İSTANBUL BİLGİ ÜNİVERSİTESİ
LİSANSÜSTÜ PROGRAMLAR ENSTİTÜSÜ
BİLİŞİM VE TEKNOLOJİ HUKUKU YÜKSEK LİSANS PROGRAMI

CEZA HUKUKU VE BİLİŞİM HUKUKU BAĞLAMINDA TCK MD. 245/A YASAK CİHAZ VEYA PROGRAMLAR SUÇU

Yasin YANAR
113691007

Dr. Öğr. Üyesi Mehmet Bedii KAYA

İSTANBUL
2019

Ceza Hukuku ve Bilişim Hukuku Bağlamında TCK Md. 245/a Yasak Cihaz veya Programlar Suçu

Article 245/a of Turkish Criminal Law: Illicit Devices or Programmes Crime in the Context of Criminal Law and Information Technology Law

Yasin YANAR
113691007

Tez Danışmanı :Dr. Öğr. Üyesi Mehmet Bedii KAYA (İmza) .....
İstanbul Bilgi Üniversitesi

Jüri Üyeleri : Doç. Dr. Leyla KESER BERBER (İmza) .....
İstanbul Bilgi Üniversitesi

Dr.Murat ÖNOK (İmza) .....
Koç Üniversitesi

Tezin Onaylandığı Tarih : .....
Toplam Sayfa Sayısı : .....

Anahtar Kelimeler (Türkçe)	Keywords (English)
1) Bilişim Suçu	1) Cyber Crime
2) Teknolojik Gelişmeler	2) Technological Developments
3) Suçla Mücadele	3) Fight Against Crime
4) Hazırlık Hareketi	4) Preparative Movement
5) Cihaz ve program	5) Device and Programme

ÖNSÖZ

Çalışmamın her aşamasında gösterdiği anlayış ve yolumu aydınlatan rehberliği için değerli hocam Dr. Mehmet Bedii Kaya' ya,

Hayatım boyunca maddi ve manevi olarak arkamda duran, dualarını esirgemeyen sevgili anneme ve babama,

Tanıştığımız ilk günden bugüne kadar en zor anımdan en mutlu anıma, attığım her adımda koşulsuz desteğini hiçbir zaman eksik etmeyen kıymetli eşim Demet Sultan Yanar' a teşekkür ediyorum.

Ayrıca çalışmamı bir gün daha iyilerini yapacağı inancıyla; aldığı ilk nefesle beraber hayatımıza huzur ve bereket getiren, ismi ile müsemma Muhammed Reha' ya, Oğlum' a armağan ediyorum.

İÇİNDEKİLER

İKİNCİ BÖLÜM

YASAK CİHAZ VEYA PROGRAMLAR SUÇU

KISALTMALAR

ARPANET	Advanced Research Project Authority Net
AKSSS	Avrupa Konseyi Siber Suçlar Sözleşmesi
ATM	Automatic Teller Machine
AÜSBFD	Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi
Bkz.	Bakınız
CD	Compact disk
CERN	Conseil Européen pour la Recherche Nucléaire
CDPC	Avrupa Suç Sorunları Komitesi
CID	Card Identification Number
CMK	Ceza Muhkemesi Kanunu
CPU	Central Process Unit (Merkezi Bilişim Birimi)
CVC2	Card Validation Code
CVV2	Card Validation Value
Çev.	Çeviren
DEÜHFD	Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi
Dos	Denial of Service
Ddos	Distributed Denial of Service
Ed.	Editör
EDVAC	Electronic Discrete Variable Computer
EFT	Electronic Funds Transfer
ENIAC	Electronic Numerical Integrator And Calculator
FSEK	Fikir ve Sanat Eserleri Kanunu
G8	Group of Eight
GPS	Global Positioning System (Küresel Konumlama Sistemi)
GSM	Global System for Mobile Communications
GÜHFD	Gazi Üniversitesini Hukuk Fakültesi Dergisi
http.	hyper text transfer protocol
LAN	Local Area Network (Yerel Alan Ağı)
md.	Madde
MILNET	Military Network
MIT	Massachusetts Institute of Technology
No.	Numara
ODTÜ	Orta Doğu Teknik Üniversitesi
OECD	Organisation for Economic Co-operation and Development
PIN	Personal Identification Number
pn.	Paragraf numarası
POS	Point Of Sale (Satış Noktası)
RAM	Random Access Memory (Rastgele Erişimli Bellek)
ROM	Read Only Memory (Salt Okunur Bellek)
RTÜK	Radyo ve Televizyon Üst Kurulu
s	Sayfa

SBE	Sosyal Bilimler Enstitüsü
SSD	Solid-Stave Drive
TBB	Türkiye Barolar Birliği
TCK	Türk Ceza Kanunu
TCP/IP	Transport Control Protocol/Internet Protocol
TDK	Türk Dil Kurumu
THD	Terazi Hukuk Dergisi
TÜBiTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USB	Universal Serial Bus
UTÖ	Uluslararası Ticaret Örgütü
vb.	Ve benzeri
vd.	Ve diğerleri
VB	Visual Basic
Vs.	Ve saire
WAN	Wide Area Network- Geniş Alan Ağı
www.	World Wide Web
Y	Yargıtay
YCGK	Yargıtay Ceza Genel Kurulu

ABSTRACT

Information is the greatest value of our era. With the rapid and continuous developments in technology, all kinds of information are easily accessible at any time. The relationship between information and technology is provided via information systems. Information systems could be seen in many areas such as economics, heath, education and scientific research. Today, many institutions and organizations such as government agencies, commercial enterprises and banks use information systems to perform all their business and transactions. It must be point out that information systems have a feature which would make the commitment of crimes easier. This feature of information systems has been used by malicious people to commit crimes and this has led to the emergence of cybercrime as a new type of crime. Apart from those new types of crimes, some previous types of crimes have now been committed by the use of information systems as well. Therefore, in order to fight the crimes, which are committed by the use of information systems, new various types of offences are regulated under the Turkish Criminal Code. The crime "*Prohibited devices or programmes*" regulated under Article 245/A of the Turkish Criminal Code is one of the offenses that was recently introduced by the legislator.

Article 245/A of the Code punishes the acts that constitute a preparatory movement for the cybercrimes. With the introduction of this crime, an important and positive step was taken for an effective and deterrent fighting against cybercrimes from the very beginning.

This study is prepared in the light of a comprehensive literature review, and all resources and doctrinal discussions related to the topic are taken into account to properly tackle the subject. As there is no judicial decision to be taken into consideration for this new type of crime as of the date of submission of this study, judicial decisions on the general concepts related to cybercrimes are examined in this work.

The aims of this study are to help the determination of the scope of application of this new type of crime, to guide the scientific studies related to cybercrimes, and to shed light on the solutions that may occur in practice.

Keywords*:* *Cybercrime, technological developments, fight against crime, preparatory movement, device and program*

ÖZET

İçinde bulunduğumuz çağın en büyük değeri bilgidir. Teknoloji dünyasında yaşanan hızlı ve süreklilik arz eden gelişmelerle birlikte, her türlü bilgiye her an kolaylıkla ulaşılabilmektedir. Bilgi ile teknoloji dünyası arasındaki ilişki bilişim sistemleri aracılığıyla sağlanmaktadır. Bilişim sistemleri ekonomi, sağlık, eğitim ve bilimsel araştırmalar gibi hayata dair birçok alanda karşımıza çıkmaktadır. Günümüzde devlet kurumları, ticari işletmeler ve bankalar gibi birçok kurum ve kuruluş bütün iş ve işlemlerini gerçekleştirirken bilişim sistemlerini kullanmaktadır. Bu denli büyük bir önem sahip olan bilişim sistemlerinin, suç işlenmesini kolaylaştıran yapısı dikkat çekmektedir. Bilişim sistemlerinin bu özelliği, kötü niyetli kişilerce suç işlemek amacıyla kullanılmıştır. Bu durumda yeni bir suç türü olan bilişim sistemlerinin ortaya çıkmasına sebep olmuştur. Bu suçların yanında var olan bazı suç tipleri de bilişim sistemlerinin kullanılması suretiyle işlenmeye başlanmıştır Bu suçlarla mücadele kapsamında Türk Ceza Kanunu' nda çeşitli bilişim suçları düzenlenmiştir. Kanun koyucu tarafından yakın geçmişte kabul edilen yeni sayılabilecek TCK 245/A maddesinde düzenlenen *' Yasak cihaz veya programlar '* suçu da bu suçlardan biridir.

TCK 245/A maddesi, bilişim suçlarına hazırlık hareketi niteliğindeki fiilleri cezalandırmaktadır. Bu suçun kabul edilmesiyle bilişim suçlarıyla daha yolun başında etkin ve caydırıcı bir şekilde mücadele edilmesi bakımından önemli ve olumlu bir adım atılmıştır

Bu çalışma kapsamlı bir kaynak araştırması ışığında hazırlanmış ve konunun uygun bir şekilde incelenebilmesi için, konu ile ilgili tüm kaynak ve doktrin çalışmaları esas alınmıştır. Hukukumuza yeni giren bu suç tipi için, çalışmamızın kaleme alındığı tarih itibariyle yolumuzu aydınlatabilecek nitelikte bir yargı kararı mevcut olmadığından bilişim suçlarıyla ilgili genel kavramlara ilişkin yargı kararlarına yer verilmiştir.

Çalışmamızın amacı, hukukumuza yeni giren bu suçun uygulama alanının belirlenmesine yardımcı olmak, bu suça yönelik olarak gerçekleştirilecek bilimsel çalışmalara rehberlik edebilmek ve uygulamada yaşanabilecek sorunların çözümüne ışık tutabilmektir.

Anahtar Kelimeler: *bilişim suçu, teknolojik gelişmeler, suçla mücadele, hazırlık hareketi, cihaz ve program*

GİRİŞ

Uygarlık adına tarihin her döneminde insanlığı bir adım ileriye götüren buluşlar yapılmıştır. İcadı teknolojik bir devrim olarak kabul edilebilecek bilgisayar artık cebimizde bile taşınabilir hale gelmiştir. Günümüz dünyasında bağımlılık boyutlarına ulaşan teknolojinin en önemli unsurları bilgisayarlar, akıllı telefonlar ve bu kavramların ortak paydası olan internettir. İnternetle beraber teknolojik gelişmeler farklı bir ivme kazanmış ve bahsi geçen cihazlar bugünkü kullanım oranlarına ulaşmıştır.

Bilgisayarın ve sonrasında internetin kişisel kullanıma açılmasıyla bu iki kavram günlük hayatımızın vazgeçilemez unsurları haline gelmiştir.

İçinde bulunduğumuz süreçte hemen hemen herkes bilişim sistemleri ve internetle bilgisayarlar, akıllı telefonlar yada başka bir şekilde bağlantı kurmaktadır. Bahsi geçen bilişim sistemleri ekonomi, sağlık, eğitim, bilimsel faaliyetler, savunma, idare gibi hayata dair birçok alanda karşımıza çıkmaktadır. İnsanlar artık bilişim sistemlerini, çoğu zaman da bilişim sistemlerinin amiral gemisi olan interneti kullanarak doktor randevusu, tatil planı, bankacılık ve ders kaydı gibi işlemlerini gerçekleştirebilmekte, ayrıca dünya genelinde olan güncel haberlere an be an erişebilmekte, yine hayata dair ürettiği, duyduğu, gördüğü herhangi bir şeyi anında paylaşabilmektedir. Ayrıca artık devlet kurumları, ticari işletmeler, bankalar gibi birçok kurum ve kuruluş bütün iş ve işlemlerini gerçekleştirirken bilişim sistemlerini kullanmaktadır. Bilişim sistemleri, para dahil her türlü bilgi ve değer, zahmetsizce ve kolaylıkla muhafaza edilmesine imkan tanımaktadır. Yine bilişim sistemleriyle, saklanan yukarıda bahsi geçen bilgi ve değerler istenilen anda ve çok fazla emek sarf etmeden hazır hale getirebilmektedir.

Görüldüğü üzere teknolojik gelişmelerle değişen ve büyüyen bilişim sistemleri, insanların hayatını kolaylaştırmaktadır. Özellikle, dünya genelinde var olan bu sistemleri birbirine bağlayan internet teknolojisiyle bilgiye erişim ve iletişim her an mümkün hale gelmiştir.

Ancak bilişim sistemleri, insanlara zarar vermek isteyenler tarafından da kullanılabilmektedir. Bu ayrıcalıklı dünya, sahip olduğu özellikleriyle kötü niyetli kimseler için bulunmaz bir nimet niteliğindedir.

Akıl almaz boyutlara ulaşan teknolojinin tehlikelere maruz kalması, yeni suç tiplerinin de ortaya çıkmasına sebep olmuştur. Klasik suçlar olarak tabir edebileceğimiz uzun yıllardır işlenen hırsızlık, dolandırıcılık, mala zarar verme, hakaret, tehdit ve yaralama gibi suç tiplerine bahsi geçen teknolojik gelişmelerle birlikte bilişim suçları da eklenmiştir.

İnternetle birlikte coğrafi sınırlar önemini yitirmiştir. Bilişim suçu failleri, suç işledikleri ülkede hiç bulunmadan eylemlerini gerçekleştirebilmekte, suç işlemek istediklerinde dijital izleri yok ederek suça anonimlik kazandırabilmektedir. Teknolojinin gelişmesiyle birlikte bilişim suçlarının da geliştiği, çeşitlendiği ve faillerinin yakalanmamakta ustalaştığını söylemek yanlış olmayacaktır. Failler çok büyük emek sarf etmeden, bilgisayarları başında oturarak geliştirdikleri yöntemlerle güvenlik açıklarından faydalanıp, insanların banka hesaplarından para transferleri yapabilmekte, çocuk kullanıcıları hedef alıp onları kandırarak cinsel yönden istismar edebilmekte ya da bilişim sistemleri ile çalışan cihazlar vasıtasıyla toplumsal hayatı felç edebilecek nitelikte zararlar verebilmektedir.

Teknoloji çağının insan hayatına kattığı en büyük olumsuzluğun bilişim suçları olduğu kabul edilebilir. Bu suç tipiyle ortaya çıkan zarar yukarıda ifade edilmeye çalışıldığı üzere çok büyük boyutlara ulaşabilmektedir. Kanun koyucu sahip olduğu önemi göz önüne alarak bilişim suçlarına sebebiyet verebilecek fiilleri düzenleme altına alarak ortaya çıkabilecek zararların önüne geçmek istemiştir.

Esasında bilişim suçlarıyla etkin bir şekilde mücadele edilmesi, daha en başında, bilişim suçu faillerinin suç işleme kararını verip bunu uygulamaya koyma yönünde attıkları ilk adımda başlamalıdır. Burada işaret etmek istediğimiz bilişim suçlarının temelini oluşturan suça ilişkin olarak faillerin gerçekleştirdiği hazırlık hareketleridir.

Bilişim suçlarıyla, etkin ve caydırıcı bir şekilde, kaynağında yani suçun en başında mücadele edilebilmesi için hazırlık hareketlerinin cezalandırılması kaçınılmazdır. Avrupa Konseyi Siber Suçlar Sözleşmesi'nin ' Cihazların kötüye kullanılması ' başlıklı 6. maddesiyle uluslararası bir düzenlemeye tabi tutulan bilişim suçlarına sebep olan hazırlık hareketleri yönünden iç hukukumuzda var olan boşluk kanun koyucunun "Yasak cihaz veya programlar" başlıklı suçu kabul etmesiyle son bulmuştur. Biz de hukukumuza yeni giren bu suç tipini incelemeye çalışacağız.

Çalışmamız için, geniş kapsamlı bir kaynak araştırması yapılmış, bu kaynakların tamamı dikkate alınmış ve bize yapacağı katkı da dikkate alınmak suretiyle doktrindeki tartışmalara da mümkün olduğunca yer vermeye gayret edilmiştir.

Çalışmamız iki bölümden oluşmaktadır. İlk bölümde inceleme konumuz olan suç tipi açısından önem arz eden bilişim sistemi ve bilişim suçlarına temel oluşturan kavramlara değinilmeye çalışılmış, bu kavramların tarihsel gelişim süreçlerinden bahsedilmiş, suç dünyasına gün be gün bir yenisi eklenen bilişim suçlarının işlenme yöntemleri izah edilmeye çalışılmış, genel olarak bilişim suçları ulusal ve uluslararası boyutuyla ele alınmıştır.

Çalışmamızın ikinci bölümünde ise "Yasak Cihaz veya Programlar" suçu açısından korunan hukuki değer, suçun unsurları ile teşebbüs, iştirak, içtima, muhakeme, yaptırım ve zamanaşımı gibi temel konular değerlendirilmiştir.

Sonuç bölümünde ise inceleme kapsamında elde etmiş olduğumuz tespitler ile değerlendirmelere yer verilmiştir.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR VE BİLİŞİM SUÇLARI

1. BİLİŞİM SİSTEMLERİNE İLİŞKİN TEMEL KAVRAMLAR

1.1.Bilişim Kavramı

İçinde bulunduğumuz ve "bilgi çağı" olarak nitelendirilen 21. yüzyılın hiç kuşkusuz en büyük değeri bilgidir. Bilgi dünyası ile teknolojik dünya arasındaki köprüyü kuran bilişim kavramının kaynağı,[1] aynı kökten gelen Fransızca *informatique* sözcüğüdür. Bu sözcük Türkçeye de çevrilmiş ve emformasyon olarak kullanılmıştır. İlerleyen süreçle birlikte bu sözcük yerine bilişim sözcüğü tercih edilmiştir. Bilgi kökenine dayandığı için bu sözcüğün tercih edilmesinin yerinde olduğu düşünülmektedir.[2] Aydın Köksal'ın dilimize kazandırdığı bu kavram, "bilişmek" fiilinden türetilmek suretiyle meydana getirilmiştir.[3]

Bilişim terimi ile ilgili olarak ortak kriterlerden yola çıkılarak farklı tanımlar yapılmıştır. Bilişim suçlarıyla ilgili olarak; hem içerik ve kapsamı hem de doktrindeki tanımların ortak yönlerine yer vermesi hususları dikkate alınmak suretiyle aşağıdaki tanımlamaya yer verilmiştir :

"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."[4]

---

[1] Altınok, Ebru/Vural, Ali Fatih, "*Bilişim Suçları*", Denetişim Dergisi, 2011, Sayı 8, s. 74.

[2] Dülger, Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayıncılık (7. Baskı), Ankara 2018, s. 68.

[3] Köksal, Aydın, *Adı Bilgisayar Olsun*, İstanbul 2010, s. 44.

[4] Dülger, s. 70.

Mevzuatımızda bilişime ilk olarak 1989 yılında TCK Ön Tasarısı'nda rastlanılmaktadır. Tasarıya ilişkin 342. maddenin gerekçesinde bilişim alanı, "bilgileri depo ettikten sonra bunları otomatik işleme tabi tutan ve sistemlerden oluşan alan" şeklinde açıklanmıştır. Ancak 765 sayılı TCK'da bilişim alanındaki suçları düzenleyen 525/a ve 525/b maddelerinde bu kavrama yer verilmemiş iken madde metninde yer almayan bu kavram, 11. babın başlığında kullanılmıştır. 5237 sayılı TCK'nın gerek ilgili maddelerinde gerekse gerekçesinde bilişim kavramının tanımı bulunmamaktadır.[5]

1.2. Bilişim Sistemi

İnceleme konumuz olan TCK md. 245/A, madde metninde de belirtildiği gibi bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçları da konu edindiği için bilişim sistemi ile ne kastedilmek istendiği önem arz etmektedir.

765 sayılı TCK'da, Fransız Ceza Kanunu'ndaki ifadesine karşılık olarak "bilgileri otomatik işleme tabi tutma" ibaresi kullanılmıştır.[6]

1989 tarihli TCK Ön Tasarısı' nın 342. maddesinin gerekçesinden yukarıda bahsedilmişti. Burada otomatik kelimesi ile kastedilen "insan müdahalesinin bulunmamasıdır."[7]

5237 sayılı TCK'da ise bilişim sistemi terimi tercih edilmiştir. 5237 sayılı Kanun'un 243. maddesinin gerekçesinde bilişim sistemi, "verileri toplayıp, yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemler" olarak tanımlanmıştır.[8]

Bilişim sistemi ile ilgili birkaç farklı tanıma daha değinmek gerekirse;

---

[5] Taşkın, Şaban Cankat, *Bilişim Suçları*, Beta Yayınları, Bursa 2008, s. 6.

[6] Yazıcıoğlu, R. Yılmaz, *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*, İstanbul 1997. s. 129.

[7] Helvacıoğlu, Aslı Deniz. "*Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi*", Yeşim Atamer (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları, 2014, No. 51, s. 280.

[8] Yalvaç, Gürsel, *Ceza ve Yargılama Hukukuna İlişkin Temel Kavramlar Gerekçeli TCK CMK CGTİK*, Adalet Yayınevi (17. Baskı), Ankara 2018, s. 529.

Bilişim sistemi, verileri işleyen ve verileri ileten araçlar bütünüdür.[9] Ancak TCK 243. madde gerekçesinde verilen bilişim sistemi tanımında, verileri otomatik işleme tabi tutma unsuru bulunmakla birlikte verileri iletme unsurunu kapsamadığı görülmektedir.

Bilişim sistemi, yazılım ve donanım teknolojisine dayalı olarak idari birimlerin karar alması adına değişik kaynaklardan bilgiyi elde eden, işleyen, muhafaza eden ve raporlayan sistemdir.[10]

TCK' da bilgisayar -bilişim sistemi noktasında bilişim sistemi terimi tercih edilmesinin nedeni bilişim sistemi teriminin daha geniş bir anlama sahip olmasıdır. Günümüzde var olan verilerin depolanmasını, işlenmesini, kullanılmasını ve nakledilmesini sağlayan tüm cihaz ve programlar ile gelecekte icat edilmesi mümkün, bu özelliği taşıyacak olası cihaz ve programlar bu kapsama dahil edilmeye çalışılmıştır.[11] Bu da dünya üzerindeki en büyük ağ olan internetin bilişim sistemi kavramına dahil olması anlamına gelmektedir.[12]

Bilişim sistemi çok geniş bir kavramdır. Bilgisayar ve yukarıda bahsi geçen diğer cihaz ve programların ürettikleri verileri başka bilgisayar veya cihazlara aktarmada kullanılan soyut veya somut ağlar da bilişim sistemi kavramına dahildir. Bilişim sistemini bilgisayardan ayıran önemli noktalardan birisi de budur.[13]

---

[9] Erdağ, Ali İhsan, "*Bilişim Alanında Suçlar (Türk ve Alman Hukukunda*)", Gazi Üniversitesi Hukuk Fakültesi Dergisi, 2010, Cilt 14, Sayı 2, s. 278.

[10] Güleş, Hasan Kürşat, "*Bilişim Sistemlerinin Toplam Kalite Yönetimindeki Yeri ve Önemi*", Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2000, Cilt 15, Sayı 1, s. 105.

[11] Kurt, Levent, *Açıklamalı, İçtihatlı Tüm Yönleriyle Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2005, s. 139.

[12] Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara 2008, s. 20.

[13] Yenidünya, A. Caner, "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*", Legal Fikri ve Sınai Haklar Dergisi, 2005, Sayı 4, s. 1030.

Bilişim sistemi tabirindeki "sistem" ile anlatılmak istenilen, sadece bilgisayarlar değil, verilerin depolanmasını, işlenmesini, kullanılmasını ve nakledilmesini sağlayan çeşitli cihazlar ve olguların bütünüdür.[14]

Bilişimin bir bilim dalı olarak gelişmesi, bilgisayarın ortaya çıkışıyla aynı döneme denk geldiği için, bilgisayar ve bilişim sürekli olarak yan yana kullanılan iki kavram olmuştur.[15] Ancak zaman içinde teknolojinin de gelişmesiyle "bilgileri otomatik işleme tabi tutabilen" yeni cihazlar ortaya çıkmış ve bilgisayar ifadesi bunları ifade etmeye yeterli olmamıştır. "Akıllı" olarak nitelenen buzdolaplarını, televizyonları, tartıları, lambaları, prizleri yine aynı şekilde sesli yardım asistanlarını, kişisel sağlık takip cihazlarını, navigasyon cihazlarını ve cep telefonlarını bu cihazlara örnek olarak verebiliriz. Esas itibariyle bu cihazların çalışma mantıkları da bilgisayarlarla benzerdir. Ancak bilgisayarlar dışında belli algoritmaya göre verileri işleyen diğer cihazlar, görecekleri fonksiyonlara göre özel bir programlama içerirken, bilgisayarlar genel programlama işlemiyle çalışırlar.[16] Bilgisayarlar, verileri işleyebilme ve kullanabilme özellikleri ile diğer makinelerden ayrılırlar. Yine pos cihazı gibi bilgisayar olarak nitelendirilemeyen diğer cihazlar da bilişim sistemi kavramı içinde değerlendirilmektedir.[17]

Bu iki kavram doktrinde ve uygulamada bazen aynı anlamda kullanılsa da her ikisi de farklı kavramlardır. Bilişim sistemi, bilgi teknolojilerini ve bilgisayarı da kapsayan üst kavramdır.

YCGK, bilişim sisteminin, bilgisayardan daha üst bir kavram olduğunu, bilginin otomasyona tabi tutulması sonucunda işlenmesini, yani verinin organize edilmesini, saklanmasını, değerlendirilmesini, çoğaltılmasını, nakledilmesini de

---

[14] Yazıcıoğlu, s. 224.

[15] Ketizmen, s. 1.

[16] Özen, Muharrem/Baştürk, İhsan, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, Ankara 2011, s. 10; Yazıcıoğlu, s. 217

[17] Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, Caner, *Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, 13. Baskı, Ankara 2013, s. 837.

kapsadığını, bilişim sistemlerinde veri iletişiminin, bilgisayarla birlikte manyetik, elektronik veya bazı mekanik araçlarla bir ağ üzerinden sağlanabileceğini belirtmiştir.[18]

CD, Hard-Disk, SSD ve hafıza kartları gibi veri taşıma niteliğine sahip araçlar da bilişim sistemi kavramı içinde kabul edilmektedir. Veri taşıma cihazları da veri depolama özelliğine sahip olmaları hasebiyle bilişim sistemi kavramına dahil olmalıdır aksi taktirde bu cihazlarda yer alan veriler, hukuki güvenlik kapsamı dışında kalma tehlikesi ile karşı karşıya kalırlar.[19]

Cep telefonlarının, kişi veya araçları elektronik olarak tanıyan güvenlik araçlarının, cep bilgisayarlarının da bilişim suçlarının konusu olması mümkündür. Öyle ki Yargıtay vermiş olduğu bir kararında ilk derece mahkemesince cep telefonunun bilişim sistemine dahil olmadığını belirten kararı bozarak cep telefonunun da bilişim sistemine dahil olduğunu belirtmiştir.[20]

Yargıtay, bilgisayar haricinde para çekme makinesi olan bankamatik olarak bilinen ATM'lerin de bilişim sistemi içerisinde sayıldığını ve ATM'lere karşı işlenen suçların da bilişim sistemlerine karşı işlenen suçlardan olduğunu kabul etmiştir.[21]

Yukarıda da değinilen akıllı cep telefonları dışındaki telefonlar, dekoderler, takograf cihazları bilişim sistemine dahil edilmemektedirler. Bu noktada bir sisteminin bilişim sistemi olup olmadığı noktasında tereddüt söz konusu olursa, alanında uzman bir bilirkişiye incelemeye yaptırılması yoluna başvurulabilir.[22]

Bunun yanı sıra otomatik daktilo, telesekreterler, taşınabilir el hesap makineleri ve

---

[18] Bkz. YCGK 19/06/2007 T., 6-136/150; YCGK 17/11/2009 T., 2009/11-193 E., ve 2009/268 K.

[19] Açıkgöz, Emre İkbal, *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu*, (Yayınlanmamış Yüksek Lisans Tezi), Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2017, s. 10.

[20] Y. CD. 18/03/2015 T, 2014/30037 E. ve 2015/2015 K. sayılı ilamı.

[21] YCGK 10/4/2001 T., 2001/76–30 E., 2001/757 K., Yargıtay Kararları Dergisi, Haziran 2001, s. 913 vd.

[22] Taşkın, Şaban Cankat, "*Bilişim Hukuku Uluslararası Anlaşmazlıklar*", Türkiye Barolar Birliği (TBB) Dergisi, 2009, Sayı 85 s. 334.

benzeri aygıtlar bilişim sistemi sayılmazlar.[23]

1.3. Bilgisayar

1.3.1. Genel Olarak

Bilgisayar, İngilizce olan "*computer*" sözcüğünün Türkçe karşılığıdır. Computer sözcüğünün "bilgisayar" olarak dilimizde kullanılmasını sağlayan elektronik, bilgisayar ve yazılım mühendisi dilbilimci Aydın Köksal'dır.[24] Computer kelimesinin dilimizdeki karşılığı olarak, yabancı dillerin etkisinde kalınmak suretiyle "kompütür", "elektronik beyin", "ordinatör" gibi kavramlar kullanılmıştır. Fakat günümüzde bütün bu kelimelerin yerine kullanılmak üzere bilgisayar kelimesi üzerinde tam bir uzlaşma sağlanmıştır. Bilgisayar kelimesi yabancı kökenli bir kelime değildir. Öz Türkçe bir kelime olan bilgisayar sözcüğü İngilizcedeki computer kelimesinden daha geniş bir anlama sahip olup sadece hesaplayıcı anlamına gelmemekte, daha geniş bir kavramı ifade etmektedir. Bilgi işleme kökünden türetilen bu kavram bilgi vermek, bilgi saymak anlamlarını ihtiva eder.[25]

Bilgisayarların bilgi işleyen ya da hesaplama yapabilen diğer araçlardan farkı programlanabilir olmalarıdır. Bu hususun bilgisayarları, hesap makinesinden ayırarak programlanabilme özelliğine sahip çamaşır makinesi ya da televizyon gibi cihazlara yaklaştırdığı kabul edilmektedir. Bilgisayarların bilişim özelliği, yani genel amaçlı kullanılabilme özelliğine sahip olması gözden kaçmamalıdır. Bir bilgisayar ile bilgiler depolanabilmekte, istenilen bilgilere ulaşılabilmekte, hesap yapılabilmekte, müzik dinlenebilmekte, ses ve görüntü kaydı yapılabilmektedir.[26]

---

[23] Ölmez, Aslan, "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma*", THD (Terazi Hukuk Dergisi), Şubat 2009, Yıl 4, Sayı 30, s. 45.

[24] Uçar, Hüdaverdi, *Türk Ceza Kanunu'nda Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2014, s. 3.

[25] Dülger, s. 58-59.

[26] Pallı, Hayati, *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008, s. 6.

Terim olarak bilgisayarın dilimize çevrilme sürecini yukarıda özetlemeye çalıştık. İcadı bilişim açısından milat olarak kabul edilen bu makinenin ana hatlarıyla incelenmesine geçmeden önce tanımının yapılmasında fayda görüyoruz:

1.3.2. Tanımı

Teknolojik ilerlemelere paralel bir şekilde gelişimini sürdüren bilgisayar önceleri büyük bir monitör ve kasa olarak üretilirken, günümüzde diz üstü bilgisayar (lap top), tablet, cep telefonu gibi birçok türde ve hatta dokunarak çalışma özelliğine sahip makineler olarak üretmeye başlanmıştır. Bu gelişim canlı bir şekilde devam etmekte, sesle çalışabilir, katlanabilir, cebe konabilir bilgisayarlar için hali hazırda çalışmalar devam etmektedir. Bu kapsamda teknolojinin hızla ilerliyor olması bilgisayarın tanımını yapmayı her geçen gün güçleştirmektedir.[27]

İnceleme konumuz olan TCK 245/A maddesinde ifade edilen yasak cihaz veya programlar başlıklı suçun en sık kullanılan uygulama alanlarından biri de bilgisayarlardır. Bu kapsamda birbirinden farklı bilgisayar tanımları yapılmıştır.

Bilgisayar, dışarıdan elde ettiği verileri, bünyesindeki programlar ile depolama, işleme, yeni sonuçlar ortaya koyma, bu sonuçları kullanıcılara ulaştırma şeklinde veri iletişimine olanak sağlayan makinelerdir.[28]

Bizim de bilgisayarın çalışma şeklini ve kullanılış amacını detaylı şekilde açıkladığı için iştirak ettiğimiz bir tanımda bilgisayar, bir giriş-çıkış aygıtı ve bir belleği bulunan, her türlü simgeselleştirilmiş işlemi yapabilen ve bu işlemleri belleğine kaydedilmiş yazılımlarla gerçekleştiren bir ana işlemciye sahip, veriler üzerinde dönüştürme işlemi yapan işletim yazılımı bulunan, bilgileri belirli bir düzende saklayan, üzerine farklı yazılımlar yüklenebilip aynı yöntemle çıkartılabilen,

---

[27] Alp, Barış Emre, *5237 Sayılı Türk CEZA Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu*, (Yayınlanmamış Yüksek lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2018, s. 3.

[28] Yenidünya, A. Caner/Değirmenci, Olgun, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık (1. Baskı), İstanbul 2003, s. 19.

veri iletişimini sağlayan, salt bir konuya özgülenmemiş, her türlü işlemi yapabilmek için genel amaçlı olarak üretilmiş veri işlem aygıtlar olarak ifade edilmiştir.[29]

Bilgisayarların bilişim suçları dünyası anlamında verileri saklama, alma ve gönderme özellikleri dikkat çekicidir. Bunun yanında depolama özellikleri de gözden uzak tutulmamalıdır. Bilgisayara ilişkin yapılan tanımlamalarda depolama özelliğine değinilmemektedir. Bilgisayarlar, veri depolama özellikleriyle bir anlamda sanal arşiv hizmeti sunmakta ve bu sanal arşivler de birçok bilişim suçunun icra sahası olabilmektedir.[30]

Yukarıda bilgisayarın tanımının yapılmasının zorluğundan bahsettik. Esasında bu durumun ana nedeni yapılacak tanımın teknolojinin an be an gelişmesi karşısında zamanla yetersiz kalacağı düşüncesidir.[31]

1.3.3. Tarihsel Gelişimi

Hesaplama yapmak için icat edilip geliştirilen bilgisayarın tarihinin, bilinen ilk hesap makinesi olarak kabul edilebilecek olan abaküs ile başladığı düşünülmektedir. Abaküs ile başlayan hesaplamaya yönelik çalışmalar birçok aşamadan geçmiş ve her seferinde üzerine koyarak gelişen sayısız denemeler sonucunda günümüzdeki bilgisayarlar ortaya çıkmıştır.[32] Bilgisayar olarak kabul edilebilecek ilk makine 1940'lı yıllarda Amerikan ordusunun topçu atışlarının yörüngelerinin hesaplanmasında kullanılmak için tasarlanan 30 ton ağırlığında 18.000 vakum tüp ve 15.000 değiştirgeçten oluşan 180 metrekarelik alana kurulu ENIAC'tır. ENIAC İngilizce "*Electronic Numerical Integrator And Calculator*" sözcüklerinin baş harflerinden oluşmaktadır.[33] Bilim adamlarının aynı yıllar süresinde çalıştığı EDVAC

---

[29] Dülger, s. 66.

[30] Alp, s. 5.

[31] Artuk/Gökçen/Yenidünya, *Özel Hükümler*, s. 835.

[32] Topaloğlu, Mustafa, *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması*, Altan Matbaacılık, İstanbul 1997, s. 21.

[33] Dülger, s. 87-89.

adında bir proje de bulunmaktadır. EDVAC'ın özelliği ilk kez belleğe yüklü programlarla çalışan sayısal bilgisayar olmasıdır.[34]

1950'li yılların sonundan itibaren bilgisayarın donanım unsuru yerine yazılım unsuruna ağırlık verilmiş, uzmanlar tarafından yazılım üretilmeye başlanmıştır. Transistörlerin (mikroçipler) küçük boyutlara indirgenmeleri Amerikalı mucit Howard H. Aiken'in, silisyum olan transistörlü işlemciyi bulmasıyla gerçekleşmiştir. 1970'li yıllarda transistörlerin yerine tümleşik devreler kullanılmaya başlanmış, bilgisayarlar artık ulaşılamaz makineler olmaktan çıkarak gündelik işlerde kullanılan makine haline gelmiştir.[35]

1970'li yıllarla birlikte uygulama yazılımları geliştirilmiş, her türlü işin bilgisayarlarda yapılması mümkün olmuştur. Başta Apple isimli bilgisayar şirketi ve devamında diğer şirketlerin de devreye girmesiyle işlemci ve tümleşik devrelerin geliştirilip küçültülmesiyle çok sayıda iş yerinde bilgisayarlar aktif halde kullanılmaya başlanmıştır. 1990'lı yıllarda internetin kişisel kullanıma açılmasıyla bilgisayar günümüzdeki kullanım boyutlarına ulaşmıştır.[36]

1.3.4. Çalışma Sistemi ve Özellikleri

Bilgisayarın çalışmaya başlayabilmesi için, ne yapacağı ve bunu nasıl yapacağı hakkında insanlardan komutlar alması gerekmektedir.[37] Bilgisayarların sahip olduğu en önemli özelliklerden biri, hem işlenmesi için kendisine girişi yapılan verilere, hem de bu verilere uygulanması istenen işlemlere hafızasında yer verebilmesidir.

Burada değinilmesi gereken bir diğer husus bilgisayarın programlanabilme özelliğidir. Ayrıca bilgisayar belli bir fonksiyonu gerçekleştirmeyi hedef almamak,

---

[34] Yazıcıoğlu, s. 35.

[35] Aydın, Emin Doğan, *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınevi Ankara 1992, s. 13.

[36] Dülger, s. 90-91.

[37] Aydın, s. 6.

genel amaçlı olarak kullanılmak suretiyle programlanabilir diğer aletlerden ayrılmaktadır.[38]

Bilgisayarı kendisiyle benzer diğer cihazlardan ayırt etmek için iki ana kriter söz konusudur :

İlk olarak bahsedilmesi gereken özellik, bilgisayarların üzerinde yüklü bulunan yazılımların programlanıp yüklenerek çalıştırılması, gerektiğinde bu yazılımların güncellenmesi, silinebilmesi ve değişiklik yapılabilmesi, ayrıca ihtiyaç duyulan başka yazılımların da yüklenebilmesidir. Bu özellik bilgisayarların, bir hesap makinesinden veya bir GPS cihazından ayırt edilmesini sağlamaktadır.[39] İkinci kriter ise, yazılım yükleme özelliğinin genel amaçlı olması, donanım özelliklerinin el verdiği ölçüde her türlü işlemi gerçekleştirebilmesidir.[40]

Bilgisayarlar sadece elektrik sinyalleriyle çalışırlar. Sayısal bir makinedirler ve veriler "0" veya "1" şeklinde iki sembolle ifade edilirler. Bilgisayarın elektronik devreleri arasında 5 volt elektrik akışı olursa bu "1" olarak; hiç elektrik akışı olmazsa bu da "0" olarak tanımlanır. Bu yüzden bilgisayarlarda işlem yapabilmek için ikilik sayı sistemine diğer adıyla binary sistemi kullanılmaktadır.[41] Deyim yerindeyse bilgisayarların alfabesi sadece 1'ler ve 0'lardan oluşur, bu da bilgisayarların bütün işlemlerini 0 ve 1'leri yan yana getirerek yaptıkları anlamına gelir. Özetlemek gerekirse resimler, müzikler, videolar, yazılar; kısaca bilgisayar ekranında görebildiğimiz her şey esasında 0 ve 1'lerin yan yana getirilmiş şeklidir. Bahsetmiş olduğumuz 0 ve 1'ler makine dilini ifade ederler.[42]

---

[38] Yazıcıoğlu, s. 26.

[39] Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayıncılık (4. Baskı), Ankara 2013, s. 36.

[40] Akbulut, Berrin Bozdoğan (2000). "*Bilişim Suçları*", SÜHFD, Milenyum Armağanı, C.8, S.1–2, 2000, Konya, s.545.

[41] Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayıncılık (5. Baskı), Ankara 2014, s.47- 48.

[42] Açıkgöz, s. 6.

1.3.5. Unsurları

Bilgisayar soyut ve somut olmak üzere iki temel unsurdan oluşmaktadır. Gözle görülen bütün fiziki parçaları donanım teknik tabiriyle hardware unsurunu oluşturur. Bir bilgisayarın klavyesi, faresi, yazıcısı, belleği, mikro işlemcisi gibi fiziksel kısımları donanım unsuruna verilebilecek örneklerdir. Bu fiziki parçaların nasıl çalıştığını belirleyen fiziki olmayan soyut kısmı yazılım yine teknik tabiriyle software olarak isimlendirilmektedir. Elle tutulamayan veri veya programlar bilgisayarın yazılımını oluşturur. Yazılım bilgisayarın ruhu donanım ise kalbidir.

1.3.5.1. Donanım (Hardware)

Bilgisayarın elle tutulabilen fiziki parçaları donanım unsurunu oluşturmaktadır. Bir bilgisayarda teknik açıdan bulunabilecek donanım unsurları olarak, merkezi işlem birimi, salt okunur bellek, rastgele erişilebilen bellek, klavye, fare, yazıcı, tarayıcı, ekran, cd-room, ekran ve ses kartı, bilgisayar giriş çıkış birimleri gibi parçalar sayılabilir. Bu unsurların en önemlilerini kısaca açıklamaya çalışalım:

1.3.5.1.1. Merkezi İşlem Birimi (Central Processor Unit – CPU)

Central Processor Unit'dan çevrilen bu bölüm, işlemlerin yapıldığı bölümdür.[43] CPU, tüm bilgisayar sisteminin yönetim birimi ve ana beynidir. Bilgisayara giriş ve çıkışları kontrol eder, işlem gören veriyi geçici olarak saklar.[44]

1.3.5.1.2. Salt Okunur Bellek (Read Only Memory-ROM)

İngilizce Read Only Memory ibaresinden dilimize çevrilmiştir. Bilgisayar kullanıcısının değiştiremediği kalıcı programları içinde barındıran bellek birimidir. Bu hafıza sadece okuma işlemi gerçekleştirir ve kayıt yapılamaz. Giriş ve çıkış birimleri arasındaki iletişimi gerçekleştiren temel programlar üretici firma tarafından buraya yerleştirilmiştir ve istenilse dahi ya da elektronik devreye gelen akım kesilse dahi

---

[43] Yaycı, Esra, *Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2007, s. 6.

[44] Beygu, Şahin, *Yayıncılıkta Bilgisayar El Kitabı*, Yalçın Ofset Matbaası, İstanbul 1990, s. 10.

bunların değiştirilmesi veya silinmesi söz konusu değildir.[45] Merkezi işlem birimi tarafından sadece okunmak için kendisine ulaşılır.[46]

1.3.5.1.3. Rastgele Erişimli Bellek (Random Access Memory-RAM)

Random Access Memory kelimelerinden Türkçeye çevrilen bölüm yüksek hızda ve CPU'nun üzerinde işlem yaptığı, okuma ve yazma işlemi gerçekleştiren, program ve verilerin geçici olarak saklandığı elektronik devreye gelen akım kapatıldığında tüm kayıtların silindiği,[47] disk ya da disketlere saklanan yazılımların yüklenip çalıştırıldığı, yapılan işlemlerin sonuç olarak üzerinde depolanmadığı bellek türü olarak karşımıza çıkar.[48]

1.3.5.1.4. Çevre Giriş-Çıkış Birimleri - Basic Input/Output System (BIOS)

Çeşitli nitelikteki bilgilerin, işlenmeden önce bilgisayarın anlayacağı şekle sokulmasına ihtiyaç duyulmaktadır. Bu işlemlerin yapılmasına yardım eden ünitelere giriş birimleri, istenilen şekildeki bilgiye dönüştürdükten sonra da insanların anlayacağı hale getiren bölümlere ise çıkış birimleri ismi verilmektedir.[49] Bilgisayarlarla bilgi ve veri alışverişini gerçekleştiren ünitelerin tamamına da çevre birimleri adı verilmektedir. Bu üniteler, veri girişinin yapıldığı klavye, fare, USB kart CD-ROM sürücü, disket sürücü, harici disk, tarayıcı, kamera, mikrofon gibi giriş birimleri ile yazıcı, ekran, hoparlör gibi çıkış birimlerinden meydana gelmektedir. Ekran (monitör), disket, sabit disk, flash bellek ve optik disk hem giriş hem de çıkış birimlerindendir.[50] Bu birimler sayesinde bilgisayar kullanıcı ile iletişim kurmakta ve

---

[45] Kan, İsmet, *Bilgisayar Temel İlkeleri ve Basic*, Uludağ Üniversitesi Yayınları, Bursa 1990, s. 10; Beygu, s. 10.

[46] Kızıltan, Mehmet Burak, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2006 s. 10, Pallı, Bilişim Suçları, s. 12.

[47] Kan, s. 10.

[48] Beygu, s. 46.

[49] Kurt, s. 34.

[50] Gürler, Fazıl, *Teknik Ve Hukuksal Yönleriyle Bilişim Alanında Suçlar,* (Yayınlanmamış Yüksek Lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2013, s. 20.

istenilen bilgileri kullanıcısına sunmaktadır.[51] Teknolojik gelişmelere paralel olarak birtakım yeni çevre giriş çıkış birimlerinin de ortaya çıkması muhtemeldir.

1.3.5.2. Yazılım (Software)

Bilgisayarın soyut bileşenini oluşturan komutların tümüne yazılım denilmektedir. Yazılım, verileri işlemek, bunlardan sağlıklı sonuçlar elde etmek amacıyla bir işi veya hesabı bilgisayara yaptırabilmek için oluşturulan, algoritma şeklinde bir düzen ve mantık silsilesi halinde yazılan, bilgisayara yapılması istenilen işlemlerden önce yüklenilen, bilgisayara işlerlik kazandıran komutlar dizisine verilen isimdir.[52] Algoritma kavramı ise verilerden arzu edilen neticenin ne şekilde elde edileceğini anlatan bir uygulama metodu şeklinde açıklanabilir.[53] Bir diğer tanımda yazılım, donanımın çalışmasını sağlayan, belli talimatları olan, bu talimatlar kullanılarak belli bir iş için işlem oluşmasını sağlayan programlar olarak belirtilmiştir.[54] Her türlü bilgisayar programları, program parçaları, yazılım dilleri bilgisayarın yazılım kısmını oluşturur.[55]

1.3.5.2.1. İşletim Yazılımı (Operating System)

İşletim yazılımları bilgisayarın işleyişini sağlamak ve kontrol etmekle görevli olup, belleğin bir bölümünde yer alarak diğer yazılımları yönlendirmektedir.[56] Bilgisayar ile kullanıcısı arasında köprü görevi görür.[57] Bilgisayar kullanıcıları ekran, klavye, disket sürücüsü gibi birimleri kullanırken farkında olmadan işletim yazılımını

---

[51] Dülger, s. 63.

[52] Değirmenci, Olgun, *Bilişim Suçları*, (Yayınlanmış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2002, s. 169.

[53] Topaloğlu, s. 25.

[54] Sönmez, Yağmur, *Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları*, (Yayınlanmamış Yüksek Lisans Tez), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018, s. 6.

[55] Demircan, Tunç, *Bilişim Alanında Suçlar*, Legal Yayıncılık, İstanbul 2016, s. 14.

[56] Kurt, s. 35.

[57] Yenidünya/Değirmenci, s. 23.

devreye sokarlar, işlemlerin nasıl yerine getirildiğinden haberleri olmadan komutlarla işletim yazılımının birimlerini yönlendirirler.[58]

Diğer bir adı da "işletim sistemi/sistem yazılımı" olarak geçen işletim yazılımları olmadan bilgisayarlar çalışamazlar.[59] Bu yazılım türü genellikle konunun uzmanları yani yazılım şirketleri veya bilgisayar üreten şirketler tarafından meydana getirilmektedir. En iyi bilinen işletim yazılımı bilgisayarın işletim sistemidir. Bu işletim sistemleri, bilişim suçu açısından bir delil toplama ortamıdır. Uzman bir kişi tarafından gerçekleştirilecek delil toplama faaliyetleri ile çok sayıda olay aydınlatılması mümkündür.[60]

1.3.5.2.2. Uygulama Yazılımı (Application Program)

Bu tür yazılımlar bilgisayarların özel bir bölgede işlem yapabilmesine imkan verirler.[61] Uygulama yazılımları kullanıcının belli bir işi yapabilmesi, kendisi için faydalı sonuçlar elde edebilmesi için kullanılmaktadır. Genel amaçlı kullanılan işletim yazılımlarından bu noktada ayrılırlar.[62]

Uygulama yazılımları genel anlamda program olarak anılmaktadır. İnceleme konumuz TCK 245/A maddesi, madde başlığında da belirtildiği üzere program kavramı üzerine kurulu bir düzenleme olduğundan bu husus son derece önemlidir.

Uygulama yazılımları yazı yazma, hesap yapma, tasarım oluşturma vb. gibi işlerin bilgisayar ortamında yapılmasına olanak sağlayan programlardır. Örneğin, okul yönetim sistemleri, muhasebe programları, bilgisayar oyunları, program dilleri derleyicileri vb.[63]

---

[58] Beygu, s. 18.

[59] Kızıltan, s.11.

[60] Alp, s. 12

[61] Kurt, s. 36.

[62] Dülger, s. 65.

[63] Sönmez, s 7.

Uygulama yazılımları olmasaydı, bilgisayarda yapılması gereken her iş ile ilgili kullanıcılar kendi yazılımını yapmak zorunda kalacak veyahut bu işin uzmanı olan şahıslara her defasında bu tarz işleri yaptırma zorunluluğu ile karşı karşıya kalmış olacaklardı.[64]

Önceki dönemlerde sadece askeri veya ticari alanlarla ilgili yazılımlar bilişim suçlarına konu olurken, günümüzde neredeyse bütün yazılımlar bilişim suçlarının icrasında kullanılmaktadır. Özellikle konumuz çerçevesinde düşünüldüğünde çalışmamızın ileriki aşamalarında değinileceği üzere birçok suç, zararlı yazılım programları üretilmesi ve bunların kullanılması suretiyle gerçekleştirilmektedir.[65]

1.3.6. Bilgisayar Ağları (Network)

Bilgisayar ağı literatürdeki adıyla network, bilgisayarların kendi aralarında iletişim kurmasına imkan veren fiziki ortam ve bu ortamın işlevini gerçekleştiren donanımdan ibarettir.[66] Bilgisayarların birbirleri ile iletişime geçebilmesi aralarında fiziksel bir altyapının kurulmuş olmasına ve bu bilgisayarların aynı dili kullanıyor olmasına bağlıdır.[67] Bilgisayarlar arasındaki ihtiyaç duyulan bağlantı bakır tel, fiber optik kablolar, radyo-link sistemleri, haberleşme uyduları, kızılötesi iletişim sistemleri, radyo dalgaları ile haberleşen sistemlerden herhangi birisi ile gerçekleştirilebilir.[68]

Bilgisayar ağları genel itibarıyla Lan ve Wan olmak üzere ikiye ayrılmaktadır:

---

[64] Yenidünya/Değirmenci, s 24-25.

[65] Dülger, s. 65.

[66] Yenidünya/Değirmenci, s 24-25.

[67] Demirkol, Zafer, *İnternet Teknolojileri*, Pusula Yayıncılık, İstanbul 2001, s. 2.

[68] Çekiç, Burak, *İnternet Aracılığı İle İşlenen Suçlar*, (Yayınlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2006, s. 45.

1.3.6.1. Lan (Local Area Network – Yerel Ağ Alanı)

Bu ağ bağlantısında esas olan, sistemlerin aynı ortamda ve birbirlerine yakın mesafede bulunmalarıdır.[69] Örnek olarak bir ofisteki bilgisayarların birbirleri ile yakın bağlantılı olması verilebilir.

1.3.6.2. Wan (Wide Area Network – Geniş Alan Ağı)

Coğrafi olarak uzak mesafedeki bilgisayarların birbirleri ile bağlantılarının kurulması suretiyle oluşturulan bilgisayar ağıdır. Geniş alan ağları, küçük ağların bir araya gelmesiyle oluşur. Bilişim suçları açısından hayati önem arz eden ve çalışmamızın ilerleyen aşamalarında detaylı şekilde açıklanacak olan internet de bu ikinci gruba yani geniş alan ağına dahil bir ağdır ve neredeyse yeryüzündeki bütün ağları birbirine bağladığını söylemek mümkündür.[70] Bilgisayarların birbirine bağlanmasındaki amaç gerçekleştirilen işlemler açısından hız, ekonomiklik ve kolaylık sağlanmaya çalışılmasıdır.

1.4. VERİ

Bilişim dünyası ve bilişim suçlarının en sık karşımıza çıkan materyallerinden biri olan veri bu kapsamda önemli bir yere sahiptir.

Veri, İngilizcede "data" sözcüğünün dilimizdeki karşılığıdır. Bilişim sistemlerinin amacı veriyi işlemek, sonuç çıkarmak ve saklamak şeklinde sıralanabilir. Bu açıdan veri kavramı, bilişim suçları açısından önemli bir yere sahiptir.

Veri kavramıyla ilgili farklı tanımlamalar mevcuttur. Veriyle ilgili şu tanımlama çerçeveyi daha belirgin bir şekilde çizmektedir : "Bilişim sistemlerinin üzerinde işlem yapabildiği, bu işlemlere dayalı sonuçlar üretebildiği, saklayabildiği,

---

[69] Özdilek, Ali Osman, *İnternet ve Hukuk*, Papatya Yayıncılık, Ankara 2002, s. 14.

[70] Ketizmen, s. 20

sakladıklarını sonradan tekrar okuyup işleyebildiği ve diğer bilişim sistemlerine iletebildiği her türlü bilgidir."[71]

Bu kapsamda üzerinde önemle durulması gereken bir noktada bilgisayar veya bilişim sistemi verilerinin yalnızca bilgisayarlarda olmadığıdır. CD, Hard-Disk, SSD ve hafıza kartları gibi veri taşıma araçlarında da veri yer alabilir; elbette ki bu araçlardaki veriler ancak bir bilgisayar veya bilişim sistemi aracılığıyla insanların anlayabileceği bir hale getirilebilir.

Bir başka önem arz eden konu da verinin Türk Ceza Kanunu' nda taşınır mal olarak kabul edilmemesidir. Bu durumda doğal olarak veri, hırsızlık suçuna konu olamayacaktır. Veri eşya olarak da kabul edilmediğinden müsaderesi de söz konusu değildir

1.5. İNTERNET

1.5.1. Genel Olarak

Tabiri caizse artık günümüz dünyasında insanların bir organı olarak kabul edilebilecek bir öneme sahip internet; bilişim, bilişim sistemleri, bilgisayar ya da veri işleme ya da nakletme gibi özelliklere sahip diğer tüm cihazların en önemli uygulama alanıdır. Yukarıda bilgisayar ağı kavramını ifade etmeye çalışmıştık. İnternet bilgisayar ağlarının birbirine bağlanmasıyla meydana gelmiştir.

Bilgisayar ve programlanabilen diğer cihazların ürettikleri verileri başka bilgisayar veya cihazlara aktarmada kullanılan soyut veya somut ağlar bilişim sistemi kapsamındadır. Tüm bilişim sistemlerini birbirine bağlayan internet bilişim sisteminin vazgeçilmez bir parçasıdır.[72]

İnternetin en önemli özelliği herhangi bir kişinin ticari malı olmaması, bir sahibi, yöneticisi ya da denetleyicisinin bulunmamasıdır. Büyük bir ağ sistemine giren kişilerce oluşturulmuş anonim yapı konumundadır. Bu nedenle internete bağlanmak

---

[71] Dülger, s. 79.

[72] Taşkın, Şaban. Cankat., *İnternete Erişim Yasakları,* Seçkin Yayıncılık, Ankara 2016, s. 31

için özel izin, onay ya da başvuru söz konusu değildir.[73] İnternet verilerin toplanmasına, sınıflandırılmasına, karşılaştırılmasına, aktarılmasına imkan sağlamış ve bu durum da bilişim alanında yaşanan gelişmelerin hızının artmasına sebep olmuştur.

İnternetin yukarıda sayılan birçok olumlu özelliğinin yanı sıra birtakım olumsuzlukları da beraberinde getirdiği, bilişim suçlarının işlenmesini daha kolay ve hızlı hale getirdiği, bu nedenlerle bilişim suçu faillerinin rahatça başvurduğu bir araç ve suça sebebiyet veren fiillerin icra edilmesine müsait bir alan haline geldiği de gözden uzak tutulmamalıdır.[74]

1.5.2. Tanımı

İnternet sözcüğü, "*international*" ve "*network*" kelimelerinden meydana gelmiştir. Uluslararası ağ anlamına gelmektedir.[75] Dünya üzerindeki tüm ağların ve bilgisayarların birbirine bağlanması ile oluşur. Her geçen gün yeni ağlar bu sisteme dahil olmaktadır. Bu yüzden internete "tüm dünya bilgisayar ağlarının ağı" ve "ağların ağı" da denilmektedir.[76]

İnsan hayatı için böylesine büyük bir öneme sahip olan internetin tanımına değinmeye çalışalım. Dülger interneti şu şekilde tanımlamıştır:

"İnternet, birden fazla haberleşme ağının birlikte meydana getirdiği metin, resim, müzik, grafik, yazılı metin vb. gibi dosyalar ile bilgisayar yazılımlarının, kısaca insanlar tarafından oluşturulmuş her türlü bilginin veri halinde paylaşıldığı ve iletildiği bilişim sistemleri arasındaki ağ şeklinde ifade edilebilir."[77]

---

[73] Dülger, s. 83.

[74] Mahmutoğlu, Fatih Selami, "Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu", *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, İnternet Özel Bölümü, 2001, Cilt 59, Sayı 1-2, s. 39.

[75] Güngör, Necmi Murat, *Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2007, s. 15.

[76] Dülger, s. 80.

[77] Dülger, s. 80.

1.5.3. Tarihsel Gelişimi

İnternetin ortaya çıkış süreci ABD'nin "Advanced Research Project Authority Net" (ARPANET) projesi ile başlamıştır. Soğuk savaş döneminde ABD ve o zaman ki adıyla Sovyetler Birliği arasındaki mücadele ve karşılıklı duyulan bir kaygı durumu söz konusuydu. Sovyetlerin 1957' de Sputnik'i uzaya göndermesi Amerika Birleşik Devletleri'nde Sovyetlerin teknolojik gücü daha net bir şekilde anlaşılmasına sebep olmuştur. ABD'de bulunan ve "think-thank" olarak bilinen politik ve askeri strateji geliştirme kuruluşlarından olan RAND Corparation tarafından olası bir nükleer savaş sonrasında haberleşme ve iletişimin nasıl sağlanacağı endişesiyle 1964 yılında bir ağ sistemi geliştirilmesi fikri doğmuştur. Sistemin kurulma amacı nükleer savaş veyahut sosyal karışıklık ortaya çıkması halinde yöneticilerin birbirleriyle, askeri kaynakların çeşitli silah üreticileriyle haberleşmesini kesintisiz ve güvenli bir şekilde sağlamaktan ibaretti. Bu yüzden tek bir servis sağlayıcı bilgisayar kullanmak yerine birçok bilgisayarın birbiriyle iletişim kurduğu bir ağ sistemini kurmak için hükümet destekli ve temelli olarak çalışmalar başlatılmıştır. Bu sistemi geliştirmek için Amerikan Hükümeti, Savunma Bakanlığı bünyesinde ARPA isimli bir daire kurulmuş daha sonraki süreçte bu farklı sistemleri birbirine bağlamak için ARPANET adlı bir askeri bilgisayar ağı kurulmuştur. 1969 yılında California'daki üç ayrı merkez ile Utah'daki bir merkezde bulunan toplam dört düğüm noktasındaki bilgisayarlar arasında bağlantı sağlayan ve geliştirilen bu teknoloji sayesinde bilgi aktarımı yapılmıştır.[78] Bundan sonra ARPANET başarıya ulaştığı için uygulamaya konulmuş ve bu sistemden önce ordu sonraları ise üniversiteler faydalanmaya başlamıştır.[79]

Daha sonralarında ise bu sistemdeki farklı özellikteki bilgisayarların birbirini tanımasına yarayan ve aralarındaki uyuşmazlıkları çözme amacı taşıyan, günümüzde de dünyadaki milyonlarca bilgisayarın ve yerel ağların birbiriyle iletişim kurması işlemini gerçekleştiren kurallar bütünü olarak bilinen, TCP/IP kuralları ortaya

[78] Dülger, s. 92-93.

[79] Değirmenci, s. 24.

çıkmıştır. İlerleyen süreçte de bu sistem sivil bilgisayarlarında kullanımına açılmış ve 1990'da sistem daha da geliştirilerek adım adım bugünkü halini almaya başlamıştır.[80]

Askeri amaçlar için oluşturulan ARPANET, zamanla diğer kamu kurumlarının bilgisayarlar aracılığıyla iletişimini sağlayacak şekilde geliştirilmiştir. İlerleyen süreçte askeri amaçlarla kullanılan ağ, 1983 yılında MILNET olarak ayrılmış, ARPANET tamamen kamusal kullanıma açılmış ve internet kendisine her gün daha fazla bilgisayar eklenerek günümüzdeki inanılması güç konumuna gelmiştir.[81]

1989' da world wide web (www) teknolojisi ortaya çıkmıştır. 1990' da dosya transfer protokolü "http"[82] geliştirilmiştir. Bu suretle ARPANET ilga olmuştur. Ağ omurgaları tek yapıda birleştirilmiştir. İnternetin bireysel kullanıma açılmıştır. Akabinde çok sayıda bilgisayar kullanıcısı tek ağa bağlanmıştır. Bütün bu gelişmelerle birlikte internetin yaygınlaşması sağlanmıştır.[83]

1.5.4. Türkiye'de İnternet ve Gelişimi

Ülkemizde bu konuda ilk çalışma 12 Nisan 1993 tarihinde ODTÜ'de gerçekleştirilmiştir. Bu proje TÜBİTAK tarafından desteklenmiştir.[84] Başlangıçta akademik hayatta bilimsel veri alışverişi ve iletişim amaçlı kullanılmıştır. Sonrasında internet, kısa süre içerisinde Türkiye'de bireysel kullanıma açılmıştır.[85]

Ülkemizde ilk olarak ODTÜ'de kullanılan internet bir süre bütün ülkenin tek internet çıkışı görevi görmüştür. Daha sonra 1994 yılı başında Ege Üniversitesi'nde başka bir internet çıkışı oluşturulmuştur. Ardından sırasıyla, 1995'de

---

[80] Sınar, Hasan, *İnternet ve Ceza Hukuku*, Beta Yayınevi (1. Baskı), İstanbul 2001, s. 22.

[81] Kaya, Mehmet Bedii, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi,* İstanbul 2010, s. 6-7.

[82] İngilizce hyper text transfer protocol sözcüklerinin baş harflerinden oluşmaktadır.

[83] Sınar, s. 111; Özdilek, s. 19; Dülger, s. 94.

[84] Değirmenci, s. 22; Sınar, s. 111.

[85] Dülger, s. 94.

Bilkent ve Boğaziçi Üniversiteleri'nde bu işlem gerçekleştirilmiştir. 1996' da ise İTÜ'de internet bağlantısı sağlanmıştır.

1.5.5. İnternete İlişkin Kavramlar

1.5.5.1. TCP/IP Protokolü (Transmission Control Protocol/Internet Protocol İletim Kontol Protokolü/ İnternet Protokolü)

Birbirlerine bağlı bilgisayarların aynı özellikte olmaması sebebiyle, bilgisayarlar arasında veri iletişimini kolaylaştırmak amacıyla çeşitli protokoller kullanılmaya başlanmıştır. Protokoller, iletişimdeki eşler arasındaki mesaj trafiğinin kurallarını oluşturmaktadır. Amaçları ise daha etkin bir iletişim sağlanmasıdır.[86] Şu anda en yaygın olarak kullanılan protokol TCP/IP protokolleridir. Bu kavram, çok sayıda bilgisayarın kendi aralarında iletişime geçmelerine imkan veren ortak dil şeklinde açıklanabilir. IP bilginin makine diline yani dijital formata dönüştürülmesini, TCP ise dijital formata dönüştürülen bilginin yani verinin nihai iletim adresine ulaştırılmasını sağlamaktadır.[87] TCP/IP, dört katmanlı (uygulama, ulaşım, yönlendirme ve fiziksel katmanı) bir yapıya sahip internet ağ mimarisinin protokol kümelerinden oluşmaktadır.[88]

1.5.5.2. World Wide Web Sistemi

1989 yılında CERN bilimsel araştırma kuruluşu tarafından world wide web (www) geliştirilmiştir. Dünyayı saran ağ olarak dilimize çevrilen ve kısaca web olarak anılan bu sistem aracılığıyla yazı, resim, ses, film ve yapay canlandırma gibi pek çok farklı veri türüne ulaşılması mümkün hale gelmiştir. Bu sayede 90'lı yılların başında isimle aranabilen ve yüklenebilen dosyalar internet ortamında yerini almıştır. Tarayıcı olarak adlandırılan, istenilen verilerin bulunmasını sağlayan ve genellikle web sayfası yada web sitesi olarak anılan, istenilen verilerin görüntülenmesini sağlayan uygulama yazılımları bir araya gelerek bu sistemi meydana getirirler. World Wide Web ile bilgiye ulaşım ve bilginin aktarımı kolaylaşmıştır. İnternet hiyerarşisi olmayan ticari

---

[86] Özdilek, s. 16.

[87] Sınar, s. 24.

[88] Yenidünya/Değirmenci, s. 39.

bir yapıya bürünmüştür. 90'ların ikinci yarısı itibariyle internet küresel ekonomik rekabetin önemli bir aktörü olmuştur.[89]

Günlük hayatımızın birçok kısmında internet kullanılmaktadır. İnternet aracılığıyla bankacılık işlemleri yapılabilmekte, canlı olarak görüntülü konuşma gerçekleştirilebilmekte, elektronik ileti yoluyla hızlı, ucuz ve basit haberleşme sağlanabilmekte; haberler internetten takip edilebilmekte dosya, fotoğraf ve görüntü aktarımı gerçekleştirilebilmektedir. Ayrıca bazı internet sayfaları kullanılarak bilimsel araştırmalar yapılabilmekte; çeşitli bilimsel yazılara ve kitaplara erişim sağlanabilmektedir. Cep telefonlarına kadar giren ve kullanılan internetle insanlar kendilerine hayat arkadaşı bile bulma imkanına sahiptir.[90]

Verilerin hızlı bir şekilde iletilmesine fırsat veren bilişim dünyasında gelişmeler devam etmektedir. Bu durum birçok noktada yarar sağlamaktadır. Ancak bu gelişmeler beraberinde birtakım olumsuzlukları da getirmekte ve yeni ihlal alanları oluşturmaktadır. Bilişim sistemlerini birleştirerek uluslararası bir iletişim ağı oluşturan internetin birçok faydası olmakla birlikte, suç işlenmesi için çok uygun bir ortam konumundadır.[91]

2. BİLİŞİM SUÇLARI

2.1. Genel Olarak

Teknolojik gelişmeler maliyetleri azaltmaktadır. Bu da daha çok insanın bilişim sistemlerini aktif şekilde kullanmasına yol açmaktadır. Bilişim sistemlerinin yaygın şekilde kullanılması bilişim suçlarının ortaya çıkmasında önemli bir unsurdur.

Bilişim sistemleri ile çok yüksek düzeyde bilginin muhafaza edilmesi, bu sistemlere karşı yapılan suçların mağdurunun belli olmaması, suçun sisteme karşı

---

[89] Avcı, Artun, *Türkiye'de İnternet ve İfade Özgürlüğü*, Legal Yayıncılık, İstanbul 2013, s. 30; Dülger, s. 83.

[90] Taşkın, *Bilişim Suçları*, s. 15.

[91] Mahmutoğlu, s. 39.

işlenmesi, faillerin tespitinde yaşanana zorluklar faillerin iştahını kabartmakta ve bilişim suçu faillerine fırsat yaratmaktadır.[92]

2.2.Tanımı

Bilişim suçu; siber suç, bilgisayar suçu, sanal suç veya internet suçu şeklinde isimlendirilmektedir. Bu isimlerle "bilişim sistemine karşı ya da bilişim sisteminin kullanıldığı suçlar" kastedilmek istenmektedir.[93]

Yukarıda bilişim suçlarının değişik şekillerde isimlendirildiğinden bahsettik. Bilişimin, bilgisayara göre daha kapsayıcı olması ve günlük hayatta kullanılan birçok elektronik aletin (örneğin cep telefonları, bankamatikler, pos makinesi), bilgisayar olmadığı hâlde bilişim sistemi olması hususları göz önüne alındığında, işlenen suçlara bilgisayar suçları denmesi uygun bulunmamıştır. Bu suçların internet suçları olarak adlandırılması da yerinde değildir. İnternet, bilişim suçlarının işlenmesi açısından birçok imkânı içinde barındırmasına rağmen, internet dışında başka bilgisayar ağları da mevcut olup bunlar üzerinde de bilişim suçları işlenmesi mümkündür.[94]

Burada bilişim suçları- siber suçlar kavramları arasındaki ilişkiye dikkat çekmek istiyoruz. Genel itibariyle yukarıda bahsedilmeye çalışılan suç tipi için uluslararası kaynaklarda "siber suç" tabiri kullanılmaktadır.[95] Ancak bilişim suçlarının siber suçları da içine alan bir üst kavram olduğuna yönelik görüşler de mevcuttur.[96] Yine siber suç kavramı, Türkçe karşılığının sanal suç olması, sanal suç ifadesinin amaçlanan kavramı ifade etmekte yetersiz kalması, işlenen suçların sanal değil tamamen gerçek olması kimi zaman internet gibi bilişim ağları üzerinde işlenmesinin bu suçların fiziki gerçeklikten yoksun olduğu anlamına gelmediği

---

[92] Aydın, Emin Doğan, "Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları", *Marmara İletişim Dergisi*, 1992, Sayı 1, s. 20.

[93] Karagülmez*, Bilişim Suçları* (4. Baskı), s. 43.

[94] Yenidünya/Değirmenci, s. 32.

[95] Ermeydan, Damla, *Türk Ceza Kanunu'nda Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Çağ Üniversitesi SBE, Mersin 2018, s. 1.

[96] Yenidünya/Değirmenci, s. 33.

hususları belirtilmek suretiyle eleştiriye uğramaktadır.[97] Bugün itibariyle bu suçları ifade etmede bilişim suçları kavramı üzerinde uzlaşma sağlanmış bulunmaktadır.

Suç dünyasında bilişim teknolojilerinin ilk kez kullanıldığı tarihten günümüze kadar bir tanımlama yapmak zor olmuştur. Bilişim alanının yeni bir alan olması, bunun yanında her geçen gün yeni bir bilişim suçunun işlenme şeklinin ortaya çıkması sebebiyle bilişim suçu kavramı üzerinde görüş birliği sağlanamamıştır. Ayrıca bilişim teknolojilerinin gelişme düzeyi ve kullanım oranı dünyanın her yerinde aynı değildir. Bu yüzden herkesin kabul ettiği üzerinde uzlaşma sağlanan bir tanım yapılamamıştır.[98] Uzlaşı sağlanamamasının sebebi tanım yapılırken hangi eylemin bilişim suçu olarak değerlendirilip hangilerinin bu kapsam dışında bırakılacağının kesinlik kazanamamış olmasıdır. Hukukumuzda da bilişim suçunun tanımına ilişkin herhangi bir bilgi bulunmamaktadır.[99]

Bu alanda en çok itibar edilen tanım Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983'teki Paris Toplantısı'nda yaptığı tanımdır. Burada bilgisayar suçları, 'bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sitemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış' şeklinde tanımlanır.[100]

AKSSS'de de tanımlama yapmaktan kaçınılmış ve bilişim suçu olabileceği düşünülen eylemlerin tek tek sayılması tercih edilmiştir.

Bilişim suçlarının tanımının yapılmasına yönelik çalışmalarda dikkat edilmesi gereken, yapılacak tanımın temelinin bilgisayar veya bilişim sisteminin kendisine değil, bunlardaki veriye dayanmasıdır. Bilişim suçlarını klasik suçlardan ayırt edebilmek ve sürekli şekilde değişim ve gelişim gösteren teknoloji karşısında eskiyecek ve yetersiz kalacak tanımlamalardan uzak durulması adına bu husus önem

---

[97] Dülger, s. 74.

[98] Kurt, s. 20.

[99] Dülger, s. 75.

[100] Yazıcıoğlu, s. 142.

arz etmektedir. Bilişim suçlarında faillerin amacının bilişim sistemlerinin olmadığı, sistemdeki veriler olduğu herkesin malumudur. Bilişim sisteminin fiziki varlığı hedef alındığında bu bir bilişim suçuna değil ancak klasik suç tiplerinden mala zarar verme yahut hırsızlık gibi mal varlığına karşı suçlardan birisini oluşturacaktır. Anılan sebepler dolayısıyla bilişim suçlarını, bilişim sistemlerindeki verilere karşı ya da sistemdeki veriler hedef alınmak suretiyle sisteme karşı, bunların güvenliğini ve bütünlüğünü bozacak nitelikteki suçlar şeklinde tanımlamak yerinde olacaktır.[101]

2.3. Tarihsel Gelişimi

Yukarıda verilen bilgiler ışığında bilinen ilk bilişim suçu ABD'de işlenmiş ve 18 Ekim 1966 tarihli "*Minneapolis Tribune*"de yayınlanan "bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı yazı ile kamuoyuna duyurulmuştur.[102]

Ülkemizde ise çocukların pornografik görüntü ve resimlerini çekip internet aracılığıyla satmak iddiasıyla yakalanan rehber öğretmen Özgen İmamoğlu'nun Türkiye'de bu konudaki ilk suçlu olduğu kabul edilmektedir.[103]

Bilgisayar teknolojisindeki takibi son derece güç ve insan hayatını bir o kadar kolaylaştıran gelişmeler, başta ticaret, eğitim, özel kurumlar ve devlet kurumlarının bu anlamda boyut değiştirmesini sağlamıştır. Bilgisayar ve teknolojinin yoğun olarak kullanılmaya başlanmasıyla birlikte bilişim suçları da ortaya çıkmıştır. İnternetin keşfedilmesi ve bunun kişisel kullanıma açılmasıyla birlikte de bilişim suçlarının işlenme sayısı oldukça artış göstermiştir. Suçun teknolojinin içinde vücut bulması, bilgisayar ve teknolojiyi birçok kullanıcı için güvensiz ortam olarak kılmaktadır.[104] Bilgisayar ve teknoloji, daha geniş bir tabirle elektronik ortama ilişkin

---

[101] Açıkgöz, s 17.

[102] Aydın, *Bilişim Suçları ve Hukukuna Giriş*, s. 13.

[103] Kurt, s. 54.

[104] Sönmez, 41.

hukuki düzenlemeleri zamanında yaparak günümüz bilişim teknolojilerine uyum sağlayan toplumlar, diğer toplumlara göre bir adım önde olacaklardır.[105]

2.4. Bilişim Suçlarının Tasnifi

Bilişim suçlarının tasnifinde yapılan çalışmaların çıkış noktası bilişim teknolojilerinin "amaç" ve "araç" olarak kullanılması olduğunu söyleyebiliriz. Bu kapsamda bilişim suçları ve bilişim yoluyla işlenen suçlar şeklinde tasnifin gerçekleştirilmesi daha yerinde olmakta, yapılan diğer tasniflerle de uyum göstermektedir.[106]

Türk hukuk öğretisinde kabul edilen genel görüşe göre, bilişim suçları dar anlamda bilişim suçları ve geniş anlamda bilişim suçları olmak üzere ikiye ayrılmaktadır.[107] Bu ayrım oldukça önemlidir. Dar anlamda bilişim suçlarıyla, bilişim sistemlerinin varlığı ile ortaya çıkan suçlar kastedilmektedir.[108] Geniş anlamda bilişim suçları ile klasik suçlar olarak tabir edilen, bilişim sistemlerinin keşfinden önce de hukuk düzeninde mevcut olan suçların, bilişim sistemlerinin araç olarak kullanılmasıyla işlenmesi ifade edilmek istenmektedir.[109]

5237 sayılı TCK'da dar anlamda bilişim suçları ve geniş anlamda bilişim suçlarının her ikisinin de düzenleme alanı bulduğu görülmektedir. 5237 sayılı TCK'da dar anlamda bilişim suçları, topluma karşı suçlar kısmının onuncu bölümünde bilişim alanında suçlar ile kişilere karşı suçlar kısmının dokuzuncu bölümünde özel hayata ve hayatın gizli alanına karşı suçlar olarak kabul edilirken, geniş anlamda bilişim suçları ayrı bir bölüm olarak düzenlenmemiş bilişim sistemlerinin araç olarak kullanıldığı suçlar ilgili kanun maddelerinde ayrı ayrı hüküm altına alınmıştır.

---

[105] Çekiç, s. 1.

[106] Akarslan, Hüseyin, *Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2012, s. 39-40.

[107] Avşar, Zakir/Öngören, Gürsel; *Bilişim Hukuku*, İstanbul 2010, s. 124; Dülger, s. 77-78;

[108] Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* Ankara 2008, s. 29.

[109] Gürler, s. 82.

2.5. Bilişim Suçlarının İşlenme Yöntemleri (Modus Operandi)

2.5.1. Genel Olarak

Gelişen teknoloji, suç işleme düşüncesine sahip olan faillere yeni fırsatlar sağlamaktadır.[110] Bilişim teknolojilerinde yaşanan gelişmelere paralel olarak bu suçların işlenmesinde yeni yöntemler ve teknikler ortaya çıkmaktadır. Aşağıda kısaca bahsedilen yöntemler, işlenen bilişim suçlarının tespit edilmiş yöntemlerine ilişkindir. Bunların yanında henüz tespit edilemeyen yöntemler bulunduğu gibi bu alanda her an yeni işleme suç yöntemlerinin ortaya çıkması da söz konusudur. Bu yüzden, bahsedilen yöntem ve teknikler sınırlayıcı olarak ele alınmamalı, kanun uygulayıcıları bakımından örnekleyici ve açıklayıcı olarak kabul edilmelidir:

2.5.2. Truva Atı (Trojan Horse)

Truva atı yazılımı, adını Yunan mitolojisinde ki Troyalılar ile Akhalılar arasında yapılan savaş içinde gerçekleştirilen taktikten almaktadır. Bu yöntemde fail, bilgisayarda kullanılan programın istediği çalışmayı gerçekleştirmesi için programın içine gizli başka bir bilgisayar programı eklemektedir.[111]

Bu yazılım kendisini bir uygulama programı içerisinde gösterebileceği gibi internetten indirilen müzik, oyun ya da herhangi bir dosyanın içerisine de yerleştirilmesi de mümkündür. Aynı şekilde elektronik posta gönderilmesi yoluyla da bu yazılım kullanıcılara ulaşabilir. Bu zararlı yazılımın yüklenmesi, yazılımı gönderen kişinin, mağdurun tüm bilgisayarı üzerinde hakimiyet kurmasına imkan tanır.[112] Kendi kendilerine çalışamazlar, işlem gerçekleştiremezler. Bu zararlı yazılım ancak mağdurun programı çalıştırmasıyla harekete geçer.[113]

Truva atları bir bilişim suçu failinin, hedefte bulunan uzaktaki bir bilgisayar sistemini kontrol etmesini sağlamaktadır. Bu yazılımın kullanım alanı çok geniştir. Bu

---

[110] Kurt, s. 60.

[111] Yazıcıoğlu, s. 153.

[112] Dülger, s. 104, Çakır, Hüseyin/Kılıç, Mehmet Serkan, *Güncel Tehdit Siber Suçlar*, Seçkin Yayıncılık, Ankara 2014.s. 28.

[113] Akarslan, s. 94.

zararlı yazılım ile,yazılımın sahibi ya da kullanıcısı bilişim sisteminde hemen hemen her türlü eylemi gerçekl eştirebilmektedir. Bilişim suçu failleri bu suç işleme yöntemiyle, CD-ROM'u açıp kapatabilmekte, sistemin ekranına istediği yazıları gönderebilmekte, istediği dosyaları silebilmekte, sistemi kapatabilmekte, istediği bilgileri kendi bilgisayarına internet vasıtasıyla transfer edebilmekte,, istediği bir uygulamayı bilgisayara yükleyebilmekte, hedef bilgisayarın şifresi, kredi kartı şifresi gibi bilgiler temin edebilmektedir.[114] Bu sebeple bilişim alanındaki suçların hemen hemen hepsi bu yazılım yolu ile işlenebilmektedir.[115]

İlk Truva atı türü zararlı yazılım olarak "IBM Christmes Tree" virüsü bilinmektedir.[116] "Promis" isimli yazılımı barındıran bilişim sistemlerinin Ürdün'e satılması Truva atı türü yazılıma verilebilecek bir diğer örnektir. Bu yazılımla Ürdün'ün Filistin hakkında ellerinde bulundurdukları dosyalar, Truva atı yazılımının işletilmesi yoluyla ABD ve İsrail tarafından öğrenilmiştir.[117]

2.5.3. Salam Tekniği (Salami Teqniques)

Salam tekniği ile kastedilen, fazla sayıdaki kaynaktan, az sayıdaki değerlerin transferi ve tek bir hesapta toplanmasıdır.[118] Bu bilişim suçu işleme yöntemi bankaların bilişim sisteminde yaygın olarak gerçekleştirilmektedir. Bilişim sistemleri ile hesap edilen bankacılık alanındaki değerlerin çarpımları sonucu ortaya çıkan değerler çok basamaklı olmasına karşın, bu değerler uygun bir basamağa kadar hesap edilir, günlük konuşma dilindeki tabiriyle yuvarlanır. Bulunan rakam, belli bir hesaba transfer edilir. Böylelikle hesaplarda fark edilemeyecek değişiklikler yapılmaktadır. Hesaplardaki rakamların virgülden sonra ki küsuratlarının ya son rakamı ya da son iki rakamı yani kuruşlar failin belirlediği başka bir hesaba aktarılmakta ve orada

---

[114] Güngör, s. 62; Doğan, Ramazan, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*, Adalet Yayıncılık, Ankara 2014, s. 24.

[115] Dülger, s. 104.

[116] Güngör, s. 62-63, Boğa, Uğur, *Bilişim Suçlarıyla Mücadele Yöntemleri*, (Yayınlanmamış Uzmanlık Tezi), RTÜK, Ankara 2011, s. 36-37.

[117] Odabaşı, Arda, *Bilgi Toplumu mu, Gözetim Toplumu mu? Bilim ve Ütopya*, İstanbul 1999, s. 29-30.

[118] Değirmenci, s. 84.

birikmesi sağlanmaktadır.[119] Ancak bir hesap için çok değersiz görünen bu değerlerin, alternatif bir hesaba aktarılması durumunda toplanan miktarlar büyük rakamlara tekabül etmektedir. Yani bu değerler başka bir hesapta toplanarak yüksek meblağlara ulaşmakta, fail içinde büyük oranda bir hukuka aykırı yarar oluşturmaktadır.

2.5.4. Gizli Kapılar (Trap Door)

Tuzak kapısı, hile kapısı ya da açık kapı isimleriyle de anılmaktadırlar. Sistemin yazılımını gerçekleştiren kişilerce, yazılıma gizlice bir virüs yerleştirilmektedir. Bu kişiler, uzaktan erişimle hedef bilgisayara erişim sağlayabilmektedir. Ayrıca failler sistem kontrollerine yakalanmadan bilişim sistemine sızabilmektedir. Yine failler ileride ortaya çıkabilecek yeni durumlara göre gerekli değişiklikleri gerçekleştirebilme ya da sistem üzerine yeni şifreler girebilmek amacıyla ayarlama yapabilme imkânı yaratmak istemektedir.[120]

Gizli kapılar hataları onarmak için gidermek amacıyla konulurlar. Program ve işletim sistemi tamamlandığında programcılar tarafından temizlenmeli ve kapatılmalıdırlar. Bazı durumlarda hata sonucu olarak veya ileride kullanılmak için bırakıldıkları da olabilir. Kapatılmazlarsa kötü niyetli şahıslar sisteme sızma fırsatı bulabileceklerdir.[121] Zarar vermekten ziyade, teknoloji hırsızlığı ve ticari kaygılar nedeniyle ortay çıkmıştır.[122]

Yazılımı gerçekleştiren kişilerce konulduklarından bilişim uzmanı olmayan kullanıcının fark etmesi mümkün değildir. Herhangi bir sorun çıkması durumunda yazılımı inceleyen uzmanlar tarafından tespit edilebilmeleri mümkün olacaktır.[123]

---

[119] Yazıcıoğlu, s. 155.

[120] Boğa, s. 50, Yazıcıoğlu, s. 156.

[121] Boğa, s. 50.

[122] Alaca, Bahaddin, *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)*, (Yayınlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2008, s. 62.

[123] Ermeydan, s. 15.

2.5.5. Ağ Solucanları (Nextwork Worms)

Ağ solucanları kullanıcının etkisi olmadan bilgisayar yerine ağ üzerinde kendi kendine çoğalıp çalışabilen ve aynen kendisi gibi bir kopyasını, veri iletim ağına bağlantısı olan diğer bilişim sistemlerine, ağlara kopyalayabilen ve bilgisayardan bilgisayara dolaşabilen yazılım türlerine verilen genel isimdir.[124]

Ağ solucanları, iyi oluşturulmamış güvenlik duvarından sızarak eylemlerini gerçekleştirmektedir.[125] Üzerinde taşıdığı Truva atı yazılımını sisteme bırakabileceği gibi doğrudan kendisi de yazılıma zarar verebilir. Ağ solucanları bunları yaparken arkasında bıraktığı izleri silmekte ve bu sebeple bulunmaları imkansız hale gelmektedir.[126] Kendi başlarına ilerleyebilirler. Kendilerini büyük sayılarda çoğaltabilmeleri dikkat çekici bir özelliktir. Solucanların kontrol dışı çoğalmaları, sistem kaynaklarını aşırı kullandığında veya diğer işlemekte olan görevleri yavaşlattığında veya bu görevlerin sonlanmalarına neden olduğunda fark edilebilir.[127] Ağ solucanları sistem içinde bu eylemlerini gerçekleştirirken, girdikleri ağlarda da her türlü veriyi toplar, gizemli mesaj bırakır, hareketlerine ilişkin tüm izleri siler, bu durumda bulunmalarını çok güçleştirir.[128]

İlk olarak 2 Kasım 1988 tarihinde ABD'de ortaya çıkan ağ solucanları o günkü veri iletim ağına yüklenen yazılım, ülkenin tüm bilim kuruluşlarına ve askeri araştırma merkezlerinin sistemlerine bulaşmış ve çok hızlı bir şekilde yayılarak sistemleri kullanılamaz hale getirmiştir.[129]

---

[124] Dülger, s. 109; Kurt, s. 67.

[125] Yaycı, s. 35.

[126] Turhan, Oğuz, *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar*), Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Uzmanlık Tezi, Ankara 2006.

[127] Canbek, Gürol/Sarıoğlu, Şeref, "*Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma*", Başkaya, Şenol (Ed.), Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 2007, Cilt 22, No. 1, s. 124.

[128] Değirmenci, s. 87.

[129] Dülger, s. 110.

2.5.6. Sistem Güvenliğini Kırma- Bilişim Korsanlığı (Hacking)

2.5.6.1. Genel Olarak

Hacking eyleminden önce "hacker" kavramını açıklayalım. "Hacker" deyimi ilk olarak 1960'lı yıllarda, Amerika'da ki Massachusetts Institute of Technology (MIT) bilişim laboratuvarlarında, kullanılan programları geliştirenler için kullanılmıştır. Hackerlar ilk olarak "phreaker" adıyla 1960'lı yıllarda Amerika'da bir telefon şirketinin bilişim sistemlerinin işleyişini merak edip bu sistemlere müdahale eden kişiler olarak ortaya çıkmışlardır. Bilgisayarın bulunmasıyla, bu kişiler kendilerine "hacker" demiştir. Ancak zaman içerisinde bu kavramının yanında bir de "cracker" kavramı ortaya çıkmıştır. Crackerlar kötü niyetli olarak kendisine veya başkasına çıkar sağlamak maksadıyla sistemlerin güvenlik duvarlarını aşarak, sistem dâhilindeki verileri bozan değiştiren kimselere verilen addır. Hackerlar ise, bilişim sisteminin içine girerek her türlü bilgiye ulaşmalarına rağmen sisteme herhangi bir zarar vermezler. Ancak bugün itibarıyla her iki kavramda iç içe geçtiği söylenebilir. Bu kişilere bir bütün olarak bilişim korsanları denilmektedir.[130]

Bilişim sistemlerinin güvenliğinin kırılıp içeri girilmesi eylemini; diğer suç tiplerinden ayıran en önemli özellikse, genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmadan eylemin bizzat bilişim suçu failinin becerisiyle gerçekleştirilmesidir.[131]

Bu yöntem kademe kademe gerçekleştirilmektedir ve ilk adımı da keşif yapmaktır.[132] İkinci kısmı ise tarama yapmaktır. Hedef sistemi taramanın amacı ise işletim sistemini, çalışan servisleriyle paylaşılan kaynakları belirlemektir. Üçüncü adım sisteme sızmaktır. Gerçek anlamda hacking olayı da aslında bu aşama da gerçekleşir. Sisteme sızmak için hackerlar pek çok farklı yöntem denemektedir.

---

[130] Dülger, s. 106; Yaycı, s. 31.

[131] Dülger, s. 107.

[132] Ergün, s. 19.

Oturum çalmak, şifre kırmak, ağı gözetlemek, tampon belleği taşırmak, dos saldırıları yapmak bu yöntemlerden ilk akla gelenleridir.[133]

1997 yılında ABD'de bulunan bir havaalanının bilişim sistemine genç bir korsan girmiş ve havaalanı telefonlarını altı saat boyunca devre dışı bırakmıştır. Buna bağlı olarak havaalanı bir süre kullanılamamıştır. Aynı bilişim korsanı bir eczanenin bilişim sistemine girerek hastalarla ilgili bütün kayıtları ele geçirmiştir. Bu korsan ABD'de yargılanan ilk korsan olmuş ve iki yıl boyunca gözetim altında tutulma ve 250 saat sosyal hizmetlerde çalıştırılma cezası verilmiştir. Aynı şekilde 2008 yılında bir grup bilişim korsanı 40 milyon kredi kartı bilgilerini ele geçirmiştir.[134]

Ülkemizde ise TBMM basın mensuplarına "tbmm.gov.tr" uzantılı bir e-posta gönderilmiş, hatta bu e-posta meclis başkanlığından gönderilmiş gibi gösterilmiştir. Bu e-postada "tüm milletvekillerimize geçmiş olsun, sistemin bu kadar basit ele geçirilmemesi gerektiği, bilgi işlem dairesinde çalışanların aforoz edilmesi gerektiği, bu karışık ortamda bu konunun önemsenmesi gerektiği, saygılarımla; MUSE" yazılmış ve basın mensuplarına gönderilmiştir.[135]

2.5.6.2. Ethical Hacker Kavramı

İnceleme konumuz olan md. TCK 245/A Avrupa Konseyi Siber Suçlar Sözleşmesi'nin 6. maddesinin hukukumuzdaki karşılığı konumundadır. Açıklayıcı raporda da belirtildiği üzere pentest adı verilen testler (sızma faaliyetleri) önem taşımaktadır. Tam da bu nokta da ethical hacker kavramı önem kazanmaktadır.

Bilişim alanının gerçekleşen hızlı gelişmelere paralel olarak bilişim alanındaki suçlar da artış göstermektedir. Bilişim sistemlerini kullanan kişiler ve kurumlar bu suçlardan korunmak için güvenlik önlemleri almaktadırlar. Bu güvenlik

---

[133] Yılmaz, Davut, *Hacking Bilişim Korsanlığı ve Korunma Yöntemleri*, Hayat Yayınları, İstanbul 2004, s. 227.

[134] Dülger, s. 107.

[135] Dülger, s. 108.

önlemlerinin aktif halde çalışıp çalışmadığını görmek için test etme faaliyetlerinde bulunmuşlardır. Bu kapsamda "ethical hacker" kavramı ortaya çıkmıştır.[136]

Bir bilişim sisteminin güvenliğinin, daha önceden korsanlık yapmayan bir kişiye kontrol ettirilmesi yeterince başarı göstermeyince daha önceleri bilişim korsanlığı yapmış olanlar, yani suç işleyenler ethical hackerler olarak kullanılmaya başlanmıştır. Ethical hackerler, test edilecek bilişim sistemine gerçekten bir saldırı olması halinde ilk nerenin hedef alınacağını ve bu hedef alınan yerlerden ne gibi bir bilgilere ulaşılabileceğini, bu saptamaları yaptıktan sonra sisteme neler yapılabileceğini belirlerler ve son olarak sisteme yetkisiz erişim halinde bu yetkisiz erişimlerin fark edilip edilmediğini tespit etmeye çalışırlar.[137]

Ethical hackerler, sistemi test ederken müşterilerinin gizli bilgileri öğrendikleri için güvenilir bir karaktere sahip olmalıdırlar. Ayrıca kendi alanlarında bilgi ve güçlü bir donanıma sahip olmaları, bilgisayar konusunda uzman olmaları, ileri teknolojiyi iyi derecede bilmeleri, sabırlı ve inisiyatif sahibi olmaları aranmaktadır.[138] Ethical hackerlik kapsamında ilk çalışma James Christy'nin oluşturduğu takımın 15 saniyede Pentagon'un erişime kapalı sistemine girmeyi başarmasıdır.

ABD'de "Dijital Millennium Copyright Act" adlı kanunun 1201. maddesiyle bu kavram kanuni güvence altına almıştır.[139]

Ethical hacker kavramı ABD'de yasal düzenleme altına alınmışken ülkemizde herhangi bir yasal düzenleme bulunmamaktadır. Ülkemizde yasal düzenleme noktasında var olan boşluk inceleme konumuz olan TCK md. 245/A'nın kabul edilmesiyle son bulmuştur. Bilişim sistemlerini ethical hackerlarına test ettirmek istenmesi halinde, sistem sahibinin yapılan test işlemine rızasının, onayının

---

[136] Karagülmez, *Bilişim Suçları*, (5. Baskı), s. 91.

[137] Karagülmez, *Bilişim Suçları*, (5. Baskı), s. 92-93.

[138] Karagülmez, *Bilişim Suçları*, (5. Baskı), s. 96-97.

[139] Altınok E/Vural A. F., s. 83.

bulunması sebebiyle hukuka uygunluk nedeni kapsamında değerlendirilecektir. Özetle test eylemi herhangi bir suç oluşturmayacaktır.

2.5.7. Bilişim- Bilgisayar Virüsleri

Bilişim virüsleri, kendi kendini çoğaltabilme özelliğine sahip olan, kopyalarını çeşitli yöntemlerle diğer sistemlere bulaştırarak bu sistemleri de etkileyen zararlı yazılım türleridir.[140] Bilgisayar virüsleri, yazılımdan yazılıma, dosyadan dosyaya rahatlıkla kopyalanabilmektedir. Bu küçük yazılımlara virüs denmesinin nedeni, biyolojik olan virüslerde ki gibi kendi kendine çoğalıp, bulaşabilme ve sistemi hasta ederek kullanılmaz hale getirmelerinden dolayıdır.[141] Bilgisayar veya bilişim virüsleri özellikle internet vasıtası ile çok hızlı bir şekilde yayılmaktadır.[142] Bu konuda ki en bilinen örneklerden biri de, 2001 yılında Filipinli bir bilgisayar öğrencisi tarafından yazılan LoveBug (Aşk Virüsü) isimli virüs programının, yayılmaya başladıktan 18 saat sonra Dünya'da yüz milyon bilgisayara bulaşmış olmasıdır.[143]

Virüsler, en eski ve aynı zamanda en tehlikeli kötücül özellikteki yazılımdır.[144] İlk ortaya çıktıklarında başka kullanıcıların bilgisayarlarında sorun çıkarma ya da tabiri caizse, muziplik yapma amacı taşımaktaydılar.[145] Ancak zaman içerisinde virüsler, başkalarının bilgisayarlarına girerek çok çeşitli suçların işlenmesinde kullanılmıştır. Virüslerin bulaşması önce disketlerin yaygınlaşması ile artmış, ardından ağ teknolojileri ve en büyük ağ olan internetle beraber en üst noktaya çıkmıştır.[146]

---

[140] Değirmenci, s. 88.

[141] Yazıcıoğlu, s. 161.

[142] Ergün, s. 27.

[143] Ergün, s. 27

[144] Canbek G./Sarıoğlu Ş., s. 123.

[145] Özkaya, Elif, "*Bilgi Teknolojisinin Yarattığı Parazitler*", Gürdilek, Raşit (Ed.), NTV Bilim Dergisi, 2009, Sayı 1, s. 61.

[146] Kurt, s. 70.

Tarihte belgelenen ilk virüs saldırısı 22 Ekim 1987 tarihinde Pakistanlı iki kardeşin zarar verme amacı olmaksızın meydana getirdikleri "brian virüsü" dür. Bu virüs çok büyük çabalar sonucu temizlenebilmiştir.[147]

Virüslerin, ekranda rahatsız edici, çalışmaya kısa süreliğine de olsa mani olan mesajlar göstermek gibi zararsız sayılabilecek türlerinin de bulunmasına karşın, çoğu virüs programlarının, önemli dosyaları silmek veya konak (host) sistemini tamamen çalışmaz hale getirmek gibi yıkıcı etkilerinin olduğu bilinmektedir. Virüslerin en belirgin farkı, insan etkileşimiyle harekete geçmesidir. Yani bir e-postanın açılması, bir dosyanın çalıştırılması ile virüs kendiliğinden yayılmaya başlamaktadır.

Virüsler ile diğer bilişim suçlarının işlenme yöntemleri olan Truva atı, solucanlar ve mantık bombaları birbirlerine benzeseler de virüsüler kendi kendilerine çoğalabilme ve diğer programlara bulaşabilme özellikleriyle bu yöntemlerden ayrılırlar.[148]

Virüsten korunmanın yöntemi Antivirüs programları kullanmaktır. Ancak bazı virüsler kendini geliştirerek antivirüs programlarına takılmayarak yayılabilmektedir. Bu nedenle antivirüs programlarını sürekli güncellemek gerekir. Ayrıca elektronik ticaretin yaygınlaşması ve bankacılık hizmetlerinin internet üzerinden yürütülmesi nedeniyle virüs yazmanın kazançlı bir meslek hâline geldiği düşünülmektedir.

2.5.8. Casus Yazılımlar (Spyware)

Casus yazılım türleri, kendilerini gizlerler ve tespit edilmeleri oldukça zordur. Başka programlar kurulurken, onayınız alınarak bilgisayarınıza kurulurlar. Bu yazılım türleri genellikle, reklam pencereleri görüntüleyen yazılımla ya da kişisel veya önemli bilgileri takip eden yazılımla bağlantılı hale getirilir. Bu şekildeki her yazılımın kötü olduğu sonucu çıkarılmamalıdır. Reklamları almayı kabul ettiğinizde

---

[147] Dülger, s. 113; Güngör, s. 69.

[148] Doğan, s. 30.

bir müzik hizmetine bedel ödemeden kaydolma imkanına sahip olabilirsiniz. Casus yazılımlar bilgisayarınızda rahatsız edici değişikliklere, yavaşlamalara veya kilitlenmelere sebebiyet verebilir. Ayrıca söz konusu yazılımlar, ayarlarınızı daha önceki orijinal değerlerine döndürmenizi de güçleştirir.[149]

2.5.9. Oltalama (Phishing)

Fishing ve password sözcüklerinin birleşmesi ile elde edilen bir terimdir.[150] Phishing, kredi kartı bilgileri ya da parolalar gibi çeşitli özel ve gizli kalması gereken, başkaları tarafından bilindiğinde kişilerin zor durumda kalmasına neden olabilecek gizli bilgilere erişmek ve onları elde etmek için sanki bu bilgileri kişiye veren ve güvenilir bir yerden geliyormuşcasına görünen e-postalar ya da web siteleri hazırlayıp kullanıcılardan bu bilgileri paylaşmalarını isteme eylemlerinin genel adıdır.

Bu tür saldırılardan kurtulmak için bankaları internet sitelerine adres çubuğuna manuel yani el ile yazılmak suretiyle giriş yapılmalı, kullanıcılar gereksiz e-postaları açmamaları konusunda bilgilendirilmeli, bu tür saldırıların sosyal medya siteleri üzerinden de yapılabileceği düşünülerek kullanıcıların tanımadıkları kişileri arkadaş olarak eklememeleri, şüpheli kişilerden gelen mesajları açmamaları önerilmektedir.[151]

2.5.10. Veri Aldatmacası (Data Didding)

Veri aldatmacası ismi verilen suç işleme yöntemi, verinin bilgisayara ya da belleğe kaydı esnasında verinin değiştirilmesi ya da bilgisayara yanlış veri girilmesi şeklinde açıklanabilir. Bilişim suçları içerisinde işlendikten sonra meydana çıkarılmasının çok zor olması nedeniyle en çok tercih edilen suç yöntemidir.[152]

---

149 http://www.mugla.pol.tr/fethiye/Sayfalar/Casus-Yaz%C4%B1l%C4%B1m-Nedir.aspx (erişim tarihi 21.04.2019); https://eezgiozgenn.wordpress.com/zararli-yazilim-nedir/ (erişim tarihi 21.04.2019).

150 http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi 11.04.2019).

151 Hekim, Hakan, "Oltalama (Phishing) Saldırıları", Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.), *Siber Suçlar Tehditler, Farkındalık ve Mücadele*, Global Politika ve Strateji, Ankara 2015, s. 75-78.

152 Kurt, s. 62.

Veri aldatmacası yetkisiz erişimle depolanmış bilgilerin değiştirilmesini ifade eder. Belgelerin bozulması, değiştirilmesi, ek karakter kaydı, bazı kayıtların iptali gibi aldatmacalar gerçekleştirilebilir.[153] Bu hareketlere örnek olarak, disketlerin, sabit disklerin ya da manyetik bantların önceden hazırlanan kopyasıyla değiştirilmesini sayabiliriz.[154]

2.5.11. Mantık Bombaları (Logic Bombs), Yazılım Bombaları, Saatli Bombalar (Time Bombs)

Truva atı metodunun bir çeşididirler. Mantık bombası, bilgisayar sisteminde, kötü niyetli bir hareket gerçekleştirebilmek için uygun durumlarda veya sürekli olarak faaliyet gösteren bir program olup, bilgisayar sistemlerini bozmak, işlemez hale getirmek amacıyla kullanılmaktadır.[155] Önceden belirlenmiş özel durum gerçekleşene kadar "Truva atı" konumundadır. Özel durum gerçekleştikten sonra zararlı etkisini gösterir.

Bu konuda Çernobil Virüsü örnek olarak verilebilir. Çernobil virüsü bellekte beklemekte ve her ayın 26'sında harekete geçerek etkisini göstermektedir.[156] 2002 yılında Amerika'nın New Jersey eyaletinde işvereni ile arası iyi olmayan bir çalışanın işten ayrılmadan önce sisteme zaman ayarlı bir kod yerleştirmesi, bu kodun sistemin yazılımlarını ve satış bilgilerini silmesi bu suç işleme yöntemine verilecek bir başka örnektir.[157]

Yazılım bombaları ise üretilmesi kolay ve yaygın olarak kullanılan zararlı yazılımlardandır. Herhangi bir uyarı ve belirti olmaksızın çarpma anında patlayarak verileri ortadan kaldıran yazılımlardır. [158]

---

[153] Doğan, s. 48.

[154] Çakır, H./Kılıç, M. S., s. 29, Yaycı, s. 33-34.

[155] Yazıcıoğlu, s. 157.

[156] Dülger, s. 112.

[157] Alp, s. 33.

[158] Kurt, s. 76.

Saatli Bombalar (Time Bombs) mantık bombaları ile benzer özelliklere sahiptir. Belirli bir sayıda çalıştırıldıktan sonra, belli bir tarihte patlayacak şekilde programlanabilirler.[159] Herhangi bir tarih patlama tarihi olarak belirlenerek eylem gerçekleştirilebimektedir.

2.5.12. Eş Zamansız Saldırılar (Asynchronous)

Bilgisayarların birden fazla işlemi aynı anda yapabilmelerine eşzamanlı çalışma denilirken bazı durumlarda belirli bir sırada çalışmalarına, bir işlemin başlayabilmesi için diğer işlemin sonucu beklenilmesine ise eş zamansız çalışma adı verilmektedir.[160] Bu yöntem bilişim sistemlerinin programlarının eş zamansız olarak çalışmasından faydalanır.[161] Sistemin mevcut programları eş zamanlı yani aynı anda kullanılmadığından, bilgisayar kullanıcının taleplerini belirli bir düzen ve sıra içinde yerine getirirken, bekleme anında bazı failler saldırılar yapmakta ve veriler üzerinde çeşitli ihlaller, değişiklikler gerçekleştirmektedir.[162]

2.5.13. İstem Dışı Alınan Elektronik Postalar (Spam-Spiced Pork And Ham)

Spamlar günümüzde birçok internet kullanıcısının ve özellikle büyük bilişim sistemlerinin uğraştığı önemli bir sorundur. Türkçede "istem dışı ileti" ya da "yığın ileti" terimleriyle karşılık bulan spamlar[163] kısaca, istem dışı alınan e-postaları ifade etmek için kullanılır.[164] Bilgi bankalarından, tartışma platformlarından veya herhangi bir yolla elde edilen elektronik posta adreslerine kişilik haklarına yönelik bir ihlal teşkil etmese de rahatsız edici ve istem dışı olarak atılan her türlü ileti ve ekleri olarak spam kapsamında değerlendirilir.[165]

---

[159] Aydın, *Bilişim Suçları ve Hukukuna Giriş*, s. 51.

[160] Boğa, s. 51.

[161] Değirmenci, s. 83.

[162] Yazıcıoğlu, s. 158.

[163] Doğan, s. 31.

[164] Ünal, Cahide/Şahin, İsmail, "*İstenmeyen Elektronik Postaların (SPAM) Filtrelenmesi İçin Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi*", Politeknik Dergisi, 2017, Sayı 20, s. 268

[165] Kurt, s. 71- 72; Dülger, s. 113.

Dilimizdeki karşılığı "baharatlı domuz eti ve jambon" olarak tercüme edilebilecek spamın, ABD kaynaklı "*Hormel Foods Corparation*" isimli bir şirketin ürettiği gıdalar ile ilgili kullandığı bir kısaltmadır "spiced pork and ham" sözcüklerinin baş harflerinden oluşmaktadır. İlgisiz olmasına rağmen istem dışı gönderilen elektronik postaları ifade etmek için kullanılmıştır.

Spamları gönderen kişiye spammer denilir. Her türlü ticari, ideolojik veya pornografik duyuru yapmak isteyen kişiler spammerlara başvurarak geniş kitlelere ulaşabilir. Spammerlar bu e-posta adreslerini, web siteleri, haber grupları, posta listeleri, forumlar, yeniden iletilen e-postalar, sohbet odaları gibi yerlerden temin ederler.[166] Bir ürünün pazarlanması, reklamı ve pornografik içerikli reklam veya mesajların dünya çapında geniş kitlelere ulaştırılması amacıyla spamlar kullanılmaktadır. Bu tür mesajların, bünyesinde birçok kişinin elektronik adresi bulunan çeşitli firma ve şirketlerin sahip oldukları veri tabanlarını satmalarıyla arttığı düşüncesi hakimdir.[167] Günümüzde internet üzerinden yapılan ticaretteki artış, şüphesiz ki spamların artmasına çok büyük katkı sağlamıştır.

Ülkemizde spam konusunu düzenleyen yasal bir düzenleme 2014 yılına kadar yer almamaktaydı. Elektronik Ticaretin Düzenlenmesi Hakkında Kanun ile spamlar mevzuatımıza dahil edildi. Bu kanunun 6. maddesinde kişilere ticari amaçlı gönderilen e-postalarda kişilerin önceden onayının alınması şartı getirildi. Bu onayın yazılı olması gerektiği ayrıca kanunda belirtildi. Bu kanun haricinde spamlar herhangi bir yerde bahsedilmemektedir. İstem dışı alınan elektronik postalara ilişkin mevzuatımızda özel bir düzenleme yer almamaktadır. Ancak e-postaların içeriğine göre ceza kanunlarımızdaki suç türlerine ait hükümler uygulanabilir. E-postanın içeriğinde tehdit var ise TCK 106. maddesi, hakaret var ise TCK'nın 125. maddesi, bu e-postalar, sistemi engelleyecek boyuta gelirse TCK'nın 244. maddesi, istemediğimiz halde kanun maddesindeki ifadesiyle sırf huzur ve sükunu bozmak amacıyla ısrarla e-

[166] Çakır H./Kılıç, M. S., s. 31.; Güngör, s. 71-72.

[167] Değirmenci, s. 96-98.

posta gönderilmesi halinde TCK'nın 123. maddesi, terör örgütü propagandaları varsa Terörle Mücadele Kanunu'nun ilgili hükümleri devreye girecektir.[168]

2.5.14. Dos ve Ddos Saldırıları

Dos saldırısı, bir tür hizmet aksatma yöntemidir ve bu alan içerisindeki en bilinen saldırı türüdür.[169] Bu yöntemde sisteme düzenli ve sık sık saldırılmaktadır. Hedefteki sistemin hizmet veremez duruma gelmesi veya sistemin bütün kaynaklarının sıfırlanması amaçlanır. Sunucuya durmadan istekte bulunularak hem sunucuyu hem de bilişim sistemini meşgul etme olarak açıklanabilir. Farklı yöntemlerle hizmet aksatma saldırıları gerçekleştirilmesi mümkündür. Bir markete sadece gezinmek amacıyla bir yığın insan gönderilmesi, bu insanlar yüzünden gerçek alışveriş yapmak isteyen kişilerin kalabalıktan dolayı alışverişlerini yapamaması hali örnek olarak verilebilir. Bu tür saldırılar genellikle internet alt yapısından kaynaklandığı için engellenmesi de çok zordur.[170] Bu saldırı, Dos saldırısı yapılacak olan sisteme erişilerek ardından saldırıyı yapacak olan programın yüklendiği toplu güvenlik kırma aşaması ve hedefteki sisteme saldırının yapıldığı saldırı aşaması olmak üzere iki aşamalıdır.[171]

"Ddos" saldırılarında hedef internet siteleri ve bilişim sistemlerine internet üzerinden bunların kapasitelerinin çok üzerinde taleplerde bulunarak, hedef sistemin gerçek kullanıcıların taleplerine cevap verememesine neden olmaktadır. Ddos saldırıları kimi zaman çok büyük zararlara sebep olmaktadır. 21 Ekim 2016'da bir ABD'de bir internet alan adı sağlayıcısı şirketine yapılan "Ddos" saldırısında neredeyse internetin yarısına dünya genelinde erişim sağlanamamıştır.[172] Eşzamanlı

---

[168] Yaycı, s. 34.

[169] Hekim, s. 143.

[170] Ünal, Ahmet., "*Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele"* Tombul F.; Güneştaş M.; Başıbüyük O. (Ed.), Siber Suçlar Tehditler, Farkındalık ve Mücadele, Global Politika ve Strateji, Ankara 2015, s. 14-15.

[171] http://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri (erişim tarihi 11.04.2019).

[172] Açıkgöz, s. 22.

olarak yapılan bu saldırılar, saldırının boyutunu arttıracağı gibi saldırıyı yapan kişinin gizlenmesine de imkan vermektedir. Bu işlemleri yapan araçlar "zombie" olarak anılmaktadır. Bu tür saldırı yapan failin tespiti ise çok güçtür.[173]

Dos saldırısını Ddos saldırısından ayıran en önemli fark, Dos saldırısında genelde tek bilgisayar ve tek internet bağlantısı kullanılırken, Ddos saldırılarında aynı anda birden fazla bilgisayar ve birden fazla bağlantı desteğinin olmasıdır. Bu yüzden Ddos saldırıları daha kapsamlı ve büyük olup verebileceği zararlar daha fazladır ve önlem alınmasında da bir o kadar zorluk yaşanmaktadır. Bu iki tür saldırı yöntemiyle bir bölgenin elektriğinin kesilmesi, sularının boşa akıtılması, uçakların rotalarından çıkartılması, kurumların alt yapısının çökertilmesi gibi saldırıların yapılması mümkündür. Bu durumda birçok istihbarat örgütünün dikkatini çekmektedir.[174]

2.5.15. Tavşanlar (Rabbits)

Bir bilgisayar virüsü olup adını aldıkları hayvan gibi hızla üreme özelliğine sahiptirler. Yerleştikleri sisteme gereksiz işler yapması yönünde aralıksız komut gönderirler. Hızla çoğalma özelliği veri işleme gücüne zarar vermektedir. Bu durum zamanla sistemin işlemez hale gelmesine sebep olmaktadır.[175] Zararlı etkisini göstermesi için dosyanın çalıştırılması ya da açılması gerekmez.[176]

2.5.16. Web Sayfası Hırsızlığı ve Yönlendirmesi

Bu suç işleme yönteminde, genellikle bir internet adresi almak isteyenler kurban seçilmektedir. Mağdur internet servis sağlayıcıya başvuruda bulunduğu sırada, sisteme müdahale eden bir bilgisayar korsanı veya bu bilgiye ulaşan bir internet servis sağlayıcı çalışanı tarafından kendileri veya üçüncü bir kişi adına daha hızlı

---

[173] Dülger, s. 117.

[174] Bölükbaş, Candan, "Yeni Nesil Teknolojik Silahlar: DoS/DDoS" (22 Aralık 2014), https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (erişim tarihi 11.04.2019).

[175] Değirmenci, s. 103.

[176] Henkoğlu, Türkay, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Yayınları, İstanbul 2014, s. 190.

davranılarak kaydettirilmesi ve daha sonra bu adresin yüksek ücretle satılması şeklinde gerçekleştirilir.[177]

Web sayfası yönlendirme ise, bir web sayfasına ulaşmak isteyen kullanıcının, ulaşmak istediği web sayfasına benzer şekilde hazırlanmış başka bir sayfaya yönlendirilmesi ve bu sayfada işlem yapmak isteyen kişinin kendiliğinden verdiği kullanıcı adı ve şifresine ulaşmak olarak tanımlanmaktadır.[178] Bilişim sistemleri aracığıyla işlenen dolandırıcılık suçu genel olarak bu yöntemle işlenmektedir.

2.5.17. Klavye Dinleme Sistemleri (Keylogger)

Kullanıcının klavyede basmış olduğu tuşları, basım sırasına göre bir metin dosyası içerisine yazıp daha sonra e-posta ya da uzaktan erişim yöntemiyle uzak sisteme transfer eden yazılım türüne keylogger denilmektedir.[179]

2.5.18. Sosyal Mühendislik

İnsanlar arasındaki iletişimde karşı tarafı ikna ya da başka bir şekilde yanıltıp güvenlik süreçlerini atlatma hali sosyal mühendislik olarak tanımlanabilir. Bu teknik ile normalde tanımadıkları insanlara yapmayacakları şeyleri ikna, inandırma veya hile yöntemleri kullanılarak yaptırılabilir ya da bilgi elde edilebilir.

Sosyal mühendislik dört aşamalıdır. İlk aşamada kişi, karşı taraf hakkında bilgiler toplarken ikinci aşamada, bu topladığı bilgiler doğrultusunda karşı taraf ile iletişime geçer ve bu bilgileri kullanırken aynı zamanda amacı doğrultusunda kullanabileceği araçları belirler. Üçüncü aşamada kişi artık elindeki bilgiler ile uygulamaya geçer ve istediği bilgilere ulaşır. Son aşamada artık bu bilgiler istismar edilmekte ve istenilen amaçlar gerçekleştirilmektedir.[180] Sosyal mühendislik bu yönüyle telefon dolandırıcılığı ile benzerlik göstermektedir.[181]

---

[177] Değirmenci, s. 99-100.

[178] Kurt, s. 73.

[179] İlbaş, Çığır, *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Analizi*, (Yayınlanmış Yüksek Lisans Tezi), Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara 2009, s. 29.

[180] Akarslan, Hüseyin, *Bilişim Suçları*, Seçkin Yayıncılık (2. Baskı), Ankara 2015, s. 104-105.

[181] Alp, s. 31.

2.5.19. Parola Kırma Saldırıları

Parola kırma saldırıları, bir bilgisayarda saklanan veya sisteme iletilen verilerin şifrelerini öğrenme ya da çözme işlemidir. Bu yöntem bütün tahminlerin denenmesiyle hayata geçirilmekte ve şifresini unutan insanlara yardım ettiği gibi siber suçlarda gizli verilere ulaşma imkanı sağlaması sebebiyle faillere de bilişim suçu işlemek için imkan sağlamaktadır. Bir şifreyi kırmak, basit bir şekilde düzenlenen şifreler için çok kısa bir zaman alırken, karmaşık ve içeriğinde bazı karakterler olan şifreler için ise hem daha zor olmakta hem de daha fazla zamana ihtiyaç duyulmaktadır.[182]

2.5.20. Botnet Saldırıları

Botnet, robot kelimesinin "bot"u ile network kelimesinin "net"i birleştirilerek meydana getirilmiştir. Saldırganlar farklı metotlarla bilişim sistemlerinin kontrolünü sağlarlar. Ele geçirilen bilişim sistemleri zombi (bot) ismiyle anılırlar. Botnet programı da bilişim sistemine gizlice yüklenen programlardan olup, bu program ile sisteme uzaktan erişim sağlanmaktadır. Bu işleme maruz kalmış çok sayıda cihaz birleşerek bu ağı meydana getirirler. Bu tür saldırılar ile mağdurun e-posta adresindeki kişiler, şifreler, kullanıcı adları ele geçirebilir, sosyal medya hesaplarına erişilebilir, mağdurun bilgisayarı kullanılarak ddos atakları yapılabilir. Saldırgan bu bilgileri haksız kazanç sağlamak için toplayabileceği gibi bu bilgileri satmak ya da şantaj yapmak amacı içinde de olabilir. Bu yöntemle mağdurun hesap bilgileri, şifreleri, projeleri, programları, kişisel verileri, dosyaları ele geçirilebilmektedir.[183]

Özetle, birçok bilişim sisteminin kötü amaçlar doğrultusunda tek bir noktadan yönetilmesidir.[184]

---

[182] Dülger, s. 117-118.

[183] Dülger, s. 117-118.

[184] http://www.mugla.pol.tr/fethiye/Sayfalar/Botnet-Nedir.aspx (erişim tarihi 12.04.2019).

2.6. Avrupa Konseyi Siber Suçlar Sözleşmesi

2.6.1. Sözleşmeye Olan Gereksinim ve Kabulü

Bilişim suçlarıyla mücadele konusunda uluslararası alanda şu ana kadar yapılan en etkin hukuki düzenlemenin, Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suçlar Sözleşmesi olduğu kabul edilebilir. Sözleşme, ortak bir ceza politikasının oluşturulması ile toplumun bilişim suçlarına karşı korunması, özellikle gerekli mevzuatın kabul edilmesi ve uluslararası iş birliğinin geliştirilmesi amaçlı hazırlanmıştır.[185]

Bilişim suçları, genellikle çok az masrafla çok kısa sürede işlenebilen ve büyük zararlara yol açabilen suç tipleridir.[186] Klasik suçlarda failin, suçu bir bedensel veya zihinsel emekle işlemesine karşılık, bilişim suçlarında failin bilgisayarının başında sadece tuşlara basarak belki milyonlarca kişinin etkilendiği büyük zararlara yol açması dikkate alındığında hız, kolaylık ve etki alanı dikkate alındığında aradaki fark görünecektir. Örneğin, 21 Ekim 2016'da ABD'ye karşı gerçekleştirilen Ddos saldırılarında internetin neredeyse yarısına dünya genelinde erişim sağlanamamıştır. Yine 2001 yılında Avusturya'da bir "hacker", "Maroochy Shire" bölgesinin kanalizasyon arıtma tesisine siber saldırı düzenleyerek burasının kontrolünü ele geçirmiş ve milyonlarca litre kanalizasyon suyunu parklara ve nehirlere boşaltmıştır.[187] Bu kadar kolay ve az masrafla işlenen bilişim suçlarıyla tam tersine, çok büyük emek ve masrafla mücadele edilmektedir.[188]

Bilişim suçlarının kendine özgü yapısından kaynaklanan özellikleri, bu suçlarla mücadelede ulusal anlamda alınacak önlemlerin yetersiz kalmasına neden olmaktadır. Doktrinde bu yetersiz kalışın temel sebebi olarak, bilişim suçlarının coğrafi sınır tanımaması ve çok kısa sürede işlenebilir olması gösterilmektedir Tüm

---

[185] Helvacıoğlu, s. 279.

[186] Önok, Murat; "*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği"*, Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, (Prof. Dr. Nur Centel'e Armağan), 2013, Cilt 19, Sayı 2, s. 1236.

[187] Açıkgöz, 2017 s 22

[188] Önok, s. 1236.

dünyadaki bilişim sistemlerini birbirine bağlayan internet, bilişim suçlarının işlenmesinde coğrafi sınırları ortadan kaldırmaktadır.[189] Her ne kadar klasik suçlarla mücadelede uluslararası adli yardımlaşmayı mümkün kılacak anlaşmalar bulunsa da bu antlaşmalar bilişim suçlarıyla mücadelede ihtiyacı karşılamamaktadır.[190] Bilişim suçlarında fail ile mağdur arasındaki mekân farkının bulunması klasik suçlarla kıyaslandığında zorunlu bir unsurdur denilebilir. Dolayısıyla bilişim suçları çoğu zaman bir mesafe suçu olarak işlenmektedir.[191] Öyleyse bu suçlarla mücadelede klasik suçlar için olandan farklı bir iş birliğinin bulunması kaçınılmazdır. Öte yandan farklı hukuk düzenlerinde bu suçlar açısından farklı uygulamalar söz konusudur.[192]

Söz konusu suçlar bakımından kimi hukuk düzenlerinde henüz kanuni düzenlemenin dahi yapılmamış olması failler açısından bulunmaz bir fırsattır. Failler, fiillerinin suç olarak kabul edilmediği bu ülkelere giderek dünyanın her yerine internet aracılığıyla bağlanabilmekte ve bulunduğu yerde cezai anlamda hiçbir yaptırımla karşı karşıya kalmamaktadır. Böyle bir durumda suçluların iadesi için gerekli olan çifte cezalandırılabilirlik şartı da yerine getirilmiş olmadığından failin suçun mağdurunun bulunduğu ülkeye iadesi gerçekleşmemektedir.[193]

Suçla mücadelede etkili bir adli yardımlaşma için bilişim suçları bakımından, uluslararası düzlemde herkesin kabul edebileceği bir tanım yapılmalı ve maddi ceza hukuku bakımından oluşan farklılıkları giderilmesine yönelik çalışmalar yapılmalıdır.[194]

---

[189] Önok, s. 1233–1234.

[190] Önok, s. 1234.

[191] Sokullu Akıncı, Füsun; "*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2001, Cilt 59, Sayı 1-2, s. 12.

[192] Sokullu, s. 12.

[193] Önok, s. 1236.

[194] Sokullu, s. 12.

Yukarıda izah edilmeye çalışıldığı üzere, bilişim suçlarının sınır aşan yapısı dikkate alındığında, bu suçlarla mücadelede uluslararası düzeyde ortak çalışmaların yürütülmesi zorunludur.[195] Bilişim suçları ile mücadelede Birleşmiş Milletler, Avrupa Birliği, Avrupa Konseyi, OECD, G8 gibi uluslararası kuruluşların çalışmaları mevcuttur. Bu çalışmalar içinde Avrupa Konseyi Siber Suçlar Sözleşmesini, diğer uluslararası çalışmalardan ayıran nokta, sözleşmeye taraf devletlerin, bilişim suçları bakımından kendi iç hukuklarında düzenleme yapmayı ve uluslararası adli iş birliğini taahhüt etmeleridir. Söz konusu antlaşma her ne kadar Avrupa Konseyi nezdinde imzalanmış bir antlaşma olsa da bu antlaşmaya konsey üyesi olmayan ABD, Japonya, Güney Afrika, Kanada, Avustralya ve İsrail de taraf olmuşlardır.

Avrupa Konseyi, sözleşmeyle sonuçlanan sürece, konseyin alt çalışma komitelerinden biri olan Avrupa Suç Sorunları Komitesi'nin (CDPC) 1996 yılında siber suçlarla ilgilenecek bir uzmanlar komitesi kurulmasını önermesi ile ilk adımını atmıştır. 1997 yılında Avrupa Konseyi Bakanlar Kurulu, söz konusu uzmanlar komitesini (PC–CY) kurmuş ve komiteden siber suçlarla mücadeleye ilişkin bağlayıcı özelliğe sahip bir hukuki metin hazırlamasını istemiştir.[196] Bunun üzerine komite, taslak bir metin hazırlamış ve hazırlanan bu taslak Kasım 2001'de Budapeşte'de imzaya açılmıştır. Türkiye sözleşmeyi 10.11.2010'da imzalamış, 29.09.2014'da onaylamış ve sözleşme 01.01.2015'da iç hukukumuzda yürürlüğe girmiştir. Böylelikle Türkiye sözleşmeye taraf olmuş ve bu sözleşmedeki suçları, kendi iç hukukunda düzenlemeyi taahhüt etmiştir. Burada ifade etmek gerekir ki, doktrinde ve uygulamada bu sözleşmeye "Avrupa Konseyi Siber Suçlar Sözleşmesi" denilmekte ise de Sözleşme'nin uygun bulunmasına dair kanunda tercüme "Sanal Ortamda İşlenen Suçlar Sözleşmesi" olarak yapılmıştır.[197]

---

[195] İçel, Kayıhan, "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt 59, Sayı 1-2, s. 5.

[196] Dülger, s. 198; Önok, s. 1241.

[197] Erdoğan, Yavuz, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, Legal Yayıncılık (1. Baskı), İstanbul 2018, s. 1.

Günümüz itibariyle sözleşmeyi olan ülke sayısı Avrupa Konseyi üyesi olmayan devletlerle birlikte 63' tür.[198] Avrupa Konseyi Siber Suçlar Sözleşmesi (AKSSS) bilişim suçlarına yönelik imzalanmış ilk uluslararası sözleşmedir niteliğindedir.[199] Ayrıca sözleşmeye Avrupa dışından ABD, Japonya, Kanada gibi ülkelerin de taraf olması söz konusu sözleşmenin bölgesel olmadığını, küresel bir sözleşme olduğunun göstergesidir.

2.7.2. Sözleşmenin İçeriği ve Sözleşmede Düzenlenen Suçlar

AKSSS kırk sekiz madde ve dört bölümden oluşmaktadır. Bu bölümler sırasıyla; terimler, ulusal düzeyde alınacak önlemler (maddi ceza hukuku ve usul hukuku), uluslararası iş birliği ve diğer hükümlerdir. Sözleşme temel olarak şu ana ilkeler çerçevesinde şekillenmiştir: Eylemin kasten işlenmesi ve hukuka aykırı olması; ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce, kanaat ve iletişim özgürlüğü olmak üzere temel hak ve özgürlüklerin gereklerine uyulması; bilişim suçlarının belirlenip düzenlenmesinde ortak bir asgari standarda uyulması.[200]

Terimler bölümünde; bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik verisi terimleri açıklanmıştır. Ulusal düzeyde alınacak önlemlerden maddi ceza hukukuna ilişkin kısımda taraf devletlerin hangi fiilleri cezai yaptırım altına alacağı belirlenmiştir. Usul hukukuna ilişkin kısımda ise özellikle bilişim suçlarında suç delillerine ulaşmanın ve mahkeme önünde temsil edici, bütünlüğü bozulmamış delil elde etmenin zorluğu nedeniyle ulusal hukuka rehberlik edecek hükümler ortaya konuşmuştur.[201] Uluslararası iş birliği bölümünde ise klasik suçlardan farklı olarak bilişim suçlarına özgü uluslararası adli yardımlaşmaya ilişkin hükümlerden bahsedilmiştir.

---

[198] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=bcOvBBEj (erişim tarihi : 04.07.2019)

[199] Sınar, Hasan, *Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme,* Prof. Dr. Çetin Özek Armağanı, İstanbul 2004, s. 773

[200] İçel, Kayıhan, s. 6-10.

[201] Keskin Kiziroğlu, Serap, "*Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1-2, s. 155-180.

AKSSS'de düzenlenen suç tipleri şu şekilde sıralanabilir:

- Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar (sözleşme madde 2-6): Yasadışı erişim, yasadışı araya girme, verilere müdahale, sisteme müdahale, cihazların kötüye kullanımı.

- Bilgisayarla bağlantılı suçlar: (sözleşme madde 7-8): Bilgisayarla bağlantılı sahtecilik, bilgisayarla bağlantılı dolandırıcılık.

- İçerikle bağlantılı suçlar: (sözleşme madde 9): Çocuk pornografisiyle bağlantılı suçlar

- Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar (sözleşme madde 10)

İKİNCİ BÖLÜM

YASAK CİHAZ VEYA PROGRAMLAR SUÇU

1. SUÇ TİPİNE İLİŞKİN GENEL BİLGİLER

TCK md. 245/A'da düzenlenen "Yasak Cihaz veya Programlar" başlıklı suç, 24.03.2016 tarihinde 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesinin 5. fıkrasıyla Türk Ceza Kanunu'na eklenen yeni bir suç tipidir. Anılan suça ilişkin yapılan yasal düzenleme şu şekildedir:

"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 beş bin güne kadar adli para cezası ile cezalandırılır."

Bilişim suçlarının herhangi bir cihaz, program, şifre veya güvenlik kodu kullanmadan icrası mümkün olsa da genel itibariyle bunlar suçların işlenmesini kolaylaştırdığından bilişim suçu faillerinin kullandığı önemli suç unsurlarıdır. Türk hukukunda uygulamanın ve akademik çalışmaların ana gündem maddelerinden biri haline gelen ve önemi günden güne daha net bir şekilde anlaşılan bilişim suçlarıyla, daha suçun başlangıcında tabiri caizse daha yolun başında etkin ve sonuç almaya yönelik bir mücadele gerekmektedir. Bu amacın gerçekleştirilmesi için, bilişim suçlarıyla ilgili var olan düzenlemelere ek olarak, bu suçların işlenmesini sağlayan ve kolaylaştıran çeşitli cihazların, bilgisayar programlarının, şifrelerin ve güvenlik kodlarının imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulmasının da yaptırım altına alınması zaruri bir ihtiyaçtır. Bu şekilde bilişim suçlarına hazırlık hareketi mahiyetindeki bu fiiller cezalandırılarak bilişim suçlarının işlenmesinin önüne geçilebilecektir.

Tüm bu amaçlar doğrultusunda, TCK 245/A maddesi hukuk sistemimize dahil edilmiştir.[202] Söz konusu düzenlemenin hayata geçirilmesi, bilişim suçlarıyla mücadele bakımından son derece önemlidir.

Bu düzenleme ile bilişim suçları açısından büyük bir boşluk doldurulmuş bulunmaktadır. Gelişen bilişim teknolojisi ile birlikte internet kullanımı yaygınlaşmış, bu doğrultuda bilgisayar koruma programlarının güvenlik duvarlarını kolaylıkla aşabilecek nitelikteki zararlı yazılım programları da (kötücül yazılımlar) aynı oranda artış göstermiştir. Bu zararlı yazılımlar internette çeşitli şekillerde (bir linkin açılması, bir verinin indirilmesi gibi) bilgisayar niteliği taşıyan cihazlara yerleşip bu cihazlara çeşitli şekillerde zarar vermekte ya da kullanıcının bilgisi dışında veri depolamak, veri transferi sağlamak gibi suça konu işlemleri gerçekleştirmektedirler. Bilişim teknolojileri için var olan bu ve buna benzer tehlikeler sadece yazılım programları ile değil bu teknolojilerin bir parçası olan donanım unsurları yani cihazlar yoluyla da gerçekleştirilebilmektedir. Yine çalışmamızın daha önceki aşamalarında detaylı şekilde bahsedildiği üzere bilişim suçlarının işleniş çeşitliliği her geçen gün artış göstermekte olduğundan bilişim suçlarıyla mücadelede bu suçların işlenişini kolaylaştıran veya mümkün kılan bilişim teknolojisi unsurlarına ilişkin hukuki düzenlemelere mutlak suretle ihtiyaç duyulmaktadır. Tam da bu noktada Türk Ceza Kanunu 245/A hükümleri devreye girmektedir. Kanun koyucu hem uluslararası sözleşmenin gereği olarak hem de bilişim suçlarının işlenmesinin önlenmesi için bu maddeyi kabul etmiştir. Böylece bilişim suçları açısından hazırlık hareketi niteliğinde fiillerin bağımsız suç olarak cezalandırmaya tabi tutulması sağlanmıştır. Bilişim suçlarının hazırlık hareketi mahiyetinde olduğu kabul edilen ve maddede sayılan fiillerin hukuki yaptırım altına alınması bilişim suçlarıyla mücadele noktasında olumlu bir adımdır.[203]

---

[202] Korkmaz, İbrahim, "*Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu*", Terazi Hukuk Dergisi, 2018 (Haziran), Cilt 13, Sayı 148, s. 46.

[203] Özbek, Veli Özer/Doğan, Koray/Bacaksız,Pınar/Tepe, İlker., *Türk Ceza Hukuku Özel Hükümler*, Seçkin Yayıncılık (13. Baskı), Ankara 2018, s. 1033, Akbulut, *Bilişim Alanında Suçlar*, Adalet Yayınevi (2. Baskı), Ankara 2017, s. 348

Hukuk sistematiğimize yeni giren bu suçun 245/A maddesi olarak düzenlenmiş olması sadece TCK'nın 245. maddesine ilişkin bir suç olduğu anlamı taşımamaktadır. Madde metninden de anlaşılacağı üzere bu suç, tüm bilişim suçları ve bilişim sistemlerinin araç olarak kullanıldığı suçlar için uygulama alanı bulacaktır.[204]

TCK'nın 245/A maddesi, yürürlüğe girdiği tarihten sonra gerçekleşen ve madde kapsamına giren fiiller için uygulama alanı bulacaktır. Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun maddenin yürürlüğe girdiği tarihten önce imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, verilmesi, satılması, bulundurulması başka bir suç kapsamına girmedikçe cezalandırılması söz konusu olmayacaktır. Ama aynı şahıs 24.03.2016'dan sonra da sahip olduğu cihazı, bilgisayar programını, şifreyi veya sair kodu suç işlemek amacıyla naklediyor, satıyor, depoluyor, satışa arz ediyor, ithal ediyor veya sevk ediyorsa fail hakkında TCK 245/A hükümlerinin uygulanması mümkün olacaktır.[205]

AKSSS'ne taraf devletler, "Cihazların kötüye kullanımı" başlıklı 6. maddesinde sayılan eylemleri kendi içi hukuklarında suç olarak düzenleme yükümlülüğü altındadır.

TCK 245/A maddesi, iç hukukumuzun bir parçası haline gelen Avrupa Konseyi Siber Suçlar Sözleşmesi'nin bilişim alanında suç işlenmesini kolaylaştıran cihazların kötüye kullanılmasını cezalandıran "Cihazların kötüye kullanımı" başlıklı 6. maddesinin hukuk sistemimizdeki karşılığı olarak yer almaktadır. Bir anlamda TCK 245/A'nın kabulü, uluslararası arası sözleşmeye taraf olmanın gerektirdiği yükümlülükten kaynaklanmıştır.[206]

TCK'nın md. 245/A hükümleriyle AKSSS 6. madde hükümleri karşılaştırıldığında genel itibariyle uyumlu olsalar da arada bazı farklılıklar bulunmaktadır:

---

[204] Dülger, s. 454.

[205] Akbulut, *Bilişim Alanında Suçlar*, s. 347.

[206] Koca, Mahmut/Üzülmez, İlhan, "Türk Ceza Hukuku Özel Hükümler", Adalet Yayınevi (5. Baskı), Ankara 2018, s. 912.

TCK'da ve yer alan kanunilik ilkesi gereğince hareketler tek tek sayılmıştır. Sözleşmede hareketler farklı bir şekilde kaleme alınmıştır ve "başka şekilde erişilebilir hale getirilmesi" ifadesi bulunmaktadır. Sözleşmede bu ibareyle, teknolojideki gelişmeler de kapsama dahil edilmiştir.

Sözleşmede 6. maddenin uygulanacağı suçlar, 2. maddede yer alan yasadışı erişim suçu, 3. maddede düzenlenen yasa dışı araya girme suçu, 4. maddede yer alan verilere müdahale suçu ve 5. maddede yer alan sisteme müdahale suçu ile sınırlamış durumdayken TCK daha geniş belirleme yapma yoluna giderek, bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçlar için de uygulanmasını tercih etmiştir. Böylece TCK'nın uygulama alanının AKSSS'ye kıyasla daha geniş olarak görülmektedir.

Ayrıca Sözleşmenin 6. maddesinde, taraf devletlerin cezai sorumluluğunun doğması için 1. fıkranın a bendinin i ve ii bölümlerinde söz konusu öğelerden belli sayıda bulundurulmasını şart koyabileceklerine değinilmişken inceleme konumuz olan maddede böyle bir düzenleme getirilmemiştir.

Sözleşmenin 6. maddesinde sayılan fillerin suç işlemek amacıyla gerçekleştirilmemesi durumunda kişilere cezai sorumluluğun yüklenemeyeceği belirtilmiştir. TCK'nın md. 245/A'da cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların gerçekleştirilmesi amacıyla oluşturulmasının veya yapılmasını şartından bahsedilmiştir.

Sözleşmenin 6. maddesi, şifre, erişim kodu veya benzeri veriyi, bir bilgisayar sisteminin tamamına veya herhangi bir kısmına erişimi mümkün kılan ifadeleriyle belirtmişken, TCK md. 245/A'da böyle bir sınırlama yoluna gidilmemiştir. Bu açıdan TCK md. 245/A ve sözleşme hükümleri farklılık arz etmektedir.[207]

[207] Akbulut, *Bilişim Alanında Suçlar*, s. 346-347; Korkmaz, s. 48.

Bilindiği üzere Anayasamızın 90/5 gereğince, usulüne uygun şekilde yürürlüğe giren Avrupa Konseyi Siber Suçlar Sözleşmesi kanun hükmüne haizdir. Bu noktada Sözleşmenin yürürlüğe girdiği 02.05.2014 tarihi ile inceleme konumuz olan maddenin yürürlüğe girdiği 24.03.2016 tarihleri arasında gerçekleşen eylemlere uygulanıp uygulanmayacağı önem arz eden bir husustur. Zafer'e göre ulusal bir kanunda suç olarak yer verilmese de usulüne uygun şekilde yürürlüğe girmiş olan bir uluslararası sözleşmede suç olarak düzenlenmiş bir eylemi yargılayıp cezalandırmak kanunilik ilkesine uygundur.[208] Aksi görüşteki yazarlar ise, uluslararası sözleşmeler bir kanunla uygun bulunsalar bile, ceza hukukunda doğrudan uygulanabilmeleri için bir kanunun doğrudan göndermede bulunması gerektiğini savunmaktadır.[209] AKSSS'nde bu eylem suç olarak düzenlenmiş olsa da verilecek ceza noktasında uygulanabilecek bir düzenlemeye yer verilmediğinden TCK md. 245/A'nın yürürlüğe girmesinden önceki eylemlerin cezalandırılması mümkün değildir.[210] Bizde Sözleşmede yaptırım hususunda bir hüküm bulunmadığından 24.03.2016 tarihinden önceki eylemlerin cezalandırılamayacağı kanaatindeyiz.

AKSSS'de 6. maddede sayılan eylemlerin suç işlemek amacıyla yapılmaması durumunda halinde ise ceza sorumluluğunun doğmayacağından bahsedilmiştir. Daha fazla belirliliğin sağlanması için, "bilişim sisteminin yetkilendirilmiş olarak test edilmesi ya da korunması maksadıyla suç oluşturan bir eylemin gerçekleştirilmesi halinde, tedarik etme ceza sorumluluğunu gerektirir biçimde yorumlanmamalıdır" ifadesini içeren bir hükümle suç tipinin daha açık olması için eksiklikler giderilmeye çalışılmıştır. Esasında sözleşmenin bu maddesi suçun kasten işlenilmesini ifade etmektedir. Siber Suçlar Sözleşmesine İlişkin Açıklayıcı Rapor'da bu durum "hukuka aykırılık" konusu ile ilişkilendirilmiş olsa da madde odaklanmasını kastın üzerinde göstermiştir. Bu ifadeyle, hukuka uygun işlemleri gerçekleştirmek için bu tür

---

[208] Zafer, Hamide, *Ceza Hukuku Genel Hükümler TCK m 1-75*, Beta Yayınları (6. Baskı), İstanbul 2016, s. 60.

[209] Aygün Eşitli, Ezgi, "*Suçların Ve Cezaların Kanuniliği İlkesi*", TBB Dergisi, 2013, Sayı 104, s. 233.

[210] Korkmaz, s. 47.

araçlardan yararlanan veri güvenliği alanında çalışan kişilerin korunması amaçlanmıştır.[211]

Yukarıda belirtildiği gibi bilişim suçları herhangi bir cihaz, program, şifre veya koddan yararlanmaksızın da işlenebilmekle birlikte bu tür cihaz veya program veya verilerle işlenmektedir. Hatta suç işlemede kullanılan bu araçların elde edilmesine yönelik olarak, üretim ve dağıtımları alanında "deepweb"te oluşan karaborsanın bulunduğu belirtilmektedir.[212] Nitekim bu fiilin AKSSS'nde düzenlenmesi nedenlerinden biri de bilişim suçlarını işlemek için bu tür araçların elde edilmesi kapsamında, üretim ve dağıtımlarında karaborsa oluşması endişesidir. Kötücül pazar yeri olarak isimlendirilen platformda kimin, nasıl, nerede ve ne zaman kullanacağı hususunda belli bir niyeti olmaksızın, bireyler suçta kullanılacak araçları burada satma olanağı bulabilmektedirler. Bahsi geçen madde, bilişim suçlarının kaçınılmaz bir özelliği haline gelen kötücül pazar yerlerinin büyümesinin önüne geçmek ve bilişim korsanları için araç pazarlanmasını suç haline getirmek amacıyla kabul edilmiştir.[213]

Bu noktada madde başlığına getirilen eleştirilere değinme gereği duyuyoruz. Türk Ceza Kanunu'nun sistematiğinde madde başlıklarının seçiminde suçun eylem unsuru ön plana çıkartılmaktadır. TCK 245/A maddesinin başlığı "yasak cihaz ve programlar" olarak seçilmiştir. Bu madde başlığı suçun maddi konusunu ifade etmekte olup maddenin içeriğine ilişkin herhangi bir ön izlenim oluşmasına imkan vermemektedir. Ayrıca suçun maddi konusunu oluşturan cihaz ve programların yasaklı olduğu belirtilmesine rağmen madde metninde bu cihaz ve programların yasaklı olduğuna ilişkin bir ibare bulunmamaktadır. Bir cihaz veya programın yasaklı kabul edilmesi için o cihaz veya program için önceden verilmiş bir yasaklama kararı olması gerekmektedir. Oysa madde metninde yasaklı veya yasaklı olmayan ayrımı yapılmadan bilişim suçlarının işlenmesinde kullanılan cihaz ve programlar esas

---

[211] Dülger, s. 453.

[212] https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zararli-yazilim-imal-etme-bulundurma-sucu.html (erişim tarihi 22.04.2019).

[213] Dülger, s. 453-454.

alınmıştır. Sürekli gelişen bilişim teknolojisi dikkate alındığında böyle bir yasaklı cihaz ve program listesinin önceden hazırlanması mümkün olmadığı gibi bilişim suçlarıyla mücadele açısından uygun da değildir. Çalışmamıza konu olan maddenin ortaya çıkışı da bu hususlara dayanmaktadır. Özetlemek gerekirse madde başlığı bu haliyle maddenin içeriğini tam ve doğru olarak ortaya koyamamaktadır. Madde başlığının, yasak cihaz ve programların kullanıldığı bütün bilişim suçlarını ve madde metninde sayılan seçimlik hareketlerin tümünü kapsaması adına "suçta kullanılacak cihaz ve programların üretilmesi, yayılması ve bulundurulması" şeklinde olması önerilmektedir.[214]

Akbulut da eleştirilere katıldığını belirterek madde başlığının TCK md. 245'deki gibi "Program veya Cihazların Kötüye Kullanılması" şeklinde tercih edilmesinin daha uygun olacağını dile getirmiştir.[215] Korkmaz da benzer gerekçelerle madde başlığının "cihaz, program, şifre ve güvenlik kodlarının bilişim suçlarının işlenmesi amacıyla bulundurulması, imal ve ticareti suçu" olarak değiştirilmesinin daha uygun olacağını ifade etmiştir.[216] Biz de madde içeriğini tam ve doğru yansıtmaktan uzak olan bu başlığın tercih edilmesini eleştirmekte ve madde başlığının "cihaz, program, şifre veya güvenlik kodlarının bilişim suçlarının işlenmesi amacıyla üretilmesi, yayılması ve bulundurulması" şeklinde düzenlenmesinin daha yerinde olacağı kanaatindeyiz.

Koca/Üzülmez' de formülasyonunun yanlış olduğunu, düzenlemenin şu şekilde yapılması gerektiğini belirtmiştir: 'Bu bölümde düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesinde kullanmak amacıyla bir cihazı, bilgisayar programını, şifre ve güvenlik kodlarını üreten, ithal eden, temin eden, satan, satışa arz eden, satın alan veya bulunduran kişi

---

[214] Özbek/Doğan/Bacaksız/Tepe., s. 1034.

[215] Akbulut, *Bilişim Alanında Suçlar*, s. 34-38.

[216] Korkmaz, s. 49.

... cezalandırılır."[217] Dülger de yazarların bu görüşüne ve suç tanımına katıldığını beyan etmiştir.[218]

TCK md. 245/A ile benzerlik içeren suç tipleri Birleşik Krallık, ABD ve Kanada'da hukuk sistemlerinde yer almaktadır. Örneğin Birleşik Krallık hukukunda dolandırıcılık suçu açısından, dolandırıcılık eyleminde kullanılmak üzere bir aracın taşınması ya da tedarik edilmesi veya hileli bir biçimde elektronik iletişim hizmetlerinden yararlanmayı sağlayan araçların bulundurulması veya tedarik edilmesi suç olarak düzenlenmiştir. Sahtekarlık suçunda ise, belirli bir aracın yapılması için özellikle dizayn edilen ya da uyarlanan bir "makine, alet, belge ya da herhangi bir materyalin" yapılması, bulundurulması ya da kontrol altında bulundurulması yaptırım altına alınmıştır. Fikri mülkiyet hukukunda, teknolojik koruma önlemlerinden kurtulmak için dizayn edilmiş araçların tedarik edilmesi suçtur. Benzer şekilde, bilişim hukukunda da bilişim sistemlerinin bütünlüğü açısından suç işlemek için dizayn edilen araçların bulundurulması ve tedarik edilmesi suç olarak kabul edilmiştir.

ABD federal hukukuna göre, söz konusu madde, tüm kategorilerdeki bilgisayar ve siber suçları kapsayacak şekilde, "erişim araçlarını" dolandırıcılıkta kullanılması için oluşturulmuştur ve geniş bir biçimde şu şekilde tanımlanmıştır: "para, mal, hizmet veya değeri olan herhangi bir şeyi sağlamak için veya para fonlarının aktarımında kullanmak için (yalnızca kağıt belge ile yapılan aktarımlardan farklı olarak); birlikte yada tek başına erişim sağlayan; herhangi bir kart, plaka, kod, hesap numarası, elektronik seri numarası, mobil araç tanımlama numarası veya diğer telekomünikasyon hizmeti, donanımı veya tanımlayıcı aleti veya hesaba erişimde kullanılabilecek diğer araçlar ." Bu tür bir aracın üretilmesi, ticaretinin yapılması, kullanılması ve bulundurulması karşılığında yirmi yıla kadar hapis cezası öngörülmüştür.[219]

---

[217] Koca/Üzülmez*, Özel Hükümler* s. 912.

[218] Dülger, s. 453.

[219] Dülger, s. 453.

2. KORUNAN HUKUKİ DEĞER

Korunan hukuki değer kavramı, gerçekleştirilen eylemin, hukuk düzeninde doğrudan doğruya ihlal ettiği hukuki varlık ya da değeri ifade etmek için kullanılır.[220] Hukuki değer, aynı zamanda sosyal düzenin sürekliliğine yönelik manevi değerler olarak kabul edilir.[221]

Ceza kanunlarında suç olarak tanımlanan bir eylemin gerçekleştirilmesiyle bir hukuki değerin ihlali kaçınılmaz olduğundan, bir hukuki değerle ilişkilendirilemeyen suçtan söz edilmesi mümkün değildir.[222] Suç oluşturan eylemleri yaptırıma bağlayan ceza hükümleri bu suretle bir ya da birden fazla hukuki değeri korumayı amaçlamıştır.[223] Çalışmamıza konu madde, TCK'nın topluma karşı suçlar kısmının bilişim alanında suçlar bölümünde kendisine yer bulmuştur.

Bölüm başlığının, kapsayıcı olması için bilişim alanında suçlar şeklinde düzenlenmesi yoluna gidilmiştir.[224] Bu bölümdeki suçlarda korunan hukuki değerin karma nitelik taşıdığı kabul edilmektedir. Şöyle ki; bu bölümdeki suçlar için korunan özel bir hukuki değerin yanında toplumun bilişim sistemlerinin doğru işleyeceğine ilişkin güven duygusu da koruma altına alınmıştır. Bu suçların topluma karşı suçlar kısmında düzenlenmesinin asıl nedeni de toplumun bu güven duygusunun korunmak istenmesidir. Elbette ki "bilişim alanında suçlar" ifadesinin korunan hukuki değere göre değil, suçun işleneceği alana göre yapılan bir isimlendirme olduğunun da unutulmaması gerekmektedir.[225]

---

[220] Artuk/Gökcen/Yenidünya, s. 285; Zafer, s. 148.

[221] Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2016, s. 159.

[222] Ünver, Yener, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Seçkin Yayıncılık, Ankara 2003, s. 614.

[223] Soyaslan, Doğan, *Ceza Hukuku Özel Hükümler*, Yetkin Yayınları, 8. Baskı, Ankara 2010. s. 237.

[224] Koca/Üzülmez, *Özel Hükümler,* s. 843.

[225] Koca/Üzülmez, *Özel Hükümler*, s. 844.

Bu kapsamda biz de TCK'nın 245/A maddesiyle karma nitelikte bir hukuki değerin korunmaya çalışıldığı kanaatindeyiz. Bu madde ile bilişim suçlarının icrası kapsamındaki hazırlık hareketlerinin cezalandırılması suretiyle toplumsal menfaat dikkate alınarak bilişim sistemlerinin güvenliğinin ve güvenilirliğinin korunması amaçlanmıştır. Ayrıca maddenin kapsamına diğer suçlarla korunan hukuki değerler de bu madde kapsamında güvenceye alınmak istenmiştir. Örneğin bilişim sistemine girme suçunda, bir yandan kişilerin özel hayatlarının gizliliği ve haberleşme özgürlükleri korunurken diğer yandan toplumda bilişim sistemlerinin doğru işleyeceğine dair güvenin korunması amaçlanmıştır.[226]

3. SUÇUN UNSURLARI

Suç tipe uygun hukuka aykırı haksızlık şeklinde tanımlanmaktadır. Daha geniş bir tanımda ise, suç insanların toplumda birlikte yaşamalarının sağlanması için zorunlu olan hukuksal değerleri ihlal eden belli insan davranışları olarak açıklanmaktadır. Suçun unsurları konusunda doktrinde farklı ayrımlar bulunmaktadır.[227] 5237 sayılı TCK'da kabul edilen suç teorisinde ise suçun iki unsuru bulunduğunu söyleyebiliriz. Bu unsurlar "Tipiklik ve Hukuka Aykırılık" olarak ifade edilmektedir.[228]

Suçun unsurlarını maddi unsur, manevi unsur ve hukuka aykırılık unsuru sınıflandıran görüşler de mevcuttur. Yukarıda yaptığımız ikili ayrım ile bu ayrım arasında bir fark yoktur. Çünkü ikili sınıflandırmada tipikliğin altında suçun objektif (maddi) ve sübjektif (manevi) unsurları üçlü sınıflandırmadaki aynı içerikle incelenir.[229] Biz de yukarıdaki bilgiler ışığında suçun unsurlarını ikili ayrıma tabi tutarak "tipiklik ve hukuka aykırılık" şeklinde bu iki başlık altında inceleyeceğiz. Bu

---

[226] Yenidünya, A. C, *Bilişim Sistemine Hukuka Aykırı Erişim Suçu*.

[227] Artuk,M.Emin/Gökcen,Ahmet/M.Emin,Alşahin/Çakır,Kerim *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi (12. Baskı) Ankara 2018, s. 206-221

[228] Artuk/Gökcen/Alşahin/ Çakır, s. 221

[229] Dülger, s. 231.

ölümün sonunda inceleme konumuz olan suçu genel hatlarıyla inceledikten sonra suçun nitelikli hallerine de değerlendirmeye çalışacağız.

3.1. Tipiklik

Tipiklik, "tipe uygunluk, tipe uygun eylem" anlamında kullanılmaktadır. TCK'da bu ifade yerine suçun kanuni tanımı ifadesi tercih edilmiştir. TCK'nın 21. maddesinde de tipikliğin unsurları anlamında "suçun kanuni tanımındaki unsurlar" ifadesine yer verildiği görülmektedir.[230]

Tipiklik konusunda kabul gören en yaygın ayrımda tipikliği objektif (nesnel) ve sübjektif (öznel) unsurlara ayrılarak incelenmektedir. Bu kavramlar öğretide maddi unsur ve manevi unsur olarak karşılık bulmaktadır. TCK'nın md. 30/1.'de "suçun kanuni tanımındaki maddi unsurları bilmemekten" bahsedilmiştir. Görüldüğü üzere suçun kanuni tanımındaki unsurların maddi ve manevi unsur olarak ikiye ayrılarak incelenmesi TCK'nın kabul ettiği suç teorisi ile örtüşmektedir.[231]

3.1.1. Tipikliğin Maddi (Objektif) Unsurları

Tipikliğin maddi (objektif) unsuru ile, duyularla kavranabilen durumlar ve olgular, özetle suçun dış dünyadaki görünüş biçimi ifade edilmek istenmiştir.[232] Çalışmamız kapsamında tipikliğin maddi unsurları; fail, mağdur, suçun konusu, fiil ve netice olarak incelenecektir.

3.1.1.1. Fail

TCK 37. maddesinde failin, suçun yasal tanımındaki fiili icra eden kişi olduğu belirtilmiştir. Hukuk sistemimizde ancak gerçek bir gerçek kişinin suçun faili olabileceği kabul edilmiştir.

---

[230] Artuk/Gökçen/Alşahin/Çakır, s. 223.

[231] Dülger, s. 232.

[232] Artuk/Gökcen/Alşahin/Çakır, s. 232

Gerçek kişilerin icra ettikleri fiillerden dolayı tüzel kişiler cezalandırılamaz. Anayasamızda md. 38/7'de "ceza sorumluluğu şahsidir." denilerek bu husus hukuki düzenlemeye kavuşturulmuştur.[233]

Bilindiği üzere her suçun mutlaka bir faili olmak zorundadır.[234] Genel olarak suçların herkes tarafından işlenebileceği kabul edilmektedir.[235] Bazı suçların icrası için failin özel bir yükümlülük altında bulunması ve belli vasıfları taşıması aranmıştır. Bu suçlar için özgü suç veya mahsus suç ifadeleri kullanılmaktadır.[236] Bu bağlamda bilişim suçları ile ilgili sıkça telaffuz edilen "hacker" kavramı önem arz etmektedir. Hacker kavramına çalışmamızın önceki aşamalarında değinilmişti. Toplumun genelinde ve bilişim suçlarıyla ilgilenen kesimlerce bilişim suçlarını işleyen kişiler "hacker" olarak ifade edilmektedir. Bu durum, bilişim suçlarının yalnızca "hacker" olarak tanımlanan kişilerce işlenebileceği sonucunu doğurmamalıdır.

Tüzel kişilerin suç faili olamayacaklarından yukarıda bahsedilmişti. Ancak TCK md. 20/2'de, bunlar hakkında güvenlik tedbirine hükmedilebileceği belirtilmiştir. Çalışmamızın ilerleyen bölümlerinde, tüzel kişiler güvenlik tedbirlerinin düzenleyen TCK 246. maddesinden detaylı şekilde bahsedilecektir.

Fail kavramına ilişkin bu genel bilgiler ışığında;

TCK md. 245/A'da düzenlenen suçun faili herkes olabilir. Failin bir özelliğe sahip olması aranmaz. TCK 245/A'da belirtilen suçları işlemek üzere hazırlanmış cihaz, bilgisayar programı, şifre veya güvenlik kodu ile maddede sayılan fiilleri gerçekleştiren kişiler bu suçu işleyebilecek olup, bilgisayar ya da bilişim alanında uzman olmaları şartı aranmamıştır. Bu suç bazı seçimlik hareketler bakımından çok

---

[233] Hafızoğulları, Zeki/Özen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2015, s. 349.

[234] Soyaslan, s. 231, Toroslu, Nevzat/Toroslu, Haluk, *Ceza Hukuku Genel Kısım*, Savaş Yayınevi, Ankara 2016, s. 105; Zafer, s. 151.

[235] Özgenç, s. 191; Soyaslan, s. 231; Toroslu N./Toroslu H., s. 105.

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

failli bir suç özelliği taşımaktadır. Suçun konusunu oluşturan cihazları satan, başkalarına veren kişilerin karşısında, bunları satın alan veya kabul eden kişilerin bulunması zorunludur. Kanunda bu hareketleri gerçekleştiren herkesin suçun faili olarak cezalandırılacağı hüküm altına alınmıştır.[237]

3.1.1.2. Mağdur

Aksini savunanlar olsa da her suçun bir mağdurunun olması gerektiği kabul edilmektedir.[238] Suçun konusunun ait olduğu kişi veya kişiler mağdur olarak kabul edilir. [239] Tipik hareketin gerçekleştirilmesiyle suçun konusunun zarara uğratılması veya tehlikeye maruz kalması halinde ihlal edilen hukuki değerin sahibi mağdur olarak tanımlanabilir. Bu noktada suç oluşturan davranışın, üzerinde gerçekleştirildiği kişi veya şey şeklindeki tanımlama suçun konusunu açıklama da bize yardımcı olacaktır.[240]

Burada dikkat edilmesi gereken bir husus da suçun konusunun belli kişi veya kişilere ait olması durumudur. Bu durumda mağdur bu kişi veya kişiler olarak kabul edilecektir. Ancak eğer suçun konusunun sahibi belli kişi veya kişiler değil de toplumu oluşturan herkes ise bu durum toplumu oluşturan herkesin bu suçun mağduru olması sonucunu doğuracaktır.[241] Suçun mağduru ancak gerçek kişiler olabilir.[242] Tüzel kişiler veya tüzel kişiliğe haiz olmamakla birlikte hukuki topluluklar, mağdur olarak nitelendirilmezler.[243] Mağdur sıfatı ancak hareketin veya suçun üzerinde icra edildiği şeyin sahibi olan kişilere verilir. Doktrinde, tüzel kişilerin suçun mağduru

---

[237] Akbulut, *Bilişim Alanında Suçlar*, s. 351; Koca/Üzülmez, *Özel Hükümler* s. 913.

[238] Zafer, s.154; Artuk/Gökcen/Alşahin/Çakır, s. 312.

[239] Özgenç, s. 202; Artuk/Gökcen/Alşahin/ Çakır, s. 312

[240] Soyaslan, s. 233.

[241] Özgenç, s. 203-204, Artuk/Gökcen/Alşahin/ Çakır, s. 314.

[242] Akbulut, Berrin, *Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2016, s. 337, Artuk/Gökcen/Alşahin/ Çakır, s. 312.

[243] Artuk/Gökcen/Alşahin/ Çakır, s. 313, Akbulut, *Genel Hükümler*, s. 337

olamayacağının kabul edilmesi halinde, mağduru belli kişi veya kişiler olmayan suçlar bakımından, toplumu oluşturan bireylerin her birinin suçun mağduru olacağı yönünde fikirler bulunmaktadır.[244] Topluma karşı işlenen suçların mağdurunun belli kişi veya kişiler olmadığına yukarıda değinilmişti.

TCK 245/A'da düzenlenen suçta mağdur sıfatı bakımından da herhangi bir özellik aranmamıştır. Bu suçla bilişim suçlarının hazırlık hareketi niteliğindeki fiiller cezalandırılmaktadır. Belirli bir kişiye yönelik bir saldırı gerçekleştirilmemektedir. Dolayısıyla belirli bir kişi veya kişiler zarar görmemektedir. Tüm bu bilgiler ışığında TCK md. 245/A'da yer alan suçun henüz belirlenebilir mağdurun mevcut olmadığı gerçeği görülecektir. Bu kapsamda toplumu oluşturan herkes mağdur konumunda olacaktır. [245]

3.1.1.3. Suçun Konusu

Gerçekleşen her suçun bir konusu olmak zorundadır,[246] bu da konu tipik hareketin üzerinde icra edildiği, kişi veya şeyin maddi yapısını ifade eder.[247] Suçun konusunun, her zaman maddi bir bütünlük arz etmesi aranmaz.[248] Konusu şeref, soy bağı, bilişim sistemi verisi olan suçlar bu duruma örnek olarak gösterilebilir.[249]

Korunan hukuki değer ile suçun konusu kavramlarının farkına değinmek gerekmektedir.[250] Hukuki değer, eylemle ihlale uğrayan hukuki varlık ve menfaati tanımlamaya yardımcı olurken; suçun konusu ise, suça sebep olan hareketin yönelik olduğu kişi veya şeyi açıklamak için kullanılır.[251] Bu bağlamda, tipik hareketin

---

[244] Artuk/Gökcen/Alşahin/ Çakır, s. 314; Özgenç, s. 203-204.

[245] Dülger, s. 456; Akbulut, *Bilişim Alanında Suçlar*, s. 350; Koca/Üzülmez, *Özel Hükümler*, s. 913; Gül, Ahmet, *Doğrudan-Dolaylı Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2018, s. 240.

[246] Koca, Mahmut/Üzülmez, İlhan, *Türk Ceza Hukuku Genel Hükümler*, Ankara 2016., s. 111.

[247] Akbulut, *Genel Hükümler*, s. 338; Artuk/Gökcen/Alşahin/ Çakır, s. 316.

[248] Akbulut, *Genel Hükümler*, s. 338.

[249] Açıkgöz, s. 56.

[250] Özgenç, s. 199.

[251] Artuk/Gökcen/Alşahin/ Çakır, s. 316

gerçekleştirilmesi ile suçun konusunun zarara uğratılması veya konu bakımından tehlikeye neden olunması halinde korunan hukuki değerin ihlal edilmiş olacağını söyleyebiliriz.[252]

TCK 245/A maddesinde düzenlenen suçun maddi konusu madde metninde belirtildiği üzere, münhasıran bu bilişim alanında düzenlenen suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle suç işlenmesi için yapılmış ya da oluşturulmuş olan cihaz, bilgisayar programı, şifre ve sair güvenlik kodu olarak belirlenmiştir. Burada günümüz bilişim dünyası için öneme haiz bir konuya değinme gereği duymaktayız. Bu kavramlar söz konusu suçların gerçekleştirilmesi amacıyla meydana getirilmemişse TCK md. 245/A hükümleri uygulanmayacaktır. Çalışmamızın ilerleyen bölümlerinde detaylı şekilde değinilecek olan pentest (sızma/zafiyet) adı verilen testlerle bilişim sistemlerinin güvenliği belirli aralıkla denetlenmektedir. Bu kavramlar sisteminin güvenliğinin test edilmesi veya korunması maksadıyla meydana getirilmiş ise herhangi bir suç gerçekleşmeyecektir.[253] Bu durum AKSSS'nin 6. maddesinin 2. fıkrasında açık bir şekilde düzenlenmiştir.

Ayrıca AKSSS'nin 6. maddesinde, Sözleşmenin 2 ile 5. maddelerinde belirtilmiş herhangi bir suçun işlenmesi için kullanımları amacıyla üretimi ve diğer eylemlerin gerçekleştirilmesi şartı öngörülmüştür. Sözleşme taslağı düzenlenirken münhasıran suç işlemek üzere tasarlanmış cihazlarla sınırlı tutulması tartışılmış, bunun kapsamının çok dar olacağı fikrine varılmış, ancak bütün cihazların kapsam dahiline alınması da kabul edilmemiştir.[254]

Bu kavramlara sırasıyla değinelim:

---

[252] Özgenç, s. 199.

[253] Akbulut, *Bilişim Alanında Suçlar*, s. 354; Koca/Üzülmez, *Özel Hükümler*, s. 914; Dülger, s. 459; Korkmaz, s. 49

[254] Akbulut, *Bilişim Alanında Suçlar*, s. 354; Sokullu, s. 23.

3.1.1.3.1. Cihaz

Cihaz, AKSSS'de ayrıntılı bir şekilde tanımlanmamaktadır. Ancak sözleşmenin 1(a) maddesinde bilişim sisteminin tanımlanmasında, cihaz kavramından bahsedilmiştir.[255] Sözleşmeye ilişkin Açıklayıcı Rapor" da ise bir cihazın "dijital verilerin kendiliğinden işletilebilmesi için geliştirilen donanım ya da yazılımdan" oluştuğunu belirtilmiştir.[256] Sözleşmenin, donanım ile yazılım arasında bir ayrım yaptığı açıktır. Buna karşın bir bilgisayar yazılımı açıkça verinin özel bir görünümü olup bu durum potansiyel bir karışıklığa sebebiyet vermektedir. Bu nedenle TCK'da bu hüküm düzenlenirken suçun konusu oluşturabilecek hususların tek tek sayılması yoluna gidilmiştir.[257] Suçun konusunu oluşturan cihazın bir donanım unsuru olması ve fiziksel bir varlığının bulunması zorunludur. Çalışmaya konu suç bir bilişim suçu tipi olduğundan bu fiziksel varlığın bilişim teknolojileri bağlamında değerlendirmesi yapılması gerektiğinden bu fiziksel varlık donanım unsuru olarak kabul edilmelidir. Suç konusunu oluşturan cihaz, suça konu bilişim sistemine eklenebilir, bağlanabilir veya ihtiyaç halinde yeniden çıkarılabilir özelliklere sahip ve bilişim suçları ile bilişim suçlarının araç olarak kullanıldığı suçların işlenmesine elverişli fiziki parçalardır. Cihazın bilişim sistemine mutlak surette bağlı olması aranmaz. Suçun oluşabilmesi için cihazın maddede belirtilen herhangi bir suçun işlenmesinde kullanmak amacıyla tasarlanmış veya uyarlanmış olması şartı aranmaktadır.[258]

Söz konusu cihazın suça konu cihaz olup olmadığının tespiti yapılırken cihazın yapılış ve hazırlanış şekli değerlendirilerek amaca bakılması gerekmektedir.[259]

---

[255] AKSSS md. 1(a): bilgisayar sistemi, bir veya birden fazlası, bir program uyarınca otomatik veri işleyebilen herhangi bir cihaz veya birbiriyle bağlantılı veya ilgili bir grup cihazı ifade eder, bkz. (erişim tarihi 16.04.2019)

[256] AKSSS'ne İlişkin Açıklayıcı Rapor pn. 23.

[257] AKSSS'ne İlişkin Açıklayıcı Rapor pn. 23.

[258] Özbek/Doğan/Bacaksız/Tepe, s. 1035; Koca/Üzülmez, *Özel Hükümler*, s. 914; Akbulut, *Bilişim Alanında Suçlar*, s. 350.

[259] Gül, s. 240.

Dülger de cihazın, her türlü donanım olabileceğini, ATM'lere kredi kartı bilgilerini kopyalamak için takılan aygıtlardan, POS cihazı benzeri kredi kartı bilgilerini kopyalayan cihazlara kadar tümünün bu kapsamda olduğunu belirtmiştir.[260]

Cihaz kavramına verilebilecek en güzel örneklerden biri skimmer isimli ATM'lerde kullanılan, banka veya kredi kartı bilgilerini kopyalayan cihazlardır. Skimming olarak tabir edilen bu cihaz ATM'lerde kart girişinin yapılacağı bölmeye önceden yerleştirilen ve "skimmer" olarak isimlendirilen kart okuyucuları kullanıcının kartı ATM makinesine yerleştirmesiyle kartın manyetik bölümündeki tüm bilgileri tarayarak kaydeder. Sonrasında ise skimmer cihazıyla kaydedilen verilerin bilgisayar, başka cihaz veya programlar vasıtasıyla boş kartlara yüklenmesi işlemi gerçekleştirilir ve bu suretle sahte banka ve kredi kartları üretilebilmektedir. Bu cihaz sadece kart manyetiğinde yer alan bilgileri kopyaladığından, sahte klavye[261] ya da klavyeye odaklanmış ATM üzerine gizlenmiş bir kamera kullanmak suretiyle failler şifrenin ele geçirilmesi için ayrı bir yöntem izlemektedirler.[262]

Yine bilişim suçları alanında sıklıkla kullanılan ve kart bilgilerini kopyalamaya yarayan encoder isimli cihaz da örnek olarak verilebilir. Kodlayıcı (encoder), kart bilgilerini boş kartın arkasındaki manyetik şeride yükleyerek sahte kredi kartı üretilmesine imkan sağlar.[263] Reader ise suç jargonunda papağan diye anılan ve kibrit kutusu büyüklüğünde bir cihaza verilen isimdir. Bu araç, kredi kartı içindeki tüm verilerin kopyalanmasını sağlayarak kredi kartı sahteciliği suçunun işlenmesini kolaylaştırmaktadır.[264] Suça konu cihazların ileri teknoloji ürünü olan

---

[260] Dülger, s. 457.

[261] PINPAD, "PIN pedi veya PIN giriş cihazı, kart sahibinin kişisel kimlik numarasını kabul etmek ve şifrelemek için borç, kredi veya akıllı kart tabanlı işlemlerde kullanılan elektronik cihaz' olarak ifade edilebilir." Bkz. https://www.google.com/search?q=p%C4%B1npad+nedir&rlz=1C1GCEU_trTR821TR821&oq=PINPAD+&aqs=chrome.0.69i59j35i39j69i57j0l3.5456j0j8&sourceid=chrome&ie=UTF-8 (erişim tarihi 21.04.2019).

[262] Akbulut, *Bilişim Alanında Suçlar*, s. 351

[263] Akbulut, *Bilişim Alanında Suçlar*, s. 351.

[264] Akbulut, *Bilişim Alanında Suçlar*, s. 351.

cihazlar olması gerekmez. Sadece madde metninde sayılan fiilleri gerçekleştirebilecek özelliklere sahip olması, bir anlamda bu sayılan fiilleri gerçekleştirmeye özgülenmiş olması yeterlidir. Gizli kameraların suça konu cihazlar arasında olmayacağı düşünülse de ATM'lerde kart kullanıcısının şifresini kaydedebilecek şekilde dizayn edilmesi halinde TCK 245/A kapsamındaki cihazlar arasında kabul edilebileceği değerlendirilmektedir.[265]

Türkiye'de polis ekipleri şüphelileri, ilk defa rastlanılan ve tespiti güç "Deep Insert Skimmer" adı verilen kart kopyalayan makineyi kullanamadan yakalamışlar ve bu olay basına yansımıştır.[266] Failler bu cihazı ATM'lerde denemek için yerleştirirken güvenlik kameraları aracılığıyla tespit edilmiş ve yakalanmaları sağlanmıştır. Yaklaşık 6,5 cm olan "Deep Insert Skimmer" isimli düzeneğin bankamatiklere kolay yerleştirildiği ve fark edilmesinin çok zor olduğu değerlendirilmektedir.[267]

Yukarıda teknolojik gelişmelerin bilişim suçu failleri tarafından kötüye kullanıldığı ve bir takım suç boyutuna ulaşan yol açtığına işaret etmeye çalıştık. Bu noktada böcek diye tabir edilen cihazlar da önem arz etmektedir. Böcek; ortam dinleme ve izleme amaçlı, mekanda bulunan kişilerden habersiz ve gizli bir şekilde konumlandırılmış, havadan yayın yapan tüm kablolu veya kablosuz, görüntü ve ses aktarımı yapan casus sistemlere verilen ortak isimdir. Böcekler kullanılarak mesafe bağımsız yayınları, kapalı devre ya da gerçek zamanlı kayıtların izlenmesi ve dinlenmesi mümkündür. GSM ve IP tabanlı gizlenmiş kamera veya dinleme cihazları dünyanın her noktasından insanların özel hayatına dair ihlallerin yapılması noktasında ciddi bir tehdit oluşturmaktadır.[268]

Öğrencilerin ders kaydı yapması, ebeveynlerin çocuklarını koruması, şirket bilgilerinin dışarıya sızmasını önlemek gibi yararlı özellikler amacıyla da

---

[265] Özbek/Doğan/Bacaksız/Tepe, s. 1035.

[266] http://finans.mynet.com/haber/detay/ekonomi/kart-dolandiricilari-yeni-kopyalama-yontemi-deep-insert-skimmer/129517/ (erişim tarihi: 16.04.2019)

[267] Akbulut, *Bilişim Alanında Suçlar*, s. 351.

[268] http://www.bocekarama.com/ (erişim tarihi 21.04.2019).

kullanılabilmesi mümkün olan cihazların bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda TCK md. 245/A hükümlerinin uygulanacağı kanaatindeyiz.

Sinyal kesici cihaz olarak bilinen jammer cihazı ile hız sınırlarının aşılıp aşılmadığını, tespit etmekte kullanılan cihazlara ilişkin olarak çalışmamızın içtima bölümünde detaylı şekilde bilgilendirme yapılmıştır.

3.1.1.3.2. Program

TCK md. 245/A'da düzenlenen suçun bir diğer konusu da bilgisayar programlarıdır. Program, bilgisayar aracılığıyla çalıştırıldığında bilgisayarın bilgi işlemesini veya belirli bir işlemi gerçekleştirmesini sağlayan kodlanmış talimatlar ya da bildirileri temsil eden sıralı bilgiler topluluğudur.[269] Bilgisayarın istenilen şekilde çalışmasına yardımcı olduğu gibi kullanıcı ile bilgisayarın iletişiminde köprü vazifesi görür. Bilgisayarın kullanıcısı tarafından istenilen şekilde çalışması ve denetlenmesinde rol almaktadır. Programlar bilgisayarın soyut tarafını oluştururlar.[270]

Bilgisayar programları, üç başlık altında sınıflandırabiliriz:

İlki, sisteme kendi kendisini nasıl çalıştıracağını anlatan sistem programlarıdır. İkicisi ise diğer programlama dilleri ile hazırlanan ve makinenin anlamadığı programları, bilgisayarın anlayacağı dile dönüştüren çevirici programlarıdır. Üçüncü sırada ise kullanıcıların özel işlerinin yapılması maksadı taşıyan uygulama programları bulunmaktadır.[271] Bu noktada yazılım ve program kavramlarının farkından bahsetmek istiyoruz.

Yazılım program içerisinde farklı görevleri gerçekleştirmek için kullanılırken, programların her biri belirli bir işi yerine getirmek üzere kodlanır. Yazılımlar programları, kodları, komutları ve yardımcı programları içerir. Özetle

[269] Yazıcıoğlu, s. 31.

[270] Kurt, s. 39.

[271] Yenidünya/Değirmenci, s. 47.

yazılım programlar topluluğundan oluşmaktadır. Her bir programın yazılıma ait bir unsurdur. Her program bir yazılım iken her yazılım bir program değildir.[272]

TCK 245/A anlamında program ile verileri değiştirmeye, imha etmeye, sistemlerin işletimine müdahale etmeye yönelik ya da bilgisayar sistemlerine erişim sağlamak için tasarımlanmış yahut da ya da bu amaca uygun hale getirilmiş programlar kastedilmiştir.[273] Bu programlar, başkasına ait bilgisayarı ele geçirmek, şifresini kırmak, bilgilerini öğrenmek gibi amaçlarla kullanılmaktadırlar. Esasında programlar bunu da İngilizce malware (kötücül) software (yazılım), kelimelerinin kısaltılmışı malware olan kötücül (zararlı) yazılım programları ile gerçekleştirirler.[274]

Bu zararlı yazılımlar ile; e-posta hesapları, banka şifreleri ve diğer kişisel bilgilerin çalınması, işletim sistemi veya diğer programların çalışmaması, hatalı çalışması mümkün olabilmektedir. Bilgisayardaki dosya ve klasörlerin silinmesi, kopyalanması, yerlerinin değiştirilmesi veya yeni dosyaların eklenmesi mümkün olmaktadır. Yine bu zararlı yazılımlar ile klavye ve mouse (fare) ile yapılan her şey kaydedilebilmekte, ekranda can sıkıcı veya kötü amaçlı web sitelerine yönlendiren açılır pencereler oluşturulabilmekte, tüm verisiyle diskler silinebilmekte, hatta biçimlendirebilmektedir. Başka zararlı programların bulaşmasını sağlanabilmekte, bilgisayarınız üzerinden başkalarına saldırabilmekte, bilgisayarınızın kaynaklarını kullanıp, yavaşlamalara neden olabilmektedir..[275] Gelişen teknoloji ile beraber bu yazılım türleri de her geçen gün artış ve çeşitlilik göstermektedir.[276] Yukarda ifade edildiği gibi olumsuz anlamda ciddi etkileri olan ve büyük zararlara sebep olabilen bu

---

[272] http://betulsen6.blogspot.com/2014/12/program-ve-yazilim-arasindaki-farklar.html (erişim tarihi 21.04.2019); http://bagcidilara.blogspot.com/2014/12/yazlm-ile-program-arasndaki-fark.html (erişim tarihi 21.04.2019).

[273] https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zararli-yazilim-imal-etme-bulundurma-sucu.html (erişim tarihi 22.04.2019).

[274] Özbek/Doğan/Bacaksız/Tepe, s. 1036; Gül, s. 240; Çakır, H./Kılıç, M. S., s.. 114.

[275] http://www.bilgimikoruyorum.org.tr/?b311_zararli_program_ne_demektir (erişim tarihi 14.04.2019).

[276] http://www.e-data.com.tr/her-gun-780-yeni-zararli-yazilim-kullanicilarin-online-banka-bilgilerini-calmaya-calisiyor.aspx (erişim tarihi 14.04.2019).

yazılım türleri ile mücadele edebilmek için kanunlarımızda caydırıcı cezalar öngörülmelidir.[277]

Pek çok çeşidi bulunan zararlı yazılımların en fazla bilinenleri şunlardır: Virüsler (viruses), truva atları (Trojan horses), casus yazılımlar (spyware), mesaj sağanakları (spams), telefon çeviriciler (dialer), korunmasızlık sömürücüleri (exploit), solucanlar (worms), rootkitler (kök kullanıcı takımları), klavye dinleme sistemleri (keyloggers), arka kapılar (backdoors), reklam amaçlı (adware), fidye zararlısı (ransomware), tarayıcı zararlısı (browser hijacker).[278]

Yasal düzenlemede, hackleme yöntemlerine ilişkin herhangi bir ayrım yapılmamıştır. Bu yüzden, suç işlemek için oluşturulan her zararlı yazılım madde uygulamasına konu olabilecektir.[279]

3.1.1.3.3. Şifre

Şifre, bilişim sistemlerine erişim güvenliği sağlayan en önemli unsurlardan birisidir. Harf, sayı ya da sembollerden oluşturulan dijital kilitler olup, gizli kalması istenen belge, bilgi ya da sistemlere ulaşılmasını sağlayan anahtarlar bu adı almaktadır.[280] Şifrelendirilmiş bilişim sistemlerine erişim, belirlenen şifrenin girilmesiyle gerçekleştirilir. Kademelendirilmiş güvenlik bariyerleri de şifreler gibi bilişim sistemine yetkisiz erişimi engellemek amacıyla oluşturulan güvenlik tedbirleri olarak açıklanabilir. Genel itibariyle şifrenin kendisi değilse bile şifrelendirme işlemi bir yazılım destekli olarak çalışmaktadır. Bu haliyle şifreleme işlemi bir programlama olarak kabul edilebilir.[281]

---

[277] https://www.haberturk.com/zararli-yazilimdan-14-yil-hapis-cezasi-yedi-2170477-ekonomi (erişim tarihi 14.04.2019).

[278] Canbek/Sağıroğlu, s. 122; https://www.difose.com.tr/zararli-yazilim-laboratuvari/ (erişim tarihi 21.04.2019).

[279] http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (erişim tarihi 22.04.2019).

[280] Dülger, s. 457.

[281] Özbek/Doğan/Bacaksız/Tepe, s. 1037.

Akbulut şifreyi, iddia edilen kullanıcı olduğunu ispatlamak ve sisteme girmek için kullanılan harf ve/veya rakamlardan oluşan karakter dizisi şeklinde tanımlamıştır. Şifrenin bir bilişim sistemine girilmesini temin etmek için meydana getirilmesi halinde bu madde kapsamında cezalandırılacaktır. Bu husus ASSS'nin 6. maddesinde de belirtilmiştir.[282]

3.1.1.3.4. Sair Güvenlik Kodu

Sair güvenlik kodu, şifrelerin dışında güvenlik amacıyla kullanılan ses, retina, parmak izi ya da avuç içi tanıma gibi özellikleri barındıran güvenlik unsurları olarak açıklanabilir.[283]

Sair güvenlik kodu, bilişim sistemlerinin güvenliğini sağlamak için giriş şifrelerine ilaveten oluşturulmuş kodlardır. Bunlara biometrik tanıma kodları, kredi kartlarının arka yüzündeki CVV2, CVC2, CID olarak isimlendirilen kodlar örnek gösterilebilir. Genellikle telefon, faks ve internet üzerinden yapılan alışverişlerde kartın fiziksel olarak var olup olmadığının kontrolü amacıyla kullanılan kredi kartlarının arka yüzlerindeki üç haneli kodlar olarak günlük hayatta karşımıza çıkar.

Güvenlik kodları genel olarak verilerin güvenliğini sağlamak için farklı işlemlerde, farklı hizmetlerde kullanıldıklarından, kanun koyucu "sair güvenlik kodu" demek suretiyle farklı olarak adlandırılsa bile tüm güvenlik ile ilgili kodları koruma altına almak istemiştir. Güvenlik kodu sistem tarafından üretilen algoritmadır. Sınav sonuçlarıyla ilgili üretilen bir güvenlik kodunda, veriler üzerinde kişiler tarafından yapılan herhangi bir değişiklik güvenlik kodu uyumsuzluğuna sebep olmakta ve bu değişikliğin tespit edilmesi mümkün hale gelmektedir.[284]

Madde metnine yapılan bir diğer eleştiri de şifre ve sair güvenlik kodu kavramlarına yöneliktir. Cihaz ve programlara yönelik olarak suçun hukuki konusu rahatlıkla anlaşılmasına rağmen şifre ve sair güvenlik kodunun tam olarak neyi ifade

---

[282] Akbulut, *Bilişim Alanında Suçlar*, s. 352.

[283] Dülger, s. 457.

[284] Akbulut, *Bilişim Alanında Suçlar*, s. 353.

ettiğinin belirsiz kaldığı, hangi şifre ve kodların suçun hukuki konusu olarak kabul edildiğinin açıkça belirtilmesi gerektiğine yönelik eleştiriler mevcuttur.[285]

Yine Koca/Üzülmez de maddede geçen "sair güvenlik kodu" şeklindeki ifadenin "belirlilik ilkesine" aykırı olduğunun savunulabileceğini, buradaki "sair" ifadesinin, şifre veya sair ifadesiyle birlikte değerlendirilmesinin gerektiğini, şifrenin de aslında bir güvenlik kodu olduğunu, şifre gibi, sisteme girmek için belirlenen bir güvenlik kodunun yapılmış olmasının belirtilmek istendiğini ifade etmişlerdir.[286]

Önemle belirtmek gerekir ki; madde gerekçesinde failin cezalandırılabilmesi[287] bakımından söz konusu cihaz, program, şifre veya güvenlik kodunun suçun işlenmesine elverişli olması aranmaktadır. Bu cihaz, program, şifre veya güvenlik kodunu üreten kişi bunu suç işlemek maksadıyla yapmasa bile, piyasada var olduğu müddetçe, bunlar vasıtasıyla suç işlenmesi olasıdır. Bu statüdeki unsurlar için olay bazlı inceleme yapılmalıdır. Diğer bir deyişle, cihaz, program, şifre veya güvenlik kodunun hangi noktada suç işlemek için kullanıldığı ve geriye dönük olarak bunu suç işlemek aracı haline getiren kişilerin nerede devreye girdiği hususları irdelenmelidir. Bunlar haricinde, cihaz, program, şifre veya güvenlik kodunu diğer suç olmayan maksatlarla kullanan kişiler hakkında cezai işlem yapılmayacaktır. Ancak bu ayrımın tespit edilmesi, ülkemiz yargı sistemindeki yetkililerin bilişim alanında sahip olduğu bilgi seviyesi dikkate alındığında pek mümkün görünmemektedir. Bu bağlamda tehlike boyutuna sahip cihaz, program, şifre veya güvenlik kodunun paylaşılması konusunda büyük özen gösterilmeli, çoğunlukla bunların paylaşıldığı kişiler ile kullanım şartları ve koşullarını belirleyen sözleşmeler imzalanmalıdır. Aksi takdirde bunları imal eden kişiye kadar gidebilecek bir cezai yaptırım gündeme gelebilecektir. Cihaz, program, şifre veya güvenlik kodunu suç işlemek için elverişli olmaması halinde ise bunlar hakkında cezai yaptırım söz konusu olamayacaktır. Ancak burada da dikkat edilmesi gereken husus; cihaz, program, şifre veya güvenlik kodunun küçük değişiklikler marifetiyle suç işlenebilecek elverişliliğe

---

[285] Özbek/Doğan/Bacaksız/Tepe., s. 1037.

[286] Koca/Üzülmez, *Özel Hükümler*, s. 914.

[287] Yalvaç, s. 534

dönüştürülebilmesi durumudur. Bu durumda esasen cihaz, program, şifre veya güvenlik kodunu ilk oluşturan kişi her ne kadar suç işleme kastı taşımasa da bunun yargı önünde ispatı sorun olacaktır. İleride herhangi bir sorunla karşılaşılmaması için cihaz, program, şifre veya güvenlik kodunun oluşturulduğu ilk halinin tasdiklenmesi, sorulduğu zamanda tasdikli halinin ibraz edilip yargı önünde başkası tarafından değiştirildiğini ispat etmek açısından önerilmektedir.[288]

Elverişli olma ifadesi ile, bunların söz konusu suçların gerçekleştirilmesinde kullanılabilecek şekilde yapılmış veya oluşturulmuş ve fiilen kullanılabilecek durumda olmaları kastedilmektedir. Cihazlar bu suçların işlenmesi için bilişim sistemlerine eklenebilecek, bağlanabilecek ve çıkartılabilecek şekilde tasarlanmış ve çalışır durumda olmalı; programlar, şifreler ve güvenlik kodları ise bilişim suçlarının işlenmesine uygun şekilde oluşturulmuş ve fiilen kullanılabilir halde olmalıdır.[289] Cihazın, programın, şifre veya güvenlik kodunun md. 245/A'da belirtilen suçu gerçekleştirebilecek nitelikte olup olmadığı tespiti yapılırken, hakim yada savcı uzman bir kişiden görüş almalıdır.[290]

Burada ifade ettiği önem sebebiyle oyun hilelerine değinmek gerekmektedir. Dijital oyun pazarı parasal büyüklükte sinema pazarının önüne geçmiştir. Bu pazarda çevrim içi oyunların çoğunluğu ücretsiz olup, oyun firmaları gelirlerini, reklam gelirleri ve oyuncuların oyun içindeki itibarlarını ve şanslarını artırmak için "kılıç", "tüfek" ya da "can" gibi çeşitli oyun özelliklerinin satılmasından sağlamaktadırlar. Bu oyunlar kodlardan oluşmakta olup, oyunun kurgusu oyunu yaratan şirket tarafından program koduyla belirlenmekte şirketlerin bu yetkileri son kullanıcı lisans sözleşmesi ile hukuken güvence altına alınmış durumdadır. Pazarın büyüklüğü sonucunda bazı kişiler de oyunun kurallarını veya kodlarını etkisiz bırakmak veya değiştirmek suretiyle haksız kazanç elde etmektedirler. Bunun için de hile veya hack yazılımı olarak adlandırılan çeşitli program kodları yazma, bu kodları satma veya dağıtma

---

[288] http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (erişim tarihi 22.04.2019).

[289] Korkmaz, s. 51.

[290] Koca/Üzülmez, *Özel Hükümler* s. 914; Dülger, s. 457.

yollarına başvurmaktadırlar. Bu kişilerin ifade edilen bu eylemleri de TCK 245/A hükümleri gereğince cezalandırılmaktadır.[291]

TCK 245/A maddesiyle ilgili olarak uygulamada en çok karşılaşılacak durumlardan biri de şifreli uydu kanalları için üretilen şifrelerinin kırılmasını sağlayan yazılım veya cihazlar olacaktır. Bu madde, yazılımları kısmen veya tamamen devre dışı bırakan ve uygulamalarını değiştiren third party software denilen hack veya hile yazılımlarıyla mücadele noktasında sık sık uygu lama alanı bulacaktır.[292]

3.1.1.4. Fiil (Eylem) ve Netice

3.1.1.4.1. Fiil (Eylem)

Fiil, belirli bir amaca yönelen, kişinin isteğine ve iradesine bağlı, dış dünyada etki doğuran icrai yahut ihmali insan davranışıdır. Bu davranış, tüm suçların ortak ve tek temeli ve unsuru olan fiili ifade etmektedir.[293]

Çalışmamıza konu suçun fiil unsuru; bir cihaz, program, şifre ya da sair güvenlik kodunun imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulmasından oluşmaktadır. Bu anlamda inceleme konumuz olan madde seçimlik hareketli bir suçu ihtiva eder. Yukarıda sıralanan hareketlerden birinin yapılması ile suç tamamlanmış olur. Bu yönüyle de sırf hareket suçudur. Burada depolama ve bulundurma fiillerine dikkat çekmek istiyoruz. Depolama ve bulundurma fiilleri temadi özelliğine sahip olmaları nedeniyle farklılık göstermektedir. Bu yüzden bu iki fiil devam ettiği sürece suç da işlemeye devam edecektir. Yine sayılan hareketlerden birden fazlası gerçekleştirilmiş olsa bile konu aynıysa tek suç gerçekleşmiş olur. Örneğin failin ithal ettiği cihazları, bir müddet depoladıktan sonra, başka bir yere naklederek satışa arz etmesi hali bu duruma örnek gösterilebilir. Elbette ki bu durum temel cezanın belirlenmesinde göz önüne

---

[291] Korkmaz, s. 50.

[292] http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (erişim tarihi 22.04.2019).

[293] Artuk/Gökcen/Alşahin/Çakır, s. 234.

alınacaktır.[294] Kanun maddesinde suçun işlenmesine neden olan sınırlı sayıda hareketten bahsedilmesinden yola çıkarak bu suç tipinin bağlı hareketli bir suç tipi olduğu sonucuna varabilir. Bu sayılan seçimlik hareketler dışında başka herhangi bir hareketle bu suç işlenemez. Ayrıca herhangi bir zarar gerçekleşmesi şartı da aranmadığından bu suç bir tehlike suçudur denilebilir.[295]

Burada sayılan sevk etme ve nakletme birbirine karıştırılmaktadır. Aynı durum depolama ve bulundurma hareketleri içinde geçerlidir. Bu fiiller aynı veya yakın anlama gelmektedir. Bu nedenle suç tanımında hepsinin birlikte kullanılmasının uygun olmadığı değerlendirilmektedir.[296] Korkmaz bu kavramların farklı anlamları olduğunu, sevk etmek fiilinde daha çok bir aracı olan üçüncü kişi kullanılırken, nakletmek fiilinin fail tarafından gerçekleştirildiğini; bulundurmada ise failin suçun hukuki konuları üzerindeki fiili hakimiyeti ön plana çıkarken depolama da istenildiği anda ulaşılabileceği şekilde saklanması şartı öncelikli olarak arandığına vurgu yaparak bu eylemlerin birlikte kullanılmasında bir sakınca bulunmadığını belirtmiştir.[297]

Yukarıda belirtildiği gibi cihazların, programların, şifrelerin ve sair güvenlik kodlarının depolanması veya bulundurulmasında suça konu eylemlerin temadi etmesi söz konusudur. Bu durumda suça konu unsurlar depolandığı veya bulundurulduğu sürece aynı suç işlenmeye devam edecektir. Suçun işlendiği zamanın, mahkemelerin yetkisinin, hangi yasanın uygulanacağının belirlenmesi ve zamanaşımı süresinin hesaplanmasında bu duruma dikkat edilmelidir.[298]

Bu hareketler arasında "yayma" fiiline yer verilmemiştir. Dülger; madde metninde bu harekete yer verilmesinin bir artı olacağı ancak yer verilmemesinin bir

---

[294] Koca/Üzülmez, *Özel Hükümler*, s. 914.

[295] Özbek/Doğan/Bacaksız/Tepe, s. 1037; Akbulut, *Bilişim Alanında Suçlar*, s. 355.

[296] Koca/Üzülmez, *Özel Hükümler*, s. 914.

[297] Korkmaz, s. 51-52.

[298] Koca/Üzülmez, *Özel Hükümler*, s. 914; Dülger, s. 458.

eksiklik oluşturmadığı, diğer hareketlerin yayma hareketini kapsayacak nitelikte olduğunu belirtmiştir.[299]

Bilişim suçlarıyla daha iyi bir şekilde suçla mücadele sağlanabileceği kanaatiyle yayma kavramına yer verilmemesi eleştirilmektedir. Akbulut ve Korkmaz; yaymanın, bir kişinin elindeki bir şeyi birden fazla kişiye vermesi, ulaştırması olarak tanımlandığını, yaymada aktarmak için bir araç kullanıldığını ve birden fazla kişinin hedeflendiğini, bilişim sistemleri açısından tehlikeli olabilecek cihaz, program, şifre ve kodun birden çok kişiye verilmesi, ulaştırılması şeklindeki yayılması fiilinin TCK 245/A'da düzenlenen suç kapsamında yer almasının bu suçla mücadelede faydalı olacağını dile getirmişlerdir.[300]

Biz de suç kapsamına yayma fiilinin de eklenmek suretiyle geniş tutulmasının bilişim suçlarıyla daha etkin mücadele kapsamında faydalı olacağı kanaatindeyiz. Seçimlik hareketleri tek tek açıklamaya çalışalım.

3.1.1.4.1.1. İmal Etme

İmal etmek kavramı ile cihaz, program, şifreyle sair güvenlik kodunun üretilmesi kastedilmektedir. Üretim ile cihazlar için, fiziki bir varlığı olan şeyler bakımından parçaları sistemli bir şekilde bir araya getirerek kullanılabilir hale getirmek ifade edilmek istenmiştir. Cüzi tamamlama ihtiyacı gerektirmesi önemli değildir. Bir şeye, önemsiz ek çalışma yapılması durumunda da imal etme gerçekleşmiş olur. Burada gerekli parçaların üretilmesi zorunlu değildir. Yani imalatta kullanılacak devre, kablo, hafıza kartı gibi unsurların daha önceden üretilmiş olması bu seçimlik hareket bakımından imal etmenin gerçekleşmesine engel değildir. Ancak cihazın imal edilmiş kabul edilebilmesi için en azından o imalatta kullanılacak parçaların birtakım işlemlerden geçmesi, bir bütünlük oluşturması, bir anlamda tek tek parçalardan bağımsız ve yeni bir bütünlüğün ortaya çıkması aranmaktadır. Programlar da cihazlar gibi imal edilebilmektedir. İmal edilen program yeni bir yazılım

---

[299] Dülger, s. 457.

[300] Korkmaz, s. 51-52; Akbulut, *Bilişim Alanında Suçlar*, s. 357.

olabileceği gibi var olan bir yazılımın türevi de olabilir. Ancak bu türev yazılımların ana yazılımdan ayırt edilebilir birtakım özelliklere sahip olması şart koşulmaktadır.[301]

3.1.1.4.1.2. İthal Etme

İthal etme, suça konu cihaz, program, şifre ve sair güvenlik kodunun başka bir ülkeden ülkemize sokulması şeklinde tanımlanabilir. Cihaz gibi fiziki varlığı şeyler açısından herhangi bir özellik söz konusu değildir. Ancak cihaz üretimi için kullanılacak parçaların ayrı ayrı ithal edilmesi ve bunların yurt içinde birleştirilmesi suretiyle bir cihaz oluşturulmasında artık ithal etme değil imal etmek seçimlik hareketinden bahsedilebilir. Madde metninde cihazların ithal edilmesinden bahsedilmiştir. Ayrıca fiziki varlığı olmayan program, şifre ve sair güvenlik kodu bakımından ise taşınabilir bir bellek ya da kart aracılığı ile yurda sokulmuşlar ise bunlar bakımından da ithal etme seçimlik hareketi gerçekleşmiş olacaktır. Bedeli ödenerek yurt dışındaki bir kullanıcı ya da içerik sağlayıcısından dijital ortamda edinilmiş program, şifre ve güvenlik kodunun ithali mümkündür. Burada dikkat edilmesi gereken husus ithal edilmenin varlığı için mutlak surette sınır kapısı geçişinin aranmamasıdır. Önemli olan suça konu cihaz, program, şifre ve kodun yurt dışından yurt içine aktarımının sağlanmış olmasıdır. Türkiye' deki kullanıcının içinde bulunduğu içerik sağlayıcının yurt dışında bulunması da önemli değildir. Mail yoluyla gerçekleştirilen bu tarz alışverişlerde mail adresinin içinde bulunduğu içerik sağlayıcısı Türkiye' de olmasa bile, suça konu cihaz, program, şifre ve sair güvenlik kodu yurt içinden temin edilmişse ithal etme eylemi gerçekleşmiş olur. Bilişim teknolojilerinin sınırları aşan karakteristik yapısı gereği, ithal etme kavramının değerlendirmesinin de bu karakteristik yapıya uygun olarak yapılması kaçınılmazdır.[302]

3.1.1.4.1.3. Nakletme ve Sevk Etme

Cihaz, program, şifre ve sair güvenlik kodunun fail tarafından bizzat alıcıya yönlendirilmesi ve teslim edilmesi nakletme, aracılar vasıtasıyla alıcıya

---

[301] Özbek/Doğan/ Bacaksız/Tepe, s. 1037-1038.

[302] Özbek/Doğan/Bacaksız/Tepe, s. 1038.

yönlendirilmesi ise sevk etme olarak kabul edilmektedir. Bunlar fiziki olarak sevk edilebileceği, nakledilebileceği gibi, bilgisayar programı, şifre ve sair güvenlik kodları internet ve bilişim ağları vasıtasıyla gönderilebilirler.[303] Nakletme ve sevk etmede alıcı değil nakleden veya sevk eden esas alındığı için nakil ve sevkiyatın yurt içinden ya da yurt dışından olmasının bir önemi yoktur.[304]

Yurt dışından ithal etme madde metninde düzenlendiği halde ihraç etme düzenlenmediği için ihraç etmek mahiyetinde kalan eylemlerin nakletme veya sevk etme kapsamında değerlendirilmesi gerekmektedir.[305]

3.1.1.4.1.4. Depolama

Cihaz, program, şifre ve kodun istenildiğinde ulaşılabilecek herhangi bir yerde toplu olarak bulundurulmasıdır. Depolanacak yer cihazlar için fiziki bir ortam olabilecekken programlar için dijital bir ortam da olabilir. Program, şifre ve sair güvenlik kodu açısından depolama ve kaydetme arasındaki farka değinmek gerekir. Bu kavramlar açısından depolama için kaydetme zorunludur. Her kayıt otomatik olarak da bu suç anlamında depolama olarak kabul edilmemelidir. Depolama, TCK 245/A da ifade edilen suçu işlemek amacıyla yapılan kayıt olarak kabul edilmelidir. Aksi takdirde, dijital ortamda her türlü bulundurma bir çeşit kayıt işlemidir. Depolama için yapılan kaydın niteliği, boyutu ve amacı gibi unsurlar göz önünde bulundurulmalıdır.[306]

3.1.1.4.1.5. Kabul etme

Cihaz, program, şifre ve sair güvenlik kodunun belli bir ücret karşılığı olmaksızın temin edilmesi kabul etme eylemi içinde değerlendirilir. Satın almak ve kabul etmek arasındaki fark suç konusunun ticari bir ilişki sonucu el değiştirip değiştirmemesidir. Eğer ticari bir ilişki içerisinde el değiştirme söz konusuysa veren açısından satma, alan açısından ise satın alma eylemi gerçekleşmiş olur. Herhangi bir

---

[303] Korkmaz, s. 51-52.

[304] Akbulut, *Bilişim Alanında Suçlar*, s. 356.

[305] Özbek/Doğan/Bacaksız/Tepe, s .1038.

[306] Özbek/Doğan/Bacaksız/Tepe, s. 1038-1039.

ticari ilişki mevcut değilse suç konusunu elinden çıkaran için başkalarına verme, alan içinse kabul etme eylemi söz konusu olur.[307] Suçun konusunu oluşturan unsurlar, herhangi bir şekilde verilebilir.

3.1.1.4.1.6. Satma

Bir değer karşılığında cihazın, programın, şifrenin veya kodun alıcıya verilmesidir. Program veya güvenlik kodu satılırken programa erişimin veya güvenlik kodu bilgisinin de verilmesi gerekir.[308]

3.1.1.4.1.7. Satın Alma

Bir bedel karşılığında cihazın, programın, şifrenin veya kodun alınmasıdır. Ancak cihazlar için yapılan tanım doğru olsa da diğer soyut unsurlar için yeterli değildir. Alıcının satış esnasında programa erişimi, buna ilişkin güvenlik kodu bilgisini elde etmesi gereklidir.[309]

3.1.1.4.1.8.Satışa Arz atme

Cihaz, program, şifre ve kodun satış yapılabilecek şekilde piyasaya sürülmesidir. Dikkat edilirse gereken husus satışa arz etmek için somut bir alım satım ilişkisine veya ihtimaline ihtiyaç duyulmamaktadır. Önemli olan suç konusunun satılmasına yönelik irade açıklamasıdır. Reklam veya ilanlar bu kapsamda satışa arzı gösteren irade açıklamalarıdır.[310]

3.1.1.4.1.9. Başkalarına Verme

Satış niteliği olmaksızın cihazın, programın, şifrenin veya kodun bir başkasına kullanması amacıyla teslim edilmesidir. Birisi bir başkası aracılığıyla sahiplenmeyi kabul ederse bu da yeterli değildir. Cihazın, programın, şifrenin veya

---

[307] Özbek/Doğan/Bacaksız/Tepe, s. 1039.

[308] Akbulut, *Bilişim Alanında Suçlar*, s. 356.

[309] Akbulut, *Bilişim Alanında Suçlar*, s. 357.

[310] Özbek/Doğan/Bacaksız/Tepe, s. 1039; Akbulut, *Bilişim Alanında Suçlar*, s. 357

güvenlik kodunun bir başkasına verilmesi için birine teslim edilmesi başkasına vermek anlamı taşımaz.[311]

3.1.1.4.1.10. Bulundurma

Bir kimsenin bir cihazda, bilgisayar programında, şifrede veya sair güvenlik kodunda fiili hakimiyet sahibi olmasıdır. Mülkiyet ilişkisinin bulunması veya bulundurulan yerin kime ait olduğu önemli değildir. Suçun konusunun yanında bulundurulması gerekmemektedir. İstediği an ulaşabileceği yerde olması yeterlidir.[312]

En çok soruşturma açılacak olan hareketin "bulundurma" olacağı öngörülmektedir. Şöyle ki bilgisayarınız başka bir suçla ilgili incelenirken tesadüfen suça konu cihaz, program, şifre veya sair güvenlik kodu bulunduğunda, kanunda "bulundurmak" başlı başına suç olarak düzenlendiğinden, adli makamlarca bu suçu işlediğinizden bahisle hakkınızda kamu davası açılması ihtimali ortaya çıkacaktır. Kamu davası açıldığı takdirde ise, neden bu unsurları bulundurduğunuzu ve hukuka uygun amaçlarla kullandığınız noktasında kendinizi savunmanız gerekecektir. Aksi takdirde, TCK 245/A maddesi kapsamında ceza alma ihtimaliniz ortaya çıkabilecektir. Bu durum, özellikle yer sağlayıcı ve barındırma hizmeti veren hosting firmaları yönünden sıkıntı oluşturacaktır. Bu nedenle, özellikle bu tür hizmet veren firmaların, pentest yazılımlarını sistemlerinde depoluyorlarsa, şirket içerisinde bunları ortak bir alanda depolamaları, bunun için kullanılan programların veya kodların şirketteki herkesin elinde bulundurulmaması, bulundurulan yere de kimlerin erişiminin olduğunun önceden belirlenmiş olması yahut pentest yapılacak her yeni müşteri için yeni bir kopya oluşturulup bunun belirtilmesi gibi, olası bir suçlama durumunda firma yetkililerini cezai sorumluluktan kurtulmasını sağlayabilecek tedbirler alınmalıdır. Bunun yanı sıra, bu tür yazılımların ortak alanlar dışında firma yetkilisi veya çalışanların özel bilgisayarlarında bulundurulması halinde, her ne kadar bu işin meslek olarak yapıldığı geçerli bir savunma olabilecekse de ceza soruşturması ve yargılaması söz konusu olduğunda ispatla ilgili sorunlar ortaya çıkabilecektir.

---

[311] Özbek/Doğan/ Bacaksız/Tepe, s. 1039; Akbulut, *Bilişim Alanında Suçlar*, s. 357.

[312] Akbulut, *Bilişim Alanında Suçlar*, s. 357.

Anılan gerekçelerle, özellikle TCK 245/A maddesinin yürürlüğe girmesinden sonra, bu tür cihaz, program, şifre ve sair güvenlik kodunun depolanması ve bulundurulması ile ilgili yukarıdaki hususlara dikkat edilmesi gerekmektedir.[313]

AKSSS, taraf devletlere kişilere ceza sorumluluğunun yüklenebilmesi için belirli sayıda aracın bulundurulmasının gerekli olması yönünde düzenleme yapıp yapmama noktasında geniş bir alan bırakmıştır. Bu durum kast kavramıyla ilgilidir ve az sayıda araç bulundurma hukuka aykırı işlemlerde kullanma kastının varlığına işaret eder. Yüksek sayıda cihaz bulundurma ise, büyük olasılıkla, kişisel kullanımdan ziyade, başkalarına bu ürünlerin tedarik edilmesine yönelik bir işaret olarak kabul edilir. Ayrıca taraf devletler, bulundurmayı suç olarak düzenleyip düzenlememekte serbesttirler. TCK 245/A'nın düzenlenmesinde sayısal bir sınırlandırmaya yer verilmediği gibi, bulundurma da suçun seçimlik hareketlerinden biri olarak maddede yer bulmuştur.

Genel itibariyle bu kavramlar AKSSS'de genel olarak tedarik etme kavramıyla ifade edilmekte olup bu geniş anlamda "yapım, satım veya kullanmak üzere satın alma, ithal etme, dağıtma veya bir şekilde elde edilebilir hale getirme" olarak kabul edilmektedir.[314] AKSSS Açıklayıcı Raporu'na göre "dağıtım verilerini aktif olarak başkalarına iletmek, elde edilebilir hale getirmek" online cihazları başkalarının kullanımına sunmak anlamında kullanılmıştır. Bu terimin, bu tür cihazlara erişimi kolaylaştırmak için hyperlink (köprü)ler[315] yaratmayı ya da derlemeyi de içine alması amaçlanmıştır. Elde edilebilir hale getirmek deyiminin

---

313 https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zararli-yazilim-imal-etme-bulundurma-sucu.html (erişim tarihi 22.04.2019).

http://www.bilisimdergisi.org.tr/yazarlar/konuk- yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html (erişim tarihi 22.04.2019).

314 Dülger, s. 457.

315 Hyperlink, web tarayıcınızda "başka bir sayfaya geçiş yapmak" için kullanılan programlı komutlardır. Her web sayfası, sizi ilgili bazı web sayfalarına veya resim ya da dosyalara gönderen onlarca hyperlink ile doludur. Mouse işaretçisi işaret parmağına dönüştüğünde bir şeyin hyperlink olduğunu anlayabilirsiniz. Bazen, hiperlinkler açılan menüler veya küçük animasyonlu filmler veya reklamlar şeklinde olabilir." Bkz. https://www.semseo.com.tr/rehber/seo-sozlugu/hiperlink-nedir-hiperlink-ne-ise-yarar (erişim tarihi 21.04.2019).

kullanılmasıyla, bu tür cihazlara veya programlara erişimin kolaylaştırılması için elverişli bütün hareketlerin suçun kapsamına alınması amaçlanmıştır.[316] Bir materyali indirilmek üzere bir web sitesinde bulundurmak, P2P[317] ağ sistemi ya da hyperlink aracılığıyla erişim sağlamak, elde edilebilir hale getirme kavramı içinde değerlendirilir.[318]

3.1.1.4.2. Netice

Hareketin dış dünyada ortaya çıkardığı değişiklik netice olarak kabul edilir. Elbette ki durum ceza normuyla düzenlenmişse anlam kazanır. Tüm bunlar gerçekleşirse neticeli suç söz konusu olur.[319]

Neticeye göre suçlar kendi aralarında sınıflandırılmaktadır.

Tamamlanmaları bakımından neticenin gerçekleşmesinin aranmadığı suçlara sırf hareket suçları denilmektedir.[320] Doktrinde şekli suç olarak da anılmaktadır.[321] TCK md. 125'de düzenlenen hakaret, md.116' da düzenlenen konut dokunulmazlığını ihlal, md. 272'de düzenlenen yalan tanıklık bu suç tipine örnek olarak verilebilir.

Hareket ile neticenin, yer ve zaman veya zaman ve nedensellik bağı bakımından birbirinden ayrılabildiği suçlar maddi ya da neticeli suçlar olarak

---

[316] Korkmaz, s. 51.

[317] "P2P, birden fazla bilgisayarın bir araya gelerek belirli görevleri paylaştığı dağıtık ağlardır. Bu sistemlerde bulunan kullanıcılar olan eşler, sistemde hem istemci hem sunucu görevinde bulunabilmektedir. Yani, her bir kullanıcı, kaynak isteğinde bulunabilirken kaynak isteklerine de cevap verebilmektedir. P2P sistemler çift taraflı istemci-sunucu ağlar olarak görülebilir. P2P sistemlerde kullanıcılar eş olarak tanımlanmaktadır ve asıl veri akışları eşler arasında gerçekleşmektedir." Bkz. Orsorlu, Ahmet, *P2P Sistemlerde İstemci Eş Tabanlı Eş Seçim Modeli*, (Yayınlanmamış Yüksek Lisans Tezi), Gebze Yüksek Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü, Kocaeli 2011, s. 3-4.

[318] Dülger, s. 457.

[319] Artuk/Gökcen/Alşahin/Çakır, s. 271.

[320] Artuk/Gökcen/Alşahin/Çakır, s. 271.

[321] Hakeri, Hakan, *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi (21. Baskı), Ankara 2017, s. 182; Özbek/Doğan/Bacaksız/Tepe, s. 210.

isimlendirilmektedir. Kasten öldürme ve mala zarar verme suçları bu suç tipinin en bilinen örnekleridir.[322]

Suçun teşebbüs veya tamamlanmış şekli arasında yaptırım bakımından fark bulunmayan suçlar ise kalkışma suçlarını oluşturur. TCK md. 310'da düzenlenen Cumhurbaşkanına suikast bu suça örnek olarak verilebilir.[323]

TCK md. 245'A da yer alan yasak cihaz veya programlar başlıklı suç, sırf hareket suçudur ve yapılan hareketin devamında bir neticenin meydana gelmesi aranmaz.[324] Depolama ve bulundurma fiillerine ilişkin farklılıktan yukarıda bahsetmiştik. Bu husus zamanaşımı, suçun işendiği yer ve teşebbüs konuları bakımından önem taşımaktadır. Bahsi geçen kavramlara çalışmamızın ilerleyen bölümlerinde değinilecektir.

3.1.2. Tipikliğin Manevi Unsuru

Kişiyle icra ettiği fiil arasındaki manevi bağı ifade etmek için manevi unsur tabiri kullanılmaktadır.[325] "Bu bağ tesis edilmeden, gerçekleştirilen davranış fiil niteliğini taşımaz ve dolayısıyla, bir suçun varlığından söz edilemez."[326] TCK m. 22/1' de dile getirildiği üzere suçun oluşması kastın varlığına bağlı olup bu fıkra manevi unsur bakımından ana kuralın kast olduğunu ortaya koymaktadır. Kanunda açıkça ve ayrıca belirtilmediği sürece taksirli hareketlerin cezalandırılması mümkün değildir.[327]

Yukarıda da değinildiği gibi AKSSS'nin 6. maddesinin 2. fıkrasında suçun konusunu oluşturan cihazların belirtilen suçların işlenmesi amacıyla tasarlanmış olması gerektiği ifade edilerek, bu cihazlarla bir bilgisayar sisteminin, yukarıda daha

---

[322] Artuk/Gökcen/Alşahin/Çakır, s. 273.

[323] Artuk/Gökcen/Alşahin/Çakır, s. 274.

[324] Dülger, s. 458.

[325] Artuk/Gökcen/Alşahin/Çakır, s. 324; Özgenç, s. 221

[326] Özgenç, s. 221.

[327] Koca/Üzülmez, Genel Hükümler s. 139; Artuk/Gökcen/Alşahin/Çakır, s. 232.

önce bahsi geçen pentest adı verilen testlerle yetkililerce test edilmesi veya korunmasının amaçlandığı hallerde kişilere ceza sorumluluğu yüklenemeyeceği belirtilmiştir. Aynı hususa sözleşmeye ilişkin açıklayıcı raporun 77. bölümünde de yer verilmiştir. Burada ifade edilmek istenen suç işleme kastının varlığıdır.

TCK m. 245/A maddesine bakıldığında, suçun söz konusu olabilmesi için, cihaz, program, şifre veya sair güvenlik kodunun "münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için" yapılması ve oluşturulması aranmıştır. Dolayısıyla faillerin fiillerini bahsi geçen suçları gerçekleştirmeleri zorunludur. Fail bu amacı taşımıyorsa, suçun manevi unsuru olan "kast" söz konusu olmadığından, herhangi bir suçtan da bahsedilemeyecektir.[328] 5237 sayılı TCK'nın yasak cihaz veya programlar başlıklı suç kasten işlenebilen suç tiplerindendir.

Failin kasten hareket etmesi için suçun kanuni tanımında yer alan unsurları bilmesi şartı aranır. Fail madde metninde sayılan fiilleri üzerinde gerçekleştirdiği şeyin cihaz, program, şifre veya kod olduğunun farkında olmalıdır. Bununla birlikte, fail suçun konusu cihaz, program, şifre ve kodun sadece bilişim suçu ya da bilişim sistemi aracılığıyla işlenebilen suçlardan birini gerçekleştirmek amacıyla oluşturulduğunu veya yapıldığını bilmesi ya da bilebilecek durumda olması gerekmektedir. Bu amacı bilebilecek durumda olmayan, örneğin bilgisayar ve bilişim sistemi konusunda hiçbir bilgisi olmayan, başkaları tarafından oluşturulmuş veya yapılmış bir cihazı failin talebi üzerine nakleden kişiye ceza verilmemesi gerekir. Elbette ki bu durum diğer deliller ve araştırma sonucunda tespit edilmelidir.[329]

Korkmaz, TCK'nın bilişim alanında suçlar başlıklı onuncu bölümünde yer alan suçların TCK 243-245 ve 245. maddelerinde düzenlenen suçlar olduğunu, failin bu suçları bilmesi açısından bir sorun bulunmadığını, ancak TCK'da bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların hangileri

---

[328] http://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html (erişim tarihi 22.04.2019).

[329] Gül, s. 242.

olduğunun açık olarak yer almadığını, doktrinde dahi bu suçların hangileri olduğu konusunda bir fikir birliği bulunmadığını, failden bu suçların neler olduğunu tam olarak bilmesini beklememek gerektiğini, bu açıklamalar ışığında TCK md. 245/A'da yapılan hukuki düzenlemede, bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların neler olduğunun belirli olmamasının kanunilik ilkesine aykırı olduğunu belirtmiştir.[330]

Dülger, suçta amaç unsuru arandığı için bu suçun olası kastla işlenmesinin mümkün olmadığını belirtmektedir.[331] Akbulut ise, maddede failin belirtilen suçları işlemek için cihaz, program, şifre veya kodu imal etmesi, ithal etmesi, sevk etmesi, nakletmesi, depolaması, kabul etmesi, satması, satışa arz etmesi, satın alması, başkalarına vermesi veya bulundurmasının aranmadığını, failin cihaz, program, şifre veya güvenlik kodunun başkalarına iletilmesine araç olabileceğini, maddede belirtilen suçları işleme amacı taşımadığını, yalnızca nakletme işini yapıyor olabileceğini, böylelikle TCK md. 245/A düzenlenen suçun olası kastla işlenebileceğini dile getirmiştir. Akbulut TCK md. 245/A'nın bu yönüyle AKSSS'nin 6. maddesinden ayrıldığını dile getirmektedir.[332] Doktrinde Akbulut'u destekleyen görüşler mevcuttur.[333]

İnceleme konumuz olan suçun oluşabilmesi için failin suçun konusunu oluşturan cihaz, şifre veya programı maddede belirtilen suçları işlemek amacıyla imal etmesi, ithal etmesi, sevk etmesi, nakletmesi, depolaması, kabul etmesi, satması, satışa arz etmesi, satın alması, başkalarına vermesi ya da bulundurması gerekirse de bu cihaz veya programı kullanarak hedef suçları işlemesi gerekmez.[334] Bu suç taksirle işlenemez.

---

[330] Korkmaz, s. 52-53.

[331] Dülger, s. 458.

[332] Akbulut, *Bilişim Alanında Suçlar*, s. 358.

[333] Özbek/Doğan/Bacaksız/Tepe, s. 1040.

[334] Koca/Üzülmez, *Özel Hükümler* s. 915.

3.2. Hukuka Aykırılık Unsuru

Gerçekleştirilen fiilin sadece ceza hukukuyla değil bütün hukuk düzeni ile çelişki ve çatışma halinde olması, işlenen ve kanundaki tarife uygun bulunan fiile hukuk düzenince cevaz verilmemesi, bu fiilin mübah sayılmaması hukuka aykırılık unsurunun kapsamında inceleme alanı bulur.[335] Kanun koyucu tarafından karşılığında cezai yaptırım öngörülen tipik eylem hukuka aykırılığa karine teşkil etmektedir.[336] Elbette ki bu karine kesinlik arz etmez. Gerçekleştirilen eylem tipe uygun olsa bile, bir hukuka uygunluk nedeni bulunuyorsa artık eylemin hukuka aykırılığından bahsedilemeyecektir.[337]

Yukarıda tipik eylemin, hukuka aykırılığa karine teşkil ettiğini belirtmiştik. Bu durumda suçun unsurlarında, öncelikle tipik eylemin gerçekleştirilip gerçekleştirilmediği ortaya çıkartılmalı sonrasında ise bu eylemi hukuka uygun hale getiren bir nedeninin bulunup bulunmadığına bakılmalıdır.

TCK md. 245/A'da düzenlenen bu yeni suç tipi açısından hukuka aykırılık unsuruna yönelik olarak iki hukuka uygunluk nedeninden bahsedilebilir.

İlki TCK md. 24/1'de düzenlenen kanun hükmünün yerine getirilmesidir. Bu konuda verilebilecek en göze çarpıcı örneklerden birisi CMK md. 134/2'de düzenlenen: "Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir." hükmüdür. Soruşturma evresinde başvurulan bu koruma tedbirinde bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma fiillerinin icrası kapsamında soruşturma birimlerinin şifrelenmiş bilgisayar

---

[335] Artuk/Gökcen/Alşahin/Çakır, s. 422.

[336] Centel, Nur/Zafer, Hamide/Çakmut, Özlem, *Türk Ceza Hukukuna Giriş*, Beta Yayınları, İstanbul 2016, s. 285

[337] Artuk/Gökcen/Alşahin/Çakır, s. 427.

veya programların şifrelerini çözmek için kullanılmak üzere suçun TCK 245/A maddesinin hukuki konularıyla madde metninde sayılan fiilleri gerçekleştirmeleri bazı cihaz, bilgisayar programı, şifre veya sair güvenlik kodlarını imal edilmesi, ithal edilmesi, sevk edilmesi, nakledilmesi, depolanması, kabul edilmesi, satılması, satışa arz edilmesi, satın alınması, başkalarına verilmesi veya bulundurulması bir hukuka aykırı bir nitelik içermez.[338]

Kolluk güçlerinin ve adli bilişim laboratuvarlarının suçla mücadele edebilmek amacıyla bu kapsamdaki cihaz, program, şifre veya koda bünyelerinde yer vermeleri olağandır. Aynı zamanda özel adli bilişim laboratuvarları veya bilişim güvenliği şirketlerinde de şifre kırmaya yönelik programların bulunması sıradan bir durumdur. Suçların ortaya çıkarılmasına yardım etmek amacıyla yine aynı kapsamdaki cihaz, program, şifre veya kodu bulundurmakta herhangi bir hukuka aykırılık yoktur.[339]

İkinci hukuka uygunluk nedeni ise TCK md. 25/2'de düzenlenen ilgilinin rızası kavramıdır. Bilişim teknolojileri alanında faaliyette bulunan şirketler, bir takım kişi veya şirketlerle anlaşma yapmak suretiyle, ürettikleri teknolojilerin güvenlik açığı olup olmadığını araştırır. Bu anlaşma kapsamında herhangi bir güvenlik açığının olup olmadığı test etmek maksadıyla faaliyet alanına dahil teknoloji ürünlerine bir takım siber saldırılar gerçekleştirilmektedir. Bilişim sistemlerinin güvenliğinin test edilmesi için belirli aralıklarla gerçekleştirilen uygulamaya "pentest" adı verilmektedir. Testin yapılmasındaki amaç, müşterinin bilişim sistemindeki güvenlik açığını bulmak olduğu kadar, bulunan açıkların değerlendirilip sorunun çözülmesi ve sistemlere yetkili erişimler elde edilebilmesinin sağlanmasıdır. Bir başka deyişle, pentestler ile, belirlenen veya belirsiz zamanlarda sisteme "tatbikat" mahiyetinde saldırılar yapılmakta ve bu şekilde sistemin güvenlik açıkları tespit edilerek giderilmeye çalışılmaktadır. Pentest ile ilgili yazılımları birçok firma imal etmekte, bulundurmakta, satın almakta ve depolamaktadır. Elbette, bu testler, pentest yapacak

---

[338] Özbek/Doğan/Bacaksız/Tepe, s. 1039-1040.

[339] Dülger, s. 459.

güvenlik firması ile sistemine "saldırı" yapılacak müşteri arasındaki sözleşme kapsamında yapıldığından ve firmaya bununla ilgili yetki verildiğinden, sisteme yetki kapsamında girildiği veya saldırıldığı için hukuka aykırılık söz konusu olmayacaktır. Bu nedenle, pentest yapan firmalar, müşterilerden aldıkları rıza ile bu fiili gerçekleştirdiklerinden, TCK md. 245/A'daki suçu işlemiş olmayacaklardır. Ne var ki, eğer bu hususla ilgili konu Cumhuriyet Başsavcılığına intikal ettiğinde, örneğin pentest kapsamında sistemine sızma veya saldırı yapılan firma saldırıyı yapandan şikayetçi olduğunda, pentest yapan kişiler firmadan bu yetkiyi aldıklarını ispat etmek durumunda olduklarından, "penetrasyon sözleşmesi" adı verilen ve sisteme girme yetkisinin yanı sıra yapılacak testin kapsamını detaylı bir biçimde içeren sözleşmeler yapmaları son derece yerinde olacak ve aksi durumlarla karşılaşıldığında, testleri yapanların cezai sorumluluğu söz konusu olmayacaktır. Her ne kadar ortada bir sözleşme dahi olsa, eğer yapılan saldırı veya sızma işlemi verilen yetkiyi aşıyorsa, örneğin test sırasında sözleşmede girilmemesi gerektiği belirtilen alanlara da girildiyse, duruma göre pentest yapan firma personeli TCK'nın ilgili maddelerinden sorumlu olacak ve söz konusu suçların faili haline gelebilecektir. Bu nedenle yapılacak penetrasyon testlerinde "penetrasyon sözleşmesi" düzenlenmesi gerekliliği kadar, testlerin bu sözleşmedeki hükümlere uygun biçimde yapılması da hayati önem taşımaktadır.[340]

İşte bu noktada, bilişim teknolojisi alanında faaliyet gösteren şirketlerin anlaşmanın icrası kapsamında kullanılmak üzere bazı cihaz veya program üretmesi veya bulundurması herhangi bir suça sebebiyet vermez. Nitekim bu durum maddenin gerekçesinde belirtilmiştir.[341] Yine Polis Vazife ve Salahiyetleri Kanunu ek md. 6'ya eklenen fıkrada; (Ek fıkra: 2/1/2017-KHK-680/27 md.; Aynen kabul: 1/2/2018-7072/26 md.) Polis, sanal ortamda işlenen suçlarda, yetkili Cumhuriyet başsavcılığının tespiti amacıyla, internet abonelerine ait kimlik bilgilerine ulaşmaya, sanal ortamda araştırma yapmaya yetkilidir' denilmektedir.[342] Bu madde kapsamında,

---

[340] http://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html (erişim tarihi 22.04.2019).

[341] Özbek/Doğan/Bacaksız/Tepe, s. 1039-1040; Dülger, s. 459.

[342] http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf (erişim tarihi 21.04.2019).

araştırma yapmak amacıyla kolluğun cihaz, bilgisayar programı, şifre veya sair güvenlik kodu, bulundurması, temin etmesi, imal etmesi hukuka uygun olacak ve herhangi bir suça sebebiyet vermeyecektir.[343]

3.3. Suçun Nitelikli Halleri

TCK md. 245/A'da düzenlenen yasak cihaz veya programla başlıklı suç için kanunda bir nitelikli hal bulunmamaktadır.

4. SUÇUN ÖZEL GÖRÜNÜŞ ŞEKİLLERİ

4.1. Teşebbüs

Failin, suç tanımında belirlenmiş olan fiilin icrasına elverişli hareketlerle başlanmış olmasına rağmen bu fiile ilişkin icra hareketlerinin tamamlanamaması veya icra hareketleri tamamlanmış olmakla birlikte, suç tipinde ayrı bir unsur olarak belirlenmiş olan hallerde neticenin gerçekleşmemiş olması suça teşebbüsü açıklamaktadır.[344] Suçun tamamlanması ile, sırf hareket suçlarında icra hareketlerinin tamamlanması, kanuni tanımda ayrıca neticenin arandığı suçlarda ise neticenin gerçekleşmesi kastedilmektedir.

TCK'nın teşebbüs müessesini düzenleyen 35. madde hükümleri cezai sorumluluğu genişletici bir anlayışla düzenlenmiştir. Ana kural fail suçun kanuni tanımındaki unsurları gerçekleştirdiğinde yani diğer bir deyişle suç tamamlandığında cezalandırılmasıdır. Ancak suç tamamlanmasa dahi doğrudan doğruya icra hareketlerine başlanmış ancak elde olmayan sebeplerle suçun tamamlanamaması ya da neticenin arandığı suçlarda neticenin gerçekleşmemesi durumunda faile icrasına başlanan suçun cezası indirilerek verilmektedir.[345]

---

[343] Korkmaz, s. 53.

[344] Artuk/Gökcen/Alşahin/Çakır, s. 617; Akbulut, *Genel Hükümler*, s. 348

[345] Hafızoğulları, Zeki/Özen Muharrem, *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar*, U.S.A Yayıncılık, Ankara 2016, s. 308.

TCK md. 245/A'da düzenlenen suç, depolama ve bulundurma fiilleri haricinde sırf hareket suçudur ve herhangi bir neticenin gerçekleşmesi aranmaz. Düzenleme yapılırken seçimlik hareketler tek tek sayılmıştır. Seçimlik hareketlerden herhangi birisinin icrasıyla suç tamamlanır. İcra hareketlerine doğrudan doğruya başladıktan sonra failin iradesi dışında icra hareketlerinin tamamlanamaması durumunda suça teşebbüs mümkün olacaktır. Bu tür cihaz, program, şifre ve kodun üretimine başlanmasına rağmen, kolluk görevlilerinin yaptığı baskınla üretim sürecinin tamamlanamaması halinde suç teşebbüs aşamasında kalmış olur. Yine aynı şekilde, cihazın satımı aşamasında kolluk görevlilerinin olayı haber alarak satış işlemine müdahale etmesi halinde de teşebbüsten bahsedilebilir.

Bazı hallerde bir hareket tamamlanamamakla beraber diğeri gerçekleştirilmiş olabilir. Failin cihazı ithal etmek isterken bunu gerçekleştiremezse halinde ithal etme teşebbüs aşamasında kalmış olacaktır. Ancak nakletme veya bulundurma hareketlerinin tamamlanmış olması mümkündür. Yine fail satışa arz ettiği cihazı satmak isterken yakalanırsa satmak teşebbüs aşamasında kalmış olsa da satışa arz etmenin gerçekleştiği kabul edilmelidir.[346]

Temadi özelliği olan yani devamlılık arz eden hareketler ise farlılık arz eder, bu hareketlerin icrasıyla suç tamamlanmış olmakta, ancak temadi arz eden hareket devam ettiği sürece suç da işlemeye devam etmektedir. Örneğin failin bu tür cihaz, program, şifre ve kodu kendi egemenlik alanına geçirmesi maddede sayılan bulundurma hareketinin gerçekleşmesi anlamına gelmektedir. Suça konu unsurlar failin egemenlik alanında bulunduğu sürece suç da işlemeye devam edecektir.[347] Depolama fiili için de aynı hususlar geçerlidir.

Yine bu suça yönelik olarak gönüllü vazgeçme müessesesinin uygulanmasında herhangi bir hukuki engel yoktur. Gönüllü olarak icra hareketlerini yapmaktan vazgeçen ya da suçun tamamlanması imkanı varken suçun

---

[346] Akbulut, *Bilişim Alanında Suçlar* 357-60.

[347] Koca/Üzülmez, *Özel Hükümler* s. 915-916.

gerçekleşmesini önleyen fail hakkında gönüllü vazgeçme hükümleri uygulanabilecektir.[348]

4.2. İştirak

Tek bir faille icra edilebilen suçun, birden fazla failin, aralarındaki anlaşma ve iş birliğiyle icra edilmesi gerçekleştirilmesi suça iştirak olarak açıklanabilir.[349] İştirak, faillik ve şeriklik şeklinde iki bölümde incelenir. Fail, yasada tanımlanan suçu gerçekleştiren kişidir. Suçun icrasına iştirak etmekle beraber, ceza normunda yasaklanan suçu gerçekleştirmeyen diğer suç ortakları şerik sıfatına sahip olurlar. Şeriklikte kendi içinde azmettirme ve yardım etme adı altında iki başlıkta incelenmektedir.[350]

TCK md. 245/A'da düzenlenen bu suç için iştirak hükümlerinin uygulanmasında herhangi bir özel durum yoktur. TCK'nın iştirake ilişkin genel hükümler uygulanacaktır.

Bazı seçimlik hareketler açısından çok faillilik görünümü mevcuttur. Madde metninde yer alan bir satma hareketinin gerçekleşebilmesi için karşılığında satın alma, kabul etme hareketinin gerçekleşebilmesi için de karşılığında başkalarına verme hareketlerinin var olması gerekir. TCK 245/A'da satın alma ve başkalarına verme seçimlik hareketleri de suç olarak tanımlanmıştır. Madde metninde suç olarak tanımlandığından çok failli suç özelliği gösterir.[351]

4.3. Suçların İçtiması

Suça iştirak ile suçların içtimainin farkı; iştirakte birden çok failin tek suç işlerken, içtimaıda ise tek bir failin birden çok suç işlemektedir.[352]

---

[348] Akbulut, *Bilişim Alanında Suçlar*, s. 359-360; Özbek/Doğan/Bacaksız/Tepe, s. 1040.

[349] Artuk/Gökcen/Alşahin/Çakır, s. 662, İçel, Kayıhan; Ceza Hukuku Genel Hükümler, İstanbul 2016 s. 531; Özgenç, s. 19.

[350] Artuk/Gökcen/Alşahin/Çakır, s. 685.

[351] Dülger, s. 459; Koca/Üzülmez, *Özel Hükümler*, s. 916.

[352] Hakeri, s. 595.

Ceza hukukunda önemli ilkelerinden biri de "kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır" ilkesidir. Bu kapsamda ceza hukukunda cezaların içtimaı yani gerçek içtima genel kural olarak kabul edilmektedir. Bu kural uyarınca işlenen her suç için ayrı cezaya karar verilir.[353] Özetle suçların içtimaı, fail lehine getirilmiş istisnalardan biridir denilebilir.[354]

TCK md. 245/A, işlenmesi amaçlanan suçlar bakımından hazırlık hareketi niteliğindeki eylemleri cezalandırılmasını hüküm altına almıştır. Hedef suçları işlemek amacıyla bu cihazları, programları, şifre veya sair güvenlik kodları ile madde metninde sayılan fiilleri gerçekleştiren kişilerin hem bu suçtan hem de amaçladıkları hedef suçu da işlemeleri halinde o suçtan ayrı ayrı cezalandırılmaları gerekmektedir[355] yani gerçek içtima kuralları uygulama alanı bulur.

Örnek olarak failin ürettiği, satın aldığı, bulundurduğu cihaz, program, şifre kod ile TCK md. 244'de düzenlenen suçlardan herhangi birisini işlemesini verebiliriz. Bu durumda fail her iki kanun maddesinden ayrı ayrı cezalandırılacaktır. Aynı şekilde failin ürettiği, bulundurduğu, satın aldığı bir cihaz veya programla başkasına ait bir banka hesabıyla ilişkilendirerek sahte banka veya kredi kartı üretmesi durumunda faile hem TCK md. 245/2'den hem de TCK md. 245/A'dan dolayı ayrı ayrı ceza verilecektir.[356]

Mevzuatımıza yeni dahil edilen inceleme konumuz olan madde, seçimlik hareketli bir suç tipidir. Birden çok seçimlik hareket aynı anda işlense dahi tek suç söz konusu olacaktır.

Suçların içtimaı şekillerinden ilki bileşik suç kurallarıdır. Bileşik suç bağımsız suç olarak kabul edilen fiilin, bir başka suçun temel veya nitelikli halinin

---

[353] Artuk/Gökcen/Alşahin/Çakır, s. 723; Hakeri, s. 595, Göktürk, Neslihan, *Fikri İçtima*, Adalet Yayınevi, Ankara 2013, s. 6.

[354] Hakeri, s. 59.

[355] Dülger, s. 459.

[356] Özbek/Doğan/Bacaksız/Tepe, s. 1040.

unsurunu oluşturması ve failin, unsur olan bu suçtan dolayı ayrıca sorumlu olmaması şeklinde tanımlanabilir.[357] TCK md. 42 gereğince bu tür suçlarda içtima hükümleri uygulanmaz. Bu kapsamda fail aslında birden fazla suç işlese de kanundan dolayı söz konusu suçlar, hukuki anlamda tek fiil ve tek suç olarak kabul edilmekte ve fail hakkında tek bir cezaya hükmedilmektedir.[358]

Suçların içtimaı şekillerinden bir diğeri ise zincirleme suçtur. Zincirleme suçta bileşik suçtan farklı olarak birbirinden farklı suçların birden fazla işlenmesi değil, aynı suçun birden fazla defa işlenmesi söz konusudur. [359] TCK m. 43/1 çerçevesinde failin birden fazla işlediği aynı suç bakımından zincirleme suç hükümlerinden yararlanabilmesi için bu suçları aynı kişiye karşı ve aynı suç işleme kararı kapsamında farklı zamanlarda işlemesi şartları aranmaktadır. Bu şartların gerçekleşmesi halinde kanuna göre faile verilecek ceza dörtte birinden dörtte üçüne kadar artırılacaktır.

İnceleme konumuz olan suçun konusunu oluşturan cihaz, program, şifre veya kodun çok sayıda temin edilerek madde metninde sayıların fiillerin gerçekleştirilmesi halinde tek suçtan bahsedilecektir. Elbette bu durum TCK md. 61 kapsamında cezanın belirlenmesinde göz önüne alınacaktır. Bu hareketlerin bir suç işleme kararının icrası kapsamında farklı zaman dilimlerinde gerçekleştirilmesi halinde ise zincirleme suç hükümleri devreye girecektir.[360]

Suçların içtimaı şekillerinden sonuncusu olan sonuncusu, fikri içtima[361] ise, "tek fiilde birden fazla suçun birleşmesi; tek ve aynı fiil ile aynı suçun birden fazla (aynı nev'iden fikri içtima) yahut birden fazla farklı suçun (farklı nev'iden fikri içtima) işlenmesi" şeklinde açıklanabilir.[362] Buradaki temel husus, tek fiil ile birden

---

[357] Özgenç, s. 567-568.

[358] Göktürk, s. 132

[359] Özgenç, s. 572.

[360] Koca/Üzülmez, *Özel Hükümler*, s. 916; Korkmaz, s. 53.

[361] Göktürk, s. 61-63; Koca, Mahmut; "Fikri İçtima", *Ceza Hukuku Dergisi*, 2007, Cilt 2, Sayı 4, s. 199.

[362] Göktürk, s. 59.

fazla suçun işlenmesidir.[363] Tek eylem ile aynı suçun birden fazla işlenmesi durumunda aynı neviden fikri içtima hali söz konusu olurken, tek fiille birden fazla farklı suçun işlenmesi durumunda ise farklı neviden fikri içtima hali gerçekleşmektedir. TCK md. 43/2'de aynı neviden fikri içtima hali, aynı suçun birden fazla kişiye karşı tek bir fiille işlenmesi yer almaktadır. TCK md. 43/2, bir fikri içtima hali olmasına rağmen kanunun zincirleme suç başlıklı 43. maddesinde düzenlenmesi doktrinde eleştiriye uğramaktadır.[364]

Farklı neviden fikri içtimada tek bir fiil ile birden fazla farklı suç işlenmektedir.[365] TCK md. 44'te işlenen tek bir fiille birden fazla farklı suçun oluşması durumunda, failin en ağır cezayı gerektiren suçtan dolayı cezalandırılacağı düzenlenmiştir. Farklı neviden fikri içtima hükmünün uygulanmasında, tek fiille işlenen birden fazla farklı suçun, görünüşte içtima ilişkisi içerisinde olup olmadığına dikkat edilmesi gerekmektedir.[366] Görünüşte içtima halinde, bir olaya birden fazla norm uygulanabilir görünmekte ancak bunlardan yalnızca birisi uygulanabilmektedir. Bu yüzden görünüşte içtima hallerinden birinin varlığı durumunda suçların içtimaına ilişkin hükümler uygulanamayacaktır. Uygulanacak hüküm, ceza normları arasındaki ilişki ve bu konudaki ilkelere göre belirlenmektedir. Görünüşte içtima halinde fail esasen tek eylemle ile birden fazla suç işlemekte ancak işlenen bu suçlar arasında özel norm – genel norm, asli norm – tali norm ya da tüketen norm – tüketilen norm ilişkisi bulunmaktadır.[367] Görünüşte içtima halinde suçların çokluğu sadece görünüşte kalmaktadır ve gerçekleştirilen eyleme uygulanacak olan esasen bu normlardan sadece bir tanesidir.[368]

---

[363] Koca/Üzülmez, *Genel Hükümler* s. 490-497.

[364] Özgenç, s. 596.

[365] Göktürk, s. 180.

[366] Göktürk, s. 74.

[367] Hakeri, s. 639; Artuk/ Gökcen/Alşahin/Çakır, s. 724.

[368] İçel/Sokullu/Özgenç/Sözüer/Mahmutoğlu/Ünver, *Suç Teorisi*, s. 457

Burada çalışmamıza konu suç açısından bizi ilgilendiren ilişki özel-genel norm ilişkisidir. Özel-norm genel norm ilişkisi bir olaya görünüşte uygulanabilir olan özel ve genel normlarının bulunduğu hallerde ortaya çıkar. Özel norm, genel normun unsurlarını tümüyle kapsamakla birlikte, bazı ilave unsurları da içermektedir. Bu durumda "özel normun önceliği ilkesi" gereğince özel norm niteliğindeki hükümlerin uygulanacağı açıktır. Örneğin 5411 sayılı Bankacılık Kanunu' nun 160. maddesinde düzenlenen zimmet suçu, TCK md. 247'de düzenlenen zimmet suçuna göre özel norm hükmündedir.[369]

TCK md. 245/A'da düzenlenen bu suç ile bazı özel kanunlarda yer alan suçlarla özel norm-genel norm ilişkisi içindedir:

İlk olarak Fikir ve Sanat Eserleri Kanunu'nun, 72. maddesinden bahsedebiliriz. Madde metni şu şekildedir:

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

Düzenlendiği konuya ilişkin olarak FSEK'daki 72. madde, TCK md. 245/A'ya göre özel hüküm niteliğinde olduğundan önceki tarihli olmasına rağmen uygulanmasına devam edilecektir.[370] Benzer durum Elektronik İmza Kanunu'nun 16. maddesi için de geçerlidir. EİK'nın 16. maddesi şu şekildedir:

"Elektronik imza oluşturma amacı ile ilgili kişinin rızası dışında; imza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanlar bir yıldan üç yıla kadar hapis ve elli günden az olmamak üzere adlî para cezasıyla cezalandırılırlar."

---

[369] Artuk/Gökçen/Alşahin/Çakır, s. 724.

[370] Koca/Üzülmez, *Özel Hükümler* s. 916; Akbulut, *Bilişim Alanında Suçlar*, s. 361.

Bu durumda da TCK md. 245/A'ya özel hüküm niteliğinde olan EİK md. 16 uygulama alanı bulacaktır.[371]

Sinyal kesici olarak bilinen jammer cihazının TCK 245/A kapsamında anılan cihazlardan biri olup olmadığı noktasında ise; Elektronik Haberleşme Kanunu'nun "Telsiz kurma ve kullanma izni, telsiz ruhsatnamesi ve kullanıma ilişkin esaslar" başlıklı 37. maddesinin 1. fıkrası:

"Radyo ve televizyon yayınlarına ilişkin ilgili kanununda belirtilen hükümler saklı kalmak kaydıyla, Kurum düzenlemelerinde belirtilen ve işletilmesi için frekans tahsisine ihtiyaç gösteren telsiz cihaz veya sistemi kullanıcıları, telsiz kurma ile kullanma izni ve telsiz ruhsatnamesi almak zorundadır. Bu kapsamdaki kullanıcılar telsiz cihaz veya sistemlerini Kurum düzenlemeleri ve telsiz ruhsatnamesinde belirtilen esaslara uygun olarak kurmak ve kullanmak mecburiyetindedirler." şeklinde düzenlenmiştir.

Aynı kanunun 63. maddesinin 4. fıkrası ise:

"Kurma ve kullanma izni ile ruhsatname alınması gereken telsiz cihazı veya sistemlerini bu Kanunun 37. maddesine aykırı olarak, Kurumdan izin almaksızın satan, kuran, işleten ve kullananlar hakkında iki bin güne kadar adlî para cezası uygulanır." hükmü bulunmaktadır.

Sinyal kesici cihazlarla ilgili olarak, EHK'nda özel düzenleme yer aldığından, TCK md. 245/A hükümleri burada uygulama alanı bulamayacaktır.[372]

Bu noktada 2918 sayılı Karayolları Trafik Kanunu'nun 51. maddesinin 4. fıkrası önem taşımaktadır. Anılan fıkra:

"Hız sınırlarının aşılıp aşılmadığını, tespit etmekte kullanılan cihazların yerini tespit veya sürücüyü ikaz eden her türlü cihazın imalı, ithali ve araçlarda bulundurulması yasaktır." şeklinde düzenlenmiştir. Yine aynı maddenin beşinci ise

[371] Dülger, s. 459-460; Akbulut, *Bilişim Alanında Suçlar*, s. 361.

[372] Korkmaz, s. 50.

fıkrasında bu cihazları imal ve ithal edenler ile bulunduranların cezalandırılacağı hüküm altına alınmıştır."

Bahsi geçen cihazlar açısından 2918 sayılı Karayolları Trafik Kanunu'nda özel düzenleme bulunması nedeniyle TCK md. 245/A kapsamında olmadıkları düşünülmektedir.[373]

5. MUHAKEME, YAPTIRIM, ZAMANAŞIMI VE TÜZEL KİŞİLER HAKKINDA GÜVENLİK TEDBİRLERİ

5.1. Muhakeme

İddia, savunma ve yargılamadan oluşan, soruşturma ile kovuşturma olmak üzere iki aşamada tamamlanan faaliyet ceza muhakemesi olarak ifade edilir.[374]

Soruşturma aşaması, davanın maddi gerçeğe uygun biçimde sonuçlandırılmasını sağlamaya yönelik olarak kovuşturma aşamasının hazırlık evresidir.[375] Bu bağlamda soruşturma aşamasında, delilleri arayıp bulmak ve koruma altına almak amaçlanmıştı.[376] Soruşturma aşamasında toplanan delillerden iddiaların gerçek olmadığı kanaatine varılırsa ya da suçu ispata yetecek kadar delil toplanamazsa, muhakemede kovuşturma aşamasına geçiş yapılmayacaktır.[377]

Suç haberinin öğrenilmesiyle soruşturmanın mecburiliği ilkesi gereği, soruşturma savcılık tarafından resen başlatılır ve yürütülür.[378] Suçun işlendiğine ilişkin olarak yeterli şüphe oluşturacak delil elde edilmişse savcılık makamınca

---

[373] Korkmaz, s. 50.

[374] Özbek/Doğan/Bacaksız/Tepe, s. 262.

[375] Centel, Nur/Zafer, Hamide; *Ceza Muhakemesi Hukuku*, Beta Yayınları, İstanbul 2015, s. 79

[376] Centel/Zafer, s. 79; Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/SaygılarKırıt,Yasemin/Özaydın, Özdem/… Erden Tütüncü, Efser*; Nazari ve Uygulamalı Ceza Muhakemesi Hukuku,* Ankara 2016., s. 581.

[377] Toroslu, Nevzat/Feyzioğlu, Metin; *Ceza Muhakemesi Hukuku*, Savaş Yayınevi, Ankara 2016, s. 271, Soyaslan, Doğan; *Ceza Muhakemesi Hukuku*, Yetkin Yayınevi, Ankara 2014, s. 364.

[378] Centel/ Zafer, s. 621.

iddianame düzenlenir ve iddianamenin kabulü ile kovuşturma aşaması başlamış olur.[379]

Bazı durumlarda, soruşturmanın veya kovuşturmanın başlatılması belirli şartların varlığına bağlanabilir. Bu şartlara da muhakeme şartları denilmektedir.[380] Bu noktada ifade etmek gerekir ki fikri içtima ilişkisinden söz edebilmek için ilgili suç tipleri açısından aranan muhakeme şartlarının da her suç tipi açısından gerçeklemesi şarttır.[381] Muhakeme şartlarının gerçekleşmediği suçlar, fikri içtima ilişkisine konu olamazlar. Tek fiille işlenen iki suçtan biri resen, diğeri şikâyete tabi olarak takibi yapılıyorsa, şikâyet şartı gerçekleşmeyen suç, fikri içtima ilişkisi içerisinde göz önünde bulundurulmayacak ve resen kovuşturulan suçun cezası daha hafif olsa bile fail hakkında bu suçtan hüküm kurulacaktır.[382]

Bu genel bilgiler ışığında; inceleme konumuz olan yasak cihaz veya programlar başlıklı suç herhangi bir muhakeme şartına bağlı olmayıp soruşturması ve kovuşturması re'sen yapılmaktadır.[383]

5.2. Görevli ve Yetkili Mahkeme

Görevli mahkeme, 5235 sayılı Adlî Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş, Görev ve Yetkileri Hakkında Kanun'un 8. vd maddeleri uyarınca tayin edilmektedir. TCK md. 245/A'da düzenlenen suçun yaptırımının üst sınırı 3 yıl hapis cezası olduğundan 5235 sayılı Kanun'un 11. ve 12. maddeleri göz önünde bulundurulduğunda, görevli mahkeme asliye ceza mahkemesi olacaktır.

---

[379] Öztürk ve diğerleri *Ceza Muhakemesi Hukuku*, s. 602, Yenisey,Feridun/Nuhoğlu, Ayşe, *Ceza Muhakemesi Hukuku*, Seçkin Yayıncılık, Ankara 2016, s. 558.

[380] Öztürk ve diğerleri *Ceza Muhakemesi Hukuku*, s. 44.

[381] Göktürk, s. 208.

[382] Göktürk, s. 208.

[383] Koca/Üzülmez, *Özel Hükümler* s. 916; Dülger, s. 460.

Bilişim suçlarına ilişkin yetki ve uygulanacak kanun bakımından TCK ve CMK'da özel bir düzenleme bulunmamaktadır. Genel kural olarak "yer bakımından uygulama" başlıklı TCK md. 8'de "Türkiye'de işlenen suçlar hakkında Türk kanunları uygulanır. Fiilin kısmen veya tamamen Türkiye'de işlenmesi veya neticenin Türkiye'de gerçekleşmesi halinde suç, Türkiye'de işlenmiş sayılır." hükmüyle mülkilik ilkesi kabul edilmiş durumdadır.[384] Buna göre fiil kısmen ya da tamamen Türkiye'de işlenmiş ya da netice Türkiye'de gerçekleşmiş ise fail ve mağdurun vatandaşlığına bakılmaksızın eylem ile ilgili olarak Türk Ceza Kanunu uygulanacak ve Türk mahkemeleri yetkili olacaktır. Mülkilik ilkesinin yanı sıra suç Türkiye'de işlenmemiş olsa dahi faile göre şahsilik (TCK md.11), mağdura göre şahsilik (TCK md. 12) ve evrensellik ilkeleri (TCK md. 14) uyarınca da bazı suçlar açısından Türk Ceza Kanunu uygulama alanı bulacaktır.[385]

TCK md. 245/A'da düzenlenen suç, sırf hareket suçudur ve bu nedenle, hareketin kısmen veya tamamen gerçekleştirildiği yer mahkemesi yetkili mahkeme olarak kabul edilmektedir.

Yasak cihaz veya programlar suçu bakımından da failin gerçekleştirdiği fiilin, failin ülke içinde ya da ülke dışında bulunmasına bakılmaksızın, bir kısmı Türkiye'de gerçekleşiyorsa TCK md. 245/A uygulanacaktır. Akbulut da hareketin bir kısmı Türkiye' de diğer kısmı başka bir ülkede gerçekleştirildiğinde suçun Türkiye' de işlenmiş olacağını ve yetkili mahkemenin CMK md. 12'ye göre tayin edileceğini dile getirmiştir.[386]

Ülke içinde yetkili mahkemenin belirlenmesinde ise genel kural *"yetkili mahkeme"* başlıklı CMK md. 12'de dile getirilmiş,[387] suçun işlendiği yerin belli

---

[384] Centel/ Zafer, s. 63, Soyaslan, *Ceza Muhakemesi Hukuku*, s. 98.

[385] Soyaslan, *Ceza Muhakemesi Hukuku*, s. 101-110.

[386] Akbulut, *Bilişim Alanında Suçlar*, s. 362-363.

[387] CMK md. 12 şu şekilde düzenlenmiştir: "(1) Davaya bakmak yetkisi, suçun işlendiği yer mahkemesine aittir. (2) Teşebbüste son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği yer mahkemesi yetkilidir."

olmaması durumuna ilişkin olarak özel yetki kuralı ise CMK md. 13'te düzenlenmiştir.[388]

Seçimlik hareketlerden birkaçı gerçekleştirilmişse her hareketin gerçekleştirildiği yer de suçun işlendiği yer olduğundan oradaki mahkemeler de yetkili mahkeme olarak kabul edilecektir. Yine aynı şekilde seçimlik hareketlerden birinin Türkiye' de işlenmesi Türkiye' deki yer mahkemesinin yetkili olmasına sebebiyet verecektir. İnternet üzerinden fiilin işlendiği hallerde kişin beden olarak bulunduğu yer ile hedef bilgisayarın bulunduğu yer de suçun işlendiği yer olduğundan birinin Türkiye' de gerçekleşmesi halinde Türkiye'deki yer mahkemesi yetkili mahkeme olacaktır. Yetki uyuşmazlıklarında CMK'nın 17. maddesi, soruşturma aşamasında yetkiye ilişkin sorun ortaya çıkmışsa CMK'nın 161/7. maddesi uygulama alanı bulacaktır.

Ülke içinde işlenen suçlarda zincirleme suç, kesintisiz suç veya teşebbüs söz konusuysa yetkili mahkeme CMK'nın 12/2 maddesinde çözüme kavuşturulmuştur. Suç yabancı ülkede işlenmiş ve Türkiye' de yargılama yapılmasının mümkün olduğu hallerde hangi mahkemenin yetkili olduğu CMK md. 14'de ifade edilmiştir.[389]

5.3. Yaptırım

TCK md. 245/A'da yaptırım olarak, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür. Suç için yaptırım olarak hapis ve adli para cezası birlikte düzenlenmiştir. TCK'nın sisteminde bu durum, genellikle işlenmesi suretiyle ekonomik kazancın elde edildiği suçlarda tercih edilmektedir.[390] Seçimlik

---

[388] CMK md. 13 hükümleri şöyledir: "1) Suçun işlendiği yer belli değilse, şüpheli veya sanığın yakalandığı yer, yakalanmamışsa yerleşim yeri mahkemesi yetkilidir. (2) Şüpheli veya sanığın Türkiye'de yerleşim yeri yoksa Türkiye'de en son adresinin bulunduğu yer mahkemesi yetkilidir. (3) Mahkemenin bu suretle de belirlenmesi olanağı yoksa, ilk usul işleminin yapıldığı yer mahkemesi yetkilidir."

[389] Akbulut, *Bilişim Alanında Suçlar*, s. 362-363.

[390] Koca/Üzülmez, *Özel Hükümler* s. 916

ceza öngörülmediği için cezalandırılabilirliğin tüm şartları gerçekleştiğinde faile her iki ceza birden verilir.[391]

Hâkim, hapis cezasını TCK md. 61'e göre belirleyecek ve TCK md. 62 uyarınca takdiri indirim nedenlerinin varlığı halinde cezada altıda birine kadar indirim uygulayabilecektir. Her ne kadar TCK md. 245/A'da suçun karşılığında hapis cezası ve adli para cezası birlikte öngörülmüş ise de CMK md. 231'de aranan objektif koşulların da varlığı halinde verilen hapis cezası iki yıl veya altında ise hükmün açıklanmasının geri bırakılması hükümlerinin uygulanmasına bir engel yoktur. Burada hapis cezasının iki yıl veya altında olması önem taşırken birlikte verilen adli para cezasının miktarının önemi yoktur. Ancak TCK md. 51 kapsamında, iki yıl veya takdiri indirim nedeninin uygulanması suretiyle daha az hapis cezası verilirse, adli para cezasından bağımsız olarak bu hapis cezasının ertelenmesine ilişkin hükümler uygulama alanı bulabilecektir.[392]

Adli para cezasında ise hâkim, birim gün sayısını TCK md. 61/1'e göre temel ceza olarak belirleyecek ve ardından bir gün karşılığı ödenecek para miktarını, kişinin ekonomik durumu, malvarlığı ile bir günde kazandığı veya kazanması gereken gelire bakarak 20 TL ile 100 TL arasında tayin edecektir.[393] Birim gün sayısının alt sınırı TCK md. 245/A'da belirlenmediğinden bu sınır beş gün olarak kabul edilmesi zorunluluktur. Kaldı ki bu suçta adli para cezasının seçimlik olarak değil hapis cezasının yanı sıra uygulanacağı belirtilmiştir. Üst sınır ise maddede beş bin gün olarak düzenlenmiştir.

Adli para cezasının, hapis cezasının yanı sıra uygulanmasının öngörüldüğü suçlarda kanun koyucu, suçla elde edilen ekonomik çıkarın tespit edilip kazanç müsaderesine ilişkin hükümlerin uygulanamaması durumunda, suçtan elde edilen gelirin kişinin yanına kâr kalmamasını sağlamayı amaçlamıştır.[394] Bundan dolayı bu

---

[391] Dülger, s. 460.

[392] Koca/Üzülmez, *Genel Hükümler*, s. 572.

[393] Erdelen, Erdal, *Cezanın Belirlenmesi (Türk-Alman Uygulaması),* Ankara 2013, s. 338-339.

[394] Özgenç, s. 779.

tür suçlarda genellikle adli para cezasının alt sınırı belirlenmemişken üst sınırın da yüksek olarak belirlenmesi yoluna gidilmiştir.[395] TCK 245/A'da düzenlenen suçu işleyen failin haksız ekonomik kazanç elde etmesi söz konusu olabilmektedir. Buna göre suçtan elde edilen gelir, tamamen müsadere edilmişse, sanığa artık adli para cezasının verilmemesi gerekecektir, ancak kanun hükmü gereği bu artık mümkün olmadığından, sanığa en azından adli para cezasının kanundaki alt sınırını yani beş günü vermek yerinde olacaktır.[396] Ancak suçtan elde edilen gelirin tespit edilememesi durumunda ise para cezasının alt sınırı ile üst sınırı arasında belirleme yapılacaktır.[397]

5.4. Zamanaşımı

Ceza hukukunda zamanaşımı, devletin ceza verme hakkını ortadan kaldırmaktadır. Dava zamanaşımı ve ceza zamanaşımı şeklinde ikiye ayrılmaktadır.

Suçun işlenmesinden sonra suça ilişkin kanun maddesinde yazılı belirli sürenin geçmesine rağmen dava açılmamışsa veya dava açılıp da sonuçlandırılmamışsa dava zamanaşımı gerçekleşmiş olur. Ancak ceza verilip kesinleştikten sonra mahkûmiyet hükmünün belirli süre içerisinde infazına başlanamaması halinde ceza zamanaşımı söz konusu olacaktır.[398]

TCK md. 245/A'da düzenlenen suçun yaptırımı olarak bir yıldan üç yıla kadar hapis ve beş bin güne kadar adli para cezası öngörülmüştür. Bu suça ilişkin dava zamanaşımı süresi TCK md. 66/1-e hükmü gereğince 8 yıl, ceza zamanaşımı süresi ise TCK md. 68/1-e'de belirtildiği üzere 10 yıldır. Zamanaşımının suçun işlendiği andan itibaren başladığı kabul edilmektedir. Bu sürelerin başlangıcı noktasında dava zamanaşımının başlangıcı çalışmamız açısından önem arz etmektedir. TCK 66. maddesinin 6. fıkrası şu şekildedir:

---

[395] Özgenç, s. 779.

[396] Koca/Üzülmez, *Genel Hükümler*, s. 656-657.

[397] Akbulut, *Bilişim Alanında Suçlar*, s. 362.

[398] Artuk/Gökcen/Alşahin/Çakır, s. 970.

"Zamanaşımı, tamamlanmış suçlarda suçun işlendiği günden, teşebbüs halinde kalan suçlarda son hareketin yapıldığı günden, kesintisiz suçlarda kesintinin gerçekleştiği ve zincirleme suçlarda son suçun işlendiği günden, çocuklara karşı üstsoy veya bunlar üzerinde hüküm ve nüfuzu olan kimseler tarafından işlenen suçlarda çocuğun on sekiz yaşını bitirdiği günden itibaren işlemeye başlar."

TCK md. 245/A'da düzenlenen suç sırf hareket suçu olduğu için hareketin yapılmasıyla suç oluşur ve zamanaşımı süresi işlemeye başlar. Eğer temadi eden bir fiille bu suç işlenmiş ise temadinin kesildiği anda zamanaşımı süresi başlamış olur.[399]

5.5. Tüzel Kişiler Hakkındaki Güvenlik Tedbirleri

TCK m. 246'da[400] "bilişim alanında suçlar" bölümünde düzenlenen suçların işlenmesi suretiyle, tüzel kişi yararına haksız menfaat sağlanması durumunda tüzel kişilere özgü güvenlik tedbirlerine karar verileceği düzenleme altına alınmıştır. Bu kapsamda TCK md. 245/A'da düzenlenen suç bakımından da tüzel kişilere özgü güvenlik tedbirleri uygulama alanı bulacaktır. Bu güvenlik tedbirleri TCK m. 60'a göre faaliyet izninin iptali ve müsadere olarak düzenlenmiştir.[401] Yine söz konusu güvenlik tedbirleri, aynı madde uyarınca ancak özel hukuk tüzel kişileri hakkında uygulanır. Bu tedbirlerin uygulanması için bahsi geçen tüzel kişilerin işlenen suç ile haksız bir menfaat elde edilmesi durumunda hükmedilebilecektir.[402] Burada tüzel kişilerin suç işlenmesinin odak noktası olmalarının önünde geçmek amaçlanmıştır. Hükmün uygulanabilmesi için haksız menfaatin ekonomik nitelik taşıması da şart değildir.[403]

---

[399] Artuk/Gökçen/Alşahin/Çakır, s. 995.

[400] TCK Madde 246- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

[401] Demirbaş, s. 661.

[402] Akbulut, *Genel Hükümler*, s. 826.

[403] Gül, s. 243, Parlar, Ali, *Türk Ceza Hukuku'nda Bilişim Suçları*, Bilge Yayınları (2. Baskı), Ankara 2014, s. 210.

Faaliyet izni ile, TCK m. 60'da belirtildiği üzere, bir kamu kurumunun verdiği faaliyet izni kastedilmektedir. Faaliyet izninin iptali güvenlik tedbirine hükmedilmesi halinde tüzel kişilik son bulmamaktadır.[404] Bu güvenlik tedbirine hükmedilebilmesi için suçun, tüzel kişinin organ veya temsilcisi tarafından gerçekleştirilmesi ve suçu işleyen ya da suça iştirak eden organ veya temsilci hakkında mahkumiyete karar verilmiş olması aranır.[405] Ayrıca organ veya temsilcinin işlediği suçun, faaliyet izninin sağladığı yetkinin kötüye kullanılması suretiyle işlenmesi şarttır. Gerçekleştirilen suçla faaliyet izninin kullanılması arasında bir nedensellik bağının bulunması kaçınılmazdır.[406]

Faaliyet izninin yanında tüzel kişi hakkında eşya veya kazanç müsaderesine hükmedilmesi TCK m. 246'da hüküm altına alınmıştır. TCK md. 60/2'de müsadere için tek şart olarak işlenen suç ile tüzel kişi yararına bir menfaat elde edilmiş olması şartı aranmaktadır.[407] Bu şart gerçekleşmiş olmak kaydıyla, tüzel kişi yararına işlendiği belirlenen TCK md. 245/A bakımından, suçla bağlantılı olan eşya veya maddi çıkarların müsaderesine karar verilecektir.

Önemle belirtmek gerekir ki, TCK md. 60/3'te lehine haksız menfaat elde edilen tüzel kişi hakkında güvenlik tedbirinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkaracağı durumlarda hâkimin bu tedbirlere hükmetmeyebileceği düzenlenmiştir. Hâkim, suçun verdiği zarar ile tedbirin verilmesi ile ortaya çıkacak zararı karşılaştırmalı ve tedbir uygulandığında daha büyük bir zarar ortaya çıkacağına kanaat getiriyorsa, söz konusu tedbire hükmetmekten kaçınmalıdır.[408]

---

[404] Akbulut, *Genel Hükümler*, s. 827.

[405] Öztürk ve diğerleri, *Ceza Muhakemesi Hukuku,* s. 535.

[406] Artuk/Gökçen/Alşahin/Çakır, s. 960.

[407] Öztürk ve diğerleri, *Ceza Muhakemesi Hukuku,* s. 535.

[408] Gedik, Doğan; *Müsadere*, Adalet Yayınları, Ankara 2007, s. 154.

SONUÇ

"Yasak cihaz veya programlar" suçu, 5237 sayılı TCK'nın "topluma karşı suçlar" kısmının, "bilişim alanında suçlar" başlıklı onuncu bölümünde düzenlenmiştir.

Bu suç, 24.03.2016 tarihinde kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 30. maddesinin 5. fıkrasıyla Türk Ceza Kanunu'na eklenen yeni bir suç tipidir. Bu maddenin düzenleniş amacı, bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen diğer suçların icrası kapsamında gerçekleştirilen hazırlık hareketlerinin cezalandırılmasıdır. Bilişim suçlarıyla etkin ve caydırıcı bir mücadele politikasının izlenmesi adına, bilişim suçu faillerinin suç işleme kararı verdikleri ve suçun icrası kapsamında gerçekleştirdikleri hazırlık hareketlerinin hüküm altına alınıp cezalandırılmasının sağlanması son derece olumlu bir adımdır. Böylece TCK'nın 245/A maddesinin kabulüyle hukuk sistemimizdeki önemli bir boşluk da doldurulmuştur.

AKSSS'ye taraf devletler, bu sözleşmeyi imzalayarak sözleşmede düzenlenen suçları iç hukuklarına dahil etme yükümlülüğü altına girmişlerdir. AKSSS'yi imzalayarak sözleşmeye taraf olan Türkiye de uluslararası sözleşmeden doğan bir yükümlük altındadır. Bu kapsamda kanun koyucu, AKSSS'nin " Cihazların kötüye kullanımı" başlıklı 6. maddesinin karşılığı olarak inceleme konumuz olan TCK m. 245/A' yı düzenlemiş ve uluslararası sözleşmeden doğan yükümlülüğünü yerine getirmiştir.

TCK 245/A maddesinin başlığı, suçun konusunu ifade etmekte olduğu, maddenin içeriğine ilişkin herhangi bir ön izlenim oluşturmadığı, ayrıca suçun konusunu oluşturan cihaz ve programların yasaklı olduğu belirtilmesine rağmen madde metninde bu cihaz ve programların yasaklı olduğuna ilişkin bir ibare bulunmadığı hususlarından yola çıkılarak doktrinde bizimde hak verdiğimiz şekilde eleştirilmektedir.

TCK 245/A maddesi, madde metninde açık bir şekilde belirtildiği gibi, münhasıran bilişim alanında suçlar bölümünde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenen suçların icrası kapsamındaki hazırlık hareketlerini cezalandırmaktadır. Bu husus dikkate alındığında suçla korunan hukuki değer karma nitelik arz etmektedir. Maddede sayılan fiillerin gerçekleştirilmesi, günümüzde hayatın her alanına giren bilişim sistemlerinin hukuka aykırı amaçlar için kullanıldığına yönelik toplumda bir kanaat oluşmasına sebebiyet verecektir. Bu kapsamda ilk olarak kamunun bilişim sistemlerine yönelik güveni korunmak istenmiştir. Ayrıca maddenin kapsamına giren diğer suçlarla korunan hukuki değerler de bu madde ile güvence altına alınmak istenmiştir.

TCK 245/A maddesinde düzenlenen suçun hukuki konusu, bilişim suçları ve bilişim sistemlerinin araç olarak kullanılması suretiyle suç işlenmesi için yapılmış ya da oluşturulmuş olan cihaz, bilgisayar programı, şifre ve sair güvenlik kodu olarak belirlenmiştir. Burada pentest (sızma/zafiyet) adı verilen testler farklılık arz etmektedir. Bu testlerle bilişim sistemlerinin güvenliği belirli aralıkla denetlenmektedir. Eğer cihaz, bilgisayar programı, şifre veya sair güvenlik kodunun bir bilişim sisteminin güvenliğinin test edilmesi veya korunması amacıyla yapılmış veya oluşturulmuş ise herhangi bir suçun gerçekleşmediği kabul edilecektir.

Madde metnine yapılan bir diğer eleştiri de şifre ve sair güvenlik kodu kavramlarına yöneliktir. Cihaz ve programlara yönelik olarak suçun hukuki konusu rahatlıkla anlaşılmasına rağmen şifre ve sair güvenlik kodunun tam olarak neyi ifade ettiğinin belirsiz kaldığı, kanun koyucunun ne tür şifre ve kodları suçun hukuki konusu olarak kabul ettiğinin anlaşılamadığı yönünde eleştiriler mevcuttur. Belirlilik ilkesi kapsamında biz de bu eleştirilere katılıyoruz.

TCK 245/A maddesinde sayılan suçun işlenmesine neden olan fiillerin sınırlı sayıda olduğu ve bu kapsamda suçun bağlı hareketli bir suç tipi olduğu kabul edilmektedir. Ayrıca “yayma” fiiline de yer verilmemiştir. Yayma fiili, bir kişinin elindeki bir şeyi birden fazla kişiye vermesi, ulaştırması olarak tanımlanmaktadır.

Cihaz, program, şifre veya güvenlik kodunun birden çok kişiye verilmesi, ulaştırılması anlamına gelecek olan yayma fiili bilişim sistemleri açısından tehlikeye neden olabilecektir. TCK 245/A'da düzenlenen suç kapsamında yayma fiilinin yer almasının bu suçla mücadelede açısından faydalı olacağı kanaatindeyiz. Ayrıca bilişim suçu işleme yöntemlerine her geçen gün bir yenisinin eklendiği hususunu da göz önünde bulundurduğumuzda maddedeki fiillerin sınırlı sayıda sayılmasının bu suçla mücadele açısından yerinde bir düzenleme olmadığını düşünüyoruz.

Bu suç ancak kasten işlenebilir. Failin suçun konusunu oluşturan cihaz, şifre veya programı maddede belirtilen suçları işlemek amacıyla imal etmesi, ithal etmesi, sevk etmesi, nakletmesi, depolaması, kabul etmesi, satması, satışa arz etmesi, satın alması, başkalarına vermesi ya da bulundurması gerekirse de bu cihaz veya programı kullanarak hedef suçları işlemesi gerekmemektedir.

İnceleme konumuz olan TCK 245/A maddesi için iki hukuka uygun nedeni söz konusu olabilir.

İlki kanun hükmünün yerine getirilmesi, ikinci ise ilgilinin rızası kavramıdır.

TCK 245/A maddesinin kabulüyle beraber hem internet kullanıcıları hem de hosting ve bilgi güvenliği firmaları, ceza sorumluluğu ile karşı karşıya kalmamak için, pentest başta olmak üzere bu tür yazılımları temin ederken veya bulundururken en üst düzeyde özen göstermeleri, yapacakları faaliyetleri muhakkak yazılı bir sözleşme ile ve bu sözleşme kapsamında kalarak yapmaları önerilmektedir. Aksi takdirde, bir suç isnadıyla karşılaştıklarında bu yazılımları hukuka uygun nedenlerle bulundurdukları hususunda kendilerinin savunurken sorun yaşamaları muhtemeldir.

TCK md. 245/A, işlenmesi amaçlanan suçlar bakımından hazırlık hareketi niteliğindeki eylemlerin cezalandırılmasını hüküm altına almıştır. Hedef suçları işlemek amacıyla bu cihazları, programları, şifre veya sair güvenlik kodlarını imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişilerin hem bu suçtan hem de amaçladıkları hedef suçu da işlemeleri halinde o suçtan ayrı ayrı cezalandırılacaklardır.

Bir anlamda hedef suçların da gerçekleşmesi durumunda gerçek içtima hükümleri uygulanacaktır.

TCK md. 245/A'da düzenlenen bu suç ile bazı özel kanunlarda yer alan suçlarla özel norm-genel norm ilişkisi söz konusudur. TCK 245/A maddesi ile

Fikir ve Sanat Eserleri Kanunu'nun 72. maddesi,

Elektronik İmza Kanunu'nun 16. maddesi,

Karayolları Trafik Kanunu'nun 51. maddesi

Elektronik Haberleşme Kanunu'un 37. ve 63. maddeleri arasında özel-norm genel norm ilişkisi bulunmaktadır. Sayılan kanun maddelerine ilişkin bir suç işlenirse TCK'nın 245/A maddesi değil özel norm niteliğindeki yukarıda sayılan kanun maddeleri uygulanacaktır.

Kanaatimizce inceleme konumuz olan maddede öngörülen cezanın alt ve üst sınırı düşüktür. TCK'nın 245/A maddesinde öngörülen cezanın alt sınırı 1 yıldan başlamaktadır. Bilindiği üzere, bilişim suçu faillerinin tespit edilmesi ve yakalanması oldukça zordur ve bilişim suçlarının yıkıcı sonuçları diğer suçlara nazaran çok daha fazladır. Tüm bu hususlar göz önüne bulundurulduğunda, bilişim suçlarına sebep olan hazırlık hareketlerinin cezalandırılması noktasında, ülkemizde yürürlükte olan ceza infaz rejimleri de dikkate alındığında öngörülen cezanın yeterli etkinlikte ve caydırıcılıkta olduğunu düşünmüyoruz. Bu doğrultuda yasada gerekli değişiklik yapılarak suç için öngörülen alt ve üst sınırlar arttırılmalıdır.

Çalışmamız boyunca ifade etmeye çalıştığımız üzere TCK'nın 245/A maddesi ile münhasıran bilişim alanında yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların icrası kapsamındaki hazırlık hareketleri cezalandırılmak istenmiştir. Bu yeni suç tipinin düzenlenmesi ile hem bilişim suçlarıyla mücadele noktasında hukukumuzda var olan boşluk doldurulmuş hem de AKSSS'ye taraf olmanın getirdiği uluslararası sözleşmeden doğan yükümlülük yerine getirilmiştir. Biz kanun maddesine ilişkin olarak düşündüğümüz eksiklikleri yeri geldiğince belirtmeye çalıştık.

Uygulama noktasında ise çalışmamızın kaleme alındığı tarih baz alındığında suç tipinin yeni olması nedeniyle bize ışık tutabilecek ya da eksiklikleri giderebilecek nitelikte bir yargı kararı ortaya çıkmamıştır. Bahsettiğimiz eksiklikler yasal düzenlemelerle giderildiği takdirde bilişim suçlarıyla mücadelede kritik bir öneme sahip olan hazırlık hareketlerinin cezalandırılması amacı tam manasıyla yerine getirilmiş olacaktır.

Bu noktada, bilişim suçlarıyla mücadele açısından bütün akademik çalışmaların ortak paydası niteliğindeki tedbirlere, önemlerini bir kez daha dile getirmek ve altlarını bir kez daha çizmek adına biz de burada yer veriyoruz.

Bilişim suçları için, kendisine özgü yapısı gereği coğrafi alan sınırlaması söz konusu değildir, internet bulunan her yerde işlenebilmektedir. Suç işleyen kişilerin bu suçları yaptırım altına almayan ülkelere sığınması ve suçları orada işlemeleri halinde gerçekleştirdikleri suç cezasız kalabilmektedir. Bu durumun önüne geçilebilmesi için uluslararası iş birliğinin arttırılması kaçınılmazdır. Bu kapsamda AKSSS'ye üye devletlerin sayısının arttırılması ilk akla gelen çözüm önerilerinden biridir.

Yine bilişim suçlarının önlenebilmesi için, bilişim sistemi kullanıcıları suça karşı nasıl davranacakları noktasında aydınlatıp eğitilmeli, bu suçlara ilişkin olarak konusunda uzman hukukçu ve kolluk görevlilerinin sayısının artması için gereken adımların atılmalı, gelişen teknolojiye ve beraberinde ortaya çıkan yeni bilişim suçu işleme yöntemlerine uygun şekilde hem güncel hem de bilişim suçlarıyla mücadelede etkin ve caydırıcı yasal düzenlemeler yapılmalıdır.

KAYNAKÇA

Açıkgöz, Emre İkbal, *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu*, (Yayınlanmamış Yüksek Lisans Tezi), Yıldırım Beyazıt Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2017.

Akarslan, Hüseyin, *Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2012.

Akarslan, Hüseyin, *Bilişim Suçları*, Seçkin Yayıncılık (2. Baskı), Ankara 2015.

Akbulut, Berrin, *Bilişim Alanında Suçlar*, Adalet Yayınevi (2. Baskı), Ankara 2017.

Akbulut, Berrin, *Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2016.

Akbulut, Berrin Bozdoğan, *"Bilişim Suçları*", Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, Konya, Cilt 8, Sayı 1-2, s. 545-555.

Alaca, Bahaddin, *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)*, (Yayınlanmamış Yüksek Lisans Tezi), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2008.

Alp, Barış Emre, *5237 Sayılı Türk CEZA Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu*, (Yayınlanmamış Yüksek lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2018.

Altınok, Ebru/Vural, Ali Fatih, *"Bilişim Suçları*", Denetişim Dergisi, 2011, Sayı 8, s. 74-84.

Artuk, M. Emin/Gökçen, Ahmet/Yenidünya, Caner, *Ceza Hukuku Özel Hükümler*, Adalet Yayınevi, 13. Baskı, Ankara 2013.

Artuk,M.Emin/Gökcen,Ahmet/M.Emin,Alşahin/Çakır,Kerim *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi (12. Baskı) Ankara 2018

Avcı, Artun, *Türkiye'de İnternet ve İfade Özgürlüğü*, Legal Yayıncılık, İstanbul 2013.

Avşar, Zakir/Öngören, Gürsel; *Bilişim Hukuku*, İstanbul 2010.

Aydın, Emin Doğan, *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınevi Ankara 1992.

Aydın, Emin Doğan, "*Bilişim Sistemlerinde Güvenlik, Güvenilirlik, Mahremiyet ve Bilişim Suçları*", Marmara İletişim Dergisi, 1992, Sayı 1.

Aygün Eşitli, Ezgi, "*Suçların Ve Cezaların Kanuniliği İlkesi*", TBB Dergisi, 2013, Sayı 104, s. 225-246.

Beygu, Şahin, *Yayıncılıkta Bilgisayar El Kitabı*, Yalçın Ofset Matbaası, İstanbul 1990.

Boğa, Uğur, *Bilişim Suçlarıyla Mücadele Yöntemleri*, (Yayınlanmamış Uzmanlık Tezi), RTÜK, Ankara 2011.

Canbek, Gürol/Sarıoğlu, Şeref, "*Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma"*, Başkaya, Şenol (Ed.), Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 2007, Cilt 22, No. 1.

Centel, Nur/Zafer, Hamide; *Ceza Muhakemesi Hukuku*, Beta Yayınları, İstanbul 2015.

Centel, Nur/Zafer, Hamide/Çakmut, Özlem, *Türk Ceza Hukukuna Giriş*, Beta Yayınları, İstanbul 2016.

Çakır, Hüseyin/Kılıç, Mehmet Serkan**,** *Güncel Tehdit Siber Suçlar*, Seçkin Yayıncılık, Ankara 2014.

Çekiç, Burak, *İnternet Aracılığı İle İşlenen Suçlar*, (Yayınlanmamış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2006.

Değirmenci, Olgun, *Bilişim Suçları*, (Yayınlanmış Yüksek Lisans Tezi), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2002.

Demirbaş, Timur, *Ceza Hukuku Genel Hükümler,* Seçkin Yayıncılık, Ankara 2016.

Demircan, Tunç, *Bilişim Alanında Suçlar*, Legal Yayıncılık, İstanbul 2016.

Demirkol, Zafer, *İnternet Teknolojileri*, Pusula Yayıncılık, İstanbul 2001.

Doğan, Ramazan, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Suçları*, Adalet Yayıncılık, Ankara 2014.

Dülger, Murat Volkan, *Bilişim Suçları ve İnternet İletişim Hukuku*, Seçkin Yayıncılık (7. Baskı), Ankara 2018.

Erdağ, Ali İhsan, "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)", *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, 2010, Cilt 14, Sayı 2, s. 75-303.

Erdelen, Erdal, *Cezanın Belirlenmesi (Türk-Alman Uygulaması),* Ankara 2013.

Erdoğan, Yavuz, *Avrupa Konseyi Siber Suçlar Sözleşmesi'nde Yer Alan Koruma Tedbirleri ve Bu Tedbirlerin Türk Hukukundaki Yeri*, Legal Yayıncılık (1. Baskı), İstanbul 2018.

Ergün, İsmail, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* Ankara 2008.

Ermeydan, Damla, *Türk Ceza Kanunu'nda Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Çağ Üniversitesi SBE, Mersin 2018.

Gedik, Doğan; *Müsadere*, Adalet Yayınları, Ankara 2007.

Göktürk, Neslihan, *Fikri İçtima*, Adalet Yayınevi, Ankara 2013.

Güleş, Hasan Kürşat, "*Bilişim Sistemlerinin Toplam Kalite Yönetimindeki Yeri ve Önemi",* Dokuz Eylül Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2000, Cilt 15, Sayı 1.

Güngör, Necmi Murat, *Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2007.

Gül, Ahmet, *Doğrudan-Dolaylı Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2018.

Gürler, Fazıl, *Teknik Ve Hukuksal Yönleriyle Bilişim Alanında Suçlar,* (Yayınlanmamış Yüksek Lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2013.

Hafızoğulları, Zeki/Özen, Muharrem, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2015.

Hafızoğulları Zeki/Özen Muharrem, *Türk Ceza Hukuku Özel Hükümler Topluma Karşı Suçlar*, U.S.A Yayıncılık, Ankara 2016.

Hakeri, Hakan, *Ceza Hukuku Genel Hükümler*, Adalet Yayınevi (21. Baskı), Ankara 2017.

Hekim, Hakan., "*Oltalama (Phishing) Saldırıları",* Tombul, F., Güneştaş, M., Başıbüyük, O. (Ed.), Siber Suçlar Tehditler, Farkındalık ve Mücadele, Global Politika ve Strateji, Ankara 2015.

Helvacıoğlu, Aslı Deniz, "*Avrupa Konseyi Siber Suç Sözleşmesi-Temel Hükümlerin İncelenmesi"*, Yeşim Atamer (Ed.), İnternet ve Hukuk, İstanbul, Bilgi Üniversitesi Yayınları, 2004, No. 51.

Henkoğlu, Türkay, *Adli Bilişim Dijital Delillerin Elde Edilmesi ve Analizi*, Pusula Yayınları, İstanbul 2014.

İçel, Kayıhan, "*Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt 59, Sayı 1-2.

İçel, Kayıhan; *Ceza Hukuku Genel Hükümler*, İstanbul 2016.

İçel, Kayıhan/Sokullu Akıncı,Füsun/Özgenç, İzzet/Sözüer, Adem/Mahmutoğlu, Fatih Selami/Ünver, Yener; *Suç Teorisi*, İstanbul 2000.

İlbaş, Çığır, *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Analizi*, (Yayınlanmış Yüksek Lisans Tezi), Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara 2009.

Kan, İsmet, *Bilgisayar Temel İlkeleri ve Basic*, Uludağ Üniversitesi Yayınları, Bursa 1990.

Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayıncılık (4. Baskı), Ankara 2013.

Karagülmez, Ali, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri*, Seçkin Yayıncılık (5. Baskı), Ankara 2014,

Kaya, Mehmet Bedii, *Teknik ve Hukuki Boyutlarıyla İnternete Erişimin Engellenmesi*, İstanbul 2010.

Keskin Kiziroğlu, Serap, "*Avrupa Konseyi Siber Suç Sözleşmesinde Ceza Muhakemesine İlişkin Hükümlerin Değerlendirilmesi*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 2013, Cilt 59, Sayı 1-2, s. 155-180.

Ketizmen, Muammer, *Türk Ceza Hukukunda Bilişim Suçları*, Ankara 2008.

Kızıltan, Mehmet Burak, *5237 Sayılı Türk Ceza Kanunu'nda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2006.

Koca, Mahmut; "*Fikri İçtima*", Ceza Hukuku Dergisi, 2007, Cilt 2, Sayı 4.

Koca, Mahmut/Üzülmez, İlhan, "Türk Ceza Hukuku Genel Hükümler", Ankara 2016.

Koca, Mahmut/Üzülmez, İlhan, "Türk Ceza Hukuku Özel Hükümler", Adalet Yayınevi (5. Baskı), Ankara 2018.

Korkmaz, İbrahim, "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu", *Terazi Hukuk Dergisi*, 2018 (Haziran), Cilt 13, Sayı 148.

Köksal, Aydın, *Adı Bilgisayar Olsun*, İstanbul 2010.

Kurt, Levent, *Açıklamalı, İçtihatlı Tüm Yönleriyle Bilişim Suçları*, Seçkin Yayıncılık, Ankara 2005.

Mahmutoğlu, Fatih Selami, "*Karşılaştırmalı Hukuk Bakımından İnternet Sujelerinin Ceza Sorumluluğu*", İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, 2001, Cilt 59, Sayı 1-2.

Odabaşı, Arda, *Bilgi Toplumu mu, Gözetim Toplumu mu? Bilim ve Ütopya*, İstanbul 1999.

Orsorlu, Ahmet, *P2P Sistemlerde İstemci Eş Tabanlı Eş Seçim Modeli*, (Yayınlanmamış Yüksek Lisans Tezi), Gebze Yüksek Teknoloji Enstitüsü Mühendislik ve Fen Bilimleri Enstitüsü, Kocaeli 2011.

Ölmez, Aslan, "*Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Kopyalama ve Bunlara El Koyma*", THD (Terazi Hukuk Dergisi), Şubat 2009, Yıl 4, Sayı 30.

Önok, Murat; "*Avrupa Konseyi Siber Suç Sözleşmesi Işığında Siber Suçlarla Mücadelede Uluslararası İşbirliği*", Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, (Prof. Dr. Nur Centel'e Armağan), 2013, Cilt 19, Sayı 2.

Özbek, Veli Özer, "*Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu*", Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi (DEÜHFD), 2007, Cilt 9 (Özel Sayı).

Özbek, Veli Özer/Doğan, Koray/Bacaksız,Pınar/Tepe, İlker., *Türk Ceza Hukuku Özel Hükümler*, Seçkin Yayıncılık (13. Baskı), Ankara 2018.

Özdilek, Ali Osman, *İnternet ve Hukuk*, Papatya Yayıncılık, Ankara 2002.

Özen, Muharrem/Baştürk, İhsan, *Temel Hak ve Özgürlükler Bağlamında Bilişim-İnternet ve Ceza Hukuku*, Ankara 2011.

Özgenç, İzzet, *Türk Ceza Hukuku Genel Hükümler*, Seçkin Yayıncılık, Ankara 2016.

Özkaya, Elif, "*Bilgi Teknolojisinin Yarattığı Parazitler*", Gürdilek, Raşit (Ed.), NTV Bilim Dergisi, 2009, Sayı 1.

Öztürk, Bahri/Tezcan, Durmuş/Erdem, Mustafa Ruhan/Sırma Gezer, Özge/SaygılarKırıt,Yasemin/Özaydın, Özdem/… Erden Tütüncü, Efser; *Nazari ve Uygulamalı Ceza Muhakemesi Hukuku*, Ankara 2016

Pallı, Hayati, *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri 2008.

Parlar, Ali, *Türk Ceza Hukuku'nda Bilişim Suçları*, Bilge Yayınları (2. Baskı), Ankara 2014.

Sınar, Hasan, *Avrupa Konseyi Siber Suç Sözleşmesi Üzerine Bir Deneme,* Prof. Dr. Çetin Özek Armağanı, İstanbul 2004.

Sınar, Hasan, *İnternet ve Ceza Hukuku*, Beta Yayınevi (1. Baskı), İstanbul 2001.

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

Soyaslan, Doğan; *Ceza Muhakemesi Hukuku*, Yetkin Yayınevi, Ankara 2014.

Soyaslan, Doğan, *Ceza Hukuku Özel Hükümler*, Yetkin Yayınları, 8. Baskı, Ankara 2010.

Sönmez, Yağmur, *Günümüz İnternet Ortamında Bilişim Suçları ve Türkiye'deki İnternet Haber Sitelerine Yansımaları*, (Yayınlanmamış Yüksek Lisans Tez), Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul 2018.

Taşkın, Şaban Cankat, "*Bilişim Hukuku Uluslararası Anlaşmazlıklar*", Türkiye Barolar Birliği (TBB) Dergisi, 2009, Sayı 85.

Taşkın, Şaban Cankat, *Bilişim Suçları*, Beta Yayınları, Bursa 2008.

Taşkın, Şaban Cankat, *İnternete Erişim Yasakları,* Ankara 2016.

Topaloğlu, Mustafa, *Bilgisayar Programları Üzerindeki Haklar ve Bu Hakların Korunması*, Altan Matbaacılık, İstanbul 1997.

Toroslu, Nevzat/Toroslu, Haluk, *Ceza Hukuku Genel Kısım*, Savaş Yayınevi, Ankara 2016.

Toroslu, Nevzat/Feyzioğlu, Metin, *Ceza Muhakemesi Hukuku*, Savaş Yayınevi, Ankara 2016.

Turhan, Oğuz, *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar*), Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Uzmanlık Tezi, Ankara 2006.

Uçar, Hüdaverdi, *Türk Ceza Kanunu'nda Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2014.

Ünal, Ahmet, *"Dağıtık Servis Dışı Bırakma (DDOS) Saldırıları: Güncel Yöntemler ve Mücadele"* Tombul F.; Güneştaş M.; Başıbüyük O. (Ed.), Siber Suçlar Tehditler, Farkındalık ve Mücadele, Global Politika ve Strateji, Ankara 2015, s. 11-36.

Ünal, Cahide/ Şahin, İsmail, "*İstenmeyen Elektronik Postaların (SPAM) Filtrelenmesi İçin Bir Uzman Sistem Tasarımı ve Gerçekleştirilmesi",* Politeknik Dergisi, 2017, Sayı 20.

Ünver, Yener, *Ceza Hukukuyla Korunması Amaçlanan Hukuksal Değer*, Seçkin Yayıncılık, Ankara 2003.

Yalvaç, Gürsel, *Ceza ve Yargılama Hukukuna İlişkin Temel Kavramlar Gerekçeli TCK CMK CGTİK*, Adalet Yayınevi (17. Baskı), Ankara 2018.

Yaycı, Esra, *Bilişim Suçları*, (Yayınlanmamış Yüksek Lisans Tezi), Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2007.

Yazıcıoğlu, R. Yılmaz, *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*, İstanbul 1997.

Yenidünya, A. Caner/Değirmenci, Olgun, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık (1. Baskı), İstanbul 2003.

Yenidünya, A. Caner, "*Bilişim Sistemine Hukuka Aykırı Erişim Suçu*", Legal Fikri ve Sınai Haklar Dergisi, 2005, Sayı 4.

Yenisey, Feridun/Nuhoğlu, Ayşe; *Ceza Muhakemesi Hukuku*, Seçkin Yayıncılık, Ankara 2016.

Yılmaz, Davut, *Hacking Bilişim Korsanlığı ve Korunma Yöntemleri*, Hayat Yayınları, İstanbul 2004.

Zafer, Hamide, *Ceza Hukuku Genel Hükümler TCK m 1-75*, Beta Yayınları (6. Baskı), İstanbul 2016.

Elektronik Kaynaklar

http://www.mugla.pol.tr/fethiye/Sayfalar/Casus-Yaz%C4%B1l%C4%B1m-Nedir.aspx (erişim tarihi 21.04.2019).

https://eezgiozgenn.wordpress.com/zararli-yazilim-nedir/ (erişim tarihi 21.04.2019).

http://www.hurriyet.com.tr/bilgisayar-kullanicilari-oltaya-geliyor-21226684 (erişim tarihi: 11.04.2019).

http://bidb.itu.edu.tr/eskiler/seyirdefteri/blog/2013/09/07/denial-of-service-(dos)-sald%C4%B1r%C4%B1lar%C4%B1-ve-korunma-y%C3%B6ntemleri (erişim tarihi 11.04.2019).

Bölükbaş, Candan, "Yeni Nesil Teknolojik Silahlar: DoS/DDoS" (22 Aralık 2014), https://siberbulten.com/makale-analiz/yeni-nesil-teknolojik-silahlar-dosddos/ (erişim tarihi 11.04.2019).

https://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zararli-yazilim-imal-etme-bulundurma-sucu.html (erişim tarihi 22.04.2019).

https://www.google.com/search?q=p%C4%B1npad+nedir&rlz=1C1GCEU_trTR821TR821&oq=PINPAD+&aqs=chrome.0.69i59j35i39j69i57j0l3.5456j0j8&sourceid=chrome&ie=UTF-8 (erişim tarihi 21.04.2019).

http://finans.mynet.com/haber/detay/ekonomi/kart-dolandiricilari-yeni-kopyalama-yontemi-deep-insert-skimmer/129517/ (erişim tarihi: 16.04.2019).

http://www.bocekarama.com/ (erişim tarihi 21.04.2019).

http://betulsen6.blogspot.com/2014/12/program-ve-yazilim-arasindaki-farklar.html (erişim tarihi 21.04.2019);

http://bagcidilara.blogspot.com/2014/12/yazlm-ile-program-arasndaki-fark.html (erişim tarihi 21.04.2019).

http://www.bilgimikoruyorum.org.tr/?b311_zararli_program_ne_demektir (erişim tarihi 14.04.2019).

http://www.e-data.com.tr/her-gun-780-yeni-zararli-yazilim-kullanicilarin-online-banka-bilgilerini-calmaya-calisiyor.aspx (erişim tarihi 14.04.2019).

https://www.haberturk.com/zararli-yazilimdan-14-yil-hapis-cezasi-yedi-2170477-ekonomi (erişim tarihi 14.04.2019).

https://www.difose.com.tr/zararli-yazilim-laboratuvari/ (erişim tarihi 21.04.2019).

http://www.elithukuk.com/yeni-bir-bilisim-sucu-zararli-yazilim-ve-yasak-cihaz/ (erişim tarihi 22.04.2019).

http://www.bilisimdergisi.org.tr/yazarlar/konuk-yazarlar/penetrasyon-testlerinin-pentestlerin-hukuki-durumu-zararli-yazilimlar.html (erişim tarihi 22.04.2019).

https://www.semseo.com.tr/rehber/seo-sozlugu/hiperlink-nedir-hiperlink-ne-ise-yarar (erişim tarihi 21.04.2019).

http://www.mevzuat.gov.tr/MevzuatMetin/1.3.2559.pdf (erişim tarihi 21.04.2019).

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=bcOvBBEj (erişim tarihi : 04.07.2019)