T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANABİLİM DALI

YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMİNE GİRME SUÇU

BÜŞRA ÖZÇELİK

2501160482

TEZ DANIŞMANI
PROF. DR. ADEM SÖZÜER

İstanbul-2019

T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS
TEZ ONAYI

ÖĞRENCİNİN;

Adı ve Soyadı	:	BÜŞRA ÖZÇELİK	**Numarası**	:	2501160482
Anabilim Dalı / Anasanat Dalı / Programı	:	KAMU HUKUKU	**Danışmanı**	:	PROF.DR. ADEM SÖZÜER
Tez Savunma Tarihi	:	01.07.2019	**Saati**	:	14.00
Tez Başlığı	:	BİLİŞİM SİSTEMİNE GİRME SUÇU			

TEZ SAVUNMA SINAVI, İÜ Lisansüstü Eğitim-Öğretim Yönetmeliği'nin **36. Maddesi** uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜNE** OYBİRLİĞİ / OYÇOKLUĞUYLA karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1-PROF. DR. ADEM SÖZÜER		Kabul
2-DOÇ. DR. ABDURRAHMAN SAVAŞ		Kabul
3-DR. ÖĞR. ÜYESİ SERDAR TALAS		Kabul
4-DR. ÖĞR. ÜYESİ ZAFER İÇER		Kabul
5-DR. ÖĞR. ÜYESİ MUHAMMED DEMİREL		Kabul

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1-PROF. DR. CEMİL KAYA		
2- DR. ÖĞR. ÜYESİ KERİM ÇAKIR		

ÖZ

BİLİŞİM SİSTEMİNE GİRME SUÇU

BÜŞRA ÖZÇELİK

Tezimizin konusunu ilk kez 5237 sayılı TCK'nın 243'üncü maddesinde düzenlenen bilişim sistemine girme suçu oluşturmaktadır.

İlk bölümde öncelikle 5237 sayılı TCK'nın 243'üncü madde yer alan terimler açıklanmış ve bilişim sistemine girme suçunun tarihsel gelişimine yer verilmiştir. Ardından bilişim sistemine girme suçunun bazı ülke mevzuatlarındaki ve Avrupa Konseyi Siber Suçlar Sözleşmesi'ndeki durumu ile bu suçla korunan hukuki değer incelenmiştir. İkinci bölümde ise bilişim sistemine girme suçunun unsurlarına yer verilmiştir. Üçüncü bölümde ise bilişim sistemine girme suçunun nitelikli hali ve neticesi sebebiyle ağırlaşmış hali açıklanmıştır. Ardından kusurluluk ve özel görünüş biçimlerine bakımından değerlendirmeler yapılmış, son olarak muhakeme kuralları ile zamanaşımı ve yaptırım konuları incelenmiştir.

20.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30'uncu maddesi ile 5237 sayılı TCK'nın 243'üncü maddesinin 4'üncü fıkrasına eklenen veri nakillerinin hukuka aykırı olarak izlenmesi suçu bağımsız bir suç tipi olduğu için çalışma kapsamında ayrıca incelenmemiştir.

Anahtar kelimeler: Bilişim sistemi, bilişim suçları, siber suçlar, bilişim sistemine girme suçu, yetkisiz erişim, TCK m. 243.

ABSTRACT

CRIME OF UNAUTHORIZED ACCESS

BÜŞRA ÖZÇELİK

The subject of the thesis is the crime of unauthorized access, which is firstly set out in Article 243 of Turkish Penal Code Law No. 5237.

In the first part, the terms used in the Article 243 of TPC Law No. 5237 and the historical development of the crime are explained. Then, the status of the crime of unauthorized access in some country legislation and the Council of Europe Convention on Cybercrime and the legal value protected by the crime are examined. In the second part, elements of the crime of unauthorized access are analyzed. Finally, in the third part, the crime of unauthorized access is evaluated in terms of reasons that affect crime, culpability, special appearance forms of the crime. Also proceedings rules, statute of limitations and sanctions are explained.

The crime of unlawful monitoring of data transfers provided in the sub-article 243/4 of TPC, which is introduced with the Article 30 of the Law on the Protection of Personal Data Law No. 6698 dated 20.03.2016, is lifted out of the context of the study because of the fact that this crime is an independent crime type.

Key words: Information system, cybercrime, computer crime, crime of access to information system, unauthorized access, article 243 of TPC.

ÖNSÖZ

Teknolojik gelişmelerle gün geçtikçe önem kazanan ve aynı zamanda sınırlarının çizilmesi de zorlaşan bilişim suçları gerek ülkemizde gerekse diğer ülkelerde önemli bir araştırma konusu olmuştur. Son yıllarda kişilerin teknolojiye olan merakı ile bilişim sistemine girme veya bilişim sisteminde kalma fiilleri herkes tarafından kolayca işlenebilir hale gelmiştir. Bilişim sistemine girme suçu başta bilişim sisteminin güvenliği ve güvenilirliği olmak üzere kişisel veriler, kişilerin özel hayatı, ticari hayat, ulusal ve uluslararası güvenlik gibi pek çok hususu tehdit edebilecek nitelikte olan ve bilişim suçlarının da çekirdeğini oluşturan temel bir bilişim suçudur. Bu sebeple 5237 sayılı TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun detaylı olarak incelenmesi ihtiyacı doğmuştur.

Yüksek lisans tez konumun belirlenmesinden bugüne kadar değerli fikirleriyle tez çalışmama yön kazandıran, tez hazırlama sürecimin tamamında çok büyük emeği olan ve akademik hayatımın başından itibaren hiçbir zaman ilgisini ve desteğini esirgemeyen saygıdeğer Hocam ve tez danışmanım Prof. Dr. Adem SÖZÜER'e bu vesileyle teşekkürlerimi sunarım.

BİRİNCİ BÖLÜM

TERİMLER, TARİHSEL GELİŞİM, BAZI ÜLKE MEVZUATLARINDA VE AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ KAPSAMINDA BİLİŞİM SİSTEMİNE GİRME SUÇU, KORUNAN HUKUKİ DEĞER

ÜÇÜNCÜ BÖLÜM

SUÇUN NİTELİKLİ HALLERİ, FİİL SEBEBİYLE BİLİŞİM SİSTEMİNDE YER ALAN VERİLERİN YOK OLMASI VEYA DEĞİŞMESİ, KUSURLULUK, SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ, MUHAKEME KURALLARI, ZAMANAŞIMI VE YAPTIRIM

KISALTMALAR LİSTESİ

A.e.	: Aynı eser
a.g.e.	: Adı geçen eser
a.g.m.	: Adı geçen makale
AİHM	: Avrupa İnsan Hakları Mahkemesi
ATM	: Automated Teller Machine (Bankamatik)
AÜHFD	: Ankara Üniversitesi Hukuk Fakültesi Dergisi
AÜSBFD	: Ankara Üniversitesi Sosyal Bilimler Fakültesi Dergisi
AYM	: Anayasa Mahkemesi
b.a.	: Bütüne atıf
Bkz	: Bakınız
C.	: Cilt
CD	: Ceza Dairesi
CFAA	: Computer Fraud and Abuse Act
CMK	: 5271 sayılı Ceza Muhakemesi Kanunu
dn.	: dipnot
E.	: Esas
Edit.	: Editör
IAPL	: International Review of Penal Law
IoT	: Internet of Things
IP	: İnternet Protokolü
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
m.	: Madde

MHB : Milletlerarası Hukuk ve Milletlerarası Özel Hukuk Bülteni

No : Numara

s. : Sayfa

S. : Sayı

T. : Tarih

t.y. : Tarih yok

TAAD : Türkiye Adalet Akademisi Dergisi

TBB Dergisi : Türkiye Barolar Birliği Dergisi

TBMM : Türkiye Büyük Millet Meclisi

TCK : 5237 sayılı Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TPC : Turkish Penal Code

USB : Universal Serial Bus (Evrensel Seri Veriyolu)

V. : Volume

v.d. : Ve diğerleri

v.s. : Ve saire

vd. : Ve devamı

WAP : Wireless Application Protocol (Kablosuz Uygulama Protokolü)

Y. : Yıl

YCGK : Yargıtay Ceza Genel Kurulu

YÜHFD : Yeditepe Üniversitesi Hukuk Fakültesi Dergisi

GİRİŞ

Her geçen gün hayatımıza bilişim sistemi olarak kabul edilebilecek yeni teknolojik cihazlar, program ve yazılımlar girmekte ve bunların pek çoğu günlük hayatın önemli unsurları haline gelmektedir. Bilişim sistemlerine duyulan güven ve sistemlerin güvenilirliği gereği kişiler özel hayatlarından ticari hayatlarına kadar pek çok faaliyetini bu sistemler üzerinden yürütmektedir. Daha da önemlisi devletler de bilişim sistemlerinde devlet sırlarından vatandaşların verilerine kadar pek çok veriyi bilişim sistemlerinde saklamaktadır. Teknolojinin getirdiği hız ve imkânlar hem gerçek kişiler hem de tüzel kişiler açısından vazgeçilmez konuma gelmiştir. Ancak teknolojinin getirdiği kolaylıklar diğer yandan birçok tehlikeyi de beraberinde getirmektedir. Dolayısıyla bilişim sistemlerinde işlenen veya bilişim sistemleri aracılığıyla işlenen bu fiillerin ceza hukukunun kapsamı içine alınması hem ulusal hem uluslararası alanda çeşitli düzenlemelerle ve doktrinde yer alan tartışmalarla kendi gündemini oluşturmuş.

Bilişim sistemine girme suçu birçok bilişim suçu ve bilişim aracılığıyla işlenen suç tipi bakımından çekirdek bir suç konumundadır. Nitekim bu suç bazı ülkelerin mevzuatlarında da temel bir suç tipi olarak düzenlenmiş ve diğer bilişim suçları bu suç tipinin kapsamında incelenmiştir. Tezin konusunu oluşturan bilişim sistemine girme suçuna ise mevzuatımızda TCK'nın 243'üncü maddesinde yer verilmiştir.

Çalışmanın ilk bölümünde öncelikle bilişim sistemine girme suçu açısından önem arz eden, suç tipinde yer alan terim ve ifadeler açıklanacaktır. Bu sayede suçta ve cezada kanunilik ilkesi gereğince suçun çerçevesinin çizilmesi amaçlanmaktadır. Akabinde mülga 765 sayılı TCK'daki duruma, 5237 sayılı TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun 2016 yılından önceki hali üstüne yapılan tartışmalara ve mevcut haline yer verilecektir. Ardından bazı ülke mevzuatlarındaki ve Avrupa Konseyi Siber Suçlar Sözleşmesinde yer alan bilişim sistemine girme suçunu karşılayan yetkisiz erişim düzenlemeleri incelenecek, ardından bu suçla korunan hukuki değere değinilecektir.

Çalışmanın ikinci bölümünde ise bilişim sistemine girme suçunun unsurları suç sistematiğine uygun olarak incelenecektir. İkinci bölümde ilk olarak suçun kanuni tanımı, suçla korunan hukuki değer, suçun maddi unsurları, manevi unsur, hukuka aykırılık unsuru ayrıntılı olarak incelenecektir. Bu kapsamda doktrinde yer alan tartışmalar ortaya koyulacak ve çeşitli Yargıtay kararlarına yer verilecektir.

Üçüncü bölümde ise ilk olarak suçun nitelikli halleri ile neticesi sebebiyle ağırlaşmış haline değinilecek, ardından kusurluluğa ilişkin bazı hususlar ve özel görünüş biçimleri ayrıntılı şekilde ele alınacaktır. Son olarak bilişim sistemine girme suçu bakımından muhakeme koşulları hususundaki değerlendirmelere ve tartışmalara yer verilecek, zamanaşımı ve yaptırım konusundaki hususlar açıklanacaktır.

BİRİNCİ BÖLÜM

TERİMLER, TARİHSEL GELİŞİM, BAZI ÜLKE MEVZUATLARINDA VE AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ KAPSAMINDA BİLİŞİM SİSTEMİNE GİRME SUÇU, KORUNAN HUKUKİ DEĞER

I. GENEL OLARAK BİLİŞİM, BİLİŞİM SİSTEMİ, BİLİŞİM SUÇLARI, VERİ

Bilişim hukukuna ilişkin terimlerin tanımlanması, özellikle ceza hukuku açısından önem arz eden bir husustur. 1982 Anayasası'nın 38'inci maddesinde yer alan "*kanunsuz suç ve ceza olmaz ilkesi*" gereğince bir kişinin işlediği suçtan dolayı cezalandırılabilmesi için fiili işlendiği sırada o fiilin açıkça suç olarak düzenlenmiş olması gerekmektedir. Kanunsuz suç ve ceza olmaz ilkesinin sonuçlarından birisi olan belirlilik ilkesi[1] gereğince, kanun koyucu suç olarak düzenleyeceği davranışı başka bir anlama gelmeyecek şekilde ve açık olarak düzenlemelidir[2].

Bilişim suçu olarak ceza mevzuatına giren suç tiplerinde birçok terime yer verilmiştir. Her ne kadar suç tanımında yer alan terim ve ifadelerin sınırlarının çizilmesi kanunilik ilkesi açısından zaruri olsa da[3] bilişim hukuku ile ilgili terimlerin tanımlanması gelişen ve değişen teknoloji dikkate alındığında zordur. Terim ve

[1] Abdullah Batuhan Baytaz, **Kanunilik İlkesi Bağlamında Ceza ve Ceza Muhakemesi Hukukunda Yorum**, İstanbul Arşivi, On İki Levha Yayıncılık, İstanbul, 2018, s. 72.
[2] Mahmut Koca, İlhan Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, 5. Baskı, Ankara, Adalet Yayınevi, 2018, s.60.
[3] Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Tamamen Güncellenmiş 7. Baskı, Ankara, Seçkin Yayıncılık, 2018, s.58.

ifadelere kanuni düzenlemeyle getirilecek tanımlar, suç sayılması gereken bazı hareketlerin kapsam dışı kalmasına sebebiyet verebilecektir.

Ancak en azından suç tipinde yer verilen terim ve ifadelerin genel hatlarıyla tanımlanması ve bu sayede belli bir terimlerden ne anlaşılması gerektiğine ışık tutarak genel bir sınırlamanın sağlanması yapılan çalışmanın bilimsel bir çalışma olarak değerlendirilebilmesi için de zaruridir[4]. Bu sebeple bu bölümde bilişim sistemine girme suçunda yer verilen terim ve ifadeler açıklanmaya çalışılacaktır.

A. Bilişim, İşlemleri Otomatik İşleme Tabi Tutan Sistemler, Bilişim Sistemi

Bilişim, TDK tarafından "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*" şeklinde tanımlanmıştır[5].

TDK'nın da tanımında yer verdiği "*enformatik*" ile aynı anlama gelen ve kökü Fransızcadan gelen "*informatique*" terimi 1962 yılında Philippe Dreydus tarafından, bilgi anlamına gelen "*information*" ve otomatik anlamına gelen "*automatique*" kelimelerinin kombinasyonundan oluşturulmuş, bilgisayar bilimi olarak tanımlanmıştır. "*Informatique*" terimi daha sonra Avrupa'nın bilgisayar uzmanları tarafından hızla benimsenmiştir[6]. Günümüzde ise, enformasyon yani bilişim terimi bilgisayar uzmanları tarafından yapay zekâ, bilişsel bilim, bilgisayar bilimi, bilgi

---

[4] Georges Ifrah, **Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi XI**, (Çeviri: Kurtuluş Dinçer), Ankara, Tübitak Popüler Bilim Kitapları, 2002, s.18; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 58.

[5] TDK, http://www.tdk.gov.tr, Erişim Tarihi: 27.10.2017.

[6] Bkz. CJB Le Roux, "Social and Community informatics Past, Present, & Future: An Historic Overview Keynote Address", **10th Annual DIS Conference: 10-11th September 2009**, (Çevrimiçi), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.551.1067&rep=rep1&type=pdf, Erişim Tarihi: 27.10.2017, s.3.
Gorn, 1983 yılında yayınladığı makalesinde Almancada "Informatik", Fransızca'da "informatique" olarak geçen "Informatics" ifadesini bilgisayar ve bilişim bilimi olarak tanımlamıştır. Bkz. Saul Gorn, "Informatics (Computer and Information Science): Its Ideology, Methodology, and Sociology", **The Studies of Information: Interdisciplinary Messages**, Edit. Machlup, F. and Mansfield, U., Eds., New York, Wiley, 1983, s. 121.

bilimi (bilginin işlenmesi, yönetimi ve bilgi edinilmesi), sosyal bilim ve bilgi teknolojisini de kapsayacak şekilde tanımlanmıştır[7].

06.06.1991 tarih ve 3756 sayılı 765 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun'un 20'nci maddesiyle 765 sayılı TCK'ya 11'inci Bab olarak eklenen ve bu Kanun'dan sonra yürürlüğe giren 5237 sayılı TCK'nın 10'uncu bölümünün de başlığı olan "*Bilişim Alanında Suçlar*" ifadesinde yer alan "*bilişim alanı*" ise doktrinde geniş anlamda ele alınmış ve hızla gelişen teknolojinin sonucu olabilecek yeni sistemleri de kapsayan bir bütünü ifade edecek şekilde tanımlanmıştır[8].

Bilişim ve bilişim sistemi terimleri yalnızca bilgisayarla sınırlı tutulamayacağından ve hızla gelişen teknolojinin vardığı ve varabileceği boyutları tahmin etmek zor olduğundan bilişim kavramının net bir tanımını yapmak zordur. Doktrinde yapılan tanımların[9] ortak noktaları bilişim sistemlerinin otomatik olarak

---

[7] Roux, **a.g.e.**, s.4.

[8] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 68.

[9] Doktrinde bilişim ve bilişim sisteminin tanımı değişik şekillerde yapılmıştır.
Akbulut bilişimi "... insanların teknik, ekonomik ve toplumsal alanlardaki iletişimde kullandığı ve bilimin temeli olan bilginin elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ses, görüntü ve veri taşıyan iletişim hatları aracılığıyla aktarılması bilimi...'' olarak tanımlamıştır. Berrin Bozdoğan Akbulut, "Bilişim Suçları", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, C.8, S. 1-2, 2000, s.546; Berrin Akbulut, **Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2017, s.13.
Aydın'a göre "bilişim, 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, şebekeler, işlevler, süreçler ve etkinliklerdir". Emin D. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınevi, 1992, s. 3; Emin D. Aydın, "Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992, s.109.
Ceyhun/Çağlayan bilişim kavramını "… insanoğlunun teknik, ekonomik ve toplumsal alandaki iletişiminde kullandığı ve biliminin de dayanağı olan bilginin, özellikle elektronik makineler aracılığı ile, düzenli ve ussal biçimde işlenmesi bilimi" olarak tanımlamıştır. Yurdakul Ceyhun/ Ufuk Çağlayan, **Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta**, Ankara, Türkiye İş Bankası Kültür Yayınları, 1997, s.1.
Dülger'e göre ise, "Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşüncel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir". Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 70.
Ifrah bilişimi "Bilgisayarların tasarım ve programlama bilimi (yani 'klasik bilişim' denmesi uygun olan şey) bilgi kurumsal profili öteki bilimlere göre çok bireyselleşmiş olan ve yapay zekâ yahut biçimselleştirilebilir olan ya da olmayan her türden düşünsel sürecin yapay olarak yeniden üretilmesi

verileri işleyebilir, aktarabilir ve depolayabilir özellikte olması sebebiyle bilişim sisteminin salt bilgisayardan oluşmadığı ve daha geniş bir kavram olduğu üzerinedir.

Genel olarak bilişim; kişilerin zihninde oluşturduğu işlemlerin programlar aracılığıyla üretilmesine imkân veren ve kullanıcıların erişimine açık olarak verilerin düzenli biçimde otomatik şekilde işlenmesi, saklanması ve aktarılmasını sağlayan bir bilim dalı olarak ifade edilebilir.

Mülga 765 sayılı TCK'nın 525a maddesinde "*bilgileri otomatik işleme tabi tutan sistem*" terimi kullanılmaktaydı. Hem 765 sayılı TCK'da hem de bilişim suçlarının eklendiği 3756 sayılı 765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun'un gerekçesinde "*bilgileri otomatik işleme tabi tutan sistem*" terimi için bir açıklama belirtilmemişti. Ancak 3756 sayılı 765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun'un madde gerekçelerinin 2'nci maddesinde "… *bilgileri otomatik olarak işleme tutmuş sisteme (bilgisayarlara)*" ifadesine yer verilmişti.

---

bilimi diye adlandırdığımız çok daha geniş bir alanın bilim dalı" şeklinde ifade etmiştir. Ifrah, **a.g.e.**, s.18.

Kardaş'a göre ise bilişim "İnsan bilgisinin, teknik, ekonomik ve sosyal alanlardaki iletişiminin otomatik makinelerde akılcı olarak işlenmesini konu alan bilim"dir. Ümit Kardaş, "Bilişim Dünyası ve Hukuk", **Karizma Dergisi**, S.13, 01.03.2003, s. 8.

Ketizmen bilişimi "enformasyonun otomatik makineler aracılığıyla ve otomatik olarak işlenmesini sağlayan sistemler" olarak tanımlamaktadır. Muammer Ketizmen, **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008, s.11.

Yazıcıoğlu'ya göre ""bilişim" (enformatik) ise bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir". R. Yılmaz Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, İstanbul, Alfa Yayınevi, 1997, s.131.

Yenidünya/Değirmenci'ye göre "bilişim, teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verilerin saklanması, saklanan verilerin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bir bilim dalıdır". Caner Yenidünya, Olgun Değirmenci: **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003, s.27. Değirmenci, yayınlanmamış yüksek lisans tezinde de aynı yönde bir tanım yapmıştır. Bkz. Olgun Değirmenci, "Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi**, İstanbul, 2002, s.7.

Doktrinde ise bilgileri otomatik sisteme tabi tutan sistem teriminin yalnızca bilgisayarı kastetmediği bununla birlikte verilerin işlenmesi, saklanması, aktarılması sürecini oluşturan ve bilişim sisteminin işleyişine hizmet eden araçları da kapsadığı savunulmaktaydı[10]. Böylece gelişen teknoloji sayesinde bulunan yeni bilişim araçlarının da düzenleme kapsamında yer alması ve suç teşkil eden fiilin ceza hukuku açısından yaptırımsız kalmasının engellenmesi amaçlanmaktaydı. Aksi bir yorum bilişime hizmet eden ve veri işleme, saklama, aktarma işlemlerini yapan bilişim sistemlerini kapsam dışı bırakırdı[11].

Nitekim Yargıtay da 765 sayılı TCK döneminde de bilgileri otomatik işleme tabi tutan sistemi salt bilgisayar olarak ele almamıştır. YCGK'nın 10.04.2001 tarih, 2001/6-30 esas ve 2001/57 karar numaralı kararına göre, "*Öyle ki, ATM'ler aracılığıyla onun bağlı bulunduğu sisteme ulaşılarak döviz, fon, hisse senedi, devlet tahvili, bono, kıymetli maden alım satımı, repo, havale ve virman işlemleri mevduat ve yatırım hesaplarının sorgulanması ve hesaplar arası aktarım ile kredi kullanımı v.b bankacılık işlemleri yapılabilmektedir. Sistemin işleyiş biçimine gelince, teknolojideki gelişmelere paralel olarak karta ihtiyaç göstermeyen, örneğin banka mudisi, müşterisi veya kredi sözleşmesinin tarafı olan kişinin ekrana dokundurduğu parmağının izini yahut onu diğer insanlardan ayıran ses ve göz özelliklerini tespit ederek sistemin merkezine aktaran, sistemin tanıyarak algılaması sonrasında yine sistemce verilen uygun komutlar ve izin doğrultusunda sisteme giriş ve işlem olanağı sağlayan ATM tasarımlarının geliştirilmeye çalışıldığı bilinmektedir. Ancak günümüzde yaygın olup ülkemizde de kullanılan tasarım modelinde ATM'lerin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan biri kart diğeri kullanıcı şifresidir. Bu iki araca sahip olmadan, bir bilgi işlem biriminin parçası olan ve ana sisteme bağlı bulunan ATM*

[10] Bkz. Erol Çetin, İsmail Malkoç, **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara, Adalet Yayınevi, 1995, s.544; Ayhan Önder, **Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar**, İstanbul, Filiz Kitapevi, 1994, s.506; Yenidünya/Değirmenci, **a.g.e.**, s.44; Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, s.224; Doğan Soyaslan, **Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2016, s.634; Kubilay Taşdemir/Ramazan Özkepir, **Uygulamada-Öğretide Belgede Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar Açıklamalı-İçtihatlı**, Ankara, Adil Kitapevi, 1999, s.1107.

[11] Yüksel Ersoy, "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **AÜSBFD**, C:49, S.3, 1994, s. 165.

makinelerini kullanma olanağı yoktur. Belirtilen karta sahip olup, önceden sisteme tanıtılmış olan şifreyi de bilen kişi, kartı makineye takıp şifreyi kodlayarak işlem sürecini başlatabilir. Ancak, kartı elinde bulunduran kişinin makine vasıtasıyla sisteme verdiği komutların yerine getirilebilmesi için ana kumanda merkezinin de bu komutları onaylaması gerekmektedir. Örneğin nakit para çekilmek istendiğinde hesapta para yoksa veya günlük çekme limiti dolmuş yada herhangi bir nedenle hesap ana merkez tarafından kullanıma kapatılmışsa, komut onaylanmayacağından işlem yapılamaz. Bu olgu da gösteriyor ki ATM makineleri bilgileri otomatik işleme tabi tutmuş bir sistemin ünitesidir. Yine, sistemi harekete geçirmede kullanılan kartların geleneksel hırsızlık suçlan bakımından "sair alet" olarak kabul edilmesi de olanaklı değildir"[12].

Yine YCGK 19.6.2007 tarih, 2007/6-136 esas ve 2007/150 karar numaralı kararında bilgileri otomatik işleme tabi tutan sistemler yönünden bir değerlendirme yaparak ATM'leri bilişim sistemi sayarken[13], ankesörlü telefonların bu kapsamda değerlendirilemeyeceğini belirtmiştir.

Mezkur kararda bu husus; "*her ne kadar çoğunlukla "bilişim" ile "bilgisayar" terimleri aynı anlamda kullanılmaktaysa da gerçekte bunlar aynı şey demek değildir.*

Zira, "bilişim" sözcüğü "bilgisayar" kelimesine oranla daha geniş kapsamlıdır. Bilgisayar, (kompütür, elektronik beyin) aritmetik ve mantık işlemi dizileriyle oluşturulmuş programlara göre verileri (bilgileri) otomatik işleme tabi tutan sistemlere verilen ortak isim iken, bilişim (enformatik) ise, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesine konu olan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir.

[12] Kazancı İçtihat Bankası, (Çevrimiçi), www.kazanci.com, Erişim Tarihi 31.10.2017. Aynı yönde; YCGK E. 2000/6-62 K. 2000/72 T. 11.4.2000.

[13] Doktrinde POS cihazı, ATM gibi bilişim sistemini tamamlayıcı cihazların bilişim sistemi olduğu kabul edilmektedir. Hatice Akıncı, A. Emre Alıç, Cüneyd Er: "Türk Ceza Kanunu ve Bilişim Suçları", **İnternet ve Hukuk**, (Derleyen: Yeşim M. Atamer), İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2004, s.173-174. Karar için bkz. CGK., E. 2006/6-136 K. 2007/150 T. 19.6.2007, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:5.4.2019.

Bir faaliyetin bilişim faaliyeti olup olmadığını tarif edebilmek için, o faaliyetin bilgisayar sistemine dahil olup olmadığına bakmak gerekir. Daha açık bir ifadeyle şu sorunun cevabı verilmek gerekir. Faaliyet bilgisayar sistemiyle mi temellenmektedir; yoksa bilgisayar o faaliyetin gerçekleşmesine yardımcı bir unsur olarak mı kullanılmaktadır? Yani bilgisayar destekli midir? Bankaların ATM uygulaması bilgisayar destekli olduğu için bilişim faaliyetidir. Zira bu sistem herhangi bir nedenle çöktüğünde bu faaliyet de asla gerçekleşmez. Bunun karşıtı bir örnek verilecek olursa, uçak firmalarının bilet satışlarında bilgisayar sistemlerinden yararlanmaları yani faaliyetin bilgisayar destekli olması bir bilişim faaliyeti değildir. Çünkü bu sistemler bu firmaların faaliyetini kolaylaştırmakla hızlandırmakla ve daha verimli kılmakla birlikte faaliyetin tarif edici unsuru değildir.

... Ancak, kartı elinde bulunduran kişinin makine vasıtasıyla sisteme verdiği komutların yerine getirilebilmesi için ana kumanda merkezinin de bu komutları onaylaması gerekir. Örneğin nakit para çekilmek istendiğinde hesapta para yoksa veya günlük çekme limiti dolmuş yada herhangi bir nedenle hesap ana merkez tarafından kullanıma kapatılmışsa komut onaylanmayacağından işlem yapılamaz. Bu olgu da gösteriyor ki, ATM makinaları bilgileri otomatik işleme tabi tutmuş bir sistemin ünitesidir.", denilmektedir.

Oysa telefon cihazının kontür yüklü sahte kartla görüşmeye açılması sağlandıktan sonra telefon santraline komut verilmesi mümkün olmadığı gibi esasen verilen bir komut olmadığı ve bir sisteme bağlanılmadığından bilişim sistemlerinin temel özelliği olan komut onaylaması da söz konusu değildir. Diğer taraftan bir bilişim sistemine bağlanılmadığından ATM kartlarında olduğu gibi şifreye de ihtiyaç yoktur çünkü bir bilişim sisteminin ünitesi değildir"[14] şeklinde ifade edilmiştir.

TCK'nın 243'üncü maddesinin gerekçesinde ise "*tasarının bu ve izleyen maddelerinde "bilgileri otomatik olarak işleme tâbi tutmuş sistem" ibaresi yerine aynı anlamı taşımak üzere "bilişim sistemi" sözcüklerinin kullanılması uygun sayılmıştır*"

[14] Kazancı İçtihat Bankası, (Çevrimiçi), http://www.kazanci.com/kho2/ibb/giris.htm, Erişim Tarihi 31.10.2017.

şeklinde açıklama getirilmiştir. Böylece TCK'da bilgileri otomatik işleme tabi tutan sistem yerine daha geniş bir kavram olan "*bilişim sistemi*"[15] kavramı kullanılmıştır. Bilişim sistemi verileri toplama, depolama ve işleme ile bilgilerin ve dijital ürünlerin parçalarını oluşturduğu bir bütün olarak tanımlanmaktadır[16]. Başka bir tanıma göre ise bilişim sistemi "*bilgisayar, çevre birimleri (bir bilgisayarın çalışması için zorunlu olmayan ancak kullanımını kolaylaştıran hoparlör, CD ROM, mouse, klavye, kulaklık, yazıcı vb), iletişim alt yapısı (elektronik haberleşme, internet, intranet gibi) ve programlardan oluşan işleme saklama ve iletmeye yönelik sistemi ifade eder*"[17]. Bilişim sistemi terimiyle 765 sayılı TCK'da yer alan "*bilgileri otomatik işleme tabi tutan sistem*" teriminden daha geniş ve kapsayıcı bir ifadeye yer verilerek yeni teknolojilere açık bir ifade kullanılmıştır[18].

Türkiye'nin de taraf olduğu Avrupa Konseyi Siber Suçlar Sözleşmesinin 1'inci Bölüm 1'inci maddesinin a bendinde "*bilgisayar sistemi*" ifadesine yer verilmiş ve "*bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder*" şeklinde tanımlanmıştır.

TCK'nın 243'üncü maddesinin hem taslağının gerekçesinde hem de komisyonun değişiklik gerekçesinde "*bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir*" şeklinde bir tanım yapılmıştır.

Günümüz teknolojisi de dikkate alındığında bilişim sisteminden yalnızca bilgisayarların anlaşılmaması gerektiği son derece açıktır. Özellikle yapay zekâ

---

[15]"…bilişim sistemini Türk ceza hukukunda ilk kez tanımlayan, Ceza Muhakemesinde Ses ve Görüntü Bilişim Sisteminin Kullanılması Hakkındaki Yönetmelik 20.09.2011 tarihinde Resmi Gazete 'de yayınlanmış olup, bu yönetmeliğin tanımları belirleyen 3(1)-b maddesinde "Bilişim sistemi: Bilgisayar, çevre birimleri, iletişim alt- yapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistemi" ifade eder şeklinde tanımlama yapılmıştır." ; Yavuz Erdoğan, "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.12, Özel S., 2012, s.1363, dn.1.

[16] Britannica, (Çevrimiçi), https://www.britannica.com/topic/information-system, Erişim Tarihi: 27.10.2017.

[17] Murat Volkan Dülger, Gözde Modoğlu**, Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi**, Ankara, Avrupa Birliği ve Konseyi Ortak Yayını, 2014, s.55.

[18] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.71.

üzerine yapılan son çalışmalar da göstermektedir ki teknolojinin varabileceği boyutları tahmin etmek neredeyse imkânsızdır. İnsan düşünme yapısına benzer sistemler geliştirilerek üretilen yapay zekâ sistemlerinin de kullanıldığı ve "*Nesnelerin İnterneti*"[19] (IoT)[20] olarak anılan ve hızla gelişmekte olan cihazların da (akıllı televizyon, tablet, akıllı saat, akıllı ev ve bina, akıllı şehir, akıllı endüstri, otonom araçlar[21] v.s.) bilişim sistemi kapsamında yer aldığı kabul edilmelidir. Yargı mercilerinin bilişim ve bilişim sistemi terimlerini belirlemede zorluk yaşaması halinde yargı merciinin bilişim bilim dalı üzerine uzman bilirkişilerden yardım alması sorunun çözümünde etkili bir yol olacaktır[22].

B. Bilişim Suçu ve Terim Sorunu

Bilişim suçlarıyla mücadele için yapılan ulusal ve uluslararası düzenlemeler dikkate alındığında herhangi bir tanım yapılmadığı ve ortak bir terim kullanılmadığı dikkat çekmektedir. Gerek Türk doktrininde gerekse diğer ülkelerde bu suçlar için

[19]Nesnelerin İnterneti (Internet of Things, IoT) internet için yeni bir devrimdir. Nesnelerin interneti kablosuz, kablolu bağlantılar ve benzersiz adresleme yöntemleri aracılığıyla nesnelerin ortak bir sonuca ulaşmak veya bir hizmet/uygulama sağlamak amacıyla birbirleriyle etkileşim kurması, birlikte çalışabilmesi adına oluşturduğu bir iletişim ağı konsepti ve teknolojisidir. Ovidiu Vermesan v.d., "Internet of Things Strategic Research and Innovation Agenda", **Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems,** Edit.: Ovidiu Vermesan, Peter Friess,(Çevrimiçi), http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf, Aalborg, River Publishers, 2013, Erişim Tarihi:31.10.2017, s.7-8. Nesnelerin internetine günümüz teknolojisinden verilecek bazı örnekler; Google tarafından satın alınan ve evin / ofisinin sıcaklığını dışarıdan kontrol edebilen Nest sistemi, akıllı telefon üzerinden desteklenen cihazlarla entegre edilerek kullanılan ve kahve makinası, ışıklandırma ve müzik sistemlerini otomatik olarak devreye sokan akıllı ürünler (Smart Things) olabilir.

[20] Siber tehditler bilişim suçluların akıllı ev cihazlarına saldırmak için ev ağı routerlarını ele geçirmesiyle çok daha tehlikeli boyutlara ulaşmıştır. Trend Micro'nun 2017 ilk yarı raporuna göre 2017'nin ilk altı ayında ev ağı routerları yoluyla 1,8 milyondan fazla siber saldırı gerçekleşmiştir. Bkz. http://newsroom.trendmicro.com/press-release/commercial/trend-micro-reveals-top-ten-regions-affected-iot-security-threats , Erişim Tarihi: 31.10.2017.

[21] Ayrıca bkz. Tuba Kelep Pekmez, "Otonom Araçların Kullanımından Doğan Cezaî Sorumluluk: Türk Hukuku Bakımından Genel Bir Değerlendirme", **Ceza Hukuku ve Kriminoloji Dergisi,** S. 6(2), 2018, s. 173-195.

[22] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1364-1365, dn.1.

terim birliği sağlanamamıştır. Ülkeler bilişim suçlarını düzenlerken daha çok kriminolojik sonuçlardan yola çıkmış ve suç tiplerini sayma yoluna gitmiştir[23].

Bilgisayarın ilk olarak geliştirildiği yer olan Amerika Birleşik Devletleri, aynı zamanda doktrin açısından bilişime ilişkin yeni suç tiplerinin isimlendirilmesinde de söz sahibi olmuştur[24]. Amerikan doktrininde bilişim suçlarının karşılığı olarak kullanılan terim "*computer crime"* yani bilgisayar suçları olmuştur. Son yıllarda ise çoğunlukla "*cybercrime*" yani siber suç terimi makalelerde kendisine yer bulmuş ve hatta "*computer crime*" terimiyle eş anlamlı bulunduğu için akademik çalışmalarda dönüşümlü olarak kullanılmıştır[25]. Bunların dışında "*computer related crime*"[26] (bilgisayarla bağlantılı suç), "*computer asistant crime*" (bilgisayar aracılığıyla suç), "*hi-tech crime*" (yüksek teknoloji suçu), "*techno crime*" (teknoloji suçu), "*technology-enabled crime*"[27] gibi terimler de doktrinde kendisine yer bulmuştur.

Yine İngilizce dilinin konuşulduğu İngiltere ve Avustralya doktrininde de terim birliği yoktur. Bazı yazarlar "*computer crime*"[28] ifadesini tercih ederken bazıları ise bilgisayar veya bilgisayara yönelik suçları "*cybercrime*", "*computer-related crime*", "*e-crime*" olarak isimlendirmiştir[29]. Bazı yazarlar ise bilişim suçlarını üç ayrı

---

[23] Carlo Sarzana di S. Ippolito, "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalya'daki Durum", (Çeviri: Vesile Sonay Daragenli), **Prof. Dr. Türkan Rado'ya Armağan**, İstanbul,1997, s.393.

[24] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.72.

[25] Yazarlar, "computer crime" ve "cybercrime" ifadelerinin aynı anlama geldiğini ve dönüşümlü olarak kullanılabildiğini makalelerinde dile getirmiştir. Bkz. Jessica Bregant / Robert Bregant: "Cybercrime and Computer Crime", **The Encyclopedia of Criminology and Criminal Justice,** First Edition, Edited by Jay S. Albanese, John Wiley & Sons Inc., 2014, s.1.

[26] Peter Stephenson, **Computer-Related Crime: a Handbook For Corporate Investigation**, Florida, CRC Press LLC, 2000. Yazar, bu terimlerin hepsini eserinde kullanmıştır. Başlıkta "Computer-Related Crime" ifadesine yer verirken tanım ve içerikte cybercrime ve computer crime ifadelerini kullanmıştır.

[27] Bkz. Sam McQuade, "Technology- enabled Crime, Policing and Security", **Journal of Technology Studies**, (Çevrimiçi), http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf, 2006, Erişim Tarihi: 02.11.2017, s.32-42.

[28] Bkz. UK Parliament, "Computer crime", **Postnote**, October 2006, No:271, Çevrimiçi, www.parliament.uk/parliamentary_offices/post/pubs2006.cfm, Erişim Tarihi: 30.10.2017.

[29] Amerikan hukukunda olduğu gibi İngiliz ve Avustralya Hukukunda da çalışmalarda terim birliği sağlanmaksızın "computer crime" ve "cybercrime" ifadelerine aynı anda yer verilmiştir. Bkz. Manoj Kumar, Anuj Rani, "Computer Crime IT Laws in Ireland and India", (Çevrimiçi), https://www.researchgate.net/publication/235769188, 2013, b.a.; Barbara Etter, "Computer Crime", **4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses 21-22 June 2001**, (Çevrimiçi), http://aic.gov.au/media_library/conferences/outlook4/etter.pdf, Erişim Tarihi: 02.11.2017, s.1, dn.1.

başlık altında incelemektedir. İlk kategoride bilgisayar aracılığıyla işlenen dolandırıcılık, sahtecilik gibi geleneksel suç tiplerinin yer aldığı "*computer related crimes (bilgisayarla bağlantılı suçlar)*"; ikinci kategoride fikri mülkiyet haklarının ihlalinin, pornografinin vs. bilgisayar ve ağlarının araç olarak kullanılarak içerik yönünden ihlalin söz konusu olduğu suçlar "*content related crimes (içerikle bağlantılı suçlar)*", üçüncü kategoride ise virüs, spam gibi kötücül yazılımların kullanılmasıyla bilgisayar ve iletişim sisteminin bütünlüğüne, gizliliğine ve erişilebilirliğine yönelik işlenen suçlar "*computer integrity crimes (bilgisayarın bütünlüğüne yönelik suçlar)"* bulunmaktadır[30].

Türk doktrininde de terim birliğinin sağlanamadığı görülmektedir. Akademik çalışmalarda "*bilgisayar suçu*"[31], "*sanal suç/sanal ortamda işlenen suç*"[32], "*siber suç*"[33], "*internet suçu*"[34], "*bilişim suçu*"[35], "*bilgisayar ile ilgili suç/bilgisayar ağları ile ilgili suçlar*"[36], "*bilişim alanında suç*"[37] gibi pek çok terimin kullanıldığına rastlanmaktadır.

Söz konusu terim sorununun altında bir sonraki terimin bir öncekine göre konunun özünü daha iyi ifade ettiği veya kriminolojik yönden yahut sistematik açıdan

[30] Walden, Ian: "Computer Crime", (Çevrimiçi), http://kavehh.com/my%20Document/KCL/Internet%20Law/Internet%20Material/Computer%2520Crime%2520%25286th%2520ed.%2529.pdf, Erişim Tarihi: 01.11.2017, s. 1-2.

[31] Bkz. Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, b.a., Çetin/Malkoç, **a.g.e.**, b.a.

[32] Örneğin Avrupa Konseyi bünyesinde hazırlanan "Convention on Cybercrime", "Sanal Suçlar Sözleşmesi" veya "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak Türkçe'ye çevrilmiştir.

[33] Sacit Yılmaz, **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016, b.a.

[34] Feridun Yenisey, "İnternet Suçlarının Yeni İşleniş Biçimleri", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002, s.447 vd; Sevil Yıldız, **Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi**, Ankara, Nobel Yayın Dağıtım, 2007, s..38.

[35] Doktrinde en çok kullanılan terimdir.

[36] Hasan Dursun, "Bilgisayar İle İlgili Suçlar", **Yargıtay Dergisi**, C.24, S.3, 1998, 334 vd; Yılmaz Yazıcıoğlu, "Bilgisayar Ağlar ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002, s. 451-470.

[37] 765 sayılı TCK'nın 11. Babının ve 5237 sayılı TCK'nın 10'uncu Bölümünün başlığında yer almaktadır.

daha iyi bir terim olduğu iddiası yatmaktadır[38]. Yani tercih edilen terimin önemi konuya yönelik yaklaşımı da ortaya koyacağından son derece önem arz etmektedir[39].

Doktrinde "*bilgisayar suçu*", "*bilgisayarlara karşı işlenen suç*", "*bilgisayar aracılığıyla işlenen suç*" kavramları dar kapsamlı terimler olduğu için sıkça eleştirilmiştir. Bilgisayar her ne kadar bu suç tipinin oluşmasının başlangıç noktası olan bir bilişim sistemi olsa da "*bilişim*" ifadesi bilgisayardan çok daha geniş kapsamlı bir ifadedir[40]. O kadar ki sınırlarının nereye varabileceğinin tahmin edilmesi zor olduğundan net bir tanımının yapılması da zordur. Doktrinde yer alan diğer bir eleştiri ise, suçların isimlendirilmesinin işlenen ortama göre yapılmasının doğru olmadığı düşüncesidir. Örneğin, adam öldürmenin binada gerçekleşmesi halinde bu suça "*bina suçu*" denmeyeceği gibi bilişim suçları da işlendikleri ortamlara göre isimlendirilmemelidir[41].

Yine "*internet suçu*", "*sanal suç*" ve "*siber suç*" terimleri de bilişim suçlarını karşılamak açısından dar bir kavram olarak görülmüş ve eleştirilmiştir. Nitekim bilişim suçlarının internet olmaksızın da işlenmesi mümkündür. Örneğin, manuel

[38] Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, s. 130.
[39] **A.e.**
[40] Yenidünya/Değirmenci, **a.g.e.**, s.30-31; Ersoy, **a.g.m.**, s.153.
[41] Yenidünya/Değirmenci, **a.g.e.**, s.32.

olarak ya da intranet[42], ekstranet[43] veya benzeri ağ sistemleri[44] aracılığıyla da bu suçlar işlenebilmektedir[45].

Siber suç (sanal suç) teriminin kaynağı olan "*siber uzay*"[46] ise sadece internet değil benzeri her türlü ağları da kapsayan bir kavram olduğu için doktrinde tercih edilmiştir[47]. Ancak her ne kadar siber suç terimi internet suçuna göre daha kapsayıcı bir ifade olsa da bilişim suçu terimi de siber suç kavramına göre daha geniş bir terimdir[48].

Bugün hem Türk doktrininde hem de TCK'da kabul gören ve en çok kullanılan terim "*bilişim suçu*" terimidir. Nitekim bilişim suçu terimi yukarıda anılan terimler

---

[42] İntranet (iç ağ) (internal internet), genellikle işyerlerinde ve çeşitli organizasyonlarda web sunucuları ve tarayıcıları gibi internet teknolojilerinin kullanıldığı, iletişimin sağlanması ve bilgi aktarımını sağlamak için kurulan özel bir ağdır. Diğer web sunucularından farklı olarak herkesin erişimine açık değildir. Bkz. Richard W. Boss, "Intranet and Extranet", **PLA Tech Notes**, American Library Association, (Çevrimiçi), https://alair.ala.org/bitstream/handle/11213/258/Intranets%20and%20Extranets.pdf?sequence=93&isAllowed=y, 2010, Erişim Tarihi: 02.11.2017.

[43] Ekstranet (dış ağ) (extended internet), genellikle işyerlerinde kullanılan ve seçili kullanıcıların dışardan erişimine izin veren ve bu kişiler arası iletişiminin sağlanması ve bilgi aktarımının sağlanması adına kurulan özel bir ağdır. Bu ağa ulaşım genellikle şifre, kullanıcı adı gibi güvenlik uygulamalarıyla sağlanmaktadır. Bkz. **A.e.**

[44] Ağ bağlantısı kablo, tel, radyo, infrare veya uydu yoluyla birden fazla bilgisayar arasında kurulan bağlantıdır. Yan yana iki bilgisayar arasında bir bağlantı kurularak ağ oluşturulabileceği gibi, dünya genelinde de bilgi paylaşımı amacıyla bilgisayar ağları kurulabilir. İki bilgisayardan bir kampüs büyüklüğüne kadar olan ağlar Yerel Alan Ağları (Local Area Network)(LAN) olarak geçerken, yerel alan ağlarından büyük olan ve bir şehrin bazı bölgelerini birbirine bağlayan ağlara Metropolitan Bilgisayar Ağları(Metropolitan Area Network)(MAN) adı verilmekredir. Farklı bölgelerdeki yerlerin telefon ağlarıyla birleştirilmesiyle oluşan ağlar ise Geniş Alan Ağlarını (Wide Area Network) (WAN) oluşturmaktadır. Yıldız, **a.g.e.**, s.17; 141.

[45] Yenidünya/Değirmenci, **a.g.e.**, s.31 vd.; Durmuş Tezcan, Mustafa Ruhan Erdem, R. Murat Önok: **Teorik ve Pratik Ceza Özel Hukuku**, 14. Baskı, Ankara, Seçkin Yayıncılık, 2017, s.977; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.74.

[46] "Siber uzay" kavramı ilk kez 1984 yılında William Gibson tarafından yazılan "Neuromancer" isimli romanda geçmiş ve bilişim sistemine girmeye yönelik hacker hareketleri somut terimlerle olarak tanımlanmıştır. Roland Heickerö, **The Dark Side of The Internet**, (Translated by Martin Peterson), Frankfurt, Peter Lang GmbH, 2013, s.9; Mohamed Chawki, "A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy", (Çevrimiçi), http://www.droit-tic.com/pdf/chawki4.pdf, Erişim Tarihi: 01.11.2017, s.5.

[47] Yazara göre "internet suçu" kavramını dar kapsamlıdır. Her internet suçu siber suçtur fakat her siber suç internet suçu değildir. Yılmaz, **a.g.e.**, s.5.
Siber uzay, bilgisayar destek ve etkileşimli sanal ortam olarak tanımlanmıştır. Nilgün Camgöz, "Siber Uzay, Sanal Gerçeklik ve Müze", Bilim ve Teknik Dergisi, Ocak 1998, Çevrimiçi, http://www.biyolojiegitim.yyu.edu.tr/fizuzaypdf/Siberuzay19984S.pdf, Erişim Tarihi: 13.11.2017, s.72.

[48] Yenidünya/Değirmenci, **a.g.e.**, s.33; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku(7),** s.74.

arasında en üst kavram olarak değerlendirilebilir. Bu sebeple çalışmamızda "*bilişim suçları*" terimi tercih edilmiştir.

Bilişim suçları doktrinde çeşitli gruplara ayrılarak incelenmektedir:

Bir görüşe göre bilişim suçları üç grupta incelenmektedir. İlk grupta bilgisayar suçun konusunu oluşturmaktadır. Örneğin; bilgisayarın yazılım veya donanımının çalınması ilk grupta yer alacaktır. İkinci grup ise bilgisayarın suçun süjesi olduğu ve virüs, solucan, spam, trojan gibi kötücül yazılımlar vasıtasıyla işlenen suçların oluşturduğu gruptur. Üçüncü grup ise bilgisayarın araç olarak kullanıldığı çocuk pornografisi, dolandırıcılık gibi suçların bulunduğu gruptur[49].

Başka bir görüş bilişim suçlarını üçe ayırmaktadır. Bilgisayarın fiziki yapısına klasik nitelikte (kırma, yakma vs.) zarar verme ilk sınıfı oluştururken, ikinci sınıfı bilgisayarın tek başına çalışmasına yönelik hareketler ve bilgisayarın hukuka aykırı olarak değişik şekilde çalışmasına yol açan hareketler oluşturmaktadır. Üçüncü grubu ise bilgisayar ağlarına yönelen hareketler oluşturmaktadır[50]. Ancak bu ayrımdan yola çıkılarak bir tanım yapılması istenilen sonuca ulaşılmasını sağlamadığı için doktrinde eleştirilmiştir. Ayrıca bu görüşün, ilk sınıfta değerlendirdiği klasik nitelikte bilgisayarın kırılması, yakılması gibi fiziki neticeleri olan bir hareket bilişim suçundan öte mala zarar verme, hırsızlık, yağma gibi geleneksel suçların kapsamında değerlendirilecektir. Bunun dışında yapılan sınıflandırmalarda yalnızca bilgisayar ifadesinin kullanılmış olması bilişim suçları açısından da kapsayıcı bir tasnif yapılmasına imkân vermemektedir[51].

Yine bir görüş ise bilişim suçlarını TCK'da yer alan suç tiplerini baz alarak üç grupta incelemiştir. İlk grupta "*bilişim sistemlerinin ve/veya içerdiği verilerin işleyişine, bütünlüğüne, güvenliğine karşı işlenen suçların yer aldığı (TCK m.243, 244,*

[49] Amerika Birleşik Devletleri Adalet Bakanlığı da bilişim suçlarının tasnifini bu şekilde yapmaktadır. Brain Craig, **Cyberlaw: The Law of the Internet and Information Technology**, New Jersey, Pearson Education, 2013, s.112.
[50] Ali Karagülmez, **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2011, s.56 vd.
[51] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.77.

245, 135, 136, 138)"; ikinci grupta "*bilişim sistemlerinin kullanılmasının suçun nitelikli unsuru olarak tanımladığı suçların yer aldığı (TCK m. 142/2-e, 158/1-f gibi)*", üçüncü grupta ise " *bilişim sistemlerinin yalnızca bir araç olarak kullanıldığı ancak suçun unsuru olarak ayrıca tanımlanmadığı suçların(TCK m. 124, 125, 132, 133,134, 226 gibi)"* yer aldığını ifade edilmiştir[52].

Başka bir görüş ise bilişim suçlarını ana başlıklar oluşturacak şekilde beş gruba ayırarak kategorileştirmiştir. Bunlar bilgisayar sistemleri ve verileri üzerine işlenen siber suçlar (hacking, yasadışı veri toplama ve izleme vs.); içerik ile bağlantılı siber suçlar (pornografi, spam ve bağlantılı tehditler vs.); telif haklarıyla ilgili siber suçlar (telif ve markaya yönelik suçlar); bilgisayarla bağlantılı geleneksel suçlar (bilgisayar aracılığıyla dolandırıcılık, sahtecilik, kimlik hırsızlığı vs.) ve birleşik suçlardır (siber terörizm, altyapı saldırıları vs.)[53].

Bilişim suçları geniş anlamda "*bilişim sistemlerinin ve/veya verilerin kullanıldığı ya da bu sistem ya da verilere karşı işlenen her türlü suçtur*". Dar anlamda bilişim suçu "*verilere ve/veya bilişim sistemlerine veya sistemin/verilerin düzgün ve işlevsel işleyişine, güvenliğine ve bütünlüğüne karşı suçlardır*"[54]. Geniş anlamda bilişim suçları, ceza kanunda yer alan suçların teknolojinin sağladığı kolaylıkla

[52] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.82-83. Mahmutoğlu da benzer yönde bir ayrıma giderek bilişim suçlarının ayrımını şu şekilde ifade etmiştir: "Bu suçları; 1- Sadece bilişim sisteminin kullanılmasıyla işlenebilen suçlar (doğrudan ya da dar anlamda veyahut gerçek bilişim suçları), 2- Bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olan suçlar ve 3- Kanunda bu sistemin kullanılması zorunlu olmamakla birlikte, söz konusu sistemin suçta vasıta olarak kullanıldığı suçlar, şeklinde ayrımlara tabi tutabiliriz.
Buna göre; sadece bilişim sisteminin kullanılmasıyla işlenebilenler; Bilişim Sistemine Girme (TCK md.243), Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme (TCK md.244), Banka ve Kredi Kartlarının Kötüye Kullanılması (TCK md.245), bilişim sisteminin kullanılması zorunlu olmamakla birlikte, bazı suçların nitelikli hali olanlar; Hırsızlık (TCK md. 142/2-e) ve Dolandırıcılık (TCK md. 158/1-f), bu sistemin kullanılması zorunlu olmamakla birlikte söz konusu sistemin suçta vasıta olabileceği suçlar ise; Haberleşmenin Gizliliğini İhlal (TCK md. 132), Haberleşmenin Engellenmesi (md. 124), Eğitim ve Öğretimin Engellenmesi (md. 112), Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetlerinin Engellenmesi (TCK md. 113), Hakaret ve Sövme (TCK md. 125), Müstehcenlik (TCK md. 226), Kumar Oynanması İçin Yer ve İmkân Sağlanması (TCK md. 228), Suç İşlemeye Tahrik (TCK md. 214), Cinsel Taciz (TCK md. 105) gibi suçlardır." Fatih Selami Mahmutoğlu, "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İÜHFM**, C. LXXI, S. 1, s. 856.

[53] Yılmaz, **a.g.e.**, s.21 vd.
[54] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.77.

işlenmesidir, dolayısıyla bu suçlar "*bilgisayarla bağlantılı suç*" olarak ifade edilmektedir[55]. Dar anlamda bilişim suçları ise, "*bilgisayar suçları*" olarak ifade edilen ve teknolojinin gelişmesinin sonucu olarak yeni suç tiplerinin oluşmasına sebebiyet veren suçlardır[56].

C. Veri

Bilişim suçlarının çoğu zaman konusunu oluşturan "*veri*" kelimesi İngilizcede "*data*" yani bilgi kelimesinden gelmektedir. Veri; bilişim sisteminin üzerinde işlem yapabileceği, aktarabileceği, saklayabileceği, yeniden erişebileceği ve sonuç üretebileceği bilgiler olarak tanımlanabilir[57]. Bilişim sistemi verilerin biçimiyle ilgilenir ve onları sayısal verilere[58] dönüştürür[59]. Bilişim sistemi içinde yer alan her türlü bilgi (yazı, belge, program vs.) veri olarak değerlendirilir[60].

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 1'inci Bölümünün 1'inci maddesinin b fıkrasında bilgisayar verisi tanımlanmıştır. Buna göre "*Bilgisayar verisi belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünüdür.*"

TCK'nın 243'üncü maddesinin gerekçesinde ise verinin kapsamı belirtilmiştir. Buna göre "*sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır*"[61].

---

[55] Akbulut, **Bilişim Alanında Suçlar**, s.39-40. Benzer yönde bkz. Yılmaz Yazıcıoğlu, "Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir, Dokuz Eylül Üniversitesi Yayını,2002, s.460.

[56] Akbulut, **Bilişim Alanında Suçlar**, s. 39.

[57] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),,** s.84.

[58] Veriler bilişim sistemi içinde yazılım diline çevrilir. C dilinde sayı, karakter ve string (karakter dizilimi) olarak üç adet ana veri tipi bulunmaktadır. Ayrıntılı bilgi için bkz. Timur Karaçay, "Veri Tipleri",http://www.baskent.edu.tr/~tkaracay/etudio/ders/prg/c/dataTypes.pdf , Erişim Tarihi: 14.11.2017.

[59] Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, s. 29-30;

[60] Yenidünya/Değirmenci, **a.g.e.**, s.48.

[61] Ayrıca 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2'nci maddesinin 1'inci fıkrasının k bendinde veri "bilgisayar tarafından üzerinde işlem yapılan her türlü değer" olarak tanımlanmıştır. 5070 sayılı Elektronik İmza Kanunu'nun tanımlara yer verdiği 3'üncü maddesinin b bendinde elektronik verinin "

II. BİLİŞİM SİSTEMİNE GİRME SUÇUNUN TARİHSEL GELİŞİMİ

A. Mülga 765 Sayılı TCK'da Durum

3756 sayılı 765 Sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun ile bilişim suçları 765 sayılı TCK kapsamına 11'inci Bab başlığı altında düzenlenmiştir. Bu suçların ceza kanunlarımıza girmesi ve düzenlenmesinde 1994 tarihli Fransız Ceza Kanunu'nda yer alan düzenlemelerden esinlenilmiştir[62].

765 sayılı TCK'nın 525a maddesinin 1'inci fıkrasında bilişim sisteminde yer alan verilerin ele geçirilmesi, 2'nci fıkrasında başkasına zarar vermek amacıyla sistemde yer alan verilerin kullanılması, nakledilmesi ve çoğaltılması suç olarak sayılmıştır. 525b maddesinin ilk fıkrasında başkasına zarar vermek ya da kendisine veya başkasına yarar sağlamak maksadıyla, bilgilerin otomatik işleme tabi tutmuş bir sistemi, verileri ya da diğer herhangi bir unsuru kısmen veya tamamen tahrip edilmesi, değiştirilmesi, silinmesi, sistemin işlemesine engel olunması veya yanlış biçimde işlemesine sebep olunması yaptırıma bağlanmıştır. Aynı maddenin ikinci fıkrasında bilgileri otomatik işleme tutan sistemin kendisi veya başkası lehine hukuka aykırı yarar sağlamak için kullanılması suç olarak düzenlenmiştir. 525c maddesinde ise "*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*" ceza verileceği belirtilmiştir.

765 sayılı TCK'nın 525a maddesinin 1'inci fıkrasına göre, "*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*".

elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları" ifade ettiği belirtilmiştir.

[62] Sulhi Dönmezer, **Kişilere ve Mala Karşı Cürümler**, 17. Baskı, İstanbul, Beta Basım A.Ş., 2004, s.613.

Söz konusu suç tipi ile izinsiz olarak kişilerin bilişim sisteminde bulunan bilgi ve verilerin bütününün veya içeriğinin hukuka aykırı olarak ele geçirilmesi yaptırıma bağlanmıştır. Kanuni tanımda yer alan "*ele geçirmek*" ifadesinden anlaşılması gerekenin bilgiye ulaşma veya öğrenme olduğu doktrinde belirtilmiştir[63]. Bu suç tipiyle bilgisayar casusluğunun önüne geçilmeye çalışılmıştır[64].

756 sayılı TCK'nın 525a/1 maddesinde yer alan bu suç tipi doktrinde "*Verilerin Ele Geçirilmesi*"[65], "*Sır Aleyhine İşlenen Suç*"[66], "*Bilgisayar İçeriğinden Yararlanma*"[67], "*Sistemde Yer Alan Bilgiyi Öğrenme, Sır Aleyhine Suç*"[68], "*Bilişim Sisteminde Yer Alan Verinin Ele Geçirilmesi*"[69] gibi farklı şekillerde isimlendirilmiştir.

Doktrinde kanun koyucunun bu maddede yer alan suç tipini TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçu ile yeniden düzenlemek istediğini savunan görüşler[70] bulunsa da ağırlıkta olan görüş 765 sayılı TCK'da bilişim sistemine girme suçunun bulunmadığı[71] yönündedir.

TCK'nın 243'üncü maddesinin gerekçesine göre, "*1/3/1926 tarihli ve 765 sayılı Kanunun 525 a ilâ 525 d maddelerinde yer alan bilişim suçları, 1989 Tasarısından çok küçük değişikliklerle alınıp 6/6/1991 tarihli ve 3756 sayılı Kanunla kanunlaştırılmış ve 765 sayılı Kanuna sokulmuştu. Aradan geçen süre içinde bu suçlar konusunda Batı hukukunda değişiklikler olduğu gibi bizde de metinler ve suçların oluşması yönünden bazı duraksamalar meydana geldi. Bu nedenle Tasarıdaki maddelerin bütünüyle yeniden ele alınması uygun sayılmıştır*". Madde gerekçesinden

---

[63] Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, s. 233-234.
[64] Dönmezer, **a.g.e.**, s.620.
[65] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, 6. Baskı, Ankara, Seçkin Yayıncılık, 2015, s.240.
[66] Önder, **a.g.e.**, s.506.
[67] Dönmezer, **a.g.e.**, s.620.
[68] Yazıcıoğlu, **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, s. 233.
[69] Yenidünya/Değirmenci, **a.g.e.**, s.51.
[70] Ketizmen, **a.g.e.**, s.80. Ayrıca bkz. Tezcan/Erdem/Önok, **a.g.e.**, 978.
[71] Koca/Üzülmez, **Ceza Hukuku Özel Hükümler**, s. 805; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1366; Ali Parlar, **Bilişim Alanında İşlenen Suçlar**, Ankara, Bilgi Yayınevi, 2011, s.15; Cengiz Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, İstanbul, Acar Matbaacılık, 2017, s.43; Olgun Değirmenci, "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **TBB Dergisi**, S.58, 2005, s.203.

de anlaşılacağı üzere, 765 sayılı TCK'da yer alan bilişim suçları kanun koyucu tarafından en baştan tekrar ele alınmıştır.

765 sayılı TCK'da yer alan düzenleme bilişim sistemine yalnızca girmeyi veya orada kalmayı yeterli saymayıp, ayrıca bilişim sisteminden programların, verilerin veya diğer herhangi bir unsurun ele geçirilmesini aramıştır[72]. Oysa 5237 sayılı TCK'da düzenlenen bilişim sistemine girme suçunda 2016 yılından önce bilişim sistemine girme ve kalma fiili, 2016 yılında yapılan değişiklikle birlikte ise yalnızca bilişim sistemine girme veya orada kalma fiili suçun oluşumu için yeterlidir. Dolayısıyla bu iki suç tipinin birbirini karşıladığı söylenemez. Dolayısıyla 5237 sayılı TCK'nın 243'üncü[73] maddesinin yürürlüğe girmesiyle bilişim sistemine girme suçunun hukukumuza ilk kez girdiğini kabul etmek gerekmektedir[74].

B. 5237 Sayılı TCK'da Durum

2001 tarihli TCK tasarısı ve akabinde yürürlüğe giren 5237 sayılı TCK ile bilişim suçlarıyla ilgili değişiklikler yapılmıştır. TCK'nın İkinci Kitabının "*Topluma Karşı Suçlar*" başlıklı 3'üncü kısmının 10'uncu bölümünde "*Bilişim Alanında Suçlar*" başlığı altında 243-246'ıncı maddeler arasında bilişim suçlarına dair düzenlemelere yer verilmiştir. Bu bölümde "*Bilişim Sistemine Girme*" (TCK m.243), "*Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme*" (TCK m.244) ve "*Banka ve Kredi Kartlarının Kötüye Kullanılması*" (TCK m. 245) yaptırım altına alınmıştır[75].

---

[72] Hayati Pallı, "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, Kayseri, 2008, s.152; Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, **Yorumlu-Uygulamalı Türk Ceza Kanunu**, C.5, 2. Baskı, Ankara, Adalet Yayınevi, 2014, s.7286.

[73] Bilişim sistemine girme suçu 5237 sayılı TCK'dan önce ilk kez 1997 TCK Öntasarısında gündeme gelmiş daha sonra 2000 ve 2003 tarihli Türk Ceza Kanunu Öntasarlarında da yer almıştır.

[74] Doktrinde 765 sayılı TCK'nın 525a-1 maddesinin 5237 sayılı TCK'nın 135 ve 136'ıncı maddelerine denk geldiği savunulmaktadır. Bkz. Murat Volkan Dülger, "Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi", **Bilişim Hukuku**, Der: Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayını, 2006, s. 400.

[75] 24.03.2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30'uncu maddesi ile 5237 sayılı TCK'da bulunan bilişim suçlarına ayrıca "Yasak Cihaz ve Programlar" suçu (TCK m.245A) eklenmiştir.

Bu bilişim suç tipleri dışında TCK'da bilişim sistemi ile ilgili olan ve özellikle içtima açısından önem arz eden bazı suçlara da yer verilmiştir. Bunlar, haberleşmenin gizliliğini ihlal (TCK m. 132), kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması (TCK m.133), özel hayatın gizliliğini ihlal (TCK m.134), kişisel verilerin kaydedilmesi (TCK m.135), verileri hukuka aykırı olarak verme veya ele geçirme (TCK m.136), verileri yok etmeme (TCK m.138) olarak sayılabilir.

Bunlar dışında TCK'da bilişim sistemine içerikle bağlantılı olarak sayılabilecek suçlar da bulunmaktadır. Bunlar müstehcenlik (TCK m.226) ve hakaret (TCK m. 125) olarak sayılabilir. Ayrıca kumar oynanması için yer ve imkân sağlama (TCK m.228/3), hırsızlık (TCK m.142/2-e) ve dolandırıcılık suçlarının (TCK m.158/1-f) bilişim sistemleri aracılığıyla işlenmesi TCK'da bu suç tiplerinin nitelikli halleri olarak sayılmıştır.

"*Bilişim Sistemine Girme Suçu*" ilk kez TCK'nın "*Özel Hükümleri*" düzenleyen ikinci kitabının "*Topluma Karşı Suçlar*" başlıklı üçüncü kısmının onuncu bölümü içinde yer alan "*Bilişim Alanında Suçlar*" içinde 243'üncü maddede düzenlenmiştir.

1997 tarihli Türk Ceza Kanunu Ön Tasarısı'nda yer alan ve Fransız Ceza Kanunu'nda yer alan düzenlemelerden[76] esinlenilerek hazırlanan 347'inci madde "*bilişim sistemine girme, verileri tahrip ve bozma*" şeklinde başlıklandırılmış[77], bilişim sistemine girme veya bilişim sisteminde kalmaya devam etme suç olarak tanımlanmıştır[78]. Tasarıda yer alan madde, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde yer alan "*Yetkisiz Erişim*" düzenlemesine paralellik

[76] Yılmaz Yazıcıoğlu, "Yeni Türk Ceza Kanunundaki Bilişim Suçlarının Değerlendirmesi", **YÜHFD**, C. II, S 2, İstanbul, 2005, s: 394.

[77] Madde 347: "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 fiil nedeniyle sistemin içerdiği veriler yok edilir ve değiştirilirse faile iki yıldan dört yıla kadar hapis ve ikiyüzmilyondan altıyüzmilyon liraya kadar ağır para cezası verilir.
Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Bkz. Akbulut, **Bilişim Alanında Suçlar**, s.113, dn. 299.

[78] İlker Tepe, "Modern Ceza Hukuku Anlayışında İnternet Suçluluğu Ve Türk Ceza Hukukundaki Yansımaları", **Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, Antalya, 2009, (Çevrimiçi), tez.yok.gov.tr, Erişim Tarihi: 03.08.2018, s.69.

oluşturacak şekilde düzenlenmiştir. Amacı ne olursa olsun failin bilişim sistemine haksız ve kasten girmesine veya sistemde kalmasına suç tipinde seçimlik hareket olarak yer verilmiştir. Böylece söz konusu düzenleme bu hareketlerden birinin yapılmasını suçun tamamlanması için yeterli saymıştır. Tasarıda yer alan maddenin 2'nci fıkrasında bilişim sistemine girme veya orada kalma fiilinin gerçekleştirilmesi sonucunda sistemde yer alan verilerin yok edilmesi veya değiştirilmesi hali neticesi sebebiyle ağırlaşmış hal olarak düzenlenmiştir. 3'üncü fıkrada ise söz konusu suç teşebbüs aşamasında kalsa dahi tamamlanmış suç gibi cezalandırılacağı hükme bağlanmıştır. Bu suça yaptırım olarak adli para cezası ve hapis cezası beraber öngörülmüştür.

2000 tarihli Türk Ceza Kanunu Ön Tasarısı'nın 345'inci[79] maddesinde ve daha sonra 5237 sayılı TCK'nın yasalaşması için 15.03.2003 tarihinde TBMM'ye sunulan Hükümet Tasarısı'nın 346'ıncı[80] maddesinde, 1997 tarihli Türk Ceza Kanunu Ön Tasarısı 347'inci maddesinden farklı olarak yalnızca para cezaları arttırılmış, geri kalan hükümler 1997 tarihli Türk Ceza Kanunu Ön Tasarısında yer aldığı şekliyle korunmuştur[81].

5237 sayılı TCK'nın 01.06.2005 tarihinde yürürlüğe girmesiyle bilişim sistemine girme suçu 243'üncü maddede hükme bağlanmıştır. Ancak Tasarıda yer alan düzenleme TBMM Genel Kurulu'nda bazı değişikliklere uğramıştır. İlk olarak, madde

[79] Madde 345: "Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve birmilyar liradan üçmilyar liraya kadar ağır para cezası verilir.
Bu fiil nedeniyle sistemin içerdiği veriler yok edilir ve değiştirilirse faile iki yıldan dört yıla kadar hapis ve ikimilyar liradan altımilyar liraya kadar ağır para cezası verilir.
Bu suçlara teşebbüs halinde faillere tamamlanmış suç cezası verilir." Bkz. Akbulut, **Bilişim Alanında Suçlar**, s.114, dn.301.

[80] TCK tasarısının 346'ıncı maddesinin "bilişim sistemine girme, verileri tahrip ve bozma" başlıklı düzenlemesi; "(1)Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıldan üç yıla kadar hapis ve üçmilyar liradan onmilyar liraya kadar ağır para cezası verilir. (2) Bu fiil nedeniyle sistemin içerdiği veriler yok edilir veya değişirse faile iki yıldan dört yıla kadar hapis ve beşmilyar liradan onbeşmilyar liraya kadar ağır para cezası verilir. (3) Bu suçlara teşebbüs hâlinde faillere tamamlanmış suç cezası verilir" şeklindeydi. Söz konusu tasarıda yer alan madde uluslararası sözleşmelere de uygun olarak düzenlenmiştir. Buna göre bilişim sisteminde kalma aranmaksızın yalnızca bilişim sistemine hukuka aykırı ve kasten giren kişi cezalandırılmaktadır. Gerekçe ve ilgili madde için bkz. http://www2.tbmm.gov.tr/d22/1/1-0593.pdf , 03.07.2018.

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

başlığı "*Bilişim Sistemine Girme*" olarak düzenlenmiştir[82]. Tasarıda yer alan düzenlemenin ve Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde yer alan "*Yetkisiz Erişim*" düzenlemesinin aksine 243'üncü maddenin 1'inci fıkrasında "*bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden"* kişinin cezalandırılacağı belirtilmiştir. Kanun koyucunun "*veya*" bağlacı yerine "*ve*" bağlacını tercih etmesindeki sebep TBMM Genel Kurulu Tutanağına göre, bilişim sistemine hatayla giren kişilerin cezalandırılmasını önlemektir[83]. Bunun dışında doktrinde söz konusu düzenlemenin Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesi ile uyumlu olduğunu savunan görüş de vardır. Bu görüşün dayandığı gerekçeye göre, Avrupa Konseyi Siber Suçlar Sözleşmesi'ne taraf devletler yetkisiz erişimi mevzuatlarında suç olarak düzenlemekle yükümlüdür, ancak mevzuatlarında yetkisiz erişimin suç oluşturması adına bazı ek koşullar konulabilmektedir ve bilişim sistemine girdikten sonra orada kalma fiili de bu ek unsurlardan sayılmalıdır[84]. Dolayısıyla bu görüşü savunanlar TCK'nın 243/1'inci fıkrasında "*ve*" bağlacının kullanılmasını Avrupa Konseyi Siber Suçlar Sözleşmesi'ne aykırı olarak değerlendirmemektedir.

Ayrıca maddede fiillerin ağırlığına göre yaptırım uygulanmadığı gerekçesiyle Tasarıda yer alan ceza aralıklarından farklı ceza aralıklarına yer verilmiş, suçun temel halinin yaptırımı bir yıla kadar hapis veya adlî para cezası şeklinde hükme bağlanmıştır[85]. Tasarıdan farklı olarak, maddenin 2'nci fıkrası, suçu oluşturan fiilin "*bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi*" halini cezayı hafifleten nitelikli hal olarak düzenlemiştir. Maddenin 3'üncü fıkrasında ise Tasarıda yer alan neticesi sebebiyle ağırlaşmış hale aynı şekilde yer verilmiş, yaptırım olarak

---

[82] Doktrinde söz konusu maddenin başlığı "bilişim sistemine girme" olsa da yaptırım konusu fiil bilişim sistemine girme ve kalma olduğu için düzenlemenin yanıltıcı olduğu ileri sürülmekteydi. Bkz. Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1368; Şaban Cankat Taşkın, **Bilişim Suçları**, Bursa, Beta Yayınları, 2008, s.2; Ketizmen, **a.g.e.**, s.81.

[83] İlgili TBMM Genel Kurul Tutanağı için bkz. http://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?_adf.ctrl-state=186sfgmhll_19&psira=18779&psorgukriteri= , Erişim Tarihi: 03.07.2018.

[84] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1369.

[85] İlgili TBMM Genel Kurul Tutanağı için bkz. http://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?_adf.ctrl-state=186sfgmhll_19&psira=18779&psorgukriteri= , Erişim Tarihi: 03.07.2018.

ise altı aydan iki yıla kadar hapis cezası öngörülmüştür. Tasarının aksine, suçun teşebbüs halinde kalmasının tamamlanmış bir suç gibi cezalandırılacağına ilişkin düzenleme maddeye konulmamıştır.

Bilişim sistemine girme ve orada kalma hareketlerine çok hareketli suç olarak yer veren düzenleme, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesi ile uyumlu olmadığı gerekçesiyle doktrinde hayli eleştirilmiş[86], 20.03.2016 tarihli 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30'uncu maddesi ile TCK madde 243'de değişiklik yapılmıştır. Böylece "*bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden*" kişinin cezalandırılacağı hükme bağlanarak kanuni tanımda bilişim sistemine girme ile orada kalma fiilleri suçun oluşması için seçimlik hareket olarak düzenlenmiştir. Maddenin gerekçesinde de "… *Sanal Ortamda İşlenen Suçlar Sözleşmesinin 3'üncü maddesiyle, üye ülkeler, yasadışı araya girme eylemini cezalandırmaya davet edildiğinden, 5237 sayılı Kanunun 243'üncü maddesinde değişiklik öngörülmüştür. Böylece bilişim sistemlerinin bütününe veya bir kısmına hukuka aykırı olarak girmekle birlikte belirli bir süre kalmak da suçun unsuru olarak düzenlenmiş olmasına rağmen Sözleşmeye uyum amacıyla sadece sisteme/sistemlere girmek fiili suç olarak düzenlenmektedir*" ifadelerine yer verilmiştir. Bunun sonucunda Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinden farklı olarak bilişim sisteminde kalma fiili de ayrıca suç oluşturmaktadır[87]. Bu sayede, rıza ile bilişim sistemine girilmesine rağmen hukuka uygunluk sebebi olan rızanın ortadan kalkmasından sonra hâlâ bilişim sisteminde kalmaya devam eden failin cezalandırılması da mümkün hale gelmiştir[88].

6698 sayılı Kanun'un 30'uncu maddesi ile TCK'nın 243'üncü maddesine 4'üncü fıkra eklenmiştir. Bu fıkra ile bilişim sistemine girmeksizin bir bilişim sisteminin kendi içinde veya diğer bilişim sistemleri ile arasında gerçekleşen veri nakillerinin teknik araçlarla hukuka aykırı olarak izlenmesi yaptırıma bağlanmıştır. Ancak söz konusu ek fıkra her ne kadar TCK'nın 243'üncü maddesinin "*bilişim*

[86] Eleştiriler için ayrıca Bkz. Taşkın, **Bilişim Suçları**, s.2; Ketizmen, **a.g.e.**, s.81, Akbulut, **Bilişim Alanında Suçlar**, s.127-128; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (6),** s.341-342.
[87] Akbulut, **Bilişim Alanında Suçlar**, s.115.
[88] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku(7),** s.236.

sistemine girme" başlığı altında yer alsa da bağımsız bir suç olarak değerlendirilmelidir[89]. Doktrinde bilişim sistemine girmeksizin veri nakillerini izleme suçunda bilişim sistemine girme söz konusu olmadığı halde kanun koyucunun bu suçu 243'üncü madde içine koymak yerine neden ayrı bir madde olarak (Örneğin; Madde 243 A gibi) düzenlemediği eleştirilmiştir[90].

III. BAZI ÜLKE MEVZUATLARINDA VE AVRUPA KONSEYİ SİBER SUÇLAR SÖZLEŞMESİ KAPSAMINDA BİLİŞİM SİSTEMİNE GİRME SUÇU

A. İngiltere

İngiltere'de bilişim suçları için "*1990 Bilgisayarın Kötüye Kullanılması Kanunu*" (Computer Misuse Act 1990) düzenlenmiş, bu Kanun 29.08.1990 yılında yürürlüğe girmiştir. Bu Kanun'un "*Bilgisayarın Kötüye Kullanılması Suçları*" (Computer Misuse Offences) bölümünün 1'inci maddesinde hukuka aykırı ve yetkisiz bir şekilde bilişim sistemine girme fiili yaptırıma bağlanmıştır[91]. Bu suça vücut veren fiiller temel olarak "*hacking*" ve "*cracking*" olarak sayılmıştır[92].

Söz konusu madde "*bilgisayar materyallerine yetkisiz erişim*" (Unauthorised Access to Computer Material) şeklinde başlıklandırılmış ve üç fıkra altında düzenlenmiştir.

İlk fıkrada sisteme güvenli erişim yetkisi olmayan kişi tarafından bilgisayarda bulunan bir program veya veriye erişimin kasten ve hukuka aykırı bir şekilde gerçekleştirilmesinin suç oluşturacağı belirtilmiştir. İkinci fıkrasında failin kastının doğrudan özel bir program veya veriye, kendine has herhangi bir program veya veriye

---

[89] Akbulut, **Bilişim Alanında Suçlar**, s.157, Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.807; Veli Özer Özbek v.d., **Türk Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Seçkin Yayıncılık, 2017, s. 938; Ahmet Gül, **Doğrudan / Dolaylı Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2016, s.57.

[90] Akbulut, **Bilişim Alanında Suçlar**, s.157.

[91] İlgili kanun metni için bkz. https://www.legislation.gov.uk/ukpga/1990/18/contents, Erişim Tarihi:10.4.2019.

[92] Walden, **Computer Crime**, s.12.

ya da özel bir bilgisayardaki program veya verilere yönelik olmasının gerekmediği belirtilmiştir. Üçüncü fıkrasında ise bu suça uygulanacak yaptırımlara yer verilmiştir[93].

Her ne kadar Kanun metninde bilgisayar, program ve veri kelimelerine yer verilse de Kanun'da bunlara ilişkin bir tanım yapılmamıştır. Gelişen ve değişen teknoloji karşısında yapılacak tanımların eski ve yetersiz kalacağı endişesiyle bu kavramlar tanımlanmamış ve somut olay çerçevesinde tekrar değerlendirilmesi gereken kavramlar olduğu düşünülmüştür[94]. Mevcut düzenleme uyarınca yetkisiz erişimin fiziksel olarak ya da uzaktan erişim şeklinde gerçekleşebilmesi mümkündür[95].

Yetkisiz erişim bakımından İngiliz hukukunda en çok tartışılan konu çalışanların yetkisi olmamasına rağmen çalıştığı yerin bilişim sistemine girmesi halinde 1990 Bilgisayarın Kötüye Kullanılması Kanunu'nun 1'inci maddesinin uygulanıp uygulanmayacağı sorunudur.

1998 yılında Denetleme Kurulu (Audit Commision) tarafından hazırlanan bir rapora göre, hastane sisteminde yer alan hasta bilgilerine girmeye yetkisi olan bir hemşire kendi ailesinin ve arkadaşlarının sağlık raporlarına ulaşabilmek için hastanenin bilişim sistemine girmiş ve bu bilgileri yakınlarıyla paylaşmıştır. Fakat hemşire bu hareketinden dolayı 1990 Bilgisayarın Kötüye Kullanılması Kanunu'nun 1'inci maddesi gereğince cezalandırılmamış, yalnızca hastaların gizlilik hakkını ihlal ettiği gerekçesiyle yazılı uyarı almıştır[96].

Ancak 1998 tarihlli DPP v Bignell davasında ise farklı bir sonuca ulaşılmıştır. Polis memuru olan Bay ve Bayan Bignell yalnızca mesleki amaçlarla kullanılması

---

[93] Mohamed Chawki, "Unauthorized Access Offences in Cyberworld", **Cybercrime, Digital Forensics and Jurisdiction**, Chawki, M./ Darwish, A., Khan, M.A., Tyagi, S., (Çevrimiçi), http://www.springer.com/gp/book/9783319151496, Switzerland, 2015, s.32.

[94] Derek Wyatt, "'Revision of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group", **All Paert Parliamentary Internet Group**, 2004, (Çevrimiçi), https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf, Erişim Tarihi: 20.11.2017, s. 4; Walden, **Computer Crime**, s.12.

[95] "Unauthorised access with intent to commit or facilitate commission of further offences", (Çevrimiçi), https://www.inbrief.co.uk/offences/unauthorised-access-to-computer-material/, Erişim Tarihi:20.11.2017.

[96] Bkz. Chawki, **Unauthorized Access Offences in Cyberworld**, s.33.

gerektiklerini bildikleri ulusal polis bilgisayarlarından (Police National Computer) resmi olmayan amaçlarla özel bilgileri araştırmışlardır. Sulh ceza mahkemesi polis memurlarını bu suçtan dolayı mahkûm etmiş fakat bu karar temyiz edilmiştir. Ancak üst derece mahkemesi bilişim suçlarıyla korunan değerin bilgisayar sistemi içinde bulunan bilgilerin bütünlüğü değil bilgisayar sisteminin bütünlüğünün olduğu[97], bir işverenin "*işin gerektirdiği*" ölçüde bilişim sistemine girmesine izin vermesi halinde erişim için belli bir yetki sınırı çizilse dahi sınırın aşılması durumunda yetkisiz erişim suçunun oluşmayacağı[98] belirtilmiş ve kararı bozmuştur. Bu karar İngiliz doktrininde yoğun tartışmaların yaşanmasına sebep olmuştur. Çünkü bilgisayar sistemine erişme yetkisi olan bir kişinin amacı dışında bilişim sistemine veya yetki dışı kalan bölümlere girmesinin bu maddenin dışında bırakılması kötü niyetli kişilere yaptırım uygulanmasını engeller nitelikteydi[99].

Bu karardan sonra 1999 yılında verilen Regina v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America davasında ise DPP v Bignell kararı tekrar değerlendirilmiştir. Bu kararın neticesinde yetki dışı amaçla bilişim sistemine girmenin veya yetki dışı bir bilişim alanına girmenin kanun kapsamında cezalandırılmasının ancak çalışanın bir programa veya bilgisayara erişiminin sınırlarının açıkça tanımlanmış olması halinde mümkün olabileceğine karar vermiştir[100,101].

---

[97] Bkz. Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future", **Criminal Law Review**, 2008, (Çevrimiçi), http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf, Erişim Tarihi:20.11.2017, s. 2.

[98] Selman Dursun, "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", **MHB- Prof. Dr. Gülören Tekinalp'e Armağan**, C. 1-2, 2003, s.279.

[99] **A.e.**; David Cook, "The Court's nonsensical approach to unauthorised access in DPP v Bignell", (Çevrimiçi), http://www.pannone.com/media-centre/blog/cybercrime-blog/the-court's-nonsensical-approach-to-unauthorised-access-in-dpp-v-bignell, Erişim Tarihi:20.11.2017; Chawki, **Unauthorized Access Offences in Cyberworld**, s.33.

[100] Karar için bkz. Regina v. Bow Street Magistrates Court and Allison (A.P.) Ex Parte Government of the United States of America (on Appeal from a Divisional Court of the Queens Bench Division), (Çevrimiçi), https://publications.parliament.uk/pa/ld199899/ldjudgmt/jd990805/bow.htm, Erişim Tarihi: 20.11.2017.

[101]Konuyla ilgili benzer kararlar için bkz. Murat Volkan Dülger, "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", **TAAD**, Y.8, S. 31, Temmuz 2017, 199-203.

B. Amerika Birleşik Devletleri

Bilgisayarın anavatanı kabul edilen Amerika Birleşik Devletleri bilişim suçlarının yaptırıma bağlanmasında da öncü bir rol üstlenmiştir. Bilişim suçlarıyla ilgili ilk kanun tasarısı 1977 yılında Senatör Abraham Ribikoff tarafından hazırlanmış ancak tasarı Amerika Birleşik Devletleri Kongresi tarafından kabul edilmemiştir[102]. Bilişim suçlarıyla ilgili pek çok federal kanunu olan Amerika Birleşik Devletleri'nde bilişim suçlarıyla ilgili en temel kanun 1986 tarihli Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu'dur (Computer Fraud and Abuse Act)[103]. CFAA'in a fıkrasında bir kişinin bilgisayara[104] yetkisiz veya yetkisini aşarak erişmesi yaptırıma bağlanmıştır. Ayrıca bu kanun kapsamında bilgisayar verilerinin tahribi ve değiştirilmesi de yaptırıma bağlanmış diğer suçlardır.

Yıllar içinde CFAA'e yapılan ekleme ve değişikliklere rağmen Amerikan doktrinde bu Kanun teknoloji alanındaki en kötü kanun olarak değerlendirilmiştir[105]. Kanunda yer alan düzenlemeler geniş kapsamlı ve belirsiz bulunmuş, bunun sonucunda keyfi ve ayrımcı uygulamalar ile aşırı suçlamalara sebebiyet vermesi nedeniyle eleştirilmiştir[106].

---

[102] U.S. Departman of Justice Bureau of Statistic, **Computer Crime Legislative Resource Manual,** (Direktor: Benjamine H. Renshaw), Washington D.C., ,1990, (Çevrimiçi), https://www.ncjrs.gov/pdffiles1/Digitization/78890NCJRS.pdf, Erişim Tarihi: 27.11.2017, s. 55.

[103] Computer Fraud and Abuse Act Amerikan Temel Kanunu olan U.S. Act'in 18'inci başlığı, 1'inci bölüm, 47'inci bölümünün 1030'uncu paragrafında yer almaktadır. Söz konusu kanun tezde "CFAA", ilgili kanun maddesi ise Amerikan Temel Kanunundaki yerine göre "18 U.S.C. 1030" şeklinde kısaltılarak kullanılacaktır.

[104] CFAA'in e fıkrasının 1'inci bendinde bilgisayarın tanımına yer verilmiştir. Bu tanıma göre bilgisayar elektronik, manyetik, optik, elektrokimyasal verileri veya yüksek hızda mantıksal ve aritmetik veri işlemeyi gerçekleştirebilen veya bunları depolayabilen, doğrudan bu işlemleri yapabilen veya bu tür aygıtlarla birlikte çalışarak her türlü veriyi depolama veya iletişim tesisini kapsayan her türlü aygıtı kapsamaktadır. Ancak kanun koyucu otomatik daktilo, dizgi makinası, taşınabilir hesap makinası ve benzeri cihazları kapsam dışı bıraktığını kanunda açıkça yazmıştır.

[105] Kristin Westerhorstmann, "The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Atacks, Fake Dating Profiles, and Employees Who Check Facebook at Work**", University of Miami National Security & Armed Conflict Law Review**, V. 145, 2015, (Çevrimiçi), https://repository.law.miami.edu/cgi/viewcontent.cgi?referer=https://www.google.com.tr/&httpsredir=1&article=1078&context=umnsac, Erişim Tarihi: 22.11.2017, s.145.

[106] **A.e.**

CFAA'in kapsamı yürürlüğe girdiğinden itibaren defalarca genişletilmiştir. Örneğin 1994 yılına kadar yalnızca milli güvenliğe, finansal kayıtlara ve kamu kurumlarına yönelik bilişim suçları CFAA kapsamındayken, 1994 yılı itibariyle yasa gerçek kişilere ait bilişim sistemlerini de kapsam içine dahil etmiş, 1996 yılında devletlerarası kullanılan ve ticari işler için kullanılan bilgisayarlar da korunan bilgisayarlar içinde sayılmıştır[107]. İlerleyen yıllarda ise her türlü bilgisayarları koruyan ve kapsam içine alan düzenlemeler yapılmıştır[108].

CFAA hakkında değişiklik yapan 2015 Aaron Kanunu (Aaron's Law Act of 2015) bilişim sistemine girmede yetki aşımını da suçun kapsamı içine alan düzenlemeler yapmayı hedeflemiş ve CFAA'de yer alan düzenlemelerin açık hale getirilmesini amaçlamıştır. Bu değişiklikle yetkisiz erişimin yaptırıma bağlanmasına ek olarak yetkinin aşıldığı erişimler de suç olarak düzenlenmiştir[109]. Amerikan doktrininde bu düzenlemenin uygulama alanını genişlettiği yönünde eleştirilerde bulunulmuş, "*insider hacking*"[110] faaliyetlerinin de cezalandırılmasını engellememek amacıyla bilişim sistemine yetki aşımıyla erişim fiilini tamamen suç olmaktan çıkarmadan yetki aşımının suç oluşturmasının belirli sınırlara tabi tutularak düzenlenmesi gerektiği savunulmuştur[111]. CFAA genel olarak aşırı suçlamalara sebep olduğu için eleştirilmektedir[112]. Örneğin kişinin eşinin şifresini bildiği e-posta adresine hizmet şartlarına aykırı şekilde girmesi kanun kapsamında suç sayıldığı için aşırı suçlamalara yol açmaktadır[113]. Amerikan doktrininde CFAA'in genel olarak eski bir

---

[107] James Juo, "The CFAA and Aaron's Law", **Virginia Lawyer**, V.62, December 2013, (Çevrimiçi), http://www.vsb.org/docs/valawyermagazine/vl1213-tech.pdf, Erişim Tarihi: 27.11.2017, s.61.
[108] **A.e.**
[109] **A.e.**
[110] CFAA'de yer alan yetki aşımı düzenlemesiyle dışardan gerçekleşen yetkisiz erişim sağlayan "outsider" yani yabancı kişilerin yanısıra verilen izin veya onayın dışına çıkarak yetki aşımına sebebiyet veren "insider" yani belli bir grubun içindeki belli bir yetkiye sahip kişilerin de cezalandırılmasının önü açılmıştır. Peter A. Winn, "The Guilty Eye: Unauthorized Access, Trespass and Privacy", **The Business Lawyer**, Vol.62, August 2007, Çevrimiçi, https://heinonline.org/HOL/Page?handle=hein.journals/busl62&collection=journals&id=1411&startid=&endid=1454 , Erişim Tarihi: 2.4.2019, s.1402.
[111] Sheldon Whitehouse, "Hacking into the Computer Fraud and Abuse Act: The CFAA at 301", **The George Washington Law Reviewer**, V.84, No.6, December 2016, (Çevrimiçi), http://www.gwlr.org/wp-content/uploads/2016/11/84-Geo.-Wash.-L.-Rev.-1437.pdf, Erişim Tarihi: 27.11.2017, s.1440.
[112] **A.e.**
[113] **A.e.**

kanun olduğu ve ihtiyaçları karşılamadığı bu sebeple bilişim suçları açısından bir reforma ihtiyaç olduğu kanaati yaygındır[114].

CFAA'de yer alan suçlar yetki olmaksızın ve verilen yetkinin aşımı[115] ile iki farklı formda işlenebilmektedir[116]. 18 U.S.C. 1030 (a)'da yetkisiz erişimden kaynaklanan yedi ayrı suç tipini bulundurmaktadır[117]. Bunlardan ilkine göre bir kişinin başka bir devlete yarar sağlayacak veya Amerika Birleşik Devletleri'ne zarar verecek bilgileri edinmek, göndermek veya göndermeye teşebbüs etmek amacıyla bir bilgisayar sistemine yetkisiz erişim veya yetkinin aşılarak erişmesi suç olarak kabul edilmiştir(18 U.S.C. 1030 (a)(1)). İkinci suç tipi ise devlet dairesi veya organına ait finansal kayıt bilgilerini içeren bilgisayarlara veya korumalı bilgisayarlara bu bilgileri edinmek için yetkisiz veya yetkinin aşılarak erişilmesidir (18 U.S.C. 1030 (a)(2)). Üçüncü suç tipi, kamuya açık olmayan devlet bilgisayarlarına yetkisiz erişimi yasaklamaktadır (18 U.S.C. 1030 (a)(3)). Dördüncü suç, devlet bilgisayarlarına, banka bilgisayarlarına, uluslararası veya dış ticaret için kullanılan bilgisayarlara yetkisiz veya verilen yetkinin aşılarak erişilmesi suretiyle dolandırıcılık suçunu düzenlemektedir(18 U.S.C. 1030 (a)(4)). Beşinci olarak devlet bilgisayarlarına, banka bilgisayarlarına, uluslararası veya dış ticaret için kullanılan bilgisayarlara zarar verme fiili suç teşkil etmektedir(18 U.S.C. 1030 (a)(5)). Altıncı olarak dolandırıcılık amacıyla devlet bilgisayarlarının, banka bilgisayarlarının veya eyaletler arası veya dış ticareti etkileyen bilgisayarların şifrelerinin veya benzeri bilgilerinin ticareti suç olarak

---

[114] Bkz. Sheldon Whitehouse, **a.g.m.**, s.1441; James Hendler, "It's Time to Reform the Computer Fraud and Abuse Act", 2013, (Çevrimiçi), https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/, Erişim Tarihi:27.11.2017.

[115] CFAA'de "yetkisiz" erişimin tanımı yapılmamasına rağmen "yetki aşımı" tanımlanmıştır. Buna göre yetki aşımı; sisteme girme yetkisi olan kişinin elde etmeye veya değiştirmeye hakkı olmadığı verileri elde etme veya değiştirme için girmesi olarak tanımlanmıştır. Ancak bu tanım aydınlatıcı bulunmamıştır. Doktrinde yetki aşımı, izin verilen veya onaylanan yetkinin ötesine geçmek olarak tanımlanmıştır. Patricia L. Bellia, "A Coda-Based Approach to Unauthorized Access Under tne Computer Fraud snd Abuse Act", **The George Washington Law Review**, Vol. 84:1442, No:6, December 2016, https://heinonline.org/HOL/Page?handle=hein.journals/gwlr84&collection=journals&id=1526&startid=&endid=1560 , s.1468-1469.

[116] Bellia, **a.g.m.**, s.1444.

[117] Orin S. Kerr, "Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes", **NYU Law Reviews**, 2003, (Çevrimiçi), http://www.nyulawreview.org/issues/volume-78-number-5/cybercrimes-scope-interpreting-access-and-authorization-computer-misuse, Erişim Tarihi:27.11.2017, s.1114.

düzenlenmiştir (18 U.S.C. 1030 (a)(6)). Son olarak bir kişiden para veya başka bir değer sızdırmak amacıyla devlet bilgisayarlarına, banka bilgisayarlarına, devletlerarası veya dış ticarette kullanılan bir bilgisayara zarar verme veya gizliliğini ihlal etme tehdidinde bulunma(18 U.S.C. 1030 (a)(7)) suç olarak sayılmıştır[118].

Maddede sayılan suç tipleri göstermektedir ki TCK'nın aksine 18 U.S.C. 1030 bilişim suçlarını ayrı ayrı maddelerde düzenlemek yerine "*yetkisiz erişim*" kavramı altında ele alarak tek bir maddede düzenlemiştir.

18 U.S.C. 1030'un (b) fıkrasında yukarda belirtilen suçlardan herhangi birini işlemenin veya teşebbüs etmenin suç teşkil ettiği ve bunun sonucunda (c) fıkrasında yer alan yaptırımların uygulanacağı belirtilmiştir. Aynı maddenin (d) fıkrası Gizli Servis'in (Secret Service) soruşturma yetkilerine, (e) fıkrası ise madde içinde geçen bazı ifadelerin tanımına yer vermiştir. Yine 18 U.S.C. 1030'un (f) fıkrasında Amerika Birleşik Devletleri'nin herhangi bir kolluk kuvvetinin soruşturma, önleme ve istihbarat faaliyetlerini yapmasının yasak olmadığı belirtilmiş, (g) fıkrası ise bu suçtan dolayı zarar gören kişilerin faile karşı hukuk davası açabileceğini düzenlemiştir. Aynı maddenin (i) ve (j) fıkrasında ise suçun işlenmesinde kullanılan suç eşyasının ve suçtan meydana gelen eşyanın müsaderesine yönelik düzenlemeler yer almaktadır.

C. Almanya

Alman hukukunda bilişim suçları genel olarak Alman Ceza Kanunu'nda düzenlenmiştir. Ancak bilgisayarla bağlantılı bazı suçlara özel ceza kanunlarında da yer verildiği görülmektedir[119].

---

[118] Charles Doyle, "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws", **Congressional Research Service**, 2014, (Çevrimiçi), https://fas.org/sgp/crs/misc/97-1025.pdf, Erişim Tarihi: 5.12.2017, s. 1-2. Elkin Girgenti"Computer Crimes", **American Criminal Law Review**, Vol.55:911, 2018, Çevrimiçi, https://heinonline.org/HOL/Page?handle=hein.journals/amcrimlr55&collection=journals&id=933&startid=&endid=982 , Erişim Tarihi:2.4.2019, s.922-923.

[119] Bettina Weisser, "Cyber Crime- The Information Society and Related Crimes, National Reports on Germany", **IAPL**, s.1.

Alman Ceza Kanunu'nun 202a maddesinde "*Veri Casusluğu*" düzenlenmiştir. Bu maddenin ilk fıkrasına göre her kim bir başkasına ait yetkisiz erişimlere karşı korunmuş verileri bu korumayı aşarak kendisi veya bir başkası için hukuka aykırı bir şekilde edinirse cezalandırılacaktır. Aynı maddenin ikinci fıkrasında ise ilk fıkrada yer alan veri ifadesinden sadece elektronik veya hemen algılanamayacak bir şekilde depolanmış veya iletilmiş veriler anlaşılması gerektiği belirtilmiştir. Alman Ceza Kanunu'nun 202b maddesinde ise bir kişinin teknik araçla veri nakilleri sırasında kendisi veya bir başkası için aleni olmayan bir veriyi edinmesi suç olarak düzenlenmiştir. Alman Ceza Kanunu'nun 202b maddesinin TCK'nın 243/4'üncü fıkrasıyla paralel olduğu söylenebilir.

Alman Ceza Kanunu doğrudan bilişim sistemine girme suçuna yer vermese de hukuka aykırı olarak veri edinmeyi suç olarak düzenlemiştir. Her ne kadar kanuni düzenleme teorik açıdan yetkisiz erişimi suç olarak düzenlemese de bilişim sistemine hukuka aykırı şekilde erişen kişinin en azından bir miktar veri edinmeden durmayacağı yönünde görüşler bulunmaktadır[120]. Başka bir görüş ise, Alman Ceza Kanunu 202 a maddesinin verilere erişimin yetkisiz olarak yapılmasını düzenlediğini ve böylece 202a'nın Avrupa Konseyi Siber Suçlar Sözleşmesi'nin yetkisiz erişimi düzenleyen 2'nci maddesini karşıladığını öngörmüştür[121]. Bu düzenlemenin bilgisayar verilerinin elde edilmesi şartına izin veren Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ikinci maddesi ile uyumlu olduğu kabul edilebilirse de, veri edinme amacı olmasa dahi bilişim sistemine hukuka aykırı erişimin ayrıca cezalandırılması korunan hukuki değer temelinde önem arz etmektedir.

Trojan veya tuş kaydedici (keylogger) yöntemiyle veri elde etme Alman Ceza Kanunu'nun 202a maddesi kapsamında cezalandırılsa da[122], Alman Hukuku'nda

[120] Ulrich Sieber, "Cybercrime and Jurisdiction in Germany, The Present Situation and the Need for New Solition",**Cybercrime and Jurisdiction**, Editor: Bert-Jaap Koops, Susan W. Brenner, Leiden, T.C.M. Asser Press, 2006, s.185, dn. 9.
[121] Ulcrich Sieber, **İnternetteki Suçlar ve Suçun İnternette Takibi**,(Edit.: Yener Ünver), Ankara, Seçkin Yayıncılık, 2014, s.65.
[122] Bettina Weisser, **a.g.e.**, s.39.

uygulama alanı bulan çevrimiçi arama yöntemiyle[123] devlet şüphelilerin bilgisayar, akıllı telefon gibi bilişim sistemlerine trojan göndererek şüphelilerin iletişimini ve verilerini her an gerçek zamanlı olarak denetleyebilmektedir[124].

D. Japonya

Japon ceza hukukunda bilişim suçları 45 sayılı ve 1907 tarihli Japon Ceza Kanunu ve 128 sayılı ile 1999 tarihli Bilgisayara Yetkisiz Erişim Kanunu'nda yer almaktadır[125].

Yetkisiz erişim için ayrıca düzenlenen Bilgisayara Yetkisiz Erişim Kanunu oldukça ayrıntılı düzenlemelere yer vermiştir[126]. Kanun'un 1'inci maddesi Kanun'un amacına, 2'nci maddesi tanımlara, 3'üncü maddesi ise yetkisiz erişim suçuna yer vermiştir. Buna göre her yetkisiz erişim her türlü hacking faaliyeti değildir ve yalnızca telekomünikasyon ağı yoluyla başka bir bilgisayara yetkisiz erişime yönelik hareketleri suç olarak düzenlemektir[127]. Yani fiziksel olarak bilişim sistemine girilmesi bu Kanun kapsamında suç sayılmamıştır. Japon doktrini 128 sayılı ve 1999 tarihli Bilgisayara Yetkisiz Erişim Kanunu'nun birtakım yeni teknolojik gelişmeleri kapsamadığı için eleştirilmektedir[128].

Kanun'un 3'üncü maddesinin 2'nci fıkrasının 1'inci bendi, telekomünikasyon hattına bağlı ve koruma altındaki bir bilgisayara başkasına ait tanıtma kodlarıyla (kimlik veya şifre gibi) girilmesi ve bunun dışındaki bilgi ve komutlarla girilmesi suç olarak düzenlenmiştir. Kanun'un 3'üncü maddesinin 2'nci fıkrasının 2'nci bendi ise özel kullanıma sunulmuş ve başka bir korumalı bilgisayarın sınırlamalarına tabi olan korumalı bir bilgisayara yetkisiz erişimi yaptırıma bağlamıştır. Kanun'un 3'üncü

---

[123] Doktrinde İngilizce karşılığı "govermental trojan/state trojan", Almanca karşılığı ise "bundestrojaner/staatstrojaner" olarak yer almaktadır.
[124] Alman hukukunda yer alan çevrimiçi arama kurumuna ve bu konudaki tartışmalara "Hukuka Aykırılık" bölümünde detaylı olarak yer verilmiştir.
[125] Takato Natsui, "Cybercrimes in Japan: Recent Cases, Legislations, Problems And Perspectives", **Meiji Law Journal**, Vol.10, March 2003, s. 5.
[126] Kanunun İngilizce metni için bkz. Act on Prohibition of Unauthorized Computer Access, https://www.npa.go.jp/cyber/english/legislation/uca_Tentative.pdf, Erişim Tarihi:14.04.2019.
[127] **A.e.**, s.12.
[128] **A.e.**, s.15, dn. 34.

maddesinin 2'nci fıkrasının 3'üncü bendinde ise, bilgisayara yetkisiz erişim kolaylaştırılmasına yönelik hareketler yasaklanmıştır[129]. Bu hareketlerden birini gerçekleştiren kişi aynı Kanun'un 8'inci ve 9'uncu maddesinde yer alan yaptırımlar çerçevesinde cezalandırılmaktadır[130].

Bilgisayara Yetkisiz Erişim Kanunu'nda yer alan düzenlemelere bakıldığı zaman görülmektedir ki; bir bilişim sistemine direkt fiziksel erişim, herhangi bir ağa bağlı olmayan bilgisayar sistemine erişim ve koruma altına alınmamış bir bilişim sistemine erişim bu kanun kapsamında yetkisiz erişim suçunun oluşumuna engel olmaktadır.

E. Rusya

Rus ceza hukukunda bilişim suçları Rusya Federasyonu Ceza Kanunu'nun 28'inci bölümünün 272'nci maddesinde düzenlenmiştir. Bu maddeye göre, "*Bilgisayar, bilgisayar sistemleri ve ağlarında yer alan yasal olarak korunan bilgisayar verilerine, yani makinanın okunabilir ortamına ilişkin bilgilere, yasa dışı olarak erişilmesi, bu fiilin verilerin imha edilmesi, engellenmesi, değiştirilmesi veya kopyalanması veya bilgisayar, bilgisayar sistemleri veya ağlarını bozmasına sebep olması halinde*" cezalandırılmaktadır[131].

Söz konusu düzenlemeye bakıldığında "*verilerin imha edilmesi, engellenmesi, değiştirilmesi veya kopyalanması veya bilgisayar, bilgisayar sistemleri veya ağlarını bozmasına sebep olması*" seçimlik neticeler olarak düzenlenmiş, böylece bilişim sistemine girmek başlı başına bir suç tipi olarak belirlenmemiştir. Aynı maddenin ikinci fıkrasında bu suçun bir grup insan tarafından tasarlanarak veya bir örgüt tarafından işlenmesi ya da kamu görevlisi tarafından veya aynı şekilde bilgisayarlara, bilgisayar sistemlerine ve ağlara erişimi olan bir kişi tarafından ilk fıkrada yer alan suçun işlenmesi cezayı ağırlaştıran nitelikli bir hal olarak düzenlenmiştir.

---

[129] Karagülmez, **a.g.e.**, s.127.
[130] Ayrıca bkz. Takato Natsui, **a.g.m.**, s. 12-13.
[131] Maddenin İngilizce metni için bkz. The Criminal Code of the Russian Federation, Çevrimiçi, https://www.wto.org/english/thewto_e/acc_e/rus_e/WTACCRUS48_LEG_6.pdf, Erişim Tarihi: 01.03.2018.

F. İtalya

İtalyan Ceza Kanunu'nun 615ter maddesi "*Bilgisayara veya Telekomünikasyon Sistemine Yetkisiz Erişim*" şeklinde başlıklandırılmış ve kanun düzenlemesinde de bilgisayar ve telekomünikasyon sistemi ifadelerine yer vermiştir. Ancak pek çok ülkede olduğu gibi İtalyan Ceza Kanunu da bilgisayar, telekomünikasyon sistemi, veri gibi kavramların tanımlarını içinde barındırmamaktadır[132].

Kanuni düzenlemeye göre, "*Güvenlik önlemleriyle korunan bilgisayar veya telekomünikasyon sistemine yetkisiz şekilde giren yada kendisini dışarda bırakma hakkına sahip kişinin açık veya zımni iradesine karşı bilgisayar veya telekomünikasyon sisteminin içinde kalan kişi, 3 yılı aşmamak üzere hapis cezasıyla cezalandırılır*"[133].

Aynı maddenin ikinci fıkrasında ise daha ağır cezayı gerektiren nitelikli hallere yer verilmiştir. 615 ter maddesinin 2'nci fıkrasının 1'inci bendine göre yetkisiz erişimin bir kamu görevlisinin görevi kötüye kullanması veya iş ve hizmetlerle bağlantılı görevlere uymaması veya lisansı olup olmadığına bakılmaksızın profesyonel özel dedektif tarafından işlenmesi veya sistem operatörünün yetkisini kötüye kullanılarak işlenmesi halinde mahkeme 1 yıldan 5 yıla kadar hapis cezasına hükmedebilecektir. Aynı fıkranın 2'nci bendine göre fail suçu işlemek için kişilere veya mala zarar vermişse veya fail açıkça silah kullanmışsa cezanın arttırılacağı belirtilmiştir. Aynı maddenin 3'üncü bendi ise TCK'nın 243/3 fıkrasıyla benzer bir düzenlemeye yer vermiştir. Buna göre failin fiili sistemin bozulmasına veya zarar görmesine veya kısmen ya da tamamen kesintiye uğramasına veya verilerin, bilgilerin

[132] Lorenzo Picotti, "Report-Italy", Preparatory Colloquium Section II, Çevrimiçi, http://www.aidpitalia.org/docs/Verso%2019%20Congresso%20AIDP/Sect%20II%20AIDP%20-%20Italy%20Report%20Picotti.pdf, 05.03.2018, s. 3.
[133] İngilizce kanun metni için bkz. Çevrimiçi, http://www.cybercrimelaw.net/Italy.html, 05.03.2018.

ya da içindeki programların yok olmasına veya zarar görmesine sebep olursa fail 1 yıldan 5 yıla kadar hapis cezasıyla cezalandırılacaktır[134].

Son olarak İtalyan Ceza Kanunu'nun 615ter maddesinin 3'üncü fıkrasında ilk iki fıkrada yer alan fiillerin askeri çıkarlara, kamu düzenine, kamu güvenliğine veya sivil savunmaya veya herhangi bir kamu yararına karşı bilgisayar veya telekomünikasyon sistemlerine karşı işlenmesi halinde ilk fıkranın yaptırımı ağırlaştırılarak 1 yıldan 5 yıla kadar veya ikinci fıkrada yer alan yaptırım ise ağırlaştırılarak 3 yıldan 8 yıla kadar hapis cezasına olacaktır. Söz konusu fıkranın son cümlesinde ise, 1'inci fıkrada öngörülen fiilin işlendiği durumlarda suçun yargılamasının şikâyete bağlı olduğu, maddede yer alan diğer fiillerin yargılamasının ise resen yapılacağı hükme bağlanmıştır.

G. Fransa

Fransız Ceza Kanunu'nun üçüncü bölümü "*otomatik veri işletim sistemlerine yetkisiz erişim*" olarak başlıklandırılmış, bu bölümün ilk maddesi olan 323-1 maddesinde de yetkisiz erişim düzenlemesine yer verilmiştir.

Fransız Ceza Kanunu'nun 323-1 maddesinin ilk fıkrasında otomatik veri sistemlerinin tamamına veya bir kısmına hileli şekilde girmenin veya orada kalmanın 1 yıla kadar hapis cezası ve 15.000 €'ya kadar para cezasıyla cezalandırılacağı hükme bağlanmıştır. Aynı maddenin ikinci fıkrasında ise bu hileli erişimin otomatik veri işletim sistemini durdurması, sistemde yer alan verilerin değişmesine yol açılması veya sistemin işleyişinde değişikliğe yol açması hali cezayı ağırlaştıran nitelikli hal olarak düzenlenmiş ve bu suçun yaptırımı 2 yıla kadar hapis cezası ve 30.000 €'ya kadar para cezası olarak belirlenmiştir[135].

---

[134] Her ne kadar bu nitelikli hal TCK madde 243/3'le benzerlik gösterse de TCK'nın belirlediği ceza ağırlığının çok daha hafif olduğunu belirtmek gerekir. TCK madde 243/3'e göre suçu işleyen failin cezai yaptırımı 6 aydan 2 yıla kadar hapis cezası olarak belirlenmiştir.

[135] İngilizce kanun metni için bkz. Çevrimiçi, www.track.unodc.org/LegalLibrary/.../France/Laws/France%20Penal%20Code.pdf , Erişim Tarihi: 09.05.2018.

H. Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Bilişim Sistemine Girme Suçu

Ülke mevzuatlarını ortak bir noktada toplama ve uluslararası işbirliğinin sağlanmasıyla taraf ülkeler arasında ortak bir ceza hukuku politikasının ortaya konulmasını amaçlayan Avrupa Konseyi Siber Suçlar Sözleşmesi metninin taslağı 2000 yılının Nisan ayında internette yayınlanmış, 23 Kasım 2001 tarihinde ise metnin son hali Budapeşte'de imzaya sunulmuştur[136]. Avrupa Konseyi Siber Suçlar Sözleşmesi günümüze kadar elli ülke tarafından imzalanmıştır. Bilişim suçlarıyla mücadele de ülkeler arası işbirliğinin önemine binaen Sözleşmeyi imzalayan ülkeler arasında Amerika Birleşik Devletleri, Japonya, Kanada gibi Avrupa Birliği üyesi olmayan ülkeler de bulunmaktadır. Türkiye ise 10 Kasım 2010 tarihinde Strazburg'da Avrupa Konseyi Siber Suçlar Sözleşmesi'ne taraf olmuştur. 22 Nisan 2014 tarih ve 6533 sayılı "*Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanunun*" 2 Mayıs 2014 tarihinde 28988 tarihli Resmi Gazete'de yayınlanmasıyla Avrupa Konseyi Siber Suçlar Sözleşmesi iç hukukumuza dâhil edilmiştir.

Avrupa Konseyi Siber Suçlar Sözleşmesi hem maddi hukuk hem usul hukuku açısından hem de taraf devletlerarası adli yardımlaşma ve suçlunun iadesi bakımından çeşitli düzenlemelere yer vermiştir. Sözleşmenin ilk bölümünde "*kullanılan terimlere*", ikinci bölümünde "*ulusal düzeyde önlemlerin alınması*" için maddi ceza hukukuna, usul hukukuna ve yargılama hukukuna ilişkin düzenlemelere, üçüncü bölümde "*uluslararası işbirliğine*" yönelik genel ilke ve özel hükümlere yer verilmiştir.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde "*Yasadışı Erişim*" başlığı altında taraf ülkelerin "*bir bilgisayar sisteminin tamamına veya bir*

[136] Sözleşme metni için bkz. Avrupa Konseyi Siber Suçlar Sözleşmesi, Çevrimiçi, https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 198. Sözleşme hakkında genel bilgiler ve bilişim suçlarıyla mücadele hakkında ayrıca bkz. Murat Önok, "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi - Prof. Dr. Nur Centel'e Armağan**, 2013, C.9, S. 2, s.1299-1269.

kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai bir suç olarak tanımlaması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri" düzenleyeceğini kabul edeceği belirtilmiş, taraf ülkelerin mevzuatlarında "*söz konusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekar niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını*" şart koşabilmesine imkan verilmiştir. Sözleşme'nin iç hukukumuza dâhil olma aşamasında 20 Aralık 2012 tarihinde hazırlanan 1/676 Esas No'lu ve 311 Karar No'lu Türkiye Büyük Millet Meclisi Dışişleri Komisyonu Raporunda Sözleşmenin 2'nci maddesi uyarınca yasadışı erişimin şarta bağlı tutulmasının hedeflenen işbirliği alanını daraltacağı yönünde muhalefet şerhine yer verilmişse de bu madde aynen ve oy çokluğu ile kabul edilmiştir. Nitekim Hükümet'in Teklif Ettiği Metne Ekli Çekince Ve Beyanlar'ın ve Dışişleri Komisyonunun Kabul Ettiği Metne Ekli Çekince ve Beyanlar'ın ilk maddesinde Türkiye Cumhuriyeti Devleti'nin 2'nci maddesine istinaden "*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 koştuğu beyan edilmiştir.

Yasadışı erişimin sistem ve verilerin güvenliğine karşı işlenen her türlü tehdit ve saldırıyı kapsadığı belirtilmiş, bu izinsiz erişimlerin şifreler, bilgi ve belgeler dâhil birçok gizli veriye erişime ve başka suçların işlenmesine teşvik amacı taşıdığına değinilmiş ve bedel karşılığı kullanılan sistemlerin ücretsiz kullanımına yol açabileceği vurgulanmıştır[137].

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin iç hukukumuza dâhil olmasıyla TCK'nın 243'üncü maddesinde "*bilişim sistemine girme*" suçu düzenlenmiş, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde yer alan yasadışı erişim maddesine uygun bir suç tipi düzenlemesine gidilmiştir. Ancak TCK'nın 243'üncü maddesinin ilk halinde "*hukuka aykırı olarak giren ve orada kalmaya devam eden*" ifadesi doktrinde Avrupa Konseyi Siber Suçlar Sözleşmesi'ne uygun olmadığı

[137] Füsun Sokullu-Akıncı, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler Ve Özellikle İnternette Çocuk Pornografisi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, S. 59 (1-2), 2011, s.14-15.

yönünde eleştirildikten sonra 24 Mart 2016 tarihinde söz konusu ifade "*hukuka aykırı olarak giren veya orada kalmaya devam eden"* olarak değiştirilmiştir.

IV. BİLİŞİM SİSTEMİNE GİRME SUÇU İLE KORUNAN HUKUKİ DEĞER

Suç tanımında yer alan fiiller mutlaka hukuki bir değerin ihlalini oluşturmaktadır[138]. Bilişim sistemine girme suçuyla korunan hukuki değer hakkında doktrinde farklı görüşlere yer verilmiştir.

Bazı yazarlar suçla korunan hukuki değerin karma bir nitelik gösterdiğini savunmaktadır. Korunan hukuki değerin karma nitelikte olduğunu savunan yazarlar da farklı görüşlerde bulunmaktadırlar. Bilişim sisteminin güvenliğinin yanında özel hayatın dokunulmazlığı, bilişim sisteminden yararlanan kişilerin verilerinin gizliliğinin korunması, kişi ve kurumların bilişim sistemine karşı güvenlik duygusu gibi pek çok kişisel menfaatin de korunduğunu ifade eden yazarlar bulunmaktadır[139].

Başka bir görüş bilişim sistemine güveni üst bir kavram olarak değerlendirmiş ve diğer korunan değerler ayrı ayrı ele alınmıştır. Suçun düzenlendiği kısmın başlığının "*Topluma Karşı Suçlar*" olması sebebiyle ilk niteliğin toplum düzeninin korunması olduğunu belirtilmiştir[140]. Ayrıca özel hayatın gizliliği, haberleşmenin gizliliği, kullanıcıların ve sistem sahibinin menfaatleri ile başka suçların işlenmesinin önlenmesi de korunan hukuki değerler olarak incelenmiştir. Bilişim sisteminin güvenliğinden anlaşılması gerekenin teknik bir güvenlik olmadığını, toplumun maddi ve manevi bütün hayatını paylaştığı bilişim sistemine duyulan psikolojik bir güven olduğunu belirtilmiş, verilerin gizliliğinin korunmasının korunan hukuki değerler içinde yer almadığını savunulmuştur. Çünkü kanun koyucu verilerin ele geçirilmesini

---

[138] Yener Ünver, **Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer**, Ankara, Seçkin Yayıncılık, 2003, s.135.

[139] Sinan Esen, **Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar, Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2007, s.628; Parlar, **a.g.e.**, s.15. Aynı yönde bkz. Soyaslan, **a.g.e.**, s.635. Tezcan/Erdem/Önok, **a.g.e.**, 978; Gül, **a.g.e.**, s.57; Taşkın, **Bilişim Suçları**, s.22 Mahmutoğlu, **a.g.m.**, 858-859.

[140] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1370. Aynı yönde bkz. Yavuz Erdoğan, **Türk Ceza Hukuku'nda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2013, 120-123.

suçun kanuni tanımına dâhil etmemiş ve buna gerekçede de yer vermemiştir[141]. Tam tersine kanun koyucu kişisel verilerin ele geçirilmesini ayrı bir suç olarak TCK'nın 136'ıncı maddesinde düzenlemiştir[142].

Bir görüş ise korunan hukuki değerleri oldukça geniş şekilde ele almış, suçla korunan hukuki değerin özel hayatın gizliliği, kişisel ve kurumsal verilerin güvenliği, iletişim özgürlüğünün korunması, kurumların bilişim sistemine olan güveni, mülkiyet ve zilyetlik haklarının korunması, kamu düzeni ve güvenliği olduğunun altını çizmiştir. Çünkü eğitim, sağlık, ticaret, iletişim, ulaşım, hukuk gibi konularda kişiler ve toplum için bilişim sistemi çok önemli bir noktada yer almaktadır[143].

Bilişim sistemine girme suçunun kullanıcıların rahatsız edilmemesi için düzenlendiğini, bu sebeple korunan hukuki değerin bilişim sistemi kullanıcılarının menfaatleri olduğunu savunan başka bir görüşe göre[144] bedeli karşılığı kullanılan bilişim sistemlerine karşı bu suçun işlenmesini daha az ceza gerektiren bir nitelikli hal olarak düzenleyen 243'üncü maddenin 2'nci fıkrası, kanun koyucunun bilişim sisteminin güvenliğini korumak istediği düşüncesini zayıflatmaktadır[145].

Doktrindeki bir görüşe göre bu suçla korunan hukuki değerin öncelikle bilişim sisteminin güvenliği olduğu, bu sayede kişilerin verilerinin korunması, bunun yanında özel hayatın dokunulmazlığı gibi kişisel menfaatlerin de korunduğu ifade edilirken[146],

---

[141] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s. 1370-1371.
[142] **A.e.**, s.1372, dn.32.
[143] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 51.
[144] Karagülmez, **a.g.e.**, s.201. Karagülmez bilişim sistemine girme suçunun 2016 değişikliğinden önceki düzenlemesini dikkate alarak, başlı başına bilişim sistemine girmenin suç oluşturmaması gerekçesine dayanarak bu görüşü ileri sürmüştür.
Dülger ise bu görüşe eleştiri olarak, her ne kadar 2016 değişikliği öncesinde bilişim sisteminde kalma fiili bağlı hareket olarak ele alınsa da kanuni tanımda bir neticeye yer verilmediği gerekçesiyle Karagülmez'in bu görüşünü aynı sonuca ulaşsalar da gerekçe bakımından eleştirmektedir. Buna eleştirisinin yanında, Karagülmez'in "kullanıcının rahatsız olması" ifadesini de eleştirmiş, kullanıcının neyden rahatsız olduğu sorusuna yanıt verilmesi gerektiğini belirtmiştir. Dülger'e göre kullanıcı bilişim sistemine güveninin ve menfaatlerinin ihlal edilmesinden rahatsız olacaktır. Dolayısıyla "kullanıcıların rahatsız olması" bilişim sistemine güvenin korunmadığını söylemek için yeterli değildir. Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (6),** s.349.
[145] Yılmaz Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu", **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C.II, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını, s.1254.
[146] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.244. Aynı yönde bkz. Yılmaz Yazıcıoğlu, "Hackerler ve Bilişim Sistemine Girme Suçu", **Ord. Prof. Dr. Sulhi Dönmezer**

diğer görüşlerden farklı olarak başka bir görüş ise, TCK'nın TBMM Genel Kurul görüşmelerinden yola çıkarak korunan hukuki değerin kişilerin malvarlığı olduğunu, diğer hukuki değerlerin ikinci derecede korunduğunu savunmuştur[147]. Ancak tam aksine korunan hukuki değer bilişim sistemine duyulan güvendir. Kişilerin malvarlığının korunması ise ancak dolaylı bir değer olarak kabul edilebilecektir[148].

Bazı yazarlar, kanun koyucunun amacının kişilerin rahatsız edilmeksizin güven içinde bilişim sistemini kullanmasını korumak istemesi olduğunu kabul ederek korunan hukuki değerin bilişim sisteminin güvenliği ve dokunulmazlığı olduğunu belirtmiştir[149].

TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun 2016 yılından önce gerçekleşebilmesi için "*bilişim sistemine girme ve orda kalmaya devam etme*" fiillerinin birlikte aranması, doktrinde korunan hukuki değerin tespitinde farklılıklara yol açmıştır. Hatta bilişim sistemine girme ve orada kalma fiillerinin birlikte aranması ile Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde yer alan yetkisiz erişim suçunun mevzuatımızda yer almadığı sonucuna ulaşılmıştır[150]. Dolayısıyla 2016 değişikliği öncesinde yazarlar farklı gerekçelerle farklı korunan hukuki değerlere yer vermiştir. 6698 sayılı Kanun'un 30'uncu maddesi ile yapılan değişiklik ile "*ve*" bağlacı Avrupa Konseyi Siber Suçlar Sözleşmesi'nin amacına uygun olarak "*veya*" şeklinde değiştirilmiştir. Dolayısıyla bu suç tipiyle korunan

---

Armağanı, C.II, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını, s.1254.

[147] Ketizmen, **a.g.e.**, s.92. Bu görüşü savunan Yazar, 2016 değişikliği öncesinde "bilişim sistemine giren ve orda kalmaya devam eden" ifadesinin eleştirilerinden yola çıkmıştır.

[148] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.246.

[149] Akbulut, **Bilişim Alanında Suçlar**, s.118; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.807. Koca/Üzülmez'e göre, bilişim sistemine haksız olarak kasten girilmesi halinin suçun oluşması için yeterli olduğundan özel hayatın gizliliğinin veya malvarlığına yönelik hakların bu suç tipiyle korunduğu söylenemez.
Koca/Üzülmez, toplumda bilişim sistemine karşı bir güven oluştuğu, dışardan bilişim sistemlerine karşı gerçekleşebilecek hukuka aykırı ve rıza dışı bir erişimin oluşan bu güveni sarsacağından bahisle bilişim sistemine girme suçu düzenlemesine gidildiği ve ayrıca bu suçun "*Topluma Karşı Suçlar*" başlığı altında yer alması sebebiyle bu suçla korunan hukuki değerin bilişim sisteminin güvenliği ve güvenilirliği olduğuna ilişkin görüşler de bulunmaktadır. Bkz. Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.947.

[150] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (6),** s.341.

hukuki değerin ne olduğu konusunda yapılan tartışmalardaki bazı argümanlar böylece ortadan kalkmıştır.

Bu suçla korunan hukuki değerin bilişim sisteminin güvenliği ve güvenilirliği olduğunu söylemek mümkündür. Nitekim gerek 243'üncü maddenin 1'inci fıkrası gerekse Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesi bilişim sistemine kasten gerçekleştirilen haksız erişimi suçun oluşması için yeterli saymıştır. Suç tipinde ayrıca herhangi bir verinin ele geçirilmesi, öğrenilmesi gibi unsurlara yer verilmemiştir. Ayrıca özel hayatın gizliliği, haberleşmenin gizliliği gibi kişilerin menfaatlerinin korunması adına TCK'da bağımsız suç tipleri düzenlenmiştir. Dolayısıyla söz edilen bu kişilerin menfaatlerinin korunması bilişim sistemine girme suçu bakımından bilişim sisteminin güvenliği çatısı altında yer alan ikinci derecede korunan hukuki değerler olabilir. Bunun dışında, bu suçla kullanıcıların malvarlığı ve zilyetliğin korunduğuna dair görüşlere katılmak da yine aynı sebeple mümkün değildir.

Ancak fiilin sistemin içerdiği verilerin yok olması veya değişmesine sebep olmasını neticesi sebebiyle ağırlaşmış hal olarak düzenleyen 243'üncü maddenin 3'ünü fıkrası açısından bilişim sisteminin güvenliği dışında verilerin dışardan gelecek müdahalelere karşı korunduğu söylenebilir[151].

[151] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.808.

İKİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE GİRME SUÇUNUN UNSURLARI

I. SUÇUN MADDİ UNSURLAR

A. Fail

TCK'nın 243'üncü maddesinin 1'inci fıkrasında bilişim sitemine giren veya orada kalmaya devam eden kimsenin cezalandırılacağı belirtilmiştir. Kanuni tanımdan da anlaşılacağı üzere bu suç fail bakımından bir özellik arz etmemektedir ve herkes tarafından işlenebilir. Ayrıca failin bilişim sistemine girme veya orada kalma fiilini kimin için gerçekleştirdiğinin bir önemi bulunmamaktadır[1].

Bilgisayarın kullanımının yaygınlaşmadığı dönemlerde bilişim suçunu işleyen failin belirli bir düzeyin üstünde özel ve teknik bir bilgisinin olması gerektiğine dikkat çekilmiştir. Bu sebeple bazı yazarlar bilişim suçlarını "*beyaz yaka suçu*" kategorisine dâhil etmiştir[2]. Bilgisayarın yaygınlaşmasıyla ve teknik altyapı oluşturan yazılım ve donanımların artmasıyla ortalamanın üstünde bilgisayar kullanma yeteneğine sahip kişilerin de bilişim suçlarının faili olabileceği kabul edilmiştir[3]. Dolayısıyla bilişim suçlarını işleyen kişilerin belirli bir meslek grubundan olması aranmamaktadır. Bilişime ilgi duyan ve bu konuda bilgi ve yeteneklerini geliştiren herkesin bilişim sistemine hukuka aykırı şekilde kasten girebilmesi veya bilişim sisteminde kalabilmesi veya hukuka uygun şekilde girdiği bilişim sisteminde hukuka aykırı şekilde kalmaya

[1] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 52.
[2] Robert J. Sciglimpaglia, Jr., "Computer Hacking: A Global Offense", Pace International Law Review, V.3, I.1., 1991, Çevrimiçi, http://digitalcommons.pace.edu/pilr/vol3/iss1/8, 05.07.2018, s. 201, dn.1; Emin D. Aydın, **Bilişim Suçları ve Hukukuna Giriş**, s.30; Ersoy, **a.g.m.**, s. 167.
[3] Yenidünya/Değirmenci, **a.g.e.**, s.57. Taşkın, kastın varlığını tespit etmek için failin bilişim sistemleri hakkında "ortalamanın üstünde" bir bilgiye sahip olması gerektiğini belirtmiştir. Bkz. Taşkın, **Bilişim Suçları**, s.23.

devam etmesi mümkündür[4]. Bir başkasına ait bilişim sistemine ait şifreyi veya güvenlik önlemlerini bilen veya bunları nasıl aşılabileceğini bilen herkes bu suçu işleyebilir[5].

Her ne kadar bu suç herkes tarafından işlenebilir bir suç olsa da, bu suçun genellikle "*hacker*" olarak nitelendirilen kişiler tarafından işlendiği dikkat çekmektedir[6]. Hacker yani bilişim korsanları kendi içinde üç temel gruba ayrılmaktadır. Bunlar; beyaz şapkalı hackerlar, gri şapkalı hackerlar, siyah şapkalı hackerlardır. Siyah şapkalı hackerlar, sistemdeki açıkları arayan ve bu açıkları kullanarak sisteme sızan, bilgileri ele geçiren, sistemi bozan veya sisteme zarar veren kötü niyetli bilişim korsanlarıdır. Beyaz şapkalı hackerlar ise siyah şapkalı hackerları engellemek adına bilişim sisteminde bulunan açıkları tespit ederek bilgilerini istihbarat örgütlerine, devletlere veya şirketlere sunar. Gri şapkalı hacker, menfaatleri doğrultusunda hareket eden iyi veya kötü olarak nitelendirilemeyen kişilerdir[7]. Her ne kadar hacker olarak anılan bilişim korsanları kendi içerisinde bazı ayrımlara tabi tutulsa da TCK'nın 243'üncü maddesi gereğince bu ayrımlar göz önüne alınmaksızın bir bilişim sistemine hukuka aykırı olan giren veya orada kalan kişi suçun faili olarak anılabilecektir[8].

Faille ilgili olarak gündeme gelen diğer bir konu ise tüzel kişilerin fail olup olamayacağı hususudur. TCK tasarısında tüzel kişilerin ceza sorumluluğu kabul edilmişse de TBMM Adalet Komisyonu'nda bu durum değiştirilmiştir. TCK'nın 20'nci maddesi ve genel suç politikamız gereğince cezaların şahsiliği ilkesi geçerlidir ve yalnızca gerçek kişiler suçun faili olabilir. Ancak tüzel kişiler aleyhine TCK'nın 60'ıncı maddesinde yer alan güvenlik tedbirlerinin uygulanabilmesi mümkündür[9].

---

[4] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.247.
[5] Akbulut, **Bilişim Alanında Suçlar**, s.120.
[6] Özbek v.d., **a.g.e.**, s.948.
[7] Elbahadır, **a.g.e.**, s.8-9.
[8] Ali İhsan Erdağ, "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", **Doç.Dr. Mustafa Yıldız'a Armağan- Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S. 2, Aralık 2010, s. 282-283; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s.53.
[9] Tüzel kişilerin fail olup olamayacağıyla ilgili ayrıntılı bilgi için ayrıca bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku(7),** s.247-255.

Özellikle ekonomik suçlar, ticari ve sanayi casusluğunda karşılaşıldığı gibi[10], failin bilişim sistemine girme veya orada kalma fiilini tüzel kişi yararına işlemesi halinde bu güvenlik tedbirleri uygulanacaktır[11].

Bilişim suçlarında failin belirlenmesi oldukça zor olduğundan uygulamada IP numarası[12] tespit edilerek fail tespit edilmeye çalışılmaktadır. Ancak bilişim sistemine girme suçunun failinin IP numarasının kayıtlı olduğu kişi[13] olarak kabul edilmesinin objektif sorumluluk esasının benimsendiği sonucunu ortaya çıkardığını ve modern ceza hukuku, Anayasamız ve TCK bakımından hukuka aykırılık oluşturduğunu söylemek mümkündür[14].

B. Mağdur

TCK'nın 243'üncü maddesinin 1'inci fıkrasında mağdur için bir özellik belirtilmemiştir. Mağdur suçun konusunun ait olduğu kişidir. Bu suçun mağduru olan

---

[10] **A.e.,** s.255.

[11] Zafer İçer, "Türk Ceza Hukukunda Tüzel Kişiler", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2011, s.130; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s.52; Apaydın, **Bilişim Sistemine Girme Suçu**, s. 259; Yavuz Erdoğan, **Türk Ceza Hukuku'nda Bilişim Suçları**, s.176.

[12] IP, kişilerin internete bağlanmasına yani bilişim sistemleri arasında veri aktarımının sağlanabilmesine imkân veren ve internete bağlanan her bilişim sisteminde farklılık gösteren adresi tanımlayan numaralar bütünü olarak ifade edilebilir. Bkz. Abdurrahman Savaş, **İnternet Ortamında Yapılan Sözleşmeler**, Konya, Adal Ofset, 2005, s.18.

[13] "E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikâyeti üzerine öncelikle erişimi engellenen adresin şikâyetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adresin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. Microsft Corporation'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde e-mail adresine giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdür lüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli ve loglar üzerinde inceleme yapılmalıdır.
Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikâyetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.
Şikâyetçiye ait e-mail adresine veya ele geçirilen adresten başkalarına, görüntü, yazı veya ses kaydı gönderildiğinin iddia olunması halinde ise, bu husus/hususlar üzerinde durularak gerekli tespitler yapılıp örnekleri de alınarak dosya içine konulmalıdır.
Şikâyetçi ve şüphelilerin bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak görüntü ve yazı ile ulaşılan adres sahipleri tanık olarak dinlenmelidir." 8. CD., E. 2013/10401 K. 2014/11835 T. 7.5.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi: 4.4.2019.

[14] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s.53.

kişinin bilişim sistemi üzerinde hak sahibi olması, yani bilişim sistemini doğrudan kullanabilmesi ve bunun için yetkisinin olması gerekmektedir[15]. Bilişim sistemi üzerinde hak sahibi olan kişi sistemin sahibi olabileceği gibi kullanıcısı da olabilir[16]. Bilişim sistemine girilen veya bilişim sisteminde kalınmasından dolayı hakları tehlikeye giren kişi bu suçun mağdurudur[17]. Doktrinde bu suçun mağdurunun kimlerin olabileceğiyle ilgili çeşitli görüşler bulunmaktadır.

Bazı yazarlar suçun mağdurunun gerçek kişilerin yanında tüzel kişilerin de olabileceğini ileri sürmüşlerdir[18]. Suçla korunan hukuki değerin bilişim sisteminin güvenilirliği olduğundan yola çıkan görüşe göre, bilişim sistemlerinin sahibi genellikle tüzel kişiler olduğu için tüzel kişilerin de bu suçun mağduru olabilmesi gerekmektedir[19].

Bazı yazarlar ise, bu suçla korunan hukuki değerin bilişim sisteminin güvenliği olduğundan yola çıkarak bu suçun mağdurunun belirli bir kişi olamayacağını ileri sürmektedir[20].

Bazı yazarlar bu suçun mağdurunun yalnızca gerçek kişiler olabileceğini savunmaktadır. Tüzel kişiler ise yalnızca bu suçtan zarar gören olabilecektir[21]. Türk ceza hukuku sistemi ve suç politikası gereğince yalnızca gerçek kişiler suçun mağduru olabilecektir. Aksi yönde bir kabul, tüm dayanaklara rağmen Türk ceza hukuku sistemiyle ters düşecektir. Sonuç olarak tüzel kişiler doğrudan veya dolaylı olarak

---

[15] Özbek v.d., **a.g.e.**, s.948; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.809.
[16] Akbulut, **Bilişim Alanında Suçlar**, s.121.
[17] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1394; Akbulut, **Bilişim Alanında Suçlar**, s.121; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s.53. Bazı yazarlar mağdurun bilişim sistemine girilen veya bilişim sisteminde kalınmasından dolayı hakları zarara uğrayan kişi olduğu yönünde bir tanım yapmıştır. Ancak bu suç bir zarar suçu olarak düzenlenmediği için hakları zarara uğrayan kişi ifadesi doğru olmadığını söylemek mümkündür. Bkz. Yılmaz, **a.g.e.**, s.182; Soyaslan, **a.g.e.**, s.636.
[18] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1393; Soyaslan, **a.g.e.**, s.636; Yılmaz, **a.g.e.**, s.182.
[19] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1394.
[20] Tezcan/Erdem/Önok, **a.g.e.**, 979.
[21] Mahmutoğlu, **a.g.m.**, s.860; Apaydın, **Bilişim Sistemine Girme Suçu**, s. 260.

zarar görse de suçtan zarar gören olarak kabul edilecek ve böylece davaya katılma hakkına sahip olacaklardır[22].

Mağdur ile ilgili diğer bir konu ise, bilişim sisteminde yer alan üçüncü kişilere ait veriler olması durumunda verilerin sahibi olan üçüncü kişilerin mağdur olarak sayılıp sayılmayacağı hususudur. Bazı yazarlar, bilişim sisteminde verileri olan kişilerin de hakları ihlal edildiğinden yola çıkarak hem bilişim sistemi sahibinin hem de verilerin ait olduğu üçüncü kişilerin mağdur olabileceğini savunmaktadır[23].

Suçla korunan hukuki değer bilişim sisteminin güvenilirliği olduğundan yalnızca bilişim sistemi üstünde hak sahibi olan kişiler mağdur olabilir[24]. Verilerin ele geçirilmesi bilişim sistemine girme suçunun unsuru değildir. Nitekim verilerin sahibi olan kişilerin hakları kişisel verilerin ele geçirilmesini düzenleyen TCK'nın 136'ıncı maddesiyle korunmaktadır[25].

C. Suçun Konusu

Bilişim sistemine girme suçunun konusu doktrinde doğrudan bilişim sistemi olarak değerlendirilse de[26], TCK'nın 243'üncü maddesinin bilişim sistemine girme suçunu düzenleyen fıkraların tamamı dikkate alınarak suçun konusunun ayrı ayrı incelenmesi gerekmektedir.

TCK'nın 243'üncü maddenin 1'inci fıkrasına göre suçun konusu hukuka aykırı olarak bütününe veya bir kısmına girilen veya içinde kalınan bilişim sistemidir. Suçun nitelikli halinin düzenlendiği söz konusu maddenin 2'nci fıkrasında ise, "*bedeli karşılığı yararlanılabilen sistemler*" suçun konusunu oluşturmaktadır. Maddenin

---

[22] Ayrıntılı bilgi için bkz. Gülfem Pamuk, "Türk ve Fransız Ceza Muhakemesi Hukukunda Mağdurum Makam Olarak Yeri", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlamamış Doktora Tezi**, İstanbul, 2012, s.181 vd.

[23] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1394-1395; Apaydın, **Bilişim Sistemine Girme Suçu**, s. 260. Gül, bu kişilerin hem 243'üncü madde hem de 135 ve136'ıcı maddeler bakımından mağdur olacağını belirtmiştir. Bu hususlar ayrıntılı olarak içtima bölümünde incelenecektir. Gül, **a.g.e.**, s.58.

[24] Akbulut, **Bilişim Alanında Suçlar**, s.122.

[25] **A.e.**

[26] Tezcan/Erdem/Önok, **a.g.e.**, 978; Akbulut, **Bilişim Alanında Suçlar**, s.122.

3'üncü fıkrasında yer alan neticesi sebebiyle ağırlaşmış suçun konusu ise "*sistemin içerdiği verilerdir*"[27].

Bilişim sistemi[28], insanların verileri otomatik olarak toplamak, süzmek, işlemek, oluşturmak, depolamak ve dağıtmak gibi aritmetik ve mantıksal işlemler için kullandığı sistem olarak tanımlanabilir[29]. Bir bilişim sistemi üç teknik tamamlayıcı unsurdan oluşmaktadır. Bunlar donanım, yazılım ve veridir[30]. Donanım bilişim sisteminin fiziksel tamamlayanlarını oluştururken, yazılım ise soyut bir kavramdır. Yazılım, donanımları kullanılabilir kılan işletim sistemleri (örneğin Microsoft Windows, Google Android) ve uygulama yazılımları (örneğin Microsoft Office programları, oyunlar gibi) olmak üzere iki ana gruba ayrılmaktadır[31]. Bilişim sistemlerinin üç temel faaliyeti vardır. Bunlar girdi, işleme ve çıktı şeklinde adlandırılmaktadır[32]. Bir bilişim sistemi, verileri elde ederek sisteme uygun hale getiren girdi faaliyetinin ardından verileri işleyerek bilgiye dönüştürür ve çıktı faaliyetiyle sonuçlarını insanlar tarafından anlaşılabilir hale getirir[33].

Bilişim sistemi, bilgisayardan daha geniş ve üst bir kavramdır. Örneğin bilgisayarların dışında WAP uyumlu cep telefonları[34], yapay zekâ sistemlerinin de

---

[27] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1395; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 54.

[28] 765 sayılı TCK'nın bilişim suçlarına ilişkin maddelerinde suçun konusu olan "bilgileri otomatik işleme tabi tutan sistem" ifadesi ile bilişim sistemi ifadesin karşılaştırmasına ve bilişim sistemi kavramı için doktrinde oldukça tanımlara Bölüm I'de yer verildiği için ayrıca bu kısımda incelenmemiştir.

[29] Bilişim sistemi ile ilgili tanımlara ayrıntılı olarak Bölüm I'de yer verilmiştir.

[30] Dave Bourgeois/ David T. Bourgeois, "What Is an Information System?", **Information Systems for Business and Beyond,** Çevrimiçi, https://bus206.pressbooks.com, 07.07.2018.

[31] **A.e.**

[32] Girdi, çıktı birimleri dışında girdiden sonra verileri ve bilgileri tutan ana hafıza birimi, ana hafızayı destekleyen ve büyük miktarda verileri ve komutları saklamaya yarayan ikincil hafıza birimi, her komutun girdi, çıktı, aritmetik mantık birimi veya saklanmasıyla ilgilenen kontrol birimi ve komutlar üzerine kurulan hesaplamaları ve karşılaştırmaları yürüten aritmetik mantık birimi olarak daha detaylı ele almak da mümkündür. Levent Şenyay, "Bilgisayar Programlama", Çevrimiçi, http://kisi.deu.edu.tr//levent.senyay/bilgisayarprogramlama/1_%20Bilg%20prog%20giris.pdf , Erişim Tarihi: 07.07.2018, s.12.

[33] **A.e.**, s.2.

[34] "Bilgisayarın çalışmasını düzenleyen tüm programlara işletim sistemi denilmekte olup işletim sistemlerinin sadece bilgisayarlarda değil cep telefonlarında, tablet PC'lerde de kullanılması mümkündür. İşletim sistemleri Windows 8, Android, Linux gibi isimler almaktadır.
Bir bilgisayarın işleyişi ve özellikle de verimliliği, işletim sistemi ile ilgilidir. İşletim sisteminin ana görevi, bilgisayarın çalışması için gerekli komutları vermek ve işlevleri sağlamaktır. Donanım ile yazılım arasındaki bağlantıyı sağlayan işletim sistemi çalışmadığı takdirde bilgisayarın kullanılması,

kullanıldığı ve "*Nesnelerin İnterneti*" (IoT) olarak anılan ve hızla gelişmekte olan akıllı cihazlar bilişim sistemi çatısı altında yer almaktadır. Sürekli gelişen teknoloji bilişim sisteminin tam bir tanımının yapılmasını ve sınırlarının çizilmesini zorlaştırmaktadır.

Dolayısıyla bilişim sisteminin özelliklerini dikkate alarak bir cihazın bilişim sistemine sahip olup olmadığını değerlendirmek gerekmektedir. Uygulamada bilişim sisteminin tespitinde zorluk yaşanması halinde yargı merciinin bilişim bilim dalı üzerine uzman bilirkişilerden yardım alınması gerekmektedir[35].

Yargıtay bilgisayarın bir kısım özelliklerine sahip olan cihazları veya tek amaçlı çalışan bilgisayar destekli cihazları ve atanmış bilgisayarı[36] bilişim sistemi kapsamı içine dâhil etmemektedir. Yargıtay bir aracın bilişim sistemine sahip olup olmadığını genel kullanılabilme özelliğine ve teknik özelliklerine bakarak tespit etmektedir[37].

---

program yüklenmesi olanaksızdır." 8. CD., E. 2014/30037 K. 2015/14023 T. 18.3.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi: 4.4.2019.

[35] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1364-1365, dn.1.

[36] "Atanmış bilgisayarlar, belirli bir görevi gerçekleştirmek üzere, üzerinde sınırlı sayıda bileşene ve bireysel bilgisayarlara oranla düşük işlemci gücüne sahip, boyutça küçük bilgisayarlardır." Mustafa Haluk Akgündüz, Eşref Adalı, "Atanmış Sistemler ile Bilgisayar Kümesi Tasarımı ve Mevcut Sistemler ile Karşılaştırması", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi**, C. 8, S. 2, 2015, s.18.

[37] "Teknik olarak bilgisayar belleğindeki programa uygun olarak aritmetik ve mantıksal işlemleri yapabilen, karar verebilen, yürüteceği programı ve işleyeceği verileri ezberinde tutabilen, çevresi ile etkileşimde bulunabilen araçtır. Diğer bir ifade ile bilişim özelliğine sahip bilgisayar yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen, bilgiyi işleyebilen, saklayabilen, organize edebilen, değerlendirebilen, aktarabilen, kullanabilen, iletebilen, değiştirebilen ve ilave yapabilen bir araçtır. Bilişim özelliğine sahip bilgisayarı diğer aygıtlardan ayıran özellik de budur: Genel kullanabilme özelliğine sahip bir araç olmasıdır. Diğer bir ifade ile bilgisayarın dışında veya bilgisayar destekli yahut bilgisayar benzeri araçlar da bilginin otomatik işlenmesine yönelik olarak çalışabilir, ancak bunlar ile bir veya birkaç amaçlı işlem yapılabilir yoksa bilgisayar gibi bilişim alanının tamamını kapsayıcı nitelikte işlemler değil, yani atanmış bilgisayarlar bilişim özelliğine sahip araç değildirler: Örneğin, elektronik hesap, makineleri, TVler, çamaşır makineleri, diyaliz makineleri, röntgen cihazları, decoderler, hatta dalış bilgisayarları, arabaların yol bilgisayarları vs. bilişim alanında alanın temelini bilgisayarlar oluşturmaktadır.
Her ne kadar çoğunlukla "bilişim" ile "bilgisayar" terimleri aynı anlamda kullanılmaktaysa da gerçekte bunlar aynı şey demek değildir.
Zira, "bilişim" sözcüğü "bilgisayar" kelimesine oranla daha geniş kapsamlıdır. Bilgisayar, (kompütür, elektronik beyin) aritmetik ve mantık işlemi dizileriyle oluşturulmuş programlara göre verileri (bilgileri) otomatik işleme tabi tutan sistemlere verilen ortak isim iken, bilişim (enformatik) ise, bilgisayardan da faydalanılmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale

TCK'nın 243'üncü maddesinin 1'inci fıkrası uyarınca bilişim sisteminin bütününün yanı sıra bilişim sisteminin bir kısmı[38] da suçun konusunu oluşturmaktadır. Bilişim sisteminin tamamından anlaşılması gereken bilişim sisteminin doğrudan kendisidir. Bilişim sisteminin bir kısmından anlaşılması gereken şey ise bilişim sisteminin ayrılmaz parçaları veya bilişim sistemini tamamlayan parçalarıdır. Dolayısıyla bilişim sisteminin tamamlayanlarından olan donanım, yazılım ile verilere girilmesi veya orada kalınması suçun oluşumuna sebebiyet verecektir[39]. Bilişim sistemleri fonksiyonlarını veriler üzerinden yürütmektedir. Bu sebeple bilişim sisteminin bir kısmına ifadesinden bilişim sistemini oluşturan donanım ve yazılımların yanı sıra bilişim sistemini tamamlayan ve içinde veri bulundurmaya müsait USB, taşınabilir bellek gibi araçlar da anlaşılmalıdır[40,41].

---

gelmesine konu olan akademik ve mesleki disipline verilen addır; yani başka bir deyişle, bilgisayar kullanma ilmidir.
Bir faaliyetin bilişim faaliyeti olup olmadığını tarif edebilmek için, o faaliyetin bilgisayar sistemine dahil olup olmadığına bakmak gerekir. Daha açık bir ifadeyle şu sorunun cevabı verilmek gerekir. Faaliyet bilgisayar sistemiyle mi temellenmektedir; yoksa bilgisayar o faaliyetin gerçekleşmesine yardımcı bir unsur olarak mı kullanılmaktadır? Yani bilgisayar destekli midir? Bankaların ATM uygulaması bilgisayar destekli olduğu için bilişim faaliyetidir. Zira bu sistem herhangi bir nedenle çöktüğünde bu faaliyet de asla gerçekleşmez. Bunun karşıtı bir örnek verilecek olursa, uçak firmalarının bilet satışlarında bilgisayar sistemlerinden yararlanmaları yani faaliyetin bilgisayar destekli olması bir bilişim faaliyeti değildir. Çünkü bu sistemler bu firmaların faaliyetini kolaylaştırmakla hızlandırmakla ve daha verimli kılmakla birlikte faaliyetin tarif edici unsuru değildir." YCGK E. 2007/6-13, K. 2007/150, T. 19.06.2007, Çevrimiçi, lexpera.com.tr , Erişim Tarihi: 08.07.2018.
Aynı yönde görüşler için bkz. Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.811; Yenidünya/Değirmenci, **a.g.e.**, s.31; Akbulut, **Bilişim Alanında Suçlar**, s.126.

[38] Erdağ, bilişim sisteme girme suçunun temel şeklini açıklarken bilişim sisteminin tamamına veya "donanım, bileşenler, dizinler, içerikle ilgili veriler gibi" sadece bir kısmına hukuka aykırı olarak girmek ve orada kalmanın suç olacağını ifade etmiştir. Böylece bilişim sisteminin bir kısmından ne anlaşılması gerektiğine örnek kabilinden açıklama getirmiştir. Erdağ, **a.g.e.**, s. 282.

[39] Aynı yönde Bkz. Akbulut, **Bilişim Alanında Suçlar**, s.126; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 54; Karakehya, **a.g.e.**, s.15.

[40] Özge Apiş, " Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri", **Yasama Dergisi Kamu Yönetiminde Teknoloji Özel Sayısı II**, C.12, S.37, Haziran 2018, s. 61; Akbulut, **Bilişim Alanında Suçlar**, s.126. Aksi görüş için bkz. Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.817.

[41] İçinde veri bulundurmaya müsait donanımların bilişim sisteminin bir kısmı sayılabilmesi ait olduğu bilişim sistemine takılı olmasını aramak gerekir. Faili mağdura ait USB, taşınabilir bellek gibi donanımları kendi bilişim sistemine takarak çalıştırması ve içindeki verilere ulaşılması halinde 5237 sayılı TCK kapsamında özel hayatın gizliliğini ihlal, verileri hukuka aykırı olarak verme veya ele geçirme suçu gibi somut olaya göre farklı suçlar gündeme gelebilecektir.

Bunun dışında belirtmek gerekir ki, yalnızca bir donanıma bağlı olmamakla birlikte başka donanımlar tarafından da erişilebilme özelliği olan e-posta, sosyal medya hesapları, bulut bilişim sistemleri[42] gibi yazılımlar[43] da bu kapsamda suçun konusunu oluşturmaktadır[44].

---

[42] Bulut bilişim sistemleri, esnek ve dinamik şekilde ölçeklendirilebilen ve büyük ölçüde sanallaştırılmış kaynakların internet üzerinden sunduğu bir imkandır. Bulut bilişim sistemlerine dünyanın hemen hemen her yerinden erişim mümkündür. Ayrıntılı bilgi için bkz. Metin Turan, **Bilişim Hukuku**, Ankara, Seçkin Yayıncılık, 2016, s.224 vd.

[43] Turan, **a.g.e**., s.112,237,252; Mine Kaya, **Elektronik Ortamda (Elektronik Haberleşme-İnternet-Sosyal Medya) Kişilik Haklarının Korunması**, Ankara, Seçkin Yayıncılık, 2015, s.192.

[44] E-posta ve sosyal medya hesaplarının bilişim sistemine girme suçunun konusunu oluşturduğu hususunda bkz. "Şikayetçiye ait hesaba izni ve bilgisi olmaksızın erişim sağlandığının tespit edildiğinden bahisle açılan davada, sanığın suçlamayı kabul etmediği, şikayetçinin bir kaç kez Facebook hesabının hacklenmesi nedeniyle yardım istediğini, bu nedenle mail adresine girdiğini, şifre değişikliği yapmadığını savunması, şikayetçinin, suç tarihinde sanıktan böyle bir talebi olmadığını ve Cumhuriyet Savcılığı'nda alınan "benim adıma kayıtlı ....@windowslive.com isimli mail adresim vardır, bu mail adresimle yaklaşık olarak 9 aydır kullandığım Facebook profilim vardır, 10.08.2011 tarihinde bu Facebook profilim şifresi kırılarak ele geçirilmiştir, bu profili Facebook sitesi üzerinden geri alabilmek için .... isimli yeni bir mail hesabı aldım, bu mail hesabı ile Facebook şifre alma yönlendirmelerini yerine getirdim, daha önce Facebook profilimin şifresinin kırıldığını fark ettiğimde hesabı kilitlemiştim, bu sebepten ele geçirilen Facebook profilimi geri almak için Facebook yönlendirmeleri esnasında bana sorduğu bilgileri doğru bir şekilde cevapladım, en son olarak bana kimliğimin renkli bir fotokopisini taratarak sistemden göndermemi istediler, bunu da yaptım ve kimlik fotokopimi gönderdim, buna rağmen Facebook sitesi bana ele geçirilen profili geri vermedi, bu güne kadar da herhangi bir dönüşte yapılmadı, benden hesabımı geri almak için kimlik bilgilerimi talep eden sitenin bir dolandırıcılık sitesi, Facebook sitesi görünümünde farklı bir site olabileceğini düşünüyorum, bu sebepten dolayı da kimlik bilgilerim benim bilgim dışında kullanılması halinde bir sorumluluk kabul etmiyorum, ben sadece bana ait olan ve şifresi kırılarak ele geçirilen Facebook profilimi geri almak için bu bilgileri ve kimlik bilgilerimi ilgili site ile paylaştım." şeklindeki beyanı, M.'tan gelen cevapta, şikayetçinin mail adresine sanık tarafından birden çok giriş yapıldığı belirlenmişse de şifre değiştirilerek şikayetçinin girişinin engellendiğine dair tespitin bulunmadığının ve şikayetçinin suç tarihi itibariyle girişe onay vermediğinin anlaşılması karşısında; şikayetçiye ait e-mail adresine izinsiz girip orada kalma şeklindeki eylemin TCK'nın 243. maddesi kapsamındaki suçu oluşturacağı gözetilmeden yazılı şekilde karar verilmesi" 8. CD. E. 2015/10534, K. 2016/7574, T. 08.06.2016. Karar için bkz. Ümit Erdem, Çağrı Şükrü Uluslu, Gökberk Dumancı, **Yargıtay (2014-2016) Kararlarında Sosyal Medya**, İstanbul, Legal Yayıncılık, 2016, s.146.

Mağdura ait sosyal medya hesabına girilmesi ile mağdura ait verilerle bir sosyal medya hesabı açılıp mağdura aitmiş gibi kullanmak aynı suçun oluşumuna sebebiyet vermez. Bilişim sistemine girme suçunun oluşabilmesi için sosyal medya hesabının mağdura ait olması ve onun tarafından kullanılıyor olması gerekir. "Sanığın, internette facebook sosyal paylaşım sitesinde, katılan adına profil hesabı oluşturup, katılanın resmini ve telefonunu koyarak başka şahıslar tarafından rahatsız edilmesine neden olduğunun ileri sürülmesine göre; eylemin kişilerin huzur ve sükununu bozma suçu yanında TCK'nın 136/1. maddesine uyan suçu oluşturacağı ve davaya bakmanın ve delilleri takdir etmenin üst Asliye Ceza Mahkemesine ait olacağı gözetilerek, görevsizlik kararı verilmesi gerekirken, duruşmaya devamla yazılı gerekçe ile beraat hükmü kurulması, Kabule göre de; Hükmün gerekçe kısmında, sanığın, katılanın isim ve telefon numaralarını kullanmak suretiyle katılan adına facebookta profil hesabı açarak, bu profilden katılan imiş gibi katılanın iş arkadaşı olan tanıkların ve üçüncü kişilerin sayfalarına eklenerek bu kişilere arkadaşlık teklifinde bulunduğu, uygunsuz görüşmeler yaptığı, bu suretle katılanın huzur ve sükununu bozarak atılı kişilerin huzur ve sükununu bozmak suçunu işlediği açıklandıktan sonra, sanığın, katılan adına facebook profil hesabı oluşturarak katılanın resmini ve telefonunu koyması

Mukayeseli hukukta yetkisiz erişim suçu düzenlemelerinde suçun konusu için bazı özelliklere yer verilmiştir. Örneğin Amerika Birleşik Devletleri'nde yetkisiz erişimi düzenleyen kanun olan 18 U.S. Code § 1030 (CFAA); devlet bilgileri, finansal kayıtlara ilişkin bilgiler, korumalı bilgisayarlarda yer alan bilgileri içeren bilgisayarlar gibi suçun konusu bakımından birtakım spesifik sınırlamalara gitmiştir. Japonya'da ise telekomünikasyon hattına bağlı ve korumalı bilgisayarların yetkisiz erişim suçunun konusu olabileceği belirtilmiştir. Başka bir örnek ise İtalya'da suçun konusunun güvenlik önlemleriyle korunan bilgisayarlar ve telekomünikasyon sistemleri olarak belirlenmesidir.

TCK'nın 243'üncü maddesinin 1'inci fıkrası konu bakımından bir sınırlamaya gitmemiştir. Bu sebeple kişisel bilişim sistemleri ve kamu kurumuna ait bilişim sistemleri bu suçun konusunu olabileceği gibi[45], bu bilişim sistemlerinin güvenlik önlemleriyle korunması da aranmamıştır. Bilişim sistemi üzerinde hak sahibi olan kişilerin bilişim sistemine erişilmesini engellemek adına özel önlemler almasının suça ve suçun yaptırımına etkisinin olup olmayacağı hususu doktrinde tartışılmıştır. Dülger, TCK'nın 141 ve 142'nci maddelerini örnek vererek kilitlenerek muhafaza altına alınan eşyanın çalınmasının cezayı ağırlaştıran nitelikli bir hal olarak düzenlendiğine dikkat çekmiştir. Yazar bu sebeple bilişim sistemine girilmesini önlemek amacıyla özel önlemler alan mağdurun bilişim sistemine girilmesi halinin cezayı ağırlaştıran nitelikli hal olarak düzenlenmesi gerektiğini savunmaktadır[46].

Öte yandan suçun konusu bakımından nitelik farkı olması sebebiyle kamu kurumlarına ait bilişim sistemlerinin önemi dikkate alınmalı ve özel bilişim sistemlerine göre daha fazla korunarak kamu kurumlarına karşı işlenen bilişim sistemine girme suçu cezayı ağırlaştıran bir nitelikli hal olarak düzenlenmelidir[47].

TCK'nın 243'üncü maddesinin 2'nci fıkrasında suçun konusu olarak "*bedeli karşılığı yararlanılabilen sistemler*" ifadesine yer verilmişse de söz konusu maddede

---

eylemi nedeniyle, bilişim sistemine girme suçundan açılan davada, atılı suç sabit olmadığından sanığın beraatine karar verildiği belirtilmek suretiyle gerekçenin karıştırılması" hukuka aykırıdır. 12. CD., E. 2014/11391 K. 2015/582 T. 19.1.2015, lexpera.com.tr, Erişim Tarihi: 3.4.2019.

[45] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1396.

[46] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (6),** s.360.

[47] Karagülmez, **a.g.e.**, s.206.

veya madde gerekçesinde bir tanıma yer verilmediği için bu ifadeden ne anlaşılması gerektiği açık değildir. Bedeli karşılığı yararlanılabilen sistemlerden ücret karşılığı hizmet veren web siteleri, belirli bir bedel karşılığı bilişim sistemlerinin kullanılması için mekânsal anlamda hizmet veren yerler (örneğin internet kafe, Playstation kafe, diğer konsol oyunlarının oynatıldığı mekânlar vb.), kuruluşlar tarafından belirli bir bedel karşılığı sunulan sistemler, belirli bir süre için sunulan internet bağlantısı servisi akla gelen ilk örneklerdir[48]. Doktrinde sadece ön ödemeli bilişim sistemlerinin değil, özellikle bulut bilişim sistemlerinde söz konusu olan "*kullandığın kadar öde*" sistemi sunan ve ödemenin sonradan gerçekleştirildiği bilişim sistemlerinin de bedeli karşılığı yararlanılabilen sistemler içinde yer aldığı belirtilmiştir[49].

Doktrinde belirli bir bedel karşılığı bilişim sistemlerinin kullanılması için mekânsal anlamda hizmet veren internet kafe gibi yerlerin sunduğu hizmetlerin 243/2'nci madde kapsamına girip girmediği tartışmalıdır. Bir görüşe göre, mekânsal anlamda hizmet veren internet kafe gibi yerler sunduğu bilişim sistemi hizmetleri için değil, mekân için bedel talep etmektedir. Dolayısıyla burada bilişim sisteminin bedeli karşılığı kullandırılması söz konusu olmadığından bu sistemlere karşı işlenen suç 2'nci fıkra kapsamına girmeyecektir[50] ve böyle bir durumda diğer koşullar oluşmuşsa TCK'nın karşılıksız yararlanmayı düzenleyen 163/2'nci fıkrası uygulanabilecektir[51]. Bu görüşün diğer bir dayanağı ise, burada suçu oluşturan fiilin bilişim sistemine girme veya orada kalmayı değil, sistemi kullanmayı içermesidir[52]. Başka bir görüş ise bu mekânların bu işi ticari kaygılarla yaptığı ve bilişim sistemlerini belirli bir süre için kiraladıklarını, dolayısıyla bedeli ödenmeksizin bu mekânlarda internet, oyun gibi hizmetlerden faydalanılmasının 243/2'nci madde kapsamında yer aldığının kabul edilmesi gerekmektedir[53]. Başka bir görüşe göre ise, karşılıksız yararlanma suçunun konusunu oluşturan otomatlar da TCK'nın 243'üncü maddesinin 2'nci fıkrasında yer

[48] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.268.
[49] Turan, **a.g.e.**, s.238.
[50] Karagülmez, **a.g.e.**, s.210.
[51] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1399; Parlar, **a.g.e.**, s.19.
[52] Karagülmez, **a.g.e.**, s.210.
[53] Yaşar/Gökcan/Artuç, **a.g.e.**, s.7299; Ketizmen, **a.g.e**., s.111; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.268-269; Mahmutoğlu, **a.g.m.**, s.863.

alan suçun değil, 163'üncü maddesinde yer alan suçun oluşmasına sebebiyet verecektir[54].

Söz konusu mekânlarda verilen hizmet, bilişim sistemlerinin kullanılmasına yönelik bir özel hukuk sözleşmesi niteliğinde kabul edilmelidir. Kişiler ödedikleri bedel karşılığında bilgisayar, oyun konsolu gibi cihazları kullanma hakkına sahip olmaktadır. TCK'nın 163'üncü maddesinde yer alan "*otomat*" kelimesi "*canlı bir varlığın yapabileceği bazı işleri yapan mekanik veya elektrikli araç*" olarak tanımlanmaktadır[55]. Dolayısıyla teknik anlamda daha kapsamlı olan bilişim sisteminin aynı zamanda otomatın şartlarını sağladığı da kabul edilebilir. Bu sebeple bilgisayar, oyun konsolu gibi bilişim sistemlerinin bedeli ödenmeksizin kullanılması söz konusu olduğu olaylarda hem karşılıksız yararlanma suçu hem de bilişim sistemine girme suçu oluşabilir. Bu durumda da farklı neviden fikri içtimaya ilişkin kuralların uygulanması gerekebilir.

Şifreli yayınların bilişim sistemine girme suçunun konusunu oluşturup oluşturmayacağı hususu da tartışma konusu olmuştur. Şifreli yayınların bedeli ödenmeksizin izlenmesinin bilişim sistemine girme suçunu mu yoksa karşılıksız yararlanma suçunu mu oluşturduğu konusunda değerlendirmeler yapılmıştır[56]. Doktrinde bilişim sistemleri aracılığıyla şifreli yayın sahibinin veya kullanıcısının rızasına aykırı olarak kaçak şekilde kullanılmasının karşılıksız yararlanma suçu

---

[54] Gül, **a.g.e.**, s.64; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1398; Tunç Demircan, **Bilişim Alanında Suçlar**, İstanbul, Legal Yayıncılık, 2016, s.79.

[55] TDK, Çevrimiçi, tdk.gov.tr, Erişim Tarihi: 23.04.2019.

[56] 765 sayılı TCK döneminde bu fiilin 525/b-2 maddesindeki suçu ihlal edip etmediği tartışmalarının yanında şifreli yayın yapan cihazların bilişim sistemi içerisinde yer alıp almadığı tartışılmıştır. Gerek Yargıtay Kararlarında gerekse doktrinde o günün teknolojisi baz alınarak bu cihazların telefon hatları veya frekanslarıyla veya elektromanyetik dalgalarla çalışan cihazlar olduğu, dolayısıyla bilişim sistemi kavramı içinde yer alamayacağı sonucuna ulaşılmıştır. Nitekim 5237 sayılı TCK'nın karşılıksız yararlanma suçunu düzenleyen 163'üncü maddesinin 2'nci fıkrasında "telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişinin" cezalandırılacağı hükme bağlanmıştır.
Bkz. Apaydın, **Bilişim Sistemine Girme Suçu**, s. 261; Karakehya, **a.g.e.**, s. 10. Karakehya karşılıksız yararlanma suçuna ilişkin özel düzenleme olduğu gerekçesiyle 243'üncü maddenin 2'nci maddesi kapsamında cezai sorumluluğun doğmayacağını savunmaktadır. Karşılıksız yararlanma suçu için ayrıca bkz. Zahit Yılmaz, Özge Apiş, "Karşılıksız Yararlanma Sucu (TCK m.163)", **Marmara Üniversitesi Hukuk Fakiltesi Hukuk Araştırmaları Dergisi Özel Sayı: Prof. Dr. Nur Centel'e Armağan**, İstanbul, C.19, S.2.,2013, s. 1759 vd.

kapsamında değerlendirilmesi gerektiğini savunan yazarlar bulunmakta ise de[57], günümüz teknolojisi dikkate alındığında internet temelinde çalışan televizyonlar ve bilişim sistemleri üzerinden yapılan şifreli yayınlardan bedeli ödenmeksizin kaçak olarak yararlanmanın bedeli karşılığı yararlanılabilen bilişim sistemine girme veya bu bilişim sistemlerinde kalma suçunun da unsurlarını oluşturduğunu dikkate almak gerekir. Bu kapsamda failin TCK'nın 243'üncü maddesinin 2'nci fıkrasından da sorumlu tutulabileceği kabul edilmelidir[58].

Yargıtay ise şifreli yayınlarla ilgili karşılıksız yararlanma suçunun oluştuğu yönünde karar vermektedir. Yargıtay 19. Ceza Dairesi'nin bir kararına göre; "*Sanıkların yöneticisi olduğu "p2pfutbol.net" isimli internet sitesi üzerinden, şifreli ve bedelli olarak yayınlanan Turkcell Süper Lig maçlarını telif hakkı almadan Lig Tv logosu dahi değiştirilmeden mediaplayer programı aracılığıyla yayınlanması, yayınları izlemek isteyenler için üyelik sistemi kurulması, üye olmak isteyenlerin sanık ...'in hesabına para yatırmaları ve Mehmet'in ise hesabında biriken paraları sanık ...'nın adına açılmış hesaba havale etmesinden ibaret olayda, sanıkların eylemi bütün halinde TCK'nın 163/2. maddesindeki karşılıksız yararlanma suçunu oluşturmasına rağmen eylem bölünerek karşılıksız yararlanma suçundan beraat, 5846 sayılı Kanuna aykırılık suçundan ve sanık ... hakkında ayrıca TCK'nın 243/1. maddesi uyarınca bilişim sistemine girme suçundan mahkumiyet kararları verilmiş ise de, eylemin bütün halinde karşılıksız yararlanma suçunu oluşturmasına karşın bu suçtan verilen beraat kararlarının temyiz edilmeden kesinleşmesi karşısında, sanıklar hakkında TCK'nın 243/1. maddesi uyarınca bilişim sistemine girme ve 5846 sayılı Kanuna aykırılık suçundan ceza verilmesine yer olmadığı kararı verilmesi gerekirken mahkumiyetlerine karar verilmesi*" hukuka aykırıdır[59]. Ancak günümüzde spor müsabakalarını yayınlayan şifreli kanallar yayınlarını internet üzerinden de yapabilmektedir. Bu

[57] Yılmaz/Apiş, **a.g.m.**, s.1761; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1398; Karakehya, **a.g.e.**, s. 10. Karakehya karşılıksız yararlanma suçuna ilişkin özel düzenleme olduğu gerekçesiyle 243'üncü maddenin 2'nci maddesi kapsamında cezai sorumluluğun doğmayacağını savunmaktadır.

[58] Akbulut, **Bilişim Alanında Suçlar**, s.147.

[59] 19. CD., E. 2015/2135 K. 2017/10023 T. 22.11.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019.

noktada tespit edilmesi gereken şifreli yayının internet üzerinden yapılan yayın üzerinden mi yoksa uydu yayını üzerinden mi çekildiğidir. Suçu oluşturan fiilde yayın internet üzerinden yapılan yayın üstünden çekiliyorsa bu durumda hem bilişim sistemine girme suçunun hem de karşılıksız yararlanma suçunun oluşması mümkündür[60].

Kablolu/kablosuz internet hatlarına erişerek başkasına ait internet hizmetinden hukuka aykırı şekilde faydalanmanın TCK'nın 163'üncü maddesi kapsamında karşılıksız yararlanma suçunu oluşturup oluşturmayacağı hususu tartışılmalıdır. İnternet, bilişim sistemlerinin birbirine bağlanmasına imkân veren geniş bir iletişim ağıdır[61]. Ancak bu ortam yalnızca ağlardan oluşmamaktadır. İnternet servis sağlayıcıları belli bir bedel karşılığında kablolu veya kablosuz hatlar aracılığıyla kişilerin internete erişimini sağlamaktadır. Dolayısıyla internet başlı başına bir bilişim sistemi sayılamasa da internete erişimi sağlayan başka bileşenler bulunmaktadır[62]. Bu bileşenler de bir bilişim sistemini oluşturmaktadır. Bu sebeple başkasına ait bir internet hizmetinden hukuka aykırı şekilde faydalanılması halinde bedeli karşılığı yararlanılabilen bilişim sistemine girme suçu oluşmalıdır.

Yargıtay kararına konu olan bir olaya göre; "*sanığın, olay tarihinde müştekinin kapatmak için ... Müdürlüğü'ne müraacat ettiği telefon ve ADSL hattına girerek bir şekilde kullanmaya devam etmesi şeklinde gerçekleşen eyleminin 5237 sayılı TCK'nın*

---

[60] "Bedeli karşılığında izlenmesi gereken şifreli televizyon yayınlarının, sahibinin rızasına aykırı olarak bedelsiz şekilde izlenmesini sağlamak eyleminde TCK'nın 163/2. maddesinde düzenlenen karşılıksız yararlanma suçunun unsurlarının oluştuğu, ancak TCK'nın 44. maddesinde yazılı işlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır hükmü gereğince, sanığın eyleminin TCK'nın 243 veya 244. Maddelerinde gösterilen suçu oluşturduğunun belirlenmesi durumunda, eylemin tek olduğu ancak iki farklı suçun oluştuğu da gözetilip, eyleminin uyduğu maddedeki cezalar ile TCK'nın 163/2. maddesinde yazılı cezanın karşılaştırılması suretiyle TCK'nın 44. maddesi de gözetilerek sonucuna göre sanığın hukuki durumunun belirlenmesi gerektiğinin gözetilmemesi," hukuka aykırı bulunmuştur. Bkz. 11. CD., E. 2012/439 K. 2013/16403 T. 11.11.2013, Çevrimiçi, sinerji.com.tr, Erişim Tarihi:4.4.2019.
Aksi yönde bkz. Özen Kaya, "5237 Sayılı Türk Ceza Kanunu'nda Karşılıksız Yararlanma Suçu", **Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi,** Ankara, (Çevrimiçi), tez.yok.gov.tr, 2011, Erişim Tarihi:12.4.2019, s.49.

[61] San Diego County Library, "Introduction to the Internet", http://www.sdcl.org/PDF/gateway_introduction-to-internet.pdf , Erişim Tarihi:4.4.2019; Onur Aktaş, **Siber Güvenlik Hacking Atölyesi**, Ankara, 2. Baskı, Gazi Kitabevi, 2018, s.27.

[62] Aktaş, **a.g.e.**, s.27.

163/2. maddesinde düzenlenen karşılıksız yararlanma suçunu oluşturduğu gözetilmeden, hatalı değerlendirme ile suça yanlış vasıf verilerek yazılı şekilde anılan yasanın 243/1. maddesinde belirtilen bilişim sistemine hukuka aykırı olarak girme ve orada kalma suçundan hüküm kurulması," bozmayı gerektirmiştir[63].

Aynı fıkrada yer alan bedel kavramının içine neler girebileceği konusu da belirlenmeye muhtaçtır. Bedelden anlaşılması gereken yalnızca para değildir. Aynı zamanda bilişim sistemi için öngörülen diğer karşılıklar da bedel ifadesinin kapsamında yer almalıdır[64].

TCK'nın 243'üncü maddesinin 3'nci fıkrasında ise "*sistemin içerdiği veriler*" suçun konusu olarak kabul edilmektedir. Veri teknik anlamda birbiriyle bağlantısı kurulmamış ham bilgilerdir ve sayısal ortamlarda var olan ve taşınan bit dizeleri/sinyaller olarak tanımlanabilir[65]. Yine teknik anlamda veriler işlenerek bilgiye dönüştürülür ve bir anlam ifade edecek bir çıktı haline getirilir[66]. Özbilgi ise bilgiden daha üst ve değerli bir kavramdır ve bir güç oluşturabilecek ve araç haline dönüştürülmek üzere özenle işlenmiş bilgidir[67]. Program ise, bilgi serisinin sistemin belli bir yönde çalışmasını sağlamak amacıyla bir araya getirilmiş halidir[68].

Hukuken veri ise 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 2'nci maddesinin 1'inci fıkrasının k bendinde "*bilgisayar tarafından üzerinde işlem yapılan her türlü değer*" olarak tanımlanmıştır. 5070 sayılı Elektronik İmza Kanunu'nun tanımlara yer verdiği 3'üncü maddesinin b bendinde elektronik verinin " *elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları*" ifade ettiği belirtilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 1'inci maddesinde "*bilgisayar verisi*" tanımlanmıştır. Bilgisayar verisi, bilgisayar

[63] 13. CD., E. 2014/34290 K. 2015/6590 T. 9.4.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:5.4.2019.
[64] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.269; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1397.
[65] Gürol Canberk/Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi**, C.9, S.3, 2006, s.165.
[66] **A.e.**
[67] **A.e.**
[68] Karakehya, **a.g.e.**, s.10.

programları dâhil olguların, bilginin ve kavramların bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü hali olarak tanımlanmıştır.

Yani veriden hukuken anlaşılması gereken teknik anlamından daha geniştir. Bilişim sisteminin soyut tamamlayanlardan olan yazılımlardan en küçük parça olan veriye kadar tüm soyut unsurların 243'üncü maddenin 3'üncü fıkrasının konusunu oluşturabileceğini kabul etmek gerekir. Ancak böyle bir kabul TCK'da düzenlenen bilişim suçlarının bütünlüğü bakımından bazı soruları gündeme getirecektir. TCK'nın 244'üncü maddesinin 1'inci fıkrası "*bilişim sisteminin işleyişinin engellenmesi*" suçunu, 2'nci fıkrası ise "*verilerin yok edilmesi veya değiştirilmesi*" suçunu düzenlemektedir. İlk fıkrada bilişim sisteminin bizzat kendisi suçun konusunu oluştururken, ikinci fıkrada ise bilişim sisteminde yer alan veriler suçun konusudur[69]. Bu iki suç bağlamında ayrım yapılırken failin kastına göre somut olay bazında bir ayrım yapılmaktadır. Bilişim sisteminin işleyişini etkileyecek verilere müdahale halinde ilk fıkra, sistemin yapı taşı olmayan diğer verilere müdahale halinde ise ikinci fıkra uygulanacaktır[70]. Diğer yandan manevi unsur bakımından ise verilerin yok edilmesi veya değiştirilmesi fiili kasten işleniyorsa TCK'nın 244/2'nci maddesi uygulanacakken, bilişim sistemine girme fiili sonucu taksirle verilerin yok olması veya değiştirilmesi halinde 243/3'üncü madde uygulanacaktır. Verilen bu bilgiler ışığında 243/3'üncü maddenin konusu belirlenecek olursa sistemin işleyişine etki etmeyen verilerin ve yazılımların bu fıkranın konusunu oluşturacağının ifade edilmesi gerekir. Bu noktada ise bilişim sistemine girme suçu sonucunda taksirle bilişim sisteminin işleyişine etki eden verilerin ve yazılımların değiştirilmesi veya yok edilmesi fiili boşlukta kalmaktadır. Korunan hukuki değer ve bilişim suçlarının düzenlenmesindeki amaç dikkate alındığında taksirle bilişim sisteminin yapı taşı olmayan verilerin yok edilmesi veya değiştirilmesi hukuk düzenince korunurken, bilişim sistemine girme suçu neticesinde taksirle bilişim sisteminin bizzat işleyişine etki eden veri ve programların yok edilmesi veya değiştirilmesinin de hukuk düzenince korunması evleviyetle gereklidir[71].

[69] Yaşar/Gökcan/Artuç, **a.g.e.,** s.7288-7289.
[70] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.332
[71] Aynı yönde bkz. Karagülmez, **a.g.e.**, s.207.

D. Fiil

1. Bilişim Sistemine Girme Suçunun Muhtelif İşlenme Şekilleri

Bilişim sistemine girme suçu pek çok şekilde işlenebilmektedir. Hedef bilişim sistemine doğrudan hiçbir araç ve yöntem kullanmadan manuel olarak erişilebileceği gibi, çeşitli yazılımlarla veya yöntem ya da tekniklerle işlenebilmesi mümkündür. Bu yöntemler mevcut açıklardan yararlanarak gerçekleştirilebileceği gibi, açık yaratarak veya bilinen şifre/parolaların kullanımıyla yetkisiz şekilde hesaplara ulaşılarak da yapılabilir[72]. Bilişim sistemine girme suçunun işlenme şekilleri her geçen gün değişmekte ve gelişmektedir.

Bilişim sistemine erişimde en sık kullanılan yöntemlerden biri "hacking" yani bilişim korsanlığıdır. Bilişim korsanları bilişim sisteminin güvenliğini tehlikeye sokan pek çok araç ve yöntem kullanmaktadır. Bilişim sistemine hukuka aykırı olarak teknik yöntemlerle girilebileceği gibi, sosyal mühendislik gibi teknik yönü olmayan yöntemlerle de sisteme erişilebilmektedir [73].

Bilişim korsanları, girmeyi amaçladıkları bilişim sisteminin DNS, IP bilgileri, port tarama, işletim sistemini bulma veya sistemdeki kodlama hataları, karmaşık sistemlerin yarattığı açık ve hatalardan faydalanma gibi işlemlerle hedef bilişim sisteminde yer alan eksiklik, açıklık veya zafiyetleri tespit ederek bilişim sistemine sızabilir[74]. Bunun dışında bilişim korsanları, sahte e-postalar yoluyla bilişim sistemine ait verilere ulaşarak bilişim sistemlerine girebilir. Sahte e-postada yer alan bağlantıların yönlendirdiği sayfalara girilen kullanıcı adı, şifre gibi önemli bilgilerin girilmesiyle veya üçüncül linklerin bilişim sistemine indirdiği zararlı yazılımlarla bilişim korsanları kolayca hedef bilişim sistemlerine erişebilmektedir[75].

---

[72] Bkz. öAkıncı/Alıç/Er, **a.g.m.**, s.181-184.
[73] Jason V. Chang, "Computer Hacking: Making the Case for a National Reporting Requirement", **The Berkman Center for Internet & Society Research Publication Series**, Research Publication No. 2004-07, 2004, Çevrimiçi, http://cyber.law.harvard.edu/publications , Erişim Tarihi: 27.09.2018, s. 35.
[74] Hamza Elbahadır, **Hacking Interface**, 17. Baskı, İstanbul, Kodlab, 2018, s.73.
[75] **A.e.**, s.108-110.

Bunun dışında birtakım zararlı yazılımlarda da hedef bilişim sistemine erişim sağlanabilmektedir. Bunlardan biri hedef bilgisayardaki işlemleri kaydetmeye yarayan "*tuş kaydedici (keylogger)*" yöntemidir. Tuş kaydedici (keylogger) yöntemi donanımsal veya yazılımsal olarak gerçekleştirilebilir. Donanımsal tuş kaydedici (keylogger) yönteminde hedef bilişim sistemine takılan bir cihaz bilişim sistemine girerek işlemleri kaydeder. Yazılımsal tuş kaydedici (keylogger) ise bir trojan veya rootkit'in parçası olarak bilişim sistemine yerleşir[76].

Trojan hedef bilgisayarın kullanıcısının bilişim sistemine yararlı bir yazılım gibi yerleşen, bilişim sisteminde yer alan bilgilere erişim sağlayan kötücül yazılımlardır. Trojan aracılığıyla hedef bilişim sisteminde yer alan ekrana müdahale etme dâhil tüm özellikleri kontrol edebilme yetkisi bilişim korsanı tarafından gerçekleştirilebilir hale gelir[77].

Sisteme erişim sağlayan bilişim korsanı çoğu zaman bilişim sisteminde kendisine kolayca erişim sağlama imkânı veren "backdoor" yani arka kapı[78] kurar. Böylece bilişim sistemine erişen bilişim korsanı yerini garantileyerek, bilişim sahibinin izni olmaksızın istediği zaman bilişim sistemine erişim sağlayabilir[79]. Bilişim sisteminde böyle bir kötücül yazılımın tespit edilmesi halinde, hakimin bilişim sistemine girme suçu açısından zincirleme suç hükümlerinin gündeme gelebileceğini göz önüne alması gerekmektedir.

Bilişim korsanları bazen de bilişim sistemlerinde yer alan kodlama hataları ve dikkatsizliklerden faydalanarak uygulamalara yönelik komut saldırıları yapabilir. Örneğin, "*command injection*" yani komut enjeksiyonu, bilişim korsanına bilişim

[76] **A.e.**, 108-109.
[77] **A.e.**, 109.
[78] Backdoor, daha sonra hukuka aykırı olarak erişim sağlamak için bir program veya sisteme gizli şekilde eklenen kodlardır. Bkz. Kabay, M. E.: "Glossary of Computer Crime Terms", (Çevrimiçi), http://www.mekabay.com/overviews/glossary.pdf, 2008, s.1.
[79] Elbahadır, **a.g.e.**, s.226.

sisteminde yer alan zafiyetlerden faydalanma yoluyla komut enjekte etmesini, böylece sızılan bilişim sisteminde bilişim korsanının dilediği komutu çalıştırmasını sağlar[80].

Rootkit ise bilişim sisteminin dosya ve işlemlerini gizleyerek manipüle eden yazılımlar olup, bilişim sistemi sahibinin bilişim sistemine erişildiğini anlamasını zorlaştırmakta ve tespit edilmesini engellemektedir. Hedef sisteme trojan göndermek veya arka kapı bırakmak isteyen bilişim korsanı için rootkitler "*can simidi*" görevini üstlenmektedir[81]. Örneğin anti-virüs programlarındaki basit bir taramayla ortaya çıkabilecek bir trojan türü, rootkitler yardımıyla görünmez hale gelir.

Sosyal mühendislik, bilişim korsanlarının insanların doğal güvenme eğiliminin akıllıca manipüle edilmesi olarak tanımlanmaktadır. Bilişim korsanının bu yolu kullanmada amacı bilişim sistemine ve sistemde yer alan bilgilere yetkisiz erişim sağlamaktır[82]. Bunun dışında haksız yarar sağlama veya sisteme zarar verme gibi amaçlar da söz konusu olabilir[83]. Böylece bilişim sistemindeki güvenlik açıklarından faydalanmaksızın kişiler etkilenir, zorlanır veya aldatılır; bu kişilerin bilişim sistemine erişim sağlanır ve bu sayede bu kişilerin gizli bilgileri edinilmeye çalışılır [84]. En çok karşılaşılan sosyal mühendislik teknikleri oltalama (phishing), sahte senaryolar uydurmak (pretexting), tuzak donanım ve yazılımlar kullanmak (baiting), bir menfaat karşılığı bilgilerin paylaşılması veya satılmasını sağlamaktır (quid pro quo)[85].

---

[80] Guy-Vincen Jourdan, "Command Injection", Çevrimiçi, http://www.site.uottawa.ca/~gvj/Courses/CSI4539-OLD/lectures/CommandInjections.pdf, Erişim Tarihi: 12.02.2019, s.2.

[81] Elbahadır, **a.g.e.**, s.237.

[82] Sarah Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics", Çevrimiçi, https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics , Erişim Tarihi:3.10.2018.

[83] Francois Mouton/Louise Leenen/ H.S. Venter, "Social engineering attack examples,templates and scenarios", **Computers & Security,** V. 59, 2016, Çevrimiçi, https://www.researchgate.net/publication/299344351_Social_engineering_attack_examples_templates_and_scenarios , Erişim Tarihi: 3.10.2018, s. 188.

[84] Hasan Bağcı, "Sosyal Mühendislik ve Denetim", **Denetişim Dergisi**, Kış 2009, s.43.

[85] Francois Mouton/Louise Leenen/ H.S. Venter, **a.g.m.**, s. 188.

2. Bilişim Sistemine Girme veya Bilişim Sisteminde Kalma Fiilleri

6698 sayılı Kanun'un 30'uncu maddesi ile TCK madde 243'de değişiklik yapılmadan önce bilişim sistemine girme suçunun oluşabilmesi için bilişim sisteminin bir kısmına veya tamamına hukuka aykırı olarak girmek ve orada kalmak gerekiyordu. Kanun koyucu özel belgede sahtecilik (TCK m.207) suçunda olduğu gibi suçun oluşması için birden fazla hareketin yapılmasının arandığı çok hareketli bir suç[86] düzenlemişti[87]. Yani bilişim sistemine girilmesi tek başına yeterli olmamakta, aynı zamanda bilişim sisteminde bir süre kalınması gerekmekteydi.

Doktrinde 243'üncü maddenin "*bilişim sistemine girme*" başlığı altında düzenlenmesi suçun çok hareketli olması sebebiyle yanıltıcı olduğundan eleştirilmişti[88]. Zira başlığından sadece bilişim sistemine girmenin suçun oluşması için yeterli olacağı izlenimi oluşmaktaydı. Bazı yazarlar bu sebeple bu suç tipini "*bilişim sistemine girme ve kalma suçu*"[89], "*bilişim sistemine girme ve kalmaya devam etme suçu*"[90] olarak adlandırmaktaydı.

Bilişim sistemine girme hareketinin ardından bilişim sisteminde kalınmasıyla suç tamamlanmakta, dolayısıyla burada seçimlik hareketli bir suçtan bahsedilememekteydi[91]. Bir görüş, bilişim sisteminde kalma hareketinin gerçekleştirilebilmesi için her halükarda ve doğal olarak bilişim sistemine girilmesi gerektiği için suç tipinde yer alan "*bilişim sistemine girme*" ifadesinin kaldırılması gerektiğini savunmuştur[92].

---

[86] Doktrinde suçun 2016 düzenlemesinden önceki hali için doktrinde "birleşik hareketli suç" ifadesi kullanılsa da ifade olarak çok hareketli suç ifadesinin kullanılması gerekmektedir. Çok hareketli suçlarda suçun yapılması için birden fazla hareketin fail tarafından gerçekleştirilmesi gerekir. Bilişim sistemine girme suçunun 2016 düzenlemesinden önce suçu oluşturan bilişim sistemine girme ve orada kalma fiillerinin her ikisinin de gerçekleştirilmesi arandığı için söz konusu suç çok hareketli suç olarak kabul edilmelidir. Çok hareketli suçlar için ayrıca Bkz. Koca/Üzülmez, **a.g.e.**, s.122.
[87] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1373.
[88] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1374.
[89] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, 1363.
[90] Karagülmez, **a.g.e.**, 199.
[91] **A.e.**
[92] **A.e.**, s.204.

6698 sayılı Kanun ile değişiklik yapılmadan önce, bir görüşe göre bilişim sistemine girildikten sonra bir süre kalındığı bilişim sistemine girme suçu için sadece girmenin yeterli olduğu, kalma süresinin hâkimin takdir edeceği cezanın ağırlığına etki edeceği düşünülmekteydi[93]. Ancak doktrindeki ağırlıklı görüşe göre; bilişim sistemine girme suçu mütemadi bir suç olarak düzenlenmişti[94]. Kanun koyucunun "*kalma*" ifadesi yerine "*kalmaya devam etme*" ifadesini tercih etmesi de daha nitelikli ve uzun bir sürenin geçmesine işaret ettiği şeklinde yorumlanmaktaydı[95]. Bu sebeple suç tipiyle ilgili tartışılan konulardan birisi bilişim sisteminde kalmaya devam etme fiilinin suç teşkil edebilmesi için ne kadar süre geçmesi gerektiğiydi. Somut olay bazında her bilişim sisteminin özel güvenlik yapısı olduğu dikkate alındığında bilişim sisteminde kalma süresi değişiklik gösterebileceğinden sabit bir asgari sürenin belirlenmesi mümkün değildi. Bu sebeple, hâkimin somut olaya göre kalma süresinin suçun oluşumu için yeterli olup olmayacağına karar vermesinin daha doğru olacağı savunulmaktaydı[96].

Yine 6698 sayılı Kanun ile değişiklik yapılmadan önce, bilişim sistemine girme suçunun çok hareketli bir suç olarak düzenlenmesi sebebiyle yalnızca bilişim sistemine girme fiilinin suç oluşturmamasının yanı sıra hukuka uygun şekilde bilişim sistemine girildiği halde daha sonra hukuka aykırı olarak kalmak da suç oluşturmamaktaydı. Söz konusu düzenlemenin aksine yalnızca bilişim sistemine girme veya yalnızca bilişim sisteminde kalmanın suç oluşturması yönünde bir kabul suçta ve cezada kanunilik ilkesine aykırılık oluşturmaktaydı[97].

6698 sayılı Kanun'un 30'uncu maddesi ile TCK madde 243'de yer alan "*giren ve orada kalmaya devam eden*" ifadesi "*giren veya orada kalmaya devam eden*" şeklinde değiştirilmiştir. Böylelikle düzenlemenin ilk hali çok hareketli bir suçken, bu değişiklikle bilişim sistemine girme suçu seçimlik hareketli suça dönüşmüştür[98].

---

[93] Soyaslan, **a.g.e.**, s.636; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1377.
[94] Parlar, **a.g.e.**, s.20.
[95] Karagülmez, **a.g.e.**, s.204.
[96] Parlar, **a.g.e.**, s.16; Gül, **a.g.e.**, s.59.
[97] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1380.
[98] Özbek v.d., **a.g.e.**, s.950; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.811; Akbulut, **Bilişim Alanında Suçlar**, s.126.

Bilişim sistemine girmek güvenlik önlemleri aşılarak bilişim sisteminin tamamına veya bir kısmına girilmesi, bilişim sisteminde kalmak ise erişilen bilişim sisteminde bir süre kalınmasını ifade etmektedir[99].

Mevcut düzenleme kapsamında bilişim sistemine hukuka aykırı şekilde girmek veya hukuka aykırı şekilde bilişim sisteminde kalmak suçun oluşumu için yeterlidir. Seçimlik hareketli bir suç olması sebebiyle her iki hareketin de gerçekleştirilmesi halinde yani hukuka aykırı olarak bilişim sistemine girilmesi ve burada kalınması halinde yine tek suç oluşacaktır[100].

Düzenlemede yapılan değişiklikle kast olmaksızın başkasının bilişim sistemine girdiğinden haberi olmadığı halde sonradan hukuka aykırılığın fark edilmesine rağmen bilişim sisteminde kalınması veya hukuka uygun olarak bilişim sistemine girildiği halde hukuka aykırı olarak bilişim sisteminde kalınması[101] veya belirli bir süre için bilişim sisteminde kalınmasına izin verildiği halde bu sürenin dışında bilişim sisteminde kalınması[102] da bilişim sistemine girme suçunun oluşumuna sebebiyet verecektir. Yine bilişim sistemine girmek bir bilişim sisteminin kullanılmasıyla hedef bilişim sistemine girilmesiyle gerçekleştirilebileceği gibi, aracı bir araç kullanılmaksızın doğrudan hedef bilişim sistemine girilmesiyle de suç gerçekleştirilebilmektedir[103].

Önceki düzenlemede çok hareketli bir suç olması sebebiyle bilişim sisteminde kalma süresi tartışma konusuyken, değişiklikle birlikte bilişim sisteminde ne kadar süre kalındığının bir önemi kalmamıştır[104]. Hukuka aykırı olarak bilişim sisteminde kalma süresi suçun oluşturduğu tehlikeye etki edeceğinden TCK'nın 61'inci maddesi kapsamında temel cezanın belirlenmesine ve ağırlığına etki edecektir[105].

---

[99] Tezcan/Erdem/Önok, **a.g.e.**, 980.
[100] Özbek v.d., **a.g.e.**, s.951; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.812; Akbulut, **Bilişim Alanında Suçlar**, s.126.
[101] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.812.
[102] Özbek v.d., **a.g.e.**, s.951.
[103] Ketizmen, **a.g.e.**, s.101; Yılmaz, **a.g.e.**, s.185.
[104] Tezcan/Erdem/Önok, **a.g.e.**, 981; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1376.
[105] Özbek v.d., **a.g.e.**, s.951; Akbulut, **Bilişim Alanında Suçlar**, s.136.

Değinilmesi gereken diğer bir husus ise, 2016 yılından önceki düzenlemede çok hareketli olan bu suç bir bütün olarak mütemadi bir suçken, 2016 yılı sonrasında suçun seçimlik hareketli hale gelmesiyle yalnızca bilişim sisteminde kalma fiili mütemadi suç olma vasfını haizdir[106].

Bilişim sistemine girme suçunun başlığı içeriği anlatmada yetersiz olduğu için eleştirilmektedir. TCK'nın 243'üncü maddesinin son fıkrası bağımsız bir suç olan bilişim sistemine girmeksizin veri nakillerinin izlenmesi suçunu da düzenlediği için yanıltıcıdır[107].

Terminolojik açıdan eleştirilen bir diğer husus ise fiil için bilişim sistemine girme ifadesinin kullanılmasıdır. Doktrinde bazı yazarlar girme fiilinin fiziksel bir alana girmeyi çağrıştırdığını, bu fiil yerine erişim ifadesinin kullanılmasının daha doğru bir ifade olacağını savunmaktadır[108]. İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik'in 3'üncü maddesinin e bendinde erişim "*herhangi bir vasıtayla internet ortamına bağlanarak kullanım olanağı kazanılması*" şeklinde tanımlanmıştır. Bazı yazarlar Yönetmelikte yer alan bu tanımdan yola çıkarak erişim ifadesinin bilişim sistemine yalnızca internet gibi kablolu veya kablosuz ağlar aracılığıyla girilmesini karşıladığını belirtmiştir. Oysaki bilişim sistemine girme ağlar aracılığıyla gerçekleştirilebileceği gibi manuel olarak da gerçekleştirilebilmektedir[109]. Dolayısıyla girme ifadesinin tercih edilmesinin doğru

---

[106] Tezcan/Erdem/Önok, **a.g.e.**, 980.
[107] Akbulut, **Bilişim Alanında Suçlar**, s.128.
[108] Özbek v.d., **a.g.e.**, s. 950.
[109] ""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 (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. G.., 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 (windows,linux vs.), bir başka internet kullanıcısının, mağdurun rızası olmaksızın girmesi de suç oluşturacaktır." 8. CD., E. 2013/10401 K. 2014/11835 T. 7.5.2014, lexpera.com.tr, Erişim Tarihi:3.4.2019.

olduğu belirtilmiştir[110]. Girmek ifadesi ise dışardan içeriye geçmek, erişmek, ulaşmak gibi anlamları karşılamaktadır[111]. Dolayısıyla bilişim fiziki anlamda dışarıdan içeriye geçmek anlamını karşıladığı gibi, bilişim sisteminin içine girilmesi, erişilmesi anlamını da karşılayan daha geniş bir kavramdır[112]. Bu bakımdan kanuni düzenleme dikkate alındığında fiziksel erişim de bu suçun oluşması için yeterli olduğundan girmek ifadesinin kullanılması yerindedir.

Bilişim sistemine girme suçu bakımından bilişim sistemine girme fiilinin bilişim sisteminin fiziki tamamlayanlarına yani donanımına girme değil, soyut tamamlayanlarına girme olduğu ifade edilmiştir[113]. Soyut tamamlayanlara girmek kablolu veya kablosuz ağ bağlantısı yoluyla olabileceği gibi, fiziken de gerçekleştirilebilir[114]. Yine uzaktan erişim veya yardımcı yazılımlarla da bilişim sisteminin soyut tamamlayanlarına girmek mümkündür[115], bilişim sistemine e-posta aracılığıyla casus yazılımlar, virüs gibi kötücül yazılımlar gönderilerek erişilebilir[116].

Özbek'e göre, bilişim sistemine girmenin hukuka aykırı olarak gerçekleşebilmesi için asgari olarak iki unsurun oluşması aranmaktadır. Bunlardan ilki girilen bilişim sisteminin herkesin kullanımına açık ve her an erişilebilir bilişim sistemlerinden olmaması gerekir. Yani bilişim sistemi birtakım tedbir ve uygulamalarla sınırlandırılmalıdır. İkincisi ise bilişim sistemi yöneticisinin belirlediği usul ve yetkiye uygun olarak bilişim sistemine girilmesi hukuka uygundur. Fakat belirlenen yetkiye uygun olmadan bilişim sistemine giriş yapılması yine suçun oluşumuna meydan verecektir. Ayrıca bu usul ve yetkiye uygun olarak alınmış kullanıcı adı ve şifresinin kullanıcının rızasına aykırı olarak kullanılması da bu kapsamda suçun oluşumuna sebebiyet verecektir[117]. Dolayısıyla her an herkesin ulaşımına açık olan bilişim sistemlerine girilmesi ya da açık veya zımni olarak sisteme

[110] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.812.
[111] TDK, Çevrimiçi, tdk.gov.tr, Erişim Tarihi: 10.07.2018.
[112] Aynı yönde bkz. Akbulut, **Bilişim Alanında Suçlar**, s.128.
[113] Parlar, **a.g.e.**, s.18; Soyaslan, **a.g.e.**, s.636; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.812; Akbulut, **Bilişim Alanında Suçlar**, s.130.
[114] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 62.
[115] Özbek v.d., **a.g.e.**, s.954; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.258.
[116] Tezcan/Erdem/Önok, **a.g.e.**, 981.
[117] Özbek v.d., **a.g.e.**, s.950.

girme izni olan kişilerin bilişim sistemi girmesi bilişim sistemine girme suçunu oluşturmayacaktır[118].

Bilişim sisteminin donanımına fiziken müdahale edilmesi ise TCK'nın 151'inci maddesi kapsamında mala zarar verme suçunu oluşturabilecektir[119]. Bilişim sistemine girme fiili, sistemde yer alan şifre veya güvenlik önleminin aşılması yoluyla sisteme girilmesi şeklinde gerçekleşebileceği gibi, şifrenin bilinmesi halinde sistem sahibi veya kullanıcısının rızası olmaksızın şifrenin girilmesi yoluyla da işlenebilir[120]. Dolayısıyla bu suç serbest hareketli bir suçtur[121].

Bilişim sistemine girme suçunun girme hareketi icrai hareket, kalma ise ihmali hareket olarak nitelendirilmiştir[122]. Ancak Dülger'e göre, bilişim sistemine girme hareketinin icrai bir hareketle gerçekleşeceği tartışmasız olsa da bilişim sisteminde kalma hareketi için failin sistemden atılmamak amacıyla bazı yazılımları kullanarak icrai hareketlerle sistemde kalmaya devam etmesi de mümkündür. Dolayısıyla bilişim sisteminde kalma hareketi icrai veya ihmali bir hareketle gerçekleştirilebilmektedir[123].

Failin sisteme girdikten sonra bilgi edinmesi suç tipi bakımından önem arz etmemektedir[124]. Yorum yoluyla böyle bir şartın aranması ceza hukukunda kıyasa varan genişletici yorum yasağına girmesi sebebiyle mümkün değildir[125]. Bu suçu fail kendisinin veya başkasının menfaatine işleyebilmesi mümkündür[126]. Ayrıca bu suç tipinde bir neticenin gerçekleşmesi aranmamaktadır. Dolayısıyla bu suç sırf hareket suçu olarak nitelendirilmiştir[127]. Yani failin bir zarara yol açması veya bilişim

[118] Akbulut, **Bilişim Alanında Suçlar**, s.133-134.
[119] Taşkın, **Bilişim Suçları**, s.25.
[120] Bkz. Taşkın, **Bilişim Suçları**, s.26; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.813; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1375.
[121] Gül, **a.g.e.**, s.60; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1378.
[122] Gül, **a.g.e.**, s.59; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.812; Akbulut, **Bilişim Alanında Suçlar**, s.126; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 56.
[123] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.259.
[124] Soyaslan, **a.g.e.**, s.636; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.262.
[125] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.262.
[126] Soyaslan, **a.g.e.**, s.637.
[127] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.263; Akbulut, **Bilişim Alanında Suçlar**, s.126.

sisteminin zarara uğramasına yönelik yakın bir tehlikenin gerçekleşmesi aranmadığı için bilişim sistemine girme suçu soyut tehlike suçudur[128].

II. MANEVİ UNSUR

Bilişim sistemine girme suçunu düzenleyen 243'üncü maddeye göre bu suç yalnızca kasten işlenebilmektedir[129]. Failin bilişim sisteminin tamamına veya bir kısmına bilerek ve isteyerek hukuka aykırı şekilde girmesi veya burada bilerek ve isteyerek hukuka aykırı şekilde kalması suçun oluşması için yeterli olacaktır[130]. Yani kişinin bilişim sistemine dikkat ve özen yükümlülüğüne aykırı davranarak girip, buradan çıkması halinde suç oluşmayacaktır[131]. Hatayla bilişim sistemine girilmesi veya burada kalınması halinde ise TCK'nın hataya ilişkin maddesi olan 30'uncu maddesinin 1'inci fıkrası uygulama alanı bulacaktır[132]. Dolayısıyla kişi kasten hareket etmiş sayılmayacağından sorumlu tutulamayacaktır.

Kastın unsurları bilme ve istemedir. Buna göre fail, bilişim sistemine girme veya orada kalma yetkisi olmadığını ve bu fiilleri gerçekleştirmenin hukuka aykırı olduğunu bilmeli ve bu fiilleri gerçekleştirmeyi istemelidir[133].

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesi uyarınca taraf devletler "*bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman*" bu erişimi cezalandırmalıdır. TCK'da yer alan düzenleme de Avrupa Konseyi Siber Suçlar Sözleşmesi'yle uyumludur[134].

Avrupa Konseyi Siber Suçlar Sözleşmesi taraf ülkelerin mevzuatlarında bilişim sistemine girmenin " *bilgisayar verilerini elde etmek veya başka bir sahtekar niyetle"* işlenmesini de suç olarak düzenleyebilmesine imkan verse de kanun koyucu

[128] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.813; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 60; Yazıcıoğlu, **Hackerler ve Bilişim Sistemine Girme Suçu**, s.1257.
[129] Akbulut, **Bilişim Alanında Suçlar**, s.139.
[130] Gül, **a.g.e.**, s.64; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.814.
[131] Akbulut, **Bilişim Alanında Suçlar**, s.139; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.814.
[132] Akbulut, **Bilişim Alanında Suçlar**, s.139.
[133] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 275.
[134] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1405.

5237 sayı TCK'da böyle bir şarta yer vermemiştir[135]. Dolayısıyla suçun işlenmesinde genel kast yeterli olup failin eğlence, kendini deneme, merak veya başka hangi sebeple bu suçu işlediğinin önemi bulunmamaktadır[136]. Ancak failin kastı bilişim sisteminin işleyişini bozmak veya engellemek, bilişim sistemine girerek haksız yarar sağlamak veya bilişim sisteminde yer alan verileri yok etme veya değiştirmeye yönelikse bu durumda TCK'nın 244'üncü maddesinde yer alan suçlar gündeme gelecektir[137,138].

Kanuni tanımda bu suçun taksirle de işlenebileceğine yer verilmediği için bilişim sistemine girme suçu taksirle işlenemez[139]. Ancak bilişim sistemine hatayla giren kişinin bu durumun hukuka aykırı olduğunu fark etmesiyle teknik sebeplerle bilişim sisteminden çıkamayıp bir süre kalmasıyla taksirle bu suçu işleyebileceğini savunan bir görüş de bulunmaktadır. Bu görüşe göre suç oluşsa da suçun ancak kasten işlenmesi cezalandırılabilir olduğundan taksirle işlenmesi cezalandırılamayacaktır[140].

Türk ceza hukuku açısından kanunda taksirle işlenebileceği düzenlenmedikçe hiçbir suçun taksirle işlenebilmesi mümkün olmadığı için böyle bir kabul mümkün değildir[141]. Ancak TCK'nın 243'üncü maddesinin 3'üncü fıkrasında yer alan ve fiil sebebiyle verilerin değişmesi veya yok olması durumunda neticesi sebebiyle ağırlaşmış suç söz konusu olduğundan, her ne kadar bilişim sistemine kasten girilmiş olsa da verilerin yok olması veya değiştirilmesi taksirle gerçekleşmelidir[142]. Failin verilerin yok olması veya değiştirilmesi konusunda kastı olması durumunda TCK'nın 244'üncü maddesi kapsamında sorumluluğu da gündeme gelebilecektir. Neticesi

---

[135] **A.e.**

[136] Karakehya, **a.g.e.**, s.14; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1402; Tezcan/Erdem/Önok, **a.g.e.**,s.982; Gül, **a.g.e.**, s.64.

[137] Tezcan/Erdem/Önok, **a.g.e.**,s.982.

[138] Failin seçimlik hareketine göre bilişim sistemine girme suçunun da oluşabilmesi mümkündür. Bilişim sistemine girme le ilgili içtima tartışmaları için tezin III. Bölümünde yer alan "İçtima" başlığına bakınız.

[139] Soyaslan, **a.g.e.**, s.638; Karakehya, **a.g.e.**, s.15; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1405.

[140] İnci Biçkin, "Siber Suç Sözleşmesi ve 5237 sayılı Türk Ceza Kanununda Bilişim Suçları", **Yargıtay Dergisi**, Ankara, C.32, S.1-2, Ocak-Nisan 2006, s.153; Demircan, **a.g.e.**, s.76.

[141] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 275.

[142] Taşkın, **Bilişim Suçları**, s.28-29.

sebebiyle ağırlaşmış hal olan 243'üncü maddenin 3'üncü fıkrası bakımından kast-taksir kombinasyonu aranmaktadır[143].

Bilişim sistemine girme suçunun olası kastla işlenip işlenemeyeceği ise tartışmalıdır. Bazı yazarlar bu suçun olası kastla da işlenebileceğini ileri sürmektedir[144]. Bu görüşü savunan bazı yazarlar bilişim sistemine girme suçunda herhangi bir özel saik aranmadığı gerekçesine dayanmaktadır[145].

Ancak bu suçun yalnızca doğrudan kastla işlenebileceği kabul edilmelidir[146]. Çünkü failin bilişim sistemine girerken yetkisiz olarak haksız şekilde bilişim sistemine girdiğinin bilincinde olması gerekir. Ayrıca kanun koyucunun madde metninde yer verdiği "*hukuka aykırı olarak*" ifadesinden[147,148] ve "*kalmaya devam etme*" fiiline yer vermesinin gerekçesinden[149] de bu suçun doğrudan kastla işlenebileceğine işaret edildiği savunulmaktadır. Ayrıca bilişim sistemine girme fiilinin olası kastla gerçekleştirilebilme imkânı olsa da, bilişim sisteminde kalmanın olası kastla gerçekleştirilemeyeceği doktrinde belirtilmiştir[150].

III. HUKUKA AYKIRILIK UNSURU

TCK'da yer alan suç tiplerinde genel olarak hukuka aykırılık ifadesine yer verilmese de kanun koyucu bazı suçların kanuni tanımında hukuka aykırılığı belirten

---

[143] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 278.
[144] Tezcan/Erdem/Önok, **a.g.e.**,s.982; Mahmutoğlu, **a.g.m.**, 862; Caner Yenidünya, "Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243)", **Legal Fikri ve Sınai Haklar Dergisi**, S.4, 2005, s.1037; Yaşar/Gökcan/Artuç, **a.g.e.**, s.7294.
[145] Karagülmez, **a.g.e.**, s.172.
[146] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.815.
[147] Akbulut, **Bilişim Alanında Suçlar**, s.159.
[148] Failin kusurlu sayılabilmesi için doğrudan haksızlık bilinciyle hareket etmesi gerektiği için bu suçlar yalnızca doğrudan kastla işlenebilir. Neslihan Göktürk, "Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1, 2016, s.434.
[149] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.815; Akbulut, **Bilişim Alanında Suçlar**, s.139.
[150] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1045-1406. Erdoğan 2016 tarihinden önceki düzenlemeyi dikkate alarak bilişim sisteminde doğrudan kastla kalınması durumunda bilişim sistemine girme eylemindeki olası kastın da doğrudan kasta dönüşeceğini belirtmiştir. Bu sebeple 2016 değişikliğinden önce suçun olası kastla işlenemeyeceğine dikkat çekmiştir.

bazı ifadelere yer vermiştir[151]. Bilişim sistemine girme suçunun kanuni tanımında da hukuka aykırılık ifadesine ayrıca yer verilmiş, "*bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden*" şeklinde bir düzenlemeye gidilmiştir.

Doktrinde yer alan görüşlerden birine göre, kanun koyucu tarafından bilişim sistemine giren veya orada kalan kişinin hukuka aykırı hareket ettiğini bilmesi gerektiği ayrıca aranmış ve hukuka aykırılık tipikliğe dâhil edilmiştir[152,153]. Dolayısıyla bilişim sistemine girme veya bilişim sisteminde kalma fiilini hukuka aykırı şekilde gerçekleştirdiği konusunda hataya düşen fail suçun maddi unsurlarında hataya düşmüş olacağından TCK'nın 30'uncu maddesinin 1'inci fıkrası gereğince hata halinden yararlanacaktır[154]. Hukuka uygunluk sebeplerinin maddi koşulları dışındaki hatalar ise kusurluluğa ilişkin olacağından, maddi unsurlar dışında kaçınılmaz bir hataya düşen fail bu hatasından yararlanacaktır[155,156].

Doktrinde kanuni tanımda ayrıca hukuka aykırılık ifadesine yer verilmesinin klasik suç teorisinden kaynaklandığı, somut yargılamada failin haksızlık bilincinin ve özellikle hukuka aykırı hareket ettiğinin ispatlanmasında güçlük yaratacağı gerekçesiyle hukuka özel aykırılık halinin bulunmadığını savunan görüş de bulunmaktadır. Bu görüşe göre, suç tipinden "*hukuka aykırı olarak*" ifadesi çıkarıldığında suçun unsurları açısından bir fark oluşmamaktadır[157].

Kanun koyucunun amacının hakim tarafından bilişim sistemine girme suçu bağlamında bir hukuka uygunluk sebebinin var olup olmadığının araştırılması

---

[151] **A.e.**, s.116.
[152] Akbulut, **Bilişim Alanında Suçlar**, s.136.
[153] Doktrinde bazı yazarlar hukuka aykırılığı belirten ifadelerin kanuni tanımda yer almasını "*hukuka özel aykırılık*"[153] hali olarak adlandırmıştır. Bkz. Kayıhan İçel, İzzet Özgenç, Adem Sözüer, Fatih S. Mahmutoğlu, Yener Ünver, **Suç Teorisi**, İstanbul, Sebat Mümessillik Yayıncılık, 1999, s.101.
[154] Akbulut, **Bilişim Alanında Suçlar**, s.136; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 76.
[155] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 76.
[156] Hukuka aykırılık bilinci ile ilgili bkz. Adem Sözüer, "Hukuki Hata", **Yargıtay Dergisi**, C.21, S.4, Ekim 1995, s.478.
[157] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 281. Dülger; Bilişim Suçları kitabının ilk basısında bilişim sistemine girme suçunu oluşturan fiili işleyen failin aynı zamanda bu fiili hukuka aykırı şekilde davranması gerektiğini savunmuş, diğer basılarda görüşünü değiştirmiştir. Bkz. Murat Volkan Dülger, **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2004, s.219.

gerekliliğine dikkat çekme olduğu kabul edilmelidir.. Failin hukuka uygunluk sebeplerinin maddi koşullarında bir hataya düşmesi halinde ise TCK'nın 30'uncu maddesinin 1'inci fıkrasının uygulanıp uygulanmayacağı dikkate alınmalıdır. Burada ayrıca failin fiilinin suç oluşturduğu konusunda hataya düşmesi gündeme gelebileceğinden TCK'nın 30'uncu maddesinin 4'üncü fıkrası uyarınca kaçınılmaz bir hataya düşüp düşmediğine bakmak gerekecektir. Failin hatasının kaçınılmaz olması halinde failin bu hatasından yararlanması gerekir

Yalnızca yetkili kişilerin girebildiği veya bir şifreyle korunan bilişim sistemine giren kişilerin söz konusu koruma önlemlerine rağmen bilişim sistemine girmesi veya orada kalması halinde failin hukuka aykırı olarak bilişim sistemine girdiğinin ispatının daha kolay olduğu ileri sürülebilir[158]. Bazı ülke mevzuatlarında suçun ön koşulu olarak bilişim sisteminin şifre veya benzeri bir yapıyla korunması esasına yer verilmesine rağmen[159] TCK'nın 243'üncü maddesinde böyle bir ön koşula yer verilmemiştir. Ancak bilişim sisteminin güvenlik önlemlerini almakla yetkili kişinin bu önlemleri ihmal ederek bilişim sistemini herkesin erişimine açık bırakması halinde sisteme giriş yapan veya orda kalan kişilerin bilişim sistemine girme suçunun faili olmayacağı ileri sürülmektedir[160]. Burada somut olayın koşullarına ve söz konusu bilişim sisteminin ne olduğuna dikkat etmek gerekmektedir. Örneğin bir web sitesinde bir bedel veya üyelik karşılığı sunulan bir hizmetin gerekli önlemler alınmadığı için herkese açık hale gelmesi ve web sitesinden açık şekilde bu hizmetin herkese açık bir hizmet olmadığının anlaşılmaması halinde failin fiilinin suç oluşturduğu konusunda kaçınılmaz bir hataya düştüğü söylenebilecektir[161]. Ancak sırf mağdurun gerekli

---

[158] Taşkın, **Bilişim Suçları**, s.27.

[159] Örneğin Japonya'da bilgisayarlara erişimin şifreyle sınırlandırılmış olması aranırken, Amerika'da CFAA'da korunan bilgisayarlara karşı işlenen bilişim suçlarından bahsedilmiştir.

[160] Akbulut, **Bilişim Alanında Suçlar**, s.138.

[161] Bu kapsamda suç oluşacaktır fakat 5237 sayılı TCK'nın 30/4'üncü fıkrası gereğince fail işlediği fiilin haksızlık teşkil ettiği konusunda kaçınılmaz bir hataya düşmüşse bundan faydalanacaktır.
"Olay tarihinde, ... servisinde abonelere ait fatura detaylarının başkaları tarafından rahatlıkla görüntülenebildiğini fark eden sanığın, sistemde güvenlik açığı bulunduğunu göstermek amacıyla, ilgili firmanın bilişim sistemine girip, daha önce iznini aldığını beyan ettiği arkadaşlarının fatura detay bilgilerini, konuya ilişkin açıklamalarını içeren yazılarla birlikte video olarak kaydedip, bilişim sisteminden çıktıktan sonra, söz konusu videoyu, kendisine ait olan web sayfasında yayımladığı olayda, ... abonesi olan sanığın, sistemde, kendisine de zarar verebilecek nitelikte bir güvenlik açığı bulunduğunu delillendirme amacını taşıyan eylemlerinde, hukuka aykırı hareket ettiği bilinciyle hareket ettiği kabul edilemeyeceğinden, Yapılan yargılama sonunda, sanığa yüklenen fiillerin kanunda suç

güvenlik önlemlerini almasında ihmali olduğu için failin mağdura ait bir bilişim sistemine girmesi veya orada kalması fiilinin suç oluşturmayacağı söylenemez. Aksi bir yorum, bir kişinin evinin kapısını açık unutması halinde bu kişiye karşı konut dokunulmazlığının ihlali suçu işlenemeyeceği sonucuna ulaşılmasına sebep olacaktır.

Doktrinde bilişim sistemi kullanıcılarının bilinçlenmesi adına bu tarz koruyucu önlemlerin alınması gerektiği, en azından şifre veya benzeri bir yapıyla korunmayan bilişim sistemine girilmesi veya burada kalınması fiillerinin daha az cezayı gerektiren nitelikli bir hal olarak düzenlenmesi gerektiği savunulmaktadır[162]. Ancak mağdurun bilişim sistemine şifre veya başka bir koruyucu önlem koymaksızın kullanması korunan hukuki değer açısından bu kişinin bilişim sisteminin korunmayacağı sonucunu doğurmamalıdır. Ancak şifre veya başka bir yöntemle başka kişilerin bilişim sistemine erişmesini önlemeye çalışan kişilere karşı işlenen bilişim sistemine girme veya orada kalma fiilinin kanun koyucu tarafından daha fazla cezayı gerektiren nitelikli bir hal olarak düzenlenmesi gerektiği savunulabilir. Çünkü failin tehlikeliliğinin arttığı söylenebilir. Yine doktrinde izinsiz erişimlere karşı koruyucu önlemler alınmış bilişim sistemlerinin, yalnızca yetki verilen kişilerin girmesine izin verilen veri bankalarının veya ücrete tabi olduğu bilinmesine rağmen ücreti ödenmeden yetkisiz şekilde girilen bilişim sistemlerinin hukuka aykırılık açısından bir tartışma yaratmaksızın yalnızca daha ağır cezayı gerektiren nitelikli haller olarak düzenlenip düzenlenmeyeceği hususunun tartışılabileceği savunulmuştur[163].

TCK'da yer alan hukuka uygunluk sebepleri kanun hükmünün yerine getirilmesi, amirin emrinin yerine getirilmesi, ilgilinin rızası, hakkın kullanılması ve meşru savunmadır. Amirin emrinin yerine getirilmesi bakımından konusu suç

---

olarak tanımlanmamış olduğu gerekçeleri gösterilerek mahkemece kabul ve takdir kılınmış olduğundan, katılan vekilinin sübuta ilişkin yerinde görülmeyen diğer temyiz itirazlarının reddine" karar verilmiştir. Bkz. 12. CD., E. 2013/15781 K. 2014/5842 T. 10.3.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi: 3.4.2019.

[162] Doktrinde bazı web sitelerine kişilere ait bir takım veriler girilmiş olmasına rağmen herhangi bir şifre veya koruyucu önlem konulmamış olması halinde bu web sitelerine girme veya orada kalma fiilinin suç oluşturmayacağı savunulmaktadır. Bu durum sokağa bir ilan asıp kimsenin okumamasını istemek gibidir. Dolayısıyla aleniyetin oluştuğu ve kamunun bilgisine sunulmuş bir internet ortamında bilişim sistemine girme suçunun işlenebileceğini kabul etmek doğru değildir. Ancak söz konusu web sitesi şifre veya başka bir koruma önlemine tabi tutulmuşsa bilişim sistemine girme suçu oluşacaktır. Bkz. Karakehya, **a.g.e.**, s.17.

[163] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 283.

oluşturan emirler hukuka uygunluk oluşturmayacağından amirin hukuka aykırı olarak bilişim sistemine girme veya orada kalma doğrultusunda astına verdiği suç konusu emir hukuka uygunluk sebebi oluşturmayacaktır. Bilişim sistemine girme suçu bakımından kanun hükmünün yerine getirilmesi, meşru savunma ve ilgilinin rızası hukuka uygunluk sebebi olarak kabul edilebilir.

A. İlgilinin Rızası

Bir bilişim sistemi üzerinde tasarruf hakkı olan kişinin örtülü veya açık rızasıyla söz konusu bilişim sistemine giren veya orada kalan kişinin hareketi suç oluşturmayacaktır[164]. Örneğin; bir kişinin arkadaşını bilgisayarına girerken görmesine rağmen bir şey söylememesi halinde örtülü bir rıza söz konusu olacağından suç oluşmayacaktır[165]. Rızanın mutlaka en geç fiilin icrası sırasında verilmiş olması gerektiğinden sonradan verilen rıza fiili hukuka uygun hale gelmeyecektir[166]. Yine bir bilişim sistemindeki açıkları tespit etmek için hackerlara verilen yetki de rıza kapsamında yer alacağından bu hackerların fiilleri de suç oluşturmayacaktır[167]. Bilişim sisteminde kalmaya devam etme seçimlik hareketi mütemadi suç oluşturduğu için, bir bilişim sistemine girilmiş ve orada kalınmaya devam ederken mağdurun verdiği rıza geçerli olacağından fiil hukuka uygun olacaktır[168].

Bilişim sistemine girme suçu açısından verilen rızanın sadece bilişim sistemine girmeye yönelik mi olduğu yoksa bilişim sisteminde kalmayı da kapsayıp kapsamadığı hususu önem arz etmektedir. Doktrinde bazı yazarlar bilişim sistemine girmeye

---

[164] Rıza vermeye yetkili kişi bilişim sistemi üzerinde hak sahibi olmalıdır. Yani bir bilişim sistemine girme veya orada kalma bakımından rıza gösterilen kişinin başka bir kişiye rıza vermesi halinde bilişim sistemine girme suçu oluşur. Örneğin; bir banka personelinin şifresini bankayla alakası olmayan birine vermesi halinde suçun oluşmaması için gerekli rıza yetkili kişi tarafından verilmediği için suç oluşur. Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 284; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.159. Rızayı açıklamaya yetkili kişi korunan hukuki değerle bağlantılıdır. Dolayısıyla bilişim sistemi üzerinde hak sahibi olan gerçek ve tüzel kişiler rıza açıklamasında bulunabilir. Bkz. Tezcan/Erdem/Önok, **a.g.e.**, 984; Mahmutoğlu, **a.g.m.**, s.862.

[165] Akbulut, **Bilişim Alanında Suçlar**, s.137.

[166] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 284.

[167] Akbulut, **Bilişim Alanında Suçlar**, s.137. Uygulamada bilişim sisteminde bulunan açıkları ve güvenlik zafiyetlerini tespit ederek bu bilgileri istihbarat örgütlerine, devletlere ve ticari kuruluşlara hizmet veren kişilere beyaz şapkalı hacker/etik hacker denmektedir.

[168] Özbek v.d., **a.g.e.**, s.954; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1409.

yönelik verilen rızanın bilişim sisteminde kalmayı da kapsadığını savunmaktadır[169]. Ancak böyle bir durumda bilişim sistemine girme veya orada kalmanın seçimlik hareketler oluşturduğunu dikkate almak gerekmektedir. Dolayısıyla sadece bilişim sistemine girme için verilmiş bir rızanın varlığına rağmen failin bilişim sisteminde kalmaya devam etmesi halinde bilişim sisteminde kalma fiili suç oluşturacaktır. Ancak rızanın bilişim sistemine girmeye mi yoksa bilişim sisteminde kalmaya mı yönelik olduğu açık şekilde anlaşılamıyorsa rızanın seçimlik hareketlerin her ikisi bakımından da geçerli olduğu kabul edilmelidir[170]. Yine fail, mağdurun bilişim sistemindeyken mağdurun rızasını geri almasına rağmen failin bilişim sisteminde kalmaya devam etmesi halinde de suç oluşacaktır[171]. Rızanın varlığı halinde bu rızanın sakatlanmamış olması önemli olup, bilişim sistemine girme veya orada kalmaya yönelik rızanın varlığının ispatı faile aittir[172].

Bir bilişim sistemine güvenlik önlemleri konulmuş ve bu güvenlik önlemine rağmen bilişim sistemi üzerinde tasarruf hakkı olan kişi tarafından başka kişilere rıza verilmişse, bu kişilerin bilişim sistemine girmesi suç oluşturmayacaktır. Ancak bilişim sistemi üzerinde tasarruf sahibi olan kişi daha sonradan bu güvenlik önlemlerini değiştirirse rıza da ortadan kalmış sayılacağından artık bu kişilerin sisteme girmesi hukuka aykırılık oluşturacaktır[173].

Bunun dışında mağdurun daha önceden aralarındaki şahsi ilişkiye dayanarak bilişim sistemine girme veya orada kalmaya gösterdiği rıza sonrasında bu şahsi

---

[169] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.160.
[170] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 284.
[171] **A.e.**
[172] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.159; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 284. Parlar, ispat yükünün faile ait olduğunu ifade ederken gerekçe olarak bilişim sistemine nasıl gireceğini bilen bir kişinin teknik bilgisi olduğu kabul edilebileceğinden fiilinin hukuka aykırı olduğunun farkında olmayacağının düşünülemez olduğunu belirtmiştir. Her ne kadar ispat yükü fail üzerinde olsa da gerekçe olarak bir bilişim sistemine girme veya orada kalmaya yönelik teknik bilgi günümüzde oldukça yaygın olarak bilinmektedir. Dolayısıyla hukuka aykırı hareket ettiğinin bilincinde olmak ile teknik bilgi ilişkisi kurmak her zaman doğru sonuç vermeyebilir. Bkz. Parlar, **a.g.e.**, s.20.
[173] Akbulut, **Bilişim Alanında Suçlar**, s.137.

ilişkinin sona ermesi halinde mağdurun rıza verme sebebi ortadan kalktığından verilen rıza da ortadan kalkar[174].

Yine hukuki bir ilişkiye dayanılarak bilişim sistemine girmeye veya orada kalmaya yönelik verilen rıza açısından da hukuki ilişkinin sona ermesi halinde dayanağı kalmadığı için rıza zımnen ortadan kalkar. Örneğin, bir şirket veya kamu kurumunda çalışan kişinin işten çıkarılmasının ardından şirket veya kuruma ait bilişim sistemlerine girme veya orada kalmaya yönelik rızanın kaldırıldığı açık olarak ifade edilmese dahi zımnen rızanın ortadan kalktığı kabul edilmelidir. Nitekim Yargıtay 12. Ceza Dairesi'nin kararına göre; "*sanığın, bir şirkette satış pazarlama elemanı olarak çalıştığı, sebepsiz olarak işe gelmemesi nedeniyle işten çıkartılmasından önce, ele geçirdiği şifre ile yetkisiz olarak şirket bilgisayarına girerek şirket çalışanlarının işe geliş gidiş saatlerine ilişkin çizelge ile kendisine ait maaş bordroları, sigortalı işe giriş bildirgesi ve iş sözleşmesi örneklerini çıkartıp, bu belgelerle maaş ve diğer haklarının eksik ödendiği ve bir kısmının ödenmediği, sigortasının süresinde yatırılmadığı iddiasıyla şirket hakkında ÇSGB İzmir Bölge Müdürlüğü'ne şikâyetçi olduğu olayda; şirketin bilgisayar kayıtlarından alınan belgelerin yasal anlamda kişisel veri kapsamında kabul edilemeyeceği ancak sanığın kendi ikrarı ile sabit olan şifreyle girilebilen şirket bilgisayarına ele geçirdiği şifre ile yetkisiz olarak hukuka aykırı girmesi eyleminin TCK'nın 243/1. maddesine uyan bilişim sistemine girme suçunu*

[174] "Müşteki Sibel'in kolluktaki ifadesinde, kendisine ait facebook adresine izinsiz girildiğinden bahsettiği, kollukta verdiği dilekçesinde ise, şikayetten vazgeçtiğini belirttiği, sanığın savunmasında, müşteki Sibel ile birlikte olduğu dönemde müştekinin rızasıyla kendi facebook şifresini verdiğini beyan ettiği dikkate alındığında, sanığın, müştekiye ait facebook giriş şifresini hukuka aykırı olarak ele geçirdiğine dair hiçbir delil bulunmadığı gibi, müşteki Sibel'in bu yönde bir iddiasının da bulunmadığı anlaşılmakla, sanığın, müşteki Sibel'in bilgisi ve rızası dışında müştekiye ait facebook sayfasına girme eyleminin, TCK'nın 136.maddesinde düzenlenen verileri hukuka aykırı olarak verme veya ele geçirme suçunu değil, TCK'nın 243/1.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturduğu göz önünde bulundurularak bu suçtan ceza verilmesi gerektiği gözetilmeden suçun vasfında yanılgıya düşülerek yazılı şekilde hüküm kurulması,
Kanuna aykırı olup, sanığın, temyiz itirazları bu itibarla yerinde görüldüğünden, bu sebepten dolayı 5320 sayılı Kanun'un 8. maddesi gereğince halen uygulanmakta olan 1412 sayılı CMUK'un 321. maddesi uyarınca, hükmün isteme aykırı olarak BOZULMASINA, 14/10/2015 tarihinde oybirliğiyle karar verildi." 12. CD., E. 2015/2309 K. 2015/15364 T. 14.10.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi: 3.4.2019.

oluşturacağı gözetilerek, bu suçtan mahkumiyetine hükmedilmesi" gerektiği hükme bağlanmıştır[175].

Bilişim sistemine girme suçu bakımından verilen rıza şarta bağlanabilir. Rızanın neye ilişkin olduğu yani fiilin nasıl, ne şekilde, ne zaman ve kim tarafından gerçekleştirileceğine ilişkin irade özelleştirilmiş bir rızadır. Bu rızanın dışında gerçekleştirilen fiil hukuka aykırılık teşkil edecektir[176]. Doktrinde bilişim sistemine girme için verilen rızanın şarta bağlı olabileceği kabul edilse de bilişim sistemine belli bir amaç doğrultusunda girmesi için rıza verilmesine rağmen failin başka bir amaçla bilişim sistemine girmesinin suç oluşturmayacağı ileri sürülmüştür[177]. Ancak mağdurun şarta bağlı olarak verdiği rıza amacı da kapsar niteliktedir. Dolayısıyla rızanın veriliş amacının dışında bir bilişim sistemine girilmesi veya orada kalınması da suçun oluşumuna sebebiyet verecektir. Örneğin, mağdurun faile akıllı telefonunu yalnızca bir telefon görüşmesi yapması amacıyla vermesine rağmen, failin rızanın kapsamı dışına çıkarak mağdura ait WhatsApp konuşmalarına girmesi yine bilişim sistemine girme suçunu oluşturmalıdır.

Mukayeseli hukuka bakıldığında ise Amerika Birleşik Devletleri düzenlemesi olan CFAA'de yetkisiz erişime ilişkin suç dışında ayrıca verilen yetkinin aşıldığı erişimler de suç olarak düzenlenmiştir. İngiltere de ise çalışanın bir programa veya bilgisayara erişiminin sınırlarının açıkça tanımlanmış olması halinde yetki dışı amaçla bilişim sistemine girmenin veya yetki dışı bir bilişim alanına girmenin yetkisiz erişim suçunu oluşturabileceği yargı kararlarında belirtilmiştir. Rızanın şarta bağlı olarak verilebileceği kabul edildiğinden, söz konusu rızanın dışına çıkarak işlenen bilişim sistemine girme veya orada kalma fiili suçun oluşumuna sebebiyet vermelidir. Ancak doktrinde TCK'daki düzenlemenin CFAA'de yer alan düzenleme dikkate alınarak kapsamlı bir şekilde ele alınması gerektiği savunulmaktadır[178].

---

[175] 12. CD., E. 2014/2525 K. 2014/17259 T. 8.9.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.
[176] Ayrıntı için bkz. Meral Ekici Şahin, "Ceza Hukukunda Rıza", **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, Ankara, 2010, s. 120.
[177] Akbulut, **Bilişim Alanında Suçlar**, s.137.
[178] Karagülmez, **a.g.e.**, s.230.

Avrupa İnsan Hakları Mahkemesi'nin 03.04.2007 tarihli Copland/Birleşik Krallık kararında yer aldığı üzere, bir devlet kurumunda çalışan başvurucuya kendisine tahsis edilen e-mail, telefon ve internet kullanımında aşırı şahsi kullanımın var olup olmadığının denetlenmesi adına devlet başvurucunun bu verilerini izlemiştir. Avrupa İnsan Hakları Mahkemesi bu olayda elde edilen verilerin üçüncü kişilere açıklanması veya disiplin işlemleri için aleyhine kullanılmasına önem vermeksizin devletin yaptığı bu izlemeyi AİHS'in 8'inci maddesi uyarınca özel yaşama ve haberleşme hakkına saygı ilkesine aykırı bulmuştur[179].

Öte yandan işverenin bilişim sistemlerini yalnızca iş amaçlı kullanıma yani yapılan işin ifasına özgülemesi mümkündür[180]. Ancak bilişim sistemleri yalnızca işin ifası için kullanıma özgülenebilse de işverenin denetleme yapabilmesi için çalışanı bu konuda önceden bilgilendirmesi gerekmektedir. Avrupa İnsan Hakları Mahkemesi Büyük Daire'nin 5.9.2017 tarih ve 61496/08 başvuru numaralı Bărbulescu v. Romania kararında "*işverenin çalışanın haberleşmesini ve diğer iletişimini izlemeye yönelik tedbirler alabilme ihtimalinin, ve bu tip tedbirler alındıysa bunların uygulanıyor olduğunun çalışana bildirip bildirilmediği, AİHM'e göre, burada söz konusu olan bildirimin Sözleşmenin 8. Maddesinin gereklerine uygun addedilebilmesi için, bildirimin izleme faaliyetinin niteliğini açık şekilde içermesi ve izleme faaliyetinden önce yapılması*" gerektiği belirtilmiştir[181].

AYM'nin 24.3.2016 tarihli 2013/4825 başvuru numaralı Ömür Kara ve Onursal Özbek kararında ise çalışanların kendilerine tahsis edilen bilgisayar, e-posta, internet gibi iletişim kaynak ve araçlarını zaruri olmadıkça özel amaçlarla kullanamayacakları hususunda ve gerektiğinde haber vermeksizin ve uyarı yapmaksızın bu bilişim sistemlerinin takip edilebileceği, kopyalanabileceği,

---

[179] Kararla ilgili ayrıntı için bkz. Tezcan/Erdem/Önok, **a.g.e.**, 982; İlke Gürsel, **İşçinin Kişisel Verilerinin Korunması Hakkı**, Ankara, Adalet Yayınevi, 2016, s.379.

[180] Gürsel, **a.g.e.**, 380.

[181] Kararın kısmi çevirisi ve karar hakkında inceleme için bkz. H. Burak Gemalmaz, "Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı", **Lexpera Blog**, Çevrimiçi, http://blog.lexpera.com.tr/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-tarihli-barbulescu-karari/ , 7.9.2017, Erişim Tarihi: 27.01.2019.

raporlanabileceği hususunda çalışanların kabul beyanı ve taahhütnamelerinin bulunduğu belirtilmiştir. Kararda başvurucu olan çalışanların mesai saatleri içinde şahsi hesap ve iletişim araçlarını kullanma imkânı varken özel yazışmaları için kurumsal e-posta adreslerini kullanmasına dikkat çekilerek söz konusu yazışmaların korunması konusunda çalışanların makul beklenti içinde olması sonucuna ulaşılamadığı belirtilmiş ve özel hayata saygı hakkının ve haberleşmenin gizliliği hakkının ihlalinin bulunmadığı yönünde karar verilmiştir[182].

Bahsedilen kararlardan da anlaşılacağı üzere, işverenlerin haklı nedenlerle bilişim sistemlerini izlemesi mümkündür. Ancak bu amaç dışı kullanımların tespiti amacıyla bir bilişim sistemine girilebileceği yönünde uyarı yapılmamışsa suçun oluşacağı kabul edilmelidir[183]. Ancak işverenin çalışana tahsis ettiği bilişim sistemlerini yalnızca işe özgülememiş olması halinde çalışanın bu sistemleri şahsi işleri için de kullanabileceği kabul edilmelidir. Dolayısıyla çalışana ait kişisel dosya, kişisel e-posta, sosyal medya hesapları ve benzeri mesleki olmayan verilerin işveren tarafından denetlenememesi ve izlenememesi konusunda çalışanın gizlilik beklentisi haklı bir beklenti olarak kabul edilmelidir[184]. İşverenin bu haklı beklentiye rağmen şahsi verilere ulaşmak için yaptığı bilişim sistemine girme veya orada kalma fiilleri de suçun oluşumuna sebebiyet vermelidir.

Bu görüşün aksini savunan yazarların gerekçesi ise bir çalışana bilişim sisteminin kurumu tarafından verildiği, kullanım amacının özel işleri barındırmadığı ve yetkili merciin her an bu bilişim sistemini kişiden geri alabileceği üzerine kuruludur. Yani kişiler kendilerine iş için verilen bilişim sistemlerinde özel verilerini bulundurmamalıdır. Bir görüş, 657 sayılı Devlet Memurları Kanunu'nda cihazların özel amaçlarla kullanılmasının disiplin suçu oluşturacağı belirtilmiş olduğundan bilişim sistemlerinin denetlenmesi halinde devlet memurunun rızasının aranmayacağını ve yapılan denetlemenin hukuka aykırı olmayacağını ileri sürmektedir[185]. 657 sayılı Devlet Memurları Kanunu'nun 125/B-e bendinde "*devlete*

[182] Karar için bkz. http://www.kararlaryeni.anayasa.gov.tr/Content/pdfkarar/2013-4825.pdf
[183] Bkz. Akbulut, **Bilişim Alanında Suçlar**, s.139.
[184] Aynı yönde bkz. Gürsel, **a.g.e.**, 391,394-395.
[185] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.159; Yaşar/Gökcan/Artuç, **a.g.e.**, s.7296.

ait resmi araç, gereç ve benzeri eşyayı özel işlerinde kullanmak" disiplin cezasına bağlanmıştır. Söz konusu fiilin tespit edilebilmesi için yapılan denetleme kapsamında kanun hükmünü icra gereği devletin soruşturmaya uygun şekilde delil etmemesi halinde deliller hukuka aykırı hale gelecektir. Söz konusu fiilin disiplin cezasını gerektiriyor olması, devlet kurumu tarafından her halükarda memurun kullandığı kamuya ait bir bilişim sisteminde denetleme yapılabilmesi sonucunu doğurmamalıdır[186].

B. Hakkın Kullanılması

Hukuk düzeni tarafından bir kişiye herhangi bir konuda belirli bir hak tanınmışsa, kişinin kendisine tanınan hakkın sınırlarına uygun şekilde gerçekleştirdiği fiiller hukuka uygundur. Bu hakkın kaynağı kamu hukuku olabileceği gibi, özel hukuk da olabilir[187]. Bu haklar sınırlı sayıda değildir.

1. Haber Verme Hakkı

Hakkın kullanılması kapsamında verilebilecek örneklerden birisi haber verme hakkı kapsamında gazetecilik mesleğinin icrasıdır. Bir gazetecinin haber verme hakkının icrası kapsamında başka bir kişinin bilişim sistemine girerek sistemi izlemesi ve bunun hukuka uygunluk sebebi olup olmadığının değerlendirilmesi gerekmektedir[188].

---

[186] "Hukuka aykırı delil kavramı önce ceza yargılamasında benimsenen bir kavram olup, daha sonra hukuk muhakemesinde de benimsenmiştir. Kavramın tüm yargılama hukuku bakımından benimsenmesi gerektiği genel olarak kabul görmekle birlikte, disiplin soruşturmaları bir yargılama usulü olmadığından, ilkenin soruşturmalarda uygulanabilirliğini; ceza yargılaması ilkelerinin disiplin soruşturmalarında dikkate alınıp alınamayacağı göz önünde bulundurarak irdelemek gerekmektedir." "…İletişimin izinsiz dinlenmesi, gizli ses ve görüntü alınması, bilgisayarların izinsiz incelenmesi, gizli soruşturmacı görevlendirilerek disiplin soruşturmasının yürütülmesi gibi hallerde hukuka aykırı yöntemlerle delil elde edilmiş olacaktır." Gül Fiş Üstün, "*Disiplin Soruşturmalarında Hukuka Aykırı Deliller",* **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 24, S.1, İstanbul, Haziran 2018, s. 19, 24.

[187] Faruk Erem, "Ceza Hukukunda "Hakkın Kullanılması"", **AÜHFD**, C.41, S.1, Ankara, 1990, s.8.

[188] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 286.

ABD'de verilen bir kararda[189] George Ventura, Chiquita şirketinde çalışmakta olup Cincinnati Enquirer'de gazetecilik yapan ve Chiquita şirketi hakkında araştırma yapan Michael Gallagher ile iletişime geçerek ona gizli bilgileri ulaştırabileceğini söylemiştir. Ventura hem Chiquita şirketine ait bilişim sistemlerine girmiş hem de şifre ve sesli mesajları Gallagher'e vererek haberlerinde kullanması için anlaşmıştır. Ventura yapılan yargılama sonucunda birden çok kez bilişim sistemine yetkisiz erişim sağlamaktan, Gallagher ise yetkisiz erişim ve iletişimin dinlenmesi suçlarından mahkum edilmiştir[190].

İngiltere'de verilen bir kararda yer alan olayda ise Independent gazetesi yazarı John Arlidge, British Telecom'a ait bilişim sistemlerinin güvenilir olmadığıyla ilgili araştırmalar yapmaktadır. British Telecom'da bilgisayar operatörü olan bir çalışan Arlidge'ye ulaşarak onu bilişim sistemlerinin güvenli olmadığını göstermek amacıyla British Telecom'un binasına davet etmiş ve şirketteki bilgisayarları kullanarak çok kolay bir şekilde hassas verilere ulaşıldığını göstermiştir. Bunun üzerine bilgisayar operatörüne ve Arlidge'ye dava açılmıştır. Operatör kendisine ait şifre ve kullanıcı adıyla verilen yetkiye dayanarak bilişim sistemine girdiği için bilişim sistemine girme fiilinden dolayı sorumlu tutulmamıştır. Arlidge ise bilgisayarla karşılıklı etkileşimde bulunmadığı ve sadece erişimin nasıl olduğunu izlediği gerekçesiyle yetkisiz erişim suçundan sorumlu tutulmamıştır[191]. Burada operatörün kendisinin gazeteciyi çağırması durumu gazetecinin azmettiren olmadığını göstermektedir. Öte yandan gazeteci sadece bilişim sistemine nasıl girildiğini ve hassas verilere nasıl ulaşıldığını izlemiştir. Doktrinde söz konusu somut olay bakımından yapılan değerlendirmede gazeteci yardım eden sıfatını da haiz değildir. Türk ceza hukuku açısından da problemin bu şekilde çözülmesinin hukuka uygun olduğu belirtilmiştir[192].

Haber verme hakkının hukuka uygunluk sağlayabilmesi için haber konusu olayın gerçek ve güncel olması, haberin yapılmasında kamu yararının bulunması ve

---

[189] Karar için bkz. Ventura v. the Cincinnati Enquirer, 396 F.3d 784 (6th Cir. 2005).
[190] Gene Foreman, **The Ethical Journalist: Making Responsible Decisions in the Pursuit of News**, Wiley-Blackwell, United Kingdom, 2010, s.131-132.
[191] Karar için bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 286-287.
[192] **A.e.**, s. 287.

bunun orantılı şekilde yapılması halinde bilişim sistemine girme suçu bakımından hukuka uygunluk sebebinin oluşması mümkündür[193].

2. Özel Hukuk Sözleşmeleri Bağlamında Hakkın Kullanılması

6098 sayılı Türk Borçlar Kanunu 1'inci maddesi uyarınca bir sözleşmenin kurulabilmesi için tarafların karşılıklı iradelerinin birbiriyle uyumlu olması yeterlidir. Bir kişinin başka bir kişinin bilişim sistemini kullanmaya dair iznini istemesi ve bilişim sahibinin bunu kabul etmesiyle aralarında sözleşme kurulmuş varsayılabilecektir. Dolayısıyla hukuka uygunluk sebeplerinden ilgilinin rızasıyla benzer olarak, bilişim sistemini kullanma hakkı olan kişinin fiili hukuka uygun olacaktır.

Günümüzde pek çok yazılım belirli şart ve koşullarda bilişim sistemi sahibi tarafından kullanıcılara abonelik sözleşmesi, lisanslama sözleşmesi, iş görme sözleşmesi ve benzeri sözleşmelerle[194] bu yazılımları kullanım hakkı tanımaktadır. Söz konusu sözleşmelerin içerdiği maddeler süre, bedel, kullanım şekli gibi sınırlamaya tabi tutulabilmektedir. Kullanım hakkına sahip olan kişinin sözleşmenin şartlarına uymaksızın bilişim sistemine girmesi hukuki sorumluluğun yanında cezai sorumluluğu da gündeme getirebilir[195].

Doktrinde yer alan bir görüşe göre, bilişim sisteminin kullanım hakkının tanındığı sözleşmeler kira sözleşmelerine benzemektedir. Kullanıcıyla bilişim sistemi sahibi arasındaki sözleşmede hakkın üçüncü kişilere devredilebileceğine ilişkin

---

[193] "Haber verme hakkının hukuka uygun bir biçimde kullanılabilmesi için gereken ölçütler dört başlık altında toplanmaktadır.
Bunlar;
1-) Haber gerçek olmalı,
2-) Haber güncel olmalı,
3-) Haberin verilmesinde kamu yararı bulunmalı,
4-) Haberin veriliş biçimi ile özü arasında düşünsel bir bağ bulunmalıdır." YCGK, E. 2007/7-28, K. 2007/34, T. 13.2.2007, (Çevrimiçi),Kazancı İçtihat Bankası, kazancı.com.tr, Erişim Tarihi: 17.06.2019.

[194] Bu sözleşmeler çoğunlukla internet üzerinden yapılmaktadır. Elektronik sistemler üzerinden yapılan bu sözleşmeler doktrinde elektronik sözleşme olarak anılmaktadır. Ayrıntılı bilgi için bkz. Savaş, **a.g.e**., 55 vd.

[195] Aynı yönde; Kurt, **a.g.e.**, s.157.

hüküm yoksa bilişim sistemini kullanım hakkına sahip kişinin başka birisine sisteme erişim yetkisi vermesi halinde bilişim sistemi sahibinin rızasının olmadığı kabul edilmelidir. Bu sebeple söz konusu fiil hukuka aykırılık arz edecektir[196]. Ancak belirtmek gerekir ki her bilişim sistemi ve buna ilişkin kullanım sözleşmeleri bakımından sözleşmede kullanıcıya üçüncü kişilere yetki devri yapılabileceğine ilişkin hükmün aranması doğru bir yaklaşım olamayacaktır. Bilişim sistemi sahibi yapılan sözleşme ile sistemi kullanım hakkının üçüncü kişilere devrinin mümkün olmadığını hükme bağlamalıdır. Bu sayede bilişim sistemi kullanıcısına tanınan hakkın sınırları çizilmiş ve belirlenmiş olacaktır.

Özel hukuk sözleşmelerinde yer alan hükümlere aykırı fiiller sözleşmeye aykırılık oluşturmakla birlikte haksız fiilin oluşmasına da sebebiyet verebilir. Söz konusu sözleşmeye aykırılık veya haksız fiilin aynı zamanda ceza hukuku bakımından bir suç tipinde yer alan fiili oluşturması halinde failin ceza hukuku bakımından da sorumluluğu gündeme gelecektir. Bilişim sistemleri otomatik sistemler olması sebebiyle bilişim sistemi sahipleri genellikle kullanıcılara kullanım hakkını devretmeden önce birtakım koruyucu önlemler alarak bilişim sistemine girişi engellemektedirler. Taraflar arasında sözleşme kurulduktan sonra bilişim sistemi sahibi kullanıcıya kullanım hakkını tanımakta ve şifre, kullanıcı adı gibi sisteme girişi sağlayacak verileri sunmaktadır. Bilişim sistemine girişi sağlayan bu kullanıcı adı, şifre gibi verilerin geçerliliği de aralarında kurulan sözleşmede yer alan kapsam ve süre için geçerli olmaktadır. Şayet fail sözleşmede yer alan hakkın kullanılmasına ilişkin şart ve sınırlara aykırı hareket ederse bu fiili aynı zamanda ceza sorumluluğunu gündeme getirebilecektir. Örneğin, sözleşmeye göre belli ücret karşılığında internet üstünden süper lig maç yayınlarının yalnızca şahsi kullanım alanlarında izlenmesine yönelik yapılan bir sözleşmeye rağmen kullanıcının maç yayınlarının işyerinde göstermesi halinde kullanıcının kendisine tanınan hakkın dışına çıktığı açıktır. Dolayısıyla kullanıcının sözleşmeye aykırı şekilde işyerinde maç yayını yapması bilişim sistemine girme suçunun "*bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesine"* sebebiyet vermelidir.

[196] **A.e.**

Bilişim sistemine girme veya orada kalma hakkı olan kişinin bu hakkını başkalarıyla paylaşması konusunda yetkisi olmaması halinde de hem hak sahibinin hem de yetki dışı sisteme giriş yapan kişinin cezai sorumluluğu gündeme gelebilecektir. Örneğin, bir mevzuat ve içtihat bankası otomasyon sistemi sahibi şirketin söz konusu sistemden kullanım hakkını yalnızca kullanıcıya tanındığına ve üçüncü kişilerle paylaşılamayacağına dair hükmü açık şekilde sözleşmesinde düzenlemesine rağmen kullanıcı sisteme giriş bilgilerini üçüncü bir kişiyle paylaşıp sisteme girebileceğini ifade ederse sözleşmenin tanıdığı hakkın sınırı göz önüne alındığında kullanıcı bilişim sistemine girme suçu bakımından somut olaya göre azmettiren veya yardım eden[197], üçüncü kişiler ise suçun faili olarak sorumlu tutulabilecektir.

Öte yandan beyaz şapkalı hacker/bilişim uzmanları şirket veya kurumlara ait bilişim sistemindeki açıkların bulunması adına sistemin güvenlik duvarlarının zorlanması ve sızma testlerinin yapılması için şirket veya kurumlarla sözleşme yapabilirler. Beyaz şapkalı hackerların sözleşme kapsamında yaptıkları erişimler bu kapsamda hukuka uygunluk sebebi olduğundan suç oluşturmayacaktır. Ancak beyaz şapkalı hackerların açıkları bulmasına rağmen şirket veya kuruma bu bilgileri vermeyerek sisteme sızmaya devam etmesi halinde sözleşmenin amacı dışına çıkılması söz konusu olduğundan suç oluşacaktır[198].

Bilişim sistemi sahibinin verdiği yetkinin dışına çıkılarak bilişim sistemine erişilmesi halinde mevcut düzenleme gereğince suçun oluştuğunun kabul edilmesi gerekse de söz konusu yetki aşımının sözleşmenin ihlalini oluşturduğu ve yalnızca özel hukuk açısından sorumluluk doğuracağı yönünde bir algının oluşması da muhtemeldir. Ancak korunan hukuki değerin bilişim sistemine duyulan güven olduğu dikkate alınmalıdır. Bu sebeple yetki aşımının suç oluşturup oluşturmayacağına ilişkin ihtilafların önüne geçebilmek adına CFAA'de yer alan düzenleme gibi yetki aşımının da suç oluşturacak şekilde düzenlenmesi önemlidir.

[197] Somut olayın koşullarına göre, müşterek faillik değerlendirmesinin yapılması da mümkündür. Nitekim şifre ve kullanıcı adının verilmesi somut olayda işlenen fiil üzerinde müşterek hâkimiyet kurmaları sonucunu da doğurabilir.
[198] Kurt, **a.g.e.**, s.148.

C. Meşru Savunma

Bilişim sistemine girme suçunun mağduru olan kişinin bilişim sistemine saldıran faile karşı meşru savunmada bulunup bulunamayacağı konusunda doktrinde farklı görüşlere yer verilmiştir. Bir görüşe göre, bilişim sistemine yapılan saldırılarda mağdurun saldırıdan önce kendi bilişim sistemini korumaya yönelik önlemleri alması gerekir. Failin bilişim sistemine yaptığı saldırının büyüklüğü ve kapsamı saldırı anında tam anlamıyla anlaşılamayacağından meşru savunmada bulunurken "*saldırıyı orantılı bir biçimde defetme zorunluluğu*" şartlarını sağlamak mümkün görünmemektedir. Nitekim meşru savunmanın şartlarının gerçekleşip gerçekleşmediğinin ispatı da oldukça zordur. Meşru savunmanın mümkün olabileceğini kabul etmek "*uğramış olduğum saldırıya karşılık veriyordum*" şeklindeki savunmalara imkân sağlayarak bilişim suçlarının işlenmesinin de önünü açacaktır ve başka haksızlıkların oluşmasına sebebiyet verecektir[199].

Bilişim sistemine girme suçu bakımından mağdurun failin kimliği ve adresini tespit edebilmek amacıyla bilişim sistemine girmesinin meşru savunmanın şartlarını sağlamadığı ancak mağdurun fiili işlerken hukuka aykırılık bilinci olmadığını savunan görüşler de bulunmaktadır[200].

Bilişim sistemine girme suçu bakımından meşru savunmanın varlığını kabul edebilmemiz için meşru savunmaya ilişkin şartların incelenmesi gerekir. Bilişim sistemine girme suçunu işleyen bir faile karşı saldırıda bulunulması halinde teorik olarak saldırıya ilişkin şartların oluşması mümkündür. Ancak savunmaya ilişkin şartlara bakıldığında savunmanın zorunlu olması ve orantılı olması şartlarının sağlanması oldukça güç görünmektedir. Bilişim sistemine yönelik saldırılarda savunmanın zorunlu olması o saldırıyı başka türlü şekilde defetme imkânının olmamasını gerektirmektedir. Öte yandan mağdurun savunmasına yönelik hareketin saldırıyı defedecek ölçüde kalması gerekmektedir. Bu açıdan bakıldığında bilişim

[199] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 286.
[200] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 82.

sistemine yönelik saldırının niteliğinin ne olduğu ve nasıl gerçekleştiğine göre meşru savunmanın mümkün olup olamayacağı tartışılmalıdır.

Saldırının niteliğine göre bazı hallerde meşru savunmanın mümkün olduğu kabul edilebilir. Bilişim sistemine saldırı ağ bağlantısı üzerinden yapılıyorsa ve mağdur bunun farkındaysa bilişim sistemi kapatıldığında veya ağ bağlantısı kesildiğinde saldırı engellenmiş olacağından meşru savunma mümkün olmayabilecektir[201]. Öte yandan bilişim sistemine yapılan saldırıya karşı meşru savunmada bulunabilecek kişinin bilişim sistemleri ve saldırılar bakımından yeterli teknik bilgiye sahip olduğu dikkate alınmalıdır. Bu kişilerin yapılan saldırıların ne olduğunu ve bunları nasıl engelleyebileceğini bilmesi de ihtimal dâhilindedir. Nitekim günümüzde devlet kurumları ve birçok şirket bilişim sistemine yapılacak saldırılara karşı bilişim güvenliği uzmanları (beyaz şapkalı hacker/ etik hacker) ile çalışarak olası saldırılara yönelik önlemler almaktadır. Bu doğrultuda teknik bilgiye sahip bu kişilerin bilişim sistemi saldırılarına karşı meşru savunmada zorunluluk ve orantılılık şartlarını sağlaması halinde söz konusu fiilin hukuka uygun olduğu söylenebilecektir. Yine aynı şekilde fiziki olarak bilişim sistemine girme veya orada kalmaya yönelik bir saldırı olması halinde meşru savunma gündeme gelebilecektir[202].

D. Kanun Hükmünü Yerine Getirme

Kanun hükmünü yerine getirme TCK'da sayılan diğer bir hukuka uygunluk sebebidir. Bu hukuka uygunluk sebebinin bilişim sistemine girme suçu açısından uygulama alanı bulacağı maddelerden biri 5271 sayılı CMK'nın 135'inci maddede yer alan "*İletişimin Tespiti, Dinlenmesi ve Kayda Alınması*" koruma tedbiridir[203]. Söz

[201] Bu noktada bilişim sisteminin kapatılması her zaman saldırının defedilmesi anlamına gelmeyebilir. Örneğin e-ticaret şirketlerinin bilişim sistemlerine yönelik bir saldırıda bu şirketin yetkililerine bilişim sistemlerini kapatarak saldırıyı defetmesini beklemek doğru değildir. E-ticaret internet sitesinin bir saat bile erişime kapatılması ciddi ekonomik zararlar doğurabilir niteliktedir. Bu kapsamda şirket bünyesinde çalışan bilişim güvenliği uzmanlarının saldırıyı defetmek için uygulayacağı orantılı savunma hukuka uygunluk sebebi oluşturabilmelidir.

[202] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1411; Erdoğan, **Türk Ceza Hukuku'nda Bilişim Suçları**, s.162.

[203] Apaydın, 5271 sayılı CMK'nın 140'ıncı maddesinde yer alan "Teknik Araçlarla İzleme" koruma tedbirinin de bilişim sistemine girme suçu açısından hukuka uygunluk sebebi olarak anılabileceği belirtilse de teknik araçlarla izleme bilişim sistemine girilmeksizin bir izleme yapılması sebebiyle 5237

konusu maddeye göre "*bir suç dolayısıyla yapılan soruşturma ve kovuşturmada, suç islendiğine ilişkin somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka suretle delil elde edilmesi imkânının bulunmaması durumunda, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının kararıyla şüpheli veya sanığın telekomünikasyon yoluyla iletişimi (...) dinlenebilir, kayda alınabilir ve sinyal bilgileri değerlendirilebilir…*"

Polis Vazife ve Salahiyet Kanunu'nun 13/A maddesinde de "*kaybolan çocukların bulunması amacıyla, polis, sulh ceza hâkiminin veya gecikmesinde sakınca bulunan hallerde mülki idare amirinin yazılı veya sonradan yazılı hale getirilmek üzere sözlü emri ile kayıp çocuğa ait veya başkasına ait olmakla birlikte kayıp çocuk tarafından kullanılan her türlü banka hesap hareketlerini talep edebilir, telekomünikasyon yoluyla iletişimini denetleyebilir ve sinyal bilgilerini değerlendirebilir*" şeklinde bir hükme yer verilerek kaybolan çocukların bulunması amacıyla belirli koşullara bağlı olarak iletişimin denetlenmesi de hukuka uygunluk sebebi olarak kabul edilmiştir.

Yine Polis Vazife ve Salahiyet Kanunu'nun Ek 7'inci maddesi uyarınca *"Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, Anayasa düzenine ve genel güvenliğine dair önleyici ve koruyucu tedbirleri almak, emniyet ve asayişi sağlamak*" amacıyla "*...4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçlar ile bilişim suçlarının işlenmesinin önlenmesi amacıyla hâkim kararı veya gecikmesinde sakınca bulunan hallerde Emniyet Genel Müdürünün, Emniyet Genel Müdürlüğü İstihbarat Dairesi Başkanının veya bilişim suçlarıyla sınırlı olmak üzere bilişim suçları ile ilgili daire başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişim veya internet bağlantı adresleriyle internet kaynakları arasındaki veri trafiği ile iletilen veriler tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir…*"

sayılı TCK'nın 243/4'üncü fıkrasında yer alan ve ayrı bir suç oluşturan "veri nakillerinin hukuka aykırı olarak izlenmesi suçu" açısından bir hukuka uygunluk sebebi oluşturabilecektir. Bkz. Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 77.

2937 sayılı Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu'nun 6'ıncı maddesinde yine iletişimin denetlenmesine ilişkin bir hükme yer verilmiştir. Buna göre "*...Anayasanın 2 nci maddesinde belirtilen temel niteliklere ve demokratik hukuk devletine yönelik ciddi bir tehlikenin varlığı halinde Devlet güvenliğinin sağlanması, casusluk faaliyetlerinin ortaya çıkarılması, Devlet sırrının ifşasının tespiti ve terörist faaliyetlerin önlenmesine ilişkin olarak, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Teşkilat Başkanı veya yardımcısının yazılı emriyle telekomünikasyon yoluyla yapılan iletişim tespit edilebilir, dinlenebilir, sinyal bilgileri değerlendirilebilir, kayda alınabilir…"*

2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu'nun Ek 5'inci maddesi gereğince "*Jandarma, bu Kanunun 7 nci maddesinin (a) bendine ilişkin görevleri yerine getirirken önleyici ve koruyucu tedbirleri almak üzere, sadece kendi sorumluluk alanında 4.12.2004 tarihli ve 5271 sayılı Ceza Muhakemesi Kanununun, casusluk suçları hariç, 250 nci maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesinin önlenmesi amacıyla, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı veya istihbarat başkanının yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilir, dinleyebilir, sinyal bilgilerini değerlendirebilir, kayda alabilir*".

İletişimin denetlenmesine ilişkin hükümlerde yer alan "*telekomünikasyon yoluyla iletişim*" ifadesi bilişim sistemine girme suçu açısından sisteme girme ve orada kalma fiilini hukuka uygun hale getirmektedir. Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'in 4/1-j bendinde telekomünikasyon kelimesinin tanımına yer verilmiştir. Buna göre telekomünikasyon "*işaret, sembol, ses ve görüntü ile elektrik sinyallerine dönüştürülebilen her türlü verinin; kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektro kimyasal, elektro mekanik ve diğer iletim sistemleri vasıtasıyla iletilmesi, gönderilmesi ve alınmasını*" ifade etmektedir. Söz konusu tanım

bilişim sistemini kapsar niteliktedir[204]. Dolayısıyla internet üzerinden sağlanabilen her türlü iletişim de (örneğin facebook, instagram, twitter, e-posta vs.) iletişimin denetlenmesi koruma tedbirinin kapsamındadır[205].

5271 sayılı CMK'nın 134'üncü maddesinde yer alan "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve Elkoyma*" koruma tedbiri kanun hükmünü yerine getirme kapsamında hukuka uygunluk sebeplerinden biridir. Söz konusu madde uyarınca "*Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (...) karar verilir*". Bunun dışında Adli ve Önleme Aramaları Yönetmeliği'nin 17'inci maddesinde bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma koruma tedbirine ilişkin bir hüküm bulunmaktadır. Genel olarak Yönetmelik 5271 sayılı CMK ile paralellik gösterse de Yönetmelik'in 17'inci maddesinin 3'üncü fıkrasının 2'nci cümlesi tedbirin konusunu kısmen daha geniş tutulmuş, "*bu işlem, bilgisayar ağları ve diğer uzak bilgisayar kütükleri ile çıkarılabilir donanımları hakkında da uygulanır*" şeklinde düzenlemeye gidilmiştir.

Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koymaya ilişkin bir düzenlemenin bilişim sistemine girme suçu açısından bir hukuka uygunluk sebebi oluşturması hususunda özel olarak ele alınması gereken bazı noktalar bulunmaktadır. Söz konusu koruma tedbirinde yer alan "*bilgisayar*", "*bilgisayar programları*" ve "*bilgisayar kütükleri*" ifadelerinden şüpheliye ait elektronik delillerin elde edilmesi amaçlandığı anlaşılmaktadır[206]. Elektronik delil, *"bir elektronik araç üzerinde saklanan veya bu araçlar aracılığıyla iletilen soruşturma açısından değeri olan bilgi ve veriler"* şeklinde tanımlanmaktadır[207]. Bu

[204] Mahmutoğlu ileri teknoloji ürünü cep telefonları da bilişim sistemi olduğunu belirterek m.135 kapsamında yer aldığını belirtmiştir. Mahmutoğlu, **a.g.m.**, s.862.
[205] Cumhur Şahin, **Ceza Muhakemesi Hukuku I**, 9. Baskı, Ankara, Seçkin Yayıncılık, 2018, s. 366.
[206] Apiş, **a.g.m.**, s.73.
[207] Leyla Keser Berber, **Adli Bilişim**, Ankara, Yetkin Yayınları, 2004, s.46.

elektronik delillerin elde edilmesi amacıyla bilgisayar dışındaki bilişim sistemlerinde arama ve el koyma koruma tedbirinin söz konusu olduğu hallerde 5271 sayılı CMK'daki hangi tedbirin uygulanacağının tartışılması gerekir.

Doktrinde bir görüşe göre, cep telefonuna el koyma biçiminde ortaya çıkan bir tedbir 5271 sayılı CMK'nın 134'üncü maddesinde yer alan tedbirin konusuna girmemektedir[208]. Zira kanun koyucu açık açık bilgisayar kelimesini tercih etmiştir. Dolayısıyla bilgisayar dışındaki araçlara karşı yapılacak arama ve el koyma işlemi 5271 sayılı CMK'nın 116-129'uncu maddeleri aralığında yer alan tedbirler uyarınca yapılmalıdır. Bu görüşe göre, aksi bir uygulama kişisel verilerin ve özel hayatın gizliliği konusunda hukuka aykırı uygulamalara yol açacak niteliktedir. Dolayısıyla cep telefonlarına el koymada ikili bir ayrım yapılması gerektiği savunulmaktadır. Cep telefonunda yer alan konuşma veya kısa mesaj gibi telefonun özelliğiyle ilgili bir arama ve el koyma kararları 119'uncu maddeye göre genel arama hükmüne tabi olmalıdır. Ancak cihazın bilgisayar özelliğiyle ilgili e-posta, arama motoru gibi kayıtları incelenecekse yine 5271 sayılı CMK'nın 134'üncü maddesi uygulama alanı bulmalıdır[209].

Başka bir görüşe göre ise, bilgisayar ifadesi dar yorumlanmalıdır. Dolayısıyla arama hangi içeriğe yönelik olursa olsun cep telefonları hakkında verilecek arama kararı için 5271 sayılı CMK'nın 134'üncü madde uygulanamayacaktır[210].

Doktrinde yer alan bir görüşe göre, kanun koyucu TCK'da "*bilişim sistemi*" ifadesini tercih ederken, 5271 sayılı CMK'nın 134'üncü maddede "*bilişim sistemi*" ifadesini kullanmak yerine "*bilgisayar*", "*bilgisayar programları*" ve "*bilgisayar kütükleri*" ifadesini tercih etmiştir. Kanun koyucunun aksine bir iradesi olsaydı bunu açıkça ortaya koyması beklenirdi. Özel koruma tedbirlerinin getirilmesindeki amaç maddi gerçeğe ulaşırken kişilerin hak ve özgürlüklerini makul ölçüde korumaktır. Bu görüş, kişilerin özel hayatıyla doğrudan ilişkili olmayan bilişim sistemlerinin bu

[208] Muharrem Özen, Gürkan Özocak, "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", **Ankara Barosu Dergisi (1)**, 2015, s.47,70.
[209] **A.e.**, s.69-70.
[210] Taşkın, **Bilişim Suçları**, s.173-174.

anlamda özel bir korumaya tabi olmadığını savunmaktadır. Dolayısıyla cep telefonu gibi kişinin özel hayatıyla sıkı ilişki içinde olan bilişim sistemleri dışındaki sistemler 5271 sayılı CMK'nın 134'üncü madde kapsamında değerlendirilmeyecektir[211].

Doktrinde bir görüşe göre, bilgisayar kavramı geniş ele alınmış ve cep telefonları, tabletler, akıllı televizyon, oyun konsolları gibi otomatik işlem yapan ve depolayabilen cihazlar da bilgisayar tanımına dâhil edilmiştir. Bu sebeple, anılan akıllı cihazlar bakımından da 5271 sayılı CMK'nın 134'üncü madde uygulama alanı bulmalıdır[212].

Yargıtay ise 5271 sayılı CMK'nın 134'üncü maddesini dar yorumlamaktadır[213].

Doktrinde 5271 sayılı CMK'nın 140'ıncı maddesinde yer alan "*Teknik Araçlarla İzleme*" koruma tedbirinin de kanun emrinin yerine getirilmesi söz konusu olduğundan bilişim sistemine girme suçu bakımından hukuka uygunluk sebebi olduğu belirtilmiştir[214]. Ancak Ceza Muhakemesi Kanununda Öngörülen Telekomünikasyon Yoluyla Yapılan İletişimin Denetlenmesi, Gizli Soruşturmacı ve Teknik Araçlarla İzleme Tedbirlerinin Uygulanmasına İlişkin Yönetmelik'in "*Teknik Araçlarla İzleme İşlemi*" başlıklı 17'inci maddesine göre "*izlenen kişinin iş yeri ve kamuya açık yerlerdeki her türlü faaliyeti teknik araçlarla gizli olarak gözetlenebilir, izlenebilir, ses ve görüntü kaydı alınabilir*". Dolayısıyla burada bilişim sistemine girme veya

---

[211] Apiş, **a.g.m.**, s.79.

[212] Dülger/Modoğlu, **a.g.e.**, s.112; Murat Volkan Dülger, "Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri", (Çevrimiçi), https://www.academia.edu/9449240/BİLİŞİM_SİSTEMLERİ_ÜZERİNDE_ARAMA_KOPYALAMA_VE_EL_KOYMA_TEDBİRİ, s. 7.

[213] "Mahkeme kararına istinaden yapılan aramada sanığa ait cd'ler ve bilgisayar kasasının muhafaza altına alındığının belirtildiği, aynı gün Sulh Ceza Mahkemesi'nden el koymanın onaylanmasına dair CMK'nın 127/1 maddesi uyarınca karar alındığı ancak, arama sonrası bilgisayarların yedeklemesinin yapılıp şüpheliye verildiğine dair bir ibareye tutanakta yer verilmediği gibi, bilgisayar kütüklerinde arama yapılmasından önce mahkemeden bu hususta karar alınmadığının anlaşıldığı, bu suretle CMK'nın 134. maddesi hükümlerine riayet edilmeyerek bilgisayar kütüklerinde bilirkişi incelemesi yaptırıldığı, bilgisayar kasasında hukuka aykırı yapılan bu arama ve el koyma sonucu elde edilen delillerin de hukuka aykırı yöntemle elde edilmiş delil niteliğinde bulunduğunun anlaşılması karşısında, yalnızca cd'lerin delil olarak kullanılabileceği…"17. CD., E.2015/23959, K. 2016/6096, T.28.03.2016. Karar için bkz. Apiş, **a.g.m.**,s.75, dn.83.

[214] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1410; Yılmaz, **a.g.e.**, s.189; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s.77.

orada kalma fiili söz konusu değildir[215]. Teknik araçlarla izleme, iletişimin denetlenmesinden farklı bir yol izler. İletişimin denetlenmesinde telekomünikasyon yoluyla yapılan iletişimler araya bir vasıta konularak denetlenmektedir. Ancak teknik araçlarla takipte şüpheli veya sanığın kamuya açık alanlardaki faaliyetleri ve ortamdaki konuşmaları gözetlenir, izlenir ve kayıt altına alınır. Teknik araçlarla izleme koruma tedbirinin kanunda gösterilen şartlara uygun yapılmaması halinde TCK'nın 243'üncü maddesinin 4'üncü maddesinde ayrı bir suç olarak düzenlenen veri nakillerinin hukuka aykırı olarak izlenmesi suçu, 134'üncü maddede düzenlenen özel hayatın gizliliğini ihlal suçu, 135'inci maddesinde yer alan kişisel verilerin kaydedilmesi suçu, 136'ıncı maddede yer alan verileri hukuka aykırı olarak verme veya ele geçirme suçunu gündeme getirmesi söz konusu olabilir. Örneğin, bir kişinin konutundaki bilgisayarın konuta kurulmuş gizli kamera aracılığıyla izlenmesi halinde bilişim sistemine girme suçu zaten oluşmayacaktır.

Kanun ve yönetmeliklere uygun şekilde ve koşulların sağlanarak yetkili kişiler tarafından bilişim sistemine girilmesi veya orada kalınması halinde hukuka uygunluk sebeplerinden kanun hükmünün yerine getirilmesi söz konusu olacaktır.

Kanun hükmünü yerine getirme bakımından kendi hukukumuzdan farklı olarak özellikle Almanya'da uygulaması olan ve üzerine kanuni düzenlemelerin yapıldığı devlet trojanı (Almanca "*bundestrojaner*", İngilizce "*state trojan*", "*govware*") kullanılarak uygulanan "*çevrimiçi arama*"[216] tedbirine değinmek gerekir. Alman hukukunda 2011'den beri[217] yer alan çevrimiçi arama tedbiri ile devlet şüphelilerin

---

[215] Aynı yönde bkz. Apiş, **a.g.m.**, s.80.

[216] Doktrinde genellikle "online arama" olarak geçmektedir. Bkz. Hans Kudlich, "Ceza Kovuşturmasında Federal Truva Atları-Dijital Çağda Özel Yaşam Alanının Korunması", (Çev. Rabia Ünlü), **Alman-Türk Karşılaştırmalı Ceza Hukuku**, (Haz. Eric Hilgendorf, Yener Ünver), C.1, Yeditepe Üniversitesi Hukuk Fakültesi, İstanbul, 2010; Kudlich, Hans/ İlker Tepe: "Online Aramaların Uygulanabilirliği Üzerine", **Ceza Muhakemesi Önlemleri ve Özellikle Gizli Araştırma Önlemleri**, (Proje Yöneticisi: Kayıhan İçel, Edit.: Yener Ünver), Ankara, Seçkin Yayıncılık, 2011.

[217] 2006 yılında Almanya'da Federal Anayasa Mahkemesi'nin Kuzey Ren-Vestfalya Eyaleti Anayasayı Koruma Kanunu'nda yer alan internet içeriklerinin gizli şekilde takibi ve bilişim sistemlerine gizli erişim tedbirlerini içeren soruşturma tekniği maddelerinin şikayet konusu olduğu bir davayı görmüştür. Federal Anayasa Mahkemesi gizli internet içeriklerinin açığa çıkartılmasını haberleşmenin/telekomünikasyon gizliliğini ihlal olarak değerlendirmiştir. Söz konusu gizli içeriklerin ortaya çıkarılmasının yalnızca şüphelinin değil aynı zamanda üçüncü kişilerin de haklarını ihlal edebileceği ifade edilmiştir. İlgili kararın sistematik incelemesi için bkz. İlker Tepe, "Yeni Bir Temel

bilgisayarlarına sızmak için R2D2 olarak adlandırılan trojan casus yazılımı göndererek şüphelilerin e-postalarına, internet üzerinden yapılan görüşmelerine ulaşabilmektedir. Söz konusu casus yazılım ekran görüntüsünü kaydetme, kamera ve mikrofonu etkinleştirme özelliğine de sahiptir. Almanya dışında Avusturya, İsviçre, Hollanda'da çevrimiçi arama tedbirinin uygulandığı ortaya çıkmıştır. Yeterli yasal dayanak olmaksızın geniş siyasi iradeye dayanan bu çevrimiçi arama tedbirin uygulanması yasadışı hükümet fiili olarak değerlendirilmiş ve eleştirilmiştir. Kanunilik ilkesi gereğince kişilerin çevrimiçi arama tedbirinin ne zaman ve ne şartlarda uygulandığını bilmesi gerektiği ileri sürülmüş, belirlilik ve öngörülebilirliğin gereği olarak, soruşturmanın gizliliği de dikkate alındığında bu tedbirin uygulanmasında katı kurallara gidilmesi gerektiği belirtilmiştir[218]. Almanya'da 24 Ağustos 2017 tarihinden önce Alman Ceza Muhakemesi Kanunu'nda iletişimin denetlenmesi daha dar kapsamlıyken, Federal Ceza Polis Bürosu Kanunu[219] gereğince Polis Bürosu uluslararası terörizm suçlarıyla ilgili çevrimiçi arama tedbirini kullanmaya yetkiliydi. Alman Ceza Muhakemesi Kanunu'nda yapılan değişikliklerle kanun koyucu tarafından kolluk kuvvetlerinin çevrimiçi arama ve telekomünikasyonun denetlenmesine ilişkin tedbirlere yönelik yetkileri genişletilmiştir. Daha Etkin ve Uygulanabilir Bir Ceza Muhakemesi Tasarlama Yasası'nın 3'üncü maddesiyle[220] savcılara mahkeme kararına dayanarak telekomünikasyonun denetlenmesi çerçevesinde devlet trojanlarıyla şüpheliye ait bilişim sistemlerini denetleme yetkisi

---

Hak Olarak "Bilişim Teknolojisi Sistemlerinin Gizliliğinin ve Bütünlüğünün Korunması Hakkı"-Alman Federal Anayasa Mahkemesi'nin "Online Arama" Kararının Sistematik Analizi", **Karşılaştırmalı Güncel Ceza Hukuku Serisi (13)-İnternet Hukuku**, (Proje Yöneticisi: Kayıhan İçel, Editör: Yener Ünver), Ankara, Seçkin Yayıncılık, 2013, s.387-413.

[218] Basil Cupa, "Trojan Horse Resurrected - On The Legality Of The Use Of Government Spyware", **Living in Surveillance Societies: 'The State of Surveillance**, Edit. Webster, C William R. Living, Zurich Open Repository and Archive, University of Zurich, 2013, s.419-421.

[219] Yasanın orijinsal adı "Bundeskriminalamtgesetz" şeklindedir. İngilizce'ye "Act on the Federal Criminal Police Office" şeklinde geçmiştir. Bkz. Jenny Gesley, "Germany: Expanded Telecommunications Surveillance and Online Search Powers", Çevrimiçi, http://www.loc.gov/law/foreign-news/article/germany-expanded-telecommunications-surveillance-and-online-search-powers/, Erişim Tarihi: 13.02.2019.

[220] Yasanın orijinsal adı "Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" şeklindedir. İngilizce'ye "Act to Make Criminal Proceedings More Effective and Practicable" şeklinde geçmiştir. Bkz. Gesley, **a.g.e.**

verilmiştir[221]. Aynı maddenin devamında "*çevrimiçi arama*" tedbirinin insanlığa karşı suçlar, savaş suçları, saldırganlık, öldürme suçları gibi ağır suçlardan hırsızlık, kara para aklama, uyuşturucu madde suçlarına kadar geniş bir katalog suç yelpazesine uygulanabileceği hükme bağlanmıştır. Almanya'da bir görüşe göre; "*çevrimiçi arama*" tedbiri yalnızca terörle mücadele bakımından yeterli kamu yararını oluşturmaktayken, başka bir görüşe göre ise aşırıcılık ve organize suçlarla mücadelede de bu tedbirin uygulanmasında yeterli kamu yararını oluşturmaktadır[222]. Kanun koyucunun söz konusu düzenlemeye ilişkin iradesi pek çok kanattan eleştirilmiştir.

Çevrimiçi arama hakkındaki eleştiriler genellikle güvenliğin ve özel hayatın gizliliğinin tehlike altında olduğu yönündedir. Çevrimiçi arama için katalog suçların bu kadar geniş tutulması şüphesiz ki özel hayatın gizliliği, haberleşme özgürlüğü, bilişim sistemine duyulan güven gibi birçok hukuki değerin önemsenmemesi sonucunu doğuracaktır. Bu açıdan söz konusu tedbirin yalnızca kamu yararının çok yüksek olduğu terör suçları gibi ağır suçlarda ağır koşullara bağlı olarak uygulanması gerekmektedir. Öte yandan söz konusu trojanların devlet eliyle gönderilmesinin bilişim sistemi sahibinin haberi veya izni olmaksızın sistemdeki hata ve zayıflıkları kullanarak gerçekleştirilmesinin kötü niyetli olduğu kabul edilmelidir. Devletler çevrimiçi arama tedbirini bu şekilde uygulayarak bir nevi suçluluğu desteklemektedir[223].

Çevrimiçi arama tedbiriyle sağlık durumu, özel ilişkiler, malvarlığı bilgileri gibi pek çok bilgiye erişim sağlanmaktadır. Her ne kadar kamu yararı adına önemli bilgilere ulaşılsa da, söz konusu tedbirin kötüye kullanılması da çok olasıdır. Böyle bir tehlikenin varlığında "*gizlenmeye ihtiyacı olmayanın korkmaya da ihtiyacının*

[221] Alexander Duisberg, "Q&A: The use of court-ordered Trojans in Germany", Çevrimiçi, https://www.twobirds.com/en/news/articles/2017/germany/q-and-a-the-use-of-court-ordered-trojans-in-germany, Erişim Tarihi: 13.02.2019.
[222] Basil Cupa, **a.g.m.**, s.420.
[223] İlgili haber ve görüşler için bkz. Nicole Lorenz, " German party FDP also brings up constitutional complaint against federal trojan", Çevrimiçi, https://blog.avira.com/germany-constitutional-complaint-against-federal-trojan/, Erişim Tarihi: 13.02.2019.

olmadığı" yönünde bir görüş uygun değildir. Nitekim yukarıda da belirtildiği üzere, özel hayata ilişkin hakların ihlali gündeme gelebilecektir[224].

E. Hukuka Uygunluk Sebeplerinde Sınırın Aşılması

Bilişim sistemine girme suçu bakımından hukuka uygunluk sebeplerinde sınırın aşılması söz konusu olabilir. Örneğin rıza verilen kişinin rızanın sınırları dışına çıkması yahut hakkın kullanılması kapsamında özel hukuk sözleşmesinin tanıdığı hakların sınırının dışına çıkılması olasıdır.

Yine hukuka uygunluk sebeplerinden kanun hükmünün yerine getirilmesi bakımından da sınırın aşılması söz konusu olabilir. 5271 sayılı CMK uyarınca verilmiş koruma tedbirlerinde tedbirin konusu ve sınırları açıkça belirtilmelidir. Örneğin, 5271 sayılı CMK'nın 134'üncü maddesince verilecek bir kararda arama veya el koymanın bilgisayarda mı, bilgisayar kütüklerinde mi yoksa bilgisayar programlarında mı yapılacağı ve sistemin hangi kısmını kapsayan bir arama ya da el koymaya tabi olacağı belirtilmelidir. Aksi takdirde sınır aşılmış olacaktır[225].

TCK'nın 27'inci maddesinin 1'incı fıkrasına göre "*Ceza sorumluluğunu kaldıran nedenlerde sınırın kast olmaksızın aşılması halinde, fiil taksirle işlendiğinde de cezalandırılıyorsa, taksirli suç için kanunda yazılı cezanın altıda birinden üçte birine kadarı indirilerek hükmolunur"*. Fail, bir hukuka uygunluk sebebinin sınırını taksirli hareketi sonucu aşıyorsa, bilişim sistemine girme suçunun taksirli hali düzenlenmediği için cezalandırılmayacaktır. Ancak sınırın kasten aşılması halinde failin cezai sorumluğu aynen devam edecektir[226].

Bilişim sistemine karşı gerçekleşen veya gerçekleşmesi ya da tekrarı muhakkak olan bir siber saldırıya karşı meşru savunmanın mümkün olduğu kabul edilen hallerde sınırın aşılması halinde ise "*sınırın aşılması mazur görülebilecek bir*

[224] Kudlich, **a.g.m.**, s.215-223.
[225] Apiş, **a.g.m.**, s.80.
[226] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.287-288.

heyecan, korku veya telaştan ileri gelmiş ise" TCK'nın 27/2 fıkrası gereğince ceza verilmeyecektir.

ÜÇÜNCÜ BÖLÜM

SUÇUN NİTELİKLİ HALLERİ, FİİL SEBEBİYLE BİLİŞİM SİSTEMİNDE YER ALAN VERİLERİN YOK OLMASI VEYA DEĞİŞMESİ, KUSURLULUK, SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ, MUHAKEME KURALLARI, ZAMANAŞIMI VE YAPTIRIM

I. NİTELİKLİ HALLER

A. Suçun Bedeli Karşılığı Yararlanılabilen Sistemler Hakkında İşlenmesi

TCK'nın 243'üncü maddesinin 2'nci fıkrasında "*Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir*" düzenlemesine yer verilmiştir. Kanuni düzenlemede yer verilen "*yukarıdaki fıkrada tanımlanan fiiller"* ifadesi bilişim sisteminin tamamına veya bir kısmına hukuka aykırı olarak girme veya kalma fiilini karşılamaktadır. Doktrinde, 2016 değişikliğinden önceki düzenlemede, yani "*girme ve kalma*" hareketlerinin bağlı hareketli suç oluşturduğu dönemde yukarıda anılan "*tanımlanan fiiller*" ifadesi eleştirilmiş, bunun yerine "*tanımlanan suçun*" ifadesi kullanılması gerektiği belirtilmiştir[1]. Mevcut düzenlemede bilişim sistemine girme ile sistemde kalma fiilleri seçimlik hareketli suç oluşturduğu için düzenleme bu yönüyle yerindedir.

[1] Karagülmez, **a.g.e.**, s.208.

Düzenlemeye göre genel olarak herkesin erişimine açık olmayan ve belirli bir bedel karşılığı kullanıcıların erişimine açılan bilişim sistemlerine hukuka aykırı olarak giren veya burada kalan failin cezası hâkim tarafından yarı oranına kadar indirilecektir.

Söz konusu daha az cezayı gerektiren nitelikli hale ilişkin fıkrada ve gerekçesinde bedeli karşılığı yararlanılabilen sistemlere girmenin veya orada kalmanın neden indirim sebebi olarak düzenlendiğine yer verilmemiştir. Doktrinde ise bedeli karşılığı yararlanılabilen sistemlere girme veya kalma fiillerinin cezanın indirilmesini gerektiren bir nitelikli hal olarak düzenlenmesi hakkında bazı değerlendirmelere yer verilmiştir. Bazı yazarlar bedeli karşılığı yararlanılabilen sistemlere girme veya orada kalmanın cezanın arttırılmasını gerektirecek bir nitelikli hal olduğunu ileri sürmüşleridir[2]. Bir görüşe göre, bu nitelikli hal ile hem bilişim sistemine girme suçunun temel halinde korunan hukuki değeri yani bilişim sisteminin güvenliği hem de bedeli ödenmeksizin sisteme girme veya kalma söz konusu olduğu için bilişim sistemi sahibinin veya kullanıcısının malvarlığından kaynaklanan hakları ihlal edilmektedir[3]. Bu görüş, suç ve yaptırım teorisi gereğince iki farklı hukuki değer ihlal edildiği için bu nitelikli halin cezanın indirilmesini değil artırılmasını gerektiren bir nitelikli hal olarak düzenlenmesi gerektiğini ve mevcut düzenlemenin adeta faili ödüllendirdiğini savunmaktadır[4].

---

[2] Tezcan/Erdem/Önok, **a.g.e.**, 982; Cengiz Apaydın, "Bilişim Sistemine Girme Suçu", **TAAD**, Yıl:7, Sayı:24, Ocak 2016, s. 272.

[3] Nitelikli halin uygulanması bakımından bilişim sistemini kullanım için belirlenen bedelin ödenme zamanının suça etki edip etmediği tartışılmıştır. Bir görüşe göre, fail bedeli ödedikten sonra kullanma süresi sona erdikten sonra sisteme girerse fail daha önceden de sisteme girmek için gerekli araçlara sahip olduğu için hafifletici bir sebep olabilir. Ancak hiç ödeme yapılmadan bu sistemlere girilmesi halinde bilişim sistemi sahibi ekonomik zarara uğrayacağı için cezanın ağırlaştırılması gerekir. Dülger, **Bilişim Suçları**, s. 227. Dülger, ilk basısındaki bu görüşe daha sonra yer vermemiştir.
Ancak bilişim sistemine bedeli ödendikten sonra girilmesi zaten suç oluşturmayacaktır. Bilişim sistemi sahibi de bedeli geri ödemeksizin sisteme girme hakkını suçlama hakkına sahip olmayacaktır. Bu sebeple bedelin ne zaman ödendiğinin suçun ağırlığına bir etkisi bulunmamaktadır. Pallı, **a.g.m.**, s.155.

[4] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.272. Aynı yönde, Taşkın, **Bilişim Suçları**, s.36.
Doktrinde yer alan benzer bir görüş, söz konusu nitelikli hal ile bilişim sistemi sahibinin, sisteminin bedel ödenmeden kullanılmasından kaynaklanan haklarının ve sistem üzerindeki haklarının ihlal edildiği dikkate alındığında bedeli karşılığı yararlanılabilen sistemlere girme veya orada kalma fiillerinin hafifletici sebep olarak kabul edilmesi ile ihlal edilen korunan hukuki değerler çelişki içinde olduğunu savunmaktadır. Dolayısıyla böyle bir hafifletici sebep düzenlemesine ihtiyaç yoktur. Bkz. Özbek v.d., **a.g.e.**, s.952; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1400.

Cezanın indirilmesini gerektiren bu nitelikli hali yerinde bulan görüşler de bulunmaktadır. Bu görüşlerin temelinde 243'üncü maddenin 1'inci fıkrasına konu olan kamunun kullanımına tamamen kapalı bir bilişim sistemindense bedeli ödendiği takdirde erişimi herkes tarafından mümkün olan bilişim sistemlerinin[5] suçun konusunu oluşturması gerekçesi yatmaktadır[6]. Dolayısıyla korunan hukuki değerin önemi ve niteliği farklılık arz etmektedir[7]. Cezanın indirilmesini yerinde bulan bir diğer görüşe göre, bilişim sistemine girme suçunun temel halinde bilişim sisteminin güvenliğinin yanında bireylerin mahremiyeti korunurken bedeli karşılığı yararlanılabilen sistemlerde ekonomik yararlar korunmaktadır[8].

Benzer bir görüşe göre, bedeli karşılığı yararlanılabilen sistemlere giren kişi, içerik sahibinin gizli bilgilerini değil bedel karşılığı herkes tarafından erişilebilen bilgileri öğrendiği için kanun koyucu bilişim sistemi sahibinin ekonomik değerlerinin korunması amacıyla böyle bir nitelikli hal düzenlemesine gitmiştir[9]. Bir görüş nitelikli hali işin mahiyeti itibariyle yerinde bulsa da, düzenlemede yer verilen bedeli karşılığı yararlanılabilen sistemlerle sınırlı tutulan bu nitelikli halin suçla korunan alan bakımından caydırıcılığı azalttığını savunmaktadır[10]. Düzenlemenin temelinde kamuya açık olan bilişim sistemine girmenin indirim sebebi olduğu gerekçesi olduğunu savunan bu görüş, bedel ödenmeksizin belirli kişilerin kullanımına açık olan bilişim sistemlerine girme veya kalma fiilinin 243'üncü maddenin 2'nci maddesine

---

Benzer şekilde Dülger de bu nitelikli halin kanun değişikliğiyle ya kaldırılması gerektiğini ya da Yazar'a göre daha doğru olacak şekilde cezayı ağırlaştıran bir nitelikli hal olarak düzenlenmesi gerektiğini savunmaktadır. Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.272.

[5] Dülger, bu nitelikli halin bedeli ödendiği takdirde bilişim sisteminin herkese açık olması gerekçesine dayandırılmasını eleştirmektedir. Yazar'a göre kamuya açık yerlere izinsiz girmek mümkün olamayacağından kamuya açık yerlere girmek suç oluşturmayacağı gibi kamunun veya bazı kişilerin kullanımına açılmamış yerlere girilmesi de cezanın indirilmesini gerektiren bir nitelikli hal olarak değerlendirilemez. Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.271.

[6] Bkz. Mahmutoğlu, **a.g.m.**, s.863; Soyarslan, **a.g.e.**, s.640; Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**,s.816; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 63-64.

[7] Karagülmez, **a.g.e.**, s.211.

[8] Artuk/Gökcen/Yenidünya, **a.g.e.**, s.847; Levent Kurt, **Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yayıncılık, 2005, s.147; Yazıcıoğlu, **Hackerler ve Bilişim Sistemine Girme Suçu**, s.1259; Yaşar/Gökcan/Artuç, **a.g.e.**, s.7295.

[9] Karakehya, **a.g.e.**, s.18, dn.49. Dülger, malvarlığına ilişkin hakların daha önemli olduğunu dolayısıyla düzenlemeyi bu gerekçeyle savunmanın mümkün olmadığını ifade etmiştir. Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.272.

[10] Karagülmez, **a.g.e.**, s.210.

girmemesinin de adalet duygusunu sarstığını ileri sürmüştür[11]. Doktrinde bilişim sisteminin bir bedel karşılığı olup olmadığına bakılmaksızın kamu kurumlarına ait bilişim sistemlerine girme veya orada kalma ile özel hukuk kişilerine ait bilişim sistemlerine girme veya orada kalma fiili arasında bir ayrım yapılması gerektiği savunulmaktadır[12].

Akbulut, cezayı azaltan nitelikli hal için suçu oluşturan seçimlik hareketleri dikkate alarak bir değerlendirme yapmıştır. Yazar'a göre, TCK'nın konut dokunulmazlığını ihlal suçunun daha az cezayı gerektiren nitelikli halini düzenleyen 116'ıncı maddesinin 2'nci fıkrasında yer alan işyeri ve eklentilerine rızaya aykırı şekilde girme ve çıkma fiilleri bedeli karşılığı yararlanılabilen sistemlere girme veya orada kalma suçuyla benzerlik gösterse[13] de konut dokunulmazlığından farklı olarak bedeli karşılığı yararlanılabilen bilişim sistemlerinde kalma fiilinde ekonomik yarar sağlanması söz konusudur[14]. Dolayısıyla daha az cezayı gerektiren bu nitelikli halin değerlendirilmesinde bedeli karşılığı yararlanılabilen sistemlere girme fiili ile burada kalma fiili aynı şekilde nitelendirilemez. Yazar'a göre, bedeli karşılığı yararlanılabilen sistemlerde kalma fiili bilişim sistemi sahibinin ekonomik menfaatlerini de ihlal ettiği için daha az cezayı gerektiren bir nitelikli hal olarak kabul edilemez[15]. Dolayısıyla kanun koyucu bedeli karşılığı yararlanılabilen bilişim sistemlerine girme ve burada kalma arasındaki ayrımı gözeterek ya bu fiilleri bağımsız şekilde ele alarak bir düzenleme yoluna gitmeli ya da bedeli karşılığı yararlanılabilen sistemlerinde kalma fiilini 244'üncü maddenin 1'inci ve 2'nci fıkralarında yer alan suç tiplerini de

[11] **A.e.**, s.210-211; Taşkın, **Bilişim Suçları**, s.35-36.
[12] Ketizmen, **a.g.e.**, s.110; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1400; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 67.
[13] Dülger, korunan hukuki değerler farklı olduğu için, bu nitelikli halin konut dokunulmazlığını ihlal suçuna benzetmeyi doğru bulmamaktadır. Bedeli karşılığı yararlanılabilen sistemler ancak birçok fakülteyi bir arada bulunduran bir kampüse benzetilebilir. Bu durumda da benzer düzenlemeler olduğu düşünüldüğünde, okulda ders dinlemeye yetkili kişinin dekanın odasında hırsızlık yapmasının cezanın indirilmesini gerektiren bir neden olarak düzenlenmesi gibi bir sonuç ortaya çıkacaktır. Dolayısıyla bedeli karşılığı yararlanılabilen sistemlere girme veya kalma fiilinin cezanın indirilmesine sebep olan bir nitelikli hal olarak kabul edilmesi doğru bir yaklaşım değildir. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7),** s.270. Benzer görüşler için bkz. Taşkın, **Bilişim Suçları**, s. 35-36.
[14] Akbulut, **Bilişim Alanında Suçlar**, s.142. Ketizmen ise 5237 sayılı TCK'nın 163'üncü maddenin 2'nci fıkrasında yer alan karşılıksız yararlanma suçunun yaptırımıyla paralellik kurulası açısından kanun koyucunun böyle bir nitelikli hale yer verdiği sonucuna ulaşmaktadır. Ketizmen, **a.g.e.**, s.111.
[15] Akbulut, **Bilişim Alanında Suçlar**, s.143.

kapsayacak ancak bununla sınırlı olmayacak şekilde 244'üncü maddenin 4'üncü fıkrasında yer alan bilişim sistemleri aracılığıyla haksız yarar sağlama suçu altında ele alınmalıdır[16].

Bedeli karşılığı yararlanılabilen bilişim sistemlerine girme veya orada kalma suçunun cezanın hafifletilmesini sağlayan bir nitelikli hal olarak düzenlenmesi suçla korunan hukuki değerin yarattığı bir farklılığın sonucudur. Bedeli olsun yahut olmasın bu suç tipiyle korunmak istenen temel hukuki değer bilişim sisteminin güvenliği ve güvenilirliğidir. Belirli bir kesime açık veya kapalı olması bilişim sisteminin güvenliği ve güvenilirliğinin korunan hukuki değer olmasını ortadan kaldırmayacağı gibi, önemini de azaltmayacaktır. Bedeli karşılığı yararlanılabilen bilişim sistemlerine girme ve orada kalma fiilleri hem temel hal hem de nitelikli hal ile korunan hukuki değer açısından ayrı ayrı değerlendirmeye muhtaçtır. Bedeli ödenmeksizin bir bilişim sistemine girme ve orada kalma fiili bedel olarak istenen şeyin niteliğine de bağlı olarak bilişim sistemi sahibinin ve zilyedinin malvarlığı haklarını ihlal edici niteliktedir. Dolayısıyla bedeli ödenmeksizin bir bilişim sisteminde kalma fiilinin cezayı hafifleten değil ağırlaştıran bir nitelikli hal olarak düzenlenmesi gerekmektedir[17].

B. Bilişim Sistemine Girme Suçunun Terör Amacıyla İşlenmesi

3713 sayılı Terörle Mücadele Kanunu'nun 4'üncü maddesi uyarınca bu maddede sayılan suçların "*cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasada belirtilen Cumhuriyetin niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devletinin ve Cumhuriyetin varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu*

[16] **A.e.**
[17] Aynı yönde; Akbulut, **Bilişim Alanında Suçlar**, s.143.

düzenini veya genel sağlığı bozmak amacıyla"[18] işlenmesi halinde bu suçlar "*terör amacı ile işlenen suçlar*"[19] olarak kabul edilmektedir.

Söz konusu 4'üncü maddede terör amacıyla işlenen suçlar arasında TCK'nın 243'üncü maddesi de sayılmıştır. Bu sebeple bilişim sistemine girme suçu terör amacıyla işlenirse 3713 sayılı Terörle Mücadele Kanunu'nun 5'inci maddesi uyarınca cezası ağırlaştırılacaktır[20].

II. FİİL SEBEBİYLE BİLİŞİM SİSTEMİNDE YER ALAN VERİLERİN YOK OLMASI VEYA DEĞİŞMESİ

TCK'nın 243'üncü maddesinin 3'üncü fıkrasında "*bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur*" düzenlemesine yer verilmiştir.

Maddenin gerekçesine göre "*üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir*". Dolayısıyla düzenlemede yer alan "*bu fiil nedeniyle*" ifadesinden bilişim sistemine girme suçunun temel halinde yer alan fiiller yani bilişim sistemine girme veya burada kalma fiilleri kastedilmektedir. 243'üncü maddenin bütünü dikkate alındığında TBMM Genel Kurulu'nda TCK tasarısında yapılan değişiklikler ve 2016 değişikliği sonucu ortaya çıkan bazı ifade sorunları burada da

[18] 3713 sayılı Terörle Mücadele Kanunu'nun 1'inci maddesinde "Terör Tanımı" yapılmıştır. Bir örgüte mensup kişi veya kişilerin yukarıda belirtilen amaçlarla işlediği her türlü suç terör eylemi kapsamında değerlendirilmiştir. 29/6/2006 tarihli ve 5532 sayılı Kanunun 1 inci maddesiyle, 1 inci maddenin başlığı ''Terör ve örgüt tanımı", 4 üncü maddenin başlığı "Terör amacı ile işlenilen suçlar" iken, metne işlendiği şekilde değiştirilmiştir.

[19] 4'üncü maddenin başlığı Kanun'un önceki halinde "Terör amacı ile işlenilen suçlar" iken 29/6/2006 tarihli ve 5532 sayılı Kanunun 1 inci maddesiyle "Terör amacı ile işlenen suçlar" şeklinde değiştirilmiştir.

[20] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 274.

görülmektedir. Seçimlik hareketli bir suç olması sebebiyle "*bu fiil nedeniyle*" ifadesi yerine "*bu fiiller nedeniyle*" ifadesinin kullanılması daha açık ve doğru olacaktır.

Doktrinde fiil sebebiyle sistemin içerdiği verilerin yok olması veya değişmesini ayrı bir suç olarak değerlendiren görüşler olduğu gibi, suçun nitelikli hali olduğunu ifade eden yazarlar da bulunmaktadır. Bir görüşe göre verilerin yok olması veya değişmesi failin taksirli hareketin neticesi olması sebebiyle bu suç bağımsız bir suçtur. Suçun özel bir neticesi sebebiyle ağırlaşmış hal olarak yaptırımının suçun temel halinden bağımsız şekilde gösterilmesi sebebiyle de bu suçun bağımsız bir suç oluşturduğu savunulmaktadır[21]. Söz konusu fıkrayı nitelikli hal olarak ele alan yazarlar[22] da bulunmaktadır.

Doktrinde çoğunlukta olan ve katıldığım görüş ise, verilerin yok olması veya değiştirilmesinin bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali olduğu görüşüdür. Söz konusu fıkranın uygulanabilmesi için failin 243'üncü maddenin 1'inci fıkrasında yer alan fiilleri kasten gerçekleştirmesi sonucunda taksirle sistem içindeki verilerin yok olması veya değişmesi gerekmektedir. Dolayısıyla 3'üncü fıkrada yer alan düzenlemede yer alan neticesi sebebiyle ağırlaşmış suçun unsurları suçun temel şekliyle ortaklık göstermektedir. Nitekim 243'üncü maddenin 3'üncü fıkrasında yer alan "*bu fiil sebebiyle*" ifadesi birinci fıkraya atıf yapmaktadır. Dolayısıyla bu fıkranın suçun temel halinden bağımsız bir suç olduğunu kabul etmek doğru değildir[23]. Maddenin gerekçesinde de "*birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde*" diyerek bilişim sistemine girme suçunun temel şekli olan 1'inci fıkraya atıf yapılmıştır.

Bilişim sistemine giren veya orada kalmaya devam eden failin verilerin yok olması ve değişmesinde kastı bulunmaması gerektiği maddenin gerekçesinde açıkça ifade edilmiştir[24]. Neticesi sebebiyle ağırlaşmış suçu düzenleyen TCK'nın 23'üncü maddesi gereğince "*Bir fiilin, kastedilenden daha ağır veya başka bir neticenin*

[21] Özbek v.d., **a.g.e.**, s.951.
[22] Tezcan/Erdem/Önok, **a.g.e.**, 982; Esen, **a.g.e.**, s.630.
[23] Aynı yönde; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 69; Apaydın, **Bilişim Sistemine Girme Suçu**, s. 274.
[24] Yılmaz, **a.g.e.**, s.187.

oluşumuna sebebiyet vermesi hâlinde, kişinin bundan dolayı sorumlu tutulabilmesi için bu netice bakımından en azından taksirle hareket etmesi gerekir". Ancak burada failin verilerin yok olması veya değişmesinde kastı bulunduğu takdirde neticesi sebebiyle ağırlaşmış suç değil, TCK'nın 244'üncü maddesinin 2'nci fıkrası uygulama alanı bulacaktır. Dolayısıyla faili 243'üncü maddenin 3'üncü fıkrasından sorumlu tutabilmek için bilişim sistemine girme ve orada kalma açısından failin kastı aranırken, verilerin yok olması veya değişmesi neticeleri bakımından sadece taksirinin bulunması gerekir[25]. Nitekim kanun koyucunun kullandığı "*veriler yok olur veya değişirse*" ifadesi faili pasif konumda nitelendirmiş ve fiile vurgu yapmıştır[26].

Söz konusu fıkra uyarınca verilerin yok olması ve değişmesi seçimlik neticeler olup, failin neticesi sebebiyle ağırlaşmış suçtan sorumlu tutulabilmesi için neticelerden birinin gerçekleşmesi yeterlidir[27]. Failin kasten ve hukuka aykırı şekilde bilişim sistemine girmesi veya orada kalması sonucu taksirle her iki neticenin de gerçekleşmesine sebep olması halinde, hâkim somut olaya göre failin cezasını TCK'nın 61'inci maddesinin e ve f fıkraları uyarınca failin meydana getirdiği "*zarar veya tehlikenin ağırlığı*" ve "*failin kast ve taksire dayalı kusurunun ağırlığına*" göre belirleyecektir[28].

Neticesi sebebiyle ağırlaşmış halden sorumluluğun doğabilmesi için önce suçun temel halin gerçekleşmesi gerekmektedir. Failin kast olmaksızın bilişim sistemine girmesi veya orada kalması halinde suçun temel hali oluşmayacağı için taksiri sebebiyle sistemde yer alan verilerin yok olması veya değişmesi halinde de failin sorumluluğu doğmayacaktır[29]. Söz konusu halde neticesi sebebiyle ağırlaşmış suçun düzenlendiği 243'üncü maddenin 3'üncü fıkrası uygulanamayacağı gibi, 244'üncü maddenin 2'nci fıkrasında yer alan suçun da kasten işlenebilen bir suç olduğu dikkate alındığında fail sebep olduğu bu neticeden dolayı cezalandırılamayacaktır[30].

---

[25] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 70.
[26] Karagülmez, **a.g.e.**, s.212.
[27] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 70.
[28] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 70.
[29] Parlar, **a.g.e.**, s.19; Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 71.
[30] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 71.

Doktrinde kast olmaksızın bilişim sistemindeki verilerin yok olması ve değişmesi seçimlik neticelerine ek olarak, Fransız Ceza Kanunu'nun 323-1'inci maddesinde de yer alan "*bilişim sisteminin işleyişinin herhangi bir şekilde değişimine neden olunması*" seçimlik neticesinin de fıkraya eklenmesi gerektiği savunulmaktadır. Nitekim bilişim sisteminin işleyişinin engellenmesi veya bozulması da en az verilerin yok olması veya değişmesi kadar önemli ve ağır neticelerdir[31]. Dolayısıyla bu ağır neticelere yol açacak taksirli hareketlerin de ceza hukukunca korunması gerekir.

Bir görüş, bilişim sistemine giren failin taksirli hareketiyle bilişim sisteminde bir açık oluşturarak bilişim sistemini başkalarının erişimine olanak sağlaması neticesinin de suça etki eden bir hal olarak düzenlenmesi gerektiğini savunmaktadır. Çünkü failin taksirli hareketi sonucu başkalarının bilişim sistemine erişebilmesi 3'üncü fıkradan nitelik itibariyle farklı olarak başkaları tarafından verilerin elde edilmesi tehlikesini ortaya çıkarmaktadır[32]. Söz konusu sistem açığına taksirle sebebiyet verilmesi halinde her ne kadar üçüncü kişilerin bu verilere ulaşması farklı suçların oluşumuna sebebiyet verebilecek olsa da, sistemdeki bu verilere ulaşılmasına yol açan kişinin yarattığı zarar tehlikesi de dikkate alınarak failin bu taksirli hareketinin de cezayı ağırlaştıran hal olarak düzenlenmesi önem arz etmektedir.

III. KUSURLULUK

Kusurluluk, suçu oluşturan fiilin bir unsuru değildir[33]. Failin işlediği suç sebebiyle kusurlu olup olmaması, söz konusu suçu oluşturan fiilin oluşturduğu haksızlık üzerinde etki doğurmayacaktır[34]. TCK'nın 24 ile 34'üncü maddesi aralığında kusurluluğu azaltan ve kaldıran sebeplere yer verilmiştir. Bunlar; yaş küçüklüğü (m. 31), akıl hastalığı (m. 32), sağırlık ve dilsizlik (m.33), geçici nedenler,

[31] Karagülmez, **a.g.e.**, 207.
[32] **A.e.**
[33] Özgenç, **a.g.e.**, s.390. Karakehya, kusurluluğu kaldıran hallerden birinin bulunması halinde suç oluşmayacağı görüşünde olup, bilişim sistemine girme suçunu işleyen kişinin kusurluluğunun bulunmaması halinde cezai sorumluluğunun bulunmadığını ileri sürmüştür. Bkz. Karakehya, **a.g.e.**, s.15.
[34] Özgenç, **a.g.e.**, s.390.

alkol veya uyuşturucu madde etkisinde olma (m.34) [35], cebir veya tehdit dolayısıyla kişinin irade yeteneğinin etkilenmesi (m. 28), zorunluluk hali dolayısıyla kişinin irade yeteneğinin etkilenmesi (m. 25/2; m.92; m.99/2; m.143), hukuka aykırı ve fakat bağlayıcı emrin yerine getirilmesi (m. 24/2; m.24/4), haksız tahrik (m.29) ve çeşitli hata halleri (m.30/3; m.30/4) olarak sayılabilir[36]. Bilişim sistemine girme suçu bakımından hukuka aykırı fakat bağlayıcı emrin yerine getirilmesi hariç kusurluluğu azaltan ve kaldıran sebeplerin hepsinin gündeme gelebilmesi mümkündür. Bununla birlikte cebir veya tehdit ile zorunluluk haline ve hukuka aykırı fakat bağlayıcı emrin yerine getirilmesi haline ayrıca değinilebilir.

Kişinin karşı koyması veya kurtulması mümkün olmayan bir cebir ve şiddet altında ya da muhakkak ve ağır bir korkutma veya tehdit sebebiyle hukuka aykırı şekilde başkasına ait bir bilişim sistemine girmesi veya orada kalması halinde TCK'nın 28'inci maddesi gereğince ceza verilmeyecektir. Örneğin; bir bilişim uzmanı kafasına silah dayanması sebebiyle bilişim uzmanı başkasına ait bilişim sistemine girmiş veya bilişim sisteminde kalmışsa bu durumda bilişim uzmanının kusurluluğunun kalktığından bahisle bilişim uzmanının cezalandırılması gündeme gelmeyecektir. Ancak TCK'nın 28'inci maddesi gereğince cebir veya tehdit yoluyla faili suç teşkil eden fiili işlemeye zorlayan kişinin dolaylı fail olarak sorumluluğu oluşacaktır.

Kişinin cebir ve tehdit altında bilişim sistemine girmesi veya orada kalması neticesinde kusurluluğunun ortadan kalkması için kendisine karşı kullanılan cebir veya tehdidin hangi hukuki değere yönelik olduğu önem arz etmektedir. Maruz kalınan cebir veya tehdidin, yapılması zorlanan haksız davranışı gerçekleştirmeye mecbur edecek ağırlıkta ve irade özgürlüğünü kaldırıcı nitelikte olup olmadığı normatif bir değerlendirme sonucu tespit edilebilecektir. Örneğin; ölümle tehdit edilen bir kişinin bilişim sistemine girme suçunu işlemesi halinde yaşam hakkı bilişim sisteminin

[35] Belirtmek gerekir ki, fail hakkında TCK'nın 34'üncü maddenin uygulanabilmesi için failin kusur yeteneğini ortadan kaldıran durumun oluşmasında kastının veya taksirinin bulunmaması gerekmektedir. Bkz. Serdar Talas, " Ceza Hukukunda Kusur İlkesi Bağlamında Nedeninde Serbest Hareket (actio libera in causa) Kavramı ve Geçici Nedenlerin Ceza Sorumluluğuna Etkisi", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011, s.171 vd.
[36] Özgenç, **a.g.e.**, s.403.

güvenliğinden öncelikli olduğu için söz konusu tehdit failin kusurluluğunu ortadan kaldıracaktır[37].

TCK'nın 25'inci maddesinin 2'nci fıkrasında zorunluluk hali düzenlenmiştir. Buna göre failin kendisinin bilerek sebep olmadığı ve başka türlü kurtulma imkânın olmadığı, kendisinin veya başkasının bir hakkına yönelik ağır ve muhakkak tehlikeden korunmak için işlediği fiillerin orantılı olması halinde fail cezalandırılmamaktadır. Buna göre, failin TCK'nın 25'inci maddesinin 2'nci fıkrasında yer alan şartlara da bağlı olarak bir tehlikeden korunmak için bilişim sistemine girmesi veya orada kalması halinde failin cezalandırılmaması mümkündür. Yangın çıkan bir binada mahsur kalan ve yanında hiçbir iletişim aracı olmayan kişinin, o sırada binada dumandan zehirlenmiş ve baygın halde bulunan başka bir kişinin akıllı telefonunu o kişinin parmak izini kullanarak açması ve akıllı telefon aracılığıyla yardım çağrısında bulunması örneğinde zorunluluk halinin bütün şartlarının sağlanması durumunda fail bilişim sistemine girme suçundan dolayı cezalandırılmayacaktır.

Hukuka aykırı bağlayıcı emirin yerine getirilmesini düzenleyen TCK'nın 24'üncü maddesinin 3'üncü fıkrası uyarınca amiri tarafından emredilse dahi konusu suç teşkil eden bir fiilin kamu görevlisi tarafından işlenmesi halinde kamu görevlisinin de cezai sorumluluğu gündeme gelecektir[38]. Örneğin; 5271 sayılı CMK'nın 134'üncü maddesine uygun olarak verilmiş bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama kararı olmadığı bilindiği halde, kolluk amirinin kolluğa bilgisayarlarda arama emri vermesi halinde emri veren amirin de işlemi gerçekleştiren kolluğun da bilişim sistemine girme suçundan sorumluluğu doğabilecektir.

Kusurluluğu kaldıran veya azaltan hallerde hataya düşmesi halinde ise TCK'nın 30'uncu maddesinin 3'üncü fıkrası gereğince failin hatasının kaçınılmaz olması halinde fail bu hatasından yararlanacaktır.

[37] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 291-292.
[38] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 292.

IV. SUÇUN ÖZEL GÖRÜNÜŞ BİÇİMLERİ

A. Teşebbüs

Bilişim sistemine girme suçunu düzenleyen TCK'nın 243'üncü maddesinin 24.03.2016 tarihinden önceki halinde bilişim sistemine girme ve orada kalma fiilleri çok hareketli suç oluşturduğu için teşebbüs değerlendirmesi mevcut düzenlemeden farklı bir değerlendirmeyi gerektirmekteydi. Eski düzenlemeye göre yapılan teşebbüs değerlendirmesi de doktrinde farklı görüşleri beraberinde getirmekteydi.

Bir görüşe göre, bilişim sistemine giren kişi aynı zamanda bilişim sisteminde kalmış olacağından bu suça teşebbüsün mümkün olmayacağı ileri sürülmekteydi[39]. Başka bir görüşe göre ise, ilk hareketin yani bilişim sistemine girmenin gerçekleştirilmesinden sonra ikinci hareket olan bilişim sisteminde kalma fiili gerçekleştirilememişse suç teşebbüs aşamasında kalmış sayılmalıydı[40]. Buna göre fail bilişim sistemine girmeyi başarmış fakat elinde olmayan sebeplerle bilişim sisteminde kalamamışsa suç teşebbüs aşamasında kalmıştır. Fakat fail bilişim sistemine girdikten sonra kendisi bilişim sisteminde kalmak istememişse burada teşebbüs değil gönüllü vazgeçmenin söz konusu olması gerektiği savunulmaktaydı[41]. Bir görüş ise, bilişim sistemine giren kişinin kalma fiilini gerçekleştirip gerçekleştiremediğinin takdirini hâkim yapmalı, buna göre failin fiilinin teşebbüs aşamasında mı kaldığına yoksa tamamlanmış suç gibi cezalandırılması gerektiğine karar verilmeliydi[42].

6698 sayılı Kanun ile 24.03.2016 tarihinde yapılan değişiklik sonrasında bilişim sistemine girme ve orada kalma fiilleri seçimlik hareketli suç oluşturacak şekilde düzenlendiği için doktrindeki görüşler de yeniden şekillenmiştir.

---

[39] Taşkın, **Bilişim Suçları**, s.30; Parlar, **a.g.e.**, s.18.
[40] Karagülmez, **a.g.e.**, s.19. Karagülmez ise, sisteme girmeye çalışmak veya sistemde kalmayı başaramamayı da teşebbüs hali olarak değerlendirmiştir.
[41] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1414.
[42] Karagülmez, **a.g.e.**, s.171.

Bir görüşe göre bu suça teşebbüs mümkün değildir. Çünkü bu suç bir tehlike suçudur. Dolayısıyla girme veya kalma fiillerinin gerçekleştirilmesiyle suç tamamlanır[43].

Başka bir görüşe göre ise, bilişim sistemine girme ve bilişim sisteminde kalma fiilleri için teşebbüsün ayrı ayrı değerlendirilmesi gerekir[44]. Eğer hukuka aykırı şekilde bilişim sistemine girme fiili gerçekleştirilmişse artık suç tamamlanmış olacağından ayrıca bilişim sisteminde kalma için teşebbüs değerlendirmesi yapmaya gerek yoktur. Ayrıca belirtmek gerekir ki failin kastı bilişim sisteminin tamamına girmeye yönelik olsa da failin bilişim sisteminin bir kısmına girmesi halinde dahi suç tamamlanmış olacaktır[45].

Bilişim sistemine girme fiili açısından teşebbüs mümkündür. Fail bilişim sistemine girmeye çalışırken elinde olmayan sebeplerle bilişim sistemine giremezse suç teşebbüs aşamasında kalacaktır[46]. Örneğin; fail bilişim sistemine girmeye yönelik icra hareketlerine başlamasına rağmen güvenlik önlemlerine takılması[47] veya elektriklerin kesilmesi sonucunda[48] sisteme giremezse suç teşebbüs aşamasında kalır. Bu bakımdan teşebbüs TCK'nın 243'üncü maddesinin 1'inci fıkrasında düzenlenen suçun temel şeklinde yer alan bilişim sistemine girme fiili ve 2'nci fıkrasında düzenlenen "*bedeli karşılığı yararlanılabilen sistemlere girme*" fiili için geçerlidir[49].

Bilişim sisteminde kalmaya devam etme fiili bakımından teşebbüsün mümkün olup olmayacağıyla ilgili değerlendirme yapılması gereken husus hukuka uygun şekilde bilişim sistemine girildikten sonra hukuka aykırı olarak kalınması halidir. Bu bakımdan teşebbüs mümkün değildir. Hem bilişim sistemine girme hem de bilişim sisteminde kalma fiili açısından bir netice aranmasa da girme fiilinin icra hareketleri kısımlara bölünebilir nitelikteyken, kalma fiili için bu mümkün değildir. Yani bilişim

[43] Yılmaz, **a.g.e.**, s.190.
[44] Özbek v.d., **a.g.e.**, s.955.
[45] Akbulut, **Bilişim Alanında Suçlar**, s.150; Tezcan/Erdem/Önok, **a.g.e.**, 984.
[46] Failin hareketinin neticeyi meydana getirmeye getirme gücünün tespiti somut olaya göre ex-ante bir değerlendirmeyle tespit edilir. Adem Sözüer, **Suça Teşebbüs**, İstanbul, Kazancı, 1994, s.187.
[47] Esen, **a.g.e.**, s.631; Özbek v.d., **a.g.e.**, s.955.
[48] Soyaslan, **a.g.e.**, s.638.
[49] Akbulut, **Bilişim Alanında Suçlar**, s.151.

sisteminde bir an dahi olsa hukuka aykırı olarak kalınmışsa suç tamamlanmış sayılacaktır[50]. Doktrinde bir görüşe göre bilişim sistemine hukuka uygun olarak giren kişinin bilişim sisteminde hukuka aykırı olarak kalması halinde fail sistemden çıkmak istemesine rağmen çıkamamışsa yine suçun oluşacağı kabul edilmiştir[51]. Ancak burada failin işlediği fiili hukuka uygun kılan sebebin (örneğin rızanın) kalktığını öğrenir öğrenmez sistemi terk etmeye çalışmasına rağmen sistemden çıkamaz ve sistemde kalırsa bilişim sisteminin tamamında veya bir kısmında hukuka aykırı olarak kalma bakımından suçun işlenmesine yönelik iradi bir hareket olmadığı için bilişim sistemine girme suçunun oluşmadığını söylemek mümkündür.

TCK'nın 243'üncü maddesinin 3'üncü fıkrasında yer alan bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali için ayrı bir teşebbüs değerlendirmesi gerekmektedir. Söz konusu fıkrada suçun temel şekli kasten işlenebilirken, ağır netice olan sistemin içerdiği veriler yok olması veya değişmesinin taksirle gerçekleşmesi gerekir. Ağır netice bakımından olası kast veya doğrudan kastın olması halinde ağırlaşan netice bakımından TCK'nın 244'üncü maddesinde yer alan suç oluşacaktır. TCK'nın teşebbüsü düzenleyen 35'inci maddesi gereği taksirli suçlara teşebbüs mümkün değildir. Dolayısıyla 243'üncü maddesinin 3'üncü fıkrası açısından yani bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali bakımından teşebbüs mümkün değildir[52].

TCK'nın 36'ıncı maddesi gereğince "*suçun icra hareketlerinden gönüllü vazgeçer veya kendi çabalarıyla suçun tamamlanmasını*" önlerse teşebbüsten cezalandırılmamaktadır. Bilişim sistemine girmeye yönelik icra hareketlerini tamamlamadan önce failin sisteme girmekten vazgeçmesi halinde de gönüllü vazgeçme mümkündür[53]. Örneğin, fail birtakım yazılımlar yoluyla mağdurun e-posta şifresini ele geçirse fakat sisteme e-posta adresi ve şifreyi yazdıktan sonra vazgeçip

[50] Özbek v.d., **a.g.e.**, s.955; Akbulut, **Bilişim Alanında Suçlar**, s.151; Tezcan/Erdem/Önok, **a.g.e.**, 984.
[51] Akbulut, **Bilişim Alanında Suçlar**, s.151.
[52] Akbulut, **Bilişim Alanında Suçlar**, s.151; Özbek v.d., **a.g.e.**, s.955. Özbek, hareket ile neticenin ayrılabileceği hallerde istisnaen teşebbüsün mümkün olabileceğini ileri sürmüştür.
[53] Apaydın, **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 86.

ekranı kapatırsa gönüllü vazgeçme mümkün olacaktır[54]. Ancak fail e-posta şifresini[55] hukuka aykırı olarak ele geçirdiği için TCK'nın 136'ıncı maddesinde yer alan kişisel verilerin ele geçirilmesi suçundan sorumlu tutulabilecektir.

Teşebbüs aşamasında değerlendirilmesi gereken başka bir husus, casus yazılımların mağdurun bilişim sistemine gönderilmesi ve mağdurun bu yazılımları bilişim sistemine indirmesinin sonuçlarıdır[56]. Örneğin fail bir trojanı mağdura e-posta yoluyla bir başka dosya içinde gönderir fakat mağdur bu dosyayı bilişim sistemine indirmemesi yahut failin gönderdiği trojan gizli dosyanın mağdur tarafından kendi bilişim sistemine indirmesine rağmen fail daha sisteme girmeden mağdurun anti-virüs programıyla zararlı yazılımı silmesi halinde teşebbüs halinin gerçekleşip gerçekleşmediği tartışmasıdır. Bir görüşe göre, fail henüz bilişim sistemine girmediği için teşebbüsten de sorumlu tutulmayacaktır[57]. Ancak failin bilişim sistemine girmeye yönelik hareketine zorunlu olarak bağlı olarak kabul edilebilecek bu hareket[58] icra hareketi niteliğindedir ve failin sisteme girme fiili elinde olmayan sebeplerle tamamlanamadığı için suçun teşebbüs halinde kaldığını kabul etmek gerekir.

Teşebbüsün mümkün olabilmesi için failin elverişli hareketlerle doğrudan doğruya icraya başlaması gerekmektedir. Bilişim sistemine girmek için yapılan fiilin elverişliliği somut olaya göre değerlendirilmelidir. Örneğin son derece güvenlik

---

[54] Taşkın, **Bilişim Suçları**, s.30.

[55] Kişisel veri kişileri toplumdaki diğer kişilerden yer ayıran bilgiler olarak ifade edilebilir. Bu anlamda kişilere ait e-posta adresleri ve şifreler de kişisel veri kabul edilmelidir. Yargıtay'ın da kişisel veri tanımlaması bu yöndedir. "Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan "kişisel veri" kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir." 12. CD., E. 2014/2525 K. 2014/17259 T. 8.9.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

[56] Mahmutoğlu, **a.g.m.**, 861.

[57] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1415.

[58] Hazırlık hareketleri-icra hareketleri ayrımında TCK açısından da kabul edilen maddi objektif teori için bkz. Zafer İçer, "Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması Meselesi", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2017, s.89; Koca/Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, s.425.

önlemleri alınmış bir bilişim sistemine ait şifreyi failin manuel olarak rastgele denemesiyle tespit edebilmesi oldukça düşük bir olasılıktır. Bu bakımdan failin manuel olarak yaptığı bu fiil elverişsiz kabul edilebileceğinden teşebbüs oluşmayabilecektir. Ancak şifre kırma konusunda uzman bir kişinin şifreyi tespit etmek için yaptığı fiillerin somut olaya göre elverişli kabul edilebilmesi de mümkündür[59]. Örneğin bir bilişim sisteminin şifresini bulmak için hackerlar tarafından sıklıkla kullanılan Dictionary, Hybrid veya Brute Force[60] saldırı yöntemleriyle rastgele ve seri şekilde bir bilişim sistemine ait şifreyi bulmaya yönelik icra hareketlerinin elverişli olduğu kabul edilmelidir. Elverişliliğin sağlanması durumunda failin elinde olmadan sisteme girememesi halinde teşebbüs gündeme gelecektir.

B. İştirak

Tek bir kişi tarafından işlenmesi mümkün olan bilişim sistemine girme suçu birden fazla kişinin işbirliğiyle de işlenebilir. Söz konusu husus iştirak açısından özellik arz etmemektedir. Dolayısıyla bilişim sistemine girme suçunun iştirak halinde işlenmesi halinde TCK'nın 37'inci, 38'inci, 39'uncu, 40'ıncı ve 41'inci maddeleri uygulama alanı bulacaktır.

Bilişim sistemine girme veya orada kalma ile ilgili yeterli teknik bilgisi olmayan bir kişinin bir bilişim uzmanını hukuka aykırı olarak başka birine ait bilişim sistemine girmeye veya orada kalmaya ikna eden ve fiilin işlenmesine sebep olan kişinin azmettiren olarak sorumluluğu gündeme gelecektir[61].

---

[59] Karakehya, **a.g.e.**, s.19.

[60] Dictionary yöntemiyle sözlük şeklinde oluşturulmuş kelime ve ifadeler denenerek bilişim sisteminin şifresi bulunabilmektedir.
Hybrid ise sözlükte yer alan kelimeler ile özel karakterlerin kombinasyonlarını deneyerek şifreyi tespit edebilen bir atak türüdür.
Brute Force ise bütün şifre ihtimallerini değerlendirerek özel karakter, harf ve rakamların kombinasyonlarını deneyerek şifreyi tespit etmeyi sağlayan ve şifrenin belirlenmesinde çok uzun zaman alan bir atak türüdür. Bkz. Cybrary, https://www.cybrary.it/glossary/, Erişim Tarihi: 2.5.2019

[61] Karakehya, **a.g.e.**, s.20.

Bilişim sistemine girme suçu bakımından kalmaya devam etme seçimlik hareketi temadi etmektedir. Suçun bu seçimlik hareketle işlenmesi halinde mütemadi suçun sonuçları gereğince suçun bitme anına kadar azmettirme hariç iştirakin bütün şekillerinin gerçekleşmesi mümkündür[62].

Bu suça yardım eden olarak katılmak da mümkündür. Örneğin bir hakkın kullanılması veya rıza gibi hukuka uygunluk sebepleriyle bir bilişim sistemine girme yetkisi olan kişinin bu hakkını üçüncü kişilere devretme yetkisi olmamasına rağmen üçüncü kişilerin söz konusu bilişim sistemine erişimine imkan sağlaması halinde de somut olaya göre azmettiren ya da yardım eden sıfatıyla suça iştiraki mümkündür.

Bu konuda tartışılması gereken önemli bir husus failin tanımadığı diğer kişilerin bilişim sistemine girişini kolaylaştırmak için kasten bilişim sisteminde bir açık oluşturması halinde başkalarının bilişim sistemine girme suçunu işlemesini kolaylaştırdığı gerekçesiyle somut olaya göre diğer kişilerin işlediği bilişim sistemine girme suçuna azmettiren veya yardım eden olarak iştirakten sorumlu tutulup tutulamayacağı hususudur. Suça iştirakte bağlılık kuralının düzenlendiği TCK'nın 40'ıncı maddesi gereğince kişinin suça iştirakten sorumlu tutulabilmesi için "*kasten ve hukuka aykırı işlenmiş bir fiilin varlığı yeterlidir*". Böyle bir durumda fail başkaları da bilişim sistemine girebilsin diye kasten ve hukuka aykırı olarak bilişim sisteminde açık oluşturmaktadır. Dolayısıyla bağlılık kuralı[63] gereğince failin kendi işlediği suçun yanında başkalarının işlediği bilişim sistemine girme suçu bakımından da sorumlu tutulması mümkündür. Ancak failin kastının özellikle sistemdeki açıktan faydalanarak bilişim sistemine giren kişilerin şahsını bilmesine gerek olmasa da belirli bir kişiye yönelik olması gerekir[64]. Dolayısıyla suça iştirak eden kişilerin belirli olmaması halinde bilişim sisteminde açık oluşturan kişi şerik olarak sorumlu tutulmamalıdır. Ancak sistemde açık oluşturan kişi belirli kişi veya kişilerin bilişim sistemine erişimini kolaylaştırmak için bu fiili işlerse dahi, bu durumda failliğin şerikliğe asliliği kuralı

[62] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295.
[63] Bağlılık kuralının gerekleri için ayrıca bkz. Muhammed Demirel, **Suça İştirakte Bağlılık Kuralı**, İstanbul Arşivi, İstanbul, On İki Levha Yayınları, 2017, s.357 vd.
[64] Suç işleme kararının aldırıldığı kişilerin muayyen kişiler olması halinde diğer şartların da varlığında 5237 sayılı TCK'nın 214'üncü maddesi gereğince kişi suç işlemeye tahrik suçundan sorumlu tutulabilir. Bkz. Özgenç, **a.g.e.**, s.554.

gereğince fail bu suça yardım eden olarak değil, kendi fiilinden dolayı 244'üncü madde ve 245-A madde sebebiyle doğrudan fail olarak cezalandırılacaktır.

C. İçtima

Suçların içtimaına ilişkin genel düzenlemeler TCK'nın 42, 43 ve 44'üncü maddelerinde yer almaktadır.

Doktrinde, bilişim sistemine girme suçunu düzenleyen 243'üncü maddenin 2'nci ve 3'üncü fıkrasının aynı anda gündeme geldiği hallerde nasıl bir yol izlenmesi gerektiği tartışılmıştır. TCK'nın 243'üncü maddesi kapsamında failin bedeli karşılığı yararlanılabilen bir sisteme girip taksirli hareketi neticesinde bu sistemde yer alan verilerin yok olması veya değişmesi halinde failin cezai sorumluluğunun nasıl belirlenmesi gerektiği konusunda iki yaklaşım ortaya konulmaktadır. İlk yaklaşıma göre 243'üncü maddenin 2'nci fıkrasında yer alan "*yukarıdaki fıkrada tanımlanan fiillerin*" ifadesi dikkate alınarak bedeli karşılığı yararlanılan sistemlere girmek suçun ilk fıkrasının yani suçun temel şeklinin kapsamı içine giren şekilde ele alınmıştır. Böylece bedeli karşılığı yararlanılabilen bilişim sistemlerine girilmesi sonucu taksirle verilerin yok olmasına veya değişmesine yol açılırsa doğrudan 243'üncü maddenin 3'üncü fıkrası uygulama alanı bulmalıdır[65].

İkinci yaklaşıma göre ise, TCK'nın 61'inci maddesinin 4'üncü fıkrasını izleyerek bir sonuca ulaşmaktadır. Bu fıkraya göre "*bir suçun temel şekline nazaran daha ağır veya daha az cezayı gerektiren birden fazla nitelikli hallerin gerçekleşmesi durumunda; temel cezada önce artırma sonra indirme yapılır*". Yani hâkim önce 243'üncü maddenin 3'üncü fıkrası uyarınca verilerin yok olması veya değişmesi dikkate alınarak cezada bir artırım yapmalı, daha sonra girilen sistemin bedeli karşılığı yararlanılan sistem olmasından dolayı 2'nci fıkra gereği indirime gitmelidir. Doktrinde bir yazar, ilk yaklaşımı kabul ederek böyle bir durumda doğrudan 243/3 uyarınca temel cezada bir artırım yapılması gerektiğini, 3'üncü fıkranın bir neticesi sebebiyle ağırlaşmış hal olduğunu bu sebeple cezayı artıran nitelikli halin olmadığını

[65] Karagülmez, **a.g.e.**, s.214.

savunmaktadır[66]. İlk yaklaşımı kabul eden başka bir yazar ise neticesi sebebiyle ağırlaşmış suçu düzenleyen 3'üncü fıkrada suça ilişkin yaptırımın alt ve üst sınırının bulunması sebebiyle 61'inci maddenin 4'üncü fıkrasını uygulama imkânı olmadığını gerekçe olarak belirtmiştir. Yazara göre, failin bu fiilinin birden fazla hükmü ihlal ettiği kabul edilmeli, bu sebeple en ağır cezayı içeren 243/3'ten hüküm kurulmalıdır[67].

İşlenen fiilin kanunda öngörülen ağır neticelere yol açtığı hallerde, özel norm-genel norm ilişkisi gereğince fail temel suçtan değil neticesi sebebiyle ağırlaşmış suçtan sorumlu olacaktır[68]. Neticesi sebebiyle ağırlaşmış hal bakımından alt ve üst sınırların yer aldığı suçlarda nitelikli hallerin söz konusu olması halinde nitelikli hallere ilişkin kurallardan hareket edilmesi gerekecek ve 61'ici madde uyarınca daha az cezayı gerektiren nitelikli hal uygulanacaktır[69]. Bu doğrultuda ilk önce 243/3'üncü fıkra uyarınca neticesi sebebiyle ağırlaşmış suça ilişkin ceza belirlenmeli, daha sonra 243/2 uyarınca bedeli karşılığı yararlanılan sistemler suçun konusunu oluşturduğu için failin cezasında indirime gidilmelidir.

1. Zincirleme Suç

TCK'nın 44'üncü maddesinin 1'inci fıkrası uyarınca aynı suç işleme kararıyla bir kişiye karşı aynı suçun temel halinin veya nitelikli hallerinin değişik zamanlarda işlenmesi halinde zincirleme suç oluşur ve failin cezası artırılır. 243'üncü maddenin 3'üncü fıkrasında yer alan neticesi sebebiyle ağırlaşmış suç da zincirleme suç hükümleri bakımından aynı suç sayılır[70]. Bilişim sistemine girme suçu bakımından zincirleme suç hükümlerinin uygulanması mümkündür[71]. Failin bir kişiye ait bilişim sistemine değişik zamanlarda ve aynı suç işleme kararıyla birden fazla kez girmesi

[66] **A.e.**, 215.
[67] Erdoğan, **Türk Ceza Hukuku'nda Bilişim Suçları**, s. 171-172.
[68] Koca/Üzülmez, **Türk Ceza Hukuku Genel Hükümler**, s.549.
[69] **A.e.**, s.685.
[70] Akbulut, **Bilişim Alanında Suçlar**, s.152.
[71] "Oluşa ve dosya kapsamına göre, bir dönem arkadaşlık yaptığı katılanın şifresini bildiği facebook hesabına rızası dışında girerek, katılanların mesaj içeriklerini alıp aynı suç işleme kararının icrası kapsamında tanıklara gösterdiği ve katılan ...'nın çalıştığı kuruma gönderdiği olayda sanık hakkında TCK'nın 43/1 maddesin uygulanması gerektiğinin gözetilmemesi aleyhe temyiz olmadığından bozma nedeni yapılmamıştır." 12. CD., E. 2015/15370 K. 2017/3455 T. 26.4.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019.

veya orada kalması halinde failin cezası dörtte birinden dörtte üçüne kadar artırılacaktır.

Failin çok kısa zaman aralıklarıyla birden fazla kez bilişim sistemine girmesinin zincirleme suç hükümleri kapsamında yer alıp almayacağı hususu tartışılabilir. Örneğin bir bilişim korsanın mağdurun bilişim sistemine girdikten sonra her seferinde teknik bir nedenle sistemden atılmasına rağmen arka arkaya bilişim sistemine girmesi durumunda kısa zaman aralığında yapılan birden fazla hareketin var olduğu kabul edilebilir. Bu sebeple zincirleme suçtan dolayı tek suçtan dolayı ceza verilip cezasının artırılması gerekir[72]. Nitekim fail kısa aralıklarla da olsa aynı suçu işlemek kastıyla değişik zamanlarda bilişim sistemine girme suçunu işlemiştir.

Öte yandan failin mağdura ait bir donanım aracılığıyla söz konusu donanımın parçasını oluşturduğu bir bilişim sistemine girmesinin ardından bu bilişim sistemi ile bağlanabilmekle birlikte mağdura ait başka program ve yazılımlara erişmesi halinin içtima açısından tartışılması gerekir. Örneğin mağdura ait bir bilgisayara giren failin bilgisayarı açmasının ardından söz konusu donanımla erişilebilmesine rağmen başka sunucularda kayıtlı bulunan e-posta, sosyal medya hesapları ve/veya bulut bilişim sistemlerine erişmesi durumunda failin tek bir bilişim sistemine girme suçundan mı yoksa birden fazla suçtan mı cezalandırılacağı ele alınmalıdır. Her ne kadar suçun konusunun farklı olabileceği kabul edilebilir olsa da[73] hukuki anlamda suçu oluşturan tek bir fiil vardır. Benzer bir durum TCK'nın 141'inci maddesinde düzenlenen hırsızlık suçu bakımından da geçerlidir. Örneğin; aynı mağdura ait olan birden fazla eşyanın fail tarafından mağdurun rızası olmaksızın yarar sağlamak amacıyla alınması halinde tek bir hareket olduğu kabul edilmektedir[74]. Dolayısıyla somut olayın da koşulları dikkate alınarak, mağdura ait bir donanım aracılığıyla bilişim sistemine

[72] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295. Aynı yönde; Soyaslan, **a.g.e.**, s.638. Aksi yönde; Mahmutoğlu, **a.g.m.**, s.864.

[73] Avrupa Konseyi Siber Suçlar Sözleşmesinin 1'inci Bölüm 1'inci maddesinin a bendinde "bilgisayar sistemi" ifadesine yer verilmiş ve "bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder" şeklinde tanımlanmıştır. Dolayısıyla Avrupa Konseyi Siber Suçlar Sözleşmesi kapsamında birbiriyle bağlantılı veya ilgili grup cihazların hukuken tek bir bilgisayar sistemi olarak kabul edilmesi mümkündür.

[74] Bkz. Kayıhan İçel, **Suçların İçtimaı**, İstanbul, İstanbul Üniversitesi Hukuk Fakültesi Yayını, 1972, s.29; Neslihan Göktürk, **Fikri İçtima (Suçların İçtimaı)**, Ankara, Adalet Yayınevi, 2013, s.29 vd.

girildikten sonra ve hala bilişim sisteminde kalmaya devam ederken mağdura ait olan fakat farklı sunucularda kayıtlı olan program ve yazılımlara erişilmesi halinde fail tek bir bilişim sistemine girme suçundan sorumlu olmalıdır.

Failin daha uzun zaman aralığında mağdurun bilişim sistemine girmesi veya orada kalması halinde ise failin aynı suç işleme kararıyla hareket edip etmediğinin tespiti önem arz etmektedir. Doktrinde bir görüşe göre, aynı suç işleme kararından bahsedilemeyecek kadar uzun bir sürenin söz konusu olduğu hallerde failin aynı suç işleme kararıyla hareket etmediği kabul edilmelidir ve gerçek içtima gereğince faile her suç için ayrı ayrı ceza verilmelidir[75]. Ancak bilişim sistemine girme veya orada kalma fiilinin hangi teknik kullanılarak işlendiği somut olay bazında failin aynı suç işleme kastıyla hareket edip etmediğine ışık tutabilir. Örneğin failin mağdura ait bilişim sistemine tekrar tekrar kolaylıkla girmesini sağlayan ve bilişim sistemini bilişim korsanının girişine her an açık tutan "*backdoorların*" tespit edilmiş ve mağdura ait bilişim sistemine birden fazla kez girilmiş olması halinde ilk girişten itibaren uzun bir süre geçmiş olsa da aynı suç işleme kararı olup olmadığının araştırılması gerekir.

Bilişim sistemine girme suçunun diğer bir seçimlik hareketi olan bilişim sisteminde kalma ise mütemadi suçtur ve suç failin bilişim sisteminden çıkmasıyla biter. Dolayısıyla bilişim sisteminde kalma süresi kesilmedikçe failin fiili tek bir suç oluşacaktır[76]. Hâkim ise bilişim sisteminde kalma süresine göre cezaların alt ve üst sınırını dikkate alarak TCK'nın 61'inci maddesi uyarınca cezanın ağırlığını belirleyecektir[77].

Failin farklı bilişim sistemlerine girmesi veya bu sistemlerde kalması halinde birden fazla suç oluşacaktır[78]. Fakat aynı mağdura ait farklı bilişim sistemlerine aynı suç işleme kastıyla farklı zamanlarda girilmesi halinde zincirleme suç oluşmalıdır. Nitekim bilişim sistemi burada suçun konusudur. Aynı mağdura ait olduktan sonra bilişim sistemlerinin farklı olması bu manada farklılık arz etmemelidir. Örneğin; failin

[75] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295. Aynı yönde; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1417, dn.200.
[76] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1417.
[77] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295; Tezcan/Erdem/Önok, **a.g.e.**,s.984.
[78] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1417.

mağdura ait fotoğraflara erişmek amacıyla mağdurun önce bilgisayarındaki fotoğraflarına erişip, daha sonraki bir zamanda akıllı telefonundaki fotoğraflara erişmesi halinde zincirleme suç hükümleri uygulanmalıdır.

2. Aynı Neviden Fikri İçtima

Bilişim sistemine girme suçu açısından aynı neviden fikri içtimaın uygulanabilmesi de mümkündür[79]. Örneğin fail tek bir e-posta gönderimi ile birden fazla kişiye ait bilişim sistemine trojan gönderebilir. Bu sayede e-posta gönderilen kişilerin bilişim sistemine girebilir veya orada kalabilir. Bu durumda TCK'nın 43'üncü maddesinin 2'nci fıkrası gereğince failin cezasında artırım yapılacaktır.

3. Farklı Neviden Fikri İçtima

Doktrindeki tartışmaların esas noktası bilişim sistemine girme suçu ile diğer bilişim suçlarının fikri içtimaı üzerinedir. Bilişim sistemine girme veya orada kalma fiili hemen hemen bütün bilişim suçlarının işlenebilmesi için gerekli bir hareket oluşturmaktadır[80].

Bu konuda doktrinde çeşitli görüşler bulunmaktadır. İlk görüşe göre, bilişim sistemine girme suçu diğer bilişim suçlarının işlenmesi adına zorunluluk oluşturduğu için geçit suçu özelliği taşır. Bu sebeple TCK'da yer alan "*sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçu (md.244), "*banka veya kredi kartlarının kötüye kullanılması*" suçu (md.245), "*haberleşmenin gizliliğini ihlal*" suçu (md.132)[81], "*kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması*" suçu (md.133), "*özel*

[79] Yenidünya/Değirmenci, **a.g.e.**, s.22.
[80] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 295.
[81] Aksi yönde; "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" hukuka aykırıdır. 12. CD., E. 2014/15082 K. 2015/1624 T. 2.2.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.1.2019.

hayatın gizliliğini ihlal" suçu (md. 134)[82], "*Kişisel verilerin kaydedilmesi*" suçu (md.135), "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçu (md.136), "*bilişim sistemlerinin kullanılması suretiyle hırsızlık*" suçu (md.142/2-e), "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*" suçu (md.158/1-f) ile 5846 sayılı Fikir ve Sanat Eserleri Kanunu ve 5070 sayılı Elektronik İmza Kanunu'nda düzenlenen bazı suçlarda failin mağdura ait bilişim sistemine hukuka aykırı olarak girerek veya orada kalarak bu suçları işlemesi mümkün olduğu için fail bilişim sistemine girme suçundan değil, ikinci suçtan cezalandırılmalıdır[83].

Diğer bir görüşe göre ise bilişim sistemine girme suçu bazı suçlar bakımından tüketen-tüketilen norm özelliği taşırken, bazı suçlarda bu özelliği göstermemektedir. TCK'da yer alan *"sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçunun (md.244) işlenebilmesi için failin mağdurun bilişim sistemine girmesi veya orada kalması zorunludur. Dolayısıyla 244'üncü maddede yer alan fiil 243'üncü madde yer alan haksızlık içeriğini de taşıdığından fail yalnızca 244'üncü maddeden sorumlu olmalıdır. Ancak "*bilişim sistemlerinin kullanılması suretiyle hırsızlık*" suçu (md.142/2-e), "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*"

[82]Aksi yönde Yargıtay 12. Ceza Dairesi "Başkasına ait facebook hesabına girerek, arkadaş hanesine bir başka kişiyi ekleme eyleminin sübutu halinde, haberleşmenin gizliliğini ihlal suçunu değil, TCK'nın 243.maddesinde düzenlenen bilişim sistemine girme suçunu oluşturacağı" yönünde karar vermiştir. Karar için bkz. 12. CD., E. 2014/12315 K. 2015/1153 T. 26.1.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.1.2019.
Ancak mezkûr karar dikkate alındığında somut olayda her ne kadar haberleşmenin gizliliği ihlal edilmemiş olsa da bilişim sistemine girme suçunun yanı sıra sosyal medya hesabına arkadaş yüklemek suretiyle bilişim sistemine veri yüklenmesi söz konusu olduğundan sanığın 5237 sayılı TCK'nın 244/2 fıkrası gereğince de sorumlu tutulması, icra hareketlerinin örtüşmesi halinde iki suç arasında fikri içtima kurallarının uygulanması gerekmektedir.

[83] Parlar, **a.g.e.**, s. 21; Soyaslan, **a.g.e.**, s.639; Yenidünya, **a.g.m.**, s.1039; Artuk/Gökcen/Yenidünya, **a.g.e.**, s.878; Yaşar/Gökcan/Artuç, **a.g.e.**, s.7295; Şaban Cankat Taşkın, "Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2008, s.39; Dülger, **Bilişim Suçları**, s.225-226. Dülger kitabının ilk basısında yer verdiği bu görüşü daha sonraki basılarda değiştirmiştir.
Korkmaz, haberleşmenin gizliliğini ihlal suçu, kişiler arasındaki konuşmaların dinlenilmesi ve kayda alınması suçu ve özel hayatın gizliliğini ihlal suçu bakımından bilişim sistemine girme suçu ile görünüşte içtimaa tabi olabileceğini savunmaktadır. Ancak örneğin failin bilişim sistemine girdikten belli bir süre sonra verileri kaydetmeye karar verip kaydetmesi halinde gerçek içtimaın uygulanması gerektiğini belirtmektedir. İbrahim Korkmaz, **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara, Seçkin Yayıncılık, 2017, s267-268.

suçu (md.158/1-f) gibi suçlarda failin ayrıca 243'üncü maddeden de cezalandırılması gerekmektedir[84].

Ancak bu görüşe göre, "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçu (md.136) diğer bilişim aracılığıyla işlenen suçlardan farklı olarak 243'üncü maddenin haksızlık içeriğini kapsamaktadır ve tüketen-tüketilen norm ilişkisi gereği fail yalnızca 136'ıncı maddeden sorumlu olmadır[85].

Doktrindeki başka bir görüş ise, geçitli suç kavramını kabul etmemektedir. Failin hangi suçu işlemeye yönelik kastını dikkate alarak cezai sorumluluğunun belirlenmesi gerektiği ileri sürülmüştür. Buna göre failin amacı bilişim sistemini engellemek, bozmak veya verilerin yok edilmesi ya da değiştirilmesine yönelikse cezai sorumluluğu 244'üncü madde kapsamında değerlendirilmelidir. Fail bilişim sistemine girerek hırsızlık veya dolandırıcılık yapmak kastıyla hareket etmekteyse nitelikli hırsızlık veya nitelikli dolandırıcılıktan sorumlu olmalıdır[86].

Bazı yazarlar ise, böyle bir durumda tek hareketle birden fazla suçun ihlal edildiğini dolayısıyla fikri içtima kurallarının uygulanması gerektiğini savunmaktadır[87]. Farklı neviden fikri içtima açısından bir suçun icra hareketlerinin başka bir suçun icra hareketleriyle kısmen veya tamamen uyuşması yeterlidir. Bilişim sistemine girme suçunun icra hareketleri olan bilişim sistemine girme veya bilişim sisteminde kalma fiillerini 244'üncü maddede yer sistemi engelleme, bozma, verileri yok etme veya değiştirme suçunun icra hareketleriyle uyuştuğu için daha ağır ceza öngören 244'üncü madde yer alan cezanın uygulanması gerektiği ileri sürülmüştür[88]. Ancak iki suçun icra hareketleri kısmen veya tamamen uyuşmuyorsa farklı neviden

---

[84] Yavuz Erdoğan, "Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011, s.171.

[85] Tezcan/Erdem/Önok, **a.g.e.**, s. 985.

[86] Yılmaz, **a.g.e.**,s.190; Özbek v.d., **a.g.e.**, s.956.

[87] Akbulut, **Bilişim Alanında Suçlar**, s.152; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1419.

[88] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.819. Sevük, haberleşmenin gizliliğini ihlal suçunun bilişim sistemine girme suçu ile birlikte işlenmesi halinde fikri içtimaın uygulanması gerektiğini savunmaktadır. Handan Yokuş Sevük, **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018, s. 237,

fikri içtima söz konusu olmayacak, fail her iki suçtan da ayrı ayrı cezalandırılacaktır[89]. Karakehya da fikri içtimaın mümkün olduğunu kabul etmekle birlikte, failin başkaca suçları işlemek için bilişim sistemine girme suçunu işlemesi halinde TCK'nın 42'nci maddesini temel alarak her iki suçtan da sorumluluğun doğması gerektiğini ileri sürmüştür. Bileşik suçun tanımını yapan 42'nci madde uyarınca "*biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturması dolayısıyla tek fiil sayılan*" suçlarda içtima hükmü uygulanmamaktadır. Bunun tersinden anlaşılması gereken ise biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturmayan suçlar bileşik suç oluşturmayacağından fail her iki suçtan da sorumlu olmalıdır. Örneğin, "*bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık*" suçunun işlenmesi halinde fail hem bilişim sistemine girme suçundan hem de amaç suç olan nitelikli dolandırıcılıktan sorumlu olmalıdır[90].

Yargıtay bir kararında somut olay bazında geçit suç kavramını kabul etmeyerek failin işlediği suçlardan ayrı ayrı cezalandırılması gerektiğini belirtmiştir. Kararda "*sanığın katılanın telefon hafıza kartını bir şekilde ele geçirip facebook şifrelerini de kırarak bu hesabı kullanmaya başlayıp elde ettiği fotoğrafları facebooktan yaymaya başlayacağını söyleyerek kendisiyle görüşmeye devam etmesi için kendine ait telefondan katılana ait telefona gönderdiği "elimde görüntülerin var, bunları yayınlayacağım", "faceteki resimleri beğenmediysen değiştireyim mesela oteldeki faturayı ya da seni s... görüntüleri koyayım", "Nazillideyim gel görüşelim yoksa orayı başınıza yıkarım haber bekliyorum", "benim sana yaptığım masrafı yollamazsan 29 Nisan gecesi ... Otelde kaldığımızı belgeleyen faturayı bütün Nazilli'ye, eşine, ailesine yollarım, kesinlikle haber bekliyorum en geç yarına" gibi mesajların içerikleri ve tüm dosya kapsamına göre, sanığın şantaj, bilişim sistemine girme ve özel hayatın gizliliğini ihlal suçlarını işlediği anlaşılmakla, TCK'nın 107/2, 243/1 ve 134/2. maddeleri uyarınca cezalandırılması gerekirken, yerinde olmayan gerekçelerle beraat hükümleri kurulması*" kanuna aykırı bulunarak bozma sebebi yapılmıştır[91].

[89] **A.e.**, s.818
[90] Karakehya, **a.g.e.**, s.21.
[91] 4. CD., E. 2014/2222 K. 2015/24755 T. 18.3.2015, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019.

Dülger[92] ise somut olayın koşullarına göre bir değerlendirilme yapılması gerektiğini savunmaktadır. Failin kastının en ağır neticeye yönelik olmadığı ve ilk suçla ağır suçun hukuki değeri korumadığı suçlar bakımından geçit suçu söz konusu olmayacaktır[93]. Dolayısıyla bilişim sistemine girme suçuyla korunan hukuki değerle aynı hukuki değeri koruyan 244'üncü madde hariç diğer suç tipleri açısından geçit suç kavramı kabul edilemez[94]. 244'üncü madde bağlamında da suçun nasıl işlendiği önem arz etmektedir. Örneğin, bir sabit diski suyla temas ettirerek verilerin yok edilmesi halinde 244'üncü maddenin gerçekleşmesi için bilişim sistemine girme suçu geçit suç ilişkisini taşımayacaktır[95]. Yazar, fikri içtima açısından da benzer bir düşünceyle somut olaya bakılması gerektiğini savunmaktadır. Fikri içtima kapsamında failin tek hareketinden bahsedilebilmesi için fiiller arasında zamansal bir yakınlığın mevcut olması gerekir. Dolayısıyla somut olayda failin bilişim sistemine girme suçunu

Aynı yönde nitelikli dolandırıcılık ve bilişim sistemine girme suçunun ayrı ayrı cezalandırılmasıyla ilgili bkz. "Sanığın nitelikli dolandırıcılık ve hukuka aykırı surette bilişim sistemine girme suçlarından mahkumiyetine ilişkin hükümler, sanık tarafından temyiz edilmekle, dosya incelenerek gereği düşünüldü,…
…Sanığın müşteki ...'ın mail adresinin şifresini kırarak kendisi ... gibi tanıtıp müşteki ...'a mesaj atarak 500 TL istediği, müşteki Cihan'ın parayı sanığın bildirdiği hesaba yatırdığı ve mağdur ...'dan 500 kontör istediği, müşteki ...'in mail adresinin şifresini kırarak kendisini... gibi tanıtıp müşteki ...'a mesaj atarak 500 TL istediği, müştekinin parayı sanığın bildirdiği hesaba yatırdığı, sanığın, mağdur ...'in arkadaşının mail adresinden mağdura teyzesini hastaneye yatırdığını söyleyerek 1000 TL para istediği, durumdan şüphelenen mağdurun parayı göndermediği, müşteki ...'ın arkadaşının mail adresinden arkadaşıymış gibi davranarak 400 TL para istediği, müşteki ...'in arkadaşının mail adresinden arkadaşıymış gibi davranarak 250 kontör istediği, mağdur ...'nun arkadaşının mail adresinden arkadaşıymış gibi davranarak cep bankacılığına gönderilmek üzere 20 TL para istediği, mağdur ...'ın arkadaşının mail adresinden arkadaşıymış gibi davranarak Brezilya'da bulunan yeğeni için 400 TL para istediği olaylarda…
… Sanığın üzerlerine atılı suçları işlediğine dair mahkemenin mahkumiyet yönünde kabulünde isabetsizlik görülmemiştir." 15. CD., E. 2016/2793 K. 2016/7012 T. 22.9.2016, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019. Aynı yönde bkz. 23. CD., E. 2015/3995 K. 2015/6595 T. 16.11.2015.
Aynı yönde nitelikli hırsızlık ve bilişim sistemine girme suçunun ayrı ayrı cezalandırılmasıyla ilgili bkz. "-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," 13. CD., E. 2014/2924 K. 2014/36282 T. 18.12.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:4.4.2019. Aynı yönde bkz. 13. CD., E. 2014/23539 K. 2015/8515 T. 6.5.2015; 17. CD., E. 2016/10724 K. 2018/12290 T. 10.10.2018.

[92] Dülger kitabının ilk basısında yer verdiği bu görüşü daha sonraki basılarda değiştirmiştir.

[93] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 299.

[94] **A.e.**

[95] **A.e.**, s.300.

işlemesiyle diğer suçları işlemesi arasında zamansal bir farklılık olması halinde farklı neviden fikri içtima hükmünün uygulanması söz konusu olmayacaktır[96].

Görünüşte içtimaın bir türü olan asal norm-yardımcı norm ilişkisi bağlamında bir suçun diğer suç açısından yardımcı norm olup olmadığı kanunda açıkça belirtilmemiş olabilir[97]. Geçit suçun söz konusu olabilmesi için doktrinde bazı şartlara yer verilmiştir. Bu sebeple geçit suça ilişkin şartlar belirtilirken yukarıda anılan suçlar açısından bilişim sistemine girme suçunun geçit suç olup olamayacağı ortaya konulmalıdır.

Öncelikle geçit suç için bir suçu işlemek amacıyla başka bir suçun geçilmesi gerekir. Bu hallerde önceki hareketin cezalandırılmaması için işlenen her iki suçun da aynı hukuki değeri koruması gerekmektedir[98]. Bu bakımdan 244/1-2'nci fıkralar hariç diğer suçlarda farklı hukuki değerler gündeme gelmektedir[99]. Geçit suç kavramının tartışılabileceği diğer suçların da korunan hukuki değerini ortaya koymak gerekir. Banka veya kredi kartlarının kötüye kullanılması suçu (md.245) ile korunan hukuki değer hem malvarlığına ilişkin hakları hem de ticari hayatı kapsayan kamu düzeni ve güveliğini içeren haklar olarak ifade edilebilir ve karma niteliklidir[100]. Haberleşmenin gizliliğini ihlali suçu (md.132) ile korunan hukuki değer ise haberleşme hürriyetidir[101]. Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu (md.133) ve özel hayatın gizliliğini ihlal suçu (md. 134) ile korunan hukuki değerler ise temel olarak kişilerin özel hayatının gizliliğidir[102]. Kişisel verilerin kaydedilmesi suçu (md.135) ve verileri hukuka aykırı olarak verme veya ele geçirme suçunda (md.136) korunan hukuki değerler genel olarak özel hayatın gizliliği, özel olarak ise kişisel verilerin

---

[96] **A.e.**, s.300.
[97] Kayıhan İçel, "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Y. 7, S. 14, Güz 2008, s. 42.
[98] **A.e.**, s.46.
[99] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 299.
[100] Apaydın **Bilişim Suçları ve Bilişim Ceza Hukuku**, s. 408.
[101] Korkmaz, **a.g.e.**, s.317. Başka bir görüşe göre ise burada korunan hukuki değer haberleşmenin gizliliği ve mahremiyetidir. Bkz. Mahmut Koca, "Haberleşmenin, Konuşmanın ve Özel Hayatın Gizliliğini İhlal Suçları (TCK m.132-134)", **Ceza Hukukunun Güncel Sorunları**, Erzurum, 8 Ekim 2010, s.66-67.
[102]Korkmaz, **a.g.e.**, s. 318, 320. Koca'ya göre ise burada korunan hukuki değer sözün mahremiyetidir. Bkz. Koca, **a.g.m.**,s.84.

korunmasıdır[103]. Bilişim sistemlerinin kullanılması suretiyle hırsızlık suçu (md.142/2-e) ve bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılık suçu (md.158/1-f) açısından korunan hukuki değerler ise genel olarak malvarlığına ilişkin değerler olarak kabul edilebilir[104]. Karşılıksız yararlanma suçu (md. 163) ile korunan hukuki değer de yine malvarlığına yönelik haklardır[105].

5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 1-B maddesinin g bendi uyarınca bilgisayar programları da bu Kanun kapsamında sayılmış, aynı Kanunun "*manevi, mali veya bağlantılı haklara tecavüz*" başlıklı 71'inci maddesi "*bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek*" "*hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan*" kişinin cezalandırılacağı hükme bağlanmıştır. Söz konusu suç bilişim sistemine girme suçu ile birlikte işlense dahi Kanun metninden de anlaşılacağı üzere burada korunan hukuki değerler genel olarak "*fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı*"[106] haklar[107], bilgisayar programları için mali haklardır[108]. 5070 sayılı Elektronik İmza Kanunu'nun 16'ıncı maddesi uyarınca ise "*Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar*" cezalandırılmaktadır. Burada korunan

[103] Dülger, Murat Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması", İ**stanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, S.3 (2), Güz 2016, s. 101-167.
[104] Özbek v.d., **a.g.e.**, s.610,710.
[105] Kaya, **5237 Sayılı Türk Ceza Kanunu'nda Karşılıksız Yararlanma Suçu**, s.22.
[106] Aynı yönde; Hüseyin Çakır, Mehmet Serkan Kılıç, **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014, s.192.
[107] Bkz. Esra Dikmen, "Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçları (FSEK m. 71/1-1)", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2018, s.68 vd.
[108] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s.504.

hukuki değerin ise kamunun elektronik imza ile onaylanan belgelere ve bunların doğruluğuna duyulan güven olduğu ifade edilebilir[109].

Bilişim sistemine girme suçu ile korunan hukuki değer ise daha önce de belirtildiği üzere bilişim sisteminin güvenliği ve güvenilirliğidir. Dolayısıyla bilişim sistemine girme suçu yukarıda anılan suç tiplerinin hiçbiri ile aynı hukuki değeri korumadığı için geçit suç olarak değerlendirilemeyecektir. Bilişim sistemine girme suçu ile yukarıda anılan suçlara ilişkin hareketlerin tamamının veya bir kısmının aynı hareketle gerçekleştirilmesi halinde farklı neviden fikri içtima söz konusu olabileceği gibi, bu hareketlerin kesişmemesi yani tek hareket olarak değerlendirilememesi halinde ise gerçek içtima uygulanarak failin her iki suçtan da ayrı ayrı cezalandırılması gündeme gelebilecektir[110]. TCK'nın 244/1-2'nci fıkralarında yer alan suçlar bakımından korunan farklı hukuki değerler gündeme gelebilse de bilişim sisteminin güvenliğinin de bu fıkralar kapsamında korunduğu kabul edilebilir nitelikte olduğundan geçit suçun diğer şartları açısından değerlendirme yapmak gerekir.

Bir suçun işlemesi için başka bir suçun içinden geçilmesi gereken hallerde failin kastının mutlaka ağırlaşan sonucun gerçekleşmesine yönelik olması gerekmektedir[111]. Bu bakımdan 244/1-2'nci fıkralarda yer alana suçların işlenmesi amacıyla 243'üncü maddenin işlenmesi hali geçit suç bakımından bu şartı

---

[109] **A.e.**, s.527.

[110] Yargıtay bazı kararlarında bilişim sistemine girme suçu ile bilişim aracılığıyla işlenen suçların ayrı ayrı ele alınması gerektiğini belirtmiştir. "Sanık hakkında 08/02/2010 tarih ve 2009/5363 soruşturma numaralı iddianame ile hukuka aykırı olarak bilişim sistemine girme ve orada kalma suçundan TCK'nın 243/1 maddesi uyarınca kamu davası açılmasına rağmen bu suçla ilgili tartışma ve değerlendirme yapılmadığı gibi hüküm de kurulmadığı anlaşıldığından, zamanaşımı içerisinde işlem yapılması mümkün görülmüştür.
Sanık ...'ın, hakkında mahkumiyet kararı verilen ve temyiz kapsamında olmayan diğer sanık... ile birlikte, ..., ... ve ...'a ait MSN Messenger adreslerinin şifresini ele geçirip farklı zamanlarda internete girerek MSN adreslerindeki arkadaş listesinde bulunan kişilerden acil olarak kontör istedikleri, ...'in arkadaşı olan şikayetçi ...'in 12 adet, ...'un dayısının kızı olan şikayetçi ...'in 1 adet, ...'in de öğrencisi olan şikayetçi...'in 2 adet 250'lik kontör şifresini bilgisayara yazıp gönderdikleri, gönderilen kontör şifrelerinin sanıklar tarafından piyasada ucuza satıldığı şeklinde gerçekleşen eylemlerinin nitelikli dolandırıcılık suçlarını oluşturduğu anlaşıldığından mahkemenin kabulünde bir isabetsizlik görülmemiştir." 15. CD., E. 2016/4937 K. 2017/19032 T. 28.9.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

[111] İçer, **Türk Ceza Hukukunda Tüzel Kişiler**, s.47.

sağlamaktadır. Ancak sadece bu koşulun sağlanması geçit suçun varlığını kabul etmeye yetmeyecektir.

Belirtmek gerekir ki ağır sonuca yönelik suçun işlenmesi için içinden geçilen suç, işlenmek istenen suçun hazırlık hareketi olmamalıdır. Burada ayrıca TCK'nın 245/A maddesinde yer alan "*yasak cihazlar ve programlar*" suçunun değerlendirilmesi gerekir[112]. Söz konusu maddeye göre "*bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır*".

Bilişim sistemine girme suçunu işlemek amacıyla söz konusu maddede anılan yasak cihaz ve programları imal edip veya bulundurup kullanan kişi bakımından bu suç bir araç suç özelliği taşıyacaktır[113]. Öte yandan bu yasak cihaz ve programlar bilişim sistemine girme suçu için bir hazırlık hareketi olarak değerlendirilebileceğinden gerçek içtima kurallarına tabi tutulacaktır.

Her ne kadar farklı hukuki değerler korunduğu için geçit suç söz konusu olamayacak olsa da belirtmek gerekir ki 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 72'nci maddesinde düzenlenen "*koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri*" başlıklı suç ile "*bir bilgisayar programının hukuka aykırı olarak çoğaltılmasının önüne geçmek amacıyla oluşturulmuş ilave programları etkisiz kılmaya yönelik program veya teknik donanımları üreten, satışa arz eden, satan veya kişisel kullanım amacı dışında elinde*" bulundurmak da hazırlık hareketleri olarak değerlendirilebileceğinden bu suç ile bilişim sistemine girme suçunun işlenmesi halinde fail her iki suçtan da cezalandırılmalıdır.

[112] Bkz. İçer, **Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması Meselesi**, s. 66.
[113] Akbulut, **Bilişim Alanında Suçlar**, s.153.

Geçit suçtan söz edebilmek için ağırlaşan sonucun gerçekleşmesinde geçilen hafif suçun işlenmesinin zorunlu olması gerekir[114]. Bu bağlamda aynı hukuki değerin korunmadığı suçlar açısından ayrıca bir zorunluluk değerlendirilmesi yapılmasına gerek yoktur. Ancak 244/1-2'nci fıkralar açısından bilişim sistemine girme suçunun zorunlu olup olmadığının incelenmesi gerekir. Sistemi engelleme, bozma veya verileri yok etme, değiştirme suçlarının işlenmesi için bilişim sistemine girme suçunun her zaman zorunlu olduğundan bahsedilemeyecektir. Örneğin, bilgisayarın çekiçle kırılması veya hard diskin sıvı içine atılarak bozulması hareketleriyle fail 244/1-2'nci fıkralarda yer alan suçlarda yer alan seçimlik hareketlerden bazılarını bilişim sistemine girmeksizin işleyebilmektedir[115]. Ancak failin bilgisayara trojan göndererek bilgisayar işletim sisteminin çökmesine yol açması veya sistemde yer alan dosyaları yok etmesi halinde fail 244/1-2'nci fıkralarında yer alan suçları işlemek için zorunlu olarak bilişim sistemine girme suçunu da işlemiştir. Doktrinde somut olay çerçevesinde geçit suç söz konusu olduğu için fail yalnızca 244'üncü maddeden sorumlu olması gerektiği ileri sürülmüştür[116]. Ancak burada somut olay bazında bir zorunluluk aranması gerektiği mi yoksa genel olarak tüm ihtimaller dâhilinde ağır sonuca yönelik suçun işlenmesi için geçit olarak kullanılan hafif suçun işlenmesi zorunluluğunun mu olması gerektiği sorusunun cevaplanması gereklidir. Somut olay bazında bir zorunluluk halinin bulunması geçit suçtan öte farklı neviden fikri içtimaı gündeme getirebilecektir.

Dolayısıyla TCK'nın gerek 244'üncü maddesinin 1'inci fıkrasında yer alan bilişim sisteminin işleyişini engelleme ve bozma gerekse 2'nci fıkrada yer alan bilişim sistemindeki verileri değiştirme veya erişilmez kılma, sisteme veri yerleştirme ve var olan verileri başka bir yere gönderme bakımından somut olaya göre değil seçimlik harekete göre bir değerlendirme yapılması gerekir. Bu bağlamda 244'üncü maddenin 1'inci fıkrası bakımından bilişim sisteminin işleyişini engelleme seçimlik hareketinin işlenmesi ile 244'üncü maddenin 2'nci fıkrasında yer alan bilişim sistemindeki verileri değiştirme, sisteme veri yerleştirme veya var olan verileri başka bir yere gönderme

[114] İçel, **a.g.m.**, s.47.
[115] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 300.
[116] **A.e.**, s. 300.

seçimlik hareketleri bakımından bilişim sistemine girme suçunun işlenmesinin zorunlu olduğu kabul edilebilir[117].

Yargıtay bilişim sisteminde şifre değişikliğinin söz konusu olduğu olaylarda 243'üncü madde ile 244'üncü maddenin içtimaı konusunda farklı kararlar vermiştir. Yargıtay 12. Ceza Dairesi'nin TCK'nın 244/2'nci fıkrasında ile 243'üncü maddesi arasında geçit suç olduğu sonucuna ulaştığı bir kararına göre; "*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*" hukuka aykırıdır[118].

Yargıtay başka şifre değiştirmenin söz konusu olduğu bir kararında bilişim suçuna girme suçunun yanında ayrıca TCK'nın 244/2'nci fıkrasından hüküm kurulması gerektiği yönünde görüş beyan etmiştir. Karara göre, "*sanığın katılan ...'in hesaplarının şifresini ele geçirip, ardından şifreleri değiştirmesi şeklindeki eylemi ile şikayetçi ...'dan para istemesi eyleminin iki ayrı suçu oluşturması karşısında; TCK'nın 44. maddesinin uygulanma imkanının bulunmadığı, ayrıca iddia makamının talep ettiği kanun maddesinin sanık için kazanılmış hak oluşturmayacağı da göz önüne*

[117] Dülger diğer seçimlik hareketler için somut olaya göre değerlendirme yapılması gerektiğini ileri sürmektedir. bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 298.
Yazıcıoğlu, 243'üncü madde ile 244'üncü madde arasında zorunluluk unsurunun oluştuğu gerekçesiyle geçit suç söz konusu olduğunu, bu sebeple failin yalnızca ağır suçtan sorumluluğun doğması gerektiğini savunmaktadır. Bkz.Yazıcıoğlu, **Hackerler ve Bilişim Sistemine Girme Suçu**, s. 1260.

[118] 12. CD., E. 2016/10818 K. 2017/7390 T. 11.10.2017, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.

alındığında, tebilğnamedeki TCK'nın 243/1 maddesi gereğince bozma isteyen düşünceye iştirak edilmemiş olup, sanığın katılan ...'in e posta adresinin ve facebook hesabının şifresini kırması, ardından da şifreyi değiştirmesi şeklindeki eyleminden dolayı TCK'nın 244/2 maddesinde düzenlenen bilişim sistemindeki verileri bozma yok etme, erişilmez kılma, sisteme veri yerleştirme suçundan da mahkumiyet kararı verilmesi gerekirken yazılı şekilde hüküm kurulması" kararı verilmiştir[119].

TCK'nın 244'üncü maddesinin 1'inci ve 2'nci fıkrasında yer alan seçimlik hareketler aynı zamanda serbest hareketli suçlar olduğu için failin fiilinin her iki fıkrada yer alan seçimlik harekete de girmesi mümkündür. Böyle bir durumda 1'inci fıkra 2'nci fıkraya göre daha öncelikli konumda yer aldığı için 1'inci fıkranın uygulanması gerekir[120]. Bir bilişim sistemine ait şifrenin değiştirilmesi Yargıtay uygulamalarında farklılık arz etse de, TCK'nın 244'üncü maddesi bakımından ilk fıkrada yer alan bilişim sisteminin işleyişinin engellenmesi seçimlik hareketini de oluşturacağından şifrenin değiştirilmesi halinde 244/1 gereğince hüküm kurulması gerekmektedir[121]. Bu sebeple bilişim sistemine girilerek şifre değiştirilmesi halinde geçit suç bakımından zorunluluk unsuru oluşmayacağından 243'üncü maddeyle 244/1'inci maddeden cezai sorumluluğun doğması gerekir.

Yargıtay 4. Ceza Dairesi ise "*Sanığın katılanın şifresini kırmak suretiyle girdiği facebook hesabında katılan tarafından yazılmış intiba uyandıracak biçimde ve*

---

[119] 15. CD., E. 2017/31912 K. 2018/2652 T. 17.4.2018, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.
Aynı yönde bkz. "Sanığın katılanın şifresini kırmak suretiyle girdiği facebook hesabında katılan tarafından yazılmış intiba uyandıracak biçimde ve katılanı küçük düşürücü ifadeler yazma şeklindeki eyleminin TCK'nın 244/2. maddesinde düzenlenen bilişim sistemine veri yerleştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede hataya düşülmek suretiyle sanığın TCK'nın 243/1. maddesi gereğince cezalandırılmasına ve ayrıca bilişim sistemine veri yerleştirme suçundan dolayı suç duyurusunda bulunulmasına karar verilmiş ise de, karşı temyiz olmadığından bozma yapılamayacağı" 4. CD., E. 2013/19106 K. 2014/14018 T. 28.4.2014, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019. "Katılan şirketin sistemine hukuka aykırı olarak girerek, sistemin işleyişini engelleme, bozma, sistemdeki verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme, var olan verileri başka bir yere gönderme şeklindeki TCK.nun 244/1-3. madde ve fıkralarında yazılı hallerin gerçekleşmemesi nedeniyle, anılan mad- denin 4. fıkrasının uygulanamayacağı, katılan şirkete ait sisteme hukuka aykırı olarak girme ve orada kalmaya devam etme şeklindeki eylemin TCK.nun 243/1. madde ve fıkrasında düzenlenen suçu oluşturacağının gözetilmemesi, Yasaya aykırı", 8. CD., E. 2016/104 K. 2016/7753 T. 13.6.2016, Çevrimiçi, lexpera.com.tr, Erişim Tarihi:3.4.2019.
[120] Karagülmez, **a.g.e**., s.239.
[121] Bkz. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 298,332.

katılanı küçük düşürücü ifadeler yazma şeklindeki eyleminin TCK'nın 244/2. maddesinde düzenlenen bilişim sistemine veri yerleştirme suçunu oluşturduğu gözetilmeden, hukuki nitelendirmede hataya düşülmek suretiyle sanığın TCK'nın 243/1. maddesi gereğince cezalandırılmasına ve ayrıca bilişim sistemine veri yerleştirme suçundan dolayı suç duyurusunda bulunulmasına karar verilmiş ise de, karşı temyiz olmadığından bozma yapılamayacağı" yönünde karar vermiştir. Ancak sanığın sosyal medya hesabına veri yükleyebilmesi için mevcut teknolojik gelişmeler altında sosyal medya hesabına girmesi zorunludur. Dolayısıyla 244/2 fıkrası kapsamındaki sisteme veri yerleştirme seçimlik hareketinin işlenmesi için bilişim sistemine girme suçundan geçilmesi gerektiğinden failin yalnızca 244/2'den cezai sorumluluğunun doğması gerekmektedir.

Diğer yandan ağır suçun fail ve mağdurunun hafif suçun fail ve mağduruyla aynı olması zorunludur. Önceki hafif suçla sonraki ağır suçun fail ve mağdurlarının farklı olması halinde her fiil bağımsız olarak değerlendirilecektir[122]. Bilişim sistemine girme suçundan geçilerek bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçunun işlenmesi halinde hâkim somut olayda fail ve mağdurların kim olduğunu tespit ederek geçit suçun olup olmadığına karar vermelidir.

Geçit suçun varlığı için aranan diğer bir koşul ise, ağırlaşan sonuç ile failin bu sonuca yönelik hareketinde tek bir nedensellik bağının olması gerekir[123]. Yine belirtmek gerekir ki geçit suçun söz konusu olduğu hallerde failin kastı baştan itibaren ağırlaşan neticeye yönelik olduğu için ağır sonucun meydana gelmemesi halinde fail ağır suça teşebbüsten sorumlu olmalıdır[124]. Örneğin bilişim sisteminde yer alan verileri değiştirmek amacıyla bilişim sistemine giren fail verilere müdahale edecekken elektriklerin kesilmesi halinde bilişim sistemine girme suçundan değil, bilişim sisteminde yer alan verileri değiştirme veya yok etme suçuna teşebbüsten sorumlu tutulmalıdır.

[122] İçel, **a.g.m.**, s.47.
[123] **A.e.**
[124] **A.e.**, s.48.

Sonuç olarak, sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesi seçimlik hareketlerinin işlenmesiyle TCK'nın 244'üncü maddesinin 2'nci fıkrasında yer alan suçun oluşumuna meydan verilmesi halinde bilişim sistemine girme suçunun geçit suç olduğu kabul edilebilir. Ancak teknolojinin gelişimi de dikkate alınmalıdır. Bu noktada bilişim sistemine girmeksizin sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesini mümkün kılan bir teknolojinin varlığında artık zorunluluk unsuru ortadan kalkacağından geçit suçun varlığından da bahsedilemeyecektir.

Yukarıda ayrıntılı şekilde açıklandığı üzere görünüşte içtima için suçların haksızlık muhtevalarının örtüşmesi gerekmektedir[125]. Ancak yukarıda anılan diğer suçlarla bilişim sistemine girme suçunun haksızlık muhtevası örtüşmediği için görünüşte içtima gündeme gelmeyecektir. Ancak birden fazla suçun icra hareketlerinin kısmen veya tamamen örtüşmesi halinde farklı neviden fikri içtimaın kabulü gerekir[126]. İcra hareketlerinin örtüşmemesi halinde ise fail hem bilişim sistemine girme suçundan hem de işlediği diğer suçtan ayrı ayrı cezalandırılmalıdır.

V. MUHAKEME KURALLARI, ZAMANAŞIMI VE YAPTIRIM

A. Muhakeme Kuralları

Bilişim sistemine girme suçunun gerek temel hali gerekse nitelikli ve neticesi sebebiyle ağırlaşmış halinin yargılaması açısından görevli mahkeme 5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev Ve

[125] Göktürk, **Fikri İçtima (Suçların İçtimaı)**, s.76.

[126] Görünüşte içtima ile fikri içtimaın farklarının sonuçları vardır. Bu bakımdan bu ayrımın yapılması önem arz etmektedir.
Görünüşte içtima halinde suçlar gerçek anlamda içtima ettirilmediğinden yalnızca cezalandırılması gereken suçun kararda anılması yeterliyken fikri içtima da içtima ettiren suçların hepsinin anılması gerekir. Diğer bir sonuç ise cezanın belirlenmesi açısındandır. Görünüşte içtimada yalnızca bir suç işlendiği kabul edildiğinden cezanın bireyselleştirilmesinde cezalandırılmayan suç önem arz etmez. Ancak fikri içtimada fikri içtimaya tabi tutulan suçlar cezanın bireyselleştirilmesine etki etmektedir. Son olarak görünüşte içtimada zamanaşımı cezalandırılan suçtan itibaren başlarken fikri içtimada ise her suç bakımından ayrı ayrı işlemektedir. Bkz. Göktürk, **Fikri İçtima (Suçların İçtimaı)**, s.75-76.

Yetkileri Hakkında Kanun'un 11'inci ve 12'nci maddeleri uyarınca Asliye Ceza Mahkemeleridir.

Yetkili mahkeme ise 5271 sayılı CMK'nın 12'nci maddesi uyarınca suçun işlendiği yer mahkemesidir. Yine aynı maddesin 2'nci fıkrası uyarınca bilişim sisteminde kalma seçimlik hareketi mütemadi suç olduğu için yetkili mahkeme temadin kesildiği yer mahkemesi olacaktır. Suçun teşebbüs halinde kalması halinde son icra hareketinin yapıldığı, zincirleme suçun söz konusu olduğu durumlarda ise son suçun işlendiği yer mahkemesi yetkilidir[127].

Fiziken aynı ortamda bilişim sistemine girme suçun işlenmesi halinde yetkili mahkemenin neresi olduğunun tespitinde bir sorun bulunmamaktadır. Ancak bilişim suçları genellikle ağlar arasında işlenmektedir ve hatta söz konusu saldırılar çoğu zaman uluslararası özellik gösterebilmektedir. Bu bakımdan suçun işlendiği yer mahkemesinden ne anlaşılması gerektiği önem arz etmektedir[128].

Failin bulunduğu yer ile mağdura ait bilişim sisteminin bulunduğu yerin farklı yerlerde olduğu durumlarda ise soruşturma ve kovuşturmada yetki konusu açık bir çözüm getirmemektedir. Uygulamada ilk başlarda bu konuda tereddütler söz konusuyken son zamanlarda hem savcılıklar hem de mahkemeler mağdurun bilişim sisteminin bulunduğu yer mahkemesinin yetkili olduğu yönünde hareket etmektedir. Bazı kovuşturmalarda ise mağdurun bulunduğu yer yargı yeri olarak kabul edilmektedir. Dülger uygulamadaki bu çözümü hızlı şekilde yargılama yapmaya imkân verdiği için uygun ve işlevsel bulmasına rağmen kuramsal olarak tartışmaya açık bulmaktadır[129]. Akbulut ise fiilin işlendiği yerin failin bedenen bulunduğu yer dışında hedeflenen bilişim sisteminin bulunduğu yeri de kapsadığını belirtmiştir. Dolayısıyla yetkili mahkeme hem failin bulunduğu yer hem de bilişim sisteminin bulunduğu yer mahkemeleridir[130].

---

[127] Ahmet Gökcen, Murat Balcı, Mehmet Emin Alşahin, Kerim Çakır, **Ceza Muhakemesi Hukuku**, 3. Baskı, Ankara, Adalet Yayınevi, 2018, s. 180.
[128] Gökcen/Balcı/Alşahin/Çakır, **a.g.e.** s. 180.
[129] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 301-302.
[130] Akbulut, **Bilişim Alanında Suçlar**, s.156.

Daha az giderle ve daha süratli şekilde davaların sonuçlandırılması amaçlandığından ceza muhakemesinde yer bakımından yetki kuralları kamu düzenine ilişkin değildir[131]. Bilişim suçlarında özellikle soruşturma aşamasında delillere daha hızlı ve kolay şekilde ulaşma açısından mağdura ait bilişim sisteminin bulunduğu yerin yetki bakımından kabul edilmesi önemlidir. Nitekim bilişim suçlarında failin kimliğinin hemen tespit edilmesi mümkün olmamakta ve gerekli incelemelerin yapılmasından sonra failin kimliği ortaya çıkmaktadır. Bilişim sistemine girme suçu bakımından işlenen fiilin konusu mağdura ait bilişim sistemi olsa da ve etkisini mağdura ait bilişim sisteminde gerçekleştirse de fail suçu oluşturan fiili kendi bilişim sistemini kullanarak gerçekleştirmektedir[132]. Dolayısıyla fiilin işlendiği yer hem faile ait bilişim sisteminin hem de mağdura ait bilişim sisteminin bulunduğu yer olarak kabul edilmelidir[133].

---

[131] Gökcen, Balcı, Alşahin, Çakır, **a.g.e.** s. 182.

[132] Her ne kadar bilişim sistemine girme suçu soyut tehlike suçu olsa da, Coşkun soyut tehlike suçlarında netice bulunmadığı gerekçesiyle sadece fiilin işlendiği yerin bağlama noktası olarak kabul edilmesini doğru bulmamaktadır. İnternet kavramsal bir gerçeklik olduğu için global bir yapıdadır. Bu görüşe göre her suçun doğurduğu bir netice vardır ve neticenin doğduğu yer de bağlama noktası olarak kabul edilmelidir. Öte yandan sistemin bağlı bulunduğu serverların bulunduğu yer de bir bağlama noktası oluşturur. İnternette işlenen suçların bağlama noktalarıyla ilgili ayrıntılı bilgi ve teoriler için ayrıca bkz. Neslihan Coşkun, "İnternette Suçun İşlendiği Yer Sorunu", **Hukuki Perspektifler Dergisi**, S.4, Ağustos 2005, s.244-245. Burada neticeden öte işlenen suçun bir etkisinin olduğunun kabulüyle tipik fiilin etki ettiği yerin de bağlama noktası olarak kabul edilmesi daha uygundur.

[133] Bilişim suçlarında suçun işlendiği yer ve etki doğurduğu yerler farklı olduğu için soruşturma aşamasında delillerin elde edilmesine yönelik çalışmalar da bu yönde ilerlemektedir. Yargıtay'ın işleyişi bu yönde devam etmektedir. "E-posta adresi kullanıcısının erişiminin engellendiğine ilişkin şikâyeti üzerine öncelikle erişimi engellenen adresin ve sanığa ait olduğu iddia olunan e-mail adresinin sanığa ve şikâyetçiye ait olup olmadığı saptanmalı, bu husus ilgili internet sağlayıcısından sorularak adreslerin oluşturulma tarihi, kim tarafından oluşturulduğu ve IP (internet Protokolu) numarası sorulmalıdır. ... ...'den de erişimin engellediği iddia olunan tarih/tarihler ve takip eden günlerde şikâyetçinin e-mail adresine giriş yapılıp yapılmadığı, erişim sağlanmışsa IP bilgileri, bu tarihler itibariyle e-mail adresine ait şifrenin değiştirilip değiştirilmediği, değiştirilmiş ise ne zaman ve hangi IP numarası ile yapıldığı araştırılmalıdır. IP adresi kayıt bilgilerinden, ilgili Telekom Müdürlüklerinden, sisteme giriş yapan veya başarısız olan IP numaraları kullanıcılarının adres ve telefon bilgileri istenmeli, aynı şekilde sanığa ait olduğu iddia olunan e-mail adresini kullanan IP numaraları saptanıp adres ve telefon bilgileri de istenmelidir.

Erişimin sağlanamaması halinde, giriş yapmak isteyenler arasında şikâyetçinin de bulunup bulunmadığının IP numarasından tespit edilerek iddianın doğruluğu belirlenmelidir.

Şikâyetçi ve sanığın bilgisayarlarına el konulup hard diskleri incelenerek bilgisayarlar arasında bağlantı ve veri akışı olup olmadığı saptanıp ele geçirilen adresten bir başka adrese yazı veya görüntü gönderilmiş ise, bu olaya ilişkin bilgi sahipleri ile ele geçirilen adres kullanılarak ulaşılan adres sahipleri varsa tanık olarak dinlenmelidir." 8. CD., E. 2014/21961 K. 2015/12125 T. 18.2.2015, lexpera.com.tr, Erişim Tarihi: 3.4.2019.

Bilişim sistemine girme suçunun temel şekli (m. 243/1) ile daha az cezayı gerektiren halinin (m. 243/2) yabancı ülkelerde işlendiği hallerde TCK'nın 11'inci ve 12'nci maddeleri uyarınca Türkiye'de soruşturma ve kovuşturma yapılamayacaktır. Nitekim TCK'nın 14'üncü maddesi uyarınca "*11 ve 12 nci maddelerde belirtilen hallerde, soruşturma konusu suçun yer aldığı kanun maddesinde hapis cezası ile adli para cezasından birinin uygulanması seçimlik sayılmış ise soruşturma veya kovuşturma*" yapılamayacaktır. Ancak bilişim sistemine girme suçunun neticesi sebebiyle ağırlaşmış hali bakımından seçenek yaptırımlara yer verilmemiştir. Bu sebeple Türk vatandaşının yurtdışında 243/3'üncü maddede yer alan suçu işlemesi halinde TCK'nın 11/2'nci fıkra uyarınca "*yargılama yapılması zarar görenin veya yabancı hükûmetin şikâyetine bağlıdır. Bu durumda şikâyet, vatandaşın Türkiye'ye girdiği tarihten itibaren altı ay içinde yapılmalıdır*".

Bilişim sistemine girme suçuna ilişkin soruşturmalarda failin hukuka aykırı şekilde bilişim sistemine erişiminin devam edip etmediğinin tespit edilmesi önem arz etmektedir. Bu sebeple suçun konusunu oluşturan bilişim sistemine erişimin sağlandığı yerlerin özenle araştırılıp tespit edilmesi gerekmekte, bilişim sistemi içinde erişilen veriler ve kısımlar listelenmelidir[134].

B. Yaptırım ve Zamanaşımı

Bilişim sistemine girme suçunun temel hali "*bir yıla kadar hapis veya adlî para cezası*" olarak seçimlik yaptırıma tabi tutulmuştur. Bu sebeple faile hem hapis cezası hem de para cezası uygulanamaz[135]. Kanunda suçun temel şeklinde ayrıca bir alt sınır öngörülmediği için TCK'nın 49'uncu maddesi gereğince hapis cezasının alt sınır bir aydır ve 61/9'uncu fıkra gereğince adli para cezasının sınırları gün bakımından hapis cezasının sınırlarından fazla olamayacaktır. Bedeli karşılığı yararlanılabilen sistemlere karşı işlenen bilişim sistemine girme suçunun yaptırımı ise 243/3'de temel cezanın yarı oranına kadar indirilmesi şeklinde belirtilmiştir. Neticesi sebebiyle ağırlaşmış hal

[134] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 302.
[135] Yargıtay her iki yaptırımın da aynı anda uygulandığı bir kararı kanun yararına bozma sebebi sayarak, adli para cezasının uygulanmasına karar vermiştir. Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 300.

olan söz konusu suç sebebiyle sistemin içerdiği veriler yok olması ve değişmesinin yaptırımı ise "*altı aydan iki yıla kadar hapis cezası*" şeklinde belirlenmiştir. Dolayısıyla 243/3'üncü fıkranın söz konusu olduğu hallerde hâkim adli para cezasına hükmedemeyecektir.

3713 sayılı Terörle Mücadele Kanunu'nun 4'üncü maddesi kapsamında bilişim sistemine girme suçunun terör amacıyla işlenmesi hali nitelikli hal olarak kabul edilmiştir. 3713 sayılı Terörle Mücadele Kanunu'nun 5'inci maddesinin 1'inci fıkrası uyarınca bilişim sistemine girme suçunun faili yine TCK'nın 243'üncü maddesinde yer alan yaptırımlar dikkate alınarak cezalandırılacak, fakat cezası yarı oranında arttırılacaktır. Yine söz konusu fıkra, terör amacıyla işlenen bilişim sistemine girme suçu için tayin edilecek cezanın TCK'nın 243'üncü maddesinde belirlenen cezada yer alan üst sınırları aşabilmesini mümkün kılmıştır. Maddenin son fıkrasında ise cezanın ağırlaştırılmasına ilişkin bu düzenlemenin çocuklar için geçerli olmayacağı hükme bağlanmıştır[136].

TCK'nın 246'ncı maddesinde bilişim suçlarının "*işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine*" hükmolunacağı belirtilmiştir. Ancak bu düzenleme tüzel kişilere uygulanan güvenlik tedbirlerine ilişkin TCK'nın 20/2 ve 60'ıncı maddeleri ile uyumlu değildir. Nitekim 60'ıncı madde uyarınca "*bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına*" işlenmesi halinde güvenlik tedbirleri gündeme gelecektir. Bu sebeple genel hükümlerde yer alan "*tüzel kişi yararına*" ifadesi varken 246'ıncı maddede yer alan "*yararına haksız menfaat sağlanan"* ifadesi gereksiz ve fazladır. 246'ıncı maddede yer alan düzenlemenin "*bu bölümdeki suçlardan dolayı tüzel kişilere de kendilerine özgü güvenlik tedbirleri uygulanır"* şeklinde değiştirilmesi daha yerinde olacaktır[137]. TCK'nın 246'ıncı maddesi sayesinde, bilişim sistemine girme suçunun servis sağlayıcı tüzel kişinin

[136] Akbulut, **Bilişim Alanında Suçlar**, s.151; Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 274.
[137] Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku (7)**, s. 301. Aynı yönde; Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1424.

organ veya temsilcilerinin iştirakiyle ve bir kamu kurumunun verdiği iznin yetkilerinin kötüye kullanılması suretiyle işlenmesi halinde tüzel kişi sıfatını haiz servis sağlayıcılara karşı da güvenlik tedbirlerinin uygulanması söz konusu olabilecektir[138].

Bilişim sistemine girme suçunun gerek temel şekli gerekse nitelikli ve neticesi sebebiyle ağırlaşmış hali resen takip edilen suçlardır. Doktrinde bu suça ilişkin yaptırımlar da dikkate alındığında bu suçun takibinin şikâyete tutulması daha yerinde olacağı savunulmaktadır[139]. Ancak bu suçla korunan hukuki değer dikkate alındığında suçun resen takip edilen suç olarak düzenlenmesi yerindedir.

Bilişim sistemine girme suçundan mahkûm edilen kişi hakkında bir yıl veya daha az süreli hapis cezasına hükmedilmesi halinde failin kısa süreli hapis cezasının TCK'nın 50'nci maddesindeki seçenek yaptırımlara çevrilmesi mümkündür[140].

TCK'nın 66'ıncı maddesinin 3'üncü fıkrasına uyarınca "*dava zamanaşımı süresinin belirlenmesinde dosyadaki mevcut deliller itibarıyla suçun daha ağır cezayı gerektiren nitelikli halleri de göz önünde bulundurulur*" ve 4'üncü fıkrası uyarınca "… *sürelerin belirlenmesinde suçun kanunda yer alan cezasının yukarı sınırı göz önünde bulundurulur; seçimlik cezaları gerektiren suçlarda zamanaşımı bakımından hapis cezası esas alınır*".

Bilişim sistemine girme suçu bakımından seçimlik yaptırımların yer aldığı 243'ünü maddenin 1'inci fıkrası gereğince üst sınır 1 yıl iken, 2'nci fıkrası gereğince ise ilk fıkrada yer alan yaptırımlar yarı oranına kadar indirilebilmektedir. 3'üncü fıkrada yer alan neticesi sebebiyle ağırlaşmış hal bakımından ise üst sınır 2 yıldır. 3713 sayılı Terörle Mücadele Kanunu'nun 5'inci maddesinin 1'inci fıkrası gereğince TCK'nın 243'üncü maddesinde yer alan bilişim sistemine girme suçunun işlenmesi halinde ise yaptırımlar yarı oranında arttırılacaktır.

---

[138] Erdoğan, **Bilişim Sistemine Girme ve Kalma Suçu**, s.1425.
[139] Koca/Üzülmez, **Türk Ceza Hukuku Özel Hükümler**, s.819.
[140] Kısa süreli hapis cezalarının seçenek yaptırımlara çevrilme şartları ve seçenek yaptırım türleri için ayrıca bkz. Mehmet Maden, **Hapis Cezasına Seçenek Yaptırımlar**, Ankara, Adalet Yayınevi, 2012, s.151 vd.

TCK'nın 66'ıncı maddesinde yaptırımların ağırlığına göre dava zamanaşımı sürelerine yer verilmiş, söz konusu maddenin e bendinde "*beş yıldan fazla olmamak üzere hapis veya adlî para cezasını gerektiren suçlarda*" dava zamanaşımı süresinin 8 yıl olduğu hükme bağlanmıştır. Dolayısıyla bilişim sistemine girme suçu bakımından dava zamanaşımı süresi fiilin işlendiği tarihten itibaren 8 yıldır[141].

Aynı şekilde bilişim sistemine girme suçunun yaptırımları dikkate alındığında TCK'nın 68/1-e bendi gereğince ceza zamanaşımı 10 yıldır. Yani ceza zamanaşımını kesen veya durduran bir sebep olmaması halinde, bilişim sistemine girme suçuna ilişkin mahkûmiyet kararının verilmesinden itibaren 10 yıl geçtikten sonra söz konusu karara ilişkin ceza infaz edilemeyecektir.

[141] 5237 sayılı TCK'nın 66'ıncı maddesinin 2'nci fıkrasına göre "*fiili işlediği sırada oniki yaşını doldurmuş olup da onbeş yaşını doldurmamış olanlar hakkında, bu sürelerin yarısının; onbeş yaşını doldurmuş olup da onsekiz yaşını doldurmamış olan kişiler hakkında ise, üçte ikisinin geçmesiyle kamu davası düşer*". Kanun koyucu 12-15 yaş grubu ve 15-18 yaş grubu çocuklar için genel zamanaşımı sürelerini daha kısa tutmuştur. 0-12 yaş grubu arasında çocuğun cezai sorumluluğu olmadığı için bu yaş grubu için zamanaşımı belirlenmemiştir. TCK'nın maddeye ilişkin gerekçesinde neden çocuklar için daha kısa zamanaşımı kabul edildiğine ilişkin bir açıklama bulunmamaktadır.
Psikolojik değişme görüşünde ise, insanın zaman içinde kişiliğinin ve ruh halinin değiştiği fikrinden yola çıkılmaktadır. Dolayısıyla zaman içinde fiil ile fail arasındaki bağ zayıflamaktadır. Bkz. Nurullah Kunter, "Ceza Hukukunda Zamanaşımı", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doçentlik Tezi**, 1951, s.16.
Bu görüşe göre, çocukların ve ergenlerin psikolojik gelişim ve değişimi yetişkinlere göre daha hızlı olduğundan, çocuklar için daha kısa zamanaşımı öngörülmelidir. Fahri Gökçen Taner**, Ceza Hukukunda Zamanaşımı**, Ankara, Seçkin Yayıncılık, 2008, s.38.

SONUÇ

Çalışmanın ilk bölümünde ilk olarak bilişim sistemine girme suçunda yer alan terim ve ifadeler ile bilişim sistemine girme suçunun tarihsel gelişimine yer verilmiştir. Ardından bilişim sistemine girme suçunun bazı ülke mevzuatlarındaki ve Avrupa Konseyi Siber Suçlar Sözleşmesinde durumu ile suçla korunan hukuki değer incelenmiştir.

Bilişim sistemine girme suçu özel hayatın korunması, haberleşmenin gizliliği, malvarlığı hakları gibi farklı hukuki değerleri koruyan bilişim suçları ve bilişim aracılığıyla işlenen suçlar ile açısından temel bir suç tipini oluşturmaktadır. Bu sebeple bilişim sistemine girme suçunda yer alan terim ve ifadelerin ele alınması suçta ve cezada kanunilik ilkesi ve bilimsellik açısından zaruridir.

Bilişim sistemi bilgisayarı da kapsayan, kişilerin zihninde oluşturduğu işlemlerin programlar aracılığıyla üretilmesine imkân veren, kullanıcıların erişimine açık olarak verilerin düzenli ve otomatik şekilde işlenmesi, saklanması ve aktarılmasını sağlayan sistemlerdir. Her gün bilişim sistemi olarak sayılabilecek yeni teknolojik gelişmelerin getirdiği yazılım ve donanımlar hayatımıza dâhil olmaktadır. Bu sebeple yapılan bilişim sistemi tanımlarının ışığında yargı mercilerinin suçun konusunu oluşturan bir sistemin bilişim sistemi olup olmadığıyla ilgili tereddüte düşmesi halinde bilişim bilim dalı üzerine uzman bilirkişilerden yardım alması gereklidir.

TCK'nın 243'üncü maddesinin gerekçesinde ise verinin kapsamı belirtilmiştir. Buna göre "*sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır*".

Türk doktrininde gerek bilişim suçları gerekse bilişim sistemine girme suçu açısından bir terim birliğine varılamamıştır. Ancak TCK'da kabul edilen ve doktrinde de en çok kullanılan terim olan "*bilişim suçu*" terimi bu çalışmada da kullanılmıştır. Nitekim bilişim suçu terimi ilk bölümde de yer verildiği üzere doktrinde yer alan terimler arasında en üst kavram olarak değerlendirilebilir. Yine TCK ile uyumlu olması açısından "*bilişim sistemine girme suçu*" terimi çalışma içinde kullanılmıştır.

Ancak belirtmek gerekir ki bu suç seçimlik hareketli bir suçtur. Dolayısıyla bilişim sistemine girme suçu ifadesi yanlış anlaşılmalara yol açabilecek niteliktedir. Bu sebeple TCK'nın 243'üncü maddesinin başlığının "*bilişim sistemine girme veya bilişim sisteminde kalma*" olarak değiştirilmesi suç tipindeki yanılgının da önüne geçecektir.

Her ne kadar 765 sayılı TCK'da bilişim alanında suçlara yer verilse de bilişim sistemine girme suçuna suç tipi açısından en yakın suç kabul edilebilecek 765 sayılı TCK'nın 525a maddesinin 1'inci fıkrası ile izinsiz olarak kişilerin bilişim sisteminde bulunan bilgi ve verilerin bütününün veya içeriğinin hukuka aykırı olarak ele geçirilmesi yaptırıma bağlanmıştır. Dolayısıyla mülga 765 sayılı TCK döneminde bilişim sistemine girme veya orada kalma fiili tek başına bir suç tipi olarak yer almadığından, bilişim sistemine girme suçunun ilk kez 5237 sayılı TCK'da düzenlendiği kabul edilmelidir.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nin iç hukukumuza dâhil olmasıyla TCK'nın 243'üncü maddesinde "*bilişim sistemine girme*" suçu düzenlenmiş, Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 2'nci maddesinde yer alan yasadışı erişim maddesine uygun bir suç tipi düzenlemesine gidilmiştir. Ancak TCK'nın 243'üncü maddesinin ilk halinde "*hukuka aykırı olarak giren ve orada kalmaya devam eden*" ifadesi doktrinde Avrupa Konseyi Siber Suçlar Sözleşmesi'ne uygun olmadığı yönündeki haklı eleştirilerin ardından 20.3.2016 tarih ve 6698 sayılı Kanun ile "*hukuka aykırı olarak giren veya orada kalmaya devam eden*" olarak değiştirilmiştir.

Öte yandan 6698 sayılı Kanun'un 30'uncu maddesi ile getirilen veri nakillerinin hukuka aykırı olarak izlenmesi suçu bağımsız bir suç tipi olmasına rağmen ile TCK'nın 243'üncü maddesinin 4'üncü fıkrasına eklenmiştir. Bu durum suç sistematiği açısından hatalıdır. Nitekim veri nakillerinin hukuka aykırı olarak izlenmesinde suç tipinden de anlaşılacağı üzere bilişim sistemine girilmemektedir. Dolayısıyla bu suçun ayrı bir maddede düzenlenmesi gerekmektedir.

Bilişim sistemine girme suçuyla korunan hukuki değer bilişim sisteminin güvenliği ve güvenilirliğidir. Nitekim suç tipinde ayrıca herhangi bir verinin ele

geçirilmesi, öğrenilmesi gibi unsurlara yer verilmemiştir. Özel hayatın gizliliği, haberleşmenin gizliliği gibi kişilerin diğer hak ve menfaatlerinin korunması bilişim sistemine girme suçu bakımından bilişim sisteminin güvenliği çatısı altında yer alan eriyen ikinci derecede korunan hukuki değerler olabilir. Ancak fiilin sistemin içerdiği verilerin yok olması veya değişmesine sebep olmasını neticesi sebebiyle ağırlaşmış hal olarak düzenleyen 243'üncü maddenin 3'ünü fıkrası açısından bilişim sisteminin güvenliği dışında verileri gelecek müdahalelere karşı korunmaktadır.

Çalışmanın ikinci bölümünde bilişim sistemine girme suçunun unsurları detaylı olarak incelenmiştir.

TCK'nın 243'üncü maddenin 1'inci fıkrası uyarınca bilişim sisteminin bütününün yanı sıra bilişim sisteminin bir kısmı da suçun konusunu oluşturmaktadır. Bilişim sisteminin tamamından anlaşılması gereken bilişim sisteminin doğrudan kendisidir. Bilişim sisteminin bir kısmından anlaşılması gereken şey ise bilişim sisteminin ayrılmaz parçaları veya bilişim sistemini tamamlayan parçalarıdır. Dolayısıyla bilişim sisteminin tamamlayanlarından olan donanım, yazılım ile verilere girilmesi veya orada kalınması suçun oluşumuna sebebiyet verecektir. Bilişim sistemleri fonksiyonlarını veriler üzerinden yürütmektedir. Bu sebeple bilişim sisteminin bir kısmına ifadesinden bilişim sistemini oluşturan donanım ve yazılımların yanı sıra bilişim sistemini tamamlayan ve içinde veri bulundurmaya müsait USB, taşınabilir bellek gibi araçlar da anlaşılmalıdır. Bunun dışında belirtmek gerekir ki, yalnızca bir donanıma bağlı olmamakla birlikte ilgilinin mülkiyetinde olmayan donanımlar tarafından da erişilebilme özelliği olan e-posta, sosyal medya hesapları, bulut bilişim sistemleri gibi yazılımlar da bu kapsamda suçun konusunu oluşturmaktadır.

Bazı ülke mevzuatlarında yer alan düzenlemelerde yalnızca özel güvenlik önlemleriyle korunan bilişim sistemlerinin suçun konusunu oluşturduğu görülmektedir. Bilişim sistemine girme suçu ile korunan hukuki değerler dikkate alındığında bilişim sisteminin özel güvenlik önlemleriyle korunmasının aranmaması yerindedir. Fakat bilişim sistemine girilmesini önlemek amacıyla özel önlemler alan mağdurun korunması ve güvenlik önlemlerini yıkarak bilişim sistemine giren failin

tehlikeliliği açısından özel güvenlik önlemleriyle korunan bilişim sistemine girilme fiilinin cezayı ağırlaştıran nitelikli hal olarak düzenlenmesi yerinde olacaktır.

Öte yandan suçun konusu bakımından nitelik farkı olması sebebiyle kamu kurumlarına ait bilişim sistemlerinin önemi dikkate alınmalı ve özel bilişim sistemlerine göre daha fazla korunarak kamu kurumlarına karşı işlenen bilişim sistemine girme suçu cezayı ağırlaştıran bir nitelikli hal olarak düzenlenmelidir.

Doktrinde belirli bir bedel karşılığı bilişim sistemlerinin kullanılması için mekânsal anlamda hizmet veren internet kafe gibi yerlerin sunduğu hizmetlerin 243/2'nci madde kapsamına girip girmediği tartışmalıdır. Söz konusu mekânlarda verilen hizmet, bilişim sistemlerinin kullanılmasına yönelik bir özel hukuk sözleşmesi niteliğindedir. Teknik anlamda daha kapsamlı olan bilişim sisteminin aynı zamanda otomatın şartlarını sağladığı da kabul edilebilir. Bu sebeple bilgisayar, oyun konsolu gibi bilişim sistemlerinin bedeli ödenmeksizin kullanılması halinde hem karşılıksız yararlanma suçu hem de bilişim sistemine girme suçu oluşmalıdır. Bu durumda da farklı neviden fikri içtima kuralının uygulanması gerekir.

Şifreli yayınların bilişim sistemine girme suçunun konusunu oluşturup oluşturmayacağı hususu tartışma konusu olmuştur. Bu noktada tespit edilmesi gereken şifreli yayının internet üzerinden yapılan yayın üzerinden mi yoksa uydu üzerinden mi çekildiğidir. Suçu oluşturan fiilde yayın internet üzerinden çekiliyorsa bu durumda hem bilişim sistemine girme suçunun hem de karşılıksız yararlanma suçunun oluşması mümkündür.

Kablolu/kablosuz internet hatlarına erişerek başkasına ait internet hizmetinden hukuka aykırı şekilde faydalanmak TCK'nın 163'üncü maddesi kapsamında karşılıksız yararlanma suçunu oluşturmayacağı tartışılmalıdır. İnternet bilişim sistemlerinin birbirine bağlanmasına imkân veren geniş bir iletişim ağıdır. Ancak bu ortam yalnızca ağlardan oluşmamaktadır. İnternet servis sağlayıcıları belli bir bedel karşılığında kablolu veya kablosuz hatlar aracılığıyla kişilerin internete erişimini sağlamaktadır. Dolayısıyla internet başlı başına bir bilişim sistemi sayılamasa da internete erişimi sağlayan başka bileşenler bulunmaktadır. Bu bileşenler de bir bilişim

sistemini oluşturmaktadır. Bu sebeple başkasına ait bir internet hizmetinden hukuka aykırı şekilde faydalanılması halinde bilişim sistemine girme suçu oluşmalıdır.

Bilişim sisteminin soyut tamamlayanlardan olan yazılımlardan en küçük parça olan veriye kadar tüm soyut unsurların 243'üncü maddenin 3'üncü fıkrasının konusunu oluşturabileceği kabul edilmelidir.

Bilişim sistemine girme suçu bakımından bilişim sistemine girme fiilinin bilişim sisteminin fiziki tamamlayanlarına yani donanımına girme değil, soyut tamamlayanlarına girme olduğu ifade edilmiştir. Soyut tamamlayanlara girmek kablolu veya kablosuz ağ bağlantısı yoluyla olabileceği gibi, fiziki olarak da gerçekleştirilebilir.

Bilişim sistemine girme suçunun temel halinin düzenlendiği TCK'nın 243'üncü maddesinin 1'inci fıkrasında "*hukuka aykırı olarak*" ifadesine yer verilmiştir. Kanun koyucunun bu ifadeye yer vermesindeki amaç hâkimin dikkatini hukuka uygunluk sebebinin var olup olmadığının araştırılması gerekliliğine çekmektir. Burada da failin fiilinin suç oluşturduğu konusunda hataya düşmesi gündeme gelebileceğinden TCK'nın 30'uncu maddesinin 4'üncü fıkrası uyarınca kaçınılmaz bir hataya düşüp düşmediğine bakmak gerekir. Failin hatasının kaçınılmaz olması halinde fail bu hatasından yararlanır. Failin hukuka uygunluk sebeplerinin maddi koşullarında bir hataya düşmesi halinde ise TCK'nın 30'uncu maddesinin 1'inci fıkrasının uygulanıp uygulanmayacağı dikkate alınmalıdır.

Bilişim sistemine girme suçu bakımından kanun hükmünün yerine getirilmesi, meşru savunma ve ilgilinin rızası hukuka uygunluk sebebi olarak kabul edilebilir.

Rıza olmaksızın başkasına ait bir bilişim sistemine girilmesi dışında rızanın veriliş amacının dışında bilişim sistemine girilmesi veya orada kalınması da suçun oluşumuna sebebiyet verecektir. Bunun dışında mağdurun daha önceden aralarındaki şahsi ilişki ve/veya hukuki bir ilişkiye dayanarak bilişim sistemine girme veya orada kalmaya gösterdiği rıza sonrasında bu şahsi ve/veya hukuki ilişkinin sona ermesi halinde mağdurun rıza verme sebebi de ortadan kalktığından verilen rıza ortadan kalkar.

Bilişim sisteminin kullanılması konusunda rıza gösteren ve işçiye bu konuda hak devreden işverenlerin haklı nedenlerle bilişim sistemlerini izlemesi mümkündür. Ancak bu izlemenin hukuka uygunluğu işveren tarafından amaç dışı kullanımların tespiti amacıyla bilişim sistemine girilebileceği yönünde uyarı yapılmasını gerektirir. Aksi takdirde suçun oluşacağı kabul edilmelidir.

Bir bilişim sistemi sahibinin başka bir kişinin bilişim sistemini kullanmaya dair iznini istemesi ve bilişim sistemi sahibinin bunu kabul etmesiyle aralarında sözleşme kurulmuş varsayılır. Günümüzde pek çok yazılım belirli şart ve koşullarda bilişim sistemi sahibi tarafından kullanıcılara abonelik sözleşmesi, lisanslama sözleşmesi, iş görme sözleşmesi ve benzeri sözleşmelerle bu yazılımları kullanım hakkı tanımaktadır. Söz konusu sözleşmelerin içerdiği maddeler süre, bedel, kullanım şekli gibi sınırlamaya tabi tutulabilmektedir. Kullanım hakkına sahip olan kişinin sözleşmenin şartlarına uymaksızın bilişim sistemine girmesi hukuki sorumluluğun yanında cezai sorumluluğu da gündeme getirebilir. Ancak belirtmek gerekir ki her bilişim sistemi ve buna ilişkin kullanım sözleşmeleri bakımından sözleşmede kullanıcıya üçüncü kişilere yetki devri yapılabileceğine ilişkin hükmün aranması doğru bir yaklaşım olamayacaktır. Bilişim sistemi sahibi yapılan sözleşme ile sistemi kullanım hakkının üçüncü kişilere devrinin mümkün olmadığını hükme bağlamalıdır. Bu sayede bilişim sistemi kullanıcısına tanınan hakkın sınırları çizilmiş ve belirlenmiş olacaktır. Bilişim sistemine girme veya orada kalma hakkı olan kişinin bu hakkını başkalarıyla paylaşması konusunda yetkisi olmaması halinde de hem hak sahibinin hem de yetki dışı sisteme giriş yapan kişinin cezai sorumluluğu gündeme gelebilecektir.

Bilişim sistemi sahibinin verdiği yetkinin dışına çıkılarak bilişim sistemine erişilmesi halinde mevcut düzenleme gereğince suçun oluştuğunun kabul edilmesi gerekse de söz konusu yetki aşımının sözleşmenin ihlalini oluşturduğu ve yalnızca özel hukuk açısından sorumluluk doğuracağı yönünde bir algının oluşması da muhtemeldir. Ancak korunan hukuki değerin bilişim sistemine duyulan güven olduğu dikkate alınmalıdır. Bu sebeple yetki aşımının suç oluşturup oluşturmayacağına ilişkin

ihtilafların önüne geçebilmek adına CFAA'de yer alan düzenleme gibi yetki aşımının da suç oluşturacak şekilde düzenlenmesi önemlidir.

Meşru savunmanın mümkün olup olmadığı saldırının niteliğine göre bazı hallerde kabul edilebilir. Bilişim sistemine saldırı ağ bağlantısı üzerinden yapılıyorsa ve mağdur bunun farkındaysa bilişim sistemi kapatıldığında veya ağ bağlantısı kesildiğinde saldırı engellenmiş olacağından meşru savunma mümkün olmayacaktır. Öte yandan bilişim sistemine yapılan saldırıya karşı meşru savunmada bulunabilecek kişinin bilişim sistemleri ve saldırılar bakımından yeterli teknik bilgiye sahip olduğu dikkate alınmalıdır. Bu kişilerin yapılan saldırıların ne olduğunu ve bunları nasıl engelleyebileceğini bilmesi de ihtimal dâhilindedir. Dolayısıyla somut olaya göre meşru savunmanın şartlarının oluşup oluşmadığına bakılmalıdır.

Kanun hükmünü yerine getirme TCK'da sayılan diğer bir hukuka uygunluk sebebidir. Kanun ve yönetmeliklere uygun şekilde ve koşulların sağlanarak yetkili kişiler tarafından bilişim sistemine girilmesi veya kalınması halinde hukuka uygunluk sebeplerinden kanun hükmünün yerine getirilmesi söz konusu olacaktır.

Üçüncü bölümde ise suçun nitelikli hallerine ve neticesi sebebiyle ağırlaşmış haline yer verilmiş, bilişim sistemine girme suçu bakımından kusurluluk, özel görünüş biçimleri, muhakeme kuralları ve zamanaşımı ile ilgili değerlendirmeler yapılmıştır.

Bedeli karşılığı yararlanılabilen bilişim sistemlerine girme veya orada kalma suçunun cezanın hafifletilmesini sağlayan bir nitelikli hal olarak düzenlenmiştir. Bedeli olsun yahut olmasın bu suç tipiyle korunmak istenen temel hukuki değer bilişim sisteminin güvenliği ve güvenilirliğidir. Belirli bir kesime açık veya kapalı olması bilişim sisteminin güvenliği ve güvenilirliğinin korunan hukuki değer olmasını ortadan kaldırmayacağı gibi, bu durum nitelikli hal ile korunan hukuki değerin önemini de azaltmayacaktır. Bedeli karşılığı yararlanılabilen bilişim sistemlerine girme ve orada kalma fiilleri hem temel hal hem de nitelikli hal ile korunan hukuki değer açısından ayrı ayrı değerlendirmeye muhtaçtır. Bedeli ödenmeksizin bir bilişim sistemine girme ve orada kalma fiili bedel olarak istenen şeyin niteliğine de bağlı olarak bilişim sistemi sahibinin ve zilyedinin malvarlığı haklarını ihlal edici

niteliktedir. Dolayısıyla bedeli ödenmeksizin bir bilişim sisteminde kalma fiilinin cezayı hafifleten değil ağırlaştıran bir nitelikli hal olarak düzenlenmesi gerekmektedir.

Doktrinde taksirle bilişim sistemindeki verilerin yok olması ve değişmesi seçimlik neticelerine ek olarak, Fransız Ceza Kanunu'nun 323-1'inci maddesinde olduğu gibi "*bilişim sisteminin işleyişinin herhangi bir şekilde değişimine neden olunması*" da seçimlik netice olarak eklenmelidir. Nitekim bilişim sisteminin işleyişinin engellenmesi veya bozulması da en az verilerin yok olması veya değişmesi kadar önemli ve ağır neticelerdir. Bilişim sistemine girme suçu neticesinde taksirle bilişim sisteminin bizzat işleyişine etki eden veri ve programların yok edilmesi veya değiştirilmesinin de hukuk düzenince korunması evleviyetle gereklidir.

Bilişim sistemine girme suçu bakımından hukuka aykırı fakat bağlayıcı emrin yerine getirilmesi hariç kusurluluğu azaltan ve kaldıran sebeplerin hepsinin gündeme gelebilmesi mümkündür. Kusurluluğu kaldıran veya azaltan hallerde hataya düşmesi halinde ise TCK'nın 30'uncu maddesinin 3'üncü fıkrası gereğince failin hatasının kaçınılmaz olması halinde fail bu hatasından yararlanacaktır.

Bilişim sistemine girme seçimlik hareketi bakımından teşebbüs mümkündür. Hem bilişim sistemine girme hem de bilişim sisteminde kalma fiili açısından bir netice aranmasa da girme fiili icra hareketleri kısımlara bölünebilir nitelikteyken, bilişim sisteminde kalma fiili için bu mümkün olmadığından bu seçimlik hareket bakımından teşebbüs mümkün değildir.

Fail fiilini hukuka uygun kılan sebebin (örneğin rızanın) kalktığını öğrenir öğrenmez sistemi terk etmeye çalışmasına rağmen sistemden çıkamaz ve sistemde kalırsa bilişim sisteminin tamamında veya bir kısmında hukuka aykırı olarak kalma bakımından suçun işlenmesine yönelik iradi bir hareket olmadığı için bilişim sistemine girme suçunun oluşmadığını söylemek mümkündür.

Tek bir kişi tarafından işlenmesi mümkün olan bilişim sistemine girme suçu birden fazla kişinin işbirliğiyle de işlenebilir.

TCK'nın 243'üncü maddesi kapsamında failin bedeli karşılığı yararlanılabilen bir sisteme girip taksirli hareketi neticesinde bu sistemde yer alan verilerin yok olması veya değişmesi halinde failin cezai sorumluluğu tartışmalıdır. İşlenen fiilin kanunda öngörülen ağır neticelere yol açtığı hallerde, özel norm-genel norm ilişkisi gereğince fail temel suçtan değil neticesi sebebiyle ağırlaşmış suçtan sorumlu olacaktır. Bu doğrultuda ilk önce 243/3'üncü fıkra uyarınca neticesi sebebiyle ağırlaşmış suça ilişkin ceza belirlenmeli, daha sonra 243/2'inci fıkra uyarınca bedeli karşılığı yararlanılan sistemler suçun konusunu oluşturduğu için failin cezasında indirime gidilmelidir.

Failin çok uzun bir zaman aralığında mağdurun bilişim sistemine girmesi veya orada kalması halinde ise failin aynı suç işleme kararıyla hareket edip etmediğinin tespiti önem arz etmektedir. Örneğin failin mağdura ait bilişim sistemine tekrar tekrar kolaylıkla girmesini sağlayan ve bilişim sistemini bilişim korsanının girişine her an açık tutan "*backdoorların*" tespit edilmiş ve mağdura ait bilişim sistemine birden fazla kez girilmiş olması halinde ilk girişten itibaren uzun bir süre geçmiş olsa da aynı suç işleme kararı olup olmadığının araştırılması gerekir.

Mağdura ait bir donanım aracılığıyla bilişim sistemine girildikten sonra ve hala bilişim sisteminde kalmaya devam ederken mağdura ait olan fakat farklı sunucularda kayıtlı olan program ve yazılımlara erişilmesi halinde fail tek bir bilişim sistemine girme suçundan sorumlu olmalıdır. Ancak söz konusu sonuca ulaşmadan somut olayın koşulları dikkate alınarak failin fiilinin tek hareket oluşturup oluşturmadığının değerlendirilmesi gerekir.

Aynı mağdura ait farklı bilişim sistemlerine aynı suç işleme kastıyla farklı zamanlarda girilmesi halinde zincirleme suç hükümleri uygulanmalıdır. Nitekim bilişim sistemi burada suçun konusudur. Aynı mağdura ait olduktan sonra bilişim sistemlerinin farklı olması bu manada farklılık arz etmemelidir. Bilişim sistemine girme suçu açısından aynı neviden fikri içtimaın uygulanabilmesi de mümkündür.

Doktrindeki tartışmaların esas noktası bilişim sistemine girme suçu ile diğer bilişim suçlarının fikri içtimaı üzerinedir.

Doktrinde bazı yazarlar bilişim sistemine girme suçunun diğer bazı suçların işlenmesi için geçit suç oluşturduğunu savunmaktadır. Geçit suçtan söz edebilmek için ağırlaşan sonucun gerçekleşmesinde geçilen hafif suçun işlenmesinin zorunlu olması gerekir. Bu bağlamda aynı hukuki değerin korunmadığı suçlar açısından ayrıca bir zorunluluk değerlendirilmesi yapılmasına gerek yoktur. Ancak 244/1-2'nci fıkralar açısından bilişim sistemine girme suçunun zorunlu olup olmadığının incelenmesi gerekir. Sistemi engelleme, bozma veya verileri yok etme, değiştirme suçlarının işlenmesi için bilişim sistemine girme suçunun her zaman zorunlu olduğundan bahsedilemeyecektir. Sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesi seçimlik hareketlerinin işlenmesiyle TCK'nın 243'üncü maddesinin 2'nci fıkrasında yer alan suçun oluşumuna meydan verilmesi halinde bilişim sistemine girme suçunun geçit suç olduğu kabul edilebilir. Ancak teknolojinin gelişimi de dikkate alınmalıdır. Bu noktada bilişim sistemine girmeksizin sistemde bulunan verilerin değiştirilmesi, sisteme veri yerleştirilmesi veya var olan verilerin başka bir yere gönderilmesi mümkün bir teknolojinin varlığında artık zorunluluk unsuru ortadan kalkacağından geçit suçun varlığından da bahsedilemeyecektir. Görünüşte içtima için suçların haksızlık muhtevalarının örtüşmesi gerekmektedir. Ancak yukarıda anılan diğer suçlarla bilişim sistemine girme suçunun haksızlık muhtevası örtüşmemesi görünüşte içtima gündeme gelmeyecektir. Ancak suçların icra hareketlerinin kısmen veya tamamen örtüşmesi halinde farklı neviden fikri içtimaın kabulü gerekir. İcra hareketlerinin örtüşmemesi halinde ise fail hem bilişim sistemine girme suçundan hem de işlediği diğer suçtan ayrı ayrı cezalandırılmalıdır.

Bilişim suçlarında özellikle soruşturma aşamasında delillere daha hızlı ve kolay şekilde ulaşma açısından mağdura ait bilişim sisteminin bulunduğu yerin yetki bakımından kabul edilmesi önemlidir. Nitekim bilişim suçlarında failin kimliğinin hemen tespit edilmesi mümkün olmamakta ve gerekli incelemelerin yapılmasından sonra failin kimliği ortaya çıkmaktadır. Bilişim sistemine girme suçu bakımından işlenen fiilin konusu mağdura ait bilişim sistemi olsa da ve etkisini mağdura ait bilişim sisteminde gerçekleştirse de fail suçu oluşturan fiili kendi bilişim sistemini kullanarak gerçekleştirmektedir. Dolayısıyla yetki sorununun çözümünde fiilin işlendiği yer hem

faile ait bilişim sisteminin hem de mağdura ait bilişim sisteminin bulunduğu yer olarak kabul edilmelidir.

KAYNAKÇA

Akbulut, Berrin Bozdoğan: "Bilişim Suçları", **Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi**, C.8, S. 1-2, 2000, s.545-555.

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

Akgündüz, Haluk, Eşref Adalı: "Atanmış Sistemler ile Bilgisayar Kümesi Tasarımı ve Mevcut Sistemler ile Karşılaştırması", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi**, C. 8, S. 2, 2015, s.17-30.

Akıncı, Hatice, A. Emre Alıç,

Cüneyd Er: "Türk Ceza Kanunu ve Bilişim Suçları", **İnternet ve Hukuk**, (Derleyen: Yeşim M. Atamer), İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2004.

Aktaş, Onur: **Siber Güvenlik Hacking Atölyesi**, 2. Baskı, Ankara, Gazi Kitabevi, 2018.

Apaydın, Cengiz: "Bilişim Sistemine Girme Suçu", **TAAD**, Yıl:7, Sayı:24, Ocak 2016, s. 245-308.

Apaydın, Cengiz: **Bilişim Suçları ve Bilişim Ceza Hukuku**, İstanbul, Acar Matbaacılık, 2017.

Apiş, Özge: "Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri", **Yasama Dergisi Kamu Yönetiminde Teknoloji Özel Sayısı II**, C.12, S.37, Haziran 2018, s. 49-86.

Artuk, Mehmet Emin, Ahmet

Gökcen, Ahmet Caner

Yenidünya: **Ceza Hukuku Özel Hükümler**, 15. Baskı, Ankara, Adalet Yayınevi, 2015.

Aydın, Emin D.: "Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları", **Marmara İletişim Dergisi**, İstanbul, S.1, Aralık 1992.

Aydın, Emin D.: **Bilişim Suçları ve Hukukuna Giriş**, Ankara, Doruk Yayınevi, 1992.

Bağcı, Hasan: "Sosyal Mühendislik ve Denetim", **Denetişim Dergisi**, Kış 2009, s.42-51.

Baytaz, Abdullah Batuhan: **Kanunilik İlkesi Bağlamında Ceza ve Ceza Muhakemesi Hukukunda Yorum**, İstanbul Arşivi, İstanbul, On İki Levha Yayıncılık, 2018.

Bellia, Patricia L.: "A Coda-Based Approach to Unauthorized Access Under tne Computer Fraud snd Abuse Act", **The George Washington Law Review**, Vol. 84:1442, No:6, December 2016, https://heinonline.org/HOL/Page?handle=hein.journals/gwlr84&collection=journals&id=1526&startid=&endid=1560 , s.1443-1476.

Berber, Leyla Keser: **Adli Bilişim**, Ankara, Yetkin Yayınları, 2004.

Biçkin, İnci: "Siber Suç Sözleşmesi ve 5237 sayılı Türk Ceza Kanununda Bilişim Suçları", **Yargıtay Dergisi**, C.32, S.1-2, Ocak-Nisan 2006, Ankara, s.145-168.

Boss, Richard W.: "Intranet and Extranet", **PLA Tech Notes**, American Library Association, (Çevrimiçi), https://alair.ala.org/bitstream/handle/11213/258/Intranets%20and%20Extranets.pdf?sequence=93&isAllowed=y, 2010, Erişim Tarihi: 02.11.2017.

Bourgeois, Dave /David T. Bourgeois: "What Is an Information System?", **Information Systems for Business and Beyond,** Çevrimiçi, https://bus206.pressbooks.com, Erişim Tarihi: 07.07.2018.

Bregant, Jessica/ Robert Bregant: "Cybercrime and Computer Crime", **The Encyclopedia of Criminology and Criminal Justice,** First Edition, Edited by Jay S. Albanese, John Wiley & Sons Inc., 2014.

Çakır, Hüseyin, Mehmet Serkan Kılıç: **Güncel Tehdit: Siber Suçlar**, Ankara, Seçkin Yayıncılık, 2014.

Camgöz, Nilgün: "Siber Uzay, Sanal Gerçeklik ve Müze", Bilim ve Teknik Dergisi, Ocak 1998, Çevrimiçi, http://www.biyolojiegitim.yyu.edu.tr/fizuzaypdf/Siberuzay19984S.pdf, Erişim Tarihi: 13.11.2017.

Canberk, Gürol/Şeref Sağıroğlu: "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", **Politeknik Dergisi**, C.9, S.3, 2006, s.165-174.

Çetin, Erol, İsmail Malkoç: **Uygulamada Sahtekarlık Suçları, Bilgisayar Suçları, Tebligat Suçları ve İlgili Mevzuat**, Ankara, Adalet Yayınevi, 1995.

Ceyhun, Yurdakul/Ufuk

Çağlayan: **Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta**, Ankara, Türkiye İş Bankası Kültür Yayınları, 1997.

Chang, Jason V.: "Computer Hacking: Making the Case for a National Reporting Requirement", **The Berkman Center for Internet & Society Research Publication Series**, Research Publication No. 2004-07, 2004, Çevrimiçi, http://cyber.law.harvard.edu/publications , Erişim Tarihi: 27.09.2018, s. 1-39.

Chawki, Mohamed: "A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy", (Çevrimiçi), http://www.droit-tic.com/pdf/chawki4.pdf, Erişim Tarihi: 01.11.2017.

Chawki, Mohamed: "Unauthorized Access Offences in Cyberworld", **Cybercrime, Digital Forensics and Jurisdiction**, Chawki, M./ Darwish, A., Khan, M.A., Tyagi, S., (Çevrimiçi), http://www.springer.com/gp/book/9783319151496, Switzerland, 2015, s.27-37.

Cook, David: "The Court's nonsensical approach to unauthorised access in DPP v Bignell", (Çevrimiçi), http://www.pannone.com/media-centre/blog/cybercrime-blog/the-court's-nonsensical-

approach-to-unauthorised-access-in-dpp-v-bignell, Erişim Tarihi:20.11.2017.

Coşkun, Neslihan: "İnternette Suçun İşlendiği Yer Sorunu", **Hukuki Perspektifler Dergisi**, S.4, Ağustos 2005, s.238-245.

Craig, Brain: **Cyberlaw: The Law of the Internet and Information Technology**, New Jersey, Pearson Education, 2013.

Cupa, Basil: "Trojan Horse Resurrected - On The Legality Of The Use Of Government Spyware", **Living in Surveillance Societies: 'The State of Surveillance**, Edit. Webster, C William R. Living, Zurich Open Repository and Archive, University of Zurich, 2013, s.419-428.

Değirmenci, Olgun: "2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi", **TBB Dergisi**, S.58, 2005, s.195-208.

Değirmenci, Olgun: "Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi**, İstanbul, 2002.

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

Demirel, Muhammed: **Suça İştirakte Bağlılık Kuralı**, İstanbul Arşivi, İstanbul, On İki Levha Yayınları, 2017.

Dikmen, Esra: "Manevi, Mali veya Bağlantılı Haklara Tecavüz Suçları (FSEK m. 71/1-1)", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2018.

Dönmezer, Sulhi: **Kişilere ve Mala Karşı Cürümler**, 17. Baskı, İstanbul, Beta Basım A.Ş., 2004.

Doyle, Charles: "Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws", **Congressional Research Service**, 2014, (Çevrimiçi), https://fas.org/sgp/crs/misc/97-1025.pdf, Erişim Tarihi: 5.12.2017.

Duisberg, Alexander: "Q&A: The use of court-ordered Trojans in Germany", Çevrimiçi, https://www.twobirds.com/en/news/articles/2017/germany/q-and-a-the-use-of-court-ordered-trojans-in-germany, Erişim Tarihi: 13.02.2019.

Dülger, Murat Volkan, Gözde Modoğlu: **Bilişim Suçları, Soruşturma ve Kovuşturma Yöntemleri ile İnternet İletişim Hukuku Uygulama Rehberi**, Ankara, Avrupa Birliği ve Konseyi Ortak Yayını, 2014.

Dülger, Murat Volkan: "Bilişim Sistemleri Üzerinde Arama, Kopyalama ve El Koyma Tedbiri", (Çevrimiçi), https://www.academia.edu/9449240/BİLİŞİM_SİSTEMLERİ_ÜZERİNDE_ARAMA_KOPYALAMA_VE_EL_KOYMA_TEDBİRİ, t.y.

Dülger, Murat Volkan: "Karşılaştırmalı Hukuk Bağlamında Birleşik Krallık (İngiltere) Hukukunda Bilişim Suçları Mevzuatı ve Uygulaması", **TAAD**, Yıl:8, Sayı: 31, Temmuz 2017, 141-257.

Dülger, Murat Volkan: "Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla

Korunması", **İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi**, S.3 (2), Güz 2016, s. 101-167.

Dülger, Murat Volkan: "Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi", **Bilişim Hukuku**, Der: Mete Tevetoğlu, İstanbul, Kadir Has Üniversitesi Yayını, 2006, s.398–422.

Dülger, Murat Volkan: **Bilişim Suçları ve İnternet İletişim Hukuku**, 6. Baskı, Ankara, Seçkin Yayıncılık, 2015.

Dülger, Murat Volkan: **Bilişim Suçları ve İnternet İletişim Hukuku**, Tamamen Güncellenmiş 7. Baskı, Ankara, Seçkin Yayıncılık, 2018.

Dülger, Murat Volkan: **Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2004.

Dursun, Selman: "İnternetten Kaynaklanan Ceza Sorumluluğundaki Gelişmeler", **MHB- Prof. Dr. Gülören Tekinalp'e Armağan**, C. 1-2, 2003, s.253-289.

Elbahadır, Hamza: **Hacking Interface**, 17. Baskı, İstanbul, Kodlab, 2018.

Erdağ, Ali İhsan: "Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)", **Doç.Dr. Mustafa Yıldız'a Armağan-Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C. XIV, S. 2, Aralık 2010, s.275-304.

Erdem, Ümit, Çağrı Şükrü

Uluslu, Gökberk Dumancı: **Yargıtay (2014-2016) Kararlarında Sosyal Medya**, İstanbul, Legal Yayıncılık, 2016.

Erdoğan, Yavuz: "Bilişim Sistemine Girme ve Kalma Suçu", **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, C.12, Özel S., 2012, s.1363-1433.

Erdoğan, Yavuz: "Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011.

Erdoğan, Yavuz: **Türk Ceza Hukuku'nda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2013.

Erem, Faruk: "Ceza Hukukunda "Hakkın Kullanılması"", **AÜHFD**, C.41, S.1, Ankara, 1990, s.5-17.

Ersoy, Yüksel: "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", **AÜSBFD**, C:49, S.3, 1994, s.149-183.

Esen, Sinan: **Anlatımlı ve İçtihatlı Malvarlığına Karşı Suçlar, Belgede Sahtecilik ve Bilişim Alanında Suçlar**, Ankara, Adalet Yayınevi, 2007.

Etter, Barbara: "Computer Crime", **4th National Outlook Symposium on Crime in Australia, New Crimes or New Responses 21-22 June 2001**, (Çevrimiçi), http://aic.gov.au/media_library/conferences/outlook4/etter.pdf, Erişim Tarihi: 02.11.2017.

Foreman, Gene: **The Ethical Journalist: Making Responsible Decisions in the Pursuit of News**, West Sussex, Wiley-Blackwell, 2010.

Gemalmaz, H. Burak: "Çalışanların İnternet İletişiminin İşverence İzlenmesi Özel Yaşam Hakkına Aykırı Mıdır?: AİHM Büyük Dairenin 05 Eylül 2017 Tarihli Barbulescu Kararı", **Lexpera Blog**, Çevrimiçi, http://blog.lexpera.com.tr/calisanlarin-internet-iletisiminin-isverence-izlenmesi-ozel-yasam-hakkina-aykiri-midir-aihm-buyuk-dairenin-05-eylul-2017-

tarihli-barbulescu-karari/ , 7.9.2017, Erişim Tarihi: 27.01.2019.

Girgenti, Elkin: "Computer Crimes", **American Criminal Law Review**, Vol.55:911, 2018, Çevrimiçi, https://heinonline.org/HOL/Page?handle=hein.journals/amcrimlr55&collection=journals&id=933&startid=&enddid=982 , Erişim Tarihi:2.4.2019, s.912-958.

Gökcen, Ahmet, Murat

Balcı, Mehmet Emin Alşahin,

Kerim Çakır: **Ceza Muhakemesi Hukuku**, 3. Baskı, Ankara, Adalet Yayınevi, 2018.

Göktürk, Neslihan: "Suçun Yasal Tanımında Yer Alan "Hukuka Aykırılık" İfadesinin İcra Ettiği Fonksiyon", **İnönü Üniversitesi Hukuk Fakültesi Dergisi**, C. 7, S. 1, 2016, s.407-450.

Göktürk, Neslihan: **Fikri İçtima (Suçların İçtiması)**, Ankara, Adalet Yayınevi, 2013.

Gorn, Saul: "Informatics (Computer And Information Science): Its Ideology, Methodology, And Sociology", **The Studies of Information: Interdisciplinary Messages**, Edit. Machlup, F. and Mansfield, U., Eds., New York, Wiley, 1983, s. 121–140.

Granger, Sarah: "Social Engineering Fundamentals, Part I: Hacker Tactics", 2001, Çevrimiçi, https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics , Erişim Tarihi:3.10.2018.

Gül, Ahmet: **Doğrudan / Dolaylı Bilişim Suçları**, Ankara, Seçkin Yayıncılık, 2016.

Gürsel, İlke: **İşçinin Kişisel Verilerinin Korunması Hakkı**, Ankara, Adalet Yayınevi, 2016.

Heickerö, Roland: **The Dark Side of The Internet**, (Translated by Martin Peterson), Frankfurt, Peter Lang GmbH, 2013.

Hendler, James: "It's Time to Reform the Computer Fraud and Abuse Act", 2013, (Çevrimiçi), https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/, Erişim Tarihi:27.11.2017.

İçel, Kayıhan, İzzet Özgenç,

Adem Sözüer, Fatih S.

Mahmutoğlu, Yener Ünver: **Suç Teorisi**, İstanbul, Sebat Mümessillik Yayıncılık, 1999.

İçel, Kayıhan: "Görünüşte Birleşme (İçtima) İlkeleri ve Yeni Türk Ceza Kanunu", **İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi**, Y. 7, S. 14, Güz 2008, s. 35-49.

İçel, Kayıhan: **Suçların İçtimaı**, İstanbul, İstanbul Üniversitesi Hukuk Fakültesi Yayını, 1972.

İçer, Zafer: "Türk Ceza Hukukunda Tüzel Kişiler", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, İstanbul, 2011.

İçer, Zafer: "Suça Teşebbüste Hazırlık Hareketleri ile İcra Hareketlerinin Birbirinden Ayrılması Meselesi",

Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi, İstanbul, 2017.

Ifrah, Georges: **Bilgisayar Ne Sayar: Rakamların Evrensel Tarihi XI**, (Çeviri: Kurtuluş Dinçer), Ankara, Tübitak Popüler Bilim Kitapları, 2002.

Ippolito, Carlo Sarzana di S.: "Bilişim Alanındaki Yeni Teknolojilerin Hukuksal Yansıması, İtalya'daki Durum", (Çeviri: Vesile Sonay Daragenli), **Prof. Dr. Türkan Rado'ya Armağan**, İstanbul,1997, s.389-405.

Jourdan, Guy-Vincen: "Command Injection", Çevrimiçi, http://www.site.uottawa.ca/~gvj/Courses/CSI4539-OLD/lectures/CommandInjections.pdf, Erişim Tarihi: 12.02.2019.

Juo, James: "The CFAA and Aaron's Law", **Virginia Lawyer**, V.62, December 2013, (Çevrimiçi), http://www.vsb.org/docs/valawyermagazine/vl1213-tech.pdf, Erişim Tarihi: 27.11.2017, s.61-62.

Kabay, M. E.: "Glossary of Computer Crime Terms", (Çevrimiçi), http://www.mekabay.com/overviews/glossary.pdf, 2008.

Karaçay, Timur: "Veri Tipleri", http://www.baskent.edu.tr/~tkaracay/etudio/ders/prg/c/dataTypes.pdf , Erişim Tarihi: 14.11.2017.

Karagülmez, Ali: **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**, 3. Baskı, Ankara, Seçkin Yayıncılık, 2011.

Kardaş, Ümit: "Bilişim Dünyası ve Hukuk", **Karizma Dergisi**, S.13, 01.03.2003.

Kaya, Mine: **Elektronik Ortamda (Elektronik Haberleşme-İnternet –Sosyal Medya) Kişilik Haklarının Korunması**, Ankara, Seçkin Yayıncılık, 2015.

Kaya, Özen: "5237 Sayılı Türk Ceza Kanunu'nda Karşılıksız Yararlanma Suçu", **Gazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi,** Ankara, (Çevrimiçi), tez.yok.gov.tr, 2011, Erişim Tarihi:12.4.2019.

Kerr, Orin S.: "Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes", **NYU Law Reviews**, (Çevrimiçi), http://www.nyulawreview.org/issues/volume-78-number-5/cybercrimes-scope-interpreting-access-and-authorization-computer-misuse, 2003, pp. 1596-1668.

Ketizmen, Muammer: **Türk Ceza Hukukunda Bilişim Suçları**, Ankara, Adalet Yayınevi, 2008.

Koca, Mahmut, İlhan Üzülmez: **Türk Ceza Hukuku Özel Hükümler**, 5. Baskı, Ankara, Adalet Yayınevi, 2018.

Koca, Mahmut, İlhan Üzülmez: **Türk Ceza Hukuku Genel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2018

Koca, Mahmut: "Haberleşmenin, Konuşmanın ve Özel Hayatın Gizliliğini İhlal Suçları (TCK m.132-134)", **Ceza Hukukunun Güncel Sorunları**, Erzurum, 8 Ekim 2010, s.63-115.

Korkmaz, İbrahim: **Kişisel Verilerin Ceza Hukuku Kapsamında Korunması**, Ankara, Seçkin Yayıncılık, 2017.

Kudlich, Hans, İlker Tepe: "Online Aramaların Uygulanabilirliği Üzerine", **Ceza Muhakemesi Önlemleri ve Özellikle Gizli Araştırma Önlemleri**, (Proje Yöneticisi: Kayıhan İçel, Edit.: Yener Ünver), Ankara, Seçkin Yayıncılık, 2011.

Kudlich, Hans: "Ceza Kovuşturmasında Federal Truva Atları-Dijital Çağda Özel Yaşam Alanının Korunması", (Çev. Rabia Ünlü), **Alman-Türk Karşılaştırmalı Ceza Hukuku**, (Haz. Eric Hilgendorf, Yener Ünver), C.1, Yeditepe Üniversitesi Hukuk Fakültesi, İstanbul, 2010.

Kumar, Manoj, Anuj Rani: "Computer Crime IT Laws in Ireland and India", (Çevrimiçi), https://www.researchgate.net/publication/235769188, 2013.

Kunter, Nurullah: "Ceza Hukukunda Zamanaşımı", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doçentlik Tezi**, 1951.

Kurt, Levent: **Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması**, Ankara, Seçkin Yayıncılık, 2005.

Lorenz, Nicole: "German party FDP also brings up constitutional complaint against federal trojan", Çevrimiçi, https://blog.avira.com/germany-constitutional-complaint-against-federal-trojan/, Erişim Tarihi: 13.02.2019.

MacEwan, Neil: "The Computer Misuse Act 1990: lessons from its past and predictions for its future", **Criminal Law Review**, 2008, (Çevrimiçi), http://usir.salford.ac.uk/15815/7/MacEwan_Crim_LR.pdf, Erişim Tarihi:20.11.2017.

Maden, Mehmet: **Hapis Cezasına Seçenek Yaptırımlar**, Ankara, Adalet Yayınevi, 2012.

Mahmutoğlu, Fatih Selami: "Türk Ceza Kanununda Yer Alan Bilişim Alanındaki Suçlar ve Karşılaşılan Sorunların Yargı Kararları Işığında Değerlendirilmesi", **İÜHFM**, C. LXXI, S. 1, s. 891-890.

McQuade, Sam: "Technology- enabled Crime, Policing and Security", **Journal of Technology Studies**, (Çevrimiçi), http://scholar.lib.vt.edu/ejournals/JOTS/v32/v32n1/pdf/mcquade.pdf, 2006, Erişim Tarihi: 02.11.2017, s.32-42.

Mouton, Francois, Louise

Leenen, H.S. Venter: "Social engineering attack examples,templates and scenarios", **Computers & Security,** V. 59, 2016, Çevrimiçi, https://www.researchgate.net/publication/299344351_Social_engineering_attack_examples_templates_and_scenarios , Erişim Tarihi: 3.10.2018, s.186 – 209.

Natsui, Takato: "Cybercrimes in Japan: Recent Cases, Legislations, Problems And Perspectives", **Meiji Law Journal**, Vol.10, March 2003, s.1-34.

Önder, Ayhan: **Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar**, İstanbul, Filiz Kitapevi, 1994.

Önok, Murat: "Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği", **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi - Prof. Dr. Nur Centel'e Armağan**, 2013, C.9, S. 2, s.1299-1269.

Özbek, Veli Özer, Koray

Doğan, Pınar Bacaksız, İlker

Tepe: **Türk Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Seçkin Yayıncılık, 2017.

Özen, Muharrem, Gürkan

Özocak: "Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134)", **Ankara Barosu Dergisi (1)**, 2015, s.41-77.

Özgenç, İzzet: **Türk Ceza Hukuku**, 14. Baskı, Ankara, Seçkin Yayıncılık, 2018.

Pallı, Hayati: "Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları", **Erciyes Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, Kayseri, 2008.

Pamuk, Gülfem: "Türk ve Fransız Ceza Muhakemesi Hukukunda Mağdurum Makam Olarak Yeri", **Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlamamış Doktora Tezi**, İstanbul, 2012.

Parlar, Ali: **Bilişim Alanında İşlenen Suçlar**, Ankara, Bilgi Yayınevi, 2011.

Pekmez, Tuba Kelep: "Otonom Araçların Kullanımından Doğan Cezaî Sorumluluk: Türk Hukuku Bakımından Genel Bir Değerlendirme", **Ceza Hukuku ve Kriminoloji Dergisi, S.** 6(2), 2018, s. 173-195.

Picotti, Lorenzo: "Report-Italy", **Preparatory Colloquium Section II**, (Çevrimiçi),

http://www.aidpitalia.org/docs/Verso%2019%20Congresso%20AIDP/Sect%20II%20AIDP%20-%20Italy%20Report%20Picotti.pdf, 05.03.2018.

Savaş, Abdurrahman: **İnternet Ortamında Yapılan Sözleşmeler**, Konya, Adal Ofset, 2005.

Sciglimpaglia, Robert J.Jr.: "Computer Hacking: A Global Offense", **Pace International Law Review**, V.3, I.1., 1991, Çevrimiçi, http://digitalcommons.pace.edu/pilr/vol3/iss1/8, Erişim Tarihi: 05.07.2018, s. 201-253.

Sevük, Handan Yokuş: **Türk Ceza Hukuku Özel Hükümler**, Ankara, Adalet Yayınevi, 2018.

Sieber, Ulcrich: **İnternetteki Suçlar ve Suçun İnternette Takibi**, (Edit.: Yener Ünver), Ankara, Seçkin Yayıncılık, 2014.

Sieber, Ulrich: "Cybercrime and Jurisdiction in Germany, The Present Situation and the Need for New Solition",**Cybercrime and Jurisdiction**, Editor: Bert-Jaap Koops, Susan W. Brenner, Leiden, T.C.M. Asser Press, 2006.

Sokullu-Akıncı, Füsun: "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler Ve Özellikle İnternette Çocuk Pornografisi", **İstanbul Üniversitesi Hukuk Fakültesi Mecmuası**, S. 59 (1-2), 2011, s.11-38.

Soyaslan, Doğan: **Ceza Hukuku Özel Hükümler**, 11. Baskı, Ankara, Adalet Yayınevi, 2016.

Sözüer, Adem: "Hukuki Hata", **Yargıtay Dergisi**, C.21, S.4, Ekim 1995, s.466-490.

Sözüer, Adem: **Suça Teşebbüs**, İstanbul, Kazancı, 1994.

Stephenson, Peter: **Computer-Related Crime: a Handbook For Corporate Investigation**, Florida, CRC Press LLC, 2000.

Şahin, Cumhur: **Ceza Muhakemesi Hukuku I**, 9. Baskı, Ankara, Seçkin Yayıncılık, 2018.

Şahin, Meral Ekici: "Ceza Hukukunda Rıza", **Ankara Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, Ankara, 2010.

Şenay, Levent: "Bilgisayar Programlama", Çevrimiçi, http://kisi.deu.edu.tr//levent.senyay/bilgisayarprogramlama/1_%20Bilg%20prog%20giriş.pdf , Erişim Tarihi: 07.07.2018.

Taner, Fahri Gökçen: **Ceza Hukukunda Zamanaşımı**, Ankara, Seçkin Yayıncılık, 2008.

Talas, Serdar: "Ceza Hukukunda Kusur İlkesi Bağlamında Nedeninde Serbest Hareket (actio libera in causa) Kavramı ve Geçici Nedenlerin Ceza Sorumluluğuna Etkisi", **İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi**, İstanbul, 2011.

Taşdemir, Kubilay, Ramazan Özkepir: **Uygulamada-Öğretide Belgede Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar Açıklamalı-İçtihatlı**, Ankara, Adil Kitapevi, 1999.

Taşkın, Şaban Cankat: "Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları", **Marmara Üniversitesi Sosyal Bilimler**

Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul, 2008.

Taşkın, Şaban Cankat: **Bilişim Suçları**, Bursa, Beta Yayınları, 2008.

Tepe, İlker: "Modern Ceza Hukuku Anlayışında İnternet Suçluluğu Ve Türk Ceza Hukukundaki Yansımaları", **Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi**, Antalya, 2009, (Çevrimiçi), tez.yok.gov.tr , Erişim Tarihi: 03.08.2018 .

Tepe, İlker: "Yeni Bir Temel Hak Olarak "Bilişim Teknolojisi Sistemlerinin Gizliliğinin ve Bütünlüğünün Korunması Hakkı"-Alman Federal Anayasa Mahkemesi'nin "Online Arama" Kararının Sistematik Analizi", **Karşılaştırmalı Güncel Ceza Hukuku Serisi (13)-İnternet Hukuku**, (Proje Yöneticisi: Kayıhan İçel, Edit.: Yener Ünver), Ankara, Seçkin Yayıncılık, 2013, s.387-413.

Tezcan, Durmuş, Mustafa

Ruhan Erdem, R. Murat Önok: **Teorik ve Pratik Ceza Özel Hukuku**, 14. Baskı, Ankara, Seçkin Yayıncılık, 2017.

Turan, Metin: **Bilişim Hukuku**, Ankara, Seçkin Yayıncılık, 2016.

Ünver, Yener: **Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer**, Ankara, Seçkin Yayıncılık, 2003.

Üstün, Gül Fiş: "*Disiplin Soruşturmalarında Hukuka Aykırı Deliller",* **Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi**, C. 24, S.1, İstanbul, Haziran 2018, s.17-35.

Vermesan, Ovidiu/Peter

Friess/Patrick Guillemin/

Harald SundMaeker/Markus

Eissenhauer/Klaus Moessner/

Frank Le Gall/Philippe Cousin:"Internet of Things Strategic Research and Innovation Agenda", **Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems,** Edit.: Ovidiu Vermesan, Peter Friess,(Çevrimiçi), http://www.internet-of-things-research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf, Aalborg, River Publishers, 2013, Erişim Tarihi:31.10.2017.

Walden, Ian: "Computer Crime", (Çevrimiçi), http://kavehh.com/my%20Document/KCL/Internet%20Law/Internet%20Material/Computer%2520Crime%2520%25286th%2520ed.%2529.pdf, Erişim Tarihi: 01.11.2017.

Westerhorstmann, Kristin: "The Computer Fraud and Abuse Act: Protecting the United States from Cyber-Atacks, Fake Dating Profiles, and Employees Who Check Facebook at Work**", University of Miami National Security & Armed Conflict Law Review**, V. 145, 2015, (Çevrimiçi), https://repository.law.miami.edu/cgi/viewcontent.cgi?referer=https://www.google.com.tr/&httpsredir=1&article=1078&context=umnsac, Erişim Tarihi: 22.11.2017.

Whitehouse, Sheldon: "Hacking into the Computer Fraud and Abuse Act: The CFAA at 301", **The George Washington Law**

Reviewer, V.84, No.6, December 2016, (Çevrimiçi), http://www.gwlr.org/wp-content/uploads/2016/11/84-Geo.-Wash.-L.-Rev.-1437.pdf, Erişim Tarihi: 27.11.2017, s.1437-1441.

Winn, Peter A.: "The Guilty Eye: Unauthorized Access, Trespass and Privacy", **The Business Lawyer**, Vol.62, August 2007, Çevrimiçi, https://heinonline.org/HOL/Page?handle=hein.journals/busl62&collection=journals&id=1411&startid=&endid=1454 , Erişim Tarihi: 2.4.2019.

Wyatt, Derek: "'Revision of the Computer Misuse Act': Report of an Inquiry by the All Party Internet Group", **All Paert Parliamentary Internet Group**, 2004, (Çevrimiçi), https://www.cl.cam.ac.uk/~rnc1/APIG-report-cma.pdf, Erişim Tarihi: 20.11.2017.

Yaşar, Osman, Hasan Tahsin

Gökcan, Mustafa Artuç: **Yorumlu-Uygulamalı Türk Ceza Kanunu**, C.5, 2. Baskı, Ankara, Adalet Yayınevi, 2014.

Yazar Yok: U.S. Departman of Justice Bureau of Statistic, **Computer Crime Legislative Resource Manual,** (Direktor: Benjamine H. Renshaw), Washington D.C., 1990, (Çevrimiçi), https://www.ncjrs.gov/pdffiles1/Digitization/78890NCJRS.pdf, Erişim Tarihi: 27.11.2017.

Yazar Yok: UK Parliament, "Computer Crime", **Postnote**, October 2006, No:271, Çevrimiçi, www.parliament.uk/parliamentary_offices/post/pubs2006.cfm, Erişim Tarihi: 30.10.2017.

Yazıcıoğlu, R. Yılmaz: **Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları ile**, İstanbul, Alfa Yayınevi, 1997.

Yazıcıoğlu, Yılmaz: "Bilgisayar Ağlar ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002, s. 451-470.

Yazıcıoğlu, Yılmaz: "Hackerler ve Bilişim Sistemine Girme Suçu", **Ord. Prof. Dr. Sulhi Dönmezer Armağanı**, C.II, Ankara, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu, Atatürk Araştırma Merkezi ve Türk Ceza Hukuku Derneği Yayını, s. 1239-1261.

Yenidünya, Caner, Olgun Değirmenci: **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları**, İstanbul, Legal Yayıncılık, 2003.

Yenidünya, Caner: "Bilişim Sistemine Hukuka Aykırı Erişim Suçu (TCK m.243)", **Legal Fikri ve Sınai Haklar Dergisi**, S.4, 2005, s.1018-1042.

Yenisey, Feridun: "İnternet Suçlarının Yeni İşleniş Biçimleri", **Uluslararası İnternet Hukuku Sempozyumu 21-22 Mayıs 2001**, İzmir, Dokuz Eylül Üniversitesi Yayınları, 2002.

Yıldız, Sevil: **Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi**, Ankara, Nobel Yayın Dağıtım, 2007.

Yılmaz, Sacit: **Türk Ceza Hukuku Sisteminde Siber Suçlar**, Ankara, Adalet Yayınevi, 2016.

Yılmaz, Zahit, Özge Apiş: "Karşılıksız Yararlanma Sucu (TCK m.163)", **Marmara Üniversitesi Hukuk Fakiltesi Hukuk Araştırmaları**

Dergisi Özel Sayı: Prof. Dr. Nur Centel'e Armağan, İstanbul, C.19, S.2.,2013, s. 1749-1779.

İnternet Kaynakları

tdk.gov.tr

sinerji.com.tr

lexpera.com.tr

kazancı.com

https://www.cybrary.it/glossary/

http://www.cybercrimelaw.net