TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU

ANABİLİM DALI

BİLİŞİM SİSTEMİNE GİRME SUÇU (TCK m. 243)

Tezli Yüksek Lisans Tezi

Sami KABADAYI

Ankara,2021

TÜRKİYE CUMHURİYETİ

ANKARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

KAMU HUKUKU

ANABİLİM DALI

BİLİŞİM SİSTEMİNE GİRME SUÇU (TCK m. 243)

Tezli Yüksek Lisans Tezi

Sami KABADAYI

Prof. Dr. Muharrem ÖZEN

Ankara,2021

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU
ANABİLİM DALI

BİLİŞİM SİSTMEİNE GİRME SUÇU (TCK m. 243)

YÜKSEK LİSANS TEZİ

Prof. Dr. Muharrem ÖZEN

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	**İmzası**
1- Prof. Dr. Muharrem ÖZEN	
2- Prof. Dr. Devrim GÜNGÖR	
3- Doç. Dr. Önder TOZMAN	

Tez Savunması Tarihi

09.02.2021

<u>Tez Doğruluk Beyanı Belgesidir</u>.

T.C.
ANKARA ÜNİVERSİTESİ
Sosyal Bilimler Enstitüsü Müdürlüğü'ne,

Prof. Dr. Muharrem ÖZEN danışmanlığında hazırladığım "Bilişim Sistemine Girme Suçu (TCK m. 243) (Ankara,2021) " adlı yüksek lisans tezimdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallarına uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul edeceğimi beyan ederim.

Tarih:
Adı-Soyadı ve İmza

İÇİNDEKİLER

İKİNCİ BÖLÜM

TÜRK CEZA KANUNUN 243. MADDESİNDE DÜZENLENEN SUÇ TİPLERİ

KISALTMALAR

AÜ	: Ankara Üniversitesi
ABD	: Amerika Birleşik Devletleri
AET	: Avrupa Ekonomi Topluluğu
AKSSS	: Avrupa Konseyi Siber Suçlar Sözleşmesi
ANDÜ	: Anadolu Üniversitesi
AÜSBFD	: Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
B.	: Baskı
Bknz.	: Bakınız
C.	: Cilt
Çev.	: Çeviren
ÇÜ	: Çağ Üniversitesi
DARPA	: Defense Advanced Research Projects Agency
Der.	: Dergisi
Derl.	: Derleyen
DÜ	: Dicle Üniversitesi
E.	: Esas
E. T.	: Erişim Tarihi

Edt.	: Editör
GÜ	: Gazi Üniversitesi
İİBF	: İktisadi İdari Bilimler Fakültesi
INTERPOL	: The International Criminal Police Organization
İÜ	: İstanbul Üniversitesi
İÜHFM	: İstanbul Üniversitesi Hukuk Fakültesi Mecmuası
K.	: Karar
Matb.	: Matbaacılık
MMFD	: Mimarlık Mühendislik Fakültesi Dergisi
MUÜ	: Muğla Üniversitesi
MÜ	: Marmara Üniversitesi
MÜHFHD	: Marmara Üniversitesi Hukuk Fakültesi Hukuk Dergisi
NSF	: National Scince Foundation
ODTÜ	: Orta Doğu Teknik Üniversitesi
S.	: Sayı
s.	: Sayfa
SBE	: Sosyal Bilimler Enstitüsü
SÜ	: Selçuk Üniversitesi
SÜHFD	: Selçuk Üniversitesi Hukuk Fakültesi Dergisi
TBD	: Türkiye Bilişim Derneği

TBMM : Türkiye Büyük Millet Meclisi

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TMK : Terörle Mücadele Kanunu

TÜİK : Türkiye İstatistik Kurumu

Yay. : Yayıncılık

YCGK : Yargıtay Ceza Genel Kurulu

GİRİŞ

Çağımızda teknoloji ve bilişim sistemleri her geçen gün artan bir ivme ile gelişmektedir. Hatta öyle ki yakın geçmişte dahi çok uzun süreler alan iş ve işlemler teknolojinin ve bilişim sistemlerinin hızlı gelişimi sayesinde günümüzde artık çok daha kısa sürede, çok daha kolay olarak gerçekleştirilebilmektedir. Ticaretten askeri teknolojiye, eğitimden haberleşmeye kadar birçok alanda bilişim sistemleri ve teknoloji hayatımızın her alanına sirayet etmiş durumdadır.

Esasen bilişim sistemlerine yönelik gerçekleştirilen ihlallerin teker teker sayılması mümkün değildir. Değişen ve gelişen teknolojiyle birlikte her gün yeni yöntemler bulunmakta ve kullanılmakta, alınan güvenlik tedbirlerini aşılmaya çalışılmaktadır. Bu nedenle hayatın her alanında karşımıza çıkan bilişim sistemlerinin korunması büyük önem arz etmektedir.

Elbette bilişim sistemlerinin alınacak siber yahut fiziksel tedbirlerle korunması mümkündür. Ancak bunun yanında hukuk da bilişim sistemlerini korunmasında önemli bir yere sahiptir. Bu nedenle bilişim sistemlerine yönelik gerçekleştirilen hukuka aykırı eylemlerinde bir yaptırım ile karşı karşıya bırakılmıştır.

Önceleri Türk Hukuku'nda bilişim suçlarının failleri genel normlar yahut duruma uygun düşebilecek diğer kanun maddeleri uyarınca cezalandırılmaya çalışılıyordu. Hukuk sistemimizdeki bu eksiği gidermek amacıyla yapılan ilk düzenleme 1991 yılında mülga 765 Sayılı TCK'da değişiklik yapılması suretiyle gerçekleştirilmiştir. Değişen ve gelişen teknoloji ile bilişim suçlarının da değişmesi bu düzenlemelerin yetersiz kalmasına sebep olmuştur. Bu nedenle 5237 Sayılı TCK'da *"Bilişim Suçları"* bölümüne yer verilmiş ve bu bölümde yetersiz kalan hükümler değiştirilerek yeniden ele alınmış ve yeni suç tipleri düzenlenmiştir.

Çalışmanın birinci bölümünde; bilişim, bilgisayar, veri ve internet gibi temel kavramlar üzerinde durulmuş, bu kavramlar doktrin ve uygulamadaki tanımlar ile izah edilmiştir. Ayrıca bilişim suçlarının tanımı, bilişim suçlarının tarihsel gelişimi ile ulusal ve uluslararası mevzuatlarda bilişim suçlarının nasıl ele alındığı incelenmiştir. Özellikle AKSSS ile Türk Hukuku'nda yer alan bilişim suçlarına ilişkin düzenlemeler üzerinde durulmuştur. Ayrıca yine bilişim suçlarının failleri ile faillerin kullandığı yöntemler de yine ilk bölümde açıklanmaya çalışılmıştır.

İkinci bölümünde ise; 5237 Sayılı TCK'nın 243/1-2-3. fıkraları ile düzenlenen *"Bilişim sistemine girme suçu"* ile yine aynı kanunun 243/4. fıkrasında düzenlenen *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini İzleme"* suçu, suçun unsurları itibariyle ayrıntılı olarak ele alınmıştır.

BİRİNCİ BÖLÜM

TEMEL KAVRAM VE BİLGİLER

I. TEMEL KAVRAMLAR

A. BİLİŞİM

Bilişim kelimesinin tanımı için ilk başvurulması gereken kaynak doğal olarak TDK güncel sözlüğüdür. TDK, bilişim kavramı için *"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 bir tanımlama kullanmıştır. Yine tanımda kullanılan *"Enformatik"* kelimesi için TDK'nın sözlüğü incelendiğinde, kelimenin kökeninin Fransızca *"informatique"* kelimesi olduğu görülecektir.[1]

Ülkemizde *"Bilişim"* ve *"Bilgisayar"* kavramlarını ilk kullanan kişi Prof. Dr. Aydın KÖKSAL'dır. Prof. Dr. Aydın Köksal anılan kavramlara 1981 yılında yayınladığı *"Bilişim Terimleri Sözlüğü"* isimli sözlükte yer vermiştir.[2] Bu sözlükte bilişim kavramı *"İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve*

[1] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[2] Türksel KAYA **BENGSHİR**, *"Türkiye'de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler"*, Ammde İdaresi Der., C. 35, S. 1, 2002, s. 82.

ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da geniş anlamda, bilişimin kapsamı içerisinde yer alır. bk. özdevimli bilgi işlem." şeklinde tanımlanmıştır.[3]

Esasen Güncel Türkçe Sözlük'te *"Bilişim"* kavramının eş anlamlısı olarak yer alan *"Enformatik"* kelimesini bilgisayar dünyasında ilk kullanan kişi 1957 yılında *"Informatik:Automatische Informationsverarbeitung"* yani *"Enformatik: Otomatik Bilgi İşleme"* başlıklı yazısıyla Alman bilim adamı Karl Steinbuch'tır. Daha sonra *"informatique"* şeklindeki kelime Fransız bilim adamı Philippe Dreydus tarafından 1962 yılında *"bilgisayar bilimi"* olarak kabul edilmiştir. Sürecin devamındaysa kelime Orta Avrupa'da yaygınlaşmıştır.[4]

Türk Hukuku'nda *"Bilişim"* kavramı ilk olarak 1989 Tarihli Ceza Kanunu Ön Tasarısı'nda kullanılmıştır. Ön Tasarı'da yer alan 342. maddenin madde gerekçesinde bilişim *"bilgileri depo ettikten sonra bunları otomatik işleme tabi tutma sistemlerinden*

---

[3] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[4] CJB (Jerry) **LE ROUX**, *"Social and Community informatics Past, Present, & Future: An Historic Overview Keynote Address"*, 10th Annual DIS Conference: 10-11th September 2009, s. 3.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.551.1067&rep=rep1&type=pdf (E. T. 30.03.2020)

oluşan alan" şeklinde tanımlanmıştır.[5] Daha sonra mülga 765 Sayılı TCK'da 1991 tarihinde *"Bilişim Alanı'nda Suçlar"* başlıklı bazı maddelerin eklenmesiyle *"Bilişim"* kelimesi ilk kez Türk Ceza Hukuku'nda bir kanun metninde kullanılmıştır[6].

2005 tarihli 5237 Sayılı TCK'da ise *"Topluma Karşı Suçlar"* başlığı altında *"Bilişim Alanında Suçlar"* karşımıza çıkmaktadır. TCK'nın *"Bilişim sistemine girme"* başlıklı 243. maddesinin düzenleme altına alınması sırasında 1991 tarihli yasanın ön tasarı metninde kullanılan ifade, genel hatlarıyla korunmuş ve kanun koyucu tarafından kaleme alınan madde gerekçesinde bilişim sistemi *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerdir."* ifadeleriyle tanımlanmıştır.[7]

Doktrinde ise *"Bilişim"* kavramı çok çeşitli şekillerde tanımlanmıştır:

"Bilişim, hem verilerin işlenmesini, yani bilgi işlemi, hem de bilgi işlemin sonucunun aktarılmasını, yani veri iletişimini ifade eden bir kavramdır."[8]

"Bilişim, bilgi teknolojilerinin tümünü ve bu arada bilgisayar kavramını da içine alan bir üst kavram olarak karşımıza çıkmaktadır. Bilişim; insanların teknik, ekonomik, toplumsal, hukuk ve benzeri alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, elektronik makineler aracılığıyla depolanması, işlenmesi ve değerlendirilmesi,

---

[5] Murat Volkan **DÜLGER**, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yay., B. 6, Ankara 2017, s. 76-77.

[6] Ali Haydar **DOĞU**, Bilişim Hukuku, Ekin Yay., B. 2, Bursa 2017, s. 129.

[7] http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc (E.T. 30.03.2020)

[8] Berrin **BOZDOĞAN AKBULUT**, *"Bilişim Suçları"*, SÜHFD, Konya 2000, C. 8, S. 1-2, s.546.

organize edilmesi, ses, görüntü ve veri taşıyan iletişim hatları ile kullanıcılara ulaştırılması bilimidir."[9]

"Bilişim, insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir."[10]

"Bilişim, her alandaki üretilmiş bilgileri içeren verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili bilim dalıdır."[11]

"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 dalıdır."[12]

---

[9] Ramazan **DOĞAN**, 5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları, Adalet Yay., B. 1, Ankara 2014, s. 6.

[10] DÜLGER, s. 75.

[11] Levent **KURT**, Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulamaları, Seçkin Yay., B. 1, Ankara 2005, s. 25.

[12] Büşra **ÖZÇELİK**, Bilişim Sistemine Girme Suçu, Yayımlanmamış Yüksek Lisans Tezi, İÜ SBE, İstanbul 2019, s. 6.

"Bilişim: bilgisayardan yararlanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini ifade eder."[13]

Görüldüğü üzere, doktrindeki tanımlar farklı olsa da genel itibariyle *"Bilişim"* kavramının tanımı öz itibariyle birbirinden uzak değildir. Hatta tanımların bilişim sistemlerinin otomatik veri işleyen, verileri depolayabilen yahut aktarabilen özelliklerinin olması gibi birçok ortak noktası da bulunmaktadır.[14]

Enformasyon ve bilişim kelimeleri başlangıçta, bilgisayar ve bilişim dünyasıyla sınırlı bir çağrışım yapıyordu. Ancak günümüzde artık enformatik yani bilişim daha geniş bir alan olarak tanımlanmakta ve yapay zeka, bilişsel bilim, bilgisayar bilimi, bilgi bilimi, gibi çok farklı alanları kapsamaktadır.[15] Yani yukarıda yer alan tanımlar ilk olarak kişide bilgisayar kelimesini çağrıştırıyor olsa da esasen bilişim tanımları dikkatle incelendiğinde bilişim kavramının bilim ve bilgisayarı da kapsayan bir üst kavram, bilgisayar kavramının ise bu bilim dalının kullandığı araçlardan sadece birisi olduğu net bir şekilde anlaşılacaktır.[16] Nitekim Yargıtay da gerek mülga 765 Sayılı TCK döneminde vermiş olduğu bir kararında ATM'lerin otomatik işleme tabi tutulmuş bir sistem ünitesi olduğunu

---

[13] Sinan **ESEN**, Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, B. 1, Adalet Yay., Ankara 2007, s. 624.

[14] ÖZÇELİK, s. 5-6.

[15] LE ROUX, s.4.

[16] Yavuz **ERDOĞAN**, Türk Ceza Kanunu'nda Bilişim Suçları, B. 1, Legal Yay., İstanbul 2013, s. 8.

vurgulamış[17] gerekse de 5237 Sayılı TCK döneminde vermiş olduğu bir kararında bilişim sistemlerinden yalnızca bilgisayarın anlaşılmaması gerektiğini[18] açıkça ifade etmiştir.

---

[17] *"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 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 ya da 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*

Yine doktrinde de *"Bilişim"* kavramının *"Bilgisayar"* kavramından daha geniş bir anlamı olduğu ve birçok yabancı hukuktan farklı olarak mevzuatımızda *"Bilişim"* kavramının kullanılmasının daha doğru olduğu savunulmuştur. Nitekim bilişim sistemleri

---

kabul edilmesi de olanaklı değildir." YCGK, 10.04.2001, 2001/6-30 E., 2001/57 K. Sayılı Kararı, www.kazanci.com.tr (E. T. 24.03.2020).

[18] "*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. 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, 19.06.2007, 2007 / 6-136 E., 2007 / 150 K. Sayılı Kararı, www.kazanci.com.tr (E. T. 24.03.2020).

doğası gereği veri toplayabilen, işleyebilen, saklayabilen, değerlendirebilen, çoğaltabilen ve aktarabilen ve bütün bu işlemleri çok yönlü olarak yapabilen sistemlerdir. Ancak bilgisayarın bu fonksiyonların tamamı yerine bir kısmını yerine getirmesi yine de bilgisayar olarak anılması mümkündür.[19] Bilişim sistemleri kavramı, bilgisayarın yanı sıra akıllı telefonlar, tabletler, elektronik imza, E-Devlet uygulamaları, yazılımlar gibi dijital ortamdaki tüm iş ve işlemleri yapabilen sistemleri kapsamaktadır[20].

B. BİLGİSAYAR

5237 Sayılı TCK'nın 243. maddesinde doğrudan *"Bilgisayar"* ifadesi yer almamakta, *"Bilişim Sistemleri"* ibaresine yer verilmektedir. Esasen yukarıda da izah edildiği üzere *"Bilişim"* kavramı üst kavramdır. Bununla beraber *"Bilgisayar"* bilişim alanının kullandığı araçlardan en önemlisi olarak kabul edilmelidir. Bu nedenle bu kavramın da izah edilmesine yarar görmekteyim.

[19] Özge **APİŞ**, *"Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri"*, Yasama Der., 2018, S. 37, s. 82.

[20] Yağmur **SÖNMEZ**, *"Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları"*, Yayımlanmamış Yüksek Lisans Tezi, MÜ SBE, İstanbul 2018, s. 6.

TDK'ya göre bilgisayar; *"Çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"* anlamına gelmektedir.[21]

Yine Bilişim Terimleri Sözlüğü'ne göre bilgisayar: *"Çok sayıda aritmetiksel ya da mantıksal işlemlerden oluşan bir işi, çalışması sırasında bir işletmen'in işe karışması gerekmeksizin, önceden verilmiş bir izlenceye göre, özdevimli olarak yürüten bir veri işleyici. Bir bilgisayar dizgesi elektronik ve mekanik birimlerden oluşan donanım ile bu donanım birimlerini ya da kaynakları istenen işlere yöneltip verimli bir çalışma düzeni içerisinde kullanabilmek için gerekli tüm izlencelerden ve veri yapılarından oluşan yazılım öğelerini kapsar. Minibilgisayar, mikrobilgisayar tanımlarının dışındaki geleneksel bilgisayarlar ana işlem birimlerinin hız ve yapısına, ana belleklerinin sığasına, dış belleklerin ve giriş-çıkış birimlerinin türlülüğüne, sayısına ve hızına göre büyük, ortaboy ya da küçük dizgeler olarak sınıflandırılır."*[22]

Doktrinde *"Bilgisayar"* kavramına ilişkin çeşitli tanımlar mevcuttur:

"Bilgisayar, programlara ve verilen komutlara göre işlem yapan otomatik olarak çalışan, sıralı işlem yapan, verileri depolama, işleme tabi tutma, tasnif ve terkip etme, iletme özelliklerine sahip olan, elektronik ya da manyetik akımlarla çalışan, mantıklı sonuçlar üreten, programlanabilen, genel amaçlı kullanabilme özelliklerine sahip elektronik cihazlar olarak tanımlanabilir."[23]

---

[21] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[22] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[23] KURT, s. 31.

"Bilgisayar, insan tarafından hazırlanarak verilen bilgileri, yine insanlar tarafından hazırlanan komutlar dizisine uygun biçimde, istenilen düzeyde ve şekilde işleyen ve bu bilgileri veren veya depolayan elektronik cihazlardır."[24]

"Bilgisayar, kısa bir tanımla bilgi depolayıp işleme tabi tutan ve sonucunu gösteren bir araçtır. Ancak bütün unsurlarını içerecek bir şekilde tanım yapmak isteyenler, sonuçta aynı kavramı tanımlamakla beraber, birbirinden az veya çok farklı tanımlar yapmaktadır."[25]

"Bilgisayarlar, insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler şeklinde tanımlanabilir."[26]

"Bilgisayar, yeterince kavramsallaştırılmış ve iyi tanımlanabilmiş her türlü problem üzerinde çalışabilen bir aygıttır."[27]

Bütün bu tanımların ortak noktaları gözetildiğinde bilgisayar, insanlar tarafından verilen komutlar çerçevesinde bilgileri tasnif ederek saklamaya, bilgi ve sonuç üretmeye, içerisindeki bilgi ve belgelerde işlem yapmaya imkân sağlayan elektronik cihaz olarak tanımlanabilecektir.

---

[24] Halil Ünsal **NAMAZCI**, Herkes İçin Temel Bilgisayar ve İnternet Kılavuzu, Bayrak Matb., İstanbul 2012, s. 15.

[25] Yücel **ERSOY**, *"Genel Hukuki Koruma Çerçevesinde Bilişim Suçları"*, AÜSBFD, Ankara 1994, C. XLIX, No. 3-4, s. 150.

[26] BOZDOĞAN AKBULUT, s. 546.

[27] SÖNMEZ, s. 6.

İnsanlığın bu tanımlara uygun bir bilgisayarla tanışması 50 yıla yaklaşmıştır[28]. Bilgisayar esasen donanım ve yazılım olmak üzere iki temel bölümden oluşur. Donanım (hardware) bilgisayarın donanım olarak adlandırılan parçalarına, yazılım (software) ise program kısmına verilen genel isimdir. Yukarıdaki tanımlar çerçevesinde bir aygıtın hukuken bilgisayar olarak nitelendirilebilmesi için veri girişi, veri saklama, veri işleme ve veri çıkışı olmak üzere 4 temel unsuru bulundurması gerekir.[29]

Bu 4 temel unsurdan; veri girişi için aygıtın dışarıdan komut veya elektronik bir bilgi almaya yarayan klavye, fare, modem gibi bölümlerinin olması, veri saklama için aygıtın RAM veya Harddisk gibi kalıcı veya geçici belleğinin olması, veri işleme için aygıtın işlemci yani CPU bölümünün olması, veri çıkışı için ise aygıtın işlediği verileri dışarıya aktarmasını sağlayan ekran, yazıcı gibi birimlerinin olması gerekmektedir.[30]

C. VERİ

[28] Liz **DUFF** – Simon **GARDINER**, *"Computer Crime in the Global Village: Strategies for Control and Regulation — in Defence of the Hacker"*, International Journal of the Sociology of Law, 1996, S. 24, s. 213.

[29] Sinan **BAYINDIR** – Özge **APİŞ** – Oğuz **ERSÖZ**, Kitle İletişim Hukuku, B.1, Onikilevha Yay., İstanbul 2018, s. 228.

[30] BAYINDIR – APİŞ – ERSÖZ, s. 228-229; Ayrıntılı bilgi için bknz: Tunç **DEMİRCAN**, Bilişim Alanında Suçlar, B. 1, Legal Yay., İstanbul 2016, s. 12-15.

TDK'ya göre veri; *"Bilgi, data", "Olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi"* anlamlarına gelmektedir.[31]

Yine Bilişim Terimleri Sözlüğü'ne göre veri *"Olgu, kavram ya da komutların, iletişim, yorum ve işlem için elverişli biçimsel ve uzlaşımsal bir gösterimi. Elverişlilik, kişiler ya da özdevimli makinelerle iletişim, yorum ya da işleme uygunluk biçiminde düşünülür."* anlamına gelmektedir.[32]

TDK'da yer alan tanımlardan da anlaşılacağı üzere *"veri"* kelimesini kökenini İngilizce *"data"* kelimesinden almaktadır.

Doktrinde ise veri, *"her türlü bilginin, bilgisayarların işlem yapabileceği, sonuçlar üretebileceği, saklayabileceği ve gerektiğinde yeniden okuyabileceği şekilde sayısal birimlere dönüştürülmüş hali"* olarak tanımlanmaktadır. Yine bu tanıma göre veriyi bilgisayarın yahut diğer bilişim sistemlerinin mütemmim cüzü olarak tanımlamak mümkün olmasa da verinin bütün bilişim sistemlerinin fonksiyonlarını yerine getirebilmesi için büyük önem taşıdığı hatta mütemmim cüze oldukça yakın bir niteliği olduğu tartışmasızdır.[33]

Başka bir tanıma göre ise veri; *"bilişim sisteminin üzerinde işlem yapabildiği, üretebildiği, saklayabildiği, tekrar okuyup işleyebildiği ve başka sistemlere aktarabildiği elektronik ortamdaki her türlü işarettir."*[34]

---

[31] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[32] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

[33] APİŞ, s. 82.

[34] Mesut **ORTA**, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), B. 1, Yetkin Yay., Ankara 2015, s. 39-40.

Yine bir başka tanıma göre veri; bilgisayar veya bilişim sisteminin üzerinde çalıştığı ve bir düzen içerisinde bir araya getirdiği ham gerçekler olarak nitelendirilebilir.[35]

AKSSS'nin 1. maddesindeyse bilgisayar verisi *"Bilgisayar verisi belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünüdür."* olarak tanımlanmıştır.[36]

TCK'nın 243. maddesinde de AKSSS'de yer alan tanıma uygun olarak veriye ilişkin *"sistem içindeki bütün soyut unsurlar, fıkrada geçen "veri" teriminin kapsamındadır."* şeklindeki ifadelere yer verilmiştir.[37]

Yargıtay ise veriyi; *"Bir bilgisayar sisteminin belli bir işlevi yerine getirmesini sağlayan yazılımlarda dahil olmak üzere, bir bilgisayar sisteminde işlenmeye uygun nitelikteki her türlü bilgiyi ifade eder."* şeklinde tanımlamaktadır.[38]

Yukarıda yer alan tanımlardan da anlaşılacağı üzere veri yalnızca bilişim sistemleri yahut bilgisayarlar ile ilgilenen bilim alanları tarafından değil birçok alan tarafından kullanılan geniş kapsamlı bir terimdir. Ancak bu çalışma çerçevesinde veri kavramı ile kastedilen yalnızca bilişim sistemlerinde yer alan verilerdir.

---

[35] Ralph M. **STAIR** – George W. **REYNOLDS**, Principles of Information Systems: A Managerial Approach, B. 9, Course Technology, Boston USA 2010, s.5.

[36] ÖZÇELİK, s. 18.

[37] http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc (E.T. 30.03.2020)

[38] Yargıtay 8. Ceza Dairesi 11.06.2020, 2017 / 21566 E., 2020 / 13171 K. Sayılı Karar, Yayımlanmamış Karar.

D. İNTERNET

Bilişim sistemlerinin sağladığı veri aktarım imkanından hız yahut zaman gibi bir sınırlamaya takılmaksızın faydalanma ihtiyacı ağ yani *"Network"* kavramını ortaya çıkartmıştır. Bu ağların yaygın olarak bilgisayar aracılığıyla kullanılması nedeniyle bu ağlara *"Bilgisayar ağları"* adı verilse de bilgisayar dışında her türlü bilişim sistemi ile de bu ağlara bağlanmak mümkün olduğundan *"Bilişim sistem ağları"* ifadesi daha isabetli olacaktır.[39]

İntranet, ekstranet, sanal özel ağlar, internet gibi birden fazla ağ mevcuttur. Yani görüldüğü üzere internet sanılanın aksine tek ağ türü değildir. Veri iletimi sağlayan ağlardan yalnızca birisidir. Ancak bugün için en yaygın ve geniş ağ internettir.[40]

TDK'ya göre *"İnternet"*, *"Genel ağ"* anlamına gelmektedir. *"Genel ağ"* ifadesinin tanımı ise yine Güncel Türkçe Sözlük'te *"Bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağı"* şeklinde yapılmıştır.[41]

İnternet kelimesi İngilizce bir ifade olan *"Internationel Network"* ifadesinin kısaltmasıdır. İnternet ağı fikri ilk olarak 1962 yılında DARPA yani ABD Savunma Konulu İleri Araştırma Projeleri Dairesi tarafından bir ağa bağlı çok sayıda bilgisayar ve iletişim sistemlerinin veri iletimini sağlamak için başlatılan ve yürütülen bir proje

[39] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 25.

[40] DÜLGER, s. 86.

[41] TDK. https://sozluk.gov.tr/ (E.T. 30.03.2020)

kapsamında J.C.R. Licklider tarafından ortaya atılmıştır. Devam eden yıllarda birden fazla araştırmacı birbirinden bağımsız ve habersiz olarak çalışmalar yürütmüş ve DARPA'nın ARPANET projesini oldukça geliştirmiştir.[42]

Yapılan askeri çalışmada esas amaç ABD'nin olası bir nükleer savaşa girmesi ya da bir sosyal krizin ortaya çıkması halinde ülke yöneticilerinin ve askerlerin birbiriyle iletişimini sorunsuz ve güvenli bir şekilde sürdürmesini sağlamaktı.[43]

Başlangıçta askeri bir gaye ile tasarlanan internet ağına zamanla başkaca bilgisayarların katılmasına müsaade edilmesiyle ağ hızla büyümeye başlamıştır. İnternetin bu kadar hızlı bir şekilde büyümesindeki temel sebeplerden birisi de internetin bir sahibinin ya da yöneteninin olmaması ve bu sayede internetin sınırsız bir özgürlük alanı sağlamasıdır.[44]

İnternet günümüz itibariyle tamamen otonom bir sistemdir. Her biri birbirinden bağımsız birden fazla ağ ve katmandan oluşmuştur. Bu nedenle bireysel ya da küresel anlamda bir denetim söz konusu değildir.[45]

---

[42] Barry M. **LEINER** - Vinton G. **CERF** - David D. **CLARK** - Robert E. **KAHN** vd., *"Brief History of the Internet, Internet Society"*, 1997. https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf (E.T. 03.04.2020)

[43] Gregory **GROMOV**, *"Internet Pre-History: Ancient Roads of Telecommunications & Computers"*. http://history-of-internet.com/history_of_internet.pdf (E.T. 03.04.2020)

[44] BOZDOĞAN AKBULUT, s. 547.

[45] Sevil **YILDIZ**, *"İnternet Servis Sağlayıcılar ve Cezai Sorumlulukları"*, SÜ İİBF Sosyal ve Ekonomik Araştırmalar Der., Konya 2002, S. 3, s. 168.

İnternet tasarlanırken daha basit ve bu kadar karmaşık olmayan bir sistemin hedeflendiği açıktır. Ancak bugün geldiğimiz noktada artık yaşamımızı değiştirme noktasına gelen internet her geçen gün plansız bir şekilde büyümekte, gelişmekte ve karmaşıklaşmaktadır. İnternetteki bu değişim ve gelişim ticaret, iş, eğlence, eğitim vb. birçok alanda da devrim niteliğindeki değişikliği beraberinde getirmektedir.[46]

İnternet vasıtasıyla sağlanan iletişim de tıpkı yüz yüze iletişimdeki gibi diyalog esaslı bir iletişimdir. İnternet kullanıcısı etkin bir pozisyonda olup enformasyon üretilmesine aktif olarak katkı sağlamaktadır. Bu sayede interneti küresel bir kamusal alan olarak kabul etmek mümkün hale gelmektedir.[47]

1990'lı yıllar öncesinde de internet konusunda ve çevrimiçi hizmetler sektöründe faaliyet gösteren şirketler olsa da kitleler için internet 1990'lı yılların ortalarına doğru görülebilir ve erişilebilir bir hale gelmiştir. Yani 1990'lar öncesinde de internet kullanılıyordu ve hızla yayılıyordu. Ancak yakın dönemde internetin yaygınlaşma hızı hiç olmadığı kadar büyümüştür.[48]

Örneğin telefonun 50 milyon kullanıcıya ulaşması 75 yıl, radyonun 38 yıl, TV'nin 13 yıl sürmüşken internet sadece 4 yılda bu sayıya ulaşmıştır. İnternetin yaygın olarak

---

[46] Serhat **KOÇ** – Selva **KAYNAK**, *"Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik"*, XII. Akademik Bilişim Konferansı Bildirileri, MUÜ, 10-12 Şubat 2010, s. 72; Bknz: Şaban Cankat **TAŞKIN**, Bilişim Suçları, B. 1, Beta Yay., Bursa 2008, s. 14.

[47] BAYINDIR – APİŞ – ERSÖZ, s. 229.

[48] Andrew **ODLYZKO**, *"The History Of Communications And İts İmplications For The Internet"*. http://www.research.att.com/~amo (E.T. 03.04.2020)

kullanıldığı sosyal medya platformlarının artış hızı ise çok daha yüksektir. Yine 50 milyon kullanıcıyla Facebook 3,5 yılda ulaşmış, Instagram 300 milyon kullanıcıya 4 yıl gibi oldukça kısa bir sürede ulaşmıştır. Angry Birds isimli oyun ise sadece 35 günde 50 milyon kullanıcıya ulaşmıştır. WhatsApp isimli iletişim uygulaması uygulama faaliyete geçtikten sadece 6 yıl sonra Hristiyanlığın 19 asırda ulaştığı 700 milyon rakamına ulaşmıştır. Anılan rakamlar; internetin ve internet vasıtasıyla teknolojik yeniliklerin yayılma hızını göstermekte ve bu hızın her geçen gün daha da arttığını ortaya koymaktadır.[49]

Ülkemizde ise ilk internet bağlantısı, yine bu dönemlerde, 1993 yılında ABD NSF ile ODTÜ Bilgi İşlem Daire Başkanlığı arasında 64 kb/s Kapasiteli bir bağlantı üzerinden yapılmıştır.[50]

TÜİK'in yaptığı araştırmalara göre ülkemizde internet kullanımı her geçen gün artmaktadır. Nitekim 2016 yılında TÜİK tarafından yayınlanan çalışmaya göre; 16-74 yaş grubu aralığında internet kullanımı ise %61,2 iken 2017 yılında yine TÜİK tarafından ilan edilen çalışmaya göre aynı yaş grubu internet kullanımı ise %66,8'dir. Yine aynı çalışmalara göre 2016 yılında hanelerin %76,3'ü internete erişim sağlayabilirken 2017 yılında bu oran %80,3'e ulaşmıştır.[51]

---

[49] Ulaşan ve Erişen Türkiye Raporu, Ulaştırma ve Altyapı Bakanlığı Strateji Geliştirme Başkanlığı, Ankara 2019, s. 589. https://sgb.uab.gov.tr/uploads/pages/yayinlar/ulasan-ve-erisen-turkiye-2019.pdf (E.T. 07.04.2020)

[50] http://www.internetarsivi.metu.edu.tr/tarihce.php (E.T. 03.04.2020)

[51] http://www.tuik.gov.tr/PreHaberBultenleri.do;jsessionid=ZksNZYpByB7Y2NRT0r6T6Gfqv0TngGDh0Q31WcDQ2FvhYL2sSn8C!86854652?id=24862 (E.T. 03.04.2020)

TÜİK tarafından ilan edilen güncel oranlara geldiğimizde ise 2018 yılında 16-74 yaş grubunda internet kullanım oranı %72,9, 2019 yılında ise %75,3 olmuştur. Yine aynı çalışmalara göre 2018 yılında hanelerin %83,8'i internete erişim imkanına sahipken bu oran 2019 yılında %88,3'e ulaşmıştır.[52]

TÜİK tarafından yapılan incelemeler neticesinde son dört yılda dahi internet kullanımı gün geçtikçe büyük bir hızla artmakta, internet hayatımızın daha önemli bir parçası haline gelmektedir.

II. BİLİŞİM SUÇLARININ TANIMI VE TARİHSEL GELİŞİMİ

A. BİLİŞİM SUÇU KAVRAMI

Bilişim suçunun kavramsal tanımı TCK'Da veya AKSSS'de yapılmamıştır. Bununla beraber bilgisayarla ilgili suç oluşturan ilk hareketler ABD'de ortaya çıktığından kavramın kökeni de burada kullanılan *"Computer Crime"* yani *"Bilgisayar Suçu"* ibaresinden gelmektedir.[53]

AET Uzmanlar Komisyonu'nun Paris Toplantısı'nda 1983 yılında bilişim suçu kavramını *"Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir*

[52] http://www.tuik.gov.tr/PreHaberBultenleri.do?id=30574 (E.T. 03.04.2020)

[53] Berrin AKBULUT, Bilişim Alanında Suçlar, B. 2, Seçkin Yay., Ankara 2017, s. 55.

sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır."[54] şeklinde tanımlanmıştır.

Bilişim suçlarını tanımlamak için doktrinde bilgisayarın ve bilişimin amaç veya araç olmasını arayan kriter, suçları malvarlığı ihlalleriyle sınırlayan kriter, bilgisayar veya bilişim araçları kullanımını esas alan kriter veya veri iletişim ağlarını esas alan kriter gibi birçok kriter kullanılmaktadır.[55]

Ancak hangi kriter kullanılırsa kullanılsın bilişim suçlarını yeterli bir şekilde tanımlamak zordur. Çünkü bilişim suçlarına bir çerçeve çizmek başlı başına bir sorundur. Gelişmekte olan teknoloji her geçen gün bu suç tipinin farklı şekillerde ortaya çıkmasına imkan tanımakta, bu suç tipini kavramsal olarak tanımlamayı zorlaştırmaktadır.[56]

Bu nedenle bilişim suçlarını daha genel ve kapsayıcı bir şekilde tanımlamak gerekmektedir. Bu çerçevede bilişim suçu kavramını *"verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemlerine karşı işlenen suçlar"*[57] şeklinde veya *"bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçlar"*[58]

---

[54] Halil İbrahim **DİLEK**, Bilişim Suçları ve Türk Hukuk Sistemi'ndeki Yeri, Yayımlanmamış Yüksek Lisans Tezi, DÜ, Diyarbakır 2007, s. 5.

[55] Ayrıntılı Bilgi İçin bknz: AKBULUT, s. 59-69.

[56] Mustafa **KARABAL** vd., *"Bilişim Suçları ve Türk Polis Teşkilatı"*, Çağın Polisi Dergisi, S. 6, 2003, s.6. (http://www.caginpolisi.com.tr/bilisim-suclari-ve-turk-polis-teskilati/)

[57] AKBULUT, s. 70.

[58] Ali **KARAGÜLMEZ**, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, B. 5, Seçkin Yay., Ankara 2014, s. 57.

olarak tanımlamak daha doğru olacaktır. Yine benzer bir tanım da Alman doktrininde gelişmiş ve bilişim suçu *"amacı veya gayesi bilgisayar olan suçlar"* olarak tanımlanmıştır.[59]

B. BİLİŞİM SUÇUNUN TARİHÇESİ

Tarihsel süreçte *"Bilgisayar Suçları"* veya *"Bilgisayarla İlgili Suçlar"* olarak da adlandırılan bilişim suçlarının geçmişi 1960'lı yıllarda yayınlanan gazete haberleri ve bilimsel makalelere kadar uzanır[60]. Bu dönemde internetin ataları olan ağların ve sonrasındaysa internetin telaffuz edilmesiyle beraber bilişim sistemlerinin bağlı olduğu ağların plansızlığı, dağınıklığı ve denetiminin güçlüğü gündeme gelmiştir. Ağların bu özelliklerinin değerlendirilmeye başlanmasıyla birlikte 1960'larda bilişim sistemlerinin hukuka aykırı faaliyetlere ne kadar müsait olduğu ve güvenliğin sağlanması için bir şeyler yapılması gerektiği tartışılmaya başlanmıştır. Tam da bu gerekçeyle Amerikan Hükümeti ve Pentagon yetkilileri de dikkatlerini bu noktaya toplamıştır.[61]

1960'lı yıllarda vakalar bilgisayar manipülasyonu, sabotajı, casusluğu veya bilgisayar sistemlerinin yasadışı faaliyetlerde kullanımı olarak karşımıza çıkmaktaydı.

---

[59] Klaus **TIEDEMANN**, *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünde İncelenmesi"*, Çev. Feridun YENİSEY, İÜHFM, C. XLI, S. 1-2, 1975, s. 321.

[60] Ulrich **SIEBER**, *"Legal Aspects of Computer-Related Crime in the Information Society -COMCRIME-Study-"*, s. 19.

https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.doc (E.T. 09.04.2020)

[61] DUFF – GARDINER, s. 214.

Bununla beraber 1970'lerin ortalarından önce bu alanda bilimsel bir çalışma yapılmamıştır. İlk yapılan çalışmalardaysa sınırlı sayıda bilişim suçu vakası tespit edilmişse de tespit edilemeyen yahut bildirilmeyen birçok vaka olduğu da yine bu çalışmalardaki tespitlerde yer almıştır.[62]

Bilişim suçları üzerine Avrupa'da ilk uluslararası toplantı 1976 yılında Strazburg'da gerçekleştirilmiştir. Bu toplantı Avrupa Konseyi tarafından organize edilmiş ve toplantı neticesinde bilişim suçlarının birçok türü kamuoyuna tanıtılmıştır.[63]

Bilinen ilk mevzuat düzenlemesine yönelik teklif ABD'de senatör Abe Ribicoff tarafından Şubat 1977'de kongreye sunulmuştur. Senatör teklifinde mevcut yasal düzenlemelerin yetersiz kaldığını, bilişim suçlarına verilen cezaların ilgisiz başka mevzuat hükümlerin esas alınarak verildiğini belirtmiştir. Yine konuşmasında bilgisayarlar ve bilgisayarların izinsiz kullanımını ele aldı ve mevzuat çalışması yapılması gerektiğini ifade etmiştir. Senatörün teklifi kabul edilmemişse de bu teklif ve tartışmalar bilişim suçlarına ilişkin mevzuat çalışmaları yürütülmesi gerektiğine dikkat çekmiştir.[64]

1980'li yıllara gelindiğinde kişisel bilgisayarlar üretilmeye ve insanlığın hizmetine sunulmaya başlanmıştır[65]. Bu dönemde bilgisayar virüsleri, ağ solucanları ile hack kavramlarına ilişkin basında ve bilimsel çalışmalarda yayınlanan tespitler tamamen

---

[62] SIEBER, s. 19-20.

[63] Stein **SCHJØLBERG** – Amanda M. **HUBBARD**, *"Harmonizing National Legal Approaches On Cybercrime"*, International Telecomminication Union WSIS Thematic Meeting on Cybersecurity, Doc. No: CYB/04, 2005, s. 8.

[64] SCHJØLBERG- HUBBARD, s. 4.

[65] AKBULUT, s. 25.

değişmiştir. Yine bu dönemde gerçekleştirilen bilgisayar manipülasyonları, program korsanlığı ve iletişim sistemlerine yönelik eylemler, siber savunmanın yani bilişim sistemlerinin korunmasının ne kadar önemli olduğunu ortaya koymuştur. 1980'li yıllarda gerçekleştirilen eylemlerde gözlemlenen bir başka sonuç ise eylemlerin amacının yalnızca hukuka aykırı bir şekilde menfaat sağlamak olmadığı birçok başka sebeplerle de bu eylemlerin gerçekleştirildiğidir.[66]

Bütün bu gelişmelerin üzerine 1983 yılında AET;

- Kasten, bilgisayar sistemi üzerinde mevcut olan herhangi bir veri veya değere hukuka aykırı olarak ulaşarak bunları transfer etmek için bilgisayar sistemine girmek, bu veri ve değerleri bozmak veya yok etmek,
- Kasten, bilgisayar sistemlerinin verilerine veya programlarına sahtekarlık yapmak için girmek, bu verileri bozmak veya yok etmek,
- Kasten, bilgisayar sistemlerinin çalışmasına engel olmak için bilgisayar program veya verilerine erişmek, bunları bozmak, silmek veya yok etmek,
- Ticari bir fayda sağlamak maksadıyla bilgisayar programının sahibinin haklarını zarara uğratmak,
- Bilgisayar sisteminin kullanıcısı veya sahibinin izni olmaksızın güvenlik tedbirlerini aşarak sisteme müdahalede bulunmak eylemlerinin bir yaptırıma bağlanması konusunda tavsiye niteliğinde karar almıştır.[67]

1989 yılına gelindiğinde Avrupa Konseyi tarafından toplanan uzmanlar komitesi yasal sorunlar ve mevzuatlardaki diğer boşlukları bir kez daha değerlendirmiş ve bilişim

[66] SIEBER, s. 20.

[67] SIEBER, s. 20-21.

suçlarıyla ilgili 13 Eylül 1989 tarihinde No. R(89) 9 Sayılı tavsiye kararını Strazburg'ta yayınlamıştır. Bu tavsiye kararında suç olduğu hususunda üzerinde mutabık kalınan bir kısım eylemlerin listesi ve yine üye devletlerin tercihine bağlı bir liste bulunmakta olup üye devletlerin bu hususlarda gerekli düzenlemeleri yapması tavsiye edilmiştir.[68]

Özellikle 1990'larda internetin herkese açılması ve son dönemlerde bilgisayar, internetin gibi bilişim teknolojilerinin herkesin erişebileceği maliyette olması nedeniyle bu teknolojilerin kullanımı hızla yaygınlaşmıştır.[69] Tam da bu dönemde internetin yaygınlaşması ve kişisel kullanımın artması gibi nedenlerle yaşanabilecek daha büyük sorunların farkına varılmıştır[70].

Bu farkındalıkla birlikte 1990'lı yılların özellikle ikinci yarısında birçok ulusal hukukta düzenleme yapılmıştır. Yine uluslararası alanda da bu konu dikkatle takip edilmeye başlanmış ve özellikle de uluslararası iş birliğini sağlayabilmek için birçok çalışma yürütülmüştür.[71]

1994 yılında, Birleşmiş Milletler bünyesinde bulunan ve bilim suçlarıyla çalışmaların ağırlıkla yapıldığı "*Suç Önleme ve Cezai Adalet Komitesi"* tarafından 300 maddelik *"Birleşmiş Milletler Bilgisayarla Gerçekleştirilen Suçlara İlişkin Strateji Metni"* kabul edilmiştir. Bu metin de bir tavsiye kararı niteliğinde olmakla beraber beklenen faydayı sağlayamamıştır.[72]

---

[68] KARAGÜLMEZ, s. 99.

[69] DÜLGER, s. 111-112.

[70] SIEBER, s. 20.

[71] DÜLGER, s. 116.

[72] KARAGÜLMEZ, s. 99-100.

1995 yılında Avrupa Konseyi bir kez daha bilişim suçları ile ilgili çalışma yürütmüştür. Bu kez bilişim teknolojilerindeki yeniliklerin ceza usul mevzuatı ile ilişkisi ele alınmış arama ve el koyma, delil ve uluslararası iş birliği gibi konular tartışılmıştır. Bu toplantı neticesinde anılan konularda ceza usul mevzuatında yapılacak yeniliklere ilişkin tavsiye kararları alınmıştır.[73]

1997 yılında Aralık ayında, Washington D.C'de bir araya gelen G8 ülkeleri dış işleri bakanları *"İleri Teknoloji Suçları"* konusunu gündemlerine almış ve toplantıya katılan üye ülkeler bu suçların dünyanın hiçbir yerinde cezasız kalmaması ve suçluların kendilerine bir sığınak bulmamasında mutabık kalmıştır.[74] Bu kapsamda 40'tan fazla ülkenin daimi olarak iletişimde kalması ve INTERPOL ile işbirliği halinde olmasına da yine bu toplantıda karar verilmiştir.[75]

Başta internet gibi ağların kullanılması yaygınlaşmaya başlamasıyla birlikte insanların sosyal ve ekonomik hayatı teknoloji ve bilgi çağının getirdikleriyle büyük değişimler yaşamıştır. Elektronik ticaret hayata geçmiş, iş ve sağlık alanında devrim niteliğinde gerçekleşmiştir. Bankacılık hizmetlerinde ve eğitimde yeni gelişmeler ortaya çıkmıştır. Ayrıca birçok yenilik de bu değişim süreciyle hayatımıza dahil olmuş,

---

[73] SCHJØLBERG- HUBBARD, s. 9.

[74] https://www.cybercrimelaw.net/G8.html (E.T. 09.04.2020)

[75] Stein **SCHJOLBERG** – Solange **GHERNAOUTI-HELIE**, *"A Global Treaty on Cybersecurity and Cybercrime"*, 2011.

https://cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf (E.T. 12.04.2020)

dünyanın küreselleşmesinde büyük rol oynamıştır.[76] Yine günümüzde bilişim sistemlerinin askeri alanda, füzelerden nükleer güce ve askeri personelin yetiştirilmesine kadar değişik birçok iş ve işlemde büyük öneme sahiptir. Yani savunma sanayi büyük oranda bilişim sistemlerinin üzerine kurgulanmaktadır.

Ekonomik ve teknolojik gelişmeler neticesinde klasik suçlar dahi yeni yol ve yöntemlerle işlenebilir hale gelmiştir. Özellikle elektronik sistemlerde yaşanan yeni gelişmeler kişilerin özel hayatını tehdit etmektedir. Yine hesap ve kayıt işlemlerinin bilgisayarlar aracılığıyla yürütülmesi, bankacılık işlemlerinde bilgisayar kullanılmaya başlanması gibi nedenlerle bu sistemlerin herhangi bir suça karşı korunması büyük önem arz etmektedir.[77]

Bütün bu gelişmelerle birlikte bilişim sistemleri hayatımızın önemli bir parçası haline gelmiştir. Örneğin ticari veya şahsi her türlü kayıt bu sistemler üzerinde tutulmaktadır. Yine insanların banka kayıtları ve hesap hareketleri bu sistemler aracılığıyla düzenlenmekte ve yine bu sistemler aracılığıyla her türlü bankacılık faaliyeti gerçekleşmektedir. Devletlerin askeri gücü dahi bilişim sistemleri üzerine inşa edilmektedir. Hal böyle olunca başta yaşam hakkı olmak üzere her türlü insan hakkının korunabilmesi için bilişim sistemlerinin korunması hayati bir önem arz etmektedir.

C. ULUSAL VE ULUSLARARASI MEVZUATLARDA BİLİŞİM SUÇU

[76] AKBULUT, s. 25.

[77] TIEDEMANN, s. 319-321.

1. Avrupa Konseyi Siber Suçlar Sözleşmesi (AKSSS)

1996 yılında Avrupa Konseyi tarafından çok detaylı bir çalışma daha başlatılmıştır. Bu kapsamda CDPC/103/211196 sayılı karar ile siber suçlarla ilgilenecek bir uzman komite kurulmasına karar verilmiştir. Bu karar gereği 1997 yılında 583. Bakanlar ve Bakan Vekilleri Toplantısı'nda CM/Del/Dec(97)583 sayılı karar alınmış ve *"Siber Uzay Suçları Uzmanlar Komitesi PC-CY"* komitesi kurulmuştur. 1997 yılında faaliyetlere başlayan komite bir *"Siber Suçlar Sözleşme Taslağı"* üzerine çalışmıştır. İlk taslak komite tarafından Nisan 2000'de ilan edilmişse de alınan eleştiriler neticesinde yeniden gözden geçirilmiş ve bu kez taslak 2001 yılında Avrupa Konseyi Suç Sorunları Komitesi'ne oradan da Avrupa Konseyi Bakanlar komitesine sunulmuştur.[78]

23.11.2001 tarihinde Avrupa Konseyi üyesi 5 devletten 3'ünün onayı ile Budapeşte'de imzaya açılan AKSSS'yi imzalamaya Avrupa Konseyi'ne üye devletlerinin yanı sıra üye olmayan devletler de davet edilmiştir. Sözleşme, bilgisayarlar üzerinden gerçekleştirilen dolandırıcılık, çocuk pornografisi ve ağ güvenliği ihlallerini ele alan ilk uluslararası anlaşmadır. Yine Sözleşme içeriğinde ceza usul mevzuatına ilişkin de bir kısım hükümler bulunmaktadır.[79]

---

[78] Yavuz **ERDOĞAN**, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, B.1, Legal Yay. İstanbul 2018, s. 15.

[79] https://www.coe.int/web/conventions/full-list/-/conventions/treaty/185 (E.T. 10.04.2020)

AKSSS, 01.07.2004 tarihinde yürürlüğe girmiş olup bu sözleşme siber suçlarla mücadelede büyük ve önemli bir adımdır. Başlangıçta bu sözleşme 26 devlet tarafından imzalanmıştır. Toplantıya gözlemci olarak katılan Japonya, ABD, Güney Afrika ve Kanada gibi ülkelere de imza hakkı tanınmıştır.[80]

Ayrıca Sözleşme imzaya açıldıktan sonra Ocak 2003 yılında şiddet ve ırkçılık konusunda bir ek protokol daha hazırlanmış, bu protokol de 22 devlet tarafından imzalanmıştır.[81] Çocuk pornografisine ilişkin hazırlanan protokol ise halen yayınlanmış değildir[82].

Türkiye 10.11.2010 tarihinde AKSSS'yi Strazburg'ta imzalamış ve imzalanan Sözleşme 03.09.2012 tarihinde Başbakanlık tarafından görüşülmek üzere TBMM'ye gönderilmiştir[83]. Meclis tarafından yürütülen görüşmeler neticesinde Sözleşme 29.04.2014 tarihinde onaylamış ve 01.01.2015 tarihi itibariyle de yürürlüğe

[80] Nancy E. **MARION**, *"The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation"*, *International Journal Of Cyber Criminology, Vol. 4, Issue 1&2,* 1&2 January - July 2010 / July - December 2010, USA, 702.

[81] SCHJØLBERG- HUBBARD, s. 9.

[82] ERDOĞAN, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, s. 15.

[83] https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf (E.T. 10.04.2020)

konulmuştur[84]. Ancak Türkiye 01.03.2006 tarihinde yürürlüğe giren şiddet ve ırkçılık konulu ek protokole taraf değildir[85].

Günümüzde Türkiye dahil AKSSS'ye 65 devlet taraf olmuş bulunmaktadır. En son katılan ülke ise 16.03.2020 tarihinde Sözleşme'yi imzalayan Kolombiya'dır.[86]

Sözleşmenin, Sözleşme Önsözü'nde de ortaya konan temel amacı uluslararası iş birliğinin teşvik edilmesi suretiyle insanlığın siber suçlara karşı korunmasını sağlamak ve ortak bir ceza politikası belirlemektir.[87]

Sözleşme metni incelendiğinde Sözleşme'nin üç ana amacı olduğu ifade edilebilir[88]:

Bunlardan ilki, bazı suçların tanımının ortak yapılmasını sağlamak, böylece ulusal düzeydeki mevzuatların birbiriyle uyumlu hale gelmesini mümkün hale getirmek,

---

[84] https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm (E.T. 10.04.2020)

[85]Murat **ÖNOK**, *"Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği"*, MÜHF Hukuk Der., İstanbul 2013, C. 19, S. 12, s. 1242.

[86] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=yozk7qyT (E.T. 10.04.2020)

[87] https://www.coe.int/web/conventions/full-list/-/conventions/treaty/185 (E.T. 10.04.2020)

[88] ÖNOK, s. 1242.

İkincisi, bu suçların soruşturulması bakımından ortak yetki tanımlarını yapmak ve böylece taraf devletler açısından muhakeme kurallarının birbiriyle uyumlu hale gelmesini mümkün kılmak,

Üçüncüsü hem geleneksel hem de yeni gelişmeler çerçevesinde ortaya çıkan yöntemler çerçevesinde uluslararası iş birliği yöntemlerini belirleyerek taraf devletler arasında bir an önce hayata geçmesini mümkün kılmaktır.

Yukarıda sayılan temel amaçlarla hazırlanan ve imzalanan AKSSS dört ana bölümden oluşmaktadır. Sözleşmenin;

İlk bölümünde, kullanılan terimler ve açıklamalara,

İkinci bölümünde, ulusal düzeyde alınması gereken önlemelere, suç olarak düzenlenmesi gereken eylemlere, maddi ceza hukukuna, ceza usul hukukuna ve yargı yetkisine ilişkin hükümlere,

Üçüncü bölümde, uluslararası iş birliğine, işbirliği hususlarındaki prosedürlere, soruşturma ve kovuşturma yetkilerine ilişkin hükümlere,

Dördüncü ve son bölümde ise, diğer hükümler başlığı altında sözleşmenin yürürlüğü, çekince imkanları ve anlaşmazlıkların çözümü gibi hükümlere yer verilmiştir.[89]

Sözleşmenin ikinci bölümünde yasa dışı erişim, yasa dışı araya girme (müdahale), verilere müdahale, cihazların kötüye kullanılması, bilgisayarla bağlantılı sahtecilik,

[89] SCHJØLBERG- HUBBARD, s. 9.

bilgisayarla bağlantılı dolandırıcılık, çocuk pornosu ve telif haklarına yönelik eylemler suç olarak kabul edilmesi gereken eylemler olarak sayılmıştır[90].

Sözleşme taraf devletlere birtakım yükümlülükler getirmekle birlikte taraf devletlerin ulusal düzeyde gerekli düzenlemeleri yapmamasına yani sözleşme yükümlülüklerinin yerine getirilmemesi haline bir yaptırım bağlamamıştır.[91]

Türkiye de Sözleşme'nin kabulüne ilişkin kanunu kabul etmekle birlikte sözleşmede yer alan hükümlerin uygulanması ve yaptırıma bağlanması için ayrıca bir kanuni düzenleme yapmamıştır. Sözleşmenin bir kısım yükümlülükleri TCK'da yer alan *"Bilişim Suçları"* başlığı altında düzenlenen suçlarla yerine getirilmiştir. Ancak Sözleşme'de eylemlerin daha geniş olarak sayılmış olması ve bazı eylemlerin Türkiye tarafından suç olarak düzenlenmemesi göz önünde bulundurulduğunda Türkiye'nin bütün yükümlülüklerini yerine getirdiğini söylemek mümkün değildir.[92]

Bu çalışmanın konusu olan *"Bilişim Sistemi'ne Girme Suçu"* ve *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini Teknik Araçlarla İzleme Suçu"* bakımından Sözleşme'nin yaptırıma bağlanması yükümlülüğü getirdiği hukuka aykırı erişim ve yasadışı araya girme (müdahale) eylemleri büyük önem arz etmektedir.

---

[90] ERDOĞAN, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, s. 33.

[91] ERDOĞAN, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, s. 34.

[92] ERDOĞAN, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, s. 67-68.

Sözleşmenin *"Hukuka Aykırı Erişim"* başlıklı 2. maddesinde; *"İç hukuka uygun olarak, bir bilgisayar sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişilmesi suç haline getirmek için gerekli görülen yasal tedbirleri alma"* yükümlülüğü belirtilmiştir.

Sözleşme, taraf devletlere kişi ve kurumların sistemlerini koruma rahatsız edilmeden, engellenmeden yönetme, kullanma ve yönetme ihtiyacını giderme yükümlülüğü yüklemiştir. Elbette Sözleşme ile önüne geçilmeye çalışılan, hukuka aykırı ve yetkisiz erişimlerdir. Bu tür erişimlerin önüne geçmenin en kolay yolu güvenlik önlemlerinin ve sistemlerinin geliştirilmesidir ancak bu husus ceza hukukunun konusu değildir. Bu nedenle ceza hukuku bakımından da bilişim sistemlerinin korunmasını sağlamak taraf devletlerin bir yükümlülüğüdür.[93]

Yine Sözleşme metninde *"Yasadışı Araya Girme (Müdahale)"* başlıklı 3. maddeyle sözleşmeye taraf devletlere *"bilgisayar verileri taşıyan bir bilgisayar sisteminde elektromanyetik dalgalarla yayılma da dahil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman kendi iç hukuku ile suç olarak tanımlama"* yükümlülüğü getirilmiştir.

Sözleşme'de yer alan bu düzenleme ile veri iletişiminin gizliliğinin sağlanmasına çalışılmaktadır. Teknik yöntemler kullanılarak müdahaleden kasıt iletişimin içeriğin dinlenmesi kontrolü, izlenmesi yahut dinleme cihazlarıyla doğrudan doğruya elde

[93] Füsun **SOKULLU AKINCI**, *"Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi"*, İÜHFM, C. 59, S. 1-2, s. 14.

edilmesidir. Suçun ortaya çıkması için anılan müdahalenin kamuya açık olmayan iletilere yönelik olması gerekir. Bununla beraber kaydedilen iletiler bir bilgisayarın kendi iletileri veya iki bilgisayar arasındaki iletiler olabilir. Kusur sorumluluğunu esas olan ceza kanunumuzda bu suç bakımından taksirli bir düzenleme yer almadığından bu eylem bakımından sorumluluğun söz konusu olabilmesi için kasten ve hukuka aykırı olarak gerçekleştirilen bir eylem söz konusu olmalıdır.[94]

2. Türk Ceza Hukukunda Bilişim Suçu

a) Mülga 765 Sayılı TCK

Mülga 765 Sayılı TCK'nın ilk halinde bilişim suçlarına ilişkin herhangi bir düzenleme bulunmamaktaydı. Bu suçlara ilişkin ilk düzenleme 06.06.1991 tarihinde 3756 Sayılı Kanun ile 765 Sayılı TCK'ya dört madde halinde eklenmiştir. Eklenen bu dört hüküm Fransız Ceza Kanunu Projesi'nden esinlenerek düzenlenmiştir.[95]

765 Sayılı TCK'nın *"Bilişim Alanında Suçlar"* isimli Onbirinci Bap'ında düzenlenen bu suçlardan;

525/a-1 hükmü *"Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden, programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçiren kimseye bir yıldan üç yıla kadar hapis ve birmilyon liradan onbeşmilyon liraya kadar*

[94] SOKULLU AKINCI, s. 16-18.

[95] AKBULUT, s. 96-97.

ağır para cezası verilir." şeklinde olup bilişim sisteminde yer alan verilerin ele geçirilmesini yaptırıma bağlamıştır.

525/a-2 hükmü *"Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanan, nakleden veya çoğaltan kimseye de yukarıdaki fıkrada yazılı ceza verilir."* şeklinde olup bilişim sisteminde yer alan herhangi bir unsurun başkasına zarar vermek amacıyla nakledilmesi veya çoğaltılmasını yaptırıma bağlamıştır.

525/b-1 hükmü *"Bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan kimseye iki yıldan altı yıla kadar hapis ve beşmilyon liradan ellimilyon liraya kadar ağır para cezası verilir."* şeklinde olup bir sisteme veya sistemde yer alan verilere zarar verilmesini değiştirilmesini, silinmesini veya sistemin işlemesine engel olunmasını, yanlış bir şekilde çalışmasının sağlanmasını yaptırıma bağlamıştır.

525/b-2 hükmü *"Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve ikimilyon liradan yirmimilyon liraya kadar ağır para cezası verilir."* şeklinde olup bir bilişim sistemi kullanılarak hukuka aykırı menfaat sağlanmasını yaptırıma bağlamıştır.

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

için bir bilişim sistemine herhangi bir unsur yerleştirilmesini veya sistemde yer alan herhangi bir unsuru tahrif edilmesini yaptırıma bağlamıştır.

525/d hükmü *"525 a ve 525 b maddeleri hükümlerini ihlal eden kişiler hakkında, maddelerde yazılı cezalara ek olarak, meslek icrası sırasında veya icrası dolayısıyla suçun işlendiği bir kamu hizmetinden veya meslek veya sanat veya ticaretten altı aydan üç yıla kadar yasaklanma cezası da verilir."* şeklinde olup 525/a ve 525/b maddelerinin bir meslek icrası sırasında veya icrası dolayısıyla ihlal edilmesi haline ek yaptırım uygulanmasını düzenleme altına almıştır.

765 Sayılı TCK'da yer alan düzenlemelere, farklı hukuki değerleri ihlal eden suçların aynı kısımda düzenlenmesi, hükümlerin hukuki uyuşmazlıkları çözmekte yetersiz kalması, kavramların doğru kullanılmadığı yahut tanımlamalarının yapılmaması nedeniyle yoruma açık olması gibi hususlarda eleştiriler yöneltilmiştir.[96]

b) 5237 Sayılı TCK

1 Temmuz 1926'da yürürlüğe giren 765 sayılı TCK'nın güncelliğini yitirmesi ve sorunların çözümünde yetersiz kalması nedeniyle Adalet Bakanlığı tarafından 1960'lı yıllardan bu yana ceza hukukun ve 765 Sayılı TCK'nın geliştirilmesi için çeşitli komisyonlar kurulmuştur. Bu komisyonlar dönem dönem taslak ceza yasası metinleri hazırlamış, hazırladıkları metinlerin bir kısmı görüşülmüş bir kısmı ise görüşüldükten sonra kanunlaşmıştır. Yine bu komisyonlardan birisi tarafından hazırlanan TCK 2001

[96] Ayrıntılı bilgi için bknz: Abdulrahman Hussein Kareem **KAREEM**, Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, SÜ SBE, Konya 2019, s. 16.

Tasarısı TBMM alt komisyonu tarafından incelenmiş ve TCK 2001 Tasarısı'nda önemli değişiklikler yaparak neredeyse 12.05.2004 tarihinde neredeyse yepyeni bir tasarıyı kabul etmiştir. Meclis alt komisyonu tarafından kabul edilen bu tasarı bu kez de TBMM Adalet Komisyonu tarafından incelenmiş ve bazı değişiklikler sonrasında TBMM Genel Kurulu'na sunulmuştur.[97]

Sunulan tasarı uzun süre TBMM Genel Kurulu'nda görüşülmüş ve 26.09.2004 tarihinde 5237 Sayılı Kanun ile kabul edilmiştir. 5237 Sayılı TCK 12.10.2004 tarihinde 25611 Sayılı Resmi Gazete'de yayınlanmış ve 01.06.2005 tarihinde yürürlüğe girmiştir.

5237 Sayılı TCK'yı bilişim suçları açısından inceleyecek olursak; bilişim suçlarının özel hükümlerin düzenlendiği *"İkinci Kitap"* 'ta *"Topluma Karşı İşlenen Suçlar"* bölümünde *"Bilişim Alanında Suçlar"* başlığı altında 243 ve 246. maddeler arasında düzenlendiği görülecektir.

Kanun'un ilk halinde *"Bilişim Sistemine Girme"* (TCK 243*), "Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"* (TCK 244) ve *"Banka ve Kredi Kartlarının Kötüye Kullanılması"* (TCK 245) yaptırım altına alınmıştır. Yine *"Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması"* (TCK 246) da bu bölümde ele alınmıştır. Daha sonra 24.03.2016 tarihli 6698 Sayılı Kanun ile *"Yasak Cihaz ve Programlar"* (TCK 245/A) ile *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini Teknik Araçlarla İzleme"* (TCK 243/4) eylemleri de bu kanun kapsamında yaptırıma bağlanmıştır.

Bu bölümde yer alan suçların yanı sıra 5237 Sayılı TCK'da bilişim sistemleriyle veya bilişim suçlarıyla bağlı ve bağlantılı olan *"Haberleşmenin Gizliliğini İhlal"* (TCK 132), *"Kişiler Arasındaki Konuşmaların Dinlenmesi Ve Kayda Alınması"* (TCK 133),

[97] DÜLGER, s. 331.

"Özel Hayatın Gizliliğini İhlal" (TCK 134), *"Kişisel Verilerin Kaydedilmesi"* (TCK 135), *"Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme"* (TCK 136), *"Verileri Yok Etmeme"* (TCK 138) *"Hırsızlık"* (TCK 142) ve *"Dolandırıcılık"* (TCK 158) gibi bir çok suç tipi de bulunmaktadır.

Bilişim suçları bakımından göze çarpan en önemli özellik bu çalışmanın da konusu olan ve TCK'nın 243. maddesinde düzenlenen *"Bilişim sistemine girme suçu"*nun ilk kez düzenleme altına alınmış olmasıdır. Bu suç önceki kanun tasarılarında da yer almakla birlikte ilk kez 5237 Sayılı TCK ile hüküm altına alınmıştır.[98]

5237 Sayılı TCK'nın *"Bilişim Alanında Suçlar"* başlığı altında düzenlenen;

243/1-2-3 hükmü *"(1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.*

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

Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur." şeklinde olup bilişim sistemine kısmen veya tamamen hukuka aykırı olarak girilmesini veya girilen sistemde kalınmaya devam edilmesini yaptırım altına almıştır. İlk fıkrada düzenlenen eylemin bedeli karşılığında yararlanılabilen bir sisteme yönelik olarak işlenmesi hali indirim, ilk fıkradaki eylemin neticesinde sistemdeki verilerin yok olması yahut değişmesi hali ise artırım sebebi olarak öngörülmüştür.

[98] KURT, s. 136.

243/4 hükmü *"Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır."* şeklinde olup bir bilişim sistemi içerisindeki veya birden fazla bilişim sistemi arasındaki veri nakillerinin sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlenmesi hali yaptırıma bağlanmıştır.

244 hükmü *"Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.*

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur." şeklinde olup bilişim sisteminin işleyişinin engellenmesi veya bozulması, bir bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka yere gönderilmesi yaptırıma bağlanmış, ilk iki fıkradaki fiillerin banka, kredi kurumu ya da kamu kurum veya kuruluşlarına ait sistemler üzerinde gerçekleştirilmesi artırım nedeni olarak belirtilmiştir. Yine bu fiiller işlenerek failin kendisi ya da bir başkası yararına haksız menfaat sağlaması suçun daha ağır hali olarak düzenlenmiştir.

245 hükmü *"Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine*

verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.

Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,

c) Aynı konutta beraber yaşayan kardeşlerden birinin, Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." şeklinde olup başkasına ait bir kredi kartını ele geçiren kişinin kart sahibinin rızası olmaksızın kendisi yahut bir başkasına hukuk aykırı menfaat sağlaması hali yaptırıma bağlanmıştır. Başkasına ait kredi kartı yahut banka kartının üretimi, satımı, devri, satın alınması veya kabulü de yine ikinci fıkrada hüküm altına alınmıştır. Üçüncü fıkradaysa sahte oluşturulan yahut sahtecilik yapılan banka veya kredi kartını kullanarak haksız menfaat sağlayan failin eylemi yaptırım altına alınmıştır. Dördüncü fıkrada, ilk fıkradaki

eylemin cezasızlık haline yer verilmiş, beşinci ve son fıkradaysa failin etkin pişmanlıktan faydalanabileceği düzenlenmiştir.

245/A hükmü *"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."* şeklinde olup bir cihaz veya bilgisayar programının güvenlik sisteminin *"Bilişim Alanında Suçlar"* bölümünde düzenlenen suçlar ile bilişim sistemleri vasıtasıyla işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması halinde bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran faile yaptırım uygulanacağı düzenleme altına alınmıştır.

246 hükmü *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* şeklinde olup bu hüküm *"Bilişim Alanında Suçlar"* bölümünde düzenlenen suçların işlenerek tüzel kişilere haksız menfaat sağlanması halinde tüzel kişi hakkında bunlara özgü güvenlik tedbiri uygulanacağını düzenlemiştir.

III. SUÇ İŞLEMEK İÇİN BİLİŞİM SİSTEMLERİNİ KULLANANLAR VE SUÇ İŞLERKEN KULLANDIKLARI YÖNTEMLER

A. SUÇ İŞLEMEK İÇİN BİLİŞİM SİSTEMLERİNİ KULLANANLAR

1. Genel Olarak Hack ve Crack Kavramları

Bilgisayar veya bilişim sistemleri interaktif yani etkileşime açık sistemlerdir. Bilişim sistemlerinin erişime açık olması, erişilen bilginin fazlalığı, işletim sistemlerinin karmaşıklığı ve insan faktörü bu sistemler üzerindeki illegal faaliyetleri oldukça kolaylaştırmaktadır. Özellikle internetin yaygınlaşması ve çok fazla sayıda bilgisayar veya bilişim sisteminin de bu ağ sayesinde adeta birbirine bağlanması, bu faaliyetleri çok daha kolay bir hale getirmiştir.

Bilgisayar/bilişim korsanlığı alanlarının anavatanı ABD olup özellikle bu ülkede hacking tabiri, phreaking veya cracking gibi birçok teknik tabirin yerine geçmiş şekilde kullanılmaktadır. Bu teknik tabirlerin birebir Türkçe karşılığını bulmak ve Türkçe'ye çevirmek oldukça zordur.[99]

"Hack" veya *"Hacking"* kavramlarına ilişkin son kullanıcı düzeyindeki kullanıcılar ve kamuoyu ile bilişim teknolojileri alanında yetkin olan kişilerin tanımları birbirinden farklıdır.

Kamuoyunda bilinen ve son kullanıcı düzeyinde kabul edilen haliyle *"Hacking"* kavramının tanımı, anlam olarak tam manasıyla Türkçe'ye çevrilemese de kısaca

[99] KARAGÜLMEZ, s. 87.

program veya bilgi elde etmek yahut zarar vermek amacıyla bir bilgisayar veya bilişim sistemine yetkisiz erişim sağlanması şeklinde yapılabilecektir.[100]

Ancak bu tanım bilişim teknolojileri alanında çalışan yetkin kişiler tarafından kabul edilmemektedir. Bu kişiler kötü niyetli işlemler için topluma daha yabancı bir kavram olan *"Crack"* kavramını kullanmaktadır. *"Crack"*, bu kişilere göre en kısa tanımıyla sisteme yetkisiz erişim sağlanmasıdır. Yine bu kişiler *"hack"* kavramını ise bir bilgisayarda yapılması mümkün donanım ve/veya yazılım ile ilgili her türlü geliştirme ve/veya iyileştirmenin mümkün olan en iyi şekilde yapılması olarak tanımlamaktadırlar. Görüldüğü üzere, kamuoyunda hack ve crack kavramları iç içe geçmiş ve adeta hack kelimesi crack kelimesinin yerine kullanmaya başlanmıştır.[101]

2. Hacker ve Cracker Kavramları

Bilişim teknolojisini yahut bilişim sistemlerini suç işleme veya illegal faaliyetlerde bulunmak için kullananların sayısı her geçen gün artmaktadır. Bununla bu kişilerin tamamını tek bir isim ile anmak yahut etiketlemek mümkün değildir. Çünkü bu kişilerin teknik bilgisi, amaçları, yöntemleri, araçları gibi birçok özellikleri birbirinden

---

[100] Dorothy **DENNING**, *"Activism, Hacktivism and Cyberterorrism: The Internet as a Tool for Influencing Foring Policy"*, Chapter 8, Edited by John **ARQUILLA** – David **RONFELT**, Networks and Netwars, The Future of Terror, Crime and Militancy, National Defence Research Institue, Published by RAND, Santa Monica ABD 2001, s. 263.

[101] Gökşin **AKDENİZ**, *"Hacker Etiği"*, Hack Kültüğü ve Hacktivizm, Derl. Ali Rıza KELEŞ, Alternatif Bilişim, İstanbul 2013, s. 9.

farklıdır. Yani bu kişilerin çok geniş bir çerçevenin ufak birer parçası olarak değerlendirmek daha doğru olacaktır. [102]

Kamuoyunda bu tür teknik faaliyetlerde bulunan kişilere verilen genel isim *"Hacker"* yani *"Bilişim Korsanı*" ifadesidir. Ancak yine kamuoyu ile bilişim teknolojisinde yetkin kişiler tarafından getirilen farklı tanımlamalara başvurduğu görülmektedir.

Bilişim teknolojisinde uzman kişiler *"Hack"* ve *"Hacker"* terimlerini esasen bir felsefeye dayandırmaktadır. Bu felsefe özünde herhangi bir bilim dalının veya sanatın en yüksek noktalarına ulaşmayı, hayatın her alanında gelişmeyi ve değişmeyi en iyiye ulaşmayı barındırmaktadır.[103] Hacker, kişisel çıkarından ziyade ve denetim ve kontrol altına alınmış bilginin ötesinde bir anlam ve anlamlandırma peşindedir[104].

Nitekim 1975 ve 2004 tarihlerinde yayınlanan Hacker Manifestolarında da bir kültür ve felsefe gözetilerek bu kültürün otoriteden eğitime eğitimden üretime kadar birçok alandaki düşünce ve algılar ortaya konulmuştur.[105]

---

[102] Hüseyin **AKARSLAN**, Bilişim Suçları, B. 2, Seçkin Yay., Ankara 2015, s. 106.

[103] Eric Steven **RAYMOND**, *"How To Become A Hacker"*. http://catb.org/~esr/faqs/hacker-howto.html (E.T. 04.04.2020)

[104] Özgür **UÇKAN**, *"Hacker'lar: Viral Kültürün "Semantik Gerillalar"ı mı, Enformasyon Toplumunun Veri Hırsızları mı?"*, Hack Kültüğü ve Hacktivizm, Derl. Ali Rıza **KELEŞ**, Alternatif Bilişim, İstanbul 2013, s. 46.

[105] Salih **BIÇAKCI**, *"NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik"*, Uluslararası İlişkiler Der., C. 10, S. 40 , 2014, s. 115.

Yine bu felsefeden uzaklaşan kişiler için felsefenin kurucuları ve bu alandaki yetkin kişiler farklı terimler kullanmaya başlamıştır. Cracker da bu tabirlerden birisidir. Crackerlar temel olarak şahsi menfaat sağlamak amacıyla ve suç motivasyonuyla hareket eden kişilerdir.[106] Yani kamuoyundaki hacker tabirinin karşılığı esasen cracker kavramıdır.

Crackerların farklı bir terimle adlandırılmasının en büyük sebeplerinden birisi de hack felsefesinden uzaklaşmış olmalarının yanı sıra bilgisayar dünyasına çok önemli katkıları olan hackerların şöhretinden faydalanmaları ve bu kişiler gibi hareket etmeleridir.[107]

Nitekim Eric Steven RAYMOND editörlüğünde hackerlar tarafından hazırlanan ve kullandıkları kavramları içeren *"Jargon File"* da da hacker ve cracker kavramalarının birbirinden çok farklı anlamlar olduğu ifade edilmiştir[108].

Bütün bu hususlar çerçevesinde *"Hacker"* ile *"Cracker"* kavramlarının farklı anlamlar taşıdığı açıktır. Ancak kamuoyunda bu ayrıma gidilmemekte ve yaygın kullanıma göre *"Cracker"* yerine *"Hacker"* ifadesi tercih edilmektedir.

Bilişim uzmanlarının bu ayrımın gözetilmesi yönündeki teşvikleri netice vermemiştir. Bunun yerine kamuoyu hackerları yani bilgisayar veya bilişim korsanlarını

---

[106] RAYMOND.

[107] Malik **ASLANYÜREK**, İnternet Güvenliği ve Çevrimiçi Gizlilik Alanlarında Yaşanan Sorunlar: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik İle İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Araştırma, Yayımlanmamış Yüksek Lisans Tezi, GÜ SBE, Ankara 2015, s. 72.

[108] http://www.catb.org/jargon/html/crackers.html (E.T. 04.04.2020)

faaliyet amaçlarına göre Beyaz Şapkalı, Gri Şapkalı ve Siyah Şapkalı Bilişim Korsanları (Hackerlar) olarak 3'e ayırmıştır.[109]

a) Siyah Şapkalı Bilişim Korsanları

Cracker kavramının karşılığı olan bilişim korsanları siyah şapkalı bilişim korsanlarıdır[110]. Bir bilişim korsanı bir sistemin tespit ettiği güvenlik açığını yasadışı olarak kullanırsa ve/veya bunun nasıl kullanılacağını başkaları ile paylaşırsa artık bu bilişim korsanı siyah şapkalı bilişim korsanı olarak adlandırılmalıdır.

Siyah şapkalı bilişim korsanları tamamen kötü niyetli ve tehlikeli bilişim korsanlarıdır. En büyük hedefleri sistemin açıklarından faydalanarak gizlenen verilere erişmek, kazanç elde etmek ya da zarar vermek ve sistemi çalışmaz hale getirmektir.[111] Siyah şapkalı bilişim korsanları tamamen yasadışı çalışırlar ve amaçlarına ulaşırken

---

[109] Margaret **ROUSE**, *"Hacker"*. https://searchsecurity.techtarget.com/definition/hacker (E.T. 04.04.2020)

[110] Şerif **İNANIR**, *"Türkiye'de Internet Ortamında Hayat Bulan Hacker (Kırıcı) Kültürü ve Karakteristiği"*, TBD Bilişim 2018 35. Ulusal Bilişim Kurultayı Bildiriler Kitabı, Edt. Ali **YAZICI**, Nergiz Ercil **ÇAĞILTAY**, Çiğdem **TURHAN**, Ankara 2018, s. 168.

[111] ASLANYÜREK, s. 73.

güvenlik protokollerini ve sistemlerini ihlal eder ve atlatmaya çalışırlar. Motivasyonları kazanç elde etmek ya da zarar vermenin yanı sıra kişisel ya da politik de olabilir.[112]

b) Gri Şapkalı Bilişim Korsanları

Gri şapkalı bilişim korsanı siyah şapkalı bilişim korsanı ile beyaz şapkalı bilişim korsanı arasında kalmış bir bilişim korsanı türüdür.

Bir bilişim korsanı bir sistemin tespit ettiği güvenlik açığını yasadışı bir şekilde kullanmak yerine bunun nasıl düzeltileceğini izah etmek için sistemin sahibiyle veya kullanıcısıyla para karşılığı anlaşılırsa bu halde bu bilişim korsanı gri şapkalı bilişim korsanı olarak anılmalıdır.[113]

Genellikle gri şapkalı bilişim korsanının işi tespit ettiği güvenlik açığını düzeltmek değildir. Hatayı ya da açığı bilişim sistemi sahibine ya da kullanıcısına bildirmekle yetinir. Taleplerinin reddedilmesi halindeyse elde ettikleri verilerle ne yapacaklarını kestirmek zordur.[114]

---

[112] https://www.cybersecurityintelligence.com/blog/ethical-hacking-can-beat-black-hat-hackers-2457.html (E.T. 04.04.2020)

[113] Allen **HARPER** - Shon **HARRIS** – Jonathan **NESS** vd., Gray Hat Hacking The Ethical Hacker's Handbook, Third Edition, Mc Graw Hill Comp., USA 2014, s. 47.

[114] HARPER – HARRİS – NESS vd., s. 419-420.

c) Beyaz Şapkalı Bilişim Korsanları

Bilişim sistemlerinin yaygınlaşması ve bilişim suçlarındaki hızlı artış bilişim sistemi kullanan tüm kişi, kurum ve kuruluşlarda güvenlik endişesi yaratmıştır. Bu endişe neticesinde bilişim sistemlerinin kontrol ve test edilerek güvenlik açıklarının belirlenmesi, tespit edilen eksikliklerin de giderilmesi ihtiyacı ortaya çıkmıştır. İşte bu ihtiyaç neticesinde beyaz şapkalı bilişim korsanları yani bir diğer adıyla *"ethical hacker"* kavramı ortaya çıkmıştır.[115]

Beyaz şapkalı bilişim korsanlarının teknik yetkinliği ve bilgisi siyah şapkalı bilişim korsanlarından aşağı değildir. Ancak faaliyet amaçları sisteme zarar vermek veya sistem üzerinden şahsi menfaat sağlamak değil bilişim sistemlerinin güvenliğini sağlamaktır.[116]

B. FAİLLERİN KULLANDIĞI YÖNTEMLER

1. Virüsler

Virüsler, en çok bilinen kötücül yazılım türüdür ve kendilerince kodlarında yer alan talimatlar doğrultusunda bulaştığı doküman ve yazılımlarda çeşitli faaliyetler

[115] KARAGÜLMEZ, s. 91.

[116] ASLANYÜREK, s. 73.

gerçekleştirebilir. Virüslerin en karakteristik özelliği hedef sisteme ilk kopyalanmasının hedef sistemin kullanıcısı tarafından gerçekleştirilmesi zorunluluğudur.[117]

Bu yazılımlar en tehlikeli kötücül yazılımlardan olarak kabul edilir. Biyolojideki virüs teriminden esinlenerek isimlendirilen bu yazılımlar kendini kopyalayabilen, diğer kodlara, programlara ve belgelere yapışabilen, kendi kopyalarını çalıştırabilen yazılımlardır. Bu yazılımlar kimi zaman ekranda basit uyarı mesajları çıkartan nispeten zararsız kimi zamansa önemli dosyaları silebilen ya da bütün sistemi çalışmaz hale getirebilir.[118]

Genel olarak ve en kısa tanımıyla virüsler, bir bilişim sistemine veya bilgisayara çeşitli yöntemlerle girebilen ve zarar veren, sistemin işleyişini yavaşlatan, bozan yazılımlardır[119]. Bu nedenle sabotaj eylemleri için en sık kullanılan araçlar arasında yer almaktadır[120]. Bununla beraber virüs aktif olduktan sonra bütün faaliyetlerini otomatik

---

[117] Felix **LINDER**, *"Malware and Viruses"*, Chapter 14, The Hacker's Handbook The Strategy behind Breaking into and Defending Networks, Edt. Susan YOUNG – Dave AITEL, Auerbach Publications, USA 2004, s. 529.

[118] Gürol **CANBEK** - Şeref **SAĞIROĞLU**, *"Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma"*, GÜ MMFD., C. 22, No: 1, Ankara 2007, s. 122, 123.

[119] Ahmet **GÜL**, Doğrudan – Dolaylı Bilişim Suçları, B. 2, Seçkin Yay. Ankara 2018, s. 41.

[120] AKBULUT, s. 78.

yürüttüğünden failin amacında başarılı olması hedef sisteme anlık olarak erişim sağlamasına bağlı değildir[121].

2. Solucanlar (Worms)

Solucanlar da tıpkı virüsler gibi kötü amaçlarla yazılmış kodlardan oluşan yazılımlardır. Solucanlar ile virüsler sıklıkla karıştırılsa da çoğalma ve yayılma yöntemleri olarak tamamen farklıdırlar. Her şeyden önce solucanlar sistem üzerinde hareket ederken virüsler gibi sisteme zarar vermek zorunda değildir.[122]

Bilişim sistemine erişim sağlayan solucanlar ilk olarak bir ağa erişim sağlama amacıyla bir uygulama başlatır. Daha sonra bu ağ üzerinden kendisine yeni hedefler belirler. Çok hızlı bir şekilde çoğalma özelliği olan solucanlar çok hızlı bir şekilde ağlardan yayılır. Kendisini oluşturan kullanıcıya da aynı hızla veri aktarırken ağ trafiğini de büyük oranda yavaşlatır. Bütün bu işlemler içinse genellikle herhangi bir şekilde kullanıcının yardımına ihtiyaç duymaz, faaliyetlerini otomatik yürütür.[123] Virüslerin aktif hale geçebilmesi için kullanıcının çalıştırılması zorunluluğu karşısında solucanların

---

[121] Peter **SOMMER**, Ian **BROWN**, *"Reducing Systemic Cybersecurity Risk"*, OECD Multi-Disciplinary Issues International Futures Programme, 2011, s. 25.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1743384 , (E.T. 05.04.2020)

[122] DÜLGER, s. 125.

[123] Bahaddin **ALACA**, Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile), Yayımlanmamış Yüksek Lisans Tezi, AÜ SBE, 2008 Ankara, s. 62-63.

otomatik olarak faaliyete geçmesi nedeniyle solucanların virüslere göre daha tehlikeli yazılımlar olduğu söylenebilecektir[124].

Solucanlar çok hızlı yayılan, dolaşımını sürdürmek için çoğalan, erişim sağladıkları ağ veya sistem üzerindeki her türlü veriyi toplayan ve aktaran zaman zaman gizemli mesajlar bırakan ve kendi izlerini yok eden yazılımlardır.[125]

3. Truva Atı (Trojen Horse)

Truva Atı olarak adlandırılan yazılım, adını anlaşılacağı üzere tarihte yaşanan Truva Savaşında başvurulan meşhur Truva Atı hilesinden almaktadır[126]. Truva atları da tıpkı o hiledeki gibi bir yöntem kullanmaktadır.

Bu yazılımlar kullanıcılar tarafından internette türlü yöntemlerle erişim sağlanabilen ücretsiz programlara, ekran koruyuculara ya da ilgi çekici reklamlara kullanıcın erişim sağlaması suretiyle bilişim sistemlerine veya bilgisayara indirilmektedir.[127]

İnternetten indirilen ücretsiz programlar, müzikler, dosyalar veya ilgisiz bir adrese tıklanarak bilinçsiz olarak indirilen Truva atları kullanıcından habersiz arka planda

---

[124] Damla **ERMEYDAN**, Türk Ceza Kanunu'nda Bilişim Suçlar, Yayımlanmamış Yüksek Lisans Tezi, ÇÜ SBE, Mersin 2018, s. 16.

[125] KURT, s. 68.

[126] CANBEK – SAĞIROĞLU, s. 125.

[127] AKARSLAN, 94.

çalışmaya devam eder. Sistem internete bağlıyken de yine kullanıcının bilgisi ve iradesi dışında dış kaynaklara veri aktarımı yapar. Truva atlarının virüslerden ve solucanlardan en büyük farkı kendi kendilerini kopyalamamaları yani çoğalmamaları ve yayılmamalarıdır.[128]

İndirilen program, belge veya yazılım ilk önce kendi halinde çalışmaya başlar ya da hata verebilir. Kullanıcı genellikle bu aşamada Truva atının varlığından haberdar olmamaktadır. Sonrasındaysa içerisinde bulunan Truva atı kendi kendine ya da Truva atının kaynağının istemiyle harekete geçer. Sistem içerisindeki verileri kaynağın talimatı doğrultusunda kaynağa gönderir. Ancak Truva atının tıpkı meşhur hiledeki sistem kullanıcısı tarafından sisteme alınması gerekir.[129]

Truva atları kullanışlı görünüşünün aksine yararlı gibi görünen kodların yanı sıra kötü amaçlı kodlar da içeren bir yazılımdır[130]. Bu yazılım içerisindeki kodlar sayesinde sistemde gizli erişime imkan sağlayan bir arka kapı sistemi oluşturur. Bu sayede kullanıcıların hareketlerini izlemek, verilerini çalmak veya silmek için kullanılabilirler.

---

[128] Mehmet Akif **OCAK** – Yıldıray **YALMAN** – Hüseyin **ÇAKIR** vd., Güncel Tehdit: Siber Suçlar, Edt. Hüseyin **ÇAKIR** – Mehmet Serkan **KILIÇ**, B. 1, Seçkin Yay. Ankara 2014, s. 28.

[129] KURT, s.63-64.

[130] Peter J. **DENNING**, *"Computer Viruses"*, RIACS Technical Report, Research Institute for Advanced Computer Science NASA Ames Research Center, s. 2. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890017050.pdf

(E. T. 05.04.2020).

Yine bunun yanı sıra hedef sistem, tamamen kullanıcının kontrolü dışına çıkabilir ve sistem uzaktan kontrol edilebilir hale gelebilir.[131]

4. Tavşanlar (Rabbits)

Tavşanlar, genellikle çok kullanıcılı sistemlerin işleyişini bozmak ve ağ iletişimi tıkamak veya koparmak için kullanılan bir yazılım türüdür[132]. Çünkü bu yazılım türü tıpkı ismini aldığı hayvan gibi çok hızlı bir şekilde çoğalan bir yazılım türüdür[133].

Tavşanlar girdikleri sistem üzerinde büyük bir hızla ve sürekli çoğalarak sistem üzerindeki alanı sürekli doldurmaktadır. Bu sayede sistemin işlem gücünü sekteye uğratan tavşanlar aynı zamanda aynı zamanda sisteme sürekli gereksiz komutlar vererek sistemi durma noktasına getiren ya da tamamen durduran yazılımlardır.[134]

5. Bukalemunlar (Chameleons)

Truva atları gibi bukalemunlar da sisteme aldatma yoluyla girerler. Bukalemunlar, sistem içerisinde zararsız çalışan normal bir yazılım gibi hareket eden ve normal bir

[131] SOMMER – BROWN, s. 24-25.

[132] DÜLGER, s. 126.

[133] CANBEK – SAĞIROĞLU, s. 133.

[134] KURT, s. 75.

yazılım niteliklerindeymiş gibi görünen kötücül bir yazılım türüdür. Bu kötücül yazılım adını kendini saklamaktaki üstün yeteneğinden almıştır.[135]

Bukalemunlar aynı zamanda kullanıcı adı ve şifreleri de taklit edebilmektedir. Bu yetenekleri sayesinde sistemde istedikleri dosyaya ulaşabilmekte ve her türlü şifreyi kaydedebilmektedir. Zaman zaman sistemin ya da programın geçici olarak kapatılacağı mesajını vererek programa yeniden kullanıcı adı ve şifreyle erişim gerçekleştirilmesini sağlamakta ve böylece de en gizli uygulama ya da belgelerin kullanıcı adı ve şifresini dahi kaydedebilmektedir.[136]

6. Mantık Bombaları (Logic Bombs)

Mantık bombaları bilinen kötücül yazılımlardan en eskisidir. Kökeninin tahmini olarak 1960'lara dayandığı bilinmektedir. Bu bombalar sistemde daha önceden belirlenmiş ihtimallerde harekete geçerler. İhtimal ortaya çıktığında ekrana bir mesaj gelebilir ya da sistemi tamamen silebilir. Bu tamamen bombanın nasıl kodlandığına göre değişmektedir.[137] Bu nedenle mantık bombalarının ilk etapta fark edilmesi genellikle mümkün olmamaktadır[138].

[135] DÜLGER, s. 127.

[136] OCAK – YALMAN – ÇAKIR vd., s 31.

[137] SOMMER – BROWN, s. 24.

[138] ERMEYDAN, s. 17.

Bununla beraber mantık bombaları çok bilinen bir kötücül yazılım türü değildir. Mantık bombalarının kendini çoğaltmak gibi bir amacı yoktur ve diğer sistemlere bulaşmakla ilgilenmez.[139]

Mantık bombaları, bilgisayara ya da bilişim sistemine belirlenen koşullar altında ya da belirli bir zamanda uygulaması gereken talimatları bildirir. Bu komutlar doğum günü kutlayan bir mesaj kutusunun açılması gibi basit ve iyi niyetli de olabilir, bütün bir belleğin silinmesi şeklinde kötü niyetli de olabilir. Kimi zaman bu şekilde yazılım yoluyla sanal alemde gerçekleştirilen bir eylemin etkileri çok daha büyük olabilmektedir.[140]

Örneğin, bu virüslerden birisi Çernobil Patlaması anısına her yıl 26 nisanda harekete geçiyordu. Yani bomba 26 nisana tarihinde harekete geçmek üzere programlanmıştı.[141]

Yine bir başka örneğe göre; Michalengelo'nun doğum günü tarihi olan 6 martta sistemde aktif olmaya ve üzerinde bulunduğu sistemin sabit diskini silmeye programlanan bir mantık bombası da dünyada 5 milyon bilgisayarı hedef almıştı. Ancak bu sayının birkaç binle sınırlı kaldığı tahmin edilmektedir. Bu eylemin 2000'li yıllar öncesinde gerçekleştiği ve kullanılan bilgisayar sayısının bugüne göre ne kadar az olduğu da düşünüldüğünde eylemin büyüklüğünü kavramak daha kolay olacaktır.[142]

---

[139] LİNDER, s. 530.

[140] Neal Kumar **KATYAL**, Criminal Law in Cyberspace, Georgetown University Law Center, 2001. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030 (E.T. 05.04.2020)

[141] ORTA, s. 103.

[142] DUFF – GARDINER, s. 225.

7. Casus Yazılımlar (Spyware)

Casus yazılımlar, virüs ya da Truva atı gibi hareket eden basit yazılımlardır. Ancak hedef sistemde kendisini kopyalayarak çoğaltmaz. Bu yazılımların temel amacı hedef sistemin kullanıcısı tarafından tutulan gizli bilgi ve belgelere erişim sağlanmasıdır. Bunu çeşitli yöntemlerle yapabilir. Kimi zaman klavyede basılan tuşları kimi zaman da ziyaret edilen internet sitelerini kaydeder. Bu yazılımlar genellikle hedef sistemin kullanıcısı tarafından kurulur. Ancak kurulum çoğunlukla kullanıcı tarafından bilinçsiz gerçekleştirilir.[143]

Casus yazılımlar çoğunlukla internetten indirilen herhangi bir yazılım içerisine saklanan bir kötücül yazılım türüdür[144]. Bu kötücül yazılımlar hedef sistemin kullanıcısına ait önemli belge ve bilgileri kullanıcının bilgisi dışında topladıktan sonra kötü niyetli kişilere ulaştırır. Bu kişiler bu yöntem sayesinde hedef sistemin kullanıcısının kredi kartı bilgileri de dahil olmak üzere her türlü verisine kolayca ulaşır.[145]

8. Arka Kapılar (Backdoors)

[143] LINDER, s. 530.

[144] ASLANYÜREK, s. 48.

[145] AKBULUT, s. 84.

Arka kapı yazılımları koruma altındaki bir bilişim sistemine yetkisiz erişim imkanı sağlayan bir yazılım türüdür. Bu yazılım genellikle ana yazılımın içerisine acil bir durum ortaya çıkma ihtimali için bilerek ve meşru bir amaçla yerleştirilir. Yani olası bir sorun halinde sisteme gizlice bir giriş imkanı sağlar.[146]

Ancak özellikle sistemin inşası tamamlandıktan sonra yahut bu arka kapıya olan ihtiyacın ortadan kalkması sonrasında arka kapıların kapatılması gerekir[147]. Aksi halde bilişim sistemi kötü niyetli kullanıma ve/veya yetkisiz erişime müsait hale gelecektir.[148] Bununla beraber arka kapıların diğer zararlı yazılımlar (Truva atı vb.) aracılığıyla da açılması veya bu yazılımlar ile birlikte kullanılması da mümkündür[149].

Gizli kapı ya da açık kapı olarak da adlandırılan arka kapılar kimi zaman da kötü niyetli olarak bırakılmaktadır. Bu yazılımlar üzerinde yer aldığı uygulamaların içine uygulamayı geliştiren kişi veya şirketlerce bilinçli bir şekilde bırakılmakta ve böylece uygulamanın çalıştığı bilişim sistemine, hedef sistemin kullanıcısına yakalanmadan, uzaktan sızma imkanı sağlamaktadır.[150]

---

[146] LINDER, s. 530.

[147] Ebru **ALTINOK** – Ali Fatih **VURAL**, *"Bilişim Suçları"*, Denetişim Der, 2011, S. 8, s. 79.

[148] KURT, s. 67.

[149] AKARSLAN, s. 98.

[150] OCAK – YALMAN – ÇAKIR vd., s 32.

9. Gizlice Dinleme (Sniffing)

Gizlice dinleme yazılımları hedef sistem kullanıcısının rızası olmaksızın bir dinlemenin gerçekleştirilmesini sağlayan dinleyici ya da yakalayıcı özellikleri olan yazılımlardır. Bu yazılımlar yerel sistemler veya ağlar arasındaki trafiği yakalar ve böylece yazılımı kullanan ve yöneten kullanıcı hedef sistemin kullanıcısını gizlice dinler veya takip eder.[151]

Gizli dinleme programları en yalın tanımıyla veri yakalama yazılımlarıdır. Birbiriyle iletişim halinde olan bilgisayar ya da bilişim sistemleri muhakkak ki bir ağa dahil olacaktır. Gizli dinleme programları da bu ağa, çoğunlukla her iki bilişim sisteminin kullanıcısının da bilgisi dışında, dahil olur ve her iki sistem arasındaki iletişim trafiğini gizlice yakalar.[152] Yine bu tekniğin ağa girilmeden elektromanyetik dalgaların yakalanması suretiyle gerçekleştirilmesi de mümkündür[153]. Bu yöntemde veri akışına

---

[151] Susan **YOUNG** – Dave **AITEL**, *"IP and Layer 2 Protocols"*, Chapter 7, The Hacker's Handbook The Strategy behind Breaking into and Defending Networks, Auerbach Publications, USA 2004, s. 244, 694.

[152] Sumit **DHAR**, *"Sniffers Basics and Detection"*.

http://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf

(E. T. 06.04.2020).

[153] ALTINOK – VURAL, s. 78.

engel olmadan elde edilen veriler hedef sistemi gizlice dinleyen kişinin sistemine yine gizlice gönderilir.[154]

10. Veri Aldatmacası (Data Diddling)

Bilgi aldatmacası olarak da adlandırılan bu işlem esasen veri girişi esnasında kasten hatalı veri girişi yapılması veya verilerin girildikten sonra kasten hatalı olarak değiştirilmesidir. Veri aldatmacası, basit, yaygın ve güvenilir olması nedeniyle bilişim suçları alanında en yaygın olarak kullanılan tekniktir. Yine sabit disklerin önceden ve kasten hatalı hazırlanmış kopyalarıyla değiştirilmesi bu işleme bir örnektir.[155] Bu işlemin tercih edilmesinin bir diğer sebebi ise bu suç işlendikten sonra ortaya çıkartılmasının çok güç olmasıdır[156].

11. Süper Darbe (Supper Zapping)

Süper darbe yazılımları, sistemin bütün güvenliğini bir şekilde aşarak sisteme müdahale imkanı veren yazılımlardır[157]. Bu yazılımların esas amacı çeşitli sebeplerle

[154] ERMEYDAN, s. 12.

[155] OCAK – YALMAN – ÇAKIR vd., s 27.

[156] KURT, s. 62.

[157] ALTINOK – VURAL, s. 79.

çalışmaz, işlemez bir hale gelen sistemi kısa sürede yeniden çalışır hale getirmektedir[158]. Yani arka kapı yazılımlarına benzer bir şekilde meşru bir amaç ile yazılmış yazılımlardır.

Ancak bu yazılım türü sistemin bütün güvenlik sistemlerini aşma imkanı tanıdığından hukuka aykırı yahut gayrı meşru bir amaçla hareket edilmesi halinde bilişim sistemleri için oldukça tehlikeli bir hal almaktadır.[159]

12. DoS veya DDoS Atakları

DoS veya DDoS atakları bilişim sistemi veya ağların hizmetini aksatmak amacıyla kullanılan bir yöntemdir. Saldırıyı yürüten ve yöneten sistem organize bir şekilde yürüttüğü saldırılarla sistemin veya ağın bütün kaynaklarını tüketerek servis dışı bırakmaya çalışır. Bu sırada saldırıyı yürüten ana sistem birçok aracı sistem kullanarak hem kendisini gizler hem de saldırının boyutunu arttırır.[160]

Bir sistemin veya ağın güvenlik açıklarından faydalanarak bir sistem veya ağa karşı organize bir şekilde yürütülen DDoS ataklarının amacı hedefteki sistemin hizmet vermesini engellemektir. Bu organize saldırılar sırasında saldırıyı yapan sistem ile hedef sistem arasında genellikle özel bir iletişim kanalı bulunur ve faaliyet bu kanal üzerinden yürütülür.[161]

---

[158] OCAK – YALMAN – ÇAKIR vd., s 27.

[159] ERMEYDAN, s. 14.

[160] DÜLGER, s. 132.

[161] YOUNG – AITEL, s. 101.

Özellikle sistemlerin veya web sitelerinin diğer sistemlerle iletişim kurmasının tamamen önüne geçer. Bu tür saldırılarda bilişim korsanları sisteme bir şekilde yetkisiz erişim sağlar ve kendi sistemini yönetici hale getirmek üzere hedef sisteme bir yazılım yerleştirir. Yönetici sistem birden çok hedef sistem seçer ve birden fazla sisteme bu yazılımı yerleştirir. Böylece hedef sistemlerden birisine diğer bütün sistemleri kullanarak bu saldırıyı gerçekleştirebilir.[162]

Bu yöntemde bir sisteme veya ağa büyük ölçekli bir ağ trafiği yönlendirilir ve sistem veya ağ baskı altına alınır. DDoS ataklarının artması sonrasındaysa sistem adeta servis dışı kalır veya çalışması neredeyse durur. Bu yöntemin faile sağladığı iki önemli avantaj vardır. Bunlardan ilki failin tespitinin oldukça zor olması ikincisi ise tek bir sistem ve tek bir kişi ile bu saldırının gerçekleştirilebilmesidir.[163]

13. Diğer Yöntemler

Bilişim teknolojisinin geldiği nokta da değerlendirildiğinde şüphesiz ki bilişim suçları işlenirken kullanılan yöntemler yukarıda sayılanlarla sınırlı değildir. Her geçen gün değişen ve dönüşen bir alan olan bilişimde birçok yol ve yöntem de gelişmeye ve geliştirilmeye devam etmektedir.

[162] KATYAL, s. 25.

[163] SOMMER – BROWN, s. 25-26, 28.

Nitekim yukarıda izah edilmese de bilişim suçları işlenirken **telefon çevirici (dialers)[164], sazan avlama (oltalama-pishing)[165], çöpe dalma (scavenging)[166], tarama (scanning)[167], salam tekniği (salami techniques)[168], istem dışı alınan e- postalar**

[164] Telefon ağına girilerek uzun mesafeli veya ek ücretli telefon konuşmaları yapmayı sağlayan bir yöntem. Ayrıntılı bilgi için bknz: HARPER – HARRİS – NESS vd., s. 548.

[165] Kullanıcının kullandığı banka ya da benzeri bir kurum veya kuruluş adıyla sahte bir e-posta veya ileti gönderilerek kullanıcının kandırılması ve şifre vb. bilgilerinin ele geçirilmesinde kullanılan bir yöntem., Ayrıntılı bilgi için bknz: KURT, s. 76.

[166] Çöpe dalma veya atık toplama olarak da adlandırılan ve bir bilişim sisteminde gerçekleşen veri işleme faaliyeti sonrasında artık hale gelen verilerin toplanması yöntemi. Ayrıntılı bilgi için bknz: OCAK – YALMAN – ÇAKIR vd., s. 32.

[167] Sıralı bir dizi takip edilerek hedef sisteme bir takım verilerin girilmesi ve böylece sistemin olumlu rapor verdiği durumların raporlanmasını sağlayan bir yöntem. Genellikle sisteme erişim öncesinde sistem açıklarının tespiti için kullanılır., Ayrıntılı bilgi için bknz: DÜLGER, s. 135.

[168] Bankacılık sektöründe uygulanması daha mümkün olan ve hesap sahiplerinin hesabından fark edilmeyecek kadar düşük miktarların failin belirlediği hesaba aktarılması yöntemi., Ayrıntılı bilgi için bknz: KURT, s. 67.

(spam)[169], hukuka aykırı içerik sunulması[170] veya sırtlama (piggybacking)[171] gibi birçok yöntem de aracı olarak veya kullanılmaktadır.

[169] E-postalar aracılığıyla çok sayıda kullanıcıya gönderilen genellikle içeriği uygun olmayan veya kullanıcı tarafından istenmeyen e-postaların gönderilmesi., Ayrıntılı bilgi için bknz: ORTA, s. 106.

[170] Irkçı, ayrımcı, pornografik yahut herhangi bir şekilde suç teşkil eden içeriklerin kullanıcılara veri iletim ağları aracılığıyla sunulması., Ayrıntılı bilgi için bknz: DÜLGER, s. 131.

[171] Elektronik veya fiziksel yöntemlerle hak sahibi kişinin giriş yetkilerinin kullanılarak bir bilişim sistemine yetkisiz erişim sağlanması., Ayrıntılı bilgi için bknz: OCAK – YALMAN – ÇAKIR vd., s. 32.

İKİNCİ BÖLÜM

TÜRK CEZA KANUNUN 243. MADDESİNDE DÜZENLENEN SUÇ TİPLERİ

I. BİLİŞİM SİSTEMİNE GİRME SUÇUNA DAİR İNCELEMELER

A. GENEL OLARAK

"Bilişim sistemine girme suçu", TCK'nın ikinci kitap üçüncü kısmında *"Topluma Karşı Suçlar"* bölümünde altında *"Bilişim Alanında Suçlar"* başlığı altında 243. madde'de 3 fıkra halinde düzenleme altına almıştır. Kanunda yer alan düzenlemeyse;

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

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

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

5237 Sayılı TCK'nın 243. maddesi ilk fıkrasının ilk halinde "*hukuka aykırı olarak giren ve orada kalmaya devam eden"* şeklindeki ifade 24.03.2016 tarihli 6698 Sayılı Kanun'un 30. maddesiyle *"hukuka aykırı olarak giren veya orada kalmaya devam eden"* olarak değiştirilmiştir.

Kanunda yer alan düzenlemede de görüleceği üzere; ilk fıkrada suçun tanımına yer verilmiş, ikinci fıkrada cezada indirim sebebi öngörülmüştür. Üçüncü fıkradaysa sistem içeriğindeki verilerin yok olması yahut değişmesi hali suçun neticesi sebebiyle ağırlaşması olarak ele alınmış ve bu hale ilk fıkradan farklı bir yaptırım bağlanmıştır.

765 Sayılı Kanun'da düzenlenmeyen yukarıdaki suç, ilk kez 5237 Sayılı TCK ile karşımıza çıkmıştır. Kanunun düzenlenme amacının bilişim sisteminin ve sistem içerisinde bulunan verilerin güvenliğini ve gizliliğinin sağlanması olduğu açıktır. Zira salt *"Bilişim sistemine girme suçu"*nun ayrı bir suç olarak düzenlenmesi dahi kanunun amacını ortaya koymaktadır.[172]

Bunun yanı sıra madde metninde cezai yaptırıma bağlanan fiilin suç olarak düzenlenmesine yönelik yükümlülük Türkiye Cumhuriyeti'nin de taraf olduğu AKSSS'nin 2. maddesinden doğan bir yükümlülüktür. Bu yükümlülük anılan sözleşmenin 2. maddesinde; *"İç hukuka uygun olarak, bir bilgisayar sisteminin tamamına veya bir kısmına kasten ve haksız olarak erişilmesi suç haline getirmek için gerekli görülen yasal tedbirleri alma"* olarak belirtilmiştir. Sözleşme, Sözleşme'ye taraf devletlere erişimin suç olarak düzenlenmesi için yapılan erişimin haksız ve kasten olması koşulunu araması yükümlülüğünü de yüklemiştir[173].

Bununla beraber kanunun ilk halindeki *"ve"* bağlacı yerine *"veya"* bağlacı getirilmesi de yine AKSSS ile uyum sağlamak amacıyla yapılmıştır. TCK'da ayrıca

---

[172] Mahmut **KOCA** – İlhan **ÜZÜLMEZ**, Türk Ceza Hukuku Özel Hükümler, B. 3, Adalet Yay. Ankara 2016, s.806.

[173] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 806; Veli Özer **ÖZBEK** – Koray **DOĞAN** – Pınar **BACAKSIZ** – İlker **TEPE**, Türk Ceza Hukuku Özel Hükümler, Seçkin Yay., B. 12, Ankara 2017, s. 939; SOKULLU AKINCI, s. 14.

Sözleşme ile taraf devletlere yükümlülük olarak tanımlanmayan *"hukuka aykırı olarak kalmaya devam etme"* eylemini de seçimlik hareket olarak yaptırıma bağlamıştır. TCK'nın Sözleşme'den bir diğer farkı da, Sözleşme'de kullanılan *"bilgisayar sistemi"* ifadesi yerine *"bilişim sistemi"* ifadesine yer verilmesidir. Ayrıca Sözleşmede, TCK'dan farklı olarak suçun nitelikli haline yahut netice sebebiyle ağırlaşmış şekline yer verilmemiştir.[174]

6698 Sayılı Kanun ile 2016 yılında TCK'nın 243. maddesine 4. fıkra eklenmişse de eklenen 4. fıkranın, 243. maddenin ilk fıkrasında temel hali düzenleme altına alınan *"Bilişim sistemine girme suçu"* ile esasen bir bağlantısı bulunmamaktadır[175]. Bu nedenle bu fıkra yeni bir suç tanımı olarak kabul edilecek ve ayrıca incelenecektir.

B. HUKUKİ KONU

Her suç bir hukuki değerin yahut menfaatin ihlalidir. Bu nedenle her suçun hukuki konusu da hukuken korunan ve bu nedenle hukuki değer veya menfaat olarak anılan varlık

[174] AKBULUT, s. 115.

[175] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 807.

yani suçun kanuni tanımı ile olası saldırılardan korunmaya çalışılan şeydir.[176] Bir başka deyişle suçun hukuki konusu fail tarafından zarar verilmek istenen değerdir[177].

Doktrinde suçun hukuki konusunun tespitinde farklı görüşler mevcuttur. Bu görüşlerden ilkine göre; hukuki konu değerlendirilirken suçun düzenlendiği yer büyük önem arz etmektedir. Bu anlamda suçun düzenlendiği yerin *"Topluma Karşı Suçlar"* olması da gözetildiğinde, elbette ki suç nedeniyle kişinin çıkarı da zarar görmekle beraber, bilişim sisteminin düzgün ve güvenli olarak işlenmesinde ferdi-kamusal yarar yani karma bir yarar hukuki konu olarak kabul edilmelidir.[178]

Doktrindeki diğer görüş; suçun başta özel hayata ilişkin veriler ve kişisel veriler olmak üzere esasen verilerin korunması amacıyla düzenleme altına alındığını, dolayısıyla da verilerin korunmasını sağlayan her türlü değerin suçun hukuki konusu olduğunu kabul etmektedir.[179] Bu görüşe benzer bir görüşe göre; bu suçun hukuki konusu karma niteliktedir. Kişilerin özel hayatı ve kişisel verilerinin korunması, şirket ve kurumlarım bilişim sistemlerinin güvenli bir şekilde işlemeye devam etmesinin sağlanması, mülkiyet

---

[176] Zeki **HAFIZOĞLLARI –** Muharrem **ÖZEN**, Türk Ceza Hukuku Genel Hükümler, US-A Yay., B. 12, Ankara 2019, s. 199.

[177] Doğan **SOYASLAN**, Ceza Hukuku Genel Hükümler, B. 7, Yetkin Yay., Ankara 2016, s. 236.

[178] Muharrem **ÖZEN** – Zeki **HAFIZOĞULLARI**, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, US-A Yay., B. 2, Ankara 2016, s. 445; M. Emin **ARTUK** – Ahmet **GÖKCEN** – A. Caner **YENİDÜNYA**, Ceza Hukuku Özel Hükümler, B. 15, Adalet Yay., Ankara 2015, s. 860.

[179] AKBULUT, s. 119;

hakkı ve zilyetlik gibi hakların korunması ve kamu güvenliğinin sağlanması gibi bilişim sistemlerinin korunmasıyla korunacak tüm hak ve menfaatler bu suçun hukuki konusunu oluşturmaktadır[180].

Bir diğer görüşe göre; suç kapsamında kişinin bilişim sistemi üzerindeki özel alanının korunması amaçlanmaktadır. Her ne kadar bu özel alanın korunmasının farklı amaçları olduğu öne sürülebilecekse de nihai olarak düzenleme ile bu özel alanın korunmaya çalışıldığı açıktır.[181]

Yine bir diğer görüşe göre; bu suçun ortaya çıkabilmesi için sisteme haksız olarak ve kasten girilmesi yeterli olup sistemdeki verilerin bir kısmının ya da tamamının elde edilmesi veya sistem üzerinde bulunan verilerin zarar görmesi gerekmediğinden suçla korunan hukuki değerin kişilerin özel hayatının gizliliği veya malvarlığı değerlerinin korunması olduğu söylenemeyecektir.[182]

Benim de katıldığım görüşe göreyse; bu suçun temel olarak konusu; günümüzde hayatın her alanında hemen her kişi ve kurum tarafından kullanılan bilişim sistemlerinin

---

[180] Cengiz **APAYDIN**, Bilişim Suçları ve Bilişim Ceza Hukuku, B. 1, Acar Matb., İstanbul 2017, s. 51; ESEN, s. 628.

[181] Hakan **KARAKEHYA**, *"Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu"*, TBB Dergisi, Ankara 2009, S. 81, s. 199.

[182] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 807; Aynı görüş için bknz: Durmuş **TEZCAN** – Mustafa Ruhan **ERDEM** – R. Murat **ÖNOK**, Teorik ve Pratik Ceza Özel Hukuku, B. 13, Seçkin Yay., Ankara 2016, s. 944.

güvenliğinin sağlanmasıdır.[183] Bununla beraber yetkisiz erişimin engellenmesi suretiyle bilişim sistemlerinin güvenli hale getirilmesini sağlayarak toplumun da bilişim sistemlerine karşı güven duymasını ve kullanıcıların özel hayatının gizliliği ile haberleşme özgürlüğünün korunmasıdır[184]. Ancak özel hayatın gizliliğinin korunması kanaatimce, suçun düzenlendiği yer, suçun ortaya çıkması için özel hayata ilişkin verilerin ele geçirilmesi vs. gibi bir koşul olmaması ve özel hayata ilişkin ayrıca koruma sağlayan kanun hükümleri olması gibi hususlar da gözetildiğinde, ancak ikincil bir konu olarak kabul edilmelidir.

C. FAİL

Bir suçun faili, anılan suçun kanuni tanımında yer alan fiili gerçekleştiren kişidir[185]. Herkesin faili olması mümkün olmayan yalnızca belirli bir nitelik veya sıfata sahip olan kişiler tarafından işlenmesi mümkün olan suçlara ise özgü suç denilmektedir[186].

---

[183] DÜLGER, s. 348; Aynı görüş için bknz: KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 807.

[184] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 940; TAŞKIN, s. 23; ARTUK – GÖKCAN – YENİDÜNYA, s. 860; TEZCAN – ERDEM – ÖNOK, s. 945; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 123; Aynı görüş için bknz: GÜL, s. 59.

[185] Hakan **HAKERİ**, Ceza Hukuku Genel Hükümler, B. 19, Adalet Yay., Ankara 2016, s. 133.

[186] HAKERİ, 2016, s. 139.

5237 Sayılı TCK'nın 243. maddesinde ilk fıkrada "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimse"* denilerek kanuni düzenlemede suçun faili olmak için herhangi bir özellik aranmadığından[187] herkesin bu suçun faili olması mümkündür[188]. Bu yönüyle incelendiğinde TCK'nın 243. maddesinde düzenlenen bu suç tipi faili bakımından özgün bir suç değildir[189].

Bu suç bakımından fail bilişim sistemine yetkisiz bir şekilde erişim sağlayan ve/veya orada kalmaya devam eden kişi herhangi bir kişi bu suçun faili olarak kabul edilmelidir[190].

Tüzel kişilerin bir suçun faili olması mümkün olmadığından TCK'nın 20/2. maddesi uyarınca bir tüzel kişi hakkında işlenen suçtan dolayı ancak ve ancak tüzel kişilere özgü güvenlik tedbiri uygulanabilecektir[191]. Bu nedenle tüzel kişilerin bu suçun faili olması mümkün değildir. Bununla beraber anılan suçun işlenmesi tüzel kişi yararına

---

[187] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 808; TEZCAN – ERDEM – ÖNOK, s. 945; AKBULUT, s. 120.

[188] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 445; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 940; ARTUK – GÖKCAN – YENİDÜNYA, s. 865; DÜLGER, s. 351; GÜL, s. 60.

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

[190] APAYDIN, s. 53.

[191] Berrin **AKBULUT**, Ceza Hukuku Genel Hükümler, B. 3, Adalet Yay., Ankara 2016, s. 335.

haksız bir şekilde menfaat sağlanması sonucunu doğurmuşsa TCK'nın 246. maddesi uyarınca haksız menfaat sağlayan tüzel kişi hakkında tüzel kişilere özgü güvenlik tedbirlerinin uygulanması gerekmektedir.[192]

D. MAĞDUR

Suç neticesinde bir hukuki değer veya hukuki menfaat ihlal olduğundan doğal olarak bu fiilin bir mağdurunun ya da suçtan zarar göreninin bulunması gerekir. Suçun mağduru kavramından ise anlaşılması gereken en basit haliyle suçla ihlal edilen hukuki değer veya hukuki menfaatin sahibidir.[193]

Doktrindeki bir görüşe göre; güvenli bir bilişim olanağı sağlamak kamu düzeninden olduğundan anılan suçun mağdurunun kamu idaresi olduğunun kabulü gerekir. Suçun kanun koyucu tarafından bilerek ve isteyerek *"Kişilere Karşı Suçlar"* değil de *"Topluma Karşı Suçlar"* arasında düzenlendiği de gözetildiğinde; hak sahibi kişi veya kişilerin burada ancak suçtan zarar gören konumunda olması mümkündür.[194] Yine benzer bir görüşe göre de anılan kanuni düzenleme ile bilişim sisteminin korunması amaçlandığından belirli bir kişinin suçun mağduru olması mümkün değildir[195].

---

[192] KOCA ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 809; DÜLGER, s. 359.

[193] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 208.

[194] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 445.

[195] TEZCAN – ERDEM – ÖNOK, s. 945.

Diğer bir görüşe göreyse ilgili verilerin sahibinin mağdur olarak nitelendirilmesi mümkün değildir. Ancak yalnızca bilişim sisteminin sahibinin yahut ortaklarının failin eylemi nedeniyle itibarı zedelendiğinden ve mülkiyet hakkı ihlal edildiğinden bu suç bakımından mağdur olarak kabul edilmesi gerekmektedir.[196]

Benim de katıldığım bir başka görüşe göreyse; bu suç mağdur bakımından bir özellik göstermediğinden bir bilişim sisteminin güvenliği ihlal edilen ve sistem üzerinde hak sahibi olması nedeniyle çıkarı zarar gören herkes anılan suçun mağduru olarak kabul edilebilecektir.[197] Hak sahibi tek kişi olabileceği gibi birden fazla kişinin de hak sahibi sıfatına sahip olması mümkün olduğundan bu suçun işlenmesi halinde hak sahiplerinin tamamı bu suçun mağduru olacaktır.[198] Örneğin bir başkasına ait bilgisayarda kişisel dosyalarını tutan kimse ve bilgisayar sahibi bu dosyalara yetkisiz erişim sağlanması halinde mağdur olarak kabul edilecektir.[199]

Doktrinde tüzel kişilere ait sistemlere gerçekleştirilen erişime ilişkin olarak esasen tüzel kişilerin temel hukuki menfaati zedelenebileceği gerekçesiyle yalnızca tüzel

---

[196] AKBULUT, s. 122.

[197] DÜLGER, s. 359; Ali **PARLAR**, Bilişim Alanında Suçlar, B. 3, Bilge Yay., Ankara 2015, s.18; bknz. DEMİRCAN, s. 69.

[198] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 940; ARTUK – GÖKCAN – YENİDÜNYA, s. 867; GÜL, s. 60-61; Aynı görüş için bknz: KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 809; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 145-146.

[199] ARTUK – GÖKCAN – YENİDÜNYA, s. 867; Aynı görüş için bknz: APAYDIN, s. 53-54.

kişilerin mağdur olarak kabul edilmesi gerektiğini savunan yazarlar bulunmaktadır.[200] Bir diğer görüşe göre örneğin bankaya ait bilişim sistemine girilerek birden çok müşterinin hesabına yetkisiz erişim sağlanması halinde her müşteri ayrı ayrı mağdur, tüzel kişiliğe sahip banka ise suçtan zarar gören olarak anılacaktır.[201]

Ancak kanaatimce; bu suçun mağduru bakımından özel, tüzel veya gerçek kişi şeklinde bir ayrım yapılmadığından sistemine girilen banka ve sistemdeki veri sahibi üzerinde hak sahibi olan kişi mağdur olarak anılmalıdır.

E. BİLİŞİM SİSTEMİNE GİRME SUÇUNUN UNSURLARI

1. Fiil

Genel olarak fiil, hareket ile netice arasındaki neden sonuç ilişkisini ifade eden bir nedensellik bağından ibarettir. Hareket bedenin algılanabilir bir devinimi olarak kabul edilebilir. Hareket neticesinde dış dünyada gerçekleşen sonuç ise neticedir.[202]

Suçun maddi unsurundan bahsedebilmek için muhakkak bir icra veya ihmal hareketi gerekmektedir. Hareket olmadan suç olması mümkün değildir. Zira bir ceza

[200] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 145; AKBULUT, s. 122; Aynı görüş için bknz: GÜL, s. 60.

[201] DÜLGER, s. 360.

[202] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 167-168, 176.

kanunun ihlali anlamına gelen suç, eşyanın tabiatı gereği, failin bir hareketidir.[203] İnsanın iç dünyasında gerçekleşen herhangi bir şey suç teşkil etmez, suç daima dış dünyada gerçekleşen bir olaydır.[204]

5237 Sayılı TCK'nın 243. maddesinde ilk fıkrasında fiil "*Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam etmek"* şeklinde düzenlenmiştir.

TCK'nın 243. maddesi ilk fıkrasında düzenlenen *"Bilişim sistemine girme suçu"*nun ortaya çıkabilmesi için sistemin tamamına ve bir kısmına "*hukuka aykırı olarak girmek veya orada kalmaya devam etmek"* gerekmektedir. 6698 Sayılı Kanun ile 2016 yılında 5237 Sayılı Kanun'da yer alan düzenlemede *"ve"* ifadesi yerine *"veya"* ifadesi getirilerek suç kanunda seçimlik hareketli bir suç olarak düzenlenmiştir. Bu nedenle suçun *"sisteme hukuka aykırı olarak girmek"* fiili ile gerçekleştirilmesi mümkün olduğu gibi *"sistemde kalmaya devam etmek"* şeklinde gerçekleştirilmesi de mümkündür.[205]

243. maddenin düzenleme altına alınması sırasında kanun koyucu tarafından kaleme alınan madde gerekçesinde bilişim sistemi *"Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren*

[203] SOYASLAN, s. 229.

[204] Türkan **YALÇIN** – Timuçin **KÖPRÜLÜ**, Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları, B. 6, Savaş Yay., Ankara 2019, s. 175.

[205] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 810; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 944.

manyetik sistemlerdir." İfadeleriyle tanımlanmıştır. Yine Yargıtay da madde gerekçesindeki tanımı kabul etmiştir[206].

Doktrinde suçun tanımı sırasında kullanılan *"girmek"* kelimesi yerine *"erişmek"* kelimesinin kullanılması gerekip gerekmediği hususunda bir tartışma mevcuttur. Bu çerçevede doktrinde *"erişmek"* kelimesi yerine *"girmek*" kelimesinin kullanılmasının isabetli olduğunu savunan bir görüş mevcuttur. Bu görüşe göre; erişmek kelimesi yalnızca bir bilişim ağının vasıta olarak kullanılmasını gerekli kılan ve bu şekilde sisteme ulaşılmasının sağlanmasını ifade etmektedir. Nitekim "*Avrupa Konseyi Siber Suçlar Sözleşmesi"* ve *"5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Kanunu"*na istinaden çıkartılmış diğer mevzuat hükümlerinde de bu doğrultuda *"erişim"* kelimesi kullanılmıştır. Oysa TCK'da yer alan hüküm ile bir bilişim sisteminde hukuka aykırı bir şekilde olarak oturum açmak yahut bilişim sisteminin başına oturmak suretiyle bu suçun işlenebileceği düzenleme altına alınmıştır. Bu nedenle bu görüşe göre "*erişmek"* kelimesi yerine *"girmek*" kelimesinin kullanılması doğrudur.[207]

Bir diğer görüşe göre; kanun koyucu tarafından kullanılan *"girmek"* kavramı sistem ile kanun koyucu tarafından kastedilen bir bilgisayar ya da sunucuya mekanik yollarla yahut sistemin fiziksel olarak açılarak müdahale edilmesi değil bilişim sisteminin

---

[206] *"Yerleşmiş yargısal kararlar ve öğretideki baskın görüşlere göre de, bilişim sisteminin, verileri toplanıp yerleştirdikten sonra otomatik işleme tabi tutma imkanı veren manyetik sistemler olduğu kabul edilmiştir."* YCGK, 11.06.2013, 2013 / 15-239 E., 2013 / 432 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[207] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812; AKBULUT, s. 129.

oluşturduğu sanal alana dahil olunmasıdır[208]. Nitekim Yargıtay da bir kararında *"bilişim sistemine girme"* eyleminin esasen bilişim sistemine erişim sağlanması olduğunu vurgulamıştır[209].

Doktrinde de; suçun kanuni tanımında yer alan *"girmek"* kelimesinin fiziki bir mekana girmeyi çağrıştırdığı oysa soyut bir alan olan bilişim sistemine fiziken girişin mümkün olmadığı bu nedenle de *"bilişim sistemine girme"*ye genel olarak; *"erişim"* denilmesi gerektiği ifade edilmiştir.[210]

Esasen "*girmek"* kavramı, dilimize *"access"* kavramının çevirisi olarak girmiştir. AKSSS'nin İngilizce metninde de bu suç *"illegal access"* yani yetkisi ya da hukuka aykırı erişim olarak adlandırılmıştır.[211] Bu nedenle *"girmek"* yerine *"erişim"* ifadesinin

---

[208] DÜLGER, s. 363; Aynı görüş için bknz: ARTUK – GÖKCEN – YENİDÜNYA, s.861; YAŞAR – GÖKCAN – ARTUÇ, s. 7292.

[209] *"Bilişim sistemine girmek, bir bilişim sisteminde bulunan verilerin bir kısmına veya tamamına, fiziken ya da uzaktan başka bir cihaz yoluyla erişilmesidir."* Yargıtay 8. Ceza Dairesi, 11.03.2015, 2014 / 29566 E., 2015 / 13421 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[210] KARAGÜLMEZ, s. 204; Aynı görüş için bknz: DÜLGER, s. 365; ARTUK – GÖKCEN – YENİDÜNYA, s.861; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812-813; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 944.

[211] Muammer **KETİZMEN**, Türk Ceza Hukuku'nda Bilişim Suçları, Doktora Tezi, AÜ SBE, Ankara 2006, s. 120-121; Aynı görüş için bknz: ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 944; Aynı görüş için bknz: DOĞAN, s. 48

kullanılması, *"hukuka aykırı olarak girmeye"* yerine ise "*yetkisiz erişim"* veya *"hukuka aykırı erişim"* denilmesinin daha doğru olacaktır[212].

Elbette bir bilişim sisteminin sanal ağına dahil olunması internet yahut sair sanal yollarla olabileceği gibi bilişim sisteminin başına geçilmesi ve açma tuşunun kullanılarak sanal ağa dahil olunması suretiyle gerçekleştirilebilecektir.[213] Ancak kanaatimce fiil ister sistemin başına oturmak ve açma tuşunu kullanmak şeklinde gerçekleştirilsin isterse de bir sanal ağ üzerinden sisteme erişim sağlansın her halde sistem fiziken bir mekana girer gibi girilmeyecek, bir sanal ağa dahil olacaktır. Bu nedenle de doktrindeki *"girmek"* yerine *"erişmek"* ifadesinin kullanılması yönündeki görüşe katılmaktayım.

Genel olarak erişimin; bir *"bilişim sistemine girme"*yi ve/veya sistem içerisinde herhangi bir şekilde işlem yapılmasını kapsadığının kabulü gerekir. Doğal olarak sistemde herhangi bir şekilde işlem yapılabilmesi için sisteme öncelikle erişim sağlanması gerekmektedir.[214] Bununla beraber sistemin tamamına erişilmesi ve/veya

---

[212] KETİZMEN, s. 120-121; KARAGÜLMEZ, s. 204; Aynı görüş için bknz: HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446.

[213] DÜLGER, s. 363; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812; *"Suçun, başkasına ait bilgisayarın açılarak içindeki verilerin görülmesi biçiminde olabileceği gibi, bir ağ aracılığıyla bilişim sisteminde oturum açılması yoluyla da işlenebilir."* Yargıtay 8. Ceza Dairesi, 03.02.2015, 2014 / 19342 E., 2015 / 2322 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020); Yargıtay 8. Ceza Dairesi, 11.06.2020, 2017 / 21566 E., 2020 / 13171 K. Sayılı Karar, Yayımlanmamış Karar.

[214] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446.

erişilen sistemde hukuka aykırı olarak kalınması ile sistemin bir kısmında bu fiillerin gerçekleştirilmesi arasında hukuki sonuç anlamında bir farklılık bulunmamaktadır[215].

Bilişim sistemlerinde bir yönetici bulunması esastır. Yöneticiler sistem üzerinde teknik olarak mümkün olan bütün iş ve işlemleri gerçekleştirme konusunda yetkilidirler. Kullanıcıların yetkileri ve bu yetkilerin sınırları da genellikle yönetici tarafından belirlenmektedir.[216] Yani yönetici tarafından bir kullanıcının sistemin yalnızca bir kısmına erişim sağlanmasına yahut sistem üzerinde yalnızca belirlenen işlemlerin yapılabilmesine müsaade edecek şekilde yetkilendirilmesi mümkündür. Anılan yetkilerin ihlal edilerek yetkili olunmadığı halde bir kısım işlemlerin yapılması yahut yetki kapsamı dışında yer alan yerlere girilmesi halinde yine yetkisiz veya hukuka aykırı erişim söz konusu olacaktır.[217]

Yetkisiz erişimin birden fazla yolla gerçekleştirilmesi mümkündür. Kanuni düzenlemeye göre yetkisiz bir erişimden bahsedilebilmesi için herhangi bir özel yol veya yöntem belirlenmemiştir.[218] Bu şekildeki bir erişimin sistemi kullanmaya yetkisi olan bir kullanıcıya ait bilgilerin elde edilmesi suretiyle gerçekleştirilmesi mümkün olduğu

[215] TEZCAN – ERDEM – ÖNOK, s. 947; AKBULUT, s. 132; Aynı görüş için bknz: KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812.

[216] PARLAR, s. 19; KETİZMEN, s. 122; Aynı görüş için bknz: HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446.

[217] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446; DÜLGER, s. 377-378, PARLAR, s. 19.

[218] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 813; PARLAR, s. 18-19.

gibi[219], sistemde yer alan eksikliklerden, açıklardan faydalanmak yahut sistemde açık oluşturmak suretiyle gerçekleştirmek de mümkündür.[220] Yine sisteme yetkisiz erişimler bir başka bilgisayar kullanılarak hedef alınan bilgisayara herhangi bir şekilde erişim sağlanmak suretiyle ya da hedef bilgisayarın herhangi bir aracı kullanılmaksızın doğrudan kullanılması suretiyle de gerçekleşebilir[221]. İletişimin yöntemi kablolu yahut kablosuz olması, bir program aracılığıyla yapılıp yapılmaması ya da mesafenin kısa veya uzun olması da yine bu suç bakımından bir önem arz etmemektedir[222]. Bunun yanı sıra sisteme virüs, Truva atı, solucan vb. programlar kullanılarak da hukuka aykırı erişim sağlanabilir[223].

---

[219] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 944-945.

[220] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446.

[221] GÜL, s. 63; Aynı görüş için bknz: HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446; Ayrıntılı Bilgi için bknz: KETİZMEN, s. 124.

[222]GÜL, s. 62; *"Girmede, iletişimin kablolu veya kablosuz olmasıyla mesafenin yakın ve uzak olması arasında da fark yoktur."* Yargıtay 8. Ceza Dairesi, 11.03.2015, 2014 / 29566 E., 2015 / 13421 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020); Aynı görüş için bknz: ARTUK – GÖKCEN – YENİDÜNYA, s. 861.

[223] *"Erişimi gerçekleştirmek için gevşek güvenlik önlemlerinden faydalanılabileceği gibi, var olan güvenlik önlemlerindeki boşluklar da kullanılabilir. Ağ üzerinden virüsler (komik resimler, kutlama kartları veya ses ve görüntü dosyaları gibi ekler halinde), truva atı (trojan horse), macro virüsü, solucanlar gibi kullanılarak veya sistemin açık kapıları*

Bilişim sistemine elektronik bir sistemle erişim sağlanabileceği gibi fiziksel olarak da erişim sağlanabileceği kabul edilmekle birlikte açık ekranda bulunan bilgilerin görülmesi yahut sistemin gözle uzaktan izlenmesi bu suçu oluşturmayacaktır. Suçun ortaya çıkması için görmek yeterli olmayıp fiziksel müdahalenin de elverişli vasıtalarla gerçekleştirilmesi gerekir.[224] Yine bir kişiye e-posta yahut dosya gönderilmesi de yalnızca veri gönderimi olarak kabul edilecek ve bu suç kapsamında değerlendirilemeyecektir[225].

Netice ancak ve ancak suçun kanuni tanımında belirtilmiş ise aranması gereken bir unsurdur[226]. *"Bilişim sistemine girme suçu"* bakımından ise suçun kanuni tanımında

---

zorlanarak giriş yapılabilir." Yargıtay 8. Ceza Dairesi, 03.02.2015, 2014 / 19342 E., 2015 / 2322 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[224] ARTUK – GÖKCEN – YENİDÜNYA, s. 863; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 132; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 814.

[225] **YARGITAY CUMHURİYET BAŞSAVCILIĞI**, Ceza Muhakemesinde Toplanması Gereken Deliller (TCK – Özel Yasalar), Türkiye Adalet Akademisi, Ankara 2020, s. 861;*"Bir bilişim sistemine e-posta veya dosya gönderilmesi durumunda, bilişim sistemine girme söz konusu olmayıp yalnızca veri gönderildiğinden, bu durum girme kapsamında düşünülemez."* Yargıtay 8. Ceza Dairesi, 11.03.2015, 2014 / 29566 E., 2015 / 13421 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[226] Mahmut **KOCA** – İlhan **ÜZÜLMEZ**, Türk Ceza Hukuku Genel Hükümler, B. 9, Seçkin Yay. Ankara 2016, s. 122.

bir netice öngörülmemiştir[227]. Yani soyut bir tehlike suçudur, bir zararın ortaya çıkması gerekmemektedir[228]. *"Bilişim sistemine girme suçu"* salt hareket suçudur[229]. Suça uygun hareket, suçun oluşması için yeterlidir. Bunun dışında sistemde yer alan bilgilerin öğrenilmesi, verilerin değiştirilmesi veya silinmesi, sisteme zarar verilmesi vs. bu suçun ortaya çıkması için zorunlu değildir.[230] Hatta hareket neticesinde failin eylemi sistemdeki verilerin yok olmasına sebep olmuşsa yahut verilerin değişmesi neticesi doğurmuşsa bu halde TCK'nın 243/3. maddesinde düzenlenen suçun nitelikli hali ortaya çıkacaktır.[231]

"Bilişim sistemine girme suçu" ani hareketli suç olduğundan kesintisiz olarak işlenmesi mümkün değildir. Ancak bilişim sisteminde hukuka aykırı olarak kalmaya devam etme suçu kesintisiz suçtur. Fail sistemde kalmaya devam ettiği sürece suç işlemeye devam eder.[232]

---

[227] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 814; DÜLGER, s. 369; AKBULUT, s. 128; Aynı görüş için bknz: ARTUK – GÖKCEN – YENİDÜNYA, (14), s. 747

[228] **YARGITAY CUMHURİYET BAŞSAVCILIĞI**, Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (TCK – Özel Yasalar), Türkiye Cumhuriyeti Adalet Bakanlığı, Ankara 2018, s. 831; GÜL, s. 64.

[229] Hasan Burak **ÖNDİN**, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman",* Terazi Hukuk Der., C. 15, S. 162, Ankara 2020, s. 333. (320-337)

[230] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 813; DÜLGER, s. 369; Aynı görüş için bknz: TEZCAN – ERDEM – ÖNOK, s. 944.

[231] KARAGÜLMEZ, s. 205; GÜL, s. 63; PARLAR, s. 19.

[232] ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman",* s. 333.

Bilişim sistemine her erişim sağlama fiili aynı zamanda kalmayı da doğal olarak zorunlu kılmaktadır.[233] Ancak bahsi geçen suçun seçimlik hareketli olması nedeniyle sisteme hukuka aykırı erişim sağlanması halinde suçun ortaya çıkması için failin bir süre sistemde kalması gerekli değildir[234]. Bu suçun, failin hukuka uygun bir şekilde sisteme erişimi sonrasında veya sistemden çıkılması gerektiğini öğrenmesine rağmen hukuka aykırı bir şekilde sistemde kalınmaya devam etmesi[235] yahut failin bir başkası tarafından hukuka uygun veya aykırı bir şekilde erişilen sistemde hukuka aykırı olarak kalmaya devam etmesi suretiyle işlenmesi[236] mümkündür. Sistemde ne kadar süre kalınması halinde suçun ortaya çıkacağına ilişkin olarak ise bir düzenleme bulunmadığından sistemde kalınan süre suçun oluşması için bir unsur değildir[237].

Bu suçun ortaya çıkması için sisteme yetkisiz erişim sağlanmasını önlemek için tedbir alınmış olması şart değildir.[238] Yani hukuki bir sınırın mevcut olması yeterlidir. Ancak hak sahibince sisteme girilmesine açık veya örtülü olarak onay verildiği takdirde

[233] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 811.

[234] TEZCAN – ERDEM – ÖNOK, s. 946-947.

[235] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s 812; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 945; ARTUK – GÖKCEN – YENİDÜNYA, s. 861; AKBULUT, s. 137.

[236] TEZCAN – ERDEM – ÖNOK, s. 947.

[237] TEZCAN – ERDEM – ÖNOK, s. 947.

[238] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 813; AKBULUT, s. 32.

bu suç oluşmayacaktır.[239] Örnek vermek gerekirse; bilişim sistemine giriş yapılabilmesi için tedbir almak maksadıyla şifre konulmuşsa, sisteme yetkili olmayan kimselerin girmesinin önüne geçilmeye çalışıldığı açıktır. Ancak anılan sisteme herkesin istediği zaman erişmesine imkan tanınmışsa yani sistem kamuya açık hale getirilmişse artık burada bir suçtan bahsedilemeyecektir.[240] Ayrıca hukuki sınırın mevcudiyeti için sıkı güvenlik tedbirleri aranmamalı, boşlukları olan yahut gevşek güvenlik tedbirlerinin varlığı halinde de sisteme yetkisiz erişim sağlandığı taktirde suçun unsurlarının oluştuğu kabul edilmelidir[241].

Bununla beraber sisteme girişine izin verilen kişinin izin amacının dışına çıkarak başka bir amaçla sisteme erişim sağlaması halinde yetkisiz yahut hukuka aykırı erişimden bahsedilemeyecek dolayısıyla da suçun oluştuğu kabul edilemeyecektir[242].

Üzerinde durulması gereken bir diğer hal ise sisteme giriş yetkisi tanımlanmış kişinin başkasına ait bir kullanıcı adı ve şifreyle yahut başka bir yöntem ile sisteme erişim sağlaması halidir.

Doktrindeki bir görüşe göre; bu halde başkasına ait kullanıcı adı ve şifreyle yahut başka bir yöntemle sisteme giriş yapan failin hukuka uygun olarak sahip olduğu erişim yetkilerinin sınırları değerlendirilmelidir. Şayet fail kendisine denk bir yetkiyle yahut

[239] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 813; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 133; AKBULUT, s. 134; KARAKEHYA, 204.

[240] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 944; DÜLGER, s. 378; Aynı görüş için bknz: KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 813.

[241] AKBULUT, s. 135.

[242] Bknz: AKBULUT, s. 137.

daha az bir yetkiyle sisteme erişim sağlamış ise bu halde bu suçun unsurları oluşmayacaktır. Kendi yetkisini aşan bir halde erişim sağlayacak olursa artık bu halde suçun unsurlarının oluştuğunun kabulü gerekmektedir.[243]

Ancak benim de katıldığı görüşe göre; bu suç ile korunmak istenen temel hukuki değerlerin başında bilişim sisteminin güvenilirliğinin sağlanması olması karşısında kişinin kendi yetkisi dışına çıkmasa dahi başka bir kullanıcı adı ve şifre kullanmak yahut başka bir yöntem kullanmak suretiyle sisteme erişim sağlaması halinde suçun unsurlarının oluştuğunun kabulü gerekmektedir. [244]

Bu suçun seçimlik olarak icrai hareketle veya ihmali hareketle işlenebilmesi mümkündür. Sisteme hukuka aykırı şekilde erişim sağlamanın icrai bir hareket, sistemde hukuka aykırı bir şekilde kalmanın ise ihmali bir hareket olarak nitelendirilmesi gerekmektedir. Ancak bu hareketlerin birlikte gerçekleştirilmesi halinde tek suçun bulunduğu kabul edilmelidir.[245]

Her iki hareketten herhangi birinin tek başına gerçekleştirilmesi halinde failin cezalandırılması arasında kanunda bir fark öngörülmediğinden her iki eylemin yaptırımları arasında bir fark bulunmamaktadır[246].

---

[243] KETİZMEN, s. 125-126.

[244] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 133;

[245] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812.

[246] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 446; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 812.

2. Hukuka Aykırılık

Suç teşkil eden bir fiil gerçekleştirildiğinde yani suç işlendiğinde hukuki değer veya menfaati koruyan hukuk normu ihlal edilmiş olur.[247] İhlalsiz suç olmaz. Yani suç özünde suç teşkil eden fiil ile hukuk düzeni arasındaki çarpışma ve karşıtlık ilkesinden ortaya çıkmaktadır. Bu çerçevede suçun hukuka aykırılık unsuru olarak ceza hukukunu ihlal eden fiil anlaşılmalıdır.[248]

Bir bilişim sistemine, kısmen veya tamamen erişim yetkisi olmaksızın girmek veya orada kalmayı sürdürmek suçun hukuka aykırılık unsurudur[249]. Yine failin yetkisinin sınırları içerinde kalmaksızın sistem içerisinde iş ve işlemler yapması da failin hukuka aykırı davranması halini oluşturacaktır[250]. Suç sona ermeden, erişimin sürdüğü esnada verilen rızanın eylemi hukuka uygun hale getirmeyeceği yönünde görüş de

[247] Kayıhan **İÇEL**, Ceza Hukuku Genel Hükümler, B. 1, Beta Basım, Ankara 2016, s. 156.

[248] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 193.

[249] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 815; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 948.

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

doktrinde mevcut olmakla birlikte[251]; hukuka aykırı olarak gerçekleştirilen erişim sonrasında rıza alınması fiili hukuka uygun hale getirecektir[252].

Doktrinde yer alan bir görüşe göre; yetkisiz erişimin hiçbir suretle hukuka uygun hale gelmesi mümkün değildir. Yani hukuka uygunluk nedenlerinin bu suç bakımından uygulanması mümkün değildir.[253] Ancak bu görüşe katılmak mümkün değildir. Kanunun verdiği yetkiye dayanarak ve yine kanunun usul ve şartlarına uygun olarak yahut mağdurun rızası alınarak sisteme erişim sağlanması veya sistemde kalınması hali söz konusu ise bu halde hukuka uygunluk nedenlerinin mevcut olduğu kabul edilmelidir.[254]

3. Kusurluluk

[251] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448.

[252] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 948; DÜLGER, s. 391; Aynı görüş için bknz: ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 160.

[253] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448.

[254] YAŞAR – GÖKCAN – ARTUÇ, s. 7295; TAŞKIN, s. 27-28; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 815; DÜLGER, s. 685; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 162; Aynı görüş için bknz: ARTUK – GÖKCAN – YENİDÜNYA; s. 877.

Suç teşkil eden bir fiil icra eden fail ile fiil arasında muhakkak bir manevi bağ bulunmalıdır[255]. Yani failin fiili kendi iradesiyle icra etmesi gerekmektedir. İradesiz bir fiil kesinlikle suç oluşmayacaktır. Hukuk sistemimize göre suçun manevi unsuru olarak da kabul edilen kusurluluğun ortaya çıkması için icra yahut ihmal hareketinin muhakkak bilinçli olarak gerçekleştirilmesi gerekmektedir.[256]

Failin kusuru, ortaya çıkan hukuki değer veya menfaat ihlalini bir bütün olarak kapsamalı, ihlal edilen değer veya menfaat ile failin kusuru bir uyum içerisinde olmalıdır. Aksi halde failin kusurlu olmadığı bir hukuki değer veya menfaat ihlali söz konusu olacağından failin cezalandırılması mümkün olmayacak yahut fail kusurlu olmadığı bir ihlalden sorumlu tutulacaktır.[257]

Nitekim TCK'nın 21. maddesinde kast failin suçun kanuni tanımındaki unsurlarını iradi olarak yani bilerek ve isteyerek gerçekleştirmesi olarak tanımlanmıştır. Anılan hüküm uyarınca bir suçun ortaya çıkması için kural olarak failin kastının bulunması gerekir. Yani bir fiil kasıtlı olarak icra edilmemişse kural olarak fail sorumlu kabul edilemeyecektir. Bununla beraber TCK'nın 22. maddesinde failin dikkat ve özen yükümlülüğünü ihlal ederek suçun kanuni tanımında yer alan neticeyi gerçekleştirilmesi

[255] İzzet **ÖZGENÇ**, Türk Ceza Hukuku Genel Hükümler, B. 11, Seçkin Yay., Ankara 2016, s.221.

[256] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Genel Hükümler, s. 240.

[257] Hakan **HAKERİ**, Ceza Hukuku Genel Hükümler, B. 22, Adalet Yay. Ankara 2019, s.381.

olarak ifade edilen taksirin bir suç bakımından kanunda açıkça düzenlenen halinde failin taksirle gerçekleştirdiği fiilden de sorumlu tutulması mümkündür.[258]

"Bilişim sistemine girme suçu" genel kastla işlenebilecektir[259]. Yani failin zarar verme kastı olup olmamasını, merak, eğlence, reklam yahut eğlence saikiyle bu suçu işlemesinin suçun oluşumu bakımından bir önemi yoktur[260]. Nitekim kanun koyucu da madde gerekçesinde *"Sisteme hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir."* İfadelerine yer vererek genel kastın yeterli olduğunu açıkça ortaya koymuştur.

Suçun taksirli hali kanunda yer almadığından başkasının hak sahibi olduğu bir bilişim sistemine dikkatsizlik yahut özensizlik neticesinde erişim sağlayan ve bunu fark

---

[258] AKBULUT, Ceza Hukuku Genel Hükümler, s. 344-345.

[259] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 814. ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 948, 949; ARTUK – GÖKCAN – YENİDÜNYA; s. 875; DÜLGER, s. 381.

[260] Fazıl **GÜRLER**, Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, B. 1, Yetkin Yay., Ankara 2015, s. 126; AKBULUT, s. 139; PARLAR, s. 20; Ömer **DEMİR** – Mehmet **ARIÇ** – Halil **POLAT**, Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar, B. 1, Adalet Yay., Ankara 2015, s. 5.

eder etmez sistemden çıkan kişinin bu suçu işlediğini kabul etmek mümkün değildir.[261] Ancak başka birinin hak sahibi olduğu sisteme taksirle erişim sağlayan kişi bunu fark etmesine rağmen sistemde kalmaya devam ederse bu halde artık suçun manevi unsuru olan kastın ortaya çıktığının kabulü gerekir.[262]

Suçun olası kast ile işlenip işlenemeyeceği hususundaysa doktrinde tartışmalar mevcuttur. Bir kısım yazarlar suçun olası kastla işlenmesi de mümkün olduğunu savunmaktadır[263].

Ancak doktrindeki hakim görüşe göre suça ilişkin madde metninde *"hukuka aykırı olarak"* ifadesi özellikle belirtildiğinden suçun olası kast ile işlenmesi mümkün değildir. Kasttan anlaşılması gereken failin yetkili olmadığını, hukuka aykırı bir eylem icra ettiğini bilmesine rağmen bile isteye bir bilişim sistemine erişim sağlaması veya orada belirli bir süre kalmaya yönelik iradesidir.[264] Bu nedenle suç ancak doğrudan kastla işlenebilecektir.[265]

---

[261] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 815; ARTUK – GÖKCAN – YENİDÜNYA; s. 875, 876; KARAGÜLMEZ, s. 208.

[262] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 815; DEMİR – ARIÇ – POLAT, s. 5.

[263] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949

[264] ARTUK – GÖKCAN – YENİDÜNYA; s. 876; HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 815; DEMİR – ARIÇ – POLAT, s. 5.

[265] AKBULUT, s. 139.

Fail, erişime yetkisi olmadığını bilmeyerek, hataya düşerek, olmadığı halde kendisini yetkili sanarak sisteme erişim sağlar ve sistemde kalırsa bu durumda failin hatası lehine bir husus olarak değerlendirilmelidir[266]. Yine kusurluluğu ortadan kaldıran cebir veya tehdit gibi hallerden birisinin söz konusu olması halinde failin kınanması mümkün olmadığından suç oluşmayacaktır[267].

F. CEZAYI ETKİLEYEN HALLER

1. Hafifletici Nedenler

TCK'nın 243. maddesinde suçun bedeli karşılığında yararlanılabilen sistemler üzerinde işlenmesi hükmün ikinci fıkrasında bir indirim sebebi olarak düzenlenmiş ve verilecek cezanın yarı oranında indirileceği ifade edilmiştir.

Kanuni düzenlemede, gerekçede yahut bilinen teknik terimler arasında *"bedeli karşılığında yararlanılabilen sistemler"* tanımlanmamıştır. Bu nedenle doktrinde nerede gerçekleşen ihlallerin bu suç kapsamında değerlendirileceğine ve 2. fıkra kapsamında indirim sebebi olarak kabul edileceğine ilişkin olarak görüş ayrılıkları mevcuttur.[268]

[266] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448.

[267] KARAKEHYA, s. 202.

[268] DÜLGER, s. 374; APAYDIN, s. 64.

Doktrindeki bir görüşe göre; suçun ancak sistem üzerinde veya hizmet veren web siteleri üzerinde vs. gerçekleşmesi mümkündür zira *"internet kafe"* gibi yerlerdeki yapılan *"bilişim sistemine girme"* eylemi bir erişim değil kullanımdır.[269] Kanuni düzenlemede *"bedeli karşılığında yararlanılabilen sistemler"* ile kastedilen sistemin kullanıldığı fiziki ortamın değil sistem içinde sunulan, erişim imkanı sağlanan ücretli hizmetlerdir[270].

Diğer bir görüşe göreyse *"internet kafe ve play station salonu"* gibi yerlerde de bedel karşılığı sisteme erişim sağlanması ve bu tür işletmelerde de ticari maksatla hareket edilmesi nedeniyle diğer görüşe ek olarak *"internet kafe ve play station salonu"* gibi yerlerdeki izinsiz kullanımlar da bu suçu ortaya çıkartacak ve 2. fıkra kapsamında indirim sebebi olarak kabul edilecektir[271].

5237 Sayılı TCK'nın 163. maddesinde *"karşılıksız yararlanma"* başlığı altında ayrıca bir düzenleme yer aldığından otomatlar aracılığıyla kullanılan bir hizmetin, şifreli yahut şifresiz yayınların yahut telefon hatlarının sistemine hukuka aykırı bir şekilde erişim sağlanması bu suç kapsamında değerlendirilemeyecektir. Zira bu hususta özel bir düzenleme yapılmıştır[272]. Yine Yargıtay'ın geçmiş dönemlerde fikri bu suç ile

---

[269] KARAGÜLMEZ, s. 210; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s.149-150; AKBULUT, s. 144; Aynı görüş için bknz: ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 947.

[270] DOĞAN, s. 98-100; PARLAR, s. 22; GÜRLER, s. 129.

[271] ARTUK – GÖKCAN – YENİDÜNYA, s. 875; DÜLGER, s. 374; Aynı görüş için bknz: GÜL, s. 68.

[272] YAŞAR – GÖKCAN – ARTUÇ, s. 7299.

"karşılıksız yararlanma" suçu arasında fikri içtima gözetilmesi gerektiğine ilişkin vermiş olduğu bir karar bulunsa da[273] halihazırda Yargıtay bu içtihadını değiştirmiş ve sanıkların bir internet sitesi üzerinden bedeli karşılığında yararlanabilen bir yayını hukuka aykırı olarak para karşılığı yayınlamalarını bu suç kapsamında olmadığını belirterek suç tipini *"karşılıksız yararlanma"* olarak nitelendirmiştir[274].

---

[273] *"Bedeli karşılığında izlenmesi gereken şifreli televizyon yayınlarının, sahibinin rızasına aykırı olarak bedelsiz şekilde izlenmesini sağlamak eyleminde TCK'nun 163/2. maddesinde düzenlenen "karşılıksız yararlanma" suçunun unsurlarının oluştuğu, ancak TCK'nun 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 ey-leminin TCK'nun 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'nun 163/2. maddesinde yazılı cezanın karşılaştırılması suretiyle TCK'nun 44. maddesi de gözetilerek sonucuna göre sanığın hukuki durumunun belirlenmesi gerektiğinin gözetilmemesi, ... kanuna aykırı olup ..."* Yargıtay 11. Ceza Dairesi, 11.11.2013 2012 / 439 E., 2013 / 16403 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[274] *"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*

Kanaatimce, *"internet kafe ve play station salonu"* gibi yerlerde kullanılan sistemlerin hukuka aykırı bir şekilde kullanımı bu suç kapsamında değerlendirilemeyecek dolayısıyla da indirim sebebi olarak kabul edilemeyecektir. Nihayetinde bu gibi yerler kamuya açık yerler olup bilgisayarlara fiziken erişim herhangi bir suretle engellenmemektedir. Tek kaide bedelin ödenmesi suretiyle bilgisayarın kullanılmasıdır. Kaldı ki; hükmün amacının sanal ağa dahil olunarak bedel ödenen sistemleri korumak olduğu da gözetildiğinde failin *"internet kafe ve play station salonu"* gibi bir mekandaki fiziki bir kullanımının bu suç kapsamında değerlendirilmesi mümkün değildir. Failin fiili

---

... 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 ... kanuna aykırı olup" Yargıtay 19. Ceza Dairesi, 22.11.2017, 2015 / 2135 E., 2017 / 10023 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020); *"Katılanın tek yönlü olarak frekanslarla veya elektromanyetik dalgalar aracılığıyla yaptığı şifreli yayının sanık S.. T..'e ait uydu alıcısına (decoder) ulaş- ması üzerine gerekli donanım ve yazılım kullanılarak kartın şifre çözme kabiliyetinin internet ortamından paylaştırılması suretiyle şifreli yayınların sanık A.. A.. aracılığıyla başkaları tarafından şifresiz olarak izlenmesinin sağlandığı olayda, katılan tarafından kullanılan bilişim sistemine herhangi bir müdahalede bulunulmadığı anlaşıldığından eylemin, TCK.nun 163/2. maddesinde belirtili karşılıksız yararlanma suçunu oluşturduğu gözetilmeden, yazılı şekilde hüküm kurulması, ... yasaya aykırı olup"* Yargıtay 8. Ceza Dairesi, 07.07.2014, 2013 / 16698 E., 2014 / 17652 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

bu anlamda mahiyeti itibariyle karşılıksız yararlanma suçuna benzerlik göstermektedir ve kullanım olarak nitelendirilmelidir.

Doktrindeki bir kısım yazarlar ücreti, bedeli mukabilinde girilebilecek bir bilişim sisteminden, ücretli hizmetlerden faydalanmasının anlaşılması gerektiğini yani karşılığın mutlak suretle para olması gerektiğini savunmaktaysa da[275] hakim görüşe göre; bedelin para olması mutlak suretle beklenmemelidir. Sunulan hizmetin karşılığı olarak farklı taleplerde bulunulması, örneğin makale yollanmasının talep edilmesi yahut abone kazandırılmasının istenmesi gibi yöntemler kullanılması da mümkündür. Burada esas olan sisteme erişimin bir karşılığının olmasıdır.[276]

Yine suçun kanuni düzenlemesi bakımından isabetli olup olmadığı da doktrindeki bir başka tartışmalı husustur. İlk görüşe göre; suçun sistemler üzerinde işlenmesinin bir artırım nedeni olması gerekmektedir. Failin fiili sistem güvenliği ile malvarlığına ilişkin birden fazla hukuki değeri ihlal etmektedir ve bu nedenle de indirim sebebi şeklindeki düzenlenmesi hatalıdır.[277]

Karşıt görüş ise başka kullanıcılara hiçbir şekilde açılmayan sistemlerin bu tip sistemlere nazaran mahremiyetinin daha fazla olduğu, suçun konusu itibariyle konut

---

[275] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 449.

[276] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 816; DÜLGER, s. 375; KARAGÜLMEZ, s. 210; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 148; APAYDIN, s. 65.

[277] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 947; DÜLGER, s. 376-377; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 151.

dokunulmazlığını ihlal suçuyla benzerlik gösterdiği ve bu nedenle de daha fazla korunması gerektiği, düzenlemenin bu ihtiyacı gidermesi nedeniyle isabetli olduğu yönündedir.[278] Muhakkak ki; ticari bir gaye korunan bir sistem ile faile hiçbir suretle giriş izni verilmeyen bir sistemin korunması arasında bir fark bulunmaktadır. İlkinde korunan değer malvarlığına ilişkin ikincisinde ise bilişim sisteminin güvenliğinin yanı sıra özel hayattır. Dolayısıyla TCK'nın görece daha az tehlikeli olan bir halde indirim öngörmüş olması yerinde bir düzenleme olarak kabul edilmelidir.[279]

Suçun konusu temel itibariyle bilişim sisteminin güvenliği olmakla beraber aynı zamanda aynı zamanda verilerin güvenliğinin sağlanmasıdır. Bu anlamda özel hayatın ve kişisel verilerin korunması gibi değerler de suçun konusu kapsamında değerlendirilmelidir. Bedeli karşılığında yararlanılan sistemlerde sistemin koruma altına alınmasındaki amaç özel hayatın yahut kişisel verilerin korunması gibi amaçlar değil daha ziyade ticari endişelerdir. Bu nedenle de bedeli karşılığında yararlanılan sistemlere ilişkin fiilin, korunan değer de gözetildiğinde, bir indirim sebebi olarak düzenlenmesinde isabetsizlik olmadığı kanaatindeyim.

2. Ağırlaştırıcı Nedenler

[278] YAŞAR – GÖKCAN – ARTUÇ, s. 7298-7299; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 816; ARTUK – GÖKCEN YENİDÜNYA, s. 874; KARAGÜLMEZ, s. 211; Aynı görüş için bknz: APAYDIN, s. 66-67.

[279] DOĞAN, s. 80.

TCK'da *"Bilişim sistemine girme suçu"* kanuni düzenlemesinin üçüncü fıkrasında bu suçun neticesi sebebiyle ağırlaşmış hali *"bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur."* ifadeleriyle düzenleme altına alınmıştır.

Neticesi sebebiyle ağırlaşmış suç, failin bir suçun kanuni tanımında yer alan fiili icra ederken kastından daha ağır bir neticeyi gerçekleştirmesi halinde söz konusu olmaktadır. Yani ortaya çıkan ağır netice failin kastının dışında gerçekleşmiştir.[280]

Elbette ki; kanuni düzenlemede yer alan *"bu fiil"* ifadesiyle anlatılmak istenen bilişim sistemine girilmesi ve/veya bir süre orada kalınmasıdır. Birinci fıkrada bahsedilen fiilin gerçekleşmesi ve devamında sistemde bulunan verilerin yok olması veya değişmesi halinde fail üçüncü fıkra doğrultusunda cezalandırılmalıdır.[281]

TCK'nın 243. maddesinin gerekçesinde "*bu hükmün uygulanabilmesi için, verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir"* ifadelerine yer verilmiştir.

Verinin yok olmasından anlaşılması gereken, sistem üzerinde bulunan veriye artık ulaşılamaması verinin kaybolması yani tamamen silinmesidir. Verinin çöp kutusuna kaydolması veya başka bir şekilde yerinin değiştirilmesi verinin yok olması anlamına gelmez. Verinin değiştirilmesinden anlaşılması gereken ise verinin tamamen ortadan

[280] ÖZGENÇ, s. 280.

[281] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 449; ARTUK – GÖKCAN – YENİDÜNYA; s. 877.

kaldırılmadan içerindeki bilgilerin yenileriyle değiştirilmesi veya eskilerin ortadan kaldırılmasıdır.[282]

Failin bilişim sistemine taksirle erişim sağlaması halinde suçun temel hali oluşmayacaktır. Bu nedenle neticesi sebebiyle ağırlaşan suç bakımından failin sorumlu tutulabilmesi için suçun temel şekli için kasıtlı, ağırlaşan netice için en azından taksirle hareket etmesi gerekir.[283]

Doktrinde madde gerekçesini dikkate almayan ve suçun taksirli hali kanunda düzenlenmediğine dikkat çeken bir görüş suçun neticesi sebebiyle ağırlaşmış halinin ancak ve ancak kast ile işlenebileceğini ifade etmektedir. Yine bu görüşe göre failin eylemi hem TCK'nın 243/3. maddesinde düzenlenen hem de TCK'nın 244/2. maddesinde düzenlenen suçu birlikte oluşturacaktır.[284]

Ancak benim de katıldığım karşıt görüşe göre; failin fiilinin üçüncü fıkra kapsamında değerlendirilebilmesi için madde gerekçesinden de anlaşılacağı üzere kastının verileri yok etmek yahut değiştirmek olmaması gerekmektedir. Yani bu ağır neticeye yol açan failin taksirle hareket etmesi gerekir.[285] Aksi halde artık *"Bilişim*

[282] YAŞAR – GÖKCAN – ARTUÇ, s. 7298.

[283] APAYDIN, s. 71.

[284] KARAKEHYA, s. 205; Aynı görüş için bknz: ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949.

[285] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 817; ARTUK – GÖKCAN – YENİDÜNYA; s. 877; DÜLGER 384; GÜL, s. 68.

sistemine girme suçu" değil TCK'nın 244/2. fıkrasında yer alan *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu"* ortaya çıkacaktır.[286]

Ağırlaştırıcı nedenin uygulanması için sistem üzerinde hangi tür verilerin zarar gördüğünün bir önemi bulunmadığı gibi[287] üzerindeki verilerin zarar gördüğü sistemin bedeli karşılığında yararlanılabilen sistem olmasının da bu fıkra kapsamında bir ehemmiyeti bulunmamaktadır.[288]

Her ihtimalde failin ağırlaştırıcı nedenden sorumlu olması için, ortaya çıkan hal ile failin fiili arasında nedensellik bağının kurulabilmesi gerekmektedir.

G. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

1. Teşebbüs

[286] ARTUK – GÖKCAN – YENİDÜNYA; s. 877; DÜLGER, s. 370; KARAGÜLMEZ, s. 213; HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 450; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 817; AKBULUT, s. 149; Aynı görüş için bknz: YAŞAR – GÖKCAN – ARTUÇ, s. 7297.

[287] Ayrıntılı bilgi için bknz: KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 817; DOĞAN, s. 81.

[288] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 817.

Teşebbüs TCK'nın 35. maddesinde düzenlenmiş olup anılan hükme göre; fail bir suç işleme kastıyla suçu işlemeye elverişli hareketin icrasına başlamış ancak failin elinde olmayan nedenlerle hareketler tamamlanamamış ise suça teşebbüs söz konusudur.[289]

Bir başka deyişle failin icrasına başladığı ancak elinde olmayan sebeplerle tamamlayamadığı suçlara teşebbüs aşamasında kalmış suçlar denilmektedir. Teşebbüsün, ancak icra hareketine başlan an ile suçun tamamlandığı an arasında gerçekleşmesi mümkündür.[290]

"Bilişim sistemine girme suçu" sisteme girildiği anda tamamlanabilmekte olup bu yönüyle suç salt hareket suçudur. Bu nedenle suç teşkil eden fiil esnasında failin iradesine dayanmayan sebeplerle fiilin gerçekleşememesi mümkündür[291]. Bu halde suçun teşebbüs aşamasında kaldığının kabul edilmesi gerekmektedir.[292] Suçun ihmali hareketle işlendiği *"sistemde kalmaya devam edilmesi"* haline ise teşebbüs mümkün değildir[293].

[289] AKBULUT, Ceza Hukuku Genel Hükümler, s. 549.

[290] HAKERİ, 2019, s. 476.

[291] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 818; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949; ARTUK – GÖKCAN – YENİDÜNYA, s. 877.

[292] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 447; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 817; GÜL, s. 69; AKBULUT, s. 150.

[293] ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949; Bknz. AKBULUT, s. 151.

2. İştirak

Bir suçun kanuni tanımından ve suçun niteliğinden yola çıkarak bir suçun tek kişi tarafından işlenmesi mümkün olduğu halde birden fazla kişinin farklı yol ve yöntemlerle suça katılım sağlaması haline suça iştirak denilmektedir.[294] Daha kısa bir tanım ile iştirak; tek kişi ile işlenmesi mümkün olan bir suçun daha fazla kişi tarafından bir işbirliği halinde işlenmesidir[295].

Bu suç tek kişi tarafından işlenmesi mümkün olan bir suç olup bu suça iştirakin TCK'da yer alan genel hükümler doğrultusunda gerçekleştirilmesi mümkündür.[296]

3. İçtima

Şartların mevcut olması halinde, suçun zincirleme suç olarak işlenmesinde bir engel mevcut değildir. Yani fail bir bilişim sistemine birçok kez, farklı zamanlarda bir

[294] KOCA –ÜZÜLMEZ, Türk Ceza Hukuku Genel Hükümler, s. 431.

[295] HAKERİ, 2019, s. 527.

[296] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 447; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s 818; DÜLGER, s. 402; GÜL, s. 69; Aynı görüş için bknz: ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949

suç işleme kararının icrası kapsamında erişim sağlarsa zincirleme suç hükümleri uygulanabilecektir.[297]

Bununla beraber TCK'nın 243. maddesinde düzenlenen *"Bilişim Sistemine Girme"* suçu ile 244. maddesinde düzenlenen suçlar arasındaki ilişki bakımından doktrinde farklı görüşler mevcuttur. Doktrindeki bir görüş göre gerek bu iki suç arasındaki gerekse de bilişim sistemine girilmesi suretiyle işlenen diğer suçlarla *"Bilişim sistemine girme suçu"* arasındaki ilişkinin fikri içtima ilişkisi olduğunu ifade etmektedir[298].

Diğer görüş; *"Bilişim sistemine girme suçu"* ile *"Bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık", "Haberleşmenin gizliliğini ihlal", "Kişisel verilerin kaydedilmesi" "Verileri hukuk aykırı ele geçirme", "Özel hayatın gizliliğini ihlal", "Bilişim sistemlerinin kullanılması suretiyle hırsızlık"* gibi suçların farklı hukuki konuları olduğunu bu nedenle aralarında ancak ve ancak gerçek içtima uygulanabileceğini, TCK'nın 244/2. maddesinde yer alan *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* suçu ile hukuki konusunun aynı olması nedeniyle bu suçla arasında fikri içtima uygulanması gerektiğini savunmaktadır.[299]

---

[297] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 447; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 818; ARTUK – GÖKCAN – YENİDÜNYA; s. 878; Aynı görüş için bknz: ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 949; DÜLGER, s. 402.

[298] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 819; DÜLGER, s. 405; ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 171; AKBULUT, s. 152.

[299] APAYDIN, s. 90.

Bir diğer görüşe göre *"Bilişim sistemine girme"* suçu ile daha sonra işlenen *"Sistemi engelleme, bozma, verileri yok etme veya değiştirme"*, *"Bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık", "Haberleşmenin gizliliğini ihlal"* vb. diğer bütün suçlar arasında geçitli suç ilişkisi bulunduğundan failin yalnızca amaçladığı suç yönünden cezalandırılması gerekmektedir.[300] Nitekim Yargıtay da vermiş olduğu bir kararında kişilere ait banka hesaplarına internet bankacılığı vasıtasıyla hukuka aykırı olarak erişim sağlanması ve bu şekilde hesaplarından yine hukuka aykırı para transferleri gerçekleştirilmesi eylemlerini bu suç kapsamında değil hırsızlık suçu kapsamında değerlendirmektedir[301]. Kişilere ait bilişim sistemlerine erişim sağlayarak kontör gibi taşınır mal sayılmayan bir şeyin transferi ise Yargıtay tarafından ne bu suç kapsamında ne de hırsızlık suçu kapsamında değerlendirilmemekte, eylemin TCK'nın 244. maddesi kapsamında kaldığı kabul edilmektedir[302]. Yargıtay başka diğer kararlarında bir bilişim

---

[300] ARTUK – GÖKCAN – YENİDÜNYA; s. 878.

[301] *"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… kanuna aykırı olup …"* Yargıtay 13. Ceza Dairesi, 18.12.2014, 2014 / 2924 E., 2014 / 36282 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[302] *"Sanığın mağdura ait süper şifresini öğrenip internet vasıtasıyla Türkcell'den üçüncü bir kişinin GSM hesabına ordan da kendi GSM hesabına yâni cep telefonuna 68 adet kontür transferi yaptığı hususunda bir tereddüt yoktur. Somut olayda nitelikli hırsızlık suçunun maddi unsurlarından olan konu ve fiil unsurları oluşmamıştır. Çünki; Kontür, ekonomik bir değer ifade etmekte ise de; taşınır bir mal değildir. Bilgisayar ortamından*

sistemine girilerek sistemin şifresinin değiştirilmesi eylemine ilişkin olarak yaptığı incelemede, TCK'nın 243/1 maddesinde düzenlenen suçun değil 244/2 maddesinde düzenlenen suçun ortaya çıktığını ifade etmiş ve bu suretle de anılan suçlar arasında gerçek veya fikri içtima ilişkisi kurulamayacağını, failin amaçladığı suç yönünden cezalandırılması gerektiğini dolaylı olarak ortaya koymuştur[303].

---

temin edilen kontür, sahibine belirli süreler için telefonda görüşme yapma hakkı sağlayan bir veridir. Üstelik bulunduğu yerden fiziken de alınmış değildir. Buna karşılık sanığın işlemiş olduğu fiil; TCK'nın 244. maddesinin 2. fıkrasında düzenlenen seçimlik hareketlerden olan 'varolan verileri başka bir yere'" göndermek olup, aynı Kanun'un 4. fıkrasında belirtilen 'haksız bir çıkar sağlama' söz konusu olduğu için TCK'nın 244. maddesinin 4. fıkrasında düzenlenen bilişim suçunu oluşturmaktadır." YCGK, 25.11.2014, 2013 / 13-448 E., 2014 / 524 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[303] *"sanığın savunmasında belirttiği hususların katılana sorulması, suç tarihinden şikayet tarihine kadar olan dönemde, bu adresin faal olup olmadığı, katılan tarafından kendi adresine erişim sağlanıp sağlanmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlandığı ilgili internet sağlayıcısından ve Facebook şirketinden sorulması, gerektiğinde bilirkişiden de görüş alındıktan sonra tüm deliller birlikte değerlendirilip sonucuna göre katılana ait Facebook adresinin şifresinin değiştirilmesi halinde eylemin TCK.nın 244/2. maddesinden tanımlanan suçu oluşturacağı da dikkate alınarak sanığın hukuki durumunun takdir ve tayini gerekirken, eksik araştırma ile yazılı şekilde hüküm kurulması, yasaya aykırı…"* Yargıtay 8. Ceza Dairesi, 10.02.2020, 2018 / 11204, 2020 / 9307 K. Sayılı Karar, Yayımlanmamış Karar; *"Sanığın katılan ...'in hesaplarının şifresini ele geçirip, ardından şifreleri değiştirmesi şeklindeki eylemi ile şikayetçi ...'dan para istemesi eyleminin iki ayrı*

Doktrindeki bir diğer görüşe göreyse; *"Bilişim sistemine girme suçu"* bilişim suçu olarak adlandırılan yahut bilişim sistemleri kullanılarak işlenen suçlar bakımından bir geçitli suç niteliğindedir. Yani amaç suçun işlenebilmesi için failin öncelikle *"bilişim sistemine girme"*si gerekir. Ancak araç suç olan bilişim sistemine hukuka aykırı olarak erişim sağlama eylemi *"Bilişim sistemi aracılığıyla gerçekleştirilen dolandırıcılık", "Haberleşmenin gizliliğini ihlal", "Kişisel verilerin kaydedilmesi" "Verileri hukuk aykırı ele geçirme", "Özel hayatın gizliliğini ihlal", "Bilişim sistemlerinin kullanılması suretiyle hırsızlık", "Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* gibi suçlar bakımından icra hareketi olarak kabul edilmemektedir. Bu nedenle de failin hem *"Bilişim sistemine girme suçu"*ndan hem de faili olduğu diğer suçtan ayrı ayrı cezalandırılması gerekir.[304] Yani bu görüşe göre failin *"bilişim sistemine girme"* fiilinin hukuka aykırı olduğu bilincinde olması ve *"Bilişim sistemine girme suçu"*nu doğrudan kastla işlemesi halinde fail amaç ve araç suç bakımından gerçek içtima kuralları uyarınca cezalandırılmalıdır. Yargıtay da bir kararında bir bilişim sistemine girilmesi ve bu sistem

---

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 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, ... kanuna aykırı olup ..." Yargıtay 15. Ceza Dairesi, 02.02.2015, 2014 / 15082 E., 2015 / 1624 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[304] DOĞAN, s. 98-100; PARLAR, s. 21.

üzerinden elde edilen fotoğrafların yayılmasında fikri içtima uygulanamayacağını, iki ayrı suçun oluştuğunun kabulü gerektiğini ifade etmiştir[305]. Bir başka kararında ise sanıkların, mağdura ait MSN adresine hukuka aykırı olarak erişim sağlayıp burada yer alan tarafı olmadıkları konuşmaları kaydettiği olayda *"Haberleşmenin gizliliğini ihlal"* ve *"Bilişim sistemine girme suçları"*nın ayrı ayrı oluştuğunu kabul etmiştir[306]. Yine

---

[305] *"Sanık hakkında düzenlenen iddianamede; sanığın, mağdura ait facebook ve telefon hesaplarına rızası dışında girerek bilişim sistemine girme, mağdurun orijinal fotoğrafları ile birlikte çıplaklık içeren fotoğrafları mağdura aitmiş gibi internette paylaşarak görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçlarını işlediği iddia edilmiş olup, sanığa yüklenen farklı eylemlerden dolayı ayrı ayrı hüküm kurulması gerektiği, TCK'nın 44/1. madde ve fıkrasındaki fikri içtima koşullarının bulunmadığı gözetilmeden, "bilişim sistemlerine girme ve özel hayatın gizliliğini ihlal suçlarının sabit olmakla birlikte tek bir eylem ile icra edildiğinden TCK'nın 44. maddesinin bu suçlar yönünden tatbik edilmesine" biçimindeki yasal ve yeterli olmayan gerekçelerle yazılı şekilde görüntü veya seslerin ifşa edilmesi suretiyle özel hayatın gizliliğini ihlal suçundan mahkumiyet hükmü kurulması, ... kanuna aykırı olup ..."* Yargıtay 12. Ceza Dairesi, 29.05.2019, 2018 / 8261 E., 2019 / 6852 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[306] *"Sanık Mehmet'in, mağdura ait MSN adresine izinsizce giriş yapıp, burada kayıtlı olan mağdurun elektronik iletilerini ele geçirerek, bu elektronik iletileri, mağdurun işten çıkarılmasına gerekçe olarak kullandıkları olayda, 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*

Yargıtay bir başka kararında sanığın, hesap sahibinin şifresini değiştirip değiştirmediğinin tespit edilmesini ve buna göre TCK'nın 243. maddesinin değerlendirilmesi gerektiğini vurgulamıştır[307].

Yargıtay'ın doktrindeki birden fazla görüşe uygun kararlar verdiği görülmektedir. Esasen Yargıtay'ın somut olaya göre failin amacını yorumladığı, icra hareketlerinin başlangıcını değerlendirdiği, geçitli suç ilişkisini incelediği ve daha sonra cezalandırmayı somut olayın koşullarına göre tayin ettiği açıktır. Bu yaklaşım kanaatimce daha doğru olacaktır. Nitekim bu suçun kanuni tanımında *"hukuka aykırı olarak"* ibaresine yer verilerek suçun doğrudan kastla işlenebileceği öngörüldüğünden failin hukuka aykırı

---

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,, kanuna aykırı olup …" Yargıtay 12. Ceza Dairesi, 02.02.2015, 2014 / 15082 E., 2015 / 1624 K. Sayılı Karar, www.kazanci.com.tr (E. T. 24.03.2020).

[307] *"Sanık tarafından suç tarihinden sonra giriş yapılıp yapılmadığı, adrese ait şifrenin değiştirilip değiştirilmediği, şifre değiştirilmişse hangi tarihte ve hangi IP numarası ile erişim sağlanarak şifrenin değiştirildiği ilgili internet sağlayıcısından sorulması sonucuna göre tüm deliller birlikte değerlendirilip gerektiğinde bilirkişiden de görüş alınıp şifre değişikliği gerçekleşmediği takdirde eylemin TCK.nın 243. maddesi kapsamında değerlendirilmesi gerektiği dikkate alınarak sanığın hukuki durumunun takdir ve tayini gerekirken eksik araştırmaya dayanarak yazılı şekilde hüküm kurulması yasaya aykırı olup …"* Yargıtay 8. Ceza Dairesi, 06.05.2019, 2017 / 24009 E., 2019 / 6266 K. Sayılı Karar, Yayımlanmamış Karar.

hareket ettiği sabit olmadıkça, ispatlanmadıkça bu suç oluşmayacaktır[308]. Bu nedenle failin somut olaydaki kastının olası kast ile doğrudan kast ayrımı çerçevesinde incelenmesi ve bu doğrultuda hangi suç veya suçlardan hüküm kurulacağının belirlenmesi hukuken daha isabetlidir. Failin hem bilişim sistemine hukuka aykırı olduğu bilinciyle erişim sağlaması hem de bu yolla bir başka suçu işlemesi halinde failin gerçek içtima kuralları uyarınca cezalandırılması gerekmektedir. Failin kastının doğrudan kast dışında kalması yani olası kast veya taksir olması halinde yalnızca amaçladığı suç yönünden cezalandırılması uygun olacaktır. Bu halde araç suç olan *"Bilişim sistemine girme suçu"* bakımından ise suçun manevi unsuru oluşmadığı açık olduğundan fail bu suçtan cezalandırılamayacaktır.

H. YAPTIRIM

Kanun ile düzenlenen bir hükmün ihlal edilmesi halinde faile çektirilen uygulanan acıya ceza veya yaptırım denilmektedir[309]. TCK'da yer alan *"Bilişim sistemine girme suçu"* işleyen faile yaptırım olarak*" bir yıla kadar hapis veya adli para cezası"* belirlenmiştir. Yani kanuni düzenlemede bir seçimlik ceza öngörülmesi hali mevcuttur. Seçimlik cezalardan hangisi doğrultusunda hüküm kuracağı TCK'nın 61/1. maddesini de gözetmesi gereken hakimin takdirindedir.[310]

---

[308] APAYDIN, s. 77.

[309] YALÇIN – KÖPRÜLÜ, s. 611.

[310] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 819.

Bununla beraber yaptırımın suçun kanuni düzenlemesinde yer alan hükümler doğrultusunda arttırılması yahut hafifletilmesi de mümkündür.

Bu suç bakımından bir alt sınır öngörülmemiştir. Bilindiği üzere hapis cezası bakımından bu hallerde TCK'nın 49. maddesi uygulama alanı bulacağından hapis cezasının alt sınırı bir ay olarak kabul edilmelidir. Yine adli para cezasının uygulanmasındaysa ise TCK'nın 52, 61/8 ve 9. maddeleri dikkate alınarak hüküm kurulmalıdır.[311]

TCK'nın 246. maddesinde yer alan *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* İfadesine yer verilmek suretiyle hukuka aykırı yarar sağlayan tüzel kişilerin de bu suçlara uygulanacak yaptırımlar kapsamında güvenlik tedbiri ile karşı karşıya kalacağı açıkça ifade edilmiştir[312].

Yine belirtmek gerekir ki; şartların oluşması halinde TCK'nın 54 ve 55. maddeleri uyarınca eşya ve kazanç müsaderesine ilişkin hükümler de uygulanabilecektir.[313]

Ayrıca TMK'nın 4. maddesinde sayılan suçlardan bu suçun, bir terör örgütü faaliyeti kapsamında işlenmesi halinde terör suçu sayılması ve aynı kanunun 5. maddesi uyarınca arttırılması mümkündür.

---

[311] HAFIZOĞLLARI - ÖZEN, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, s. 448.

[312] DÜLGER, s. 408; AKBULUT, s. 155.

[313] ERDOĞAN, Türk Ceza Kanunu'nda Bilişim Suçları, s. 177.

TCK'da bu suç bakımından özel bir zamanaşımı süresi öngörülmediğinden TCK'nın 66. maddesinde düzenlenen genel zamanaşımı süreleri uyarınca bu suç bakımından dava zamanaşımı süresi sekiz yıldır.

I. SORUŞTURMA VE KOVUŞTURMA

Kanunda bu suçun şikayete bağlı olduğuna ilişkin herhangi bir düzenleme yer almadığından bu suçun soruşturulması ve kovuşturulması re'sen yürütülmektedir.[314]

Mahkemelerin görev ve yetkilerini düzenleyen *"5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemeleri'nin Kuruluş Görev ve Yetkileri Hakkında Kanun"* 'un 11. maddesine göre bu suçun hem basit hali hem de nitelikli hali bakımından görevli mahkeme ise asliye ceza mahkemesidir. [315]

Suç tarihi, failin *"Bilişim sistemine girme suçu"* bakımından sisteme girdiği andır. Sistemde hukuka aykırı olarak kalmaya devam etme halindeyse failin sistemden çıkış yaptığı ya da çıkartıldığı andır.[316]

Yetkili mahkeme CMK'nın yetkiye ilişkin hükümleri uyarınca tespit edilecektir. CMK'nın 12. maddesi uyarınca suçun işlendiği yer mahkemesi yetkili mahkeme olarak kabul edilmelidir. Suçun işlendiği yerin tespiti hususunda ise TCK'nın 8. maddesi

[314] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 819; ÖZBEK – DOĞAN – BACAKSIZ – TEPE, s. 950.

[315] DÜLGER, s. 408; GÜL, s. 70-77.

[316] ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 333.

gözetilmelidir. [317] Anılan hükme ve TCK'nın benimsediği yaklaşıma göre hareketin kısmen veya tamamen icra edildiği, hareketin devam ettiği yer yahut neticenin gerçekleştiği, sonucun ortaya çıktığı yer suçun işlendiği yer olarak kabul edilmelidir[318].

Yetkili mahkemenin tespitine ilişkin Yargıtay vermiş olduğu bir kararında failin sisteme girdiği sırada bulunduğu yerin yetkili mahkeme olduğuna karar vermiştir.[319]

Özellikle teknolojik araçlar vasıtasıyla işlenen suçların karşımıza pratikte mesafe suçu olarak çıkması mümkündür. Örneğin internet üzerinden iletişim kurma imkanı sağlayan bir yazılım aracılığıyla hakaret suçunun işlenmesi halinde hakaret edenin veya hakaret edilenin bulunduğu yerin Türkiye olması halinde ülkesellik kuralı uyarınca suç yeri Türkiye olacaktır.[320] Aynı örnek üzerinden *"Bilişim sistemine girme suçu"*nun da bir mesafe suçu olduğu açık olup hem sisteme giren kişinin bulunduğu yer hem de hedef sistemin bulunduğu yerin suç yeri olduğu kabul edilmelidir.

---

[317] AKBULUT, s. 156.

[318] İÇEL, s. 156; YALÇIN – KÖPRÜLÜ, s. 108.

[319] *"Suç, failin işlemi yaparken kullanmış olduğu bilgisayarın IP adresinin bulunduğu yerde işlenmiş olduğundan bu yer mahkemesinin yetkili olduğuna karar vermiştir."* Yargıtay 5. Ceza Dairesi, 2019 / 5729 E., 2019 / 7810 K. Sayılı ve Yargıtay 5. Ceza Dairesi 2019 / 5278 E., 2019 / 7008 K. Sayılı Kararları, Bknz: ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 333.

[320] Erdem İzzet **KÜLÇÜR**, Ceza Hukukunda Yer Bakımında Uygulama, B. 1, Onikilevha Yay., İstanbul 2017, s. 183.

"Bilişim sistemine girme suçu" bakımından hareketin gerçekleştiği yerin failin bulunduğu yer olarak kabul edilmesi gerekmektedir. Bunun yanı sıra hareketin eş zamanlı olarak ortaya çıktığı yer mahkemesi de yetkili sayılacağından erişim sağlanmak istenen sistemin bulunduğu yer mahkemesi de yetkili mahkeme olarak kabul edilmelidir. Bu nedenle de failin yahut yetkisiz erişim sağlanmak istenen sistemin Türkiye'de olması halinde Türk Mahkemeleri'nin yetkili olacağı tartışmasızdır. [321]

[321] AKBULUT, s. 156; Aynı görüş için bknz: ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 333.

II. BİLİŞİM SİSTEMLERİ İÇİNDEKİ VEYA ARASINDAKİ VERİ NAKİLLERİNİ İZLEME SUÇUNA DAİR İNCELEMELER

A. GENEL OLARAK

"Bilişim sistemine girme suçu", TCK'nın ikinci kitap üçüncü kısmında *"Topluma Karşı Suçlar"* bölümünde altında *"Bilişim Alanında Suçlar"* başlığı altında 2016 yılında çıkan 6698 Sayılı Kanun ile 243. maddede 4. fıkra olarak düzenleme altına almıştır. Kanunda yer alan düzenleme;

"Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır." şeklindedir.

2005 yılında yürürlüğe giren 5237 Sayılı TCK esasen 3 fıkradan oluşmaktaydı. Yani 4. fıkra ile düzenlenen *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini İzleme Suçu"* 2005 yılında yürürlüğe giren kanunda yer almamaktaydı. Anılan suç tipi 24.03.2016 tarihinde 6698 Sayılı Kanun ile ayrı ve bağımsız bir suç tipi olarak düzenleme altına alınmıştır.

Kanuni düzenlemenin gerekçesinde *"Verilerin izlenmesi eylemi, bilişim sistemlerine herhangi bir müdahalede bulunmaksızın teknik araçlarla bilişim sistemleri arasındaki veri nakillerinin takip edilmesini ifade etmektedir. Bütün elektronik veri transferleri, bu çerçevede korunması amaçlanan veri transferinin gizliliği kapsamında kalmaktadır. Yasadışı araya girme eylemleri, temelde bilişim sistemlerine girilmeksizin işlenen fiillerdendir. Bu doğrultuda Sözleşmeye uyum amacıyla yine aynı maddenin*

birinci fıkrasına hüküm eklemek suretiyle, bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla izleyen kişinin ... cezalandırılması öngörülmüştür." İfadelerine yer verilmiştir.[322]

TCK'nın 243. maddesinin ilk üç fıkrasında düzenlenen *"Bilişim sistemine girme suçu"*nun ortaya çıkabilmesi için sisteme yetkisiz erişim sağlanması gerekmektedir. Oysa teknolojik imkanlar ve bilişim alanındaki yenilikler artık sisteme herhangi bir şekilde erişim sağlanmaksızın da sistem içerisindeki verilere ulaşma yahut birden fazla sistem arasındaki veri akışını izleme imkanı sağlamaktadır. Bu nedenle kanun koyucu bilişim sistemine erişim sağlanmaksızın yapılan veri aktarımı izleme eylemi bakımından da cezai yaptırım uygulanabilmesi ihtiyacını giderebilmek ve AKSSS'ye uyum süreci kapsamında yükümlülüklerini yerine getirebilmek maksadıyla 2016 yılında yeni bir düzenleme getirmiştir.[323]

Esasen Sözleşme metninde *"Yasadışı Araya Girme"* başlıklı 3. maddeyle sözleşmeye taraf devletlere *"bilgisayar verileri taşıyan bir bilgisayar sisteminde elektromanyetik dalgalarla yayılma da dahil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman kendi iç hukuku ile suç olarak tanımlama"* yükümlülüğü getirilmiştir. Her ne kadar Sözleşmenin getirdiği yükümlülüklerin yerine getirilmesi maksadıyla da kanun koyucu bu suç tipini

---

[322] https://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?psira=122834&r_afr windowmode=0&_afrloop=8353709187264943&_adf.ctrl-state=17c8e6wa3h_9 (E.T. 12.04.2020)

[323] TEZCAN –ERDEM –ÖNOK, s. 951.

düzenlemişse de TCK 243/4'te yer alan hüküm ile Sözleşmenin getirdiği yükümlülük karşılaştırıldığında; TCK'nın 243/4. maddesinde yer alan düzenlemede *"verilerin izlenmesi"*, Sözleşme metnindeyse *"araya girme"* ifadelerinin kullanıldığı görülecektir. Yine Sözleşmede *"umuma kapalı olarak iletilmesini ve sisteme girmeksizin izlenmesini"* koşul olarak ararken TCK'da böyle bir koşul yer almamaktadır. Bir diğer farklılık ise TCK'da, Sözleşme'de yer alan elektromanyetik dalgalara ilişkin bir ifade bulunmamasıdır. Bu hususlar dışında Sözleşme ile TCK'da yer alan ifadeler büyük oranda paraleldir.[324]

Elbette, sistem üzerinde yetkisiz erişim sağlanmadan da koşulların varlığı halinde TCK'nın 135 vd. hükümleri yahut 132. madde hükmü uygulama alanı bulacaktır. Ancak sistem içerisindeki veriler her zaman kişisel veri niteliğinde olmayabilir. Bunun yanı sıra bir verinin herhangi bir kaydının alınmayarak yalnızca *"izlenmesi"*, *"ele geçirme"* olarak nitelendirilemeyecektir. Bu nedenle anılan kanuni düzenlemeler yeterli olarak değerlendirilemeyecektir. Kanun koyucu da bu eksikliği gidermek maksadıyla 243. maddeye 4. fıkrayı eklemiştir.[325]

B. HUKUKİ KONU

Doktrinde suçun hukuki konusunda farklı görüşler mevcuttur. Bu görüşlerden ilkine göre; Anayasa'nın 22. maddesi uyarınca haberleşme gizliliği anayasal bir haktır. Kanunun hukuki konusu kamuya açık olmayan ve gizliliğinin korunması anayasal bir hak

[324] SOKULLU AKINCI, s. 14; AKBULUT, s. 158.

[325] AKBULUT, s. 158; TEZCAN – ERDEM – ÖNOK, s. 945

olan veri iletişiminin gizliliğinin sağlanmasıdır. Kişiler, başkaları tarafından izlenmeden, gözlenmeden veri aktarımını güvenli olarak sağlayabilmelidir. Yani kişilerin veri aktarımının gizliliğindeki menfaati korunmaktadır.[326] Yine bu görüşe paralel bir görüşe sahip yazarlar da hukuki konunun veri iletişimin gizliliğinin korunması olduğunu kabul etmektedir[327].

Bir diğer görüşe göreyse; suç her ne kadar bilişim suçları arasında düzenlenmişse de suç bilişim sisteminin güvenliğinin yanı sıra özel alanın mahremiyetini de korumaktadır[328].

Bu suçun hukuki konusunun birden fazla olduğunu kabul etmekte yarar olduğu kanaatiyle, hukuki konuların bilişim sisteminin güvenliği ve veri gizliliğinin sağlanması olduğu açıktır. Veri gizliliğinin sağlanması, bilişim sisteminin güvenliğinin sağlanmasından geçmektedir. Veri gizliliğinin ihlali kullanıcılarda aynı zamanda bilişim sistemine güvenin azalması anlamına da gelmektedir. Özel hayatın gizliliğinin korunmasıysa kanaatimce suçun düzenlendiği yer ve özel hayata ilişkin ayrıca koruma sağlayan kanun hükümleri olması gibi hususlar da gözetildiğinde ancak ikincil bir konu olarak kabul edilmelidir.

---

[326] AKBULUT, s. 159

[327] KOCA –ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s.821.

[328] TEZCAN – ERDEM – ÖNOK, s. 952; Hasan Burak **ÖNDİN**, Türk Hukukunda Doğrudan Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, ANDÜ SBE, Eskişehir 2017, s. 47.

C. FAİL

5237 Sayılı TCK'nın 243. maddesinde 4. fıkrada "*Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi"* denilerek kanuni düzenlemede suçun faili olmak için herhangi bir özellik aranmamıştır. Bu nedenle de herkes suçun faili olabilir.[329]

Kanuni düzenlemede bahsedilen suçun bir tüzel kişi tarafından işlenmesi mümkün değildir. Ancak bu suç ile tüzel kişi haksız bir şekilde menfaat sağlamış ise TCK'nın 246. maddesi uyarınca tüzel kişi hakkında tüzel kişilere özgü güvenlik tedbiri uygulanmasına karar verilebilir.[330]

D. MAĞDUR

Bu suçun mağduru iletilen verinin sahibi olan kişidir[331]. Şayet veriler tüzel kişiye aitse bu halde tüzel kişinin sahibi yahut ortakları olan gerçek kişiler suçun mağduru, tüzel

[329] TEZCAN – ERDEM – ÖNOK, s. 952; AKBULUT, s. 159; KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 821.

[330] TEZCAN – ERDEM – ÖNOK, s. 952

[331] TEZCAN – ERDEM – ÖNOK, s. 952

kişi ise suçtan zarar görendir. Ancak veri bir devlet kuruluşuna ait ise, toplumun tamamı bu suçun mağduru olarak kabul edilmelidir.[332]

Doktrinde veri sahibini, nakledilen veriler üzerinde tasarruf yetkisine sahip olan kişi olduğunu olarak tanımlayan bir görüş mevcuttur. Bu görüşe göre verilerin alıcı için hazırlanmış ve alıcı tarafından bu veriler çağrılmışsa yetkili ve mağdurun artık alıcı olduğu kabul edilmelidir. Ancak veriler kişiye başkası tarafından gönderilmişse veriler alıcıya ulaşana kadar yetkili kişi gönderici olacağından bu kez mağdur gönderici olacaktır.[333]

Bir diğer görüşe göreyse, mağdur teknik araçlar kullanılarak veri trafiği izlenen bilişim sistemleri üzerinde tasarruf yetkisi bulunan kişi veya kişilerdir.[334]

Kanaatimce, suçun konusu değerlendirildiğinde hem göndericinin hem de alıcının birlikte bu suçun mağduru olarak kabul edilmesi mümkündür. Örneğin karşılıklı e-posta göndermek suretiyle yapılan bir yazışmanın izlenmesinde hem göndericinin hem de alıcının karşılıklı olarak bir trafiği içerisinde olduğu dolayısıyla da veri sahibi olduğu ve suçun mağduru olduğu açıktır. Taraflardan birisi veri trafiğinin göndericisi diğeriyse alıcısıdır. Yani izlenen veri trafiği her iki tarafın veri akışını göstermektedir. Dolayısıyla veri sahibini yalnızca veri üzerindeki tasarruf yetkilisi olarak değerlendirmek doğru olmayacaktır. Buradan yola çıkarak da hem gönderici hem de alıcının yani bilişim sistemlerinin her iki tarafının tasarruf yetkilisinin de mağdur olarak kabul edilmesi gerekmektedir.

---

[332] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 821.

[333] AKBULUT, s. 160.

[334] ÖNDİN, Türk Hukukunda Doğrudan Bilişim Suçları, s. 49.

E. BİLİŞİM SİSTEMLERİ İÇİNDEKİ VEYA ARASINDAKİ VERİ AKTARIMINI İZLEME SUÇUNUN UNSURLARI

1. Fiil

5237 Sayılı TCK'nın 243. maddesinde 4. fıkrasında fiil "*veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek"* şeklinde düzenlenmiştir. Yani bu suçun maddi unsuru sisteme erişim sağlanmadan hukuka aykırı olarak veri nakillerinin teknik araçlarla izlenmesidir.

TDK'nın güncel sözlüğüne göre suçun unsuru olan *"izlemek", "görmek, öğrenmek için bakmak, seyretmek, gözlemek, incelemek, herhangi bir olayla ilgilenmek"* anlamlarına gelmektedir[335].

Veri nakillerini izlemek ise; ağlar vasıtasıyla aktarılan verilere ait trafiği takip etmek anlamına gelmektedir[336].Yine *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* 'un *"Tanımlar"* başlıklı 2. maddesinde *"İzleme: İnternet ortamındaki verilere etki etmeksizin bilgi ve verilerin takip edilmesi"* şeklinde tanımlanmıştır.

Suçun maddi unsurunun gerçekleşebilmesi için izlemenin teknik araçlarla yapılması gerekmektedir. Fail, teknik araç kullandığı sürece izlemenin hangi yol veya

[335] TDK. https://sozluk.gov.tr/ (E. T. 24.03.2020)

[336] AKBULUT, s. 164.

yöntemle yahut hangi teknik araçla yapıldığının bir önemi yoktur. Önemli olan kullanılan teknik araçla izlemenin mümkün olması ve gerçekleştirilmesidir. Dolayısıyla teknik araç kullanılmadan yapılan çıplak gözle bakma, uzaktan seyretme gibi izlemeler bu suçu oluşturmayacaktır.[337] Teknik araç ise; veri trafiğini izleme imkanı sağlayan her tür teknik cihazı kapsamaktadır.[338]

Verilerin aktarımı içini kullanılan teknik yöntem, telefon, faks, e-posta, internet telefonu olabilir. Hangi yöntemin kullanıldığı suçun unsurları bakımından bir önem arz etmemektedir. Yine yalnızca bilgisayar ve yazıcı arasındaki küçük ölçekli ağların izlenmesi de bu suç kapsamında değerlendirilmelidir. Ancak AKSSS'nin aksine kanunumuzda elektromanyetik dalgaların izlenmesi bir suç olarak düzenlenmediğinden örneğin bilgisayardan monitör yahut klavyeye gönderilen sinyallerin izlenmesi bu suç kapsamında değerlendirilemeyecektir.[339]

Yine bu suçun oluşmasının bir diğer koşulu, veri aktarımının bir ağ yahut bilişim sistemi üzerinden izlenmesidir. Örneğin CD veya harici bellek gibi sistemler kullanılarak da veri aktarımı söz konusu olabilir. Ancak bu tür aktarımlar bir ağ yahut bilişim sistemi üzerinden aktarım olmadığından bu suç kapsamında bir fiil söz konusu olmayacaktır.[340]

Bir başka önemli husus da failin eylemini bilişim sistemine erişim sağlamadan gerçekleştirmesidir. Yani veri göndericiden çıktıktan sonra ancak alıcıya ulaşmadan önce

[337] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822.

[338] AKBULUT, s. 166.

[339] AKBULUT, s. 162.

[340] TEZCAN – ERDEM – ÖNOK, s. 952.

yani gönderim işleminin devam etmesi sırasında izleme gerçekleştirilmelidir.[341] Veri aktarım süreci başlamamışsa yahut süreç tamamlanmışsa bu suç oluşmayacaktır[342]. Şayet fail tarafından sisteme yetkisiz erişim sağlamak yahut sistemde hukuka aykırı olarak kalmaya devam etmek suretiyle veri izleniyorsa bu halde artık *"Bilişim sistemine girme suçu"*nun ortaya çıktığı kabul edilmelidir.[343]

Yine veri trafiğinin izlenmesinin herhangi bir şekilde trafiği izlenen kişilere ait internet hattına da girilmeksizin gerçekleştirilmesi gerekir. Aksi halde artık bu suç oluşmayacaktır.[344]

Doktrinde verinin gönderim işleminde verinin alıcının arabelleğine alındığı yahut server sistemine girdiğinde beklediği zaman diliminde suçun oluşup oluşmayacağı yönünde bir tartışma mevcuttur. Burada veri aktarım sürecinin bitip bitmediği değerlendirilmelidir. Bir görüşe göre; aktarım tamamlanmış ve süreç nihayete ermiştir. Bu nedenle arabellek yahut server sisteminde gerçekleşen bekleme sürecinde bu suçun oluşması mümkün değildir. Karşı görüşe göreyse; aktarım henüz nihayete ermemiş, süreç devam ettiğinden bu zaman diliminde yapılacak hukuka aykırı izlemenin de bu suçu oluşturacaktır.[345]

Kanaatimce verinin aktarım sırasında izlenmesi esas olduğundan ister arabelleğe ister server sistemine veri girişi tamamlandığı anda süreç tamamlanmıştır ve artık verinin

---

[341] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822.

[342] AKBULUT, s. 160.

[343] TEZCAN – ERDEM – ÖNOK, s. 952

[344] AKBULUT, s. 165.

[345] Ayrınılı bilgi için bknz: AKBULUT, s. 161.

aktarımından bahsedilmesi mümkün değildir. Çünkü veri trafiğinin varış noktası olan ana sunucuyu alıcının evi olarak kabul edecek olursak arabellek yahut server evin bahçesi olarak kabul edilmelidir. Yani arabellek yahut server sistemi alıcının müdahale edebileceği, tasarrufun tamamen alıcıda olduğu bilişim sisteminin ayrılmaz bir parçasıdır ve veri buraya ulaştığında alıcının tasarruf alanına girmiştir.

Doktrindeki bir görüşe göre fail, gönderim işlemi sırasında veriyi izlerken veriye herhangi bir şekilde müdahale etmemeli, yönlendirmemeli, değiştirmemeli, bozmamalı yahut bütünlüğüne müdahale etmemelidir. En önemlisi içeriğini öğrenmemelidir. Aksi halde failin fiili *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Aktarımını İzleme Suçu"* olmaktan çıkacak, *"Haberleşmenin Engellenmesi"* veya *"Haberleşmenin Gizliliğini İhlal"* gibi suçlara vücut verecektir.[346]

Doktrinde içeriğin öğrenilmesine ilişkin olarak farklı bir görüş de mevcuttur. Bu görüşe göre; bu suçun oluşması için içeriğin öğrenilip öğrenilmemesinin bir önem arz etmemektedir, her halde bu suç ortaya çıkmaktadır.[347] Ancak failin izleme sırasında içeriğe vakıf olması halinde bu suçla beraber *"Haberleşmenin Engellenmesi"*, *"Haberleşmenin Gizliliğini İhlal", "Özel Hayatın Gizliliğini İhlal"* veya *"Verilerin Hukuka Aykırı Ele Geçirilmesi"* gibi suçlar ortaya çıkacaktır[348].

Kanaatimce, *"Bilişim sistemine girme suçu"* bakımından yapılan yorumlar bu suç bakımından da geçerlidir. Veri trafiğinin izlenmesi eylemi diğer suçlar bakımından icra hareketini başlatan eylemler değildir. Burada failin amaç suç ve araç suçlar bakımından

[346] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822.

[347] TEZCAN – ERDEM – ÖNOK, s. 952; AKBULUT, s. 165.

[348] Bknz: AKBULUT, s. 165; ÖZBEK – KANBUR – BACAKSIZ – TEPE, s. 938

kastları değerlendirilmeli ve somut olaya göre karar verilmelidir. Ancak şartların uygun olması halinde failin her iki suçu birlikte işlemesi mümkündür. Yani içeriğin öğrenilmesi bu suçun oluşması bakımından bir engel teşkil etmemekle birlikte failin başka bir suçtan da sorumlu olması hali ortaya çıkabilecektir.

Netice olarak bu suçun kanuni düzenlemesinde suçun oluşması için verilerin içeriğinin öğrenilmesi, verilerin kayıt altına alınması gibi koşullar aranmadığından bu suç soyut tehlike suçudur. Suç veri nakillerinin teknik araçlarla izlenmesiyle oluşur, izleme devam ettiği sürece suç işlenmeye devam eder. Bu yönüyle bu suç bir mütemadi suçtur.[349] Suçun kanuni düzenlemesinde herhangi bir netice öngörülmediğinden bu suç bir soyut tehlike suçudur[350].

2. Hukuka Aykırılık

Suçun kanuni tanımında *"hukuka aykırı olarak izlemek"* ifadesi kullanıldığından bu suç bakımından hukuka uygunluk sebeplerinin var olduğunu kabul etmek gerekir. Yani örneğin izleme kanuni bir görevin icrası kapsamında gerçekleştiriliyorsa fiil suç oluşturmayacaktır.[351]

[349] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 823.

[350] ÖNDİN, Türk Hukukunda Doğrudan Bilişim Suçları, s. 49.

[351] AKBULUT, s. 166.

Doktrinde bu suç bakımından herhangi bir hukuka uygunluk nedenine yer verilmediğini savunan bir görüş mevcuttur.[352]

Ancak karşı görüşe göre kanuna uygun bir şekilde yapılan izleme bu suç bakımından hukuka uygunluk nedenidir.

Bu görüş çerçevesinde; kanunda veri aktarımının izlenmesine imkan tanıyan herhangi bir düzenleme olması halinde bunun hukuka uygunluk sebebi olarak kabul edilmesi gerektiğini ancak yürürlükte olan mevzuat hükümlerimizin teknik araçlarla izlemeye imkan tanımadığını savunan bir görüş mevcuttur.[353]

Ancak buna katılmak mümkün değildir. Nitekim *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"* , "*Polis Vazife ve Salahiyet Kanunu"* ve *"MİT Kanunu"* gibi birçok kanunda genel düzenlemelere yer verilerek kanuni şartların oluşması halinde veri nakillerinin izlenebilmesine imkan tanınmıştır.[354] Bununla beraber kanuni yetkinin kanunda düzenlenen usul ve şartlara uygun olarak yerine getirilmesi gerekmektedir.

Nakledilen verinin sahibinin açık yahut örtülü rızasının mevcut olması halinde fiil hukuka uygun hale gelecektir.[355] Yine bir veri trafiğinin kamuya açık halde gerçekleştirilmesi yani alenileştirilmesi halinde gerçekleştirilen izleme faaliyet artık suç teşkil etmeyecektir. İzlenen verinin aktarım sırasında şifreli olup olmamasının bir önemi yoktur. Önemli olan aktarılan verinin kamuya açık olup olmamasıdır. Veriler şifrelenerek

---

[352] ÖNDİN, Türk Hukukunda Doğrudan Bilişim Suçları, s. 50.

[353] TEZCAN – ERDEM – ÖNOK, s. 953.

[354] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822; AKBULUT, s. 166.

[355] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822.

yollanmışsa yahut alıcı sınırlı tutularak gönderilmişse artık verinin kamuya açık olmadığı kabul edilmelidir. Ancak e-posta gönderimi yahut bir kişiyle yapılan yazışmaların sınırlı alıcıya veri aktarımı olarak kabul edilmesi dolayısıyla da bu yazışmalar şifresiz dahi olsa bu yazışmaların izlenmesi halinde bu suçun oluştuğunun kabul edilmesi gerekmektedir.[356]

3. Kusurluluk

Bu suç kanuni tanımda özel bir kast aranmadığından genel kastla işlenebilir[357]. Bu suçun yalnızca kasten işlenmesi mümkündür. Fail, teknik araçlarla yapmış olduğu izleme faaliyetinin hukuka aykırı olduğunu bilmeli ve bu hukuka aykırı aykırılık bilinciyle fiili icra etmelidir. Bu nedenle suçun olası kastla işlenmesi mümkün değildir. Bu suç ancak doğrudan kastla işlenebilir. Kanunda suçun taksirli hali düzenleme altına alınmadığından bu suçun taksirle işlenmesi ise mümkün değildir.[358]

Yine tipikliğe ilişkin unsurlarda hataya düşen kişi hakkında, örneğin fail kendisinin yetkili veya görevli olduğu düşüncesiyle hataya düşerek, TCK'nın 30. maddesinde düzenlenen hükümler gözetilmelidir. [359] Cebir yahut tehdit ile suçun unsuru

[356] AKBULUT, s. 163.

[357] TEZCAN – ERDEM – ÖNOK, s. 953.

[358] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 822; AKBULUT, s. 168.

[359] AKBULUT, s. 168.

eylemi icra edecek olursa bu halde failin kusurluluğu ortadan kalkacağı için yine suçun oluşması söz konusu olmayacaktır.

F. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

1. Teşebbüs

Bu suç bir zarar suçu değil salt hareket suçudur. Yani aktarılan verinin içeriğinin ya da aktarılan verinin öğrenilip öğrenilmemesinin bir önemi yoktur. Aktarılan verilerin izlenmesi için icra hareketlerine başlanmış ancak failin iradesine dayanmayan sebeplerle, örneğin aktarımın çoktan başlamış yahut sona ermiş olması veya tam izleme faaliyetine başlanılacağı anda internet bağlantısının kesilmesi gibi, suç tamamlanamaz ise bu suça teşebbüs edilmiş olur.[360]

Suç, bilişim sistemleri arasındaki veri nakillerinin teknik araçlar vasıtasıyla izlenmesiyle tamamlanır. Ancak izlemek fiiline ara verilmeksizin devam edildiği sürece suç işlenmeye devam eder. Bu nedenle mütemadi bir suç söz konusudur. Failin veri naklini izlemeye başladığı anda suç tamamlanmış olacağından ancak ve ancak bu aşamaya kadar gerçekleştirilen fiiller teşebbüs olarak nitelendirilebilecektir. İzlemeye

[360] AKBULUT, s. 168; TEZCAN – ERDEM – ÖNOK, s. 953; ÖNDİN, Türk Hukukunda Doğrudan Bilişim Suçları, s. 50.

başlandıktan sonra devamının engellenmesi ise teşebbüs olarak değerlendirilemeyecek, bu halde tamamlanmış bir suçtan söz edilecektir.[361]

Doktrinde bu suça hazırlık hareketi niteliğindeki bazı davranışların TCK'nın 245/A hükmünde *"Yasak Cihaz veya Programlar"* başlığı altında düzenlenmesi[362] nedeniyle bu suç bakımından hazırlık hareketi boyutunda kalan bir fiilin suçun tamamlanmış halinden daha ağır şekilde bir yaptırıma bağlanmış olması haklı olarak eleştirilmiştir.[363]

2. İştirak

Suça iştirakin ise TCK'da yer alan genel hükümler doğrultusunda gerçekleştirilmesi mümkündür.[364] Bununla beraber suçun işlenmesi için teknik imkan

---

[361] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s.823.

[362] *"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."*

[363] TEZCAN – ERDEM – ÖNOK, s. 953.

[364] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s.823.

sağlayan kişi iştirak iradesi ile hareket etmemişse, onun açısından TCK'nın 245/A hükmü uygulanabilecektir.[365]

Suç mütemadi suç olduğundan fiilin icrasına devam edildiği sürece bu suça iştirak edilmesi mümkündür.[366]

3. İçtima

TCK'nın 43. maddesinde düzenlenen zincirleme suça ilişkin şartların gerçekleşmesi halinde yani failin bir suç işleme kararının icrası kapsamında değişik zamanlarda aynı kişiye ait veri trafiğini izlemesi halinde bu suç bakımından zincirleme suç hükümleri uygulanabilecektir[367].

Doktrinde bir görüşe göre; failin verileri izleme faaliyeti sırasında verilerin içeriğini öğrenmesi ya da veri akışını engellemesi halinde tek fiil ile *"Haberleşmenin Gizliliğini İhlal", "Verilerin Hukuka Aykırı Ele Geçirilmesi" , " Özel Hayatın Gizliliğini İhlal"* gibi suçların da gerçekleşmesi halinde fikri içtima uygulanmalıdır.[368]

Doktrindeki karşıt görüşe göreyse TCK'nın 243/4. maddesinde düzenlenen suçun işlenmesi sırasında ayrıca *"Haberleşmenin Gizliliğini İhlal", "Haberleşmenin Engellenmesi", "Özel Hayatın Gizliliğini İhlal"* gibi suçların işlenmesi halinde faile

---

[365] TEZCAN – ERDEM – ÖNOK, s. 954.

[366] AKBULUT, s. 169.

[367] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 823; AKBULUT, s. 169.

[368] TEZCAN -ERDEM – ÖNOK, s. 954; AKBULUT, s. 170.

gerçek içtima kuralları uyarınca hem 243/4. maddede düzenlenen suçtan hem de işlenen diğer suçtan ayrı ayrı ceza verilmesi gerekir.[369]

Kanaatimce; tıpkı *"Bilişim sistemine girme suçu"*nda olduğu gibi bu suç bakımından da fikri içtima uygulanması mümkün değildir. Bu suç yalnızca doğrudan kastla işlenebilecek bir suç olduğundan failin kastı somut olaya göre değerlendirilmeli ve failin her iki suçu da işlediği kanaatine ulaşılması halinde faile gerçek içtima kuralları uyarınca yaptırım uygulanmalıdır.

Doktrinde failin hem TCK'nın 245/A hükmünde *"Yasak Cihaz veya Programlar"* başlığı altında yer alan suçu hem de 243/4. maddesinde düzenlenen suçu işlemesi hali de tartışmalıdır. Bir görüşe göre; failin gerçek içtima kurallarınca hem 245/A hem de 243/4 hükümleri uyarınca cezalandırılması gerekmektedir[370]. Karşıt görüşe göreyse her iki norm arasında asıl norm – yardımcı norm ilişkisi mevcut olup failin TCK'nın 243/4. maddesi uyarınca cezalandırılması halinde faile 245/A hükmü uyarınca ceza tayin edilmesi mümkün değildir[371].

Kanaatimce, TCK'nın 245/A hükmü esasen 243/4. maddede düzenlenen suçun bir kısım icra hareketlerini yaptırıma bağlamış bir düzenlemedir. Bu yönüyle her iki suç arasında bir geçitli suç ilişkisinin varlığı kabul edilmelidir. Failin 243/4 maddesi kapsamında cezalandırılması halinde faile ayrıca TCK'nın 245/A hükmü uyarınca ceza verilmesi ve gerçek içtima uygulanması mümkün değildir. Failin yalnızca 243/4 maddesi

---

[369] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s 823; Aynı görüş için bknz: ÖNDİN, Türk Hukukunda Doğrudan Bilişim Suçları, s. 67.

[370] AKBULUT, s. 170.

[371] TEZCAN – ERDEM – ÖNOK, s. 954.

uyarınca cezalandırılması gerekmektedir. Bu yönüyle doktrindeki TCK'nın 245/A hükmüne bağlanan yaptırımın TCK'nın 243/4 hükmüne bağlanan yaptırımdan daha ağır olmasına yapılan eleştirilere katılmamak mümkün değildir.

G. YAPTIRIM

TCK'da yer alan *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Aktarımını İzleme Suçu"* 'nu işleyen faile yaptırım olarak*" bir yıldan üç yıla kadar hapis cezası"* belirlenmiştir. Bu suçun nitelikli haline yahut neticesi nedeniyle ağırlaşmış haline kanunda yer verilmemiştir.

Ancak TMK'nın 4. maddesinde sayılan suçlardan bu suçun, bir terör örgütü faaliyeti kapsamında işlenmesi halinde terör suçu sayılacağı ve aynı kanunun 5. maddesi uyarınca arttırılması mümkündür.

TCK'nın 246. maddesinde yer alan *"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."* İfadesine yer verilmek suretiyle hukuka aykırı yarar sağlayan tüzel kişilerin de bu suçlara uygulanacak yaptırımlar kapsamında güvenlik tedbiri ile karşı karşıya kalacağı düzenlenmiştir.

Yine belirtmek gerekir ki; şartların oluşması halinde TCK'nın 54 ve 55 maddeleri uyarınca eşya ve kazanç müsaderesine ilişkin hükümler de uygulanabilecektir.

Ayrıca TCK'da bu suç bakımından da özel bir zamanaşımı süresi yer almamaktadır. Bu nedenle TCK'nın 66. maddesinde düzenlenen genel zamanaşımı süreleri uygulama alanı bulacağından bu suç bakımından dava zamanaşımı süresi sekiz yıldır.

H. SORUŞTURMA VE KOVUŞTURMA

Kanunda bu suçun şikayete bağlı olduğuna ilişkin herhangi bir düzenleme yer almadığından bu suçun soruşturulması ve kovuşturulması re'sen yürütülmektedir.[372]

Mahkemelerin görev ve yetkilerini düzenleyen *"5235 Sayılı Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemeleri'nin Kuruluş Görev ve Yetkileri Hakkında Kanun"* 'un 11. maddesine göre bu suç bakımından görevli mahkeme ise asliye ceza mahkemesidir.[373]

Suç mütemadi suç olduğundan teknik araçlarla veri izleme faaliyeti devam ettiği sürece suç işlenmeye devam edecektir. Failin izlemeyi bıraktığı yahut izleme imkanını kaybettiği anda suç sona erecektir. Yani suç tarihi failin izleme faaliyetinin sona erdiği andır.[374]

Yetkili mahkeme ise CMK'nın yetkiye ilişkin hükümleri uyarınca tespit edilecektir. CMK'nın 12. maddesi uyarınca suçun işlendiği yer mahkemesi yetkili mahkeme olarak kabul edilmelidir. Suçun işlendiği yer bu suç bakımından bir netice öngörülmediğinden hareketin icra edildiği yerdir. Bu nedenle failin bulunduğu yer suçun işlendiği yer olarak kabul edilecektir. Hareket failin bulunduğu yerin yanı sıra hareket aynı anda veri izleme

[372] KOCA – ÜZÜLMEZ, Türk Ceza Hukuku Özel Hükümler, s. 823; AKBULUT, s. 171.

[373] AKBULUT, s. 171.

[374] ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 333.

faaliyetin gerçekleştiği sistemin bulunduğu yerde de ortaya çıkmaktadır. Bu yönüyle veri izlemenin gerçekleştiği yer mahkemesi de yetkili mahkeme olarak kabul edilmelidir.[375]

Bu suç bakımından netice öngörülmediğinden suç yeri failin fiziki olarak bulunduğu yerdir. Bunun yanı sıra fail ile veri trafiğini izlediği sistemin ayrı yerlerde olması halinde veri trafiği izlenen sistemin de suç yeri olarak kabul edilmesi gerekir. Bu nedenle hem failin hem de veri trafiği izlenen sistemin bulunduğu yerdeki mahkeme yetkili mahkemedir.

[375] AKBULUT, s. 171; ÖNDİN, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman"*, s. 333.

SONUÇ

Değişen ve gelişen teknoloji ile birlikte hayatımızın vazgeçilmez bir parçası haline gelen bilişim sistemleri ilk ortaya çıktığı andan bu yana sürekli yenilenmekte ve gelişmektedir. Bu yenilenme ve gelişim beraberinde bilişim sistemlerinin korunması zorunluluğunu arttırmakta ancak bunun yanı sıra zorlaştırmaktadır. Bu yönüyle bilişim suçlarının mevcut ceza hukukunun sınırlarını her geçen gün zorladığı da tartışmasızdır. Zira kanun koyucunun kanuni düzenlemeyi yaptığı esnada mevcut olmayan, bilinmeyen yahut değer atfetmediği bir eylem zaman içerisinde bilişim sistemlerine yönelik eylemlerin ana unsuru haline gelebilmektedir.

Bilişim sistemlerinin hayatımızda ne denli önemli bir yere sahip olduğu tartışmasızdır. Tam da bu nedenle her geçen gün bilişim sistemlerine yönelik tehditler artmakta, failler teknolojik gelişimi avantaj olarak kullanarak yeni yöntemler denemektedir.

Özellikle 2000'li yıllarda büyük bir sıçrama gerçekleştiren bilişim suçları hayatın her alanında kullanıcıları tehdit etmektedir. Örneğin banka hesap bilgilerinin çalınarak hesapta bulunan paranın başka bir hesaba aktarılması, çekilen aile fotoğraflarının yahut özel dokümanların bilgisayara izinsiz gerçekleştirilen erişimlerle istenmeyen kişilerce edilmesi, bir ülkenin nükleer füze sistemine kötü niyetli kişilerce erişim sağlanarak bu sistemlerin kötü amaçlarla kullanılması gibi birçok olayla karşılaşılması mümkündür.

Suç oranlarındaki dikkat çekici artış devletleri bilişim sistemlerine yönelik eylemlere karşı tedbir almaya itmiştir. Bu nedenle birçok ülke ulusal ve/veya uluslararası tedbirleri tartışmaya başlamış, bu tedbirleri uygulamaya koymuştur. Örneğin ülkemizde

bilişim suçları ilk olarak 1991 yılında düzenleme altına alınmış ve sonrasında da yenilerek varlığını sürdürmüştür. Bununla beraber yalnızca kendi sınırları içerisinde alınacak tedbirlerin yeterli olmayacağı bilincinde olan devletler bir kısım tedbirler almak için uluslararası birçok faaliyet düzenlemiştir. Bunlardan en önemlisi AKSSS'dir. Bu sözleşme ile birçok devlet, bilişim suçlarıyla uluslararası işbirliği kurarak mücadele etme yolunu seçmiştir.

Özellikle suçun faillerinin ve bu faillerin kullandığı yöntemlerin tespiti ve incelenmesi büyük önem arz etmektedir. Zira yapılacak düzenlemelerde bu yöntemlerin gözetilmesi bu çerçevede yeni düzenlemelerin ele alınması ve böylece hukuka aykırı eylemlerle mücadele edilmesi gerekmektedir. Aksi halde yapılacak düzenlemeler yetersiz kalacaktır.

Örneğin çalışmanın konusunu oluşturan *"Bilişim sistemine girme suçu"* bilişim sistemleri vasıtasıyla işlenen yahut işlenebilecek birçok suç tipi için temel niteliktedir. Genellikle bilişim sistemleri aracılığıyla işlenen birçok suç bilişim sistemine gerçekleştirilen yetkisiz erişimler sonrasında meydana gelmektedir. Ancak 2016 yılında yapılan değişiklikle ceza hukukumuza kazandırılan ve bu çalışmanın da konusunu oluşturan *"Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini İzleme"* suçunun sisteme girilmeden işlenmesi gerekmektedir. Yani sisteme girilmeden yapılan veri nakli izlemesinin cezalandırılmasındaki eksiklik yapılan düzenleme ile giderilmiştir.

Hukuki eksikliklerin yanı sıra gerek bu çalışmada ele alınan suç tipleri bakımından gerekse de bilişim sistemlerine yönelik veya bu sistemlerin kullanılması suretiyle işlenen suçlar bakımından yargılamalarda başka engellerle de karşılaşılmaktadır. Bu engelleri teknik engeller, uluslararası işbirliğinde yetersizlik yahut uygulayıcıların niteliğinden kaynaklanan eksiklikler olarak özetlemek mümkündür.

Bilişim suçları doğası gereği en küçük boşluktan faydalanabilmektedir. Bu nedenle de her türlü engelin ortadan kaldırılması bilişim suçları ile mücadelede büyük önem taşımaktadır.

Örneğin bilişim suçlarının tespitine yönelik birimlerde çalışan kişilere her türlü teknik altyapı sağlanması ve bu alanda çalışan personelin eğitilmesi gerekmektedir. Zira bu suçların failleri genellikle alanında yetkin ve ciddi bir altyapı kullanan kişilerdir. Dolayısıyla bu faillerin tespit edilebilmesi genellikle ciddi bir altyapı ve nitelikli personel gerektirmektedir.

Yine Amerika kıtasında bulunan bir kişinin yer değiştirmeden ve kolaylıkla Asya'da bir bilişim suçu işlemesi mümkündür. Bu nedenle faillerin cezasız kalmaması için uluslararası işbirliği muhakkak sağlanmalıdır.

Ayrıca uygulamada yargılamaların hızlı bir şekilde ve yetkin kişiler tarafından yapılması gerekmektedir. Bilişim sistemlerinin kullanıldığı yahut bilişim sistemlerine yönelik gerçekleştirilen suçlar genellikle özel yöntemlerle ve yetkin kişilerce işlendiğinden yargılama faaliyetinde görev alan savcı ve hakimlerin bilişim sistemleri üzerinde temel düzeyden daha fazla bilgi sahibi olması zorunludur. Aksi halde fail tarafından gerçekleştirilen eylem yargılama faaliyeti yürüten kişi veya kişilerce anlaşılamayacağından verilecek karar da büyük oranda hukuka aykırı olacaktır.

KAYNAKÇA

AKARSLAN Hüseyin, Bilişim Suçları, B. 2, Seçkin Yay., Ankara 2015.

AKBULUT Berrin, Bilişim Alanında Suçlar, B. 2, Seçkin Yay., Ankara 2017.

AKBULUT Berrin, Ceza Hukuku Genel Hükümler, B. 3, Adalet Yay., Ankara 2016.

AKDENİZ Gökşin, *"Hacker Etiği"*, Hack Kültüğü ve Hacktivizm, Derl. Ali Rıza **KELEŞ**, Alternatif Bilişim, İstanbul 2013.

ALACA Bahaddin, Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile), Yayımlanmamış Yüksek Lisans Tezi, AÜ SBE, 2008 Ankara.

ALTINOK Ebru – **VURAL** Ali Fatih, *"Bilişim Suçları"*, Denetişim Der., 2011, S. 8, s. 74-84.

APAYDIN Cengiz, Bilişim Suçları ve Bilişim Ceza Hukuku, B. 1, Acar Matb., İstanbul 2017.

APİŞ Özge, *"Bilişim Sistemine Girme Suçu Bakımından Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama Kopyalama Elkoyma Koruma Tedbiri"*, Yasama Der., 2018, S. 37, s. 47-86.

ARTUK M. Emin – **GÖKCEN** Ahmet – **YENİDÜNYA** A. Caner, Ceza Hukuku Özel Hükümler, B. 15, Adalet Yay., Ankara 2015.

ASLANYÜREK Malik, İnternet Güvenliği ve Çevrimiçi Gizlilik Alanlarında Yaşanan Sorunlar: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik İle İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Araştırma, Yayımlanmamış Yüksek Lisans Tezi, GÜ SBE, Ankara 2015.

BAYINDIR Sinan – **APİŞ** Özge – **ERSÖZ** Oğuz, Kitle İletişim Hukuku, B.1, Onikilevha Yay., İstanbul 2018.

BIÇAKCI Salih, *"NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik"*, Uluslararası İlişkiler Der., C. 10, S. 40, 2014, s. 101-130.

BOZDOĞAN AKBULUT Berrin, *"Bilişim Suçları"*, SÜHFD, Konya 2000, C. 8, S. 1-2, s. 545 – 555.

CANBEK Gürol - **SAĞIROĞLU** Şeref, *"Kötücül Ve Casus Yazılımlar: Kapsamlı Bir Araştırma"*, GÜ MMFD., C. 22, No: 1, Ankara 2007, s. 121-136.

DEMİR Ömer – **ARIÇ** Mehmet – **POLAT** Halil, Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar, B. 1, Adalet Yay., Ankara 2015.

DEMİRCAN Tunç, Bilişim Alanında Suçlar, B. 1, Legal Yay., İstanbul 2016.

DENNING Dorothy, *"Activism, Hacktivism and Cyberterorrism: The Internet as a Tool for Influencing Foring Policy"*, Chapter 8, Edited by **ARQUILLA** John – **RONFELT** David, Networks and Netwars, The Future of Terror, Crime and Militancy, National Defence Research Institue, Published by RAND, Santa Monica ABD 2001.

DİLEK Halil İbrahim, Bilişim Suçları ve Türk Hukuk Sistemi'ndeki Yeri, Yayımlanmamış Yüksek Lisans Tezi, DÜ SBE, Diyarbakır 2007.

DOĞAN Ramazan, Bilişim Suçları, Adalet Yay., B. 1, Ankara 2014.

DOĞU Ali Haydar, Bilişim Hukuku, Ekin Yay., B. 2, Bursa 2017.

DUFF Liz - GARDINER Simon, *"Computer Crime in the Global Village: Strategies for Control and Regulation — in Defence of the Hacker"*, International Journal of the Sociology of Law, 1996, S. 24, s. 211-228.

DÜLGER Murat Volkan, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin Yay., B. 6, Ankara 2017.

ERDOĞAN Yavuz, Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukuku'ndaki Yeri, B. 1, Legal Yay. İstanbul 2018.

ERDOĞAN Yavuz, Türk Ceza Kanunu'nda Bilişim Suçları, B. 1, Legal Yay., İstanbul 2013.

ERSOY Yücel, *"Genel Hukuki Koruma Çerçevesinde Bilişim Suçları"*, AÜSBFD, Ankara 1994, C. XLIX, No. 3-4, s. 149-183.

ERMEYDAN Damla, *"Türk Ceza Kanunu'nda Bilişim Suçlar"*, Yayımlanmamış Yüksek Lisans Tezi, ÇÜ SBE, Mersin 2018.

ESEN Sinan, Malvarlığına Karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar, B. 1, Adalet Yay., Ankara 2007.

GÜL Ahmet, Doğrudan – Dolaylı Bilişim Suçları, B. 2, Seçkin Yay. Ankara 2018.

GÜRLER Fazıl, Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar, B. 1, Yetkin Yay., Ankara 2015.

HAKERİ Hakan, Ceza Hukuku Genel Hükümler, B. 22, Adalet Yay., Ankara 2019.

HAKERİ Hakan, Ceza Hukuku Genel Hükümler, B. 19, Adalet Yay., Ankara 2016.

HARPER Allen – **HARRIS** Shon – **NESS** Jonathan vd., Gray Hat Hacking The Ethical Hacker's Handbook, Third Edition, Mc Graw Hill Comp., USA 2014.

İÇEL Kayıhan, Ceza Hukuku Genel Hükümler, B. 1, Beta Basım, Ankara 2016.

KARAGÜLMEZ Ali, Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri, B. 5, Seçkin Yay., Ankara 2014.

KARAKEHYA Hakan, *"Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu"*, TBB Dergisi, Ankara 2009, S. 81, s. 187-210.

KAREEM Abdulrahman Hussein Kareem, Bilişim Suçları, Yayımlanmamış Yüksek Lisans Tezi, SÜ SBE, Konya 2019.

KAYA BENGSHİR Türksel, *"Türkiye'de Yönetim Bilişim Sistemleri Disiplinin Gelişimi Üzerine Düşünceler"*, Ammde İdaresi Der., C. 35, S. 1, 2002, s. 76-103.

KETİZMEN Muammer, Türk Ceza Hukuku'nda Bilişim Suçları, Doktora Tezi, AÜ SBE, Ankara 2006.

KOCA Mahmut – **ÜZÜLMEZ** İlhan, Türk Ceza Hukuku Özel Hükümler, B. 3, Adalet Yay. Ankara 2016.

KOCA Mahmut – **ÜZÜLMEZ** İlhan, Türk Ceza Hukuku Genel Hükümler, B. 9, Seçkin Yay., Ankara 2016.

KOÇ Serhat, **KAYNAK** Selva, *"Bilişim Suçları Bağlamında Yeni Medya Olarak İnternet ve Kişisel Güvenlik"*, XII. Akademik Bilişim Konferansı Bildirileri, MUÜ, 10-12 Şubat 2010, s. 71-78.

KURT Levent, Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulamaları, Seçkin Yay., B. 1, Ankara 2005.

KÜLÇÜR Erdem İzzet, Ceza Hukukunda Yer Bakımında Uygulama, B. 1, Onikilevha Yay., İstanbul 2017.

LINDER Felix, *"Malware and Viruses"*, Chapter 14, The Hacker's Handbook The Strategy behind Breaking into and Defending Networks, Edt. **YOUNG** Susan – **AITEL** Dave, Auerbach Publications, USA 2004.

MARION Nancy E., *"The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation"*, *International Journal Of Cyber Criminology, Vol. 4, Issue 1&2,* 1&2 January - July 2010 / July - December 2010, USA, 699-712.

NAMAZCI Halil Ünsal, Herkes İçin Temel Bilgisayar ve İnternet Kılavuzu, Bayrak Matb., İstanbul 2012.

OCAK Mehmet Akif – **YALMAN** Yıldıray – **ÇAKIR** Hüseyin vd., Güncel Tehdit: Siber Suçlar, Edt. **ÇAKIR** Hüseyin – **KILIÇ** Mehmet Serkan, B. 1, Seçkin Yay. Ankara 2014.

ORTA Mesut, Bilişim Suçları ve Elektronik Delillerin Toplanması Muhafazası Değerlendirilmesi Sunulması (Adli Bilişim), B. 1, Yetkin Yay., Ankara 2015.

ÖNDİN Hasan Burak, *"Bilişim Suçlarında Suçun İşlendiği Yer ve Zaman",* Terazi Hukuk Der., C. 15, S. 162, Ankara 2020, s. 320-337.

ÖNDİN Hasan Burak, Türk Hukukunda Doğrudan Bilişim Suçları Yayımlanmamış Yüksek Lisans Tezi, ANDÜ SBE, Eskişehir 2017.

ÖNOK Murat, *"Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği"*, MÜHFHD., İstanbul 2013, C. 19, S. 12, s. 1229-1269.

ÖZBEK Veli Özer – DOĞAN Koray – BACAKSIZ Pınar – TEPE İlker, Türk Ceza Hukuku Özel Hükümler, Seçkin Yay., B. 12., Ankara 2017, s. 939.

ÖZÇELİK Büşra, Bilişim Sistemine Girme Suçu, Yayımlanmamış Yüksek Lisans Tezi, İÜ SBE, İstanbul 2019.

HAFIZOĞULLARI Zeki – **ÖZEN** Muharrem, Türk Ceza Hukuku Genel Hükümler, US-A Yay., B. 12, Ankara 2019.

HAFIZOĞULLARI Zeki – **ÖZEN** Muharrem, Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar, US-A Yay., B. 2, Ankara 2016.

ÖZGENÇ İzzet, Türk Ceza Hukuku Genel Hükümler, B. 12, Ankara 2016, s. 280.

PARLAR Ali, Bilişim Alanında Suçlar, B. 3, Bilge Yay., Ankara 2015.

SCHJØLBERG Stein – **HUBBARD** Amanda M., *"Harmonizing National Legal Approaches On Cybercrime"*, International Telecomminication Union WSIS Thematic Meeting on Cybersecurity, Doc. No: CYB/04, 2005.

SOKULLU AKINCI Füsun, *"Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi",* İÜHFM, C. 59, S. 1-2, s. 11-38.

SOYASLAN Doğan, Ceza Hukuku Genel Hükümler, B. 7, Yetkin Yay., Ankara 2016.

SÖNMEZ Yağmur, Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları, Yayımlanmamış Yüksek Lisans Tezi, MÜ SBE, İstanbul 2018.

STAIR Ralph M.– **REYNOLDS** George W., Principles of Information Systems: A Managerial Approach, B. 9, Course Technology, Boston ABD 2010.

TAŞKIN Şaban Cankat, Bilişim Suçları, B. 1, Beta Yay., Bursa 2008.

TEZCAN Durmuş – **ERDEM** Mustafa Ruhan – **ÖNOK** R. Murat, Teorik ve Pratik Ceza Özel Hukuku, B. 13, Seçkin Yay., Ankara 2016.

TIEDEMANN Klaus, *"Bilgisayarlarla (Kompüter) İşlenen Suçların Ceza Hukuku Yönünde İncelenmesi"*, Çev. **YENİSEY** Feridun, İÜHFM, C. XLI, S. 1-2, 1975, s. 319-332.

UÇKAN Özgür, *"Hacker'lar: Viral Kültürün "Semantik Gerillalar"ı mı, Enformasyon Toplumunun Veri Hırsızları mı?"*, Hack Kültüğü ve Hacktivizm, Derleyen Ali Rıza **KELEŞ**, Alternatif Bilişim, İstanbul 2013.

YALÇIN Türkan – KÖPRÜLÜ Timuçin, Ceza Hukuku Genel Hükümler Uygulamalı Çalışmaları, B. 6, Savaş Yay., Ankara 2019.

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

YARGITAY CUMHURİYET BAŞSAVCILIĞI, Ceza Muhakemesinde Toplanması Gereken Deliller (TCK – Özel Yasalar), Türkiye Adalet Akademisi, Ankara 2020.

YARGITAY CUMHURİYET BAŞSAVCILIĞI, Yargıtay Ceza Daireleri Uygulamasında Sıklıkla Rastlanan Bozma Sebepleri (TCK – Özel Yasalar), Türkiye Cumhuriyeti Adalet Bakanlığı, Ankara 2018.

YILDIZ Sevil, *"İnternet Servis Sağlayıcılar ve Cezai Sorumlulukları"*, SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi, Konya 2002, S. 3, s. 167-184.

YOUNG Susan – AITEL Dave, *"IP and Layer 2 Protocols"*, Chapter 7, The Hacker's Handbook The Strategy behind Breaking into and Defending Networks, Auerbach Publications, USA 2004.

ÇEVRİMİÇİ KAYNAKLAR

DENNING Peter J., *"Computer Viruses"*, RIACS Technical Report, Research Institute for Advanced Computer Science NASA Ames Research Center.

https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19890017050.pdf

DHAR Sumit, *"Sniffers Basics and Detection"*.

http://www.just.edu.jo/~tawalbeh/nyit/incs745/presentations/Sniffers.pdf

GROMOV Gregory, *"Internet Pre-History: Ancient Roads of Telecommunications & Computers"*.

http://history-of-internet.com/history_of_internet.pdf

KARABAL Mustafa vd., *"Bilişim Suçları ve Türk Polis Teşkilatı"*, Çağın Polisi Dergisi, S. 6, 2003.

http://www.caginpolisi.com.tr/bilisim-suclari-ve-turk-polis-teskilati/

KATYAL Neal Kumar, Criminal Law in Cyberspace, Georgetown University Law Center, 2001.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030

LE ROUX CJB (Jerry), *"Social and Community informatics Past, Present, & Future: An Historic Overview Keynote Address"*, 10th Annual DIS Conference: 10-11th September 2009.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.551.1067&rep=rep1&type=pdf,

LEINER Barry M. – **CERF** Vinton G.– **CLARK** David D. – **KAHN** Robert E. vd., *"Brief History of the Internet, Internet Society"*, 1997,

https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf

ODLYZKO Andrew, *"The History Of Communications And İts İmplications For The Internet"*.

http://www.research.att.com/~amo

SCHJOLBERG Stein - **GHERNAOUTI-HELIE** Solange, *"A Global Treaty on Cybersecurity and Cybercrime"*, 2011.

https://cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf

SIEBER Ulrich, *"Legal Aspects of Computer-Related Crime in the Information Society -COMCRIME-Study-"*.

https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.doc

SOMMER Peter – BROWN Ian, *"Reducing Systemic Cybersecurity Risk"*, OECD Multi-Disciplinary Issues International Futures Programme, 2011.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1743384

RAYMOND Eric Steven, *"How To Become A Hacker"*.

http://catb.org/~esr/faqs/hacker-howto.html

ROUSE Margaret, *"Hacker"*.

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

Ulaşan ve Erişen Türkiye Raporu, Ulaştırma ve Altyapı Bakanlığı Strateji Geliştirme Başkanlığı, Ankara 2019.

https://sgb.uab.gov.tr/uploads/pages/yayinlar/ulasan-ve-erisen-turkiye-2019.pdf

TDK, https://sozluk.gov.tr/

http://www.catb.org/jargon/html/crackers.html

http://www.ceza-bb.adalet.gov.tr/mevzuat/maddegerekce.doc

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=yozk7qyT

https://www.coe.int/web/conventions/full-list/-/conventions/treaty/185

https://www.cybercrimelaw.net/G8.html

https://www.cybersecurityintelligence.com/blog/ethical-hacking-can-beat-black-hat-hackers-2457.html

http://www.internetarsivi.metu.edu.tr/tarihce.php

www.kazanci.com.tr

https://mevzuat.tbmm.gov.tr/mevzuat/faces/maddedetaylari?psira=122834&r_afrwindowmode=0&_afrloop=8353709187264943&_adf.ctrl-state=17c8e6wa3h_9

https://www.resmigazete.gov.tr/eskiler/2014/05/20140502-12.htm

https://www.tbmm.gov.tr/sirasayi/donem24/yil01/ss380.pdf

http://www.tuik.gov.tr/PreHaberBultenleri.do;jsessionid=ZksNZYpByB7Y2NRT0r6T6Gfqv0TngGDh0Q31WcDQ2FvhYL2sSn8C!86854652?id=24862

http://www.tuik.gov.tr/PreHaberBultenleri.do?id=30574

ÖZET

Bu tezin konusunu; 5237 Sayılı TCK ile mevzuatımızda ilk kez düzenlenen "*Bilişim sistemine girme suçu"* ile 2016 yılında 243. maddeye eklenen 4. fıkra ile kaleme alınan ve bağımsız bir suç tipi olan Bilişim Sistemleri İçindeki veya Arasındaki Veri Nakillerini İzleme Suçu oluşturmaktadır.

Tezin ilk bölümünde; her iki suçun da kanuni düzenlemesinde yer alan teknik terimler açıklanmış ve bilişim suçlarının tanımı ile tarihsel gelişimine yer verilmiştir. Ardından ulusal ve uluslararası mevzuatlardaki bilişim suçları incelenmiş, bilişim suçlarını işleyen failler ile faillerin kullandığı teknik yöntemler ele alınmıştır. İkinci bölümde ise her iki suç tipinin de unsurları tartışılmış, bu suç tiplerinin özel görünüş şekilleri, failler için belirlenecek cezayı etkileyen haller, yaptırım ile soruşturma ve kovuşturmaya ilişkin hususlar değerlendirilmiştir.

Anahtar kelimeler: Bilişim, veri, bilişim sistemleri, bilişim suçları, siber suçlar, bilişim sistemine girme suçu, yetkisiz erişim, veri nakli, veri nakillerini izleme suçu, TCK m. 243.

ABSTRACT

The subject of this thesis is the Crime Of Accessing To Data Processing System, which was regulated for the first time in our legislation with the Turkish Penal Code No.5237 and an independent type of crime, the Crime Of Monitoring Data Transfers In Or Between Data Processing Systems, which is regulated with the 4th paragraph added to Article 243 in 2016.

In the first part of this study; the technical terms partaking in the legal regulation of both crimes are explained, and the definition and historical development of cyber crimes are expounded. Subsequently, cyber crimes in national and international legislation are examined and perpetrators of cyber crimes and technical methods used by perpetrators are discussed.

In the second part, the elements of both types of crimes are discussed, and finally the special appearance of these types of crimes, the conditions affecting the punishment to be determined for the perpetrators, the issues related to the sanction, investigation and prosecution related matters are evaluated.

Keywords: Data Processing, data, Data Processing Systems, Offenses in the Field of Data Processing Systems, cybercrime, Crime Of Accessing To Data Processing System, unauthorized access, data transfer, The Crime Of Monitoring Data Transfers, Turkish Penal Code Art. 243.