizliği gibi nedenlerle sistemi zarara uğratması halidir. Bu nedenle madde gerekçesinde de belirtildiği gibi bahse konu düzenleme bu suçun neticesi sebebiyle ağırlaştırılmış halidir.[240]

Bilişim sistemine hukuka aykırı olarak girme veya kalma suçunun neticesi sebebiyle ağırlaşmış hali olarak düzenlenen 243. maddenin 3. fıkrası ile 244. maddenin ikinci fıkrasında yer alan bilişim sistemindeki verileri bozma, yok etme, değiştirme suçu arasındaki ayrıma dikkat etmek gerekir. Burada en önemli nokta failin kastıdır. 244. maddenin 2. fıkrasında fail verileri yok etme, değiştirme kastıyla hareket etmektedir. Cezalandırma yapılırken verilerin failin dikkat ve özen yükümlülüğünü yerine getirmemesi sonucunda mı zarara uğradığı yoksa eylemin doğrudan verilere zarar vermeye yönelik mi olduğu değerlendirilmelidir.[241]

---

[239] Sanığın katılan şirkette çalıştığı sırada kendisine görevi nedeniyle verilen internet şifresini, iş yerinden ayrıldıktan sonra hakkı bulunmadığı halde kullanmak suretiyle katılan şirkete ait bilişim sistemine girdiği ve orada kalmaya devam ettiğini iddia ve sanığında bu iddiayı doğrulayan katılan şirkete ait **bilişim sistemine hükümsüz kalan şifresi ile girip**, buradaki şirket çalışanlarına ait maillerin kendi kurduğu siteye yönlendirmesini yapabilecek kadar süre ile kaldığını savunması karşısında; yüklenen TCK'nun 243/1. maddesindeki suçun bir bilişim sistemine hukuka aykırı olarak girmek ve orada kalmaya devam etmek unsurlarının gerçekleştiğinin kabulü ile mahkumiyetine karar verilmesi yerine yazılı şekilde beraatine hüküm kurulması," Yargıtay 11 Ceza Dairesinin E. 2009/22385 K. 2012/3683 T. 19.03.2012, (https://legalbank.net/arama/mahkeme-kararlari).

[240] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 846; Akbulut, Bilişim Alanında Suçlar, s. 148; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 859; Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 760.

[241] Dülger, Bilişim Suçları, s. 268.

Failin fiili neticesinde verinin değişmesi ya da yok edilmesi sonuçlarından birinin gerçekleşmesi suçun oluşması için yeterlidir. Önemli olan failin bu hususta kastının var olup olmadığıdır.

3.2.7. Suçun Nitelikli Halleri

243'üncü maddenin ikinci fıkrasında; *"Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir*."[242] hükmü ile hukuka aykırı bilişim sistemlerine erişim suçunda cezayı hafifletecek nitelikli hal düzenlenmiştir. Burada ifade edilen bedeli karşılığı yararlanılan sistemler kavramının kapsamında neler olduğu tartışmalıdır. Kanun koyucunun kastının bilişim sistemlerinin kullanıldığı mekanlar kapsamında olan internet kafe gibi yerlerin olmadığı, elektronik yapıda sunulan hizmetleri kapsadığı görüşünü savunan yazarlar mevcuttur.[243] Doktrindeki başka görüşlere göre ise, internet üzerinden belirli bir ücret ödenerek karşılığında hizmet satın alınan web siteleri, internet kafe gibi yerler, belli bir zaman ya da dönem sınırlamasıyla internet bağlantı servisinin sağlanması, alışveriş siteleri, elektronik kütüphaneler, Apple Store veya Google Play gibi üzerinden çeşitli yazılımlar kullanılan uygulamalar bedel karşılığı yararlanılabilen sistemler içerisinde değerlendirilmelidir.[244]

Doktrinde tartışmalı olan bir konu da bedel karşılığı yararlanılan sistemlerin neden cezayı azaltan nitelikli hal olarak düzenlendiği hususudur. Bu kavrama TCK'da ilk defa yer verilmesine rağmen, Kanun'un gerekçesinde de herhangi bir açıklamanın yapılmaması kavramın yoruma açık bir hal almasına sebep olmuştur.[245] Belirli bir ücret ödenerek girilmesi gereken bir sisteme herhangi bir ücret ödenmeksizin girilmesinin cezayı indiren bir sebep olması oldukça eleştirilmiştir.[246]

Özbek/Doğan/Bacaksız/Tepe, bedel ödenmesi gereken bir sistemde gereken bedel ödenmeden sistemin kullanılması durumunu bilişim sistemi işleticisinin sistem üzerindeki hakkının ihlali niteliğinde değerlendirerek düzenlemeyi çelişkili bulduğunu ifade etmiştir.[247]

---

[242] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf (Erişim Tarihi:16.04.2022).
[243] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 847; Erdoğan, Bilişim Suçları, s. 1399; Akbulut, Bilişim Alanında Suçlar, s. 144.
[244] Dülger, Bilişim Suçları, s. 270; Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 758; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 858.
[245] Dülger, Bilişim Suçları, s. 270.
[246] Tezcan, Durmuş/Erdem, Mustafa R./Önok, R. Murat, Teorik ve Pratik Ceza Özel Hukuku, Ankara, Seçkin Yayınları, 2010, s. 772-773.
[247] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 847

Dülger ise, bedel ödenerek kullanılan bilişim sistemlerine hukuka aykırı yollarla girilmesi durumunda iki farklı hukuksal değerin ihlal edildiğini savunmaktadır.[248] Hem suçun basit halindeki sistem güvenliğini hem de bedel karşılığında girilen sistemlerin güvenliğini ihlal edilen hukuksal değer olarak değerlendiren yazar ayrıca bilişim sisteminde hak sahibi kişinin veya sistemin ilgilisinin malvarlığının korunmasına yönelik hukuksal değerin de ihlal edildiğini düşünmektedir. Bu nedenlerle söz konusu fıkrada yer verilen hafifletici nedenin yerinde bir düzenleme olmadığı aksine suçun cezasını artırıcı bir neden olarak kanun metninde yer alması gerektiği görüşüne sahiptir. Maddedeki hükmü doğru bulmayan yazarlardan birisi olan Erdoğan, sistem sahibinin menfaatlerinin koruma altına alındığı bir düzenlemede bedel karşılığı girilebilen sistemlere bedel ödemeksizin girilmesinin indirim nedeni olamayacağını belirtir.[249]

Yaşar/Gökcan/Artuç fıkranın indirim sebebi olarak düzenlenmesini yerinde bularak madde 243'ün birinci fıkrasında suçla korunan hukuki yararın bilişim sistemlerinin güvenliği ve özel yaşamın gizliliği iken, maddenin ikinci fıkrasında korunan hukuki yararın ise malvarlığının korunması olması neticesinde kanun koyucunun bu düzenlemeyi yaptığı görüşündedir.[250]

Düzenlemede kullanılan bedel karşılığında yararlanılabilen sistem ifadesindeki bedelin dar yorumlanarak yalnızca para olarak düşünülmemesi gerekir. Geniş bir çerçevede günlük hayatımızda "karşılık" olarak değerlendirilmesi daha doğru olacaktır.[251]

Otomatlar tarafından sunulan ve yararlanılabilmesi için bedel ödenmesi gereken bir hizmetten ödeme yapmadan hizmet alınması durumu ve dekoderler TCK'nın 163. maddesinde ayrı bir suç tipi olarak düzenlenmiştir.[252]

3713 sayılı Terörle Mücadele Kanunu'nun 4.maddesi "Terör amacı ile işlenen suçlar" başlığı altında "Aşağıdaki suçlar 1'inci maddede belirtilen amaçlar doğrultusunda suç işlemek üzere kurulmuş bir terör örgütünün faaliyeti çerçevesinde işlendiği takdirde, terör suçu sayılır."[253] hükmü ile katalog suçlar sayılmış ve TCK'nın 243'üncü maddesi de bu suçlar içerisinde belirtilmiştir. Dolayısıyla bilişim sistemine girme suçunun bir örgüt faaliyeti kapsamında işlenmesi durumunda suçun cezasını artıran nitelikli bir hal gerçekleşecektir.

3.2.8. Suçun Özel Görünüş Şekilleri

[248] Dülger, Bilişim Suçları, s. 272.
[249] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1400.
[250] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6749.
[251] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 858; Dülger, Bilişim Suçları, s. 271.
[252] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1398.
[253] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf (Erişim Tarihi:02.05.2022).

3.2.8.1. Teşebbüs

5237 sayılı TCK'da yer verilen hukuka aykırı bir bilişim sistemine girme veya girilen bu sistemlerde kalmaya devam etme eylemini düzenleyen 243. maddenin 1. fıkrasında girme veya sistemde kalmaya devam etme olmak üzere iki hareket bulunmaktadır. Bu hareketlerden en az birinin gerçekleştirilmesi suçun tamamlanması için yeterli olacak herhangi bir zararın meydana gelmesi aranmayacaktır. Sırf hareket suçu olan bilişim sistemine girme suçunda başkasına ait bir sisteme hukuka aykırı olarak girilmesiyle suç oluşacaktır.[254]

24/03/2016 tarihli 6698 sayılı Kanun değişikliğinden önce suçun tamamlanması için bilişim sistemine girilmesi ve failin girdiği bu sistemde bir süre kalması gerektiği ifade edilmekteydi.[255] Bu dönemde bilişim sistemine girme suçunun teşebbüse elverişli olup olmadığı hususunda doktrinde farklı görüşler olduğu görülmektedir. Suça teşebbüsün mümkün olmadığını savunan Ketizmen'e göre; niteliği gereği birden fazla hareketli suç olarak kabul edilen bilişim sistemine girme suçunun sistemde kalma zorunluluğunu da araması, sistemde kalmaya hukuka aykırı olarak devam etme eyleminin de bölünemez olması suça teşebbüse olanak sağlamamaktadır.[256] Bu suça teşebbüsün gerçekleşebileceğini savunan görüşler de bulunmaktaydı. Kurt'a göre; bilişim sistemine girme suçunun icra hareketlerine başlayan failin kendisinden kaynaklanmayan sebeplerden dolayı suç eylemini tamamlayamadığı, sisteme hiç giremediği durumlarda suçun teşebbüs aşamasında kaldığı değerlendirilecektir.[257] Bu suçun birleşik hareketli suç olduğu nazara alınarak yapılan değerlendirmelerde ise teşebbüsün gerçekleşebilmesi için ilk hareketin tamamlanıp ikinci hareketinde icra hareketlerine başlanmış olması, bilişim sistemine girme eyleminin hiç gerçekleşmediği durumlarda suça teşebbüsün mümkün olmadığı belirtilmektedir.[258] Sisteme hukuka aykırı olarak girilip suçun

---

[254] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 859.

[255] "Şikayetçinin rızası olmadan **e-mail ve Facebook hesabına girip şifrelerini değiştirmek suretiyle bilişim sistemine girmesini engellediğinden** bahisle açılan davada; TCK.nun 243/1. maddesinde "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden…" ibaresinin yer aldığı dikkate alınarak, sanığın suçu kabul etmemesi, şikayetçinin hesabına sanığın giriş yaptığının tespit edildiği, dosya içerisinde **e-mail şifresinin değiştirilmesine dair bir tespitin bulunmadığı** gibi şikayetçi tarafından bildirilen 20.11.2012 tarihinden önceki tarihte hesaba girildiğinin tespit edilmesi karşısında, 20.11.2012 tarihinde girişi olup olmadığı, kalmaya devam ettirdiğine ve şifre değiştirdiğine ilişkin deliller tespit edilip sonucuna göre hukuki durumunun takdir ve tayini, sanığın **sadece giriş yaptığı ve kalmaya devam ettiğinin tespiti** halinde eyleminin **TCK.nun 243/1. maddesi** kapsamındaki suçu oluşturacağı gözetilmeden eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,…… BOZULMASINA…", Yargıtay 8. Ceza Dairesi E. 2016/8243 K. 2017/4158 T. 13.04.2017, (https://legalbank.net/arama/mahkeme-kararlari).

[256] Ketizmen, Bilişim Suçları, s. 108.

[257] Kurt, Bilişim Suçları, s. 262

[258] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 761; Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6751.

tamamlanmasını mümkün kılacak süre geçmeden failin iradesi dışında sistem güvenlik yazılımlarınca sistemden dışarı atılması veya elektrik kesintisi sebebiyle sistemin atması gibi durumlarında suç tamamlanamadığı için teşebbüs aşamasında kaldığı değerlendirmesini yapan yazarlar da bulunmaktaydı.[259] Yargıtay'ın bu dönemdeki görüşüne göre ise yalnızca bilişim sisteminin güvenlik sisteminin çözülerek sisteme girilmeye çalışılması veya bir an girip çıkılması gibi durumlarında suçun teşebbüs aşamasında kaldığı söylenemeyecekti.[260] Bilişim sistemine hukuka aykırı olarak giren bir kişinin kalmaya devam etmeden kendi iradesiyle bu sistemden ayrılması da yapılan değişikliklerden önce gönüllü vazgeçme kapsamında değerlendirilerek ceza sorumluluğu bulunmayacaktı.[261]

6698 sayılı Kanun değişikliğinin uygulamada karışıklığa yol açan ve tespiti oldukça güç suç eylemlerini "veya" bağlayıcıyla bağlayarak bilişim sistemine girme suçunu düzenleyen 243. maddenin birinci fıkrasını teşebbüse elverişli hale getirdiği görülmektedir. Bu değişikliklerle bilişim sisteminin tamamına veya bir kısmına hukuka aykırı girilmesiyle artık suçun tamamlandığı, failin sistemde kaldığı sürenin suçun oluşumunda etkisiz kaldığı düzenlenmiştir. Dolayısıyla failin sisteme girmeye yönelik hareketlerinin sonuca varamaması ve yarıda kalmasıyla suçun teşebbüs aşamasında kaldığı söylenebilecektir.[262] Örneğin fail, özel güvenlik sistemleri vasıtasıyla korunan bir sisteme girmeyi başaramamışsa, sisteme girmek isterken internet bağlantısının kesilmesi halinde, elektriğin kesilmesi durumunda ya da şifre gerektiren sistemlerde şifrenin çözülememesi durumlarında olduğu gibi suç tamamlanamadığında suçun teşebbüs aşamasında kaldığı değerlendirilir.[263] Yargıtay, failin e-posta adresini bildiği katılana ait facebook hesabına yetkisiz erişim sağlamaya çalıştığı ancak katılanın durumu fark etmesi üzerine girişiminin olumlu sonuçlanamadığı durumda bilişim sistemine girmeye teşebbüs suçunun oluştuğuna karar vermiştir.[264]

---

[259] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 847.

[260] "TCK.nun 243/1. maddesinde "bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden…" ibaresinin yer aldığı, suçun oluşabilmesi için, bilişim sistemine girilmesi ve orada bir süre kalınmasının gerektiği, somut olayda, katılanın mail adresi ile giriş yaptığı facebook sayfasına **şifre denemesi ile sanığın girmeye çalıştığı ancak giremediği** anlaşıldığından, suçun yasal unsurlarının oluşmaması nedeniyle beraatı yerine yazılı şekilde mahkumiyetine karar verilmesi,……BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2015/16089 K. 2016/4011 T. 28.03.2016, (https://legalbank.net/arama/mahkeme-kararlari).

[261] Mahmutoğlu, "TCK'da Bilişim Alanında Suçlar", s. 864.

[262] Akbulut, Bilişim Alanında Suçlar, s. 150.

[263] Özsoy, Nevzat, "Yargıtay Kararları Işığında Doğrudan Bilişim Suçları", Yaşar Hukuk Dergisi C. 1, S. 2 (2019), s. 310.

[264] "Katılana ait facebook hesabına erişim sağlayarak bu hesabın şifresini değiştirmek suretiyle bu hesaba erişimini engellediğinden bahisle açılan davada, sanığın "aleyhimde yazılar paylaştığını duyunca bende facebook hesabına e-posta adresini bildiğim için gizli sorusunu tahmin ederek hesabına erişim yapmaya çalıştım ancak başarılı olmadım," şeklindeki savunması, Facebook'un mesajla bildirimi üzerine durumu farkeden katılanın facebook hesabını kullanamaması üzerine kurtarmak için güvenlik sorusunu cevaplayıp şifreyi değiştirip hesabını

TCK'nın 243. maddesinin 1. fıkrasında düzenlenen seçimlik hareketlerden olan sistemde kalmaya devam etme suçunun teşebbüse elverişli olmadığı değerlendirilmektedir.[265] Çünkü sistemin bütününe veya sadece bir kısmına hukuka aykırı girilmesi durumunda suç tanımındaki eylemlerden biri gerçekleşeceğinden suçun tamamlandığı kabul edilmektedir. Hukuka uygun olarak bilişim sistemine giren kişi daha sonra sistemde kalmasına izin verilmemesine rağmen kalmaya devam ederse suç tamamlanmış olacaktır.

1997 tarihli TCK Tasarısı'nda bilişim sistemine girme suçlarında teşebbüs haline ayrı bir fıkra ile yer verildiği görülür.[266] Bu maddeye göre; failin bilişim sistemlerine girme eyleminin tamamlanamadığı, teşebbüs aşamasında kaldığı durumlarda suçun tamamlandığı ve failin tamamlanan suç ile cezalandırılacağı hükmüne yer verildiği görülmektedir. Tasarıdaki teşebbüs hükmü 2000 tarihli tasarıda 345. maddede ve 2003 tarihli tasarıda 346. maddede yer almıştır.[267] 1997 yılından itibaren ceza kanunu tasarılarında bilişim sistemine girme suçu içinde yer verilen teşebbüs hükmünün kanunlaşırken metne alınmadığı görülmektedir.

Bilişim sistemine girme veya kalmaya devam etme eylemi neticesinde sistemdeki verilerin yok olması ya da değişmesi durumunu düzenleyen TCK'nın 243/3. fıkrasındaki neticesi sebebiyle ağırlaşmış hali için teşebbüs değerlendirmesi yapılacak olursa; failin en azından taksirli hareketiyle verilerin yok edilmesi veya değiştirilmesiyle netice gerçekleşeceğinden teşebbüsten bahsedilemeyecektir.[268]

3.2.8.2. İştirak

5237 sayılı TCK'nın 243. maddesinde düzenlenen bilişim sistemlerine girme veya sistemde kalma suçu iştirak bakımından farklılıklar göstermemektedir ve bu suça iştirakin her türlüsü mümkündür.[269] İştirake ilişkin Türk Ceza Kanunu'nun 37. maddesi ile 40. maddesi

---

kurtardığını beyan etmesi, bilirkişi raporu içeriğinden, her ne kadar katılanın hesabına erişimi bir süre engellenmiş ise de henüz şifreyi tespit edemediğinden hesaba giremediği, katılanın müdahalesi sonucu girişiminin sonuçlanamaması ve bilişim sistemindeki verileri bozma, yok etme, değiştirme veya erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme eylemlerinin gerçekleşmediğinin anlaşılması karşısında, sanığın eyleminin **bilişim sistemine girmeye teşebbüs** suçunu oluşturup oluşturmayacağının karar yerinde tartışılmaması,…BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2016/11922 K. 2017/6655 T. 07.06.2017, (https://legalbank.net/arama/mahkeme-kararlari).

[265] Akbulut, Bilişim Alanında Suçlar, s. 151; Dülger, Bilişim Suçları, s. 300; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 860.

[266] "347. madde: "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve yüzmilyon liradan üçyüzmilyon liraya kadar ağır para cezası verilir. Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Akbulut, Bilişim Alanında Suçlar, s. 113., dipnot. 299.

[267] Akbulut, Bilişim Alanında Suçlar, s. 113-114.

[268] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 849.

[269] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6751.

arasında yer alan genel hükümler uygulanacaktır.

Bilişim sistemine girme suçunu işleyebilmek için yeterli teknik bilgi ve donanıma sahip olmayan bir kişi, eylemi gerçekleştirmek için başkasını ikna ederse bilişim sistemine girip suçu gerçekleştiren kişi fail olarak cezalandırılırken, diğer kişi ise TCK'nın 38.maddesi kapsamında azmettiren olarak sorumlu olacaktır.[270]

Bilişim sistemlerine girme veya sistemde kalma suçunun hem sisteme girme fiilini hem de sistemde kalma, kalmaya devam etme fiillerini içeren seçimlik hareketli bir suç olduğundan bahsedilmişti. Eğer sistemde kalmaya devam etme eylemiyle bu suç işleniyorsa mütemadi suç olacağından temadinin son bulma anına kadar suça iştirakin mümkün olacağı değerlendirilmektedir.[271]

Ceza Kanunu'nda düzenlenen bazı suçlar herkes tarafından işlenemeyen faillerinin belirli kişiler olması şartı aranan suçlardır. Bu suçlara "özgü suçlar" adı verilmektedir. Bilişim sistemine girme suçunda suç işleyen kişiye yönelik aranan bir unsur bulunmamakta özgü suç olarak değerlendirilmemektedir. Ancak bu suç tipinin işlenme yöntemleri incelendiğinde bazı durumlarda faillerin teknik bilgi ve donanıma sahip olması gerektiği ortaya çıkmaktadır. Bu gibi durumlarda cebir ve tehdit kullanılarak bilişim sistemleri konusunda teknik bilgili bir kişinin başkasına ait bilişim sistemine girmesi için zorlanması mümkündür. Suçun işlenmesinde başkasını araç olarak kullanan ve suçu işlemesi için zorlayan kişilerin bu suçun dolaylı faili konumunda olacağı söylenebilecektir.[272]

3.2.8.3. İçtima

Suçların içtima konusu TCK'nın genel hükümlerinde 42, 43 ve 44. maddeleri ile düzenlenmiştir. Bilişim sistemlerine girme suçunda içtima hususunda ilk değerlendirme zincirleme suçun mümkün olup olmayacağıdır. Failin aynı kişiye karşı değişik zaman dilimlerinde, aynı suç işleme kararıyla hukuka aykırı olarak bilişim sisteminin tümüne ya da sistemin sadece bir kısmına girmesi veya bu sistemde kalmaya devam etmesi durumunda zincirleme suç hükümlerinin uygulanıp uygulanamayacağının tartışılması gereklidir. [273]

Bir bilişim sistemindeki veriyi öğrenmek amacıyla sisteme giren failin; hatların kesilmesi

---

[270] Karakehya, "Bilişim Sistemine Girme Suçu", s. 20.
[271] Dülger, Bilişim Suçları, s. 301.
[272] Karakehya, "Bilişim Sistemine Girme Suçu", s. 20.
[273]"Kabule göre de; sanığın **tespit edilen IP ile suç tarihinde bir kez girdiği ve kaldığı** anlaşılmasına rağmen hakkında zincirleme suç hükümleri uygulanarak fazla ceza tayini,… BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2016/4823 K. 2016/10704 T. 23.11.2016, (https://legalbank.net/arama/mahkeme-kararlari).

nedeniyle sistemden atılıp ardı ardına sisteme giriş yaptığı durumda, kısa aralıklarla ve aynı suç işleme kararıyla sisteme giriş yaptığı bu nedenle tek suçtan mahkûmiyet kurularak zincirleme suç hükümleriyle cezasının artırılacağı değerlendirilmektedir.[274] Burada dikkat edilmesi gereken en önemli nokta failin sisteme ilk hukuka aykırı girdiği zaman dilimiyle diğer girişleri arasında geçen zaman aralıkları ve aynı suç işleme kararıdır. Aynı suç işleme kararının mümkün olamayacağı kadar uzun zaman aralıklarıyla sisteme giriş yapıldığı ve sistemde kalmaya devam edildiği durumlarda failin aynı suçu gerçekleştirme kararı ile hareket ettiği söylenemeyecek ve her hareket için ayrı ceza verilecektir.

Günümüzde Yargıtay'ın uygulamaları incelendiğinde TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme suçunda zincirleme suç hükümlerinin uygulama alanı bulduğu görülmektedir.[275] Failin tek bir eylemiyle birden fazla bilişim sistemine girmesi durumunda aynı neviden fikri içtima hükümleri de uygulanabilecektir. [276] Fail birden fazla kişiye aynı e- posta veya link ile gönderdiği bilişim virüsü, truva atı gibi yazılımlarla bilişim sistemlerine hukuka aykırı erişim sağlayabilecektir. Bu gibi durumlarda bilişim sistemine izinsiz girilen her bir kişi için ayrı suç oluşmayacak, tek bir bilişim sistemine girme suçu TCK'nın 43.maddesinin 2. fıkrası gereği temel cezasında artırım yapılarak uygulanacaktır. Suça konu bilişim sisteminde birden fazla sistem sahibi olması durumunda, örneğin hukuka aykırı girilen bilişim sisteminin mülkiyeti ortak birden fazla sahibinin olduğu hallerde tek bir suç oluşacağı kabul edilmektedir.[277] Fail hukuka aykırı olarak bir bilgisayar sistemine girip sistemdeki dosyalara ulaşabilir. Bu gibi durumlarda bilgisayar sahibi ile erişilen verilerin sahipleri farklı kişiler olması halinde her ikisi de suçun mağduru olacak, diğer koşullarında varlığı halinde failin cezasında TCK'nın 43/2. fıkrası gereği artırım yoluna gidilebilecektir.[278]

TCK'da yer alan bilişim suçlarının birçoğu bilişim sistemlerine girme veya kalma eylemlerini mecburen gerektirmektedir. Bu durum hem 243. madde ile düzenlenen suçun hem de sübut verdiği kanunda tanımlı diğer bilişim suçunun oluşmasına neden olacaktır. Bilişim

---

[274] Dülger, Bilişim Suçları, s. 302.

[275] "Sanığın, mağdura ait elektronik posta hesabına, bir suç işleme kararının icrası kapsamında **üç kez izinsizce giriş** yapması biçiminde sübutu kabul edilen eyleminin, **zincirleme şekilde TCK'nın 243/1. maddesinde** tanımlanan bilişim sistemine girme suçunu oluşturduğu gözetilmeden, anılan suçtan dolayı hakkında suç duyurusunda bulunulan sanığın, yasal ve yeterli olmayan yazılı gerekçelerle TCK'nın 134/1. madde ve fıkrasındaki özel hayatın gizliliğini ihlal suçundan mahkumiyetine karar verilmesi,…BOZULMASINA…" Yargıtay 12. Ceza Dairesi E. 2016/5905 K. 2017/7072 T. 04.10.2017, (https://legalbank.net/arama/mahkeme-kararlari).

[276] Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1418.

[277] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6751.

[278] "Bir kimsenin kişisel dosyasını arkadaşının bilgisayarında muhafaza ettiği hallerde, bu bilgisayara girilerek söz konusu dosyaya ulaşılması halinde, hem bilgisayarın sahibine hem de veri sahibine karşı suç işlenmiş olur. Bu ihtimalde diğer koşulları da varsa TCK. m.43/2 uygulanmalıdır." Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 761; Aynı görüşte Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1418.

sistemine girme suçu ile diğer suçlar arasındaki içtima konusunda doktrinde çeşitli tartışmalar bulunmaktadır.

Bu tartışmalardan ilki bilişim sistemine girme suçunun geçit suç niteliğinde olup olmadığına yöneliktir. Doktrinde yazarların büyük bir kısmı geçit suç kurumunu kabul etmesine rağmen bir kısmının da farklı görüşlerde oldukları görülmektedir. Örneğin, bilişim sistemindeki verileri bozmak, yok etmek veya değiştirmek isteyen bir kimsenin TCK'nın 244. maddesindeki bu eylemi gerçekleştirebilmesi için öncelikle bilişim sistemine girmesinin gerekli olduğu görülmektedir. Örnekteki gibi bir durumla karşılaşıldığında TCK'nın 243. maddesinin mi yoksa 244'üncü maddesinin mi uygulanacağı hususunda çeşitli görüşler bulunmaktadır.

Özbek/Kanbur/Doğan/Bacaksız/Tepe TCK'nın 243. maddesi ile 244. maddesinin 2. fıkrası arasında geçit suçunun oluşabileceğini ancak bu kurumu kabul etmediklerini, sorunun failin kastına göre çözülmesi gerektiğini ifade etmiş, sorunun çözümüne yönelikte önerilerde bulunmuştur. Buna göre; 243. maddenin 1.fıkrası suçun temel şekli olarak düzenlenerek 243. ve 244. maddelerin birleştirilmesi diğer hallerinde nitelikli hal olarak düzenlenmesi önerilmiştir.[279] Failin başlangıçta kastı hukuka aykırı olarak sisteme girilip, kalmaya devam etme eylemiyken, kastını değiştirip sistemdeki verileri bozup, yok etmesi durumunda hukuka aykırı sisteme erişim fiili, verileri değiştirme suçunun unsuru haline gelecek ve yalnızca 244.maddenin 2.fıkrasından cezalandırılması gerekecektir. Bir diğer görüş ise; bu durumlarda fikri içtima kuralının uygulanarak failin cezası daha ağır olan suçtan cezalandırılması gerektiği yönündedir.[280]

Dülger ise diğer yazarlardan farklı bir görüşe sahiptir; ne geçit suçu uygulamasına ne de fikri içtima uygulamasına katılmamaktadır. Geçit suçu kurumunun uygulanmasının şartlarının bu suç tipinde oluşmaması nedeniyle uygulanamayacağını, 244.maddedeki suçun da sisteme girme, sistemde kalma suretiyle işlenmesi dolayısıyla tek fiilden söz edilemeyeceği neticeten de fikri içtima kuralının uygulanamayacağını savunmaktadır.[281] Suça konu eylemler arasında zamansal açıdan yakınlık bulunursa 244.maddenin 2. fıkrasından, zamansal açıdan yakınlık olmayıp farklı suç işleme kasıtlarıyla eylemlerin gerçekleştiği kabul edilirse de oluşan her iki suçtan ayrı ayrı hüküm kurulması gerektiği görüşüne sahip olduğu görülmektedir.[282]

Bazı yazarlar ise bilişim sistemine girme eyleminin amaç suça ulaşmada kullanılan bir araç suç olduğu, amaç suçun unsuru veya suçun temel cezasını artıran nitelikli durumlar içinde

---

[279] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 850.
[280] Akbulut, Bilişim Alanında Suçlar, s. 152; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s.861; Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", s. 1420.
[281] Dülger, Bilişim Suçları, s. 305.
[282] Dülger, Bilişim Suçları, s. 305.

bilişim sistemine girme eylemi düzenlenmişse artık yalnızca amaç suçtan cezalandırma yapılması gerektiği savunulur.[283] Failin bilişim sistemlerine yetkisiz girmesiyle işlenen dolandırıcılık ve hırsızlık suçlarında, sisteme girme eylemi araç suç oluşturacağından yalnızca amaç suçtan ceza verilecektir.

Bizim görüşümüze göre de bilişim sistemlerine girme eylemi geçit suçu niteliğindedir. Bu suç failin hedeflediği başka bir suça ulaşmasının zorunlu sonucu olarak görülür. Bu durumlarda gerçek içtima kuralı gereğince TCK'nın hem 243. maddesinin hem de 244. maddesinin oluştuğu söylenemeyecek yalnızca sistemi engelleme bozma suçları oluşacaktır.

Bilişim sistemleri kullanılması suretiyle hırsızlık, bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık gibi suçların bilişim sistemlerine girilerek işlenmesinin zorunlu olduğu durumlarda bileşik suç söz konusudur ve fail yerine göre nitelikli hırsızlık veya nitelikli dolandırıcılıktan cezalandırılacaktır.[284] Uygulamada Yargıtay'ın da aynı yönde kararlar verdiği görülmektedir.[285]

3.2.9. Veri Nakillerini Sisteme Girmeksizin Teknik Araçla İzleme Suçu

2016'da 6698 sayılı Kanun'un 30. maddesi ile mevzuatımıza giren veri nakillerini bilişim sistemine girmeksizin teknik araçlarla hukuka aykırı izleme suçu [286], TCK'nın 243. maddesine 4. fıkra olarak eklenen yeni bir düzenlemedir. Bu suç tipine yönelik en önemli eleştiri kanunda düzenlendiği madde başlığıyla uyumsuz olmasıdır. Doktrindeki yaygın olan ve bizimde katıldığımız görüş bu fıkranın 243.maddede bilişim sistemine girme suçu başlığı altında yer almaması, sisteme girme suçundan tamamen bağımsız ayrı bir suç tipi olarak düzenlenmesi

---

[283] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6752. ; Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 761

[284] Mahmutoğlu, "TCK'da Bilişim Alanında Suçlar", s. 864.

[285] "Sanığın bilişim sistemini kullanarak www.kontör burada.net adlı **siteye şifresini ele geçirmek suretiyle girip, kendine ait iki hatta kontör yüklemesi şeklindeki eyleminde** kastının malvarlığına yönelik olması nedeniyle, **eyleminin TCK'nun 142/2-e maddesine uyan tek suç oluşturduğu gözetilmeyerek,** ayrıca TCK 243/1. maddesinden yazılı şekilde mahkumiyetine karar verilmesi,…BOZULMASINA…" Yargıtay 22. Ceza Dairesi E. 2015/3457 K. 2015/2550 T. 24.06.2015, (https://legalbank.net/arama/mahkeme-kararlari).
"Müştekiye ait banka hesabına, internet üzerinden ulaşılarak, **EFT yoluyla başka hesaplara para aktarmak** suretiyle gerçekleştirilen eylemin bir bütün halinde **TCK'nın 142/2-e** maddesinde ifade edilen hırsızlık suçunu oluşturduğu gözetilmeden sanıklar hakkında ayrıca TCK'nın 243/3. maddesindeki suçu oluşturduğundan bahisle yazılı şekilde uygulama yapılması,…BOZULMASINA…" Yargıtay 13. Ceza Dairesi E. 2014/2924 K. 2014/36282 T. 18.12.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[286] Dülger İngilizce karşılığı "interface" eylemi olan bu suçu "araya girme suçu" olarak adlandırmıştır. Dülger, Bilişim Suçları, s. 311.

gerektiği yönündedir.[287]

"*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır*."[288] şeklindeki bu fıkra AKSS 3. maddesinde[289] düzenlenen yasa dışı araya girme suçunun mevzuatımıza uyumlaştırılmasıdır.[290] AKSS'de kullanılan "yasa dışı araya girme" terimi Türk Ceza Kanunu'nda "verilerin izlenmesi" şeklinde karşılık bulmuştur. Sözleşmede düzenlenen suçlara ilişkin madde metinlerinin çeviri yoluyla birebir iç hukukta düzenlenme zorunluluğu bulunmaması nedeniyle sözleşmedeki yasa dışı araya girme suçu ile 243. maddenin 4. fıkrası arasında farklılıklar bulunmaktadır. Sözleşmede yasa dışı araya girmenin bir türü olarak bilişim sisteminden kaynaklanan elektromanyetik yayımlarda yer vermesine rağmen TCK'da bu husus düzenlenmemiştir.[291]

Günümüzde veri aktarımlarının birçoğu bilişim teknolojilerinin de gelişmesiyle bluetooth, Wi-fi gibi kablosuz iletişim araçlarıyla yapılmaktadır. 5237 sayılı TCK'da 6698 sayılı Kanunla getirilen değişikliklerin öncesinde bilişim suçlarındaki eylemler sadece sistemdeki durağan verileri hedef alarak düzenlenmişti. Bu nedenle veri aktarımları sırasında araya girme suretiyle veri elde edilmesi durumlarını karşılayacak bir kanun maddesi bulunmamaktaydı. Getirilen bu değişiklik kanun boşluğunu dolduran son derece yerinde bir düzenlemedir. Veriler üzerinde tasarruf yetkisine sahip kişilerin veri gizliliğinden kaynaklanan çıkarları ve sistemdeki verilerin güvenliği bu kapsamda korunan hukuki değerler olacaktır.[292]

Kanun'da suçun failine yönelik ve mağdura ilişkin özel nitelikler aranmamaktadır. Herkes tarafından işlenebilen özgü suç niteliğinde olmayan suçlardandır. Suçun mağduru nakledilen veriler üzerinde tasarruf yetkisi olan, verilerin ilgilisi kişidir.[293]

TCK'nın 243. madde 4. fıkrasında düzenlenen araya girme suçunun konusunu nakledilme sürecindeki veriler oluşturur. Burada dikkat edilmesi gereken nokta durağan, nakil sürecinde olmayan verilerin bu kapsamda değerlendirilemeyeceğidir. Bilişim sistemlerinin araç olarak kullanıldığı veri nakillerinde, naklin elektronik posta yoluyla mı, internetten gerçekleştirilen sesli veya görüntülü telefon görüşmesi yoluyla mı yapıldığının bir önemi yoktur.

Suçun oluşabilmesi için failin sisteme girmeksizin nakil sürecindeki verileri sisteme

---

[287] Akbulut, Bilişim Alanında Suçlar, s. 157; "Başlıkla tamamen uyumsuz olan bu suç tipinin ayrı maddede (örneğin 243/A gibi) düzenlenmesi yasa yapma tekniği açısından daha doğru olurdu." Dülger, Bilişim Suçları, s. 310.
[288] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 03.05.2022).
[289] AKSS orijinal metni için bkz; https://rm.coe.int/1680081561 (Erişim Tarihi: 09.03.2022).
[290] Çetin, "Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu", s. 23.
[291] Dülger, Bilişim Suçları, s. 312.
[292] Akbulut, Bilişim Alanında Suçlar, s. 159; Dülger, Bilişim Suçları, s. 313.
[293] Dülger, Bilişim Suçları, s. 313.

müdahalede bulunmadan teknik araçlarla izlemesi gerekir. İzleme kavramından ne anlaşılması gerektiği 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2. maddesinde, internet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi olarak tanımlanmıştır.[294] Kanun koyucu madde metninde verileri izleme hareketinin ancak teknik araçlarla yapılabileceğini açıkça belirttiğinden aksi durumlarda fiziksel olarak kişinin duyması, görmesi gibi yöntemler bu suça sübut veremeyecektir.[295] Sırf hareket suçu olarak düzenlenen veri nakillerini izleme suçunda failin sistemdeki nakil sürecini teknik araç aracılığıyla izleme eylemine başlamasıyla suç artık tamamlanmış olacaktır. Ancak failin nakli izleme süreci son buluncaya dek suç temadi edecektir.

3.2.10. Muhakeme ve Yaptırım

Bilişim sistemine girme suçunun temel halini düzenleyen 243. maddenin birinci fıkrasında faile seçimlik olarak bir yıla kadar hapis veya adli para cezası yaptırımı öngörülmüştür. Yargılama sonunda hüküm kurulurken hürriyeti bağlayıcı hapis cezası ya da adli para cezasından yalnızca biri uygulanabilecektir. Cezanın alt sınırı kanun metninde belirtilmediğinden TCK'nın genel hükmü gereği 1 ay kabul edilecektir. Yargılanan sanığın tekerrüre esas alınacak adli sicil kaydının olması durumunda ise adli para cezası seçilemeyecek hapis cezası zorunlu olacaktır. (TCK m.58/3)

Bu suçun ikinci fıkrada düzenlenen bedel karşılığında yararlanılan sistemlere yönelik işlenmesi durumunda temel ceza yarı oranına kadar indirilerek fail cezalandırılacaktır. Madde metninde kullanılan "yarı oranına kadar" ifadesi kesin bir yargı içermediği için cezanın indirim oranı her somut olayda cezaların sübjektifleştirilmesine göre belirlenecektir. Üçüncü fıkra ile düzenlenen failin sisteme girme eyleminin neticesi sebebiyle ağırlaşmış halinde ise seçimlik bir düzenlemeye yer verilmeyerek altı aydan iki yıla kadar hapis cezası öngörülmüştür. Maddenin son fıkrasında yer alan araya girme suçunun işlenmesi durumunda ise fail bir yıldan üç yıla kadar hapis cezası ile cezalandırılacaktır.

Tüzel kişiler bilişim sistemine girme suçunun işlenmesi neticesinde kendi yararlarına hukuka aykırı bir menfaat elde ediyorlarsa TCK'nın 246. maddesi gereği güvenlik tedbirine

[294] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf (Erişim Tarihi: 04.05.2022).
[295] Akbulut, Bilişim Alanında Suçlar, s. 165.

tabi olacaklardır.

5237 sayılı TCK'da 243. maddede düzenlenen bilişim sistemine girme suçunda yargılamada görevli mahkeme *5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun* ile belirtilmiştir. Bu Kanun'un 12. maddesinde ağır ceza mahkemelerinin görevine giren suçlar sayılmış, 11. maddesinde asliye ceza mahkemelerinin görevleri belirtilirken de ağır ceza mahkemeleri ile sulh ceza hakimliğinin görevi dışında kalan suçlar olduğu belirtilmiştir. Bu maddeler ışığında 243. maddenin 1. fıkrasında suçun temel cezayı gerektiren hali, ikinci fıkrasında cezayı azaltan nitelikli hali, üçüncü fıkrasında neticesi sebebiyle ağırlaşmış hali ve son fıkrasında ise araya girme suçları bakımından görevli mahkeme asliye ceza mahkemeleri olacaktır. Mağdurun şikâyetine tabi olmayan bilişim sistemine girme suçları re'sen takip edilmektedir.

Tablo 1. TCK m.243 (Soruşturma Verileri)

TCK m.243	Cumhuriyet Başsavcılıkları Soruşturma Dosya Sayısı	Kovuşturmaya Yer Olmadığı	Kamu Davası Açılan	Yetkisizlik	Görevsizlik
2021	16 632	13 819	851	1 716	3
2020	10 484	8 523	573	1 242	4
2019	9 442	7 276	883	1 102	6
2018	11 437	9 372	680	1 205	-
2017	10 004	7 761	707	1 312	1

Kaynak: https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi

Yukarıdaki tabloda bilişim sistemine girme suçuyla ilgili 2017 ile 2021 yılları arasında tüm Türkiye'deki Cumhuriyet Başsavcılıklarında yürütülen soruşturma dosya sayılarına dair istatistiksel veriler belirtilmiştir. Veriler incelendiğinde özellikle de 2021 yılındaki soruşturma sayısında önceki yıllara oranla belirgin bir artış görülmektedir. Ayrıca her yılın toplam soruşturma sayıları incelendiğinde Cumhuriyet Başsavcılıklarınca KYOK'ların toplam soruşturma sayısına oranla fazlalığı dikkat çekmektedir.

Kanaatimizce bu durumun sebeplerinden biri suça sürüklenen çocuklar yönünden bilişim sistemine girme suçunun uzlaştırma kapsamında olmasıdır. 2016 yılında yürürlüğe giren 6763 Sayılı Kanun'la suça sürüklenen çocukların üst sınırı üç yılı geçmeyen suçları mağdur veya suçtan zarar görenin gerçek kişi ya da özel hukuk tüzel kişisi olması şartıyla uzlaştırmaya tabi tutulmuştur. İnceleme konumuzu oluşturan 243. maddenin de cezasının üst sınırının üç yıl hapis olması dolayısıyla suça sürüklenen çocukların eylemleri uzlaştırma kapsamında kalacaktır. Soruşturma aşamasında mağdur ile uzlaşmanın sağlanması durumunda da KYOK kararı verilecektir.

Bir diğer sebebin de suç eylemlerinin yöneldiği bilişim sisteminin yer sağlayıcısıyla ilgili olabileceğini düşünmekteyiz. Hukuka aykırı girilen sistemin bir mail adresi veya sosyal medya hesabı olması durumunda mağdurun sistemine erişim sağlayan IP adresi ve zaman bilgisinin bildirilmesi yer sağlayıcısından talep edilmektedir. Ancak 2017 yılından itibaren Türkiye'de yer sağlayıcı olmayan sosyal ağların internet sitelerinin yasal temsilcilikleri IP paylaşımlarını belirli koşullarla sınırlamışlardır. Yalnızca insan hayatını tehdit eden durumlar ve çocuklara karşı işlenen suçlarda IP paylaşımı yapılmaktadır. Uygulamada bu gibi bilgi paylaşımı yapılmayan durumlarda başka türlü delil elde etme imkanının bulunmaması hallerinde doğrudan KYOK kararı verildiği görülmektedir.

Bilişim suçlarına ilişkin yargılamaların doğru yapılabilmesi için hakimlerin hukuki bilginin yanı sıra teknik bilgiye de sahip olmaları gerekmektedir. Bu teknik bilgiye duyulan gereksinim hakimlerin eğitilmesi ve mahkemelerde ihtisaslaşma ihtiyacını doğurmaktadır. Bu nedenlerle Hakimler ve Savcılar Kurulu (HSK) 1229 sayılı ihtisas kararını yayınlamıştır. 15 Aralık 2021 tarihinden itibaren TCK'nın 243. maddesinde düzenlenen bilişim sistemine girme suçlarına HSK'nın belirlediği ihtisas mahkemeleri bakmakla görevlendirilmiştir.[296]

[296] "Asliye ceza mahkemesinin görev alanına giren suçlar yönünden;
a) İki asliye ceza mahkemesi bulunan yerlerde 2 numaralı,
b) Üç, dört veya beş asliye ceza mahkemesi bulunan yerlerde 3 numaralı,
c) Altı, yedi, sekiz veya dokuz asliye ceza mahkemesi bulunan yerlerde 6 numaralı,
d) On veya daha fazla (yirmi beşten az) asliye ceza mahkemesi bulunan yerlerde 8 numaralı,
e) Yirmi beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20 ve 21 numaralı,

Bilişim sistemine girme suçunda yetkili savcılık ve mahkeme belirlenirken kanunda özel bir yetki kuralına yer verilmemesi nedeniyle kararsızlıklar yaşandığı görülmektedir. Bir bilişim suçu işleyen kişinin evinde bilgisayarının başında otururken başka bir şehirde suç işleyebilmesi alışılagelmiş durumlar arasında değerlendirilmemektedir. Yaşanan bu yetki kararsızlıklarının yargılamalarda yavaşlama ve delil kayıpları sorununu doğurduğu görülmektedir. Kural olarak yetkili mahkeme Ceza Muhakemeleri Kanunu'nun 12. maddesinde düzenlenen genel yetki kuralına göre belirlenecektir. Bu maddeye göre; suç nerede işlenmişse yetkili mahkeme o yer mahkemesi olmalıdır.

Genel yetki kuralı bilişim sistemine girme suçu bakımından ele alındığında bilişim sistemine hukuka aykırı olarak girilen yer ve sistemde kalınan yer mahkemeleri yetkili olacaktır. Yani hukuka aykırı girme veya kalma hareketinin gerçekleştiği failin fiziki olarak bulunduğu yer ile girilmesi amaçlanan bilişim sisteminin bulunduğu yer mahkemeleri yetkili olacaktır.[297] Günümüzde yetki belirlenirken suça konu bilişim sisteminin bulunduğu yer savcılık ve mahkemelerinin yetkisi hususunda uygulama birliği sağlandığı görülmektedir.[298]

Mekânsız suçlar olarak da anılan bilişim suçları ulusötesi suç niteliğindedir. Ancak bu suçların yargılamasının Türkiye'de yapılabilmesi için TCK'nın 8. maddesi gereği suç oluşturan eylemlerin bir kısmının veya tamamının Türkiye'de gerçekleşmesi ya da neticenin burada gerçekleşmesi gereklidir.

Yabancı bir ülkede bilişim sistemine girme suçu işleyen Türk vatandaşı Türkiye'de yargılanamayacaktır. Çünkü Türk kanunlarına göre yargılamayı düzenleyen TCK'nın 11. maddesinde kovuşturulabilirlik koşulu aranmış, 14. maddesinde ise suçun soruşturma ve kovuşturmaya tabi olabilmesi için bilişim sistemine girme suçunda öngörülen hapis ve adli para cezası gibi seçimlik ceza öngörülmemesi gerektiği hükme bağlanmıştır. TCK'nın 243.maddesi 2. fıkrası içinde aynı uygulama geçerliyken aynı maddenin 3. fıkrasında durum farklıdır. Bu halde Türkiye'de yargılama yapılabilmesi suçtan zarar gören kimsenin ya da yabancı hükümetin şikâyetine tabi olacaktır.[299]

---

f) Otuz beş veya daha fazla asliye ceza mahkemesi bulunan yerlerde 20, 21 ve 22 numaralı asliye ceza mahkemelerinin bakmasına…" https://www.hsk.gov.tr/Eklentiler/30112021092825112021-1229pdf.pdf (Erişim Tarihi:15.09.2022).

[297] Akbulut, Bilişim Alanında Suçlar, s. 156.

[298] Dülger, Bilişim Suçları, s. 308.

[299] Akbulut, Bilişim Alanında Suçlar, s. 155.

Tablo 2. TCK m. 243 Ceza Mahkemelerinde Sanıkların Yaş ve Uyruk Dağılımı

TCK m.243	Toplam Sanık Sayısı	Yabacı Uyruklu	12-14 Yaş	15-17 Yaş	18+ Yaş
2021	821	23	24	33	739
2020	526	6	17	22	481
2019	671	11	20	53	585
2018	634	5	20	47	561
2017	547	10	28	19	489

Kaynak: https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi

Ülkemizde bilişim sistemine girme suçuyla ilgili olarak ceza mahkemelerinde açılan davalarda sanıkların uyruk ve yaş grubu verileri incelendiğinde, 2017-2021 yılları arasında 12-14 yaş aralığı ile 15-17 yaş aralıklarındaki suça sürüklenen çocuk sayıları dikkate alındığında yıllara göre belirgin bir artış görülmemektedir. İnternet kullanımının oldukça popüler olduğu bu yaş gruplarında bilişim sistemine girme suçuna yönelimin 18 yaş üstü kişilere göre oldukça az olduğu görülmektedir. Bu durumun sebebi suça sürüklenen çocuklar açısından uzlaşmaya tabi olan bu suçun soruşturma aşamasında uzlaşmayla neticelenmesi ve kovuşturma aşamasına geçen dosya sayısının bu nedenle azalması olabilir. Yine verilere göre yabancı uyruklu kişilerin 2021 yılında bir önceki yıla oranla daha fazla TCK'nın 243. maddesi kapsamında suç işledikleri görülmektedir.

3.3. Bilişim Sistemini Engellenme, Bozma, Verileri Yok Etme veya Değiştirme Suçu

3.3.1. Genel olarak

TCK'nın bilişim alanında suçları düzenleyen onuncu bölümünde bilişim sistemine girme suçundan sonra yer verilen 244. maddesi;

"(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."[300] biçiminde düzenlenmiştir.

Kanun koyucu maddenin ilk iki fıkrasında suç tiplerini düzenlemiştir. Aslında iki ayrı suç tipi olan birinci ve ikinci fıkra düzenlemelerine aynı madde içerisinde yer verildiği görülmektedir. Birinci fıkrada sistemin işleyişinin engellenmesi ve bozulmasına ilişkin eylemler yaptırıma bağlanmışken, ikinci fıkrada sistemdeki verilerle ilgili birtakım eylemlerin cezalandırılması düzenlenmiştir. Üçüncü fıkrada ise cezayı artıran nitelik hal düzenlemesi yapılmıştır. Son olarak dördüncü fıkrada tanımlanan suçun başka suç mu yoksa yukarıda düzenlenen fıkraların nitelikli hali mi olduğu hususunda doktrinde tartışmalar mevcut olup görüş birliği sağlanamamıştır.

TCK'nın 244. maddesinin kanunlaşma sürecini incelediğimizde; Adalet Komisyonu tarafından kabul edilip TBMM Genel Kurulu'na getirilen madde metni ile Genel Kurul'da kabul edilip yürürlüğe giren metninin aynı olmadığı görülmektedir.[301] Meclise sunulan tasarı metninde 244. maddenin birinci ve ikinci fıkralarındaki iki farklı suç tipinin birleştirilerek birinci fıkrada düzenlendiği, bu iki ayrı suç için tek bir ceza öngörüldüğü ve maddenin toplamda üç fıkradan oluştuğu görülmektedir.[302] Verilen değişiklik önergesiyle madde metni dört fıkra biçiminde, bilişim sistemine yönelik eylemler ile sistemdeki verilere yönelik eylemler ayrı fıkralarda olacak şekliyle yürürlükteki halini almıştır.

---

[300] https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (Erişim Tarihi: 04.05.2022).

[301] Bu fıkranın TBMM Adalet Alt Komisyonunda kabul edilen metni şu şekildeydi: "(1) Bir bilişim sisteminin işleyişini engelleyen, bozan, sisteme hukuka aykırı olarak veri yerleştiren, var olan verileri başka bir yere gönderen, erişilmez kılan, değiştiren, yok eden kimseye bir yıldan üç yıla kadar hapis cezası verilir." Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 866, dipnot: 71.

[302] Dülger, Bilişim Suçları, s. 340.

765 sayılı TCK'da 525/b maddesinin 1.fıkrasında yer alan düzenlemenin 5237 sayılı TCK'da 244. maddeyi kısmen karşıladığı söylenebilir. 765 sayılı TCK'da ki hükümde suç oluşturan eylemlerin bir kimseye zarar vermesi veya bir menfaat elde edilmesi amacıyla gerçekleşmesi gerekliyken 244. maddenin bu düzenlemeden en önemli farkı kanun metninden bu hususların çıkarılmış olmasıdır. Ayrıca daha önce kullanılmayan "verileri erişilmez kılma" terimi, "sisteme veri yerleştirme" kavramı ve "var olan bir veriyi başka yere gönderen kişi" tabirine 244. madde de ilk defa yer verildiği görülür. Avrupa Siber Suç Sözleşmesi'nin verileri etkileme başlıklı 4. maddesi ve sisteme etki etme başlıklı 5. maddesindeki düzenlemelerine TCK'nın 244.maddesinde sözleşmeye uygun olarak aynı doğrultuda yer verilmeye çalışılmıştır.[303]

3.3.2. Suçla Korunan Hukuki Değer

Doktrinde TCK'nın 244. maddesi ile korunan hukuksal değerin mahiyeti hususunda bir görüş birliği bulunmamaktadır.

Bazı yazarlara göre; bu suçla korunan iki esas hukuki değer bulunmaktadır. Buna göre ilk olarak düzenlemenin birinci ve ikinci fıkralarının odağında bilişim sistemleri ve sistemdeki veriler olması sebebiyle bilişim sistemi ve verilerin güvenliğinin korunduğu, ikinci olarak da söz konusu eylemler bilişim sistemi ve verilerin üzerinde tasarruf yetkisine sahip kişilerin alanına tecavüz niteliğinde olduğu için mülkiyet hakkını koruduğu söylenebilir.[304]

Yazıcıoğlu'nun görüşüne göre ise, bu suçun koruduğu hukuki değer karma bir nitelik taşımakta verilerin mal kapsamında düşünülemeyecek olmasından dolayı hükmün birinci fıkrası bilişim sistemlerinin düzenli işleyişini korumakta, ikinci fıkrası ise veri güvenliğini sağlamaktadır.[305]

---

[303] AKSS madde 4: "Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, 1. paragrafta tanımlanan fiillerin ciddi zararla sonuçlanması gerektiğini şart koşma hakkını saklı tutabilir."
AKSS madde 5: "Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir." Akbulut, Bilişim Alanında Suçlar, s. 177.
[304] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 853.
[305] Yazıcıoğlu, Bilgisayar Suçları, s. 258.

Ketizmen ise; olaya daha farklı bir yaklaşımla bilişim sistemi ve verilere müdahalenin aslında bir mala zarar verme suçunu oluşturduğu bu doğrultuda mala zarar verme suçunun koruduğu hukuki değerle aynı yönde olması gerektiği görüşünü savunmaktadır.[306]

Kurt'a göre 244. maddenin ilk fıkrası bilişim sisteminde tasarruf yetkisi sahibinin mülkiyet hakkı, sistem dokunulmazlığı, bilişim teknolojilerinin gelişme özgürlüğünü korunmakta, ikinci fıkrası ise kabul edilen oluşa göre mülkiyet hakkı, ticari sır, fikri mülkiyet hakkı, özel hayatın gizliliği gibi hakları korumaktadır.[307] Dülger de suçla korunan hukuki değerin karma nitelik taşıdığını, bu suç tipiyle hem bilişim sisteminin hem de sistemdeki verilerin sağlam ve güvenli çalışabilirliğinin korunacağı kanaatindedir.[308]

5237 sayılı TCK'nın 244. maddesinde iki ayrı suçun düzenlenmesi nedeniyle korunan hukuksal değerlerin aynı olmadığını ve iki ayrı değerlendirme yapılmasını ifade eden Akbulut' a göre; maddenin birinci fıkrasında korunan hukuki yarar, bilişim sistemlerinde tasarruf hakkı sahipleri, işletmecileri ve kullanıcıların sistemin çalışmasındaki yararı iken ikinci fıkrada veri sahiplerinin herhangi bir bozulma, müdahale, engel olmadan verileri kullanmasındaki yararıdır.[309]

Kanun sistematiğine baktığımızda, 244. maddenin kanun koyucu tarafından ikinci kitap üçüncü kısımda yer alan "Topluma Karşı Suçlar" altında düzenlemesi bilişim sistemlerine olan toplumsal güveni koruma çabasıyla ilgilidir. Bu düzenlemenin gerekçesi incelendiğinde *"(...) sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır (...)"*[310] ifadesiyle bilişim sisteminin hem soyut yazılımsal hem de somut donanımsal özelliklerinin suç konusunu oluşturabileceği bu nedenle de kanun koyucunun aslında bilişim sistemlerinin ve sistem içerisindeki verilerin doğru ve işlevsel faaliyetlerine devam etmelerini koruduğu değerlendirilir.

3.3.3. Suçun Maddi Unsurları

3.3.3.1. Fail ve Mağdur

[306] Ketizmen, Bilişim Suçları, s. 128.
[307] Kurt, Bilişim Suçları, s. 162.
[308] Dülger, Bilişim Suçları, s. 322.
[309] Akbulut, Bilişim Alanında Suçlar, s. 181.
[310] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 764.

5237 sayılı TCK'nın 244.maddesi incelendiğinde suç işleyen kimsenin bazı niteliklere sahip olması, belli yükümlülüklerinin varlığı gibi özel ve farklı bir tabire yer verilmediği görülmektedir. Bu nedenle herkes tarafından işlenebilen fail açısından aynı 243. maddede olduğu gibi herhangi bir farklılık ve özellik göstermeyen bir suç tipi olduğundan bahsedilebilir.[311]

Suçun kim tarafından işlendiğinin tespit edilmesi noktasında suçu oluşturan eylemin bilişim sisteminin hangi unsuruna yönelik işlendiğinin doğru tespiti önemlidir.[312] Fail sahibi olmadığı bir bilişim sisteminde kendisine ait verileri yok etmek veya erişilmez kılmak için sistemin işleyişini bozup engellerse mülkiyet, kullanım ve tasarruf yetkisi göz önünde bulundurulacak ve 244. maddenin ikinci fıkrasındaki suç değil aynı maddenin birinci fıkrasındaki suçun oluştuğu kabul edilecektir.[313] Özellikle teknolojik gelişmelerin çağımızda yaygın kıldığı bulut bilişim sistemleri bu suçların işlenmesi için oldukça elverişlidir.[314]

TCK'nın 244. maddesinde suç oluşturan eylemlerin kimin tarafından işlendiğinin tespiti esnasında öncelikle eylem, bilişim sistemine mi yoksa sistemde mevcut verilere mi yönelmiş bunun tespit edilmesi gerekir. Daha sonra eylemin yöneldiği her ne ise sistem ise sistemin, veriler ise verilerin, mülkiyetinin ait olduğu kişi, kullanım hakkı ve tasarruf yetkisinin kime ait olduğu ayrıca ortaya çıkan zararı kimin oluşturduğunun doğru tespiti gereklidir.[315] Eylem hem bilişim sistemine hem de verilere yönelik gerçekleşmiş olabilir bu durumda da aynı yol izlenecektir.

Suç mağdur açısından bakıldığında da tıpkı failde olduğu gibi bir özellik göstermemektedir. Bu düzenlemede suçun mağduru bilişim sisteminin veya zarara uğrayan verilerin sahibi, zilyedi ya da tasarruf yetkisine sahip kişiler olabilir. [316]

Tüzel kişilerin veya kamu kurum ve kuruluşlarının bilişim sistemlerine veya sistemdeki verilerine karşı 244.madde kapsamında suç oluşturan eylemlerin gerçekleşmesi durumunda bu suçun mağduru topluma karşı düzenlenen suç olması nedeniyle tüm toplum olacak, kamu kurumu suçtan zarar gören kişi konumunda olacaktır.

3.3.3.2. Suçun Konusu

---

[311] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6756.
[312] Yılmaz, Sacit, "5237 Sayılı TCK'nın 244. maddesinde Düzenlenen Bilişim Alanındaki Suçlar", Türkiye Barolar Birliği Dergisi, C.23, S. 92 (Ocak 2011), s. 70.
[313] Akbulut, Berrin, "Sistemi Engelleme, Bozma Verileri Yok Etme veya Değiştirme", Selçuk Üniversitesi Hukuk Fakültesi Dergisi, C. 24, S. 2 (Aralık 2016), s. 19.
[314] Dülger, Bilişim Suçları, s. 324.
[315] Dülger, Bilişim Suçları, s. 325.
[316] Tasarruf yetkisine sahip kişi kavramı ayrıntılı bilgi için bkz: Akbulut, "Sistemi Engelleme, Bozma Verileri Yok Etme veya Değiştirme" , s. 21-23.

TCK'nın 244. maddesi birinci ve ikinci fıkralarında iki ayrı suç tipini düzenlediği için suçun konusu da her iki fıkrada farklı olmaktadır.

Birinci fıkrada düzenlenen bilişim sisteminin işleyişinin engellenmesi veya bozulması suçunun konusu bilişim sistemidir. İkinci fıkrada düzenlenen verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması ve verilerin başka yere gönderilmesi suçunda bilişim sisteminde bulunan veriler, sisteme veri yerleştirilmesi suçu bakımından bilişim sistemine yerleştirilen veriler suçun konusunu oluşturur.[317]

Birinci fıkrada suçun konusunu oluşturan bilişim sisteminin içeriği hakkında doktrinde çeşitli tartışmalar bulunur. Kimi yazarlar maddenin kanuni gerekçesini de belirterek hem yazılımların hem de donanımların suçun konusuna girdiğini, bilişim sistemi kavramının geniş yorumlanması gerektiğini ifade etmektedir.[318] Bazı yazarlara göre ise, 244. maddede kanuni düzenlemenin amacının sistemin donanımsal, maddi unsurların da meydana gelen zararları korumak değil yazılımsal, sistemsel koruma sağlamak olduğu bu nedenle donanımsal zararların mala zarar verme suçunu oluşturacağı görüşündedir.[319] Bizim görüşümüze göre, bilişim sisteminin içeriğine, sistemin işleyişine ya da sistemde bulunan verilere müdahale etme kastı ile hareket etmeyen bir failin salt bilişim sisteminin donanımına verdiği zarar neticesinde 244. madde uyarınca cezalandırılması hatalı olacak 151. maddede düzenlenen mala zarar verme hükümlerinin düşünülmesi gerekecektir.

3.3.3.3. Hareket

5237 sayılı TCK'nın 244. madde düzenlemesinde hareket unsurunun birinci ve ikinci fıkradaki suç tipleri bakımından ayrı ayrı incelenmesi gereklidir. Ancak her iki suç tipi için de ortak olan madde metinlerinde yer alan eylemlerin seçimlik hareketli olarak düzenlenmesidir.

3.3.3.3.1. Bilişim Sisteminin İşleyişini Engellemek veya Bozmak

Failin eylemi neticesinde bir bilişim sisteminin işleyişi engellenebilecek ya da sistem bozulabilecektir. TCK'nın 244'üncü maddesi birinci fıkrasında düzenlenen bu suçta seçimlik

[317] Akbulut, Bilişim Alanında Suçlar, s. 188.
[318] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 764; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 854.
[319] Taşdemir, Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması Dolandırıcılık Suçları, s.267; Dülger, Bilişim Suçları, s. 326; Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6757.

hareketli iki eylem düzenlenmiştir.[320] Suç oluşturan eylemlerin her ikisi de bilişim sistemlerine yönelik gerçekleşecektir. Failin eylemi sonucunda sistemin hem işleyişinin engellenmesi hem de bozulması söz konusu olursa aynı maddede düzenlenen seçimlik hareketli iki eylem birlikte gerçekleşmiş olacağından tek bir suç oluşacak ancak bu durum cezalandırmada temel cezayı artıran bir neden olabilecektir.

Bilişim sisteminin işleyişinin engellenmesi kavramı verilerin kullanılmasını, kaydedilmesini, depolanmasını, işlenmesini veya değerlendirilmesini veya veri aktarımını önlemeye yönelik her tür hareket olarak tanımlanabilir.[321] Yargıtay bir kararında sistemin işleyişinin engellenmesini tanımlamış ve bu durumda sistemin kendisinden beklenilen normalde gerçekleştirdiği fonksiyonları, işlemleri yerine getirememesi amacıyla yeteneğinin sınırlandırılıp yavaşlatılması ya da tamamen kilitlenmesi olarak nitelendirmiştir.[322] Kanun koyucu sistemin işleyişinin engellenmesi kavramına geniş bir alan açarak sistem işleyişini bozma hariç engelleyen her türlü eylemi bu kapsama dahil etmiştir.[323]

Sistem işleyişinin uzun süreli, daimi ya da geçici, kısa süreli engellenmesi durumları doktrinde tartışma konusudur. Bazı yazarlar, engelleme fiilinin uzun süreli olmasını artık sistemin bozulması olarak değerlendirerek geçici ve kısa süreli engellemeleri bu eylem kapsamında nitelendirmiştir.[324] Diğer bir görüş ise, bilişim sisteminin engellenmesinin bu suçun tamamlanması için yeterli olduğunu, engellenen sistemin ne kadar zaman erişim engeli olduğunun suç açısından bir özellik göstermediğini savunmaktadır.[325] Ancak Akbulut, bu konuda kanuni bir düzenleme olmamakla beraber, sistemi her türlü engellemenin cezalandırılmaması gerektiği, işleyişe önemsiz derecede engel olan durumların haksız içerik azlığı sebebiyle cezalandırılma yoluna gidilmemesi gerektiği görüşüne sahiptir.[326] Bizim görüşümüze göre de sistemin geçici veya sürekli engellenmesi ayrımının kanun metninde de düzenlenmemesi nedeniyle bir önemi bulunmamaktadır.

---

[320] Suçun seçimlik hareketli olduğu görüşünü savunanlar çoğunlukta olsa da serbest hareketli suç olduğu görüşünde olan yazarlarda vardır. Serbest hareketli suç görüşü için bkz: Erdoğan, Bilişim Suçları, s. 186.

[321] Akbulut, Bilişim Alanında Suçlar, s. 190.

[322] 5237 sayılı TCK'nın 244. Maddesinin birinci fıkrasında bilişim sisteminin işleyişinin engellenmesi ve sistemin bozulması fiilleri suç olarak düzenlemek suretiyle Avrupa Siber Suçlar Sözleşmesi'ne paralellik sağlamak amacıyla bir bilişim sisteminin işleyişinin "engellenmesi" veya "bozulması" bir yarar sağlama koşuluna bağlanmaksızın bağımsız suç olarak düzenlenmiştir. **Sistemin işleyişinin engellenmesi ibaresi ile bilişim sisteminin verimli çalışmasının önlenmesi, icra ve sahip olduğu kapasitesinin müdahale ile sınırlandırılması, yavaşlatılması ya da tamamen kilitlenme noktasına getirilmesi**,…." Yargıtay 11. Ceza Dairesi E. 2014/7245 K. 2014/5492 T. 24.03.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[323] Yılmaz, "Bilişim Alanındaki Suçlar", s. 72.

[324] Erdoğan, Bilişim Suçları, s. 190; Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 765.

[325] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6760.

[326] Akbulut, Bilişim Alanında Suçlar, s. 193.

Sistemin engellenmesi suçunda engelleme eyleminin yöneldiği unsur konusunda da doktrinde farklı görüşler bulunur. Bir görüşe göre, sistemin fiziki unsurlarına yönelik eylemler mala zarar verme suçunun konusunu oluşturacak, soyut unsurlarına yönelik müdahalelerde sistemin işleyişinin engellenmesi veya bozulması suçları söz konusu olabilecektir.[327] Başka görüşte ise suç işleyen kişilerce hedef alınan sistemin işleyişini engelleme eylemi bilişim sisteminin somut unsurlarına yönelikte gerçekleşebilecektir[328]

Sistemlere bilişim virüsü, mantık bombası, truva atı gibi zararlı yazılımların çeşitli yollarla bulaştırılması, DDoS ve DOS saldırıları en çok karşılaşılan sistemi engelleyici eylemlerdir. Sistemin elektriğinin kesilmesi, ethernet kartının işlevsizleştirilmesi gibi sistemin teknik fonksiyonlarına zarar vermek suretiyle sistemin somut unsurlarına yönelik eylemlerle de işlenebilir.[329] AKSS 5. maddesinde sistem işleyişinin engellenmesinde yalnızca sistemin soyut unsurlarına müdahalenin suç kapsamında kaldığı düzenlenmiş olsa da Türk Ceza Kanunu'ndaki düzenlemede bu içerik bulunmamasından dolayı somut unsurlara yönelik eylemlerde suç kapsamında kalacaktır. Yargıtay'ın ATM'leri bilişim sisteminin bir unsuru kabul ederek failin bu cihazlara karşı gerçekleştirdiği eylemlerin sistemin işleyişine etkisinin incelenmesi gerektiği görüşünde olduğu görülür.[330]

İcrai hareketle işlenebilen bu suç istisnai olarak ihmali suretle de işlenebilecektir; sistem güvenliğinden sorumlu teknik ekibin gerekli yazılımları sisteme yüklememesi durumu buna örnek oluşturabilir.[331]

Bilişim sisteminin bozulması, doktrinde kalıcı olarak sistemin kullanımının

---

[327] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 871.

[328] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6759; Akbulut, Bilişim Alanında Suçlar, s. 192.

[329] Erdoğan, Bilişim Suçları, s. 189; Koca/Üzülmez'e göre bilişim sisteminin maddi unsurlarına yönelik fiiller mala zarar verme suçunu oluşturmaktadır. Bkz: Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 857.

[330] " Somut olayda önceden hazırlanan düzeneğin ATM cihazına yerleştirdikten, mağdurun kartı ATM cihazına sıkıştıktan sonra banka görevlisinin gelmesi nedeniyle kartın ele geçirilemediği, bu şekilde TCK.nun 245/1. maddesindeki banka veya kredi kartının kötüye kullanılması suçunun icra hareketlerine başlanılmadığı, eylemin kartın sıkışmasını sağlamak için yerleştirilen düzeneğin takılı olduğu süre boyunca bilişim sisteminin bir parçası olan ATM'nin kullanılamaması karşısında; gerçeğin ve suç niteliğinin kuşkuya yer vermeyecek şekilde belirlenebilmesi ve sanığın **bilişim sisteminin parçası olan ATM üzerinde gerçekleştirdiği** hareketlerinin ayrıntılı olarak tespiti ve bu hareketin suça konu bankanın bilişim sisteminin bir parçası olan ATM'nin kısa süreliğine de olsa çalışmasına engel teşkil edip etmediği, bağlı bulunduğu bilişim sistemine (sistemin engellenmesi veya bozulması gibi) bir zarar verip vermediği hususları ilgili banka şubesinden sorulup, gerektiğinde bilirkişi raporu alınarak, ATM'nin ait olduğu bankanın şikayetçi olup olmayacağı hususu da sorulduktan sonra sanıkların eyleminin "bilişim sistemini engelleme veya bozmak", "mala zarar vermek" suçlarını oluşturup oluşturmadığı karar yerinde tartışılarak hukuki durumunun takdir ve tayini gerektiği gözetilmeden eksik soruşturma ve suç vasfında yanılgı sonucu yazılı şekilde "banka veya kredi kartlarının kötüye kullanılmasına teşebbüs" suçunu oluşturacağından bahisle hüküm kurulması,…" Yargıtay 8. Ceza Dairesi E. 2014/2546 K. 2014/13667 T. 03.06.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[331] Dülger, Bilişim Suçları, s. 329.

engellenmesi,[332] bilişim sisteminin kısmen veya tamamen işlemez duruma getirilmesi[333], sistemin işleyişinin kalıcı olarak sonlandırılması[334] biçimlerinde tanımlanmıştır. Bozmak kelimesinin TDK'da kelime anlamı ise *"Bir şeyi kendisinden beklenilen işi yapamayacak duruma getirmek"* tir.[335] Yargıtay kararlarında ise bilişim sistemlerinin işleyişinin bozulması, bilişim sistemine ait yazılımların ve donanımsal parçalarının normal çalışması durumunda yapması gereken görevi artık yapamayacağı hale getirmek ve sistemin tamamen işleyemez hale getirilip çökertilmesi olarak tanımlanmıştır.[336]

Bilişim sisteminin işleyişinin nasıl bozulduğu önem taşımaz. Yani bozma eylemi gerçekleşirken sistemin yazılımsal, soyut unsurları mı hedef alınıp suç gerçekleştirildi ya da fiziki unsurlarına mı zarar verildi bu suç için önemsizdir. Sistemin bozulması için en elverişli yöntem zararlı virüs yazılımları ve kurtçukların sistemlere gönderilmesidir.[337]

Bir bilişim sisteminin bozulduğu veya erişimin engellendiğine ilişkin şikâyet üzerine ilk olarak bozulan, engellenen sistemin şikâyetçiye ait olup olmadığı hususu netleştirilecek daha sonra eylem sonrasında sistem girişleri, sisteme erişilmişse IP adresleri, sistemin şifresinin değiştirilip değiştirilmediği belirlenecektir.[338]

3.3.3.3.2. Bilişim Sistemindeki Verilerin Bozulması, Yok Edilmesi, Değiştirilmesi, Erişilmez Kılınması, Sisteme Veri Yerleştirilmesi veya Mevcut Verilerin Başka Yere Gönderilmesi

TCK'nın 244. maddesinin birinci fıkrasında düzenlenen eylemler bilişim sistemine yönelik iken ikinci fıkrasında ise sistemde bulunan verileri bozma, yok etme, değiştirme,

---

[332] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 765.
[333] Dülger, Bilişim Suçları, s. 330.
[334] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 857.
[335] https://sozluk.gov.tr/ (Erişim Tarihi: 08.06.2022).
[336] Yargıtay 11. Ceza Dairesi E. 2014/7245 K. 2014/5492 T. 24.03.2014, (https://legalbank.net/arama/mahkeme-kararlari).
[337] Dülger, Bilişim Suçları, s. 330.
[338] "Somut olayda öncelikle bozularak erişimi engellenen sitenin şikayetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak sitenin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. ……dan da bozulma yada erişimin engellendiği iddia olunan tarih/tarihler ve takip eden günlerde ilgili siteye giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle site adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. İlgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalı, giriş yapmak isteyipte erişim sağlayamayanlar arasında şikayetçinin de bulunup bulunmadığı IP numarasından tespit edilerek iddianın doğruluğu belirlenmeli, şikayetçi ve şüphelinin bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri tanık olarak dinlenmelidir." Yargıtay 8. Ceza Dairesi E. 2013/15110 K. 2014/11220 T. 30.04.2014, (https://legalbank.net/arama/mahkeme-kararlari).

erişilmez kılma, sisteme veri yerleştirme veya mevcut verileri başka yere gönderme eylemlerinin sistemdeki verilere yönelik olduğu görülmektedir. Seçimlik hareketli olarak düzenlenen bu suç tipinde sayılan eylemlerden herhangi birinin gerçekleşmesi suçun oluşması için yeterliyken, birden fazla eylemin birlikte gerçekleşmesi durumunda yine tek suç oluşacak, ancak failin cezasının tayininde TCK'nın 61.maddesi gereği temel cezadan uzaklaşarak ağırlaştırılmasını gerektirecektir.[339]

3.3.3.3.2.1. Verileri bozma

Verilerin bozulması kavramı aslında zarar niteliğinde bir neticeyi ifade etmektedir.[340] Birinci fıkrada yer alan bilişim sistemin bozma eylemindeki açıklamalar verileri bozma hareketi içinde kullanılabilecektir. Bozma ile kastedilen, bilişim sistemindeki verilerden sağlanmak istenen yararın elde edilemeyecek hale getirilmesi, verilerin bir kısmının veya tamamının tahrip edilmesi veya sistemdeki verilerin niteliklerinin değiştirilmesi eylemleridir.[341]

Bilişim sisteminin işleyişinin bozulması eylemi, TCK'nın 244. maddesinin ikinci fıkrasında sayılan verilerin bozulması suretiyle gerçekleştirilebilecektir. Bu durumda hangi fıkradaki suçun oluştuğunun tespitinde failin eylemdeki maksadını değerlendirmek gerekecektir. Örneğin fail bilgisayara gönderdiği zararlı bir yazılım virüsüyle sistemdeki verileri yok etmek istemiş ancak bu yazılım bilişim sisteminin bozulmasına neden olmuşsa somut eylemde hangi fıkranın uygulanacağının belirlenmesinde kanuni bir unsur olmamasına rağmen failin amacına bakılabilecektir.[342]

3.3.3.3.2.2. Verileri Yok Etmek

Kelime anlamı "ortadan kaldırmak"[343] olan yok etme eylemi bozmadan farklıdır. Verilerin bozulmasında veri mevcut ancak kullanılamaz durumdayken, verilerin yok edilmesinde ortada kullanılabilecek bir veri bulunmamaktadır.[344]

Doktrindeki görüşe göre, yok etme kelimesinin gerçek anlamında olduğu gibi verilerin varlığına tamamen son verilebilme imkânının olmadığı, kast edilenin mantıksal, soyut bir yok

[339] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 770.
[340] Akbulut, "Sistemi Engelleme, Bozma Verileri Yok Etme veya Değiştirme", s. 32.
[341] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 770.
[342] Dülger, Bilişim Suçları, s. 331.
[343] https://sozluk.gov.tr/ (Erişim Tarihi: 08.06.2022).
[344] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 6760.

etme olduğudur.[345] Bir bilişim sistemindeki verilerin yok olması iki biçimde gerçekleşebilir; *"Birinci işlemde verilerin depolama üzerindeki varlığına tamamen son verilerek, o veriye ilişkin hiçbir iz depolama ünitesi üzerinde bırakılmamakta; ikinci tip yok etme işleminde ise, veriler depolama ünitesi üzerinden silinmemekte, sadece o verilere erişimi sağlayan anahtar veriler silinmektedir. Bu durumda, işletim sistemi o verilere ulaşamamaktadır. Veriler fiziksel olarak silinmediği için özel işlemler aracılığı ile silinmiş gözüken veriler tekrar kurtarılabilir. Depolama ünitesinden fiziksel olarak silinmiş olan veriler ise asla kurtarılamaz."*[346]

Bir bilişim sisteminde yok edilen verilerin sisteme geri getirilme imkânı bulunduğunda suç meydana gelecek mi doktrinde tartışmalıdır. Özbek/Kanbur/Doğan/Bacaksız/Tepe'ye göre, veriye erişim için verilen komuttan bir sonuç alınamayacak şekilde verinin kayıtlardan silinmesi suçun oluşumu için yeterlidir.[347] Koca/Üzülmez'e göre, verinin mağdurun tasarruf alanında çıkartılmış olması ve normal şartlarla veriye ulaşmasının güçleştirilmesi yok etmede en önemli husus olup ortadan kaldırılan verilere ulaşabilme imkânı suçun oluşumuna etki etmeyecektir.[348] Akbulut'un görüşüne göre ise verilerin bir uzman aracılığıyla, bir takım araçlar yardımıyla geri getirilme imkânı varsa verilerin yok edildiğinden bahsedilemeyeceği yönündedir.[349]

Verilerin geri dönüşüm kutusuna gönderilmek suretiyle silinmesinin eyleminin bu suçu oluşturup oluşturmadığı hususunda da doktrinde farklı görüşler bulunmaktadır. Bazı yazarlara göre, gerçekte bilişim sisteminde bir silme işlemi gerçeklememiş olmasına rağmen mantıksal anlamda bir silmeyle mağdur açısından verilerinin yok olması ve ulaşamaması verilerin yok edilmiş olduğunun kabulünü gerektirecektir.[350] Diğer bir görüşte ise verinin geri dönüşüm kutusuna atılarak silinmesi sistem içindeki bir verinin yer değiştirmesidir ve bu suçu oluşturmayacaktır.[351]

3.3.3.3.2.3. Verileri Değiştirmek

Değiştirmek kelimesi başka bir biçime sokmak, değişikliğe uğratmak, bulunduğu yerden

---

[345] Dülger, Bilişim Suçları, s. 331.
[346] Yılmaz," Bilişim Alanındaki Suçlar", s. 73.
[347] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 861.
[348] Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 872.
[349] Akbulut, Bilişim Alanında Suçlar, s. 197.
[350] Dülger, Bilişim Suçları, s. 332; Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 861, Akbulut, Bilişim Alanında Suçlar, s. 197.
[351] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6760; Koca/Üzülmez, Türk Ceza Hukuku Özel Hükümler, s. 872.

başka bir yere götürmek anlamlarında kullanılmaktadır.[352] Verilerin değiştirilmesi kavramı ise; veri veya veri grubu yerine başka verilerin konulması[353], yeni bir bilginin oluşmasını sağlayan her tür hareket[354], verilerin orijinal halinden başka hale dönüşmesi[355], verilerin başka biçime sokularak yeni içerek kazanıp niteliklerinin değişmesi[356] demektir. Failin, mağdurun sisteme koyduğu şifreyi kırmak suretiyle ulaştığı facebook hesabında şifreyi değiştirerek arkadaşlarına mesaj atması durumunu verileri değiştirme kapsamında değerlendirilmiştir.[357] Yargıtay bir kararında bilişim sistemine girerek silah ruhsatı almasına engel olan sicilde değişiklik gerçekleştiren kişinin eylemini TCK m 244/2 maddesi kapsamında değerlendirmiştir.[358]

3.3.3.3.2.4. Verileri Erişilmez Kılmak

Failin gerçekleştirdiği bazı işlemler neticesinde mağdurun kendine ait verilerine istediği zaman ulaşamaması verilerin erişilmez kılınması anlamına gelmektedir.[359] Bu eylem ile veriler yok edilmez, değişikliğe uğramaz yalnızca veriye ulaşmak için gerekli işlem bağı koparılır ve hak sahibinin veriye ulaşımı engellenir.[360] Erişilmez kılınan veriler hala bilişim sisteminde bulunur ve verilerin içeriği, niceliği aynı kalır.

---

[352] https://sozluk.gov.tr/ (Erişim Tarihi: 08.06.2022).
[353] Dülger, Bilişim Suçları, s. 333.
[354] Akbulut, Bilişim Alanında Suçlar, s. 198.
[355] Parlar/Öztürk, Doğrudan ve Dolaylı Bilişim Suçları, s. 52.
[356] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 771.
[357] "..Katılan ile sanığın bir dönem nişanlı kaldıkları, nişanın bozulmasından sonra sanığın katılanın kullanmış olduğu Facebook isimli **sosyal paylaşım sitesindeki sayfasının şifresini değiştirerek girdiği** ve katılanın Facebook üzerindeki bazı arkadaşlarına mesaj attığı olay nedeniyle……sanığın eyleminin anılan Kanun'un **244/2. maddesinde düzenlenen bir bilişim sistemindeki verileri değiştirme suçunu oluşturduğu** gözetilmeden, suç vasfında hata yapılarak yazılı şekilde karar verilmesinde isabet görülmediğinden BOZULMASINA…"Yargıtay 8. Ceza Dairesi E. 2018/8369 K. 2019/5454 T. 16.04.2019, (https://legalbank.net/arama/mahkeme-kararlari).
[358]"Somut olayda suç tarihinde ... Emniyet Müdürlüğünde Asayiş Şube Müdürü olarak görev yapan sanığın kendisine bağlı olan Aranan Şahıslar Büro Amirliğine gelerek atış eğitimine gitmek için bürodan ayrılmak üzere olan tanık ...'in kullandığı şahıs sorgulama sistemi açık olan bilgisayardan, tanık anlatımları ve bir bilişim sistemi olan ... kayıtlarına göre ... isimli şahsa ait silah ruhsatı almasına engel sicil kaydını saat 15:24'te iptal ettiği, ... **bilişim sistemine girilerek kaydın silinmesi** sonucu ... isimli kişiye ... Kaymakamlığının 18.05.2009 tarihli olurları ile silah taşıma ruhsatı verilerek başkasına haksız bir çıkar sağlanması şeklindeki eylemin TCK.nun 244/2-son maddesindeki **"bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme" suçunu oluşturduğu** gözetilmeden, yazılı biçimde hüküm kurulması,…BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2015/14782 K. 2016/4928 T. 12.04.2016, (https://legalbank.net/arama/mahkeme-kararlari).
"Mağdura ait **Facebook ve MSN hesaplarına giren ve hesap şifrelerini değiştirmek suretiyle mağdurun hesaplara erişimini engelleyen** sanığın, eylemine uyan **TCK.nun 244/2, 43. madde** ve fıkraları uyarınca mahkumiyetine karar verilmesi gerektiği gözetilmeden sanığın suç kastı bulunmadığından bahisle yasal ve yeterli olmayan gerekçeyle beraatine hükmolunması,…BOZULMASINA.." Yargıtay 8. Ceza Dairesi E. 2013/13127 K. 2014/10178 T. 21.04.2014, (https://legalbank.net/arama/mahkeme-kararlari).
[359] Apaydın, Cengiz, "Bilişim Sistemindeki Verileri Yok Etme, Bozma, Erişilmez Kılma, Değiştirme, Hukuka Aykırı Olarak Verileri Yerleştirme veya Gönderme Suçu ile Bu Suretle Hukuka Aykırı Yarar Elde Etme Suçunun Değerlendirilmesi" Terazi Hukuk Dergisi, C.10, S.111 (Kasım 2015) s. 20-21.
[360] Ketizmen, Bilişim Suçları, s. 140.

Erişilmezliğin geçici bir süreyle ya da daimi olması suçun oluşumu açısından önem arz etmemektedir.[361] Uygulamada Yargıtay'ın bir kimsenin elektronik posta şifresinin veya sosyal medya hesap şifrelerinin değiştirilmesi eylemini erişilmez kılma kapsamında değerlendirdiği görülmektedir.[362]

Eğer verilere erişimi engelleyen eylem neticesinde bilişim sisteminin işleyişi engellenir, sistem erişilmez kılınırsa bu durumda artık bilişim sistemi verileri de kapsayan bir kavram olması sebebiyle TCK'nın 244. maddesinin birinci fıkrası uygulanacaktır.[363]

3.3.3.3.2.5. Veri Yerleştirmek

Veri yerleştirme eylemi sistemdeki verilere zarar vermeyen bir eylemdir. Bu eylemle sisteme dış ortamdan veri taşıması gerçekleştirilir.[364] Sistem sahibinin rızası dışında gerçekleşen bu eylemde sisteme veri girişinin yapılma yönteminin ve sisteme eklenen verilerin içeriğinin önemi bulunmamaktadır.[365] Sisteme yerleştirilecek veri herhangi bir şekle bağlı olmaksızın sisteme donanım eklenmek suretiyle veya bilişim ağları üzerinden eklenebilir.

Veri yerleştirme sistemde daha önce hiç olmayan bir verinin sisteme bütünüyle eklenmesi biçiminde olabileceği gibi var olan bir veri içeriğine ekleme yapılmak suretiyle de gerçekleşebilecektir. Sisteme yerleştirilen veri sistemin işleyişini engelleme veya bozma gibi durumlara yol açmamış olmalıdır. Yargıtay internet sitelerine hukuka aykırı erişim sağlanarak site içeriklerine müdahale edilmesi, farklı internet sitelerine yönlendirme linkleri koyulması durumlarını bilişim sistemine veri yerleştirme olarak yorumlamıştır.[366]

---

[361] Dülger, Bilişim Suçları, s. 334.

[362] "Oluşa ve dosya içeriğine göre katılanın Facebook şifresinin 2 Nisan 2010 tarihinden itibaren değiştirildiği, şikayet üzerine yapılan soruşturma sonucunda elde edilen İP numaralarına göre 25 Mayıs 2010 ile 8 Haziran 2010 tarihleri arasında sanığın kullanmış olduğu bilgisayarlardan katılanın hesabına erişim sağlandığı, suç tarihinde sanık ile katılanın arkadaşlık ilişkilerinin bitmiş olduğu ve katılanın rızasının bulunmamasına rağmen sanığın **katılana ait hesaplara izinsiz erişim sağlayıp katılanın kullanımını engelleyecek şekilde şifreyi değiştirdiği ve bu oluşa göre sanığın TCK.nun 244/2 maddesine uyan eyleminin sabit olduğu** gözetilmeden, mahkumiyeti yerine yazılı şekilde beraat kararı verilmesi,….(BOZULMASINA)" Yargıtay 8. Ceza Dairesi E. 2013/8498 K. 2014/7850 T. 27.03.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[363] "Sanığın katılana ait **elektronik posta adresinin güvenlik şifresini kullanıp şifre değişikliği yaparak** katılanın elektronik posta adresine **kendi şifresi ile girişini engellemesi** şeklinde sübut bulan eyleminin, TCK.nun 244/2. maddesinde düzenlenen suçu oluşturduğu gözetilmeden, TCK.nun 244/1. maddesinden hüküm kurulması … (BOZULMASINA)" hükmetmiştir. Yargıtay 8. Ceza Dairesi E. 2013/11478 K. 2014/8887 T. 08.04.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[364] Akbulut, Bilişim Alanında Suçlar, s. 202.

[365] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6761.

[366] "Sanığın, katılanın sahibi bulunduğu www……..com adlı oyun **internet sitesine ilave kodlar ekleyerek başka oyun sitelerine yönlendirme yapması** şeklinde gerçekleşen eyleminin, katılana ait **bilişim sistemine erişimi engelleyip, bozmadığı ve bilişim sistemine veri yerleştirmekten ibaret olduğu** anlaşılmakla; eylemini TCK.nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden aynı maddenin 1. fıkrası ile hüküm

3.3.3.3.2.6. Bilişim Sisteminde Var Olan Verileri Başka Bir Yere Göndermek

Verileri başka yere gönderme eyleminin aynı bilişim sistemi içerisinde mi yoksa mevcut sistemden başka bir yere mi olacağı hususunun kanunda açıkça ifade edilmemesi belirsizlik yaratarak doktrinde tartışmalara neden olmuştur. Bir görüşe göre, verileri başka bir yere gönderme fiili, mağdura ait verilerin fail tarafından mağdura ait bilişim sistemindeki başka bir yere veya farklı bir bilişim sistemine gönderilmesi biçiminde ifade edilmiştir.[367] Başka bir görüş ise; mağdura ait bilişim sistemi içerisinde verilerin farklı yere gönderilmesinin bu suçu oluşturmayacağını, gönderilen verilerin başka bir sisteme aktarılması ya da veri nakil aracına kaydedilmesi veya kopyalanmasının söz konusu suçu oluşturduğu düşüncesindedir.[368] Bizim kanaatimize göre de madde metninde başka bir yer tabirine yer verilmesi sistemin dışına çıkılmadan yapılan veri göndermelerinin kapsam dışı kalması gerektiği yönündedir.

Kanun koyucunun somut bir eylemi karşılayan göndermek kelimesini cismani varlığı bulunmayan soyut veriler hakkında tercih etmesinin bilişim alanında yaygın kullanılan e-posta göndermek kavramıyla ilişkili olduğu düşünülebilir.[369]

Veri gönderilen yerin mutlaka bir bilişim sistemi olması gerekmemekte, usb, harici bellek, cd, bulut sistemleri gibi veri depolama araçları da bu kapsamda değerlendirilmektedir.

Verilerin kaydedilmesi, sistemdeki verilerin bir kopyasının çıkarılması veya verilerin aktarılması eylemleri bu suç tipini oluşturacaktır.[370] Yargıtay sanığın verileri kopyalaması eylemini değerlendirilirken hem katılana hem de sanığa ait suç tarihinde kullanımlarında olan bilgisayarların log kayıtlarının karşılıklı olarak incelenmesi gerektiğini ifade etmiştir.[371]

---

kurulması" Yargıtay 8. Ceza Dairesi E. 2017/24455 K. 2018/9694 T. 24.09.2018, (https://legalbank.net/arama/mahkeme-kararlari).

[367] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 771; Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6761.

[368] Dülger, Bilişim Suçları, s. 337.

[369] Dülger, Bilişim Suçları, s. 337.

[370] "Bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme ile bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, var olan verileri başka bir yere gönderme suçlarına ilişkin olarak, sanığın, yetkisi olmadığı halde katılan **şirkete ait bilişim sistemine girerek orada bulunan verileri alıp kendi kullandığı bilgisayara ve CD'ye aktarması şeklinde gerçekleşen eyleminin** bir bütün olarak TCK.nun 244/2. maddesinde düzenlenen suçu oluşturacağı gözetilmeden yazılı şekilde karar verilmesi,..BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2013/3173 K. 2014/18506 T. 14.07.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[371] Katılanın yetkilisi olduğu şirkete ait ücret karşılığı üyelik sistemi ile abonelerine hizmet veren "www.....com" isimli siteye girerek sistemdeki verileri kopyaladıkları iddiasıyla açılan davada, katılanın şikayet dilekçesi ekinde ibraz ettiği deliller dışında delil toplanmamıştır. Katılanın ve sanığın suç tarihinde kullandıkları bilgisayarlarına el konulup hard disklerinin, **suç tarihine ilişkin LOG kayıtları bakımından karşılıklı olarak incelenmesi**, suç tarihinde bilişim sistemindeki verilerin bozulup bozulmadığı, yok edilip edilmediği, değiştirilip değiştirilmediği veya erişilmez kılınıp kılınmadığı, sisteme veri yerleştirilip yerleştirilmediği, var olan verilerin başka bir yere

Verilerin kaydedilmesi eylemi kopyala yapıştır suretiyle yeni bir kopyanın aktarılması suretiyle olabileceği gibi kayıt sırasında bulunduğu sistemden silinerek yok da edilebilir. Verilerin yok edilmesi durumu bu suç tipinde yer alan başka bir eylemi oluşturacaktır.

3.3.4. Suçun Manevi Unsurları

TCK'da düzenlenen 244. maddenin birinci ve ikinci fıkralarındaki suçlar failin kasten işleyebileceği suçlardır. Bu suçların taksirli halleri kanunda düzenlenmediğinden dolayı failin taksirle bu suçları işlemesi cezalandırılamayacaktır. Bu madde ile düzenlenen tüm suç tipleri hem olası kastla hem de doğrudan kastla işlenme imkânına sahiptir.[372]

Failin saikine ilişkin madde metninde herhangi bir ibare olmadığından belli bir saikle hareket etme unsuru da aranmayacaktır. Karşılaştırmalı hukuk incelendiğinde İngiltere'nin kanunlarında, sistemin işleyişini engelleme veya bozma suçunu düzenleyen hükümlerinde suçun oluşması için failin özel kastının arandığı görülmektedir. Bu düzenlemelerden yetkisiz olarak bilgisayar materyallerinin değiştirilmesi suçunda failin herhangi bir bilgisayarın işleyişini engelleme, herhangi bir bilgisayarda bulunan veri veya programa erişimi engelleme, herhangi bir verinin güvenilirliğini veya bir programın işleyişini engelleme saikleriyle hareket etmesi aranır.[373]

Failin verileri bozma, yok etme, değiştirme, erişilmez kılma eylemlerini gerçekleştirmesi neticesinde sistemin işleyişinin engellenmesi veya bozulması durumlarında failin hangi fıkra kapsamında cezalandırılacağının tespiti açısından kanuni düzenlemede olmasa dahi failin saikine bakılabilir.[374]

3.3.5. Hukuka Aykırılık

Failin eylemini hukuka aykırı olmaktan çıkaran durum hukuka uygunluk sebeplerinden birinin bulunmasıdır. Hukuka uygunluk nedenlerinin varlığı bir eylemi suç olmaktan çıkararak en başından itibaren hukuka uygun hale getirmektedir. Suç oluşturan bir eylemin açıkça kanunda hukuka aykırı olduğunun belirtilmesi bir zorunluluk değildir ancak bazı suç tiplerinde

---

gönderilip gönderilmediği, nereye gönderildiği saptanıp sonucuna göre, toplanan deliller değerlendirilerek sanığın hukuki durumunun takdir ve tayini gerekirken, eksik incelemeye dayanarak yazılı şekilde hüküm kurulması,…BOZULMASINA…"Yargıtay 8. Ceza Dairesi E. 2016/5804 K. 2016/9313 T. 05.10.2016, (https://legalbank.net/arama/mahkeme-kararlari).

[372]Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6766.

[373] Artuk/Gökcen/Yenidünya, Ceza Hukuku Özel Hükümler, s. 767.

[374] Dülger, Bilişim Suçları, s. 343.

bu unsur yer almakta ve failin doğrudan kastla hareket etmesi aranmaktadır. TCK'nın 244. maddesinde düzenlenen suç tiplerinde hukuka özel aykırılık hali düzenlenmemiştir. Bu maddenin birinci fıkrasındaki eylemi bilişim sisteminin düzgün ve kesintisiz işleyişinde hak sahibi olan kişinin rızası, ikinci fıkrasındaki eylemi ise veriler üzerinde tasarruf yetkisi bulunan kişinin rızası hukuka uygun hale getirecektir. Rızanın açık veya zımni olmasının önemi bulunmaz.[375] Sistem güvenliğini test etmekle görevli kişinin sisteme yönelik eylemleri ilgili kişinin rızası dahilinde olduğu için suç teşkil etmeyecektir.[376]

Bir diğer hukuka uygunluk nedeni olan kanun hükmünün yerine getirilmesi de bu maddede belirtilen eylemleri hukuka uygun hale getirecektir. 5651 sayılı *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*un 8. maddesi internet erişiminin engellenmesini düzenler. Bu kapsamda koruma tedbiri olarak ya da idari yaptırım olarak erişimin engellenmesi mümkündür. Bu kanuna dayanarak görevin ifası çerçevesinde TCK'nın 244. maddesindeki suçun işlenmesi durumunda eylem hukuka uygun kabul edilecektir. Kanunlara aykırı faaliyet gösteren örgütlerin propaganda yapmak için kullandıkları web siteleri ile mücadele kapsamında görevlendirilen personelin imha faaliyetlerinde, personele yetki verilen ilgili kanunda açık hükmün bulunması durumunda eylem suç olarak kabul edilmeyecektir.[377] Dülger, 5651 sayılı Kanun'da erişim engeli ve içerik çıkarımının yöntemlerinin gösterildiği, herhangi bir kurum ya da kişiye bu eylemler için özel görev verilmediği, böyle bir durumun ifade özgürlüğüne de aykırı düştüğü gerekçeleriyle buna karşı çıkmaktadır.[378]

3.3.6. Suçun Nitelikli Halleri

5237 sayılı TCK'nın 244. maddesinin üçüncü fıkrasında suçun cezasını artıran nitelikli hali düzenlenmiştir. Bu düzenlenmeye göre maddenin birinci ve ikinci fıkralarında yer alan eylemlerin banka veya kredi kurumuna ait bilişim sistemi üzerinde ya da kamu kurum kuruluşlarına ait sistemlerde işlenmesi durumunda verilecek ceza yarı oranında artırılacaktır.

Söz konusu nitelikli halin düzenlenmesinde en büyük etken, bu kurumların finansal hizmetleri ile idarenin kamu hizmetlerinin bilişim sistemleri aracılığıyla yerine getirilip hizmet kayıtlarının bu sistemlerde muhafaza edilmesidir.[379] Bu nedenle 244. maddede sayılan fillerin

[375] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6767.
[376] Akbulut, Bilişim Alanında Suçlar, s. 204.
[377] Erdoğan, Bilişim Suçları, s. 201.
[378] Dülger, Bilişim Suçları, s. 345.
[379] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 863.

bahsi geçen kurum ve kuruluşlara yönelmesi ortaya çıkan neticenin daha ağır olmasına yol açacaktır. Akbulut, düzenleme kapsamının banka, kredi kurumu ve kamu kurum kuruluşlarıyla sınırlandırılmış olmasını yerinde bulunmamış, büyük bir şirket ya da işletmeler içinde bilişim sistemlerine yönelik eylemlerin de oldukça önemli olduğunu belirtmiştir.[380] Yine eleştirdiği diğer bir nokta da cezanın sabit artırımla artması yerine artırımda alt ve üst sınırların belirlenmesi gerektiğidir.[381]

Düzenlemede kullanılan banka ve kredi kurumu kavramlarının tanımları 5411 sayılı Bankacılık Kanunu'nda yapılmıştır.[382] Bu Kanun'un 157. maddesinde TCK'nın 244. maddesi kapsamında değerlendirilebilecek banka veya kredi kurumlarının bankacılık kanununa tabi kuruluşlar olduğu hükmüne yer verildiği görülmektedir. TCK'da düzenlenen bir hükmün ceza kanunu vasfında olmayan bir kanunda izah edilmesi doktrinde eleştiri konusu olmuştur.[383] Ayrıca 5237 sayılı TCK'nın 158/1-j maddesinin gerekçesinde kredi kurumu kavramının kanuni tanımına yer verildiği görülmektedir.[384] Böylece kredi kurumu kavramının iki farklı kapsamda değerlendirmeye tabi tutulduğu anlaşılmaktadır. Kanaatimizce banka veya kredi kurumu kavramlarının açıklamasına başka kanuna atıfta bulunmak suretiyle değil de TCK genel hükümlerde yer alan tanımlar başlıklı madde içerisinde yer verilmesi kanun sistematiği açısından daha doğru ve yerinde bir düzenleme olacaktır.

Suçun bir diğer nitelikli hali olarak düzenlenen kamu kurum ve kuruluşları ifadesinden ise devletin yasama, yürütme, yargı faaliyetlerini yürüttüğü merkez ve taşra teşkilatları ile yerel yönetimler, KİT'ler yani tüm idari kuruluşların anlaşılması gerekir.[385]

5237 sayılı TCK'nın 244. maddesindeki düzenleme 765 sayılı TCK'nın 525/b maddesiyle benzer eylemler içermektedir. 765 sayılı TCK'nın 525/b maddesinin yürürlükte olduğu dönemde eleştirildiği en önemli noktanın sistemin kişisel bir bilgisayar olmasıyla bir finans kuruluşunun ya da kamu kurumunun bilgisayarı olması durumlarında aynı müeyyideye tabi tutulması olduğu görülmektedir. Kişisel bir bilgisayarın erişiminin engellenmesiyle kamu kurumlarına ait bilgisayarlara erişimin engellenmesinin doğuracağı zararlar aynı boyutta

---

[380] Akbulut, Bilişim Alanında Suçlar, s. 205.
[381] Akbulut, Bilişim Alanında Suçlar, s. 205.
[382] Bankacılık kanunu madde 3'te tanımlamalar başlığı altında Banka ve kredi kurumunun tanımı yapılmıştır. Bu tanımlara göre banka; Mevduat bankaları ve katılım bankaları ile kalkınma ve yatırım bankalarını, kredi kuruluşu, Mevduat bankalarını ve katılım bankalarını ifade etmektedir. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf (Erişim Tarihi: 16.06.2022).
[383] Erdoğan, Bilişim Suçları, s. 199.
[384] "Kredi kurumu deyiminden banka olmamasına karşın, kanunen borç para vermeye yetkili kılınan kurumlar anlaşılır." https://legalbank.net/belge/turk-ceza-kanunu-gerekceler/2677276/TCK (Erişim Tarihi: 25.09.2022).
[385] Apaydın, "Bilişim Sistemindeki Verileri Yok Etme", s. 15.

olmayacaktır. Bu nedenle 244. maddenin üçüncü fıkrasının yerinde bir düzenleme olduğu söylenebilir.[386]

TCK'nın 244. maddesinin 4. fıkrasının doktrinde tartışma konusu olduğu görülmektedir. Bazı yazarlar bu eylemin bağımsız bir suç tipi olarak düzenlenmesi gerektiği görüşündedir.[387] Bu görüşe göre, bilişim sistemleri kullanılarak hukuksuz yarar sağlanması suçu maddenin ilk iki fıkrasında düzenlenen suç tiplerinden ayrı unsurlar taşıyan bir suçtur. Bazı yazarlar ise bu eylemin maddede düzenlenen suçların cezasını artıran nitelikli hal olduğunu savunmaktadır.[388] Kanun sistematiğine göre, suçun önce temel işlenme şekli ve cezası belirlenecek daha sonrada ağırlaştırıcı ve hafifletici sebepleri temel suç tipine bağlı kalınarak devamında yer alacaktır. 244. maddenin mevcut düzenlemesi incelendiğinde tartışma konusunu oluşturan dördüncü fıkranın birinci ve ikinci fıkrada yer alan suçun temel şekline bağlı kalarak düzenlendiği görülmektedir.[389] Bizim görüşümüze göre de bağımsız bir suç olarak değil, suçun basit şekline bağlı kalınarak düzenlenen nitelikli hal düzenlemesi olduğu yönündedir.

Bu fıkra ile yaşanan ikinci çelişki de madde metni ile gerekçesinin birbiriyle uyumlu olmamasıdır. 244. maddenin 4. fıkrasında eylemin başka bir suç oluşturmaması tabiri kullanılırken madde gerekçesi incelendiğinde daha ağır cezası olan başka bir suçun oluşmaması gerektiğinin ifade edildiği görülmektedir.[390] Gerekçe ile madde metni arasında uygulamayı zorlaştırabilecek nitelikte farklılık bulunsa da esas alınanın maddenin kendisi olduğu görülür.

Yargıtay'ın kararlarında da asli norm- tali norm ayrımı yapılarak tali norm niteliğindeki bilişim sistemleri aracılığıyla haksız yarar sağlama suçundaki eylemlerin başka bir suçu oluşturması halinde oluşan diğer suçtan cezalandırılma yapılacağı belirtilmiştir.[391]

---

[386] Dülger, Bilişim Suçları, s. 342.
[387] Dülger, Bilişim Suçları, s. 349; Erdoğan, Bilişim Suçları, s. 246; Yılmaz, "Bilişim Alanındaki Suçlar", s. 86.
[388] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 863.
[389] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 863.
[390] 244. maddenin 4. fıkrasının gerekçesi "Bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması halinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir." şeklindedir. Dülger, Bilişim Suçları, s. 349-350.
[391] "TCK'nın 244/4. maddesinde, "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde…" biçimindeki ifadeden bu fıkradaki düzenlemenin tali norm niteliğinde olduğunun anlaşılması, buna göre **öncelikle yasada düzenlenmiş olan bilişim sistemlerinin kullanılması suretiyle işlenebilen diğer suçların oluşup oluşmadığı değerlendirildikten sonra gerçekleştirilen eylem bu suçlardan hiçbirisinin tanımına uygun değil ise, bu durumda eylemin TCK'nın 244/4. maddesi kapsamında suç oluşturacağı** düşünülerek; müştekinin ..... Bankasında bulunan hesabına internet üzerinden ulaşan sanığın, müştekinin hesabına girerek 410,00 TL'yi havale yoluyla kendi hesabına havale ettiği, sanığın eylemindeki kastın, müştekinin banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi hesabına geçirmeye, müştekinin rızasına aykırı olarak mal varlığında azalmaya neden olmaya, var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yönelik olması nedeniyle, Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere; sanığın fiilinin TCK'nın 142/2-e maddesinde öngörülen "bilişim

Failin bir bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme, değiştirmeye yönelik eylemleriyle kendisine veya bir başkasına hukuka aykırı yarar sağlaması ve eyleminin de TCK'da başka bir suçu oluşturmaması durumlarında 244. maddenin 4. fıkrası uygulanacak ve verilecek temel cezada artırıma gidilecektir.[392] Kanun'daki bu düzenleme ile AKSS 8. maddesinde düzenlenen bilgisayarla bağlantılı dolandırıcılık hükmü karşılanmaya çalışılarak, aynı doğrultuda düzenleme yapıldığı görülmektedir.[393]

Terörle Mücadele Kanunu'nun 4. maddesinde bazı suçların sayıldığı ve suçların terör örgütünün faaliyeti çerçevesinde işlenmesi durumunda terör suçu sayılarak temel cezanın artırılacağı hükmü düzenlenmiştir. Söz konusu suçlar içerisinde TCK'nın 244. maddesine de yer verildiğinden bu suçu oluşturan eylemlerin terör faaliyeti olarak örgüt kapsamında işlenmesi cezayı artıran nitelikli hal olarak düzenlenmiştir. Aynı kanunun 5. maddesi hükmedilecek hapis cezası veya adli para cezasında hakime takdir yetkisi vermeyerek temel cezanın yarı oranında artırılacağını belirtmiştir. Suça sürüklenen çocuklar tarafından suç işlemek amacıyla kurulan bir terör örgütünün faaliyeti kapsamında TCK'nın 244. maddesinde sayılan eylemlerin gerçekleştirilmesi durumunda aynı kanun maddesi gereği nitelikli hal hükümleri uygulanmayacaktır.

3.3.7. Suçun Özel Görünüş Şekilleri

3.3.7.1. Teşebbüs

---

suretiyle hırsızlık" suçunu oluşturduğu gözetilmeden yazılı şekilde karar verilmesi,.. BOZULMASINA…" Yargıtay 17. Ceza Dairesi E. 2015/8568 K. 2016/2521 T. 29.02.2016, (https://legalbank.net/arama/mahkeme-kararlari).

[392] "Somut olayda oluşa uygun kabule göre; K... PTT Müdürlüğü Otomasyon Bölümü'nde bilgisayar teknisyeni olarak görev yapan sanık M... ile K...'de bulunan özel bir dershanede öğretmen olan diğer sanık A...'nın fikir ve eylem birliği içerisinde hareket ederek, 2002 yılının Mayıs ve Eylül ayları arasında Sivas, İstanbul-Fatih, Beyazıt, Bağcılar, Zeytinburnu, Küçükçekmece, Sefaköy, Merter, Bayrampaşa, Aksaray, Mecidiyeköy, Avcılar ve Kağıthane, Ankara- Ulus, Kızılay, Ahmetler, Emek ve Keçiören PTT merkezlerinden kabul işlemi yapılan bir kısım para havaleleri tutarlarına, PTT on-line sistemi veri tabanına girilmek suretiyle rakam ilave edilerek ödeme merkezlerince, gerçekte havale edilenden 10 veya 100 kat fazla tutarda ödeme yapılmasını sağlayarak **haksız menfaat temin eden sanıkların eylemlerinin** tamamen bilişim ortamında gerçekleştirilmiş olması, gerçek kişiye karşı yöneltilen her hangi hileli bir davranışın bulunmaması nedeniyle 765 sayılı TCK'nun 525/b-2. maddesindeki **(5237 sayılı TCK.nun 244/4 md) bilişim suçunu oluşturacağı** gözetilmeden yazılı şekilde hüküm kurulması…BOZULMASINA.." Yargıtay Ceza Genel Kurulu E. 2010/25 K. 2010/123 T. 25.05.2010, (https://legalbank.net/arama/mahkeme-kararlari).

[393] AKSS madde 8: "Taraflardan her biri, aşağıda belirtilenler, kasten ve haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir:

Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık niyetiyle;

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

b bir bilgisayar sisteminin işleyişine herhangi bir müdahalede bulunma"

https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf

TCK'nın 244. maddesinin birinci ve ikinci fıkralarında düzenlenen suç tipleri teşebbüs açısından herhangi bir özellik göstermemektedir. Söz konusu maddenin seçimlik hareketli suç olarak düzenlenmesi sebebiyle suçu oluşturan birden fazla eylemden sadece birinin gerçekleşmesi suçun tamamlanması için yeterli kabul edilmektedir.[394] Bu durumda suç tamamlandıktan sonra diğer eylemlerin henüz teşebbüs aşamasında kaldığı iddia edilemeyecektir. Failin suç işlemek amacıyla icra hareketlerine başlayıp elinde olmayan sebeplerle eylemini tamamlayamaması veya eylemin tamamlanmasına rağmen suçu oluşturan neticenin failin iradesi dışında gerçekleşmemesi gibi durumlarda suçun teşebbüs aşamasında kaldığı değerlendirilecektir.[395] Örneğin; mantık bombası zararlı yazılımıyla bilişim sistemine saldırı amaçlayan failin, sisteme gönderdiği mantık bombalarının yüklendiği ancak henüz harekete geçmeden sistem sahibi tarafından farkına varılıp müdahale edilmesiyle eylemin tamamlanamadığı durumlarda teşebbüs hükümlerinden söz edilecektir.

Sistemdeki verileri bozma amacıyla bilişim sistemine erişen fail elektriklerin kesilmesi sebebiyle verileri bozma eylemini tamamlayamadığında 244. maddenin ikinci fıkrasındaki suça teşebbüsten sorumlu olacak ancak 243. maddede düzenlenen bilişim sistemine hukuka aykırı girme veya kalma suçu tamamlanmış bir suç olduğu için bu suçtan cezalandırılacaktır.[396]

TCK'nın 244. maddesinde düzenlenen eylemleri kesin çizgilerle birbirinden ayırmak oldukça zordur. Çünkü failin bir hareketi aynı maddede belirtilen birden fazla kavramı karşılayabilmektedir. Verileri yok etmeye yönelik bir eylem aynı zamanda verileri bozma niteliğini, sistem işleyişine engel olmayı en nihayetinde her eylem hukuka aykırı bilişim sistemine girme veya kalma eylemini içermektedir. Yani failin kastettiği eylem teşebbüs aşamasında kalmış, fail icra hareketlerini tamamlamadan gönüllü olarak suçu işlemekten vazgeçmiş dahi olsa tamamlanmış başka bir suçu oluşturabilecektir.

Suç eylemlerinden biri olan verilerin değiştirilmesinde failin veri değişikliğinden sonra gönüllü vazgeçerek verileri eski haline getirmesi durumu doktrinde tartışılmıştır. Bir görüşe göre, verilerin değiştirilmesiyle birlikte suç tamamlanmış olacağından gönüllü vazgeçmenin şartları oluşmayacak ve uygulama imkânı doğmayacaktır.[397] Ancak bu durum etkin pişmanlık hükümlerini akla getirse de Kanun'da 244. maddedeki suçun etkin pişmanlık düzenlemesi bulunmaması nedeniyle o da uygulanamayacak failin cezası hafiflemeyecektir. Diğer görüş ise

[394] Yaycı, "Bilişim Suçları", s. 96.
[395] Yaşar/Gökcan/Artuç, Yorumlu - Uygulamalı Türk Ceza Kanunu, s. 6767-6738.
[396] Özbek/Kanbur/Doğan/Bacaksız/Tepe, Türk Ceza Hukuku Özel Hükümler, s. 870.
[397] Erdoğan, Bilişim Suçları, s. 234.

bu eylemi gönüllü vazgeçme hükümleri kapsamında değerlendirerek failin bu suçtan cezalandırılamayacağını ifade etmiştir.[398]

3.3.7.2. İştirak

TCK'nın 244. maddesinde düzenlenen suç tipleri iştirak bakımından bir özellik göstermemektedir. Bu sebeple 5237 sayılı TCK'nın 37 ile 41. maddeleri arasında düzenlenen suça iştirake ilişkin genel hükümler bu maddeye uygulanabilecektir.

Bir bilişim sisteminin truva atı yazılımının bir türü olarak değerlendirilen zombi bilgisayarlar suretiyle ele geçirilmesi ve ele geçirilen sistem üzerinden kötü niyetli kişilerce bilişim suçları işlenmesi durumunun iştirak bakımından bir özellik gösterip göstermediği incelenmelidir. Zombi bilgisayarlarda suçun asıl faili sistemi zararlı yazılımlarla ele geçirerek suçu işleyen kişi olmasına rağmen uygulamada ceza yargılamaları sırasında zombi bilgisayarların sistem sahiplerinin yargılandıkları görülmektedir. Failin doğru tespit edilebilmesi için sistemin asıl sahibiyle bilişim suçu işleyerek sistemi ele geçiren kişi arasındaki bağlantının irdelenerek herhangi bir anlaşma yapılıp yapılmadığı araştırılmalıdır.[399]

3.3.7.3. İçtima

TCK'nın 244. maddesinde düzenlenen suç tiplerinin hepsi zincirleme suç olarak işlenebilir. Failin aynı suç işleme kararını yerine getirmek için hareket ederken farklı zamanlarda aynı mağdura ait bilişim sistemleri veya verilerine karşı 244. maddedeki suç oluşturan eylemlerin birini veya birkaçını gerçekleştirmesi durumunda zincirleme suç hükümleri uygulanacaktır.[400] Bu maddenin ilk iki fıkrasında korunan hukuki değerleri farklı iki suç tipine yer verildiğinden zincirleme suç hükümlerinin uygulanabilmesi için failin eylemlerinin aynı fıkra kapsamında düzenlenenlere yönelik olması gereklidir.[401] Yargıtay tarafından verilen kararlarda aynı mağdura ait birden çok hesaba girilerek hesap şifrelerini

---

[398] Kurt, Bilişim Suçları, s. 266.
[399] Karagöz, "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", s. 140.
[400] 1- Sanığın öğrenim gördüğü Üniversitenin bilişim sisteminde yer alan ders notlarını yükseltmek şeklindeki eylemi nedeniyle hükmolunan cezanın üniversitenin kamu kurumu olması nedeniyle TCK.nun 244/3. maddesi gereğince arttırılması gerektiği gözetilmeden yazılı şekilde hüküm kurulması,
2- Sanığın **değişik tarihlerde dört kez, dört farklı ders notunu değiştirmiş olması nedeniyle hükmolunan cezanın TCK.nun 43. maddesi gereğince arttırılması** gerektiğinin gözetilmemesi..BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2012/33044 K. 2014/236 T. 08.01.2014, (https://legalbank.net/arama/mahkeme-kararlari).
[401] Dülger, Bilişim Suçları, s. 346-347.

değiştirme eyleminde her sistem için ayrı suç oluşmayacağı, aynı suç işleme iradesinin varlığı sebepleriyle zincirleme suç hükümlerinin uygulanacağı ifade edilmiştir.[402]

Bir bilişim sisteminin çalışmasına engel olmak amacıyla veya sistemde bulunan bir veriyi değiştirmek için aynı suç işleme kastıyla kısa zaman içerisinde birden çok kere bilişim sistemine etkide bulunulduğunda zincirleme suç hükümleri uygulanacaktır.[403] Ancak burada geçen zamana dikkat etmek gereklidir. Aradan uzun bir zaman geçtikten sonra eylem tekrar gerçekleşirse artık zincirleme suç oluşmayacak yeni bir suç olacaktır.

Söz konusu suçta aynı neviden fikri içtima hükmünün uygulanması da söz konusu olabilir. Günümüzde bilişim suçu işlenme yöntemleri içinde oldukça yaygın kullanılan bilişim virüslerinin internet ağları aracılığıyla birçok mağdurun bilişim sistemi ve verilerine bulaşarak zarar vermesi hali bu duruma örnek gösterilebilir.[404] Failin tek bir virüs bulaştırma eylemiyle birden fazla mağdur zarar görecektir. Bu gibi durumlarda her mağdur için ayrı cezalandırma yapılmayacak TCK'nın 43'üncü maddesi gereği fail hakkında tek bir hüküm kurularak cezasında artırım yapılacaktır.

Failin tek bir eylemiyle 244. maddenin birinci fıkrasında düzenlenen bilişim sistemlerine yönelik suç ile ikinci fıkrasındaki verileri korumaya yönelik suçun birlikte işlenmesi mümkündür. Bu durumda failin hangi madde kapsamındaki suçtan sorumlu olacağının iyi tespit edilmesi gereklidir. Doktrinde bu durumda fikri içtima hükümlerinin uygulanması gerektiğini ifade eden yazarlar bulunmaktadır. Buna göre; bilişim sistemlerini hedef alan eylemler

---

[402] "Sanık ...'un, mağdurlar ... ve ...'ya ait MSN adreslerinin ve facebook hesaplarının internet şifrelerini, onların rızası dışında değiştirerek, mağdurların bilişim sistemindeki hesaplarına erişimlerini engellemesi şeklinde sübutu kabul edilen eylemlerinden dolayı TCK'nın 244/2. madde ve fıkrasında tanımı yapılan sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan mağdur sayısınca iki ayrı mahkumiyet hükmü kurulması ve **MSN ile facebook hesaplarının iki farklı bilişim sistemi olmasından dolayı bir suç işleme kararının icrası kapsamında değişik zamanlarda her bir mağdura karşı aynı eylemi birden fazla işleyen sanık hakkında TCK'nın 43/1. madde ve fıkrasında düzenlenen zincirleme suç hükmünün uygulanması gerektiği gözetilmeden**, sistemi engelleme, bozma, verileri yok etme veya değiştirme suçundan tek bir mahkumiyet hükmü kurulup, zincirleme suç hükümlerinin uygulanmaması ve olayda uygulama alanı bulunmayan TCK'nın 243/1. madde ve fıkrasındaki bilişim sistemine girme suçundan da ayrıca mahkumiyet hükmü kurulması, kanuna aykırı,.." Yargıtay 12. Ceza Dairesi E. 2016/10818 K. 2017/7390 T. 11.10.2017, (https://legalbank.net/arama/mahkeme-kararlari).

"Oluşa ve tüm dosya kapsamına göre; **mağdura ait Facebook ve MSN hesaplarına giren ve hesap şifrelerini değiştirmek suretiyle mağdurun hesaplara erişimini engelleyen** sanığın, eylemine uyan TCK.nun **244/2, 43. madde** ve fıkraları uyarınca mahkumiyetine karar verilmesi gerektiği gözetilmeden sanığın suç kastı bulunmadığından bahisle yasal ve yeterli olmayan gerekçeyle beraatine hükmolunması,... BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2013/13127 K. 2014/10178 T. 21.04.2014, (https://legalbank.net/arama/mahkeme-kararlari).

[403] Dülger, Bilişim Suçları, s. 346.

"Katılan kurumun **bilişim sistemine değişik zamanlarda birden fazla girerek izinsiz veri yerleştirdiği** anlaşılan sanık hakkında koşulları oluştuğu halde, **TCK.nun 43/1. maddesinin** uygulanmayarak eksik ceza tayini,… BOZULMASINA.." Yargıtay 8. Ceza Dairesi E. 2017/21187 K. 2017/13485 T. 29.11.2017, (https://legalbank.net/arama/mahkeme-kararlari).

[404] Dülger, Bilişim Suçları, s. 347.

sistemdeki verilere yönelik eylemlerden daha ağır bir cezayı gerektirmekte ve sistemdeki verilerin hedef alınmasına rağmen bilişim sisteminin engellenmesi veya bozulması sonucu oluşuyorsa TCK'nın 244. maddesinin 1. fıkrasının uygulanması gerektiği düşünülür.[405]

Bu suçun cezayı artıran nitelikli hallerinden biri olan 244. maddenin 4. fıkrasındaki hukuka aykırı yarar sağlama suçu oluştuğunda bahse konu suçun birinci ve ikinci fıkrası suçun unsuru haline dönüşerek bileşik suç oluşturacak dolayısıyla sadece dördüncü fıkradan hüküm kurulacaktır.[406] Düzenlemede "başka bir suç oluşturmama" ifadesine açıkça yer verildiği görülmektedir. Dolayısıyla 244. maddenin 4. fıkrasına göre suç oluşturan eylemler Kanun'da düzenlenen başka bir suçu daha oluşturuyorsa, ilgili suç hükümleri uygulanacaktır.

Failin suç oluşturan eyleminin 244. maddede belirtilen suçlar ile 243. maddede bilişim sistemine girme suçu arasındaki bağlantı ve belirtilen suçların her ikisi kapsamında kaldığı durumlarda doktrindeki tartışmalara bilişim sistemine girme suçunda yer verdiğimiz için çalışmamızın bu kısmında tekrar değinilmeyecektir.

TCK'nın 244. maddesi ile bilişim sistemleri kullanılarak gerçekleştirilen dolandırıcılık suçları (TCK m. 158/1-f) ve hırsızlık suçları (TCK m.142/2-e) arasında bağlantıdan söz edilebilir. Kanun sistematiğinde dolandırıcılık ve hırsızlık suçlarının nitelikli hali olarak düzenlenen eylemler aslında bir bilişim suçunu oluşturmaktadır. Yargıtay bir kararında haksız ele geçirilen bankacılık bilgileriyle mağdurun hesabındaki paranın internet üzerinden failin kendi hesabına havale göndermesi eyleminin TCK'nın m.142/2-e'de düzenlenen hırsızlık suçunu oluşturduğunu ifade etmiştir.[407] Failin mağdura ait e-posta hesabını ve hesaba bağlı facebook adresini haksız ele geçirerek, sistem şifrelerini değiştirmesi devamında mağdurun hesabında ekli arkadaşlarına kendisini mağdur olarak tanıtarak kontör gönderilmesini istemesi

---

[405] Erdoğan, Bilişim Suçları, s. 236.

[406] Akbulut, Bilişim Alanında Suçlar, s. 210; Özbek/Kanbur/Doğan/Bacaksız/Tepe, s. 871.

[407] "Kabule göre de; Yargıtay Ceza Genel Kurulu'nun 17.11.2009 gün ve 193/268 sayılı kararında açıklandığı üzere; sanığın, bir şekilde haksız olarak ele geçirdiği katılanlara ait bankacılık bilgilerini kullanarak, internet aracılığıyla, katılanların ... Bankasına ait banka hesaplarından, kendine ait aynı bankanın... Şubesinde bulunan hesabına havale edip çektiğinin anlaşılması karşısında; sanığın kastının katılanın banka hesabında bulunan parayı bilişim sistemini kullanmak suretiyle kendisinin kullanımındaki banka hesabına geçirmeye, katılanın rızasına aykırı olarak mal varlığında azalmaya neden olmaya, başka bir anlatımla **var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil edildiği parayı alarak mal edinmeye yönelik olduğu, eyleminin 5237 sayılı TCK.nun 142/2-e maddesine uyan hırsızlık suçunu oluşturduğu** gözetilmeksizin, yazılı şekilde anılan yasanın 244. maddesinden hüküm kurulması,.. BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2014/31977 K. 2015/7086 T. 12.02.2015, (https://legalbank.net/arama/mahkeme-kararlari).
"Oluşa ve tüm dosya kapsamına göre; katılanın bir Banka Şubesinde bulunan şahsi ve ticari hesaplarına internet bankacılığı yoluyla girilerek sanığın, Bankanın bir başka şubesinde bulunan hesabına para havale edilmek suretiyle atılı suçun işlediğinin anlaşılması karşısında, sanığın eyleminin TCK.nun 142/2-e madde ve fıkrasında düzenlenen bilişim sistemlerinin kullanılması suretiyle hırsızlık suçunu oluşturduğu gözetilmeden sanığın TCK.nun 244/4 madde ve fıkrası gereğince cezalandırılmasına karar verilmesi,…BOZULMASINA…" Yargıtay 8. Ceza Dairesi E. 2014/36637 K. 2015/21012 T. 07.09.2015,(https://legalbank.net/arama/mahkeme-kararlari).

durumunda Yargıtay nitelikli dolandırıcılık ile bilişim sisteminin işleyişinin engellenmesi suçlarının oluştuğuna karar vermiştir.[408]

3.3.8. Muhakeme ve Yaptırım

5237 sayılı TCK'nın 244. maddesinin birinci ve ikinci fıkrasında düzenlenen suç tiplerinde seçimlik ceza öngörülemeyerek sadece hapis cezasına yer verilmiştir. Bu kapsamda birinci fıkrada bilişim sistemlerine yönelik gerçekleşen eylemlerin cezası bir yıldan başlayarak beş yıla kadar, ikinci fıkrada yer alan ve sistemdeki verileri hedef alan eylemlerin ise ilk fıkraya göre daha hafif nitelikte altı aydan üç yıla kadar hapis cezası olarak belirlenmiştir. Kanun koyucunun cezalandırma yaparken bilişim sistemlerini, sistemdeki verilerden üstün tuttuğu görülmektedir. Suçun daha ağır cezayı gerektiren hali birinci fıkra düzenlemesidir.

Düzenlemenin üçüncü fıkrasındaki suçun nitelikli halinde ilk iki fıkrasında belirtilen hürriyeti bağlayıcı nitelikteki temel cezanın alt ve üst sınırının yarı oranında artırılacağı hükme bağlanmıştır.

Madde içeriğinde hem hapis cezası hem de adli para cezası içeren tek düzenleme dördüncü fıkradır. Suç oluşturan eylemler neticesinde haksız bir yarar sağlanması halinde fail, iki yıldan başlayarak altı yıla kadar hapis cezasıyla ayrıca yargılamada görevli hakimin takdir yetkisinde beş bin güne kadar adli para cezasıyla da cezalandırılacaktır.

TCK'nın 244. maddesinde düzenlenen suçların soruşturulması veya kovuşturmasının yapılabilmesi için mağdurun veya suçtan zarar görenin şikâyeti aranmayacak, tüm yargılama süreci re'sen yürütülecektir. Bahse konu suçların yargılamalarında görevli mahkeme 5235

---

[408] "Sanığın mağdur M.. E..'a ait elektronik posta adresini ve bu adresine bağlı facebook hesabını ele geçirdiği, şifrelerini değiştirerek mağdurun ulaşımını engellediği, söz konusu facebook hesabına ekli olarak bulunan mağdurlar G.. T.. ve M... S... G...'a facebook adresinden ulaşarak kendisini M.. E.. olarak tanıtmak sureti kontör gönderilmesini istediği ancak mağdurların şüphelenerek kontör göndermediğinin iddia edildiği olayda,
1- Sanığın Mağdurlar G.. T.. ve M... S... G...'a karşı işlediği dolandırıcılık suçlarından dolayı kurulan hükme yönelik temyiz itirazlarının incelenmesinde, Sanığın üzerine atılı **nitelikli dolandırıcılık suçlarının sanık tarafından işlendiğine dair mahkemenin mahkumiyet yönünde kabulünde isabetsizlik görülmemiştir.**
Yapılan yargılamaya, toplanıp karar yerinde gösterilen delillere, mahkemenin kovuşturma sonuçlarına uygun olarak oluşan kanaat ve takdirine, incelenen dosya kapsamına göre; sanığın kararın usul ve yasaya aykırı olduğu, lehe hükümlerin uygulanmadığı, mağdurun şikayetinden vazgeçtiğine dair temyiz itirazlarının reddiyle, hükümlerin ONANMASINA,
2- Sanığın bilişim sisteminin işleyişi engelleme suçundan mahkumiyetine ilişkin hükme yönelik temyiz itirazlarının incelenmesinde,
Mağdura ait elektronik postaya bağlı facebook hesabının şifresini ele geçirerek bu adrese giren, yazışmalar yapan ve şifreyi değiştirmek suretiyle mağdurun anılan hesaba erişimini engelleyen sanığın eyleminin, 5237 sayılı **TCK'nın 244/2. maddesinde düzenlenen suçu oluşturacağı** gözetilmeden suç vasfında hataya düşülerek yazılı şekilde hüküm kurulması…" Yargıtay 15. Ceza Dairesi E. 2013/32575 K. 2016/5124 T. 18.05.2016, (https://legalbank.net/arama/mahkeme-kararlari).

sayılı Kanun gereği asliye ceza mahkemeleridir.[409] Bilişim suçlarının yargılamalarının doğru yapılabilmesi için hakimlerin sadece hukuki bilgiye sahip olması yetmemekte aynı zamanda teknik bazı bilgilerinin de bulunması gerekmektedir. Bu kapsamda 2021 yılında ceza mahkemelerinde ihtisaslaşmaya gidildiği görülmektedir. Çalışmamızın 243. maddesinde de değindiğimiz gibi HSK'nın 1229 sayılı ihtisas kararıyla bilişim suçlarıyla görevli asliye ceza mahkemeleri belirlenmiştir. Ancak bu ihtisas mahkemelerinde görevli hakimlerin meslek içinde yeterli bir eğitime tabi tutulup tutulmadıkları, eğitimlerin başarısı , uygulamada kolaylık sağlayıp sağlamadığı ve yargılamaların teknik ve hukuki bilgi uyumuyla hatasız sonuçlanma başarısı ileriki zamanlarda ortaya çıkacaktır.

Tablo 3. TCK m. 244 (Soruşturma Verileri)

TCK m.244	Cumhuriyet Başsavcılıkları Soruşturma Dosya Sayısı	Kovuşturmaya Yer Olmadığı	Kamu Davası Açılan	Yetkisizlik	Görevsizlik
2021	37 576	31 673	2 017	3 461	-
2020	15 172	11 649	1 361	1 912	6
2019	15 161	11 304	1 720	1 834	17
2018	16 967	13 044	1 745	1 923	6
2017	13 122	8 801	1 694	2 329	1

Kaynak: https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsiv

[409] https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf (Erişim Tarihi: 05.10.2022).

Ülkemizde geçtiğimiz son beş yılda Cumhuriyet Başsavcılıklarında 5237 sayılı Kanun'un 244. maddesi kapsamında yürütülerek karara bağlanan soruşturma dosyalarına dair veriler incelendiğinde, 2017 ile 2020 yılları arasında yürütülen soruşturma dosya sayılarının birbirine yakın olduğu ancak 2021 yılına geldiğinde ise önceki yıllara göre büyük bir artış yaşandığı gözlemlenir. Bu artış bilişim suçlarının toplumda ne kadar yaygınlaştığının bir kanıtıdır. Yine belirtilen yıllarda dosya sayılarının büyük bir bölümünün KYOK kararıyla neticelendiği görünmekte bu durumun temel sebebinin de tablo 1.'de yaptığımız yer sağlayıcılarından bilgi temini yapılamaması açıklamasıyla paralel olduğu kanaatindeyiz. Yine son beş yılda verilen yetkisizlik kararlarının da oldukça fazla olduğu görülmektedir. Bu durum uygulamada yetki hususunda yaşanan karmaşanın somut olarak verilere yansımadır. Görülmektedir ki bilişim suçlarının zamansız ve mekânsız suçlar olması dolayısıyla özel bir yetki kuralına ihtiyacı bulunmaktadır.

Tablo 4. TCK m. 244 Ceza Mahkemelerinde Sanıkların Yaş ve Uyruk Dağılımı

TCK m.244	Toplam Sanık Sayısı	Yabacı Uyruklu	12-14 Yaş	15-17 Yaş	18+ Yaş
2021	2 019	38	47	91	1 840
2020	1 334	23	48	69	1 194
2019	1 607	23	45	108	1 431
2018	1 730	35	37	94	1 564
2017	1 917	15	34	58	1 809

Kaynak: https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçuyla ilgili olarak veriler incelendiğinde 2017 ile 2020 yılları arasında azalıp artan bir dalgalanma olduğu ancak 2021 yılında bir önceki yıla göre toplam sanık sayısında iki kat bir artış olduğu görülmektedir. Bunların büyük çoğunluğunun 18 yaşın üzerinde olması sebebiyle suça sürüklenen çocukların ve yabancı uyrukluların bu suçu işleme meyillerinin az olduğu yorumlanmaktadır.

SONUÇ

Bilişim teknolojilerinde özellikle yirminci yüzyılın sonlarına doğru yaşanan değişimler hayatın her alanında bilgisayarların, bilişim sistemlerinin yaygınlaşmasına sebep olmuştur. Bu değişim ve gelişimler yeni suç tiplerini beraberinde getirmiş ayrıca faillerin suç işlerken kullandıkları yöntemleri de güncellemiştir. Klasik suç tiplerinin bu yeni suç işleme modelleriyle işlenmesiyle çok daha büyük zararlar meydana gelmesine rağmen hukuksal bir düzenlemenin bulunmaması cezalarda adalet dengesini bozan orantısızlıklara yol açmıştır. Oluşan bu kanun boşluklarının hissedilmesiyle Türk Ceza Hukuku açısından bilişim suçlarına ilişkin düzenlemeler yapılması ihtiyacı doğmuştur.

Bilişim suçlarının yarattığı tehlikenin ülkelerin sınırlarını aşan boyutta olması uluslararası mücadele ve iş birliği ihtiyaçlarını doğurmuştur. Uluslararası kuruluşların bilişim suçlarına yönelik birçok çalışmalar yaptığı ve tavsiye kararları yayınladıkları görülmektedir. Tüm bunlardaki genel amacın bilişim suçlarında uluslararası alanda geçerli normlar oluşturma olduğu söylenebilir. Avrupa Konseyi'nin bu konuda diğer kuruluşlara göre daha etkin çalıştığı ve amaca yaklaştığı değerlendirilmektedir.

Türk Ceza Hukuku'nda bilişim suçları düzenlenirken kanun koyucunun suçun koruduğu hukuki değeri esas alarak düzenleme yaptığı görülmektedir. Buna göre suçun koruduğu hukuki değeri tam olarak tespit edilebilen ve kanunda ayrı bir maddede düzenlenmiş klasik suç tiplerinin bilişim suçlarıyla işlenmesi durumlarında eylemi ilgili olduğu maddenin içerisinde düzenlemiştir. Suçla korunan hukuki değeri tam olarak tespit edilemeyen, birden fazla hukuki değeri koruyan veya bilişim sisteminin yararının korunduğu durumlarda ise Kanun'un onuncu bölümünde yer alan bilişim alanında suçlar başlığı altında düzenleme yoluna gidilmiştir. Kanun koyucunun tercih ettiği bu yaklaşım oldukça yerinde olmuştur. Çünkü bilişim alanı gelişmeye devam eden geleceği öngörülemeyen ucu oldukça geniş bir alan olarak karşımıza çıkmaktadır. Tek bir başlık altında bu suçları sınırlayabilmek birçok eylemin cezasız kalmasına neden olabilecektir. Bu nedenle bilişim suçlarıyla ilgili kanun sistematiğimizin yerinde olduğunu düşünmekteyiz.

5237 sayılı TCK'da bilişim alanında suçlar bölümünde düzenlenen suç tipleri incelendiğinde; kanun koyucunun suçu oluşturacak eylemlere tek tek ve oldukça geniş kapsamda yer verdiği görülmektedir. TCK'nın 243. maddesinde bilişim sistemlerine girme eylemi yaptırım altına alınmıştır. Bu madde ile bilişim sistemlerinin güvenliği koruma altına alınmak istenmiştir. Maddenin birinci fıkrası bilişim sistemlerine hukuka aykırı olarak girilmesi veya sistemde hukuka aykırı kalınması eylemlerini düzenlemiştir. AKSS'de yer alan yasa dışı

araya girme düzenlemesiyle kanun metnimizin aynı paralellikte olduğu görülür. Bu uyumlaştırma 2016 yılında 6698 sayılı Kanun'un 30. maddesiyle getirilen değişikliklerle gerçekleştirilmiştir. Kanun metninde yer alan "ve" bağlacı "veya" olarak değiştirilmiş böylece hem madde AKSS ile uyumlu hale gelmiş hem de uygulamadaki tartışmalar son bulmuştur. Bize göre de yapılan bu değişiklik oldukça yerinde olup madde taslağında ve madde gerekçesinde "veya" olarak kullanılan bağlacın TBMM'de "ve" olarak kabulü suçun eylem unsurunda bir hayli karışıklıklara sebep olduğundan oldukça eleştirilmekteydi. Örneğin bir bilişim sistemine haksız olarak giren kişi sistemde kalmaya makul bir süre devam etmez ise suçun eylem unsuru gerçekleşmemiş olduğundan cezalandırılamıyordu. Oysaki bir bilişim sistemi sistem sahibinin kişisel alanı niteliğindedir ve bu alana rıza dışında girilmesi yaptırımsız bırakılmamalıdır. Nitekim kanun koyucunun da yaptığı düzenlemeyle hatalı uygulamaya son verdiği görülmektedir.

TCK'nın 243. maddesinin üçüncü fıkrasında bilişim sistemindeki veriler düzenlenmiştir. Bilişim sistemine girme suçu kasten işlenebilen bir suçtur. Failin sisteme hukuka aykırı girme veya kalma hususunda kasıtlı icra hareketlerinde bulunması gereklidir. Üçüncü fıkrada ki suçun oluşabilmesi içinde failin bilişim sistemine girme, sistemde kalma kastıyla hareket ederken bu eylem neticesinde bir zarara yol açarak sistemdeki verilerin yok olup, bozulması sonucunun ortaya çıkması gereklidir. Yani failin eylemi sisteme yönelik olacaktır. 244. maddenin ikinci fıkrasında da kanun koyucu verilerin yok olması ve bozulması durumlarını düzenlemiştir. Bu iki fıkranın ayrımında failin kastı önem taşımaktadır. Öncelikle failin kastı ve hareketleri sistemdeki verileri yok etmeye mi yönelik yoksa sadece sisteme girme çabasındayken mi sonuç meydana gelmiş tespiti gereklidir.

TCK'nın 243. maddesinde suçun kamu kurumu, banka, kredi kuruluşu, büyük şirketler gibi yerlere yönelik işlenmesi durumuyla ilgili bir düzenleme yapılmamış olması büyük eksikliktir. Çünkü kişisel bir bilişim sistemine hukuka aykırı girilmesi eylemiyle bir kamu kurumuna ait bilişim sistemine hukuka aykırı girilmesi eylemlerinin aynı etkide olduğu söylenemeyecektir. Bu durumun cezayı artırıcı nitelikli hal olarak düzenlenmesi gerektiğini düşünmekteyiz. Yine aynı maddenin 4. fıkrasında yer alan veri nakillerini sisteme girmeksizin teknik araçlarla izleme suçunun düzenlendiği suç başlığından bağımsız, bilişim alanında suçlar başlığı altında ayrı bir suç olarak düzenlenmesinin daha yerinde olacağı düşüncesindeyiz.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçlarının düzenlemesinde kanun koyucunun birinci fıkra ile ikinci fıkrada iki farklı suç türüne yer verdiği görülmektedir. Birinci fıkrada suçun konusu bilişim sistemleri oluştururken ikinci fıkrada verilerin ortadan kaldırılması, erişimin engellenmesine yönelik eylemler düzenlenmiştir. Bilişim sistemini

engellenme ve bozma suçunun bu madde başlığı altında düzenlenmesi aslında kanun sistematiğiyle uyuşmamaktadır. Türk Ceza Kanunu'nda suçlar düzenlenirken ilk önce suçun temel halinin düzenlemesi yapılıp devamında nitelikli hallerine yer verilirken 244. maddenin farklı bir yaklaşımla düzenlediği görülmektedir. Buna göre ilk fıkrada düzenlenen bilişim sisteminin bozulması ikinci fıkradaki verilere yönelik eylemlerin ağırlaştırılmış hali çıkarımı yapılmaktadır. Kanun koyucunun bu hususları dikkate alarak yeni bir düzenleme yapmasına ihtiyaç olduğu kanaatindeyiz.

Düzenlemede yer verilen verilere yönelik eylemlerin birbirinden kesin ve net bir şekilde ayrılma olanağı bulunmamaktadır. Yani failin işlediği bir eylem fıkradaki birden fazla durumun oluşmasıyla neticelenebilir. Bu durumların aynı fıkrada düzenlenmiş olması, uygulamada suçun oluşumu kapsamında bir karışıklığa neden olmayacaktır. İkinci fıkrada sayılan eylemlerden birinin ya da birkaçının birlikte gerçeklemesi durumunda da yine tek bir suç oluşacak ancak cezanın belirlenmesinde bu durum dikkate alınacak ve temel cezadan uzaklaşılarak cezaya hükmedilebilecektir.

TCK'nın 244. maddesinin birinci fıkrasında düzenlenen bilişim sisteminin işleyişinin engellenmesi ve bozulması suçunun maddenin ikinci fıkrasında sayılan eylemlerle gerçekleştirildiği durumlarda hangi fıkra kapsamında değerlendirileceğine dair tartışmada; bize göre sistemi engelleme veya bozma eylemlerinin hangi yolla gerçekleştirildiğinin bir önemi bulunmamaktadır. Verilerin bozulması sistem sahibinin olağan olarak bilişim sistemine girmesini engelliyorsa burada artık sistemi engelleme veya bozma suçunun oluşacağı kanaatindeyiz.

Bilişim suçlarında yetki konusu da uygulamada oldukça karışıklıklara yol açan, belirsizlikler bulunan bir nokta olarak karşımıza çıkmaktadır. Genel yetki kurallarının bu suç tipinde uygulanması uygun görülmemektedir. Bu kararsızlıkları çözümleyecek bir düzenlemeye ihtiyaç bulunduğunu düşünmekteyiz.

KAYNAKÇA

Adli Sicil İstatistik Genel Müdürlüğü. https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adalet-istatistikleri-yayin-arsivi. (Erişim Tarihi:11.09.2022).

Akbulut Bozdoğan, B. (2000). Bilişim Suçları. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, 8*(1-2), 545-555.

Akbulut, B. (2016). Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme. *Selçuk Üniversitesi Hukuk Fakültesi, 24*(2), 7-55.

Akbulut, B. (2017). *Bilişim Alanında Suçlar.* Ankara: Adalet Yayınevi.

Ansiklopedik Kişisel Bilgisayar Klavuzu 10. (1995, Ocak). 1-9. PC World.

Apaydın, C. (2015). Bilişim Sistemindeki Verileri Yok Etme, Bozma, Erişilmez Kılma, Değiştirme, Hukuka Aykırı Olarak Verileri Yerleştirme veya Gönderme Suçu ile Bu Suretle Hukuka Aykırı Yarar Elde Etme Suçunun Değerlendirilmesi. *Terazi Hukuk Dergisi, 10*(111), 14-41.

Arslan, M. E. (20 Ağustos 2022). *SİBER GÜVENLİK VE SİBER SALDIRI TÜRLERİ*. https://www.academia.edu/31827545/S%C4%B0BER_G%C3%9CVENL%C4%B0K_VE_S%C4%B0BER_SALDIRI_T%C3%9CRLER%C4%B0_CYBER_SECURITY_AND_CYBER_ATTACK_TYPES_03_05_2016.

Artuk, M. E., Gökcen, A., ve Yenidünya, A. C. (2014). *Ceza Hukuku Özel Hükümler.* Ankara: Adalet Yayınevi.

Avrupa Konseyi Bakanlar Komitesi. https://rm.coe.int/09000016804f1094.(Erişim Tarihi: 20.03.2022)

Avrupa Konseyi Bakanlar Komitesi. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76.(Erişim Tarihi: 20.03.2022).

Aydın, E. D. (1992). *Bilişim Suçları ve Hukukuna Giriş.* Ankara: Doruk Yayınları.

Bellek Türleri. http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/06/bellek-turleri.(Erişim Tarihi: 22.04.2022).

Bilgisayarda Model Hukuku ve Bilgisayarla İlgili Suç.

https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf.(Erişim Tarihi: 17.03.2022).

Birleşmiş Milletler Suçun Önlenmesi ve Suçluların Muhafazası Kongresi. https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf.(Erişim Tarihi: 07.03.2022).

BM 8. Suçtan Korunma ve Suçluların Rehabilitasyonu Kongresi. https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf. (Erişim Tarihi: 27.03.2022).

Brenner, S. (2001). State Cybercrime Legislation in the United States of America: A Survey, Richmond Journal of Law And Technology, 7(3), 1-16. https://core.ac.uk/download/pdf/232774633.pdf.(Erişim Tarihi: 07.07.2022).

Canbek, G., ve Sağıroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *22*(1), 121-136.

Commonwealth.https://thecommonwealth.org/news/commonwealth-cybercrime-experts-barbados-call-robust-cybersecurity. (Erişim Tarihi: 17.03.2022).

Convention on Cybercrime. https://rm.coe.int/1680081561.(Erişim Tarihi: 05.05.2022).

Cybercrime - Siber Suç.https://www.unodc.org/unodc/en/cybercrime/index.html.(Erişim Tarihi: 09.03.2022).

Cybercrime Law.https://www.cybercrimelaw.net/Italy.html. (Erişim Tarihi: 12.04.2022).

Çeken, H. (07 Nisan 2022). *Amerika Birleşik Devletlerinde Siber Suçlar*. http://archiv.jura.uni-saarland.de/turkish/HCeken.html.

Çetin, M. S. (2021). Yargıtay Kararları Işığında Bilişim Sistemine Girme veya Kalma Suçu (TCK M. 243). *Türkiye Adalet Akademisi Dergisi*(45), 1-28.

Dandin, A. N. (2019). *Risk Toplumunda Bilişim Suçları ve Hukukun Etkinliği*. Yayımlanmamış Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi. Afyonkarahisar.

Değirmenci, O. (2003). Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukuktaki Düzenlenişi. *Legal Hukuk Dergisi, 1*(11), 2750-2758.

Değirmenci, O. (2005). 2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi. *Türkiye Barolar Birliği Dergisi, 18*(58), 195-208.

Değirmenci, O. (2002). *Bilişim Suçları.* Yayımlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi. İstanbul.

Değirmenci, O., ve Yenidünya, A. C. (2003). *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları* (1. b.). İstanbul: Legal Yayıncılık.

Dülger, M. V. (2017). Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması. *Türkiye Adalet Akademisi Dergisi,* 8(31), 141-258.

Dülger, M. V. (2020). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Yayıncılık.

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

ENIAC.https://tr.wikipedia.org/wiki/ENIAC. (Erişim Tarihi: 05.09.2022).

Erdağ, A. İ. (2010). Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda). *Gazi Üniversitesi Hukuk Fakültesi Dergisi,* 14(2), 275-303.

Erdoğan, Y. (2010). Bilişim Sistemine Girme ve Kalma Suçu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 12(0), 1363-1433.

Erdoğan, Y. (2012). *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle).* İstanbul: Legal Yayıncılık.

Erdoğan, Y. (2018). *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri.* İstanbul: Legal Yayıncılık.

Erem, F. (1993). Bilgisayar Suçları ve Türk Ceza Kanunu. *Türkiye Barolar Birliği Dergisi,* 5(2), 178-186.

Erkan, B., ve Songür, M. (1999). *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü.* Ankara: Hacettepe-Taş Yayınları.

Ersoy, Y. (1994). Genel Hukuki Koruma Çerçevesinde Bilişim Suçları. *Ankara Üniversitesi SBF Dergisi, 49*(3), 149-183.

Esen, H. Ö. (1998). *İşletme Yönetiminde Sistem Yaklaşımı* (3. b.). İstanbul: Alfa Yayınları.

Goodman, M. (2010). *Cybercrimes: A Multidisciplinary Analysis.* (S. Ghosh, & E. Turrini, Dü) Berlin: Springer.

Hacker.https://www.techtarget.com/searchsecurity/definition/hacker.

(ErişimTarihi:13.08.2022).

Hâkimler ve Savcılar Kurulu Birinci Dairesinin Kararı. https://www.hsk.gov.tr/Eklentiler/301120210928251120 21-1229pdf.pdf.

(Erişim Tarihi: 15.09.2022).

Hoşcan, Y. (2003). *Yönetim Bilgi Sistemi* (2. b.). Ankara: Anadolu Üniversitesi Yayınları.

İçel, K. (2001). Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 59*(1-2), 5.

İhtiyaroğlu, U. (2020). Bilişim Sistemlerine Girme Suçunun Yargı Kararları Bağlamında İncelenmesi. *Hacettepe Hukuk Fakültesi Dergisi, 10*(2), 406-440.

İletişim Ahlakı Yasası.https://www.britannica.com/topic/Communications-Decency-Act. (Erişim Tarihi: 07.04.2022).

Independent Türkçe.

https://www.indyturk.com/node/134161/haber/t%C3%BCrkiyedeki-internet-kullan%C4%B1c%C4%B1lar%C4%B1na-da-sald%C4%B1ran-truva-at%C4%B1-tespit-edildi%E2%80%A6-23. (Erişim Tarihi: 20.08.2022).

İngiliz Milletler Topluluğu.

https://tr.wikipedia.org/wiki/%C4%B0ngiliz_Milletler_Toplulu%C4%9Fu. (Erişim Tarihi: 14.03.2022).

İnternet Tarihi. http://www.internetarsivi.metu.edu.tr/tarihce.php.(Erişim Tarihi: 18.11.2021).

INTERPOL.https://www.interpol.int/Crimes/Cybercrime.(Erişim Tarihi: 17.03.2022).

Kangal, Z. T. (2011). Fransa'da İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğu. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 59*(1-2), 227-240.

Karagöz, M. C. (2019). *Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu (TCK m. 244).* Yayımlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi. Antalya.

Karahoca, D., ve Karahoca, A. (1998). *Yönetim Bilişim Sistemleri ve Uygulamaları.* İstanbul: Beta Yayınları.

Karakehya, H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *Türkiye Barolar Birliği Dergisi 22*(81), 1-24.

Keser Berber, L. (2004). *Adli Bilişim (Computer Forensic).* Ankara: Yetkin Yayınları.

Keser, H. (1991). Bilgisayarın Evrimi. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi, 24*(2), 411-422.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları.* Ankara: Adalet Yayınevi.

Koca, M., ve Üzülmez, İ. (2018). *Türk Ceza Hukuku Özel Hükümler.* Ankara: Adalet Yayınevi.

Köseoğlu, K. *E-Posta Adresini Spammer'lardan Saklayın*. https://keremkoseoglu.wordpress.com/2005/04/30/e-posta-adresini-spammerlardan-saklayin/.(Erişim Tarihi: 13.08.2022).

Kurt, L. (2005). *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması.* Ankara: Seçkin Yayıncılık.

Küresel Bilgi Toplumuna İlişkin Okinawa Sözleşmesi. https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html. (Erişim Tarihi: 11.03.2022).

Legalbank.https://legalbank.net/arama/mahkeme-kararlari.

Legalbank.https://legalbank.net/belge/turk-ceza-kanunu-gerekceler/2677276/TCK.

(Erişim Tarihi: 25.12.2021).

Mahmutoğlu, F. S. (2011). Karşılaştırmalı Hukuk Bakımından İnternet Süjelerinin Ceza Sorumluluğu. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 59*(1-2), 39-49.

Mahmutoğlu, F. S. (2013). Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 71*(1), 855-889.

Memiş, T. (2001). Hukuki Açıdan Kitlelere E-Posta Gönderilmesi . *Erzincan Hukuk Fakültesi Dergisi, 5*(1-4), 431-444.

Merkezi İşlem Birimi. https://tr.wikipedia.org/wiki/Merkez%C3%AE_i%C5%9Flem_birimi. (Erişim Tarihi: 30.08.2022).

Mevzuat Bilgi Sistemi. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf. (Erişim Tarihi: 02.05.2022).

Mevzuat Bilgi Sistemi. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf. (Erişim Tarihi: 19.04.2022).

Mevzuat Bilgi Sistemi. https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5411.pdf. (Erişim Tarihi: 16.06.2022).

OECD. https://tr.wikipedia.org/wiki/OECD. (Erişim Tarihi: 03.02.2022).

OECD Bilgi Sistemleri Güvenliği Yönergeleri, 1992. https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems 1992.htm . (Erişim Tarihi: 24.02.2022).

OECD Rehberi. https://www.oecd.org/sti/ieconomy/32493366.PDF. (Erişim Tarihi: 24.02.2022).

Oğuz, T. (2006). Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar). *Planlama Uzmanlığı Tezi, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı*. Ankara.

Önok, M.R. (2013). Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, 19*(2), 1229-1270.

Özbek, V. Ö., Kanbur, M. N., Doğan, K., Bacaksız, P., ve Tepe, İ. (2011). *Türk Ceza Hukuku Özel Hükümler.* Ankara: Seçkin Yayıncılık.

Özel, C. (2001). Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı. *İstanbul Barosu Dergisi, 75*(7-8-9), 861.

Özsoy, N. (2019). Yargıtay Kararları Işığında Doğrudan Bilişim Suçları. *Yaşar Hukuk Dergisi, 1*(2), 295-352.

Parlar, A., ve Öztürk, M. (2020). *Doğrudan ve Dolaylı Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar.* İstanbul: Aristo Yayınevi.

RAM. https://tr.wikipedia.org/wiki/RAM. (Erişim Tarihi: 30.09.2022).

Sanal Ortamda İşlenen Suçlar Sözleşmesi. https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf. (Erişim Tarihi: 16.05.2022).

Sarıusta, K. (2018). *Kişisel Verilerin Ceza Hukuku Yoluyla Korunması*. Yayımlanmamış Yüksek Lisans Tezi, Gaziantep Üniversitesi. Gaziantep.

Sınar, H. (2001). *İnternet ve Ceza Hukuku* (1. b.). İstanbul: Beta Yayıncılık.

Spam Postalar. https://www.pau.edu.tr/bidb/tr/sayfa/spam-postalar. (Erişim Tarihi: 13.08.2022).

Şamlı, R. *Türk ve Dünya Hukukunda Bilişim Suçları* . https://ab.org.tr/ab10/kitap/samli_AB10.pdf. (Erişim Tarihi: 14.04.2022).

Tanılır, M. N. (2022). *İnternet Suçları ve Bireysel Mahremiyet.* Ankara: Liberte Yayınları.

Taşdemir, K. (2009). *Bilişim Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları.* Ankara: Ütopyagrafik.

Teknoloji Geliştirme Bölgeleri Kanunu. https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4691.pdf. (Erişim Tarihi: 28.08.2022).

Tezcan, D., Erdem, M. R., ve Önok, R. M. (2010). *Teorik ve Pratik Ceza Özel Hukuku.* Ankara: Seçkin Yayınları.

Türk Dil Kurumu Sözlükleri. https://sozluk.gov.tr/. (Erişim Tarihi: 18.11.2021).

Yaşar, O., Gökcan, H. T., ve Artuç, M. (2010). *Yorumlu-Uygulamalı Türk Ceza Kanunu.* Ankara: Adalet Yayınevi.

Yaycı, E. (2007). *Bilişim Suçları*. Yayımlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi. Ankara.

Yazıcıoğlu, R. Y. (2004). Bilişim Suçları Konusunda 2001 Türk Ceza Kanunun Değerlendirilmesi. *Hukuk ve Adalet Eleştirel Hukuk Dergisi 1*(1), 177.

Yazıcıoğlu, Y. (1997). *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları ile.* İstanbul: Alfa Yayınları.

Yazılım.https://tr.wikipedia.org/wiki/Yaz%C4%B1l%C4%B1m. (Erişim Tarihi: 28.04.2022).

Yılmaz, S. (2011). 5237 Sayılı TCK'nın 244. maddesinde Düzenlenen Bilişim Alanındaki Suçlar. *Türkiye Barolar Birliği Dergisi 23*(92), 62-100.

Yücel, M. (1992). Bilişim Suçları. *Ankara Barosu Dergisi*(4), 509.