ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
KAMU HUKUKU ANA BİLİM DALI

YÜKSEK LİSANS TEZİ

TEKNİK VE HUKUKSAL YÖNLERİYLE BİLİŞİM ALANINDA SUÇLAR

FAZIL GÜRLER

MAYIS 2013

Tez Başlığı : **Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar**

Tezi Hazırlayan : **Fazıl GÜRLER**

Sosyal Bilimler Enstitüsü Onayı:

Prof. Dr. Mehmet YAZICI
Sosyal Bilimler Enstitüsü Müdür Vekili

Bu tezin yüksek lisans derecesi elde etmek için gerekli koşulları sağladığını onaylarım.

Prof. Dr. Hamdi MOLLAMAHMUTOĞLU
Kamu Hukuku Bölüm Başkanı

Bu tez, tarafımdan incelenmiş olup Yüksek Lisans Tezi olarak uygun bulunmuştur.

Prof. Dr. Doğan SOYASLAN
Tez Danışmanı

Tez Sınav Tarihi : 02.05.2013

Tez Jüri Üyeleri :

Prof.Dr. Doğan SOYASLAN (Çankaya Üniv.) .....

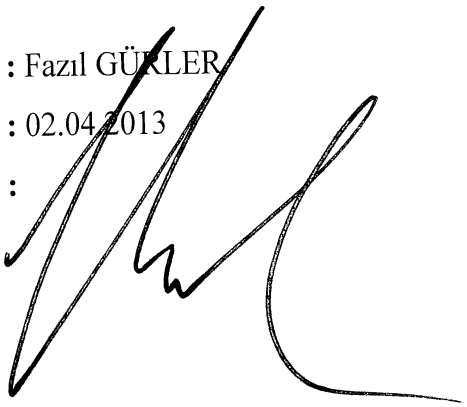
Doç.Dr. Devrim GÜNGÖR (Ankara Üniv.) .....

Y.Doç.Dr. Ali Uğur ERİŞ (Çankaya Üniv.) .....

ÇANKAYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Bu belge ile bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmamda bana ait olmayan tüm veri, düşünce ve sonuçları bilimsel etik kurallarını gözeterek ifade ettiğimi ve kaynağını gösterdiğimi de ayrıca beyan ederim.

Adı Soyadı : Fazıl GÜRLER
Tarih : 02.04.2013
İmza :



ÖZET

TEKNİK VE HUKUKSAL YÖNLERİYLE BİLİŞİM ALANINDA SUÇLAR

GÜRLER, Fazıl

Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı

Tez Danışmanı: Prof. Dr. Doğan SOYASLAN

Mayıs 2013, 186 sayfa

XX. yüzyılın ikinci yarısında, önce bilgisayarın daha sonra da bilgisayar ağları ve internetin bulunmasıyla, klasik iş ve ticaret hayatı, haberleşme yöntemleri ve sosyal hayat daha önceki dönemlerde yüzyıllar sonrasında ulaşabildiği gelişmeleri 20-30 yıl içinde kat etmiştir. Bu yeniçağa "Bilişim Çağı" adı verilmiştir.

Toplumları her alanda dönüştüren, şekillendiren, hayatımızı büyük oranda kolaylaştıran bilişim çağında teknolojinin sürekli ve hızla gelişmesine paralel olarak, kötüye kullanılması yöntemleri de ortaya çıkmıştır. Bu suç yöntemleri klasik suç işleme şekillerinin dışında "*bilişim suçu*" olarak adlandırılan yeni suç türleridir.

Maddi konular dikkate alınarak yasalaştırılmış olan klasik ceza hukuku normları, bu yeni ve soyut suç türlerini önlemekte yetersiz kalmıştır. Toplumsal ihtiyaçlara göre şekillenen hukuk düzeni, eski yasalarla önlenemeyen bilişim suçlarına karşı, yeni düzenlemeler yaparak bu ihtiyaca karşılık vermiştir. Bu düzenlemeleri bazı devletler ceza yasalarına ek hükümler koyarak yaparken, bir kısım devletler ise yeni ceza yasaları çıkarmışlardır. Ülkemiz bu yeni suç işleme yöntemlerini ceza yasasına yeni hükümler ekleyerek önlemeye çalışan ülkeler arasındadır.

Bilişim suçlarıyla ilgili ilk hukuksal düzenlemeler 1980'li yıllarda ABD'de yapılmıştır. Ülkemizde ise ilk düzenleme 1991 yılında, 765 sayılı Eski Türk Ceza Kanunu'na "Bilişim Alanında Suçlar" başlığı altında (525/a-d) maddesi eklenerek yapılmıştır. Bilişim alanında yapılan bu düzenlemeler 2005 yılında yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu'nda yine "Bilişim Alanında Suçlar" başlığı altında (m.243-246) maddeleri arasında yer almıştır. Çalışmamın konusu 5237 sayılı Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altında yer alan bu düzenlemelerdir.

Çalışmamın konusunu 5237 sayılı Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altında yer alan suçlar olarak sınırladım. Bu sınırlamaya gitmeseydim bilişim alanında işlenebilecek olan zimmet, dolandırıcılık, haberleşmenin gizliliğinin ihlali, özel hayatın gizliliğini ihlal, hakaret, tehdit gibi, ceza yasamızda yer alan bilişim alanında işlenebilecek suçlar ile diğer yasalarda düzenlenmiş olan ve bilişim alanı kullanılarak işlenebilecek suç türleri de çalışma kapsamına girecekti. Bu durumda ise incelenecek alan ve yasalar çok genişleyecek ve bir yüksek lisans teziyle karşılanamayacak noktalara gelecekti.

Bilişim suçları büyük oranda teknolojinin araç olarak kullanıldığı suç türleridir. Söz konusu teknoloji; bilgisayar, internet ve bilişim gibi teknik alt kavramları içermektedir. Bu teknik kavramlar bilişim suçlarının unsurunu veya konusunu oluşturmaları yönüyle bilişim alanındaki suçların inceleneceği bir tez çalışmasında mutlaka yer alması gereken kavramlardır. Anılan teknik kavramların tanımı ve incelemesi yapılmadan, bilişim suçları konusunun anlaşılamayacağı ortadadır. Bu nedenle, iki bölümden oluşan çalışmamın birinci bölümünde; bilişim, bilgisayar, bilgisayar ağları, internet, internetin tarihsel gelişim süreci, bilişim suçları kavramı, bilişim suçlarının sınıflandırılması ve bilişim suçlarının işlenme yöntemleri gibi teknik hususlar incelenmiştir. İkinci bölümde Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altında düzenlenen, bilişim sistemine girme, sistemi engelleme ve bozma suçlarının yanı sıra, sistemdeki verilere çeşitli fiillerle zarar verme, bu yolla menfaat elde etme suçları ile banka ve kredi kartlarının araç olarak kullanıldığı bilişim suçları üzerinde durulmuştur.

Sözkonusu suç türleri incelenirken yasayla yapılan düzenlemelerin Yargıtay uygulamaları doğrultusunda uygulamaya yansımaları üzerinde durulmaya çalışılmıştır. Her iki bölümde de yeri geldikçe karşılaştırılmalı (mukayeseli) hukukta yapılan düzenlemelere de yer verilmiştir.

Anahtar Kelimeler: Bilgisayar, Bilişim, Bilişim Alanı, İnternet, Bilişim Suçları, Siber Suçlar, Türk Ceza Kanunu, Gerçek Bilişim Suçları, Banka Kartları, Kredi Kartları

ABSTRACT

TECHNICAL AND LEGAL ASPECTS OF INFORMATICS IN THE FIELD OF CRIME

GÜRLER, Fazıl

Graduate School of Social Sciences, Department of Public Law

Thesis advisor : Prof. Dr. Doğan SOYASLAN

May 2013, 186 pages

In the second half of the XXth century, by the invention of computers and the then the computer networks, classical business and trade life, communication methods and social life covered distance only in 20-30 years which took centuries previously. This new era is called "Information Age".

In parallel to constant and rapid development of technology at this information age which transforms and shapes societies in every areas and makes our lives easier to a large extent, also methods for abusing technology have appeared. These crime methods are the new crime types called as "*cyber crime*" except classical perpetration methods.

Classical penal code norms which have been legislated by considering physical facts remain incapable for preventing this new and abstract crime types. Legal orders shaped according to communal requirements had to make new arrangements against cyber crimes which could not be prevented by old laws. While some countries carry out these arrangements by inserting additional provisions into penal codes, some countries have made new penal codes. Our country is among those who are trying to prevent these new crime methods by inserting additional provisions into penal codes.

First legal arrangements on cyber crimes were made in 1980s in the USA. In Turkey, the firs arrangement was done in 1991 by adding a provision under the title of "Crimes in the Field of Informatics" (525/a-d) into the former Turkish Penal Code No. 765. These arrangements made in the field of informatics also were included into the new Turkish Penal Code No. 5237 enacted in 2005 as provisions under the title of "Crimes in the Field of Informatics" (Articles 243-246).

My study focuses on these arrangements given under the title of "Crimes in the Field of Informatics" in Turkish Penal Code No. 5237. I limited the subject of my study with the crimes given under the title of "Crimes in the Field of Informatics" in Turkish Penal Code No. 5237. If I did not limit my study, then the crimes that might be included into the field of informatics given in our penal code such as embezzlement, fraud, violation of the confidentiality of communication, violation of privacy, libel, and threat, and other crimes set forth by other legal codes that might be committed by using field of informatics would be included into the subject of my study. In this case, the fields and laws to be analyzed would be expanded and it would come to a point that could not be provided by a postgraduate thesis.

Cyber crimes are the crime types in which technology is used as a tool substantially. The technology includes technical sub-concepts such as computer, Internet and informatics. They are the technical concepts that should take part in a thesis study where crimes in the field of informatics will be analyzed. It is obvious that cyber crimes cannot be understood without making the definition and analysis of these technical concepts. Therefore, in my study which has two chapters, technical subjects such as informatics, computers, computer networks, Internet, historical development progress of Internet, the concept of cyber crimes, classification of cyber crimes and methods of committing cyber crimes have been analyzed in the first chapter.

In the second chapter, the crimes of damaging data in the system and generating benefits in this way and also the cyber crimes where bank and credit cards are used as a tool as well as crimes of hacking into informatics system, and preventing and impairing system which have been arranged under the title of "Crimes in the Field of Informatics" in Turkish Penal Code have been emphasized.

When analyzing these crime types, it has been deliberated on the arrangements made by the laws and their reflections to practice in accordance with the decisions of Turkish Supreme Court. In both chapters, arrangements made in comparative law have been included as the occasion arises.

Keywords: Computer, Informatics, Field of Informatics, Internet, Cyber Crimes, Turkish Penal Code, Real Cyber Crimes, Bank Cards, Credit Cards,

İÇERİK

İKİNCİ BÖLÜM

TÜRK CEZA KANUNU'NDAKİ BİLİŞİM ALANINDA SUÇLAR

KISALTMALAR

a.g.e. : Adı geçen eser

a.g.m. : Adı geçen makale

AİHM : Avrupa İnsan Hakları Mahkemesi

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

ARPA : Advanced Research Project Agency (İleri Araştırma Projeleri Ajansı)

ATM : Automated Teller Machine (Otomatik Ödeme Makinesi)

AÜEHF : Atatürk Üniversitesi Erzincan Hukuk Fakültesi

AÜHF : Ankara Üniversitesi Hukuk Fakültesi

AÜSBE : Ankara Üniversitesi Sosyal Bilimler Enstitüsü

B. : Baskı, Basım

bkz. yuk. : Eserin içinde yukarıya atıf

BKKKK : 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu

BKM : Bankalararası Kart Merkezi

Bkz. : Bakınız

BÜFBE : Başkent Üniversitesi Fen Bilimleri Enstitüsü

C. : Cilt

CD : Ceza Dairesi (Yargıtay)

CK : Ceza Kanunu

CPU : Central Process Unit (Merkezi İşlem Birimi)

DEÜHF : Dokuz Eylül Üniversitesi Hukuk Fakültesi

EDVAC : Electronic Discrete Variable Automatic Computer (Kesikli Değişkenli Otomatik Elektronik Bilgisayar)

ENIAC : Electronic Numerical Integrator And Calculator (Elektronik Numara Entegreli Hesaplayıcı)

ETCK : 765 sayılı Eski Türk Ceza Kanunu (Mülga)

EÜHF : Erzincan Üniversitesi Hukuk Fakültesi

FÜSBE : Fırat Üniversitesi Sosyal Bilimler Enstitüsü

FSEK : 5846 sayılı Fikir ve Sanat Eserleri Kanunu

GÜHF : Gazi Üniversitesi Hukuk Fakültesi

GÜSBE : Gazi Üniversitesi Sosyal Bilimler Enstitüsü

İBÜ : İstanbul Bilgi Üniversitesi

İES : İnternet Erişim Sağlayıcılar

İİS : İnternet İçerik Sağlayıcılar

IP : İnternet Protocol (İnternet Protokolü)

İSS : İnternet Servis Sağlayıcı

İÜHF : İstanbul Üniversitesi Hukuk Fakültesi

k.g. : Karşı Görüş

KH : Kamu Hukuku

LAN : Local Area Network (Yerel Alan Ağı)

LDR : Işığa Duyarlı Yarı İletken Elemanlar

LED : Light Emitting Diode (Işığa Duyarlı Diyot)

m. : Madde

MAN : Metropolitan Area Network (Şehirsel Bilgisayar Ağları)

MEB : Milli Eğitim Bakanlığı

MERNİS : Merkezi Nüfus ve İdare Sistemi

MÜSBE : Marmara Üniversitesi Sosyal Bilimler Enstitüsü

ODTÜ : Orta Doğu Teknik Üniversitesi

POS Cihazı : Point of Sale (Satış Noktası Terminali)

RAM	: Read Acces Memory (Rastgele Okunan Bellek)
RG.	: Resmi Gazete
ROM	: Read Only Memory (Salt Okunabilir Bellek)
s.	: Sayfa
S.	: Sayı
SÜSBE	: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü
TAKBİS	: Tapu Kayıt ve Bilgi Sistemi
TBB	: Türkiye Barolar Birliği
TCK	: 5237 sayılı Türk Ceza Kanunu
TCP	: Transmission Control Protocol (İletim Kontrol Protokolü)
TCP/IP	: Transmission Control Protocol /İnternet Protocol (İletim Kontrol Protokolü /İnternet Protokolü)
TDK	: Türk Dil Kurumu
TRABİS	: .tr ağ bilgi sistemi
ULAKBİM	: Ulusal Akademik Ağ ve Bilgi Merkezi
ULAKNET	: Ulusal Akademik Ağ
UYAP	: Ulusal Yargı Ağı Projesi
vb.	: Ve benzeri
v.d.	: Ve diğerleri
WAN	: Wide Area Network (Geniş Alan Ağı)
www.	: World Wide Web (Dünya Çapında Ağ)
YCGK	: Yargıtay Ceza Genel Kurulu
YKD	: Yargıtay Kararları Dergisi

GİRİŞ

İlk çağlarda insanlar hayatlarını avcılık ve toplayıcılık gibi fiziksel güç gerektiren faaliyetler ile sürdürüyorlardı. Söz konusu faaliyetler için bir bilgi birikimine ihtiyaç yoktu. Sanayi devrimiyle birlikte insan gücünün yerini makine gücünün almasıyla insanların yaşam şekilleri değişti, ticaret hayatı uluslararası boyut kazandı. Makine gücünü kullanarak gemilerle, yeni yerler keşfeden ülkeler bu faaliyetlerinin neticesinde, ticari hayatta öne geçmeye ve refah seviyelerini artırmaya başladılar. Diğer tacirlerin bilmediği ticari bilgilere ulaşıp, bu bilgiyi değerlendiren ülkeler ekonomik açıdan dünyada söz sahibi olmaya başladı. Ülkelerden sonra ekonomik açıdan devletler kadar güçlü olan şirketler ve bireyler de ticari sürece dâhil oldular. Bu süreç; modern yaşamın çok önemli bir unsuru olan iletişim teknolojilerinin gelişmesine kadar devam etti.

XX. yüzyılın ikinci yarısında Amerika Birleşik Devletleri'nde, (1950-1960 arası) önce bilgisayar daha sonrada bilgisayar ağları ve internetin bulunmasıyla, hayatın her alanında bilgiye ulaşma, değerlendirme ve saklama yöntemleri hem hız kazandı hem de çok kolaylaştı. Bilişim sistemleriyle verilerin/bilginin toplanması, işlenmesi, aktarılması, kullanılması ve muhafaza edilmesi işlemleri önceki dönemlerde günler, haftalar, hatta aylar alırken, bu işlemler saatler, dakikalar ve hatta saniyeler içinde halledilebilir hale geldi. Bu arada bilişim teknolojisinin ana unsuru olan bilgisayarlar, yazılımlarının sürekli yenilenmesi nedeniyle her altı ayda bir yeni modelleri satışa sunulan, iki yıl içerisinde teknolojisi demode olan cihazlar haline geldi.

Bilişim teknolojisindeki bu baş döndüren gelişmeler ve özellikle internetin (1960-1980 yılları arasında) diğer ülkelerin paylaşımına açılmasıyla; iş, ticaret, pazarlama, reklam, kültür, sanat, edebiyat, spor, iletişim, eğitim, ulaşım ve sosyal hayat olmak üzere kısaca, hayatın her alanında daha önceki dönemlerde görülmeyen olağanüstü değişim ve dönüşümler oldu. Ancak bu derece büyük gelişmeleri

sağlayan en önemli husus, dünya çapında bilgisayar kullanımının yaygınlaşması değil, bütün bilgisayar ve bilgisayar ağlarını birbirine bağlayan genel bir ağ olan internetin yaygın olarak kullanılması oldu.

Bilişim teknolojisinin yansıması olan bu gelişmelerden uluslararası alanda öncelikle devletler ve resmi kurumlar yararlanırken, kişisel bazda kullanım için 10-15 yıllık bir süre daha geçmesi gerekti. İnternetin kişisel kullanıcılar tarafından yaygın olarak kullanılmasıyla coğrafi sınırlar ortadan kalkarak dünya küresel bir köy haline geldi. Artık insanoğlu sanal; özgür, çok hızlı ve sürekli genişleyen, sınır çizilemeyen, denetlenemeyen ama hayatın her alanını kolaylaştıran bir teknolojiyi, *interneti* kullanır hale gelmişti. Bu gelişmeleri hemen benimseyen insanoğlu televizyonun yayılma hızından 3 kat, radyoların yayılma hızından 9 kat daha kısa sürede (3 yıl içinde) 50 milyon kullanıcı sayısına ulaştı.

Uluslararası alanda 1970-1985'li yıllar arasında meydana gelen söz konusu gelişmelerin ana unsuru olan internet bağlantısı, ülkemizde ilk kez 1993 yılında Orta Doğu Teknik Üniversitesi tarafından yapılmıştır. İnternete bağlanma işlemini daha sonra sırasıyla Ege, Bilkent, Boğaziçi ve İstanbul Teknik Üniversitelerinin de sürece dâhil olması takip etti.

Günümüzde, ülkemiz kamu alanında bilişim teknolojileri hayatı kolaylaştırmanın yanında devletin tüm kurumlarında toplumu dönüştürmek ve şekillendirmek amacıyla da kullanılmaktadır. Örneğin; Adalet Bakanlığı'nda UYAP (Ulusal Yargı Ağı Projesi), Nüfus ve Vatandaşlık Genel Müdürlüğü'nde MERNİS (Merkezi Nüfus ve İdare Sistemi), Tapu ve Kadastro Genel Müdürlüğü'nde TAKBİS (Tapu Kayıt ve Bilgi Sistemi) gibi sistemlerle eğitim, ulaşım v.b. tüm alanlarda kamu hizmetinden süratle yararlanılabilmektedir. Örneğin, 24 Mart 2013 tarihindeki Yükseköğretime Geçiş Sınavına (YGS), 2 milyona yakın üniversite adayı öğrenci girerken, bu kadar çok adayın sınav sonuçlarının açıklanması önceki yıllarda birkaç ay sürerken, anılan sınavın sonucu 01.04.2013 tarihinde (8 gün sonra) açıklanmıştır.

Türkiye'de bilişim teknolojilerinin kişisel bazda kullanımı ise 2000'li yıllardan itibaren yaygınlaşmaya başlamıştır. Kişisel kullanım açısından 1990'lardan önce ülkemizde var olmayan, bilgisayar, banka kartları, kredi kartları, internet, web sitesi, GSM, cep telefonu, laptop, SMS, tablet, hotmail, mesajlaşma, sanal sistemler, sanal alışveriş, facebook, twitter, gibi yeni kavram ve sistemleri tanıyıp kullanmaya başladık.

Bilişim sistemlerinin bu kadar yaygınlaşması ve bankacılık işlemlerinde kullanılmaya başlaması, para transferlerinin bu sistemler üzerinden yapılır hale gelmesiyle birlikte, kötü niyetli kişiler de bu sistemleri kullanarak hukuka aykırı menfaat elde etmeye başladılar. "Bilişim suçu" olarak adlandırılan bu suç işleme yöntemleri, bilişim sistemlerinin yayılma hızına paralel olarak hızla yaygınlaştı. Bu sistemlerin kötüye kullanılmasındaki artışların önemli bir nedeni, mağdur ile yüz yüze gelinmediği için, tanınma riskine girmeden daha kolay bir şekilde haksız çıkar elde edilebilmesiydi.

Bilişim suçu işleme yöntemleri, soyut veri veya bilgiler üzerinde ya da aracılığıyla yapıldığı için, maddi suç unsurları için düzenlenmiş olan hukuk normları bu yöntemlere karşı yetersiz kaldı. Yasa koyucular söz konusu değişim ve gelişim hızına ayak uydurmak ve bu tür suçları engelleyebilmek için yeni yasal düzenlemeler yapmak zorunda kaldılar. Bu düzenlemeleri bazı devletler ceza yasalarına yeni hükümler koyarak yaparken, bir kısım devletler ise yeni yasalar çıkarma yoluna gittiler.

Doğal olarak bilişim suçlarını önlemek amacıyla ilk yasalar, 1980'li yıllarda sistemlerin ilk kullanıldığı ABD'de çıkarılmıştır. Uluslararası platformda devletlerin ortak olarak kurallar belirleyerek imzaladıkları ilk sözleşme ise 23.11.2001 tarihinde Macaristan'da imzalanan Avrupa Konseyi Siber Suç Sözleşmesi (Convention On Cyber Crimes)'dir.

Ülkemizde ise bu suç türlerine karşı (Fransız ceza kanunundan etkilenilerek) ilk defa 1991 yılında, 765 sayılı Ceza Yasası'na yeni hükümler eklenerek yasal düzenlemeler yapılmıştır. 765 sayılı kanun 2005 yılında kaldırılınca anılan hükümler bu sefer (Avrupa Konseyi Siber Suç Sözleşmesi hükümleri dikkate alınarak) 5237 sayılı, yeni Türk Ceza Kanunu'nda "Topluma Karşı Suçlar" başlıklı üçüncü kısmın, Onuncu Bölümünde, "Bilişim Alanında Suçlar" başlığı altında 243-246. maddeleri arasında öncekine göre daha kapsamlı olarak yer almıştır.

Çalışmamın konusu ceza yasamızda 243-246. maddeler arasında yer alan bilişim alanındaki suçlardır. Ancak bu tür yeni suç yöntemlerini değerlendirebilmek teknik konuların bilinmesini de gerektirdiğinden, teknik ve hukuksal alanı birleştirerek tez alanı ve başlığını "Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar" olarak belirledim.

Söz konusu alanı; bilişim unsurları kullanılarak işlenebilecek olan, dolandırıcılık, zimmet, güveni kötüye kullanma, özel hayatın gizliliğini ihlal, hakaret ve tehdit gibi ceza yasamızda da düzenlenen pek çok klasik suç ile ceza yasamızın dışında bilişim alanı ve sistemleriyle ilgili diğer yasalarımızda da yasal düzenlemeler olması nedeniyle 5237 sayılı Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altında yer alan düzenlemelerle sınırlamak zorunda kaldım.

İki ana bölümden oluşan çalışmamın birinci bölümünde, bilişim suçlarını inceleyebilmek ve kavrayabilmek için gerekli olan bilişim sistemine ait temel, unsurlar olan bilgisayar, yazılım, donanım, bilgisayar ağları ve internet gibi teknik kavramlar ile bilgisayar ve internetin tarihsel gelişim süreci, bilişim suçu kavramı, bilişim suçlarının sınıflandırılması ve işlenme yöntemleri gibi hususlar incelenmiştir.

İkinci bölümde ise Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altında yer alan, bilişim sistemine girme ve orada kalma (m.243), bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirmek suretiyle hukuka aykırı yarar elde etme (m.244) ve banka veya kredi kartlarının kötüye kullanılması suçları (m.245) konusundaki düzenlemelerdir. Bu bölümde bilişim alanında suçlar başlığı altındaki düzenlemelerin uygulamaya farklı şekillerde yansıması ve bu farklılıkların Yargıtay uygulamaları ışığında giderilmeye çalışılması ve Yargıtay kararlarındaki değişimler üzerinde durdum.

Bilişim alanında suçlar konusunda yapılan bir yüksek lisans tezi çalışmasında yer alması gerekli olan, mukayeseli hukukta yapılan düzenlemeler ve Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)'nin ceza yasamıza yansımalarını ise konu bütünlüğü açısından ayrı bir başlık altında incelemeyip, yeri geldikçe ilgili bölüm içinde değerlendirdim.

BİRİNCİ BÖLÜM

BİLİŞİM SİSTEMİNE AİT TEKNİK KAVRAMLAR VE BİLİŞİM SUÇLARI

1.1. BİLİŞİM VE BİLİŞİM ALANI KAVRAMLARI

İnsanlık, tarihsel süreç içerisinde çeşitli evrelerden geçmiştir. İlk insanların avcılık ve toplayıcılık yaparak yaşamlarını sürdürdükleri dönemde pek fazla bilgiye ihtiyaç yoktu. Daha sonra insan gücünün yerini makine gücünün almasıyla, özellikle ticaret hayatının devam edebilmesi için değişik niteliklere sahip, çok sayıda verinin toplanması, saklanması ve kısa sürelerde bu verilere ulaşılması gibi sorunlar ortaya çıktı. Diğer ülkelerin sahibi olmadığı bilgiye sahip olup, bu bilgiyi en verimli şekilde kullanan ülkeler dünyada söz sahibi olmaya başladı. Bu kapsamda sanayileşmesini tamamlamış, teknolojik olarak ileri seviyede olan batılı ülkeler çok sayıda bilginin toplanması, saklanması ve kısa sürelerde bu verilere ulaşılması gibi sorunları değişik belgeleme teknikleri geliştirerek çözmeye çalıştılar. Bu belgeleme teknikleri; önceleri verilerin saklanması ve bilgiye ulaşılmasını amaç edinen çalışmalarda kullanılmış, daha sonra yeni teknolojik gelişmeler ve veri saklama sistemlerinin bulunmasına bağlı olarak bilginin yönetilmesini ve işlenmesini de amaç edinen ayrı bir bilim dalı haline gelmiştir. Bu süreç; modern yaşamın çok önemli bir unsuru olan iletişim teknolojilerinin gelişmesine (özellikle bilgisayarın bulunmasına) kadar devam etmiştir.

XX. yüzyılın ikinci yarısı ile birlikte (1950'li yıllar) bilgi kavramının niteliği de değişmiştir. İletişim teknolojilerinin yaygın olarak kullanılmadığı dönemlerde durağan nitelikler taşıyan bilgi, günümüz koşullarında sürekli değişen ve takibi için özel sistemlere ihtiyaç duyulan bir biçime, "bilişim"e dönüşmüştür.

Bu çalışmanın temel konusu, bilişim ve bilişim alanında işlenen suçlar olduğundan, çalışmamızın daha iyi anlaşılabilmesi için bilişim ve bilişim alanı

kavramlarının incelenmesi gerekmektedir. Bu amaçla aşağıda sırasıyla bilişim ve bilişim alanı kavramları üzerinde durulmuştur.

1.1.1. Bilişim Kavramı

Genel olarak bilişim suçları ile ilgili tüm eserlerde de belirtildiği üzere bilişim kavramı karşılığında; Fransızcada *information* (bilgi) ve *automatique* (otomatik) kelimelerinin birleşiminden türeyen, bilgi işleyen, değerlendiren, sonuç veren anlamına gelen *"informatique"*, İngilizcede *"informatics"*, Almancada *"informatik"*, İtalyancada *"informatica"*[1] ve İskandinav ülkelerinde ise *"datalogi"* kelimeleri kullanılmaktadır.[2] Türkçede ilk başlarda "enformasyon" olarak kullanılan bu kelimenin yerini daha sonraları Türkçe bir kelime olan "bilişim"[3] terimi almıştır. Ancak daha az olsa da enformasyon kelimesi de kullanılmaktadır.[4]

"Bilişim" teriminin sözlük anlamı; Türk Dil Kurumu (TDK) sözlüğünde "*İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi, enformatik*",[5] AnaBritannica ansiklopedisinde "*Bilginin saklanması ve iletilmesini konu alan akademik ve mesleki disiplin, enformatik*"[6] ve Meydan Larousse ansiklopedisinde "*İnsan bilgisinin, teknik*

---

[1] Doğan Soyaslan, "*Bilişim Alanında Suçlar",* Prof. Dr. Mualla Öncel'e Armağan, Ankara Üniversitesi Hukuk Fakültesi Yayını, No:243, 2009, s.1563; Mesut Budak, "*Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu",* Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara, AÜHF Yayını, 2009, s.15.

[2] Çetin Gümüş, "*Bilişim Suçlarıyla Mücadelede Polisin Eğitimi"*, FÜSBE, Eğitim Bilimleri Anabilim Dalı, Yayımlanmamış Doktora Tezi, Elazığ, 2008, s.26.

[3] "*Bilişim kelimesini 1968 yılında ilk kez kullanan Prof. Dr. Aydın Köksal'dır.*" Çığır İlbaş, "*Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi"*, BÜFBE, İstatistik ve Bilgisayar Bilimleri Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2009 s.1.

[4] Serdar Havuz, "*Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği",* Genelkurmay Başkanlığı Harp Akademisi Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, Uluslararası İlişkiler Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s.14.

[5] http://www.tdk.gov.tr/index.php?option=com_gts&arama TDK sitesi, (çevrimiçi) (Erişim; 04.04.2012).

[6] "AnaBritannica Genel Kültür Ansiklopedisi", İstanbul, Ana Yayıncılık ve Sanat Ürünleri Pazarlama A.Ş. Yayını, C.IV, 1987, s.154.

ekonomik ve sosyal alanlardaki iletişimin, otomatik makinelerde akılcı olarak işlenmesini konu alan bilim"dir, şeklinde tanımlanmıştır.[7] TDK sözlüğündeki tanımda, "*elektronik makineler aracılığıyla bilgi işlenmesi*"; AnaBritannica ansiklopedisinde, "*bilginin saklanması ve iletilmesi*", Meydan Larousse ansiklopedisinin tanımında ise bilginin, "*otomatik makinelerde akılcı olarak işlenmesi*" üzerinde durulmuştur. Anılan tanımlardaki "*elektronik makine*", "*bilgiyi saklayan ve ileten* (makine)*"* ve "*otomatik makine*" olarak bahsedilen "makine"den kastın bilgisayar olduğu açıktır. Sözlüklerdeki tanımlamalar "bilişim" terimi ve "*bilişim bilimi"*nin bilgisayarın bulunmasıyla ortaya çıkan yeni bir kavram ve bilim olduğunu da dolaylı olarak ifade etmektedirler.

Doktrinde ise; "bilişim" teriminin birçok tanımı yapılmasına rağmen bu tanımların birbirinden çok farklı olmadığı, benzer noktalarının fazla olduğu görülmektedir. Bu tanımlardan bazıları şöyledir; Bilişim; insanların teknik, ekonomik ve toplumsal alanlarda iletişim amacıyla kullandığı, biliminde temeli olan bilginin; "*elektronik araçlarla özellikle bilgisayarlar aracılığıyla işlenip, ...iletişim hatları aracılığıyla aktarılması*",[8] "*elektronik makineler aracılığıyla düzenli ve akılcı biçimde toplanması ve işlenmesi*"[9] bilimidir. Bu tanımlar bilginin özellikle, elektronik makineler/bilgisayarlar aracılığıyla işlenmesine vurgu yapmaktadırlar.

Bazı tanımlar ise bilgilerin, sayısal/elektronik hale getirilip işlenmesi ve iletilmesi üzerinde durmaktadırlar. Örneğin; bilginin "*otomatik olarak işlenmesiyle ilgilenen bir yapısal bilim dalı*",[10] "*elektronik olarak işlenip, iletişim hatları aracılığıyla aktarılması*"[11] ya da "*bilgisayarlar aracılığıyla elektronik olarak*

---

[7] "Büyük Larousse, Sözlük ve Ansiklopedisi", İstanbul, Milliyet Yayını, Baskı Milliyet Gazetecilik A.Ş., C.IV, 1986, s.1645.

[8] Berrin Bozdoğan Akbulut, "*Bilişim Suçları"*, **Selçuk Üniversitesi Hukuk Fakültesi Dergisi**, Milenyum Armağanı, C.VIII, S.1-2, 2000, s.546.

[9] Ömer Kuplay, "*Bilişim Suçları ve Hukuku",* **Çağın Polisi Dergisi**, Yıl:6, S.66, Ankara, Haziran 2007, s.42; Tunç Demircan, "*Bilişim Alanında Suçlar"*, SÜSBE Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Konya, 2007, s.12; İlbaş, s.1; Cevat Özel, http://www.hukukcu.com/bilimsel/kitaplar/ bilisim_internet_suclari.htm. "*Bilişim İnternet Suçları",* (çevrimiçi), (Erişim; 28.03.2011).

[10] Gümüş, s.26.

[11] Yüksel Ersoy, "*Genel Hukuki Koruma Çerçevesinde Bilişim Suçları"*, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, Ankara, C.XLIX, S.3-4, 1994, s.151.

depolanması, işlenmesi ve iletilmesidir."[12] Diğer bazı tanımlarda ise bilişim; "*elektronik hale getirilmiş her türlü bilginin, özellikle bilgisayarlar aracılığıyla akılcı biçimde saklanması, işlenmesi ve iletilmesi yoluyla, bilginin kullanıma sunulması bilimi*",[13] "*verilerin toplanmasını, işlenmesini, değerlendirilmesini, dağıtımını ve aktarılmasını sağlayan bilim dalı*",[14] "*bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disiplin",*[15] "*bilginin elektronik ortamda üretilmesi, kaydedilmesi, saklanması, taşınması veya kullanılması ile ilgili cihaz, materyal, işlem ve yöntemler*",[16] "*teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalıdır"*[17] şeklinde tanımlanmıştır.

Yukarıda ifade edilen "bilişim" tanımlarında dikkati çeken ortak özellik; bilginin bilgisayarlar aracılığıyla, elektronik/sayısal bir hale dönüştürülerek, otomatik olarak işlenmesi, saklanması/depolanması ve aktarılmasıdır. Tüm bu tanımlar ışığında, bir tanımlama yapmak gerekirse bilişimi; "*İnsanlığın ortak mirası olarak binlerce yıl içinde ticari, teknik, ekonomik, hukuksal vb. tüm alanlarda üretebildiği ve bilimin ulaşabildiği her tür verinin, elektronik araçlarla, özellikle bilgisayarlar aracılığıyla elektronik/sayısal bir hale dönüştürülerek, düzenli ve akılcı bir biçimde toplanması, işlenmesi, kaydedilmesi, sınıflandırılması, saklanması, bilgi haline dönüştürülmesi ve tüm bu işlemlerin sonuçlarının doğrudan sunulmasını ya da ses,*

---

[12] Muharrem Özen – İhsan Baştürk, *Temel Hak ve Özgürlükler Bağlamında Bilişim–İnternet ve Ceza Hukuku*, Adalet Yayınevi, 1.B. Ankara, Ekim 2011, s.11.

[13] Havuz, s.14.

[14] Fatma Burcu Nacar, "*Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları"*, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, AB Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2010, s.6.

[15] Reşat Yılmaz Yazıcıoğlu, *Bilgisayar Suçları, Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile,* 1.B. İstanbul, Alfa Yayınları, 1997, s.131.

[16] Mustafa İlker Öztürk, "*Bilişim Cihazlarındaki Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri",* Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Disiplinlerarası Adli Tıp Ana Bilim Dalı, Fizik İncelemeler ve Kriminalistik Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2007, s.1.

[17] A. Caner Yenidünya - Olgun Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,* 1.B., İstanbul, Legal Yayıncılık, Nisan 2003, s.27.

görüntü ve/veya veri taşıyabilen kablolu veya kablosuz iletişim hatları aracılığıyla aktarılmasını sağlayan bilim dalıdır," şeklinde tanımlamamız mümkündür.

1.1.2. Bilişim Alanı

Bir eylemin "bilişim suçu" olup olmadığının tespit edilebilmesi için bu eyleme konu olan "bilişim alanı"nın iyi belirlenmesi, sınırlarının çizilmesi gerekmektedir. Bu ihtiyacı karşılayabilmek için, aşağıda önce yasa tasarıları ve yasalarımıza yansıyan yönüyle "bilişim alanı" kavramı incelenip, sonra doktrinde bu konuda yapılan tanım ve değerlendirmeler üzerinde durulacaktır.

Türk hukuk mevzuatında "bilişim" kavramı ilk kez 1989 tarihindeki Türk Ceza Kanunu Ön Tasarısı'nın 342. madde gerekçesinde "bilişim alanı"; "*bilgileri toplayıp depo ettikten sonra bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan*" şeklinde tanımlanarak yer almıştır. 1997 tarihli TCK Tasarısında yine "Bilişim Alanında Suçlar" ibaresi kullanılırken 347. maddenin gerekçesinde bilişim alanı, "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma imkânı veren manyetik sistemler*" şeklinde tanımlanarak 1989 yılındaki tasarıya "manyetik sistemler" ifadesi eklenmiştir.

2000 yılında hazırlanan TCK Tasarısının 345. maddesinde "bilişim alanı" 1997 tasarısına çok benzer şekilde "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerden oluşan alan*" şeklinde tanımlanmıştır. 2003 yılındaki TCK Ön Tasarısının 346. maddesinde ise *bilişim alanının* tanımlaması yapılmamıştır. Bu tanım yerine "bilişim sistemi" kavramı kullanılmıştır. Bilişim sistemi ise "*verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler*" olarak tanımlanmıştır.

Bu tasarıların yasa metnine dönüşmesi 765 sayılı eski Ceza Kanunu'nda yapılan bir değişiklikle mümkün olmuştur. Bu değişiklikle "bilişim alanı" kavramı ilk kez yasalarımızda yer almıştır. Değişiklik 765 sayılı Eski Türk Ceza Kanunu (ETCK)'na (06 Haziran 1991 tarihinde 3756 sayılı kanunun 21. maddesiyle) "Bilişim Alanında Suçlar" başlığı altında Onbirinci Bap eklenerek yapılmıştır. Yasa değişikliğinin gerekçesinde "bilişim alanı"; "*Bilgileri toplayıp depo ettikten sonra, bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan*" şeklinde tanımlanmıştır. Ancak anılan tanımdaki "*bilgileri toplamak*" ifadesi kavram

karmaşasına yol açmıştır. Bu karışıklığa İngilizcedeki "data" ve "information" kelimelerinin ikisinin de Türkçeye "bilgi" olarak çevrilmesi yol açmaktadır.[18] "Bilgi" ve "veri" kavramları genellikle karıştırılmalarına rağmen, eş anlamlı değildir. "Veri" terimi İngilizce "data" kelimesinin karşılığıdır ve *"bir sistem tarafından bir araya getirilip, özel yöntemlerle işlenen numerik veya alfabetik nitelikteki parçacıklardır.*"[19] "Bilgi" ise "veri"lerin işleme tabi tutulmasıyla, değerlendirilmesiyle, belirli bir formata dönüştürülmesiyle[20] ortaya çıkan "veri"nin değerlendirilmiş/dönüştürülmüş halidir.

Veri kavramının tanımı, 23 Mayıs 2007 tarihinde yürürlüğe giren 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un tanımlar bölümündeki 2. maddesinin 1. fıkrasının (k) bendinde; "*bilgisayar tarafından üzerinde işlem yapılabilen her türlü değer*" olarak yapılmıştır. Avrupa Konseyi Siber Suç Sözleşmesi'nin tanımları düzenlendiği 1/b maddesinde ise veri kavramı; "*belirli durumların, bilgilerin kaydı ya da bir bilgisayarın bir işlemi gerçekleştirmesini sağlayacak biçimleri de içeren bilgisayar sistemince icra edilebilecek bir işlemler bütünüdür*" şeklinde tanımlanmıştır. Tüm bu değerlendirmeler sonucunda ETCK gerekçesinde yer alan "bilişim alanı" tanımındaki "bilgi" kavramı yerine "veri" kavramı kullanılsaydı, daha uygun olurdu diyebiliriz.[21]

"Bilişim Alanı" kavramı 5237 sayılı yeni TCK'da da 765 sayılı Eski Türk Ceza Kanunu (ETCK)'na benzer şekilde "Bilişim Alanında Suçlar" şeklinde Onuncu Bölümün başlığı olarak yer almıştır. Doktrinde ise bilişim alanı bazı tanımlarda; "*bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden*

[18] Yenidünya-Değirmenci, s.28.

[19] Hatice Akıncı, Emre Alıç, Cüneyt Er, *Türk Ceza Kanunu ve Bilişim Suçları,* (Derleyen Yeşim M. Atamer), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1.B., İstanbul, İBÜ Yayınları, No:51, Ocak 2004, s.174.

[20] Kubilay Taşdemir, *Yargıtay Uygulamalarında İnternet Suçları,* (Hazırlayan Müslüm Saylı, D. Akdeniz), Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Sempozyumu, Bursa, 24.03.2001, s.57.

[21] Aynı yönde görüş, Akıncı-Alıç-Er, s.174; Yenidünya-Değirmenci, s.28.

oluşan alan"[22], "v*erileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler,*[23] "*verileri toplama, depo etme ve otomatik işleme tabi tutma özelliklerine sahip elektronik sistem veya sistemler, yani bilişim cihazları ile varsa kurulu düzenin çalışmaya devam edebilmesini sağlayan tamamlayıcı cihazlardan oluşan alan*"[24] şeklinde tanımlanmıştır. Doktrindeki bu tanımlarda bilişim alanının, verileri veya bilgileri iletme, aktarma özelliği üzerinde durulmamıştır. Eksik olan bu hususları da ilave ederek bilişim alanını; "*verilere ulaşma, verileri toplama, otomatik işleme tabi tutma, depo etme, sınıflandırma, bilgiye dönüştürme ve sonuçlarının doğrudan sunulmasını ya da ses, görüntü ve/veya veri taşıyabilen kablolu veya kablosuz iletişim hatları aracılığıyla iletebilme yeteneklerine sahip bilişim cihazları ile ve varsa kurulu düzenin çalışmaya devam etmesini sağlayan, elektronik veya manyetik sistem veya sistemler ile bu sistemlerin birbirine bağlanmasıyla oluşan ağların da dâhil olduğu alan"*dır şeklinde tanımlayabiliriz. Ayrıca bilişim teknolojisinin gelişme hızı karşısında kısa bir süre sonra bu tanımın da yetersiz kalacağı, bilişim alanının genişleyeceğini belirtmekte de yarar vardır.

1.2. BİLİŞİM ALANI UNSURLARI

Bu başlık altında bilişim kavramı ve bilişim alanı üzerinde durulduktan sonra, kavramsal çerçevenin tamamlanabilmesi için bilişim alanını oluşturan en önemli unsur olan bilgisayar ve bilgisayarın donanım ve yazılım unsurları ile iletişimi sağlayan bilgisayar ağları, internet ve internet ile ilgili teknik terimler ile tarihsel gelişmeler üzerinde durulacaktır.

1.2.1. Bilişim Unsuru Olarak Bilgisayar

Bilgisayarlar, gündelik yaşamımızın her alanında yer alan, hayatımızın olmazsa olmazları arasına giren, bilişim sistemlerinde en temel cihaz olarak

---

[22] Kubilay Taşdemir, *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları,* İstanbul, Ütopyagrafik Yayınevi, Temmuz 2009, s.247.

[23] Ali ihsan Erdağ, http://temyiz.net/forum/22-ceza-hukuku/613-yard-doc-dr-ali-ihsan-erdag-ekonomi-sanayi-ve-ticarete-iliskin-suclar-bilisim-alaninda-suclar-tck-9-ve-10-bolumler.html. "*Bilişim Alanında Suçlar"*, (çevrimiçi), (Erişim; 11.04.2012)

[24] Akıncı-Alıç-Er, s.170.

kullanılan ve kullanım alanları her geçen gün artan cihazlardır. Ülkemizde bilgisayar sistemleri, sosyo-ekonomik dönüşümün teknik altyapısı olarak da her alanda etkin bir şekilde kullanılmaktadır.[25] Bilgisayarlar bu kadar geniş bir yelpazede kullanılınca, doğal olarak bu alanlar da suçluların ilgisini çekmektedir. Bu bağlamda bilgisayarlar, bilişim suçlarını diğer klasik suçlardan ayırmamıza yarayan, günümüzde kullanılan tüm bilişim tekniği ve sistemlerinin temelini oluşturan en önemli cihazlardır. Bu çalışma kapsamında inceleyeceğimiz tüm teknik kavramlar ve çeşitli suçlar bilgisayara bağlı olarak ifade edebileceğimiz kavramlardır.

Bilgisayar kavramı karşılığı olarak, ABD, Hollanda ve İngiltere'de "computer", Fransa'da "ordinateur", İtalya'da "elaboratore, elaboratore elettronico", Almanya'da "computer, elektronenrechner", İspanya'da "computador, computadora, ordenador", Portekiz ve Brezilya'da "computador" terimleri kullanılmaktadır.[26]

Ülkemizde "bilgisayar" kelimesini (Hacettepe Üniversitesi'ne bilgisayar kiralamak için 1969 yılında bir gazeteye verdiği ilanda) ilk kullanan Aydın Köksal olmuştur."[27] Daha sonra "bilgisayar" terimi ile birlikte "kompütür", "komputer", "computer",[28] "elektronik beyin" ve "elektronik hesap makinesi" gibi ifadeler kullanılmışsa da zamanla bilgisayar terimi kısaca "hesap yapan" anlamındaki "computer" kelimesinden daha kapsamlı, daha uygun ve Türkçe bir kelime olduğundan benimsenmiş ve yaygın olarak kullanılmaya başlamıştır.

---

25 Bilgisayar bu kapsamda, Adalet Bakanlığı'nda UYAP (Ulusal Yargı Ağı Projesi), Nüfus ve Vatandaşlık Genel Müdürlüğü'nde MERNİS (Merkezi Nüfus ve İdare Sistemi), Tapu ve Kadastro Genel Müdürlüğü'nde TAKBİS (Tapu Kayıt ve Bilgi Sistemi), Milli Eğitim Bakanlığı'nda Fatih Projesi ve e-devlet gibi proje ve sistemlerde kullanılmaktadır.

[26] "Computer" kelimesinin kökeni Latince "computator" kelimesi olduğu için Latince'den türeyen batı dillerinde bu kelimeye benzer terimler kullanılmıştır. Murat Volkan Dülger, *Bilişim Suçları,* 1.B. Ankara, Seçkin Yayınevi, Kasım 2004, s.36.

[27] Necmi Murat Güngör, "*Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları"*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s.4.

[28] Bahaddin Alaca, "*Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile)",* Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Antropoloji (Sosyal Antropoloji) Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2008, s.4'te "computer" teriminin Faruk Erem tarafından kullanıldığını ifade etmektedir.

Bilgisayar teriminin ulusal ve uluslararası yasal düzenlemelerde nasıl yer aldığına bakacak olursak; ABD ve İngiltere'de bilgisayarlar ile ilgili suçların düzenlenmesinde *"computer";* Fransız Ceza Kanunu'nda *"verileri otomatik işleme tabi tutan sistem";* İtalyan Ceza Kanunu'nda *"informatico"* ve *"telematico";* Alman Ceza Kanunu'nda ise genellikle veri işleme ve bilgisayar teriminin kullanıldığını görmekteyiz.[29] Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)'nin tanımlar bölümünün 1/a maddesinde ise "*bilgisayar sistemi*" terimi kullanılmıştır.

Ülkemizde 765 sayılı eski TCK'nın "*Bilişim Alanında Suçlar*" başlığı altındaki "Onbirinci Babı", m.525/a'da Fransız Ceza Kanunu'ndan etkilenilerek bilgisayar terimi yerine "*bilgileri otomatik olarak işleme tâbi tutan sistem*" ifadesi kullanılmıştır.[30] 5237 sayılı yeni TCK'nın "*Bilişim Alanında Suçlar*" başlığı altındaki Onuncu Bölümünde yer alan m.243'te ise eski TCK'daki *"bilgileri otomatik işleme tabi tutan sistem"* ifadesi yerine, *"bilişim sistemi"* ifadesi kullanılmıştır. "Bilişim Sistemi" yeni TCK'nın gerekçesinde, *"verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir"* şeklinde açıklanmaktadır. Gerekçede yer alan bu tanım, 765 Sayılı TCK'da yer alan "*bilgileri otomatik işleme tabi tutan sistem*" ifadesinden, "*verilerin toplanması, yerleştirilmesi ve sistemin manyetik olması*" bakımından farklılık göstermektedir.

"*Verilerin toplanması ve yerleştirilmesi"* ifadelerinin, tanımı biraz daha kapsayıcı hale getirme çabasının bir ürünü olduğunu söyleyebiliriz. Ancak "*sistemin manyetik olması*" ifadesi, manyetik olmayan bilişim sistemlerini tanım dışında bıraktığı için, tanımı kısıtlayıcı bir ifade olmuştur. Doktrinde "*bilgileri otomatik olarak işleme tâbi tutan sistem*" ifadesinin bilgisayarı da kapsayan daha geniş anlamı olan bir terim olduğu ifade edilmektedir.[31] Ancak 5237 sayılı yeni Ceza Yasamızda kullanılan "*bilişim sistemi"* ifadesinin "*bilgileri otomatik olarak işleme tâbi tutan sistem*" ifadesinden daha geniş kapsamlı bir terim olduğunu düşünmekteyim.[32]

---

[29] Muammer Ketizmen, *Türk Ceza Hukukunda Bilişim Suçları*, Adalet Yayınevi, 1.B. Ankara, Ocak 2008, s.10.

[30] Ketizmen, a.g.e. s.10.

[31] Yenidünya - Değirmenci, s.44-45; Yazıcıoğlu, *Bilgisayar Suçları,* s.224-225; Dülger, *Bilişim Suçları,* s.45.

[32] Aynı doğrultuda görüşler, Yazıcıoğlu, *Bilgisayar Suçları,* s.130, Dülger, *Bilişim Suçları,* s.45.

Bilgisayarın tanımı; Türk Dil Kurumu (TDK) sözlüğünde; "*çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç, elektronik beyin"*[33] olarak, Milli Eğitim Bakanlığı sözlüğünde, "*bir işi önceden verilmiş bir programa göre çözüp sonuçlandıran elektronik cihaz, kompütür"*[34] olarak, Büyük Larousse Sözlük ve Ansiklopedisinde, "*aritmetik ve mantık işlem dizileriyle oluşturulmuş programlara göre verileri otomatik olarak işleyen makine (Kompütür, Elektronik Beyin*)"[35] olarak, AnaBritannica Genel Kültür Ansiklopedisi'nde ise, "*aldığı komutlar uyarınca, veri işleyerek problem çözen otomatik elektronik aygıtların ortak adı (Kompüter*)"[36] olarak tanımlanmaktadır. Bu tanımlara benzer şekilde doktrinde de bilgisayarı; "*bilgi depolayıp işleme tabi tutan ve sonucunu gösteren bir araç"*[37] şeklinde tanımlayanlar da vardır.

Avrupa Konseyi Siber Suç Sözleşmesi 1/a. maddesinde, bilgisayarın "*belirli bir yazılım çerçevesinde otomatik olarak veri işleyebilme*" özelliği vurgulanmıştır. Doktrinde ise bilgisayar; *"yüklenen programlar yardımıyla bilgileri belirli bir düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler*",[38] *"giriş birimleri ile dış dünyadan aldıkları veriler üzerinde aritmetiksel ve mantıksal işlemler yaparak işleyen ve bu işlenmiş bilgileri çıkış birimleri ile bize ileten, donanım ve yazılımdan oluşan elektronik bir makine",*[39] *"veri saklayabilen, işleyebilen, depolanmış bir programı işletebilen ve işlem akışı ile sırasını otomatik*

---

[33] www.tdk.gov.tr/index.php?option=com_gts&arama TDK internet sitesi (çevrimiçi), (Erişim; 04.04.2012).

[34] Örnekleriyle Türkçe Sözlük; MEB Yayını, MEB Basımevi, C.I., İstanbul, 2000, s.329.

[35] "Büyük Larousse Sözlük ve Ansiklopedisi", C.IV. s.1639.

[36] "AnaBritannica Genel Kültür Ansiklopedisi", C.IV. s.151.

[37] Ersoy, s.151.

[38] Berrin Bozdoğan Akbulut, "*Türk Ceza Hukukunda Bilişim Suçları"*, SÜSBE, Kamu Hukuku, Ana Bilim Dalı, Ceza ve Ceza Usul Hukuku Bilim Dalı, Yayımlanmamış Doktora Tezi, Konya, 1999, s.10.

[39] Özgür Eralp, *Hukukçular için Bilişim Terimleri Sözlüğü,* 1.B., Muğla, Eralp Kitap Basım Yayıncılık, Haziran 2007, s.26.

olarak değiştirebilen bir aygıt",[40] *"kullanıcı tarafından kendisine verilen komutlara dayalı olarak işlemleri verilen sırada yerine getiren teknolojik araç",*[41] *"çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi önceden verilmiş bir programa göre yapıp sonuçlandıran, bilgileri depolayan elektronik araç, kompütür",*[42] *"donanım ve yazılımdan oluşan, üzerine kurulan programlar aracılığıyla çalışan, yüklenen verileri depolayabilen, işleyebilen veya sonuçlar üretebilen, verileri ve sonuçları, çıkış üniteleri aracılığı ile sunabilen, iletilmesini sağlayan* cihazlar",[43] "v*erileri kendisine verilen komutlar doğrultusunda işleyen bir elektronik veri işleme aracı",*[44] "*dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan, işleyen, yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, veri iletişimini sağlayan makinelerdir"*[45] şeklinde tanımlanmıştır.

Yukarıda görüldüğü gibi doktrinde bilgisayarın çok sayıda tanımı yapılmıştır. Her tanımda bilgisayarın değişik nitelikleri (ayrı ayrı işlevi, yazılımı, donanımı veya aynı anda yazılım ve donanımı) üzerinde durulmuştur. Bilgisayar teknolojisinin ve imkân ve kabiliyetlerinin sürekli artmasına paralel yeni suç türleri de ortaya çıkmaktadır. Bu nedenle bilgisayarın kalıcı nitelikte tanımını yapmaya çalışmak yerine, bilgisayarın diğer cihazlardan farkını ortaya koyan ve günümüzde ulaştığı imkân ve kabiliyetlere uygun tanımlar yapılması gerektiğini düşünüyorum. Ancak, bilgisayarla işlenen tüm suçların bilişim suçunu oluşturup oluşturmadığı hususunda bir hükme varabilmek içinde bilgisayarın da tanımlanması gerekmektedir. Bu bilgiler ışığında bilgisayarı; "*giriş birimleri vasıtasıyla yüklenen programlara ve/veya verilen komutlara göre her türlü simgeleştirilmiş işlemi, ana işlemcisi ile otomatik olarak yapan;*[46] *verileri; sınıflandırabilen, belirli bir düzen içinde belleğinde*

[40] Yazıcıoğlu, *Bilgisayar Suçları,* s.27-28.

[41] Demircan, s.14.

[42] Esra Yaycı, *"Bilişim Suçları",* Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, Ceza ve Ceza Usulü Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, 2007, s.4.

[43] Güngör, s.4.

[44] Gümüş, s.22.

[45] Yenidünya – Değirmenci, s.19.

[46] Dülger, *Bilişim Suçları*, s.43.

saklayabilen, veriler üzerinde; değiştirme-dönüştürme işlemi yapabilen, mantıklı sonuçlar çıkarabilen, verileri; direkt olarak çıkış birimleri aracılığıyla veya kablolu-kablosuz ağlar yardımıyla iletebilen, yakından veya uzaktan yeni yazılımlar yüklenip, silinebilen, elektronik veya manyetik akımlarla çalışan[47] *donanım ve yazılım unsurlarından oluşan, her türlü işlemi yapabilecek kabiliyette ve bilişim özelliğine sahip (genel amaçlı)*[48] *olarak üretilmiş cihazlardır"* şeklinde tanımlayabiliriz.

Elbette bu tanımın da bilgisayarı tüm yönleriyle ifade ettiğini ileri sürmek fazlaca iddialı olur. Bunu ileri süren bir tanımın da, kısa bir süre sonra geçerliliğini kaybedeceği açıktır. Çünkü her geçen gün bilgisayarların işlevleri ve özellikleri değiştiği ve arttığı gibi, önceleri bilgisayar tanımlamasına girmeyen çeşitli nesne ve cihazlar da zamanla bilgisayarın işlevlerini görür hale gelmektedirler. Buna en güzel örnek olarak sesli bir iletişim aracı olarak üretilmesine rağmen gelişen teknoloji sayesinde kısmen bilgisayara dönüşmüş olan cep telefonları gösterilebilir. Ayrıca cep telefonları ile oluşturulan dosyalar, sesler, resimler, videolar vb. tüm verilerin artık internet aracılığı ile gönderilebildiği de gözden uzak tutulmamalıdır.

Bir an için dizüstü (notebook - laptop) veya netbook (küçük laptop) büyüklüğünde olan bilgisayarların ve cep telefonlarının tüm özelliklerine sahip olan yeni cihazların üretildiğini düşünelim. Bu cihazların klasik bilgisayar ve cep telefonu özelliklerinin birleşiminden olacağı, hatta bu özelliklerden çok daha fazlasına sahip olacağı ortadadır. Bu durumda anılan özelliklere sahip cep telefonlarına karşı işlenebilecek suçların da bilişim suçu kapsamında değerlendirilmesi mümkün olabilecektir. Ayrıca insanları biyometrik özelliklerinden tanıyabilen çeşitli sistemler,[49] içerdiği programlar aracılığı ile birtakım işlevleri yerine getiren ev

---

[47] Levent Kurt, *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* 1.B., Ankara, Seçkin Yayınevi, Eylül 2005, s.31.

[48] Yazıcıoğlu, *Bilgisayar Suçları*, s.27.

[49] Biyometri ya da biyometrik sistemler; bireyin ölçülebilir fiziksel ve davranışsal özelliklerini tanıyarak kimliğini tespit etmek üzere geliştirilmiş bilgisayar kontrollü sistemlerdir. Bu fiziksel ve davranışsal izler; ses, parmak izi, yüz, iris, retina, el ve parmak geometrisi gibi fiziksel özelliklerin taranması sonucu elde edilmektedir. Örneğin retina taramasında 276 farklı noktadan elde edilen izler kullanılmaktadır. Biyometri teknolojisi; bilgisayar güvenliğinde, internet bankacılığında, ATM'lerde, çağrı merkezlerinde, hastanelerde, sigorta şirketlerinde, havaalanlarında, kurumsal ağlarda, kiosklarda, SGK, vergi süreçleri gibi kamu işlem ve hizmetlerinde, evlere, ofislere ve binalara erişim ve e-ticaret işlemleri için kullanılabilmektedir. www.turkeyforum.com/satforum/archive/index. Turkey Forum (çevrimiçi), (Erişim; 13.02.2007).

aletleri[50] ve daha da önemlisi organik bilgisayar geliştirme yolundaki çalışmalar dolayısıyla bilgisayar, bilişim sistemleri ve bilişim suçlarını tanımlamak ve diğer suç türlerinden ayırmak üzere yeni terimler, yeni ayırt edici özellikler bulmak gerekecektir.[51]

1.2.2. Bilgisayarların Çalışma Yöntemi

Belirli bir amaç doğrultusunda bilgisayara girilen veriler (input), bilgisayarda aynı şekilde kaydedilmemekte, bilgisayar sistemine uygun kodlara, bilgisayarın anlayabileceği bir dile dönüştürüldükten sonra, işlem yapılabilecek bir hale getirilmektedir. Dönüştürme işlemi için sadece "0" ve "1" rakamlarının çeşitli kombinasyonlarından oluşan iki tabanlı sayı sistemi (Binary Digit) kullanılmaktadır. Bu sistemde klavyenin tuşuna basıldığında yazılan harf, rakam veya diğer özel simgeler bilgisayar tarafından hemen "0" veya "1"'e çevrildikten sonra işlem yapılmaktadır. Binary sisteminde "0" ya da "1" rakamları; kapalı veya açık, yok veya var, hayır veya evet anlamlarına gelmektedir. Bu iki rakama bilgisayar dilinde "bit" adı verilmektedir.[52]

Bilgisayarlar, çeşitli giriş üniteleri ile girilen veriler üzerinde daha önceden hafızasına yüklenmiş olan ve ona nasıl çalışması gerektiğini gösteren emirleri içeren programlar sayesinde çeşitli işlemler yapabilirler. (Örneğin word ya da Excel dosyasındaki bir isim listesinin alfabetik sıraya dizilmesi bilgisayardaki programın yaptığı bir işlemdir.) Bilgisayarların programlar aracılığıyla işlediği verilerden

---

[50] Örneğin akıllı evler projesi kapsamında geliştirilen buzdolaplarının herhangi bir besinin azalması durumunda internet aracılığı ile otomatik olarak sipariş verebilmesi. Burak Çekiç, "*İnternet Aracılığıyla İşlenen Suçlar",* MÜSBE, Hukuk Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2006, s.4.

[51] **"**Bilişim teknolojisinde bilgisayarların ebatlarının küçülmesine rağmen fonksiyonları daha da gelişirken, Japon bilim adamları da bu doğrultuda çok önemli bir buluş gerçekleştirdi. Keio Üniversitesi Hayat Bilimleri Enstitüsü uzmanları, "Bacillus subtilis" adlı bakterinin genlerine dijital bilgiyi kimyasal elementlere çeviren bir yöntem kullanarak kısa mesaj yazmayı başardı. Bu mesajla birlikte bakterinin genlerine yüzlerce yıl muhafaza edebilecek büyük boyutlarda sayısal bilgi de yüklendi. Bu organizmalar, harddisk ve hafıza kartlarıyla kıyaslandığında çok küçük kalsalar da genlerinde çok uzun süre önemli miktarda bilgiyi saklayabileceklerdir." www.milliyet.com.tr. (çevrimiçi), (Erişim; 13.02.2012).

[52] Bilgisayar için tüm harf, rakam veya karakterler ayrı bir "bit"tir. "Bit" temel bilgi birimidir. "**Bit**" terimi İngilizce "*ikili rakam*" anlamına gelen "**Bİ**nary digi**T**" kelimelerinin kısaltmasından oluşturulmuştur. Bilgisayarlar "bit" grupları ile işlem yaparlar. 8 bit biraraya gelerek bir karakterlik bilgiyi (bir byte'ı) oluşturur. Örneğin klavyemizin "A" harfine bastığımız anda aslında "A" harfini temsil eden (01000001) rakamlarını oluşturmuş oluruz.

meydana getirdiği sonuçlara ise çıktı (İng. output, Alm. Ausgabe) denir. Örneğin bilgisayar ekranında gördüğümüz veri işlem sonuçları veya matematik işlem sonuçları ve yazıcı yardımıyla elde edilen yazılı biçimler de çıktı kavramına dâhildir.

1.2.3. Bilgisayarın Unsurları

Bilgisayarlara ilişkin kapsamlı tanım yapmanın zorluğu, bilgisayarı oluşturan parçaların öncelik kazanmasına neden olmuştur. Bir bilgisayarda teknik açıdan bulunması gereken asgari unsurlar genel olarak fiziksel bileşenlerini oluşturan donanım (hardware) unsurları ile fiziksel yapıda olmayan yazılım (software) unsurlarıdır. Aşağıda bu unsurlar üzerinde durulacaktır.

1.2.3.1. Donanım Unsurları (Hardware)

Donanım unsurları (Hardware); bilgisayarlara program ve verilerin girilmesini, işlem yapıldıktan sonra çeşitli bilgilerin alınmasını sağlayan fiziksel, unsurlardır.[53] Başka bir anlatımla "*bilgisayar olarak karşımızda gördüğümüz her şey donanıma aittir.*"[54] Bir bilgisayarda teknik açıdan bulunması gereken asgari donanım unsurları, Merkezi İşlem Birimi "CPU", Salt Okunur Bellek "ROM", Rastgele Erişimli Bellek "RAM", çevre/giriş (input) - çıkış (output) birimleridir. Bu unsurlarla birlikte veri depolama birimleri ile bilişim sistem ağlarına ve özellikle internete bağlanabilmek için ağ erişim araçlarına da ihtiyaç vardır. Aşağıda sırasıyla bu donanım unsurları incelenecektir.

1.2.3.1.1. Merkezi İşlem Birimi (Central Processor Unit-CPU)

Mikro-İşlemci olarak da adlandırılan Merkezi İşlem Birimi (Central Processor Unit - CPU), içinde on binlerce çok küçük devre barındıran tümleşik yapıdaki bir yongadır.[55] CPU bilgisayarın tüm birimlerini kontrol eden, yönetim birimi ve beynidir. CPU giriş birimlerinden gelen verilerin kodlarını çözer, ikili

---

[53] Mehmet Burak Kızıltan, *"5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları",* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2007, s.9.

[54] Alaca, s.7.

[55] Yenidünya - Değirmenci, s.22; Bilgisayarlarda kullanılan önemli bazı yongaların (entegre devre) görevleri şöyledir: mikroişlemci yongaları; ikili sayıları işleyip bilgiye dönüştürür, bellek yongaları; mikroişlemcinin aldığı bilgileri depolar, arayüz yongaları; bilgisayara yazılan bilgileri ikili sinyallere çevirip bu bilgileri de işlendikten sonra tekrar bilgiye dönüştürürler. Pam Beasant, *Elektronik,* (Çev. Erol Tunalı), TUBİTAK Popüler Bilim Kitapları 103, Gençlik Kitaplığı 20, 2.B., Ankara, Nurol Matbaacılık, 1999, s.33.

sayıları işleyip bilgiye dönüştürür, gereken işlemleri yapar, yapılan işlemleri denetler ve işlem sonuçlarını geçici olarak muhafaza eder.[56] Bu nedenle bilgisayarların işlem yeteneği kapasitesi ve hızları Merkezi İşlem Birimlerinin kalitesine bağlıdır.[57]

Merkezi İşlem Birimi (CPU) ana kart üzerinde bulunur. CPU, Aritmetik ve Mantık Birimi (Arithmetic and Logic Unit - ALU) ile Kontrol Ünitesi (Control Unit - CU)'nden oluşur. ALU birimi; dört işlemi, verilerin karşılaştırılmasını, sonuca göre yeni işlemlerin seçilmesini ve kararların verilmesi işlemlerini yapar. CU birimi ise, işlem akışını düzenler, verilen komutların yerine getirilmesini sağlar.

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

İngilizce olan "ROM - Read Only Memory, " terimi, Türkçeye "Salt Okunur Bellek" şeklinde çevrilmiştir. Salt Okunur Bellek, bilgisayar üreticileri tarafından bilgisayarın çalışması için gerekli olan en temel komutların yüklendiği ve depolandığı bir birimdir.[58]

Salt Okunur Bellekler üzerinde bilgisayar açıldığında veya "reset" edildiğinde bilgisayar işletim sistemini sabit diskten Rastgele Erişimli Belleğe (RAM), yüklemeyi düzenleyen BIOS (Basic Input / Output System) adı verilen özel bir program vardır. Bu programların temel amacı bilgisayar ile çevre, giriş-çıkış birimleri ve kullanıcı arasındaki bağlantıyı ve bilgisayarın ilk çalışmasını sağlamaktır.[59] Mikroişlemci bu belleği sadece okumakta kullanır ve değiştiremez, üzerine veri kaydedemez. ROM bellekler zamanla değiştirilmesi gerekmeyen program ve verilerin sürekli tutulması için vardır. Örneğin "f" tuşuna bastığımızda sürekli "f" harfi çıkmasını sağlayan veri hiçbir zaman değişmez. Bilgisayarın asli görevini yerine getirmesi için her zaman gereksinim duyduğu ve daima belirli şekilde yaptığı işlemleri Salt Okunur Bellekler yapar.[60]

---

[56] Kurt, s.31.

[57] Eralp, *Bilişim Terimleri Sözlüğü,* s.41.

[58] Güngör, s.9; Yaycı, s.6; İsmail Tulum, "*Bilişim Suçları İle Mücadele",* Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Isparta, 2006, s.5.

[59] Kızıltan, s.10; Çekiç, s.8; Demircan, s.17.

[60] Demircan, s.17.

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

İngilizce olan "RAM - Random Access Memory" terimi Türkçeye "Rastgele Okunur Bellek" şeklinde çevrilmiştir. Rastgele Erişimli Bellek, bilgisayar çalıştığı sürece (Sabit Disk, Disket, CD-ROM, DVD-ROM, Flash Bellek gibi) depolama birimleri ve giriş birimlerinden gönderilen veri ve bilgilerin, Merkezi İşlem Birimi tarafından üzerine yüklenip, üzerinde işlem yapıldığı bellektir. RAM bellek; bilgisayara çeşitli giriş unsurlarıyla girilen verilerin üzerine yazıldığı, değiştirilebildiği, silinebildiği veya saklanabildiği, üzerinde çeşitli işlemler yapılabildiği, bilgisayar çalıştığı sürece faaliyette olan bir bellek türüdür.

RAM belleğin hem yazılabilir hem de okunabilir özelliği bulunmaktadır. Bilgisayarlar veri tutmak için, sıralı olmayan RAM belleği kullanırlar. Bunun nedeni rastgele erişimli bellekte bütün hafıza noktalarına neredeyse aynı hızda erişildiğinden veri işleme hızının yüksek olmasıdır. Diğer teknolojilerin çoğu veri okuma yöntemi olarak sıralı olarak belirli bir "bit" veya "byte" okuduklarından bu yöntem veri işleme hızlarında gecikmelere neden olmaktadır. Rastgele erişim imkânı RAM belleğin hızını artıran önemli bir avantajıdır.[61]

1.2.3.1.4. Çevre / Giriş-Çıkış Birimleri

Bilgisayarlarda yapmak istediğimiz çeşitli nitelikteki işlemlerin bilgisayarın anlayacağı dile çevrilmesini sağlayan aracı ünitelere "*giriş birimleri*", bilgisayarda istediğimiz işlemi yaptıktan sonra bu kez bizim anlayacağımız şekle dönüştürülerek çıktısını almamıza aracılık eden ünitelere ise "*çıkış birimleri*" adı verilmektedir. Bu birimler bilgisayarların dış ortamlarla irtibatını sağlayan birimlerdir.[62]

Klavye, fare (mouse), barkod okuyucu, tarayıcı (scanner), mikrofon, kamera, oyun çubuğu gibi üniteler giriş üniteleridir. Hoparlör (speaker), çizici (plotter), CD/DVD, yazıcı (printer) gibi üniteler çıkış birimleridir. Ekran/monitör, sabit disk (harddisk), disket (floppy disket) sürücü, flash bellek, optik disk sürücü (optical disk), CD-ROM ve DVD-ROM sürücüleri ve modemler ise hem giriş hem de çıkış birimlerine örnek olarak gösterebilir. Teknolojinin gelişmesiyle sayı ve çeşitleri

[61] Yenidünya-Değirmenci, s.22-24; Kızıltan, s.10.

[62] Kurt, s.34; Dülger, *Bilişim Suçları*, s.40; Yenidünya-Değirmenci, s.25.

artan, dış ortamlarla bilgisayarın veri alışverişi yapmasını sağlayan bu birimlerin tümüne birden "çevre birimleri" denmektedir.[63] Aşağıda bu birimler incelenecektir.

Klavye; üzerinde çeşitli harfler, sayılar, işaretler ve değişik bazı işlevlere yönelik fonksiyon, daktilo, numerik ve özel tuşları olan ve bu tuşlara dokunmak suretiyle bilgisayara veri gönderilen giriş birimidir. Ülkemizde genel olarak "Q" ve "F" klavye (Türkçe daktilo klavyesi) olmak üzere iki çeşidi kullanılmaktadır.[64] "Q" klavye daha yaygın olarak kullanılırken, "F" klavye ise özellikle 10 parmağını kullanarak hızlı yazanlar tarafından tercih edilmektedir.

Fare (Mouse); üzerinde bulunan tuşlar aracılığıyla, menü seçmek, işlem yapmak veya ekran üzerinde istenen noktaya gitmek gibi amaçlarla kullanılan, klavyeye yardımcı bir giriş birimi ünitesidir. Ekran üzerinde klavyedeki gösterge ve yön tuşlarıyla veya dokunmatik tuşlarla işlem yapmak gecikmelere neden olmaktadır. "Fare" birimi ile bu işlemler daha kısa sürelerde yapılabilmektedir. Fare'ler avuç içinde tutularak, elle yapılan hareketler ile ekrandaki imlecin hareketlerini kontrol eder. Fare'lerin modeline göre, üzerinde bir veya birkaç tuş veya tekerlek bulunabilir.

Fare'ler bilgisayar kullanıcısının el hareketlerini mekanik, LED'li optik, lazerli optik gibi teknik okuma yöntemleriyle algılar ve bu bilgileri bilgisayara kablo, kızılötesi ışın, radyo dalgaları veya bluetooth yöntemi ile aktarırlar. 1964 yılında ilk bulunduğunda altında bulunan top yardımıyla hareket ettirilebilen ve hatta altına rahat hareket edebilmesi için "mousepad" konulan fareler yerine, günümüzde USB, optik ve lazer (kablosuz - wireless) fareler yoğun olarak kullanılmaktadır.[65]

Tarayıcı (Scanner); üzerinde işlem yapılacak olan kâğıt, resim, gazete, grafik, bilgisayar yazısı veya el yazısı gibi nesneleri tarayıp sayısallaştırdıktan sonra bilgisayar ortamına aktaran giriş birimi ünitesidir.

---

[63] Hayati Pallı, *"Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları"*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Kayseri, Kasım 2008, s.13.

[64] Çekiç, s.13; Güngör, s.13. (Ayrıca ,"Q" klavyenin "F" klavyesine, "F" klavyenin "Q" klavyesine CTRL + Shift tuşlarına basarak çevrildiğini belirteyim. F.G.).

[65] Çekiç, s.13; Güngör, s.13; www.sessiztr.com/donanim/9022-mouse-fare-nedir.html, Mouse nedir? (çevrimiçi), (Erişim; 11.04.2012). www.bilgisayarnedir.com/mouse.html Bilgisayar Nedir? (çevrimiçi), (Erişim; 11.4.2012).

Tarayıcıların üzerinde veri bulunmaz, veri kaydetme veya depolama özellikleri yoktur. Bu nedenle resim ve grafikler bilgisayara aktarıldıktan sonra ancak bu nesneler üzerinde değişiklikler yapılabilmektedir. Tarayıcılarda tarama ve sayısallaştırma işlemi ışığa duyarlı yarı iletken elemanlar (LDR) tarafından yapılır. Tarama işlemi sonucunda elde edilen veriler öncelikle RAM'a yazılır, buradan ekrana aktarılarak üzerinde işlem yapılır ve/veya kaydedilerek saklanır. Genel amaçlı tarayıcılar dışında özel işaret ve kodları dijital (sayısal) veriye dönüştürmek amacıyla kullanılan tarayıcılar da vardır. Bu tarayıcılara; barkod tarayıcılarını, göz iris (retina) tarayıcılarını, parmak izi tarayıcılarını, tıbbi amaçlı kullanılan tarayıcıları örnek olarak verebiliriz.[66]

Yazıcı (Printer); bilgisayar ortamında üretilen şekil, grafik gibi bilgilerin ve bilgisayara dosya olarak kaydedilmiş çeşitli yazıların, kâğıt vb. nesneler üzerine siyah-beyaz veya renkli olarak yazılmasını sağlayan, bir çıkış birimi ünitesidir.

Yazıcılar, kendilerine özgü bir mikroişlemci sayesinde çalışırlar. Çıktı alabilmeye yetecek nitelikte sınırlı sayıda karakter depolamasına imkân veren bir ön hafızaya sahiptirler. Yazıcıların nokta vuruşlu, mürekkep püskürtmeli ve lazer (laser) yazıcı gibi çeşitleri bulunmaktadır. Nokta vuruşlu yazıcılar; basit ve ekonomik olan ancak resim basma özellikleri olmayan yazıcılardır. Mürekkep püskürtmeli yazıcılar; ev bilgisayarları ve az çıktı alan ofisler için idealdir. Lazer (laser) yazıcılar ise diğer yazıcılara göre daha pahalı ama daha hızlı baskı yapan yazıcılardır. CD-ROM ve DVD gibi disklere veri kaydederek diğer CD-ROM/DVD-ROM'lar tarafından okunabilmesini sağlayan yazıcı çeşitleri de vardır.[67]

Ekran (Monitör); bilgisayarların mikroişlemcisinden gönderilen verileri çıplak gözle görülebilecek şekle dönüştüren giriş ve çıkış birimidir. Başka bir anlatımla CPU tarafından işlenen bilgilerin görsel olarak kullanıcıya iletildiği birimdir.[68] Ekranda görüntüyü sağlayan en küçük birime "piksel" adı verilir.

---

66 www.pcnet.com.tr/forum/windows-ipuclari/130519-tarayici-nedir-ogrenmek-isteyenler-icin. html (çevrimiçi), (Erişim; 11.04.2012).

67www. bilisim akademi. net/kbOku.asp?kbID=31 Bilişim Akademi, Bilişim nedir? (çevrimiçi), (Erişim; 11.04.2012).

68 www.tr.wikipedia.org/wiki/Bilgisayar_monit%C3%B6r%C3%BC Wikipedia (çevrimiçi), (Erişim; 11. 04. 2012); www.bilgisayarnedir.com/monitor.html (çevrimiçi), (Erişim; 11.04. 2012).

Piksellerin sayısı ne kadar büyük olursa ekran görüntüsünün netliği o oranda büyük olur. Piksel sayılarının ifade ettiği değer "çözünürlük" olarak tanımlanır.[69] Monitörlerin önemli niteliklerinden birisi, ekrandaki görüntülerin netliği veya çözünürlüğünün ayarlanabilmesidir. Monitörler büyüklüklerine, gösterdikleri renk sayısına, saniyedeki ekran yenileme sayısına ve destekledikleri çözünürlük (resulation-ekrandaki yatay ve dikey nokta sayısı) oranlarına göre sınıflandırılırlar.

Monitör olarak ilk zamanlar (1980'li yıllar), ağır olan ve oldukça fazla yer kaplayan elektron tüplü CRT (Chatode Ray Tube-Katot Işınlı Tüp) monitörler kullanıldı. 2000'li yıllarda tüplü monitörlere göre daha ince, hafif ve görüntüyü sıvı kristal diyotlar yardımıyla sağlayan LCD (Liquid Cyristal Display - Sıvı Kristal Ekran) ekranlar kullanıldı. LCD ekranlar 2003 yılından sonra yerlerini, ekran arka aydınlatmalarını LED (Light Emitting Diode-Işık Yayan Diyot)'ler aracılığıyla yapan LED ekranlara bıraktılar. LED ekranlar da yakın bir gelecekte yerlerini OLED (Organic Light Emitting Diode-Işık Yayan Organik Diyot) teknolojisi kullanan ekranlara bırakacak diyebiliriz.[70]

Modem; temel olarak bilgisayarların telefon hatlarını kullanarak, uzak mesafelerdeki diğer bilgisayarlarla veri alışverişi yapmasını sağlayan, bu amaçla hem giriş hem de çıkış birimi olarak kullanılan cihazlardır. Başka bir ifade ile modemler bir veriyi başka bir şekle dönüştürerek gönderir veya alırlar.[71]

Modemler, bilgisayardan aldığı dijital (sayısal) nitelikteki çıktı bilgisini, analog veriye çevirerek karşı tarafa gönderir (modülasyon işlemi). Aynı şekilde karşı taraftaki bilgisayardan gelen analog veriyi de dijital veriye çevirerek (demodülasyon) bağlı olduğu bilgisayara iletirler. Bu nedenle modem terimi, modülasyon-demodülasyon kelimelerinin ilk üç harfinin birleşmesinden oluşturulmuştur. Ancak

---

[69] Sönmez Pamuk, *Dünya Parmağınızın Ucunda,* (Bilgisayarın Temelleri), Ankara, Meridyen Bilişim Yayını, 1999, s.17.

[70] Son birkaç yıldır fuarlarda kullanılan, ancak ürün henüz ticarileşmediğinden fiyatları da bir hayli yüksek olan OLED ekranların en önemli özelliği esnek bir yapıya sahip olması nedeniyle bir rulo gibi katlanabiliyor veya kıvrılabiliyor olmasıdır. www.hurriyet.com.tr (çevrimiçi), (Erişim; 07.04.2012).

[71] www. veteknoloji.com/forum/kablosuz -modem- nasil –calisir -t15004.0.html Teknoloji (çevrimiçi), (Erişim; 11.04.2012); www.bilgisayardershanesi.com/modemler.html Bilgisayar Dershanesi, Modem Nedir? (çevrimiçi), (Erişim; 11.04.2012).

günümüzde modemlerin işlevleri biraz farklılaşmıştır. Artık modemleri sayısal verileri radyo frekans sinyallerine çevirerek İnternet Servis Sağlayıcılarına (İnternet Service Provider – ISP) bağlanmak için kullanıyoruz.[72] (Veri alma durumunda radyo frekansın, sayısal hale dönüştürülmesi söz konusudur.) Son dönemlerde bu amaçla Wi-Fi (Wireless Fidelity - Kablosuz Bağlantı Alanı) teknolojisi kullanılmaktadır.[73]

1.2.3.1.5. Veri Depolama Birimleri

Veri depolama birimleri, bilgisayarların asli unsurları arasında olmayan, çalışmasını etkilemeyen kalıcı depolama birimleridir. Gelişen teknolojiye paralel olarak daha küçük hacimli depolama birimlerinde, daha büyük veriler saklanabilmektedir. Veri depolama birimleri, bilişim suçları soruşturmalarında dijital delil elde etmek için en çok incelenen bilgisayar yardımcı üniteleridir. Bu birimler Sabit Disk (Hard Disk), Disketler, CD-ROM ve DVD-ROM'lar, Flash Bellek (Flash Memory) gibi çeşitli birimlerdir. Bilişim suçlarıyla ilgili dijital veri elde edilmesinin önemli araçları olan bu depolama birimleri aşağıda sırasıyla incelenecektir.

Sabit Disk (Hard Disk - HDD); bilgisayarların bilgi depolamak için kullandığı kapalı bir kutu halinde bilgisayarın içinde bulunan, bu nedenle de taşınamayan en temel veri saklama birimidir.[74]

Sabit disk; döner bir mil üzerine sıralanmış, metal veya plastikten yapılma ve üzeri manyetik bir tabaka ile kaplı plakalar ve bu plakaların alt ve üst kısımlarında yerleşmiş olan okuma/yazma kafalarından oluşur. Veriler sabit diskteki bu manyetik tabakalar üzerine mıknatıslanma mantığı ile kaydedilir. Bu plakalar bir motora bağlıdır ve sürekli dönerler. Bu dönüş esnasında okuma - yazma kafası bu plakalar üzerine veri yazar ya da veriyi okur. Sabit diskin dönüş hızı ne kadar yüksek ise

---

[72] Veri paketlerinin modemler aracılığı ile gönderilmesini sağlayan protokole "point to point protokolü – noktadan noktaya protokolü" denir. "Bu yöntemde veri paketleri TCP/IP ile ISP üzerinden internete yönlendirilir, aynı şekilde internetten gelen veriler de ISP üzerinden bilgisayarlara yönlendirilir." www.bilgisayarnedir.com/monitor.html Bilgisayar Nedir? (çevrimiçi), (Erişim; 11.04. 2012).

[73] "*Wi-Fi ifadesi, ürünlerin kablosuz veri iletişimi sağlayabildiğini gösteren bir uyumluluk göstergesidir.*" www.tr. wikipedia. org/wiki/Wi-Fi Wikipedia (çevrimiçi), (Erişim; 11.04.2012).

[74] Çekiç, s.9; www.veteknoloji.com/bilgibank.php?id=100 Teknoloji (çevrimiçi), (Erişim; 11.04.2012).

okuma-yazma hızı da o kadar yüksek olur ve bu işlem doğrusal olarak bilgisayarın hızını etkiler. Sabit diskler bilgisayar her açıldığında işletim sistemini ve diğer yazılımları sistem belleğine yükler ve kalıcı olarak saklama komutu verilen bilgileri bilgisayar kapalı olsa dahi muhafaza etmeye devam ederler.[75]

Bilgisayardaki ilk sabit diskler "C" harfiyle ifade edilirken daha sonra eklenen sürücüler "C" harfini takip ederek adlandırılırlar. Örneğin, ikinci bir sabit disk ya da sabit diskin ikinci bölümü varsa "D sürücüsü", sonraki "E sürücüsü" olarak adlandırılır.[76]

Disket; yazılımları veya verileri manyetik ortama kaydetmeye ve kaydedilmiş yazılım veya verileri okumaya yarayan, hem giriş hem de çıkış birimi olarak kullanılabilen bir depolama ünitesidir.[77] Disketler, ince ve esnek bir manyetik veri depolama ortamıdırlar ve genellikle kare ya da dikdörtgen bir plastik muhafaza içine yerleştirilmişlerdir. Disketlerdeki veriler kopyalanabilir, silinebilir, değiştirilebilir ve üzerine yeni veri eklenebilir. İlk üretildiği zamanlarda bilgi depolama ve taşınma yönünden büyük kolaylık sağlayan disketlerin toplam hafızası ise 80 KB (Kilobyte) idi.[78]

Bilgisayarda disketleri okumak ve yazmak için kullanılan disket sürücüler (Disket yuvaları - Floppy Disk) "A" harfi ile ifade edilir. Eğer ikinci disket sürücü olursa bu disket sürücü ise "B" olarak adlandırılır. Teknolojinin gelişmesiyle teyp bandı kullanan ve kapasitesi 1,4 MB (Megabyte)'a kadar olan disketler üretildi. Ancak bir süre sonra bu disketler yerlerini depolama kapasitesi çok daha fazla olan CD'lere bırakmak zorunda kaldılar.[79] Günümüzde disket sürücülü bilgisayarlar oldukça azalmış ve yerlerini USB soketi olan bilgisayarlar almıştır.

---

[75] Güngör, s.10; www.harddisk.nedir.com/ (çevrimiçi), (Erişim; 11.04.2012).

[76] "Sabit disk, disket, CD gibi depolama birimlerinin kapasiteleri (saklayabilecekleri veri boyutları) kapasite ölçüm birimleri ile ölçülür. Kapasite ölçüm birimleri küçükten büyüğe doğru Bit, Byte (Bayt), KB (Kilo Byte), MB (Mega Byte), GB (Giga Byte), TB (Tera Byte) şeklinde sıralanırlar." www.harddisk.nedir.com/ (çevrimiçi), (Erişim; 11.04.2012).

[77] Eralp, *Bilişim Terimleri Sözlüğü,* s.49.

[78] Bu hacimdeki 8.500 disketin kapasitesiyle, (680 MB'lık) bir CD'nin kapasitesine ancak ulaşılabilir.

[79] www.bilgisayardefteri.com/ibd_disket_surucu.php. Disket Nedir? (çevrimiçi), (Erişim; 12.04.2012).

CD-ROM (Compact Disk - Read Only Memory); "Salt Okunabilir Compact Disk" anlamına gelen CD-ROM'lar disketlere göre çok daha fazla bilgiyi (650-700MB), kalıcı olarak, depolama-kaydetme kapasitesine sahip optik kayıt diskleridir.[80]

CD-ROM'lara yaygın olarak, sadece "CD" de denilmektedir. CD-ROM'lar 12 cm çaplı bir daire biçiminde, üzerinde spiral izler bulunan, alüminyum kaplamalı, ince yassı bir elektronik kayıt malzemesidir. CD üzerindeki bazı bölümler, üretim esnasında kaplama yapılarak biraz derinleştirilmiştir. CD üzerine verilerin yazılması ve CD'deki yazıların okunması; zayıf bir lazer ışınının, bu çukur ve düzlükler üzerinde yansıması veya yansımaması sonucunda gerçekleşir.

Uygulamada yaygın olarak üzerindeki bilgileri değiştirilemeyen CD'ler kullanılmaktadır. CD'ler üzerine bilgiler yazılabilir (Writable) veya yeniden yazılabilir (Rewitable) yazıcılar (CD-R/RW) gibi özel araçlarla kaydedilirler. CD-ROM sürücüler hard disklerden sonraki sürücünün adını alırlar. Bilgisayarda mevcut sabit disk (hard disk) "C" ve "D" sürücüsü ise, CD-ROM sürücü alfabetik sıralamada bu harften sonra gelen "E" sürücüsü şeklinde adlandırılır.

DVD-ROM (Digital Versatile Disc); "Sayısal Çok Amaçlı Disk" anlamına gelen DVD'ler, CD-ROM'lara göre çok daha fazla bilgiyi (4,7- 8GB), kalıcı olarak kaydetme kapasitesine sahip optik kayıt diskleridir. CD'lerle görünüm açısından bir farkları yoktur. DVD'lere kaydetme/yükleme işlemi, DVD-R/RW yazıcılarla yapılır. DVD'lerin DVD-Video, DVD-Audio, DVD-RAM gibi çeşitleri de vardır.[81]

Flash Bellek (Flash Memory); çalışırken güç kesilmesi halinde dahi içerdiği bilgileri kaybetmeyen, bilgileri tekrar tekrar yazılıp silinebilen, değiştirilebilen, verileri veya bilgileri muhafaza ederken herhangi bir güç kaynağına ihtiyaç duymayan bellek çeşididir.[82]

Flash bellekler, standart hafıza cihazı olarak bilinen harddisk'lerin çalışma yönteminden çok farklı olarak çalışırlar. Bu özellikleriyle "Katı Halli (Durağan)

[80] Eralp, *Bilişim Terimleri Sözlüğü,* s.49.

[81] www.tr.wikipedia.org/wiki/CD-ROM/DVD-ROM**.** Wikipedia (çevrimiçi), (Erişim; 12.04. 2012).

[82] Eralp, *Bilişim Terimleri Sözlüğü,* s.65.

Depolama Cihazı" (Solid State Storage Device) olarak da anılırlar. Elektronik oldukları halde bilgileri muhafaza etmek için herhangi bir güç kaynağına ihtiyaç duymazlar. Optik hafıza birimlerinin, CD ve DVD'lere göre; taşınmasının kolay olması, az yer kaplaması, çalışmasının daha hızlı olması ve kapasitelerinin daha yüksek olması nedeniyle flash bellekler mobil alanda çok yaygın olarak kullanılmaya başlanmıştır. 2000 yılından sonra "Evrensel Veri Yolu" anlamına gelen "Universal Serial Bus" teriminin ilk harflerinden oluşan USB bellekler de kullanılmaya başlamıştır. Günümüzde 2, 4, 8, 16, 32, 64, 128 ve hatta 256 GB kapasiteli USB bellekler kullanılmaktadır.[83]

1.2.3.2. Yazılım Unsurları (Software)

Yazılım (Software); bilişim sisteminin soyut bileşenlerini oluşturan, bilgisayarın ve tüm donanım unsurlarının çalışması ve temel işlevlerini yerine getirmesi için belirli bir mantık çerçevesinde yazılan, amaçlanan tüm fonksiyonların icra edilmesini sağlayan, dijital programlara (komutlara) verilen addır.[84] 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun tanımlar bölümündeki (1/B-g) maddesinde yazılım; "*bir bilgisayar sisteminin özel bir işlem veya görev yapmasını sağlayacak bir şekilde düzene konulmuş bilgisayar emir dizgesini ve bu emir dizgesinin oluşum ve gelişimini sağlayacak hazırlık çalışmalarıdır*", şeklinde tanımlanmıştır.

Bilgisayarlar üzerindeki yazılımları bir piramide benzetirsek, sırasıyla en üstte kullanıcıların çalıştığı programlar, bir alt katmanda programlama dilleri ve bu dilleri çalıştıran programlar, daha alt katmanda en temel işlemlerin yapılmasını sağlayan işletim sistemi, bir alt katmanda, işletim sisteminin üzerinde çalıştığı ve üretici firma tarafından yüklenen programlar ve en alt düzeyde ise, fiziksel bir takım işlemlere karşılık gelen mikro komutlar ve elektrik devreleri bulunur.[85]

Bilgisayarlar; yazılım programlarından gelen bütün bu karmaşık komutlar sayesinde sistemin fiziksel alt yapısını ve elektronik devrelerini harekete geçirir,

---

[83] www.usbvitrini.com/?&Bid=80873&/USB-BELLEK-NED%C, Usb Bellek Nedir? (çevrimiçi), (Erişim; 12.04.2012).

[84] Cüneyt Er, *Bilişim Suçları*, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, İstanbul, sayfa numarası yok; Kızıltan, s.11.

[85] Davut Özkul, "*Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi",* **Sayıştay Dergisi**, S.44-45, Ankara, Ocak-Haziran 2002, s.15.

gereken işlemleri yaptıktan sonra elde edilen tüm sonuçları da tekrar kullanıcının anlayabileceği biçime dönüştürürler.

Yazılımlar genel olarak Sistem Yazılımları (İşletim Sistemleri) ve Uygulama Yazılımları olmak üzere iki ana gruba ayrılırlar. Uygulama yazılımları; programlama dilleriyle yazılan kullanıcıya yönelik yazılımlardır. Sistem yazılımları ise; uygulama yazılımlarının belli bir donanım grubu üzerinde düzgün bir şekilde çalışmasını sağlayan zemin programlarını içerirler.[86]

Bilişim sistemin çalışmasını ve temel fonksiyonlarını yerine getirmesini sağlayan ve sisteme üretici firma tarafından yüklenen işletim sistemi ile ilgili bir kısım yazılımlar değiştirilemeyecek niteliktedir. Bu yazılımların değiştirilmesi sistemin çalışmamasına, arızalanmasına neden olur. Belirli bir fonksiyonun icra edilmesini, uygulanmasını sağlayan uygulama yazılımları ise; toplantı ve sunum programları, e-posta programı, yazı, resim, grafik programları, sözlük veya oyun programı ve muhasebe uygulamaları gibi yazılımlardır.[87]

Uygulama yazılımları ile işletim yazılımları birbirini tamamlayan yazılımlardır. Sadece işletim sistemine sahip bilgisayarlar verimli bir şekilde çalışamazlar. Uygulama yazılımları ise işletim yazılımı olmadan tek başına çalışamaz. Aşağıda sırasıyla bu iki yazılım türü incelenmiştir.

1.2.3.2.1. Uygulama Yazılımı (Application Program)

Uygulama yazılımları (Application Program); işletim sistemiyle uyumlu çalışan, belirli bir fonksiyonu eda etmek veya bir problemi çözmeye yönelik olarak özel hazırlanmış olan paket programlardır. Uygulama yazılımları özel amaçlara yönelik programlar olduğu için tek başlarına bilgisayarları çalıştıramazlar, sadece işletim sistemleri üzerinde çalışabilirler.[88]

İşletim sistemleri için değişik fonksiyonları yerine getirmek üzere hazırlanmış, paket program olarak adlandırılan binlerce değişik türde uygulama

[86] Güngör, s.20.

[87] Pallı, s.13; Demircan, s.19.

[88] Demircan, s.20; Çekiç, s.19; Pallı, s.15; Yaycı, s.10; Özkul, s.16; Güngör, s.21; Kızıltan, s.12.

yazılımları bulunmaktadır. Bu programlar, bilgisayar kullanıcılarının özel ihtiyaçlarını gidermek amacıyla üretilmektedirler. Başlıca uygulama yazılımları olarak; yazı, resim, tablo ve grafik programları, kelime işlemciler, karmaşık hesaplamalar ve listelemeler için matris yazılımları, istatistik, matematik, doğrusal programlama, benzetim, proje planlaması, toplantı sunum yazılımları, veri tabanı uygulamaları, muhasebe uygulamaları, video ve müzik içeren çoklu ortam yazılımları, animasyon ve oyun yazılımları, internete özgü iletişim yazılımları ile kişi ve kurumların görev sahalarıyla ilgili özel sipariş vererek yazdırdıkları programlar örnek olarak gösterilebilir.[89]

1.2.3.2.2. İşletim Yazılımı (Operating System)

Sistem yazılımı olarak da adlandırılan İşletim Yazılımı (Operating System); adından da anlaşılabileceği üzere, temel sistem işlemlerini ve donanım birimlerini, uygulama programlarını çalıştıran ve bilgisayar çalıştığı sürece bu birimleri denetleyen, yazılım ile donanım birimleri arasında bağ kuran ana kontrol yazılımıdır.

İşletim Yazılımları, bilgisayar kullanıcısıyla bilgisayar arasında köprü görevi görürler. Bilgisayar kullanıcısından gelen komutlar doğrultusunda monitör, yazıcı, hoparlör, tarayıcı gibi birimleri işletim sistemi devreye sokar.

Bilgisayarın RAM bellek kısmında çalışan işletim yazılımı sayesinde; bilgisayarların açılması, yazı yazma, dosya kopyalama, dosya silme, resim yapma, yazıcıdan çıktı alma, verilerin ağlar aracılığı ile diğer bilgisayarlara aktarılması veya verilerin alınması gibi çeşitli işlemler yapılır. İşletim sistemi temel yazılım olduğu için uygulama yazılımı ve diğer bütün programlar işletim sistemi üzerinde çalışırlar.

Bir bilgisayarın işletim sisteminin olmaması halinde hiçbir programı çalışmaz. Bu nedenle işletim yazılımlarını bilgisayar üreticisi firmalar önceden hazırlayarak bilgisayarlara yüklerler. En yaygın kullanılan işletim sistemlerine örnek olarak Novel, Windows NT, Windows 2000, DOS, Windows 3.1, Win 95, Win 98, Win Me, Win XP, Win 7, Home Edition, Vista, LİNUX/UNIX ve Macintosh grubu işletim sistemleri gösterilebilir.[90]

---

[89] Pallı, s.15; Yaycı, s.10; Kızıltan, s.12; Çekiç, s.19; Özkul, s.16; Demircan, s.20, Güngör, s.21.

[90] Akıncı – Alıç - Er, s.171; Tulum, s.6; Pallı, s.15; Demircan, s.20; Yaycı, s.10.

1.2.4. Bilgisayar Ağları (Network)

Bilgisayar Ağları (Network); en az iki bilgisayarın, sahip olduğu bilgileri paylaşmak ve/veya kaynaklarını ortak kullanmak amacıyla, bir iletim hattı üzerinden aralarında kurmuş olduğu bağlantıyla oluşan sisteme verilen addır.[91]

Network kavramı, bilişim sistemlerinde yer alan veri ve/veya bilginin hız ve zaman sınırlamasına uyulmaksızın paylaşım ihtiyacı üzerine ortaya çıkmıştır. Bilgisayar ağları ilk olarak 1960'lı yıllarda ortaya çıkmasına rağmen, 1980'lerin sonuna doğru kişisel bilgisayarların yaygınlaşması, bu alandaki teknolojinin ilerlemesi ve ucuzlaması sayesinde ancak yaygınlaşabilmiştir.

Network ağını oluşturan bilgisayarlar birbirlerine kablolu veya kablosuz olarak bağlanabilirler. Bu ağ yan yana iki bilgisayarın birbirine bağlanması ile oluşabileceği gibi ülke veya dünya genelinde tüm bilgisayarların birbirine bağlanmasıyla da oluşabilir. Her bilgisayar ağında, en az bir ana bilgisayar (server) ve ağ yöneticisi (network administrator) bulunur. Network ağına girebilmek için öncelikle o ağın yöneticisi tarafından ağa girme müracaatının kabul edilmesi ve talep sahibinin bir kullanıcı (user) olarak tanımlanması (bir kullanıcı adı ve şifresi alması) gerekir. Kullanıcıların network ağına girmesi işlemine ağ terminolojisinde "logging in" ya da kısaca "login" adı verilir. Ağdaki bir bilgisayardan dosya alma işlemine "downloading", dosya gönderme işlemine ise "uploading" adı verilir. Tüm bu işlemler belirlenmiş bir protokole göre yapılır.[92]

Bilgisayar ağlarını büyüklüklerine göre genel olarak üç grupta inceleyebiliriz. Bu gruplar; Yerel Alan Ağı (LAN - Local Area Network), Şehirsel Bilgisayar Ağları (MAN - Metropolitan Area Network) ve Geniş Alan Ağı (WAN - Wide Area Network)'dır. Bu gruplardan birincisi, en az iki bilgisayardan, bir üniversite içerisindeki tüm bilgisayarları kapsayan, birbirine yakın bilgisayarların oluşturduğu ağlardır. Bu yerel ağ (LAN)'a bağlı olan bilgisayarlar aralarında dosya paylaşımı, e-posta ve haberleşme işlemleri dışında, donanım unsurları ve çevre birimlerini de (yazıcılar, çiziciler, CD-ROM sürücüleri vb.) ortaklaşa kullanılabilmektedir.[93] Örneğin aynı kurumun binası veya kampüsü içindeki yüksek kapasiteli bir

[91] Özen-Baştürk, s.12; Özkul, s.16.

[92] Tulum, s.8.

[93] a.g.e. s.8; Özkul, s.16; Çekiç, s.16; Yaycı, s.10.

bilgisayara, aynı merkezdeki farklı birimlerin daha ufak bellekli bilgisayarlarının bağlanmasından oluşturulan ağlar gibi. Böylece merkezi bilgisayarların yüksek bellek kapasitesi ve özellikle yazıcı gibi donanım birimleri diğer bilgisayarlar tarafından da ortak olarak kullanılabilmektedir. Yerel ağ (LAN), bir şirket içinde kurulmuşsa ve tüm şirket personelinin kullanımına açık ise bu durumda ağa "intranet" adı verilir.

Ağ gruplarından ikincisi; daha uzak mesafeleri birbirlerine bağlayan "Şehirsel Bilgisayar Ağları (MAN - Metropolitan Area Network)'dır. Bu ağlar ile birden fazla yerel ağ (LAN) birbirine bağlanmaktadır. Bu ağ türünde, ağa bağlı bilgisayarlar genel olarak birbirlerine yakın değildirler, bir kurum binası veya bir kampüsten daha büyük boyutlarda bir veya birkaç şehrin bağlantısı söz konusudur."[94]

Ağ gruplarından sonuncusu; fiber optik kablolar kullanılarak çok daha uzak coğrafi bölgeler ve merkezlerin en az iki yerel ağ (LAN)'ın yönlendirici (router) ile birleşmesi sonucu oluşturduğu Geniş Alan Ağları (Wide Area Network-WAN)'dır. Doğal olarak büyük bir alan ve çok sayıdaki bilgisayarın bu ağa bağlanabilmesi için özel programlara ve protokollere ihtiyaç vardır. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulabildiği bu ağlarda, çok sayıda iş istasyonu kullanılır. WAN üzerinde milyonlarca bilgisayar çalıştığından WAN'ların hızı LAN network'lerin hızından yavaştır. Bu ağlara en iyi örnek internettir.[95]

1.2.5. Bilişim Unsuru Olarak İnternet

Geniş Alan Ağları (WAN) yöntemiyle birbirine bağlı bilgisayar ağlarının en büyüğü olan internet, dünyada kamuya açık olarak kullanılan en yaygın bilgisayar ağıdır.[96] İnternet XX. yüzyılın ikinci yarısından itibaren insanoğlunun hayatına girmesine rağmen çok kısa zamanda hayatımızın vazgeçilmezleri arasına girmiştir. Öncelikle bilgisayar ve daha sonra da internetin bulunması ve yaygın olarak kullanılması sonucunda dünya çapında o kadar büyük değişiklikler oldu ki, artık bazı

---

[94] Güngör, s.17; Çekiç, s.17.

[95] Sevil Yıldız, *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi,* Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Doktora Tezi, Konya, 2007, s.14.

[96] Özen–Baştürk, s.13.

bilim adamlarının insanlık tarihi konusunda yapmış oldukları sınıflandırmalar dahi değişti. Örneğin "Üçüncü Dalga" yaklaşımı ile internetin insan yaşamındaki önemini vurgulayacak şekilde insanlık tarihini; Tarım Dalgası, Sanayi Dalgası ve Bilişim Dalgası şeklinde dönemlere ayıran bilim adamları oldu.[97] Bu sınıflandırma kuşkusuz bilişim teknolojisinin günümüzde tüm alanlarda kullanılmasıyla insanlık tarihi boyunca meydana gelen dönüşümlere denk yeni ve kısa sürelerde meydana gelen değişimler dikkate alınarak yapılmıştır. Ancak anılan teknolojik gelişmeleri tetikleyen en önemli olay, dünya çapındaki küçüklü büyüklü bilgisayar ağlarının kurulması ve varlığı değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan "internet"in bulunup kullanılması olmuştur.[98]

İnternetin çok hızlı gelişen ve bütün dünyayı kapsayan bir iletişim ağı olması nedeniyle, teknolojik gelişmelere paralel yeni suç türlerinin de bu ağ üzerinde hızla yayıldığı ve uluslararası hukuksal düzenlemelerin yetersiz kalması nedeniyle bağımsız, denetimsiz bir ortam sunduğu da açık bir gerçektir. Tüm bu gelişmelere ek olarak yakın gelecekte ülkelerin, askeri güçleri, sayısal çoğunlukları ya da ekonomik güçleriyle değil, bilgi ve bilgiye ulaşmadaki teknolojik üstünlükleriyle dünya klasmanında yerlerini alacakları da ortadadır.[99] Tüm bu nedenlerle bu çalışmamızın konusu olarak seçtiğim, bilişim suçlarında da aracı olarak kullanılan interneti kavramamıza yardımcı olacak bazı teknik kavramları da aşağıda incelemeye çalıştım.

1.2.5.1. İnternet Kavramı

İnternet kelimesi; "Kendi Aralarında Bağlantılı Ağlar" anlamına gelen *İNTERconnected NETworks*", teriminin kısaltılmasıyla ortaya çıkmıştır.[100] İnternet kelimesinde "net" ifadesi bilgisayar ağları anlamına gelmektedir.[101] İnterneti kısaca dünya çapındaki milyarlarca bilgisayarın birbirine çeşitli ağlarla bağlanıp, veri

---

[97] Bu gruplandırmayı Alvin – Heidi Toffler çifti yapmıştır. O. Tanşu, *Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler,* (Derleyen Yeşim M. Atamer), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1.B., No:51, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, Ocak 2004, s.142.

[98] Akıncı–Alıç - Er, s.166.

[99] Demircan, s.20.

[100] Özen–Baştürk, s.13.

[101] Hasan Sınar, *İnternet ve Ceza Hukuku,* 1.B., İstanbul, Beta Yayınevi, 24 Mart 2001, s.21.

alışverişi yapabildiği ortamdır, şeklinde tanımlayabiliriz. Fakat doktrinde farklı bakış açıları ile aşağıdaki tanımlamalar yapılmıştır.

Bu tanımlar şunlardır; *"birçok bilgisayar sisteminin birbirine bağlı olduğu, dünya çapında, yaygın olan ve sürekli büyüyen bir iletişim ağı",*[102] *"hepsi aynı protokolleri kullanan birbiriyle bağlantılı çok sayıda ağdan oluşan küresel bir ağ",*[103] *"birbirine bağlı bilgisayarlardan oluşan bir bilgi otobanı",*[104] *"dünya genelindeki milyonlarca bilgisayarın birbirine ağlar ile bağlanmasının oluşturduğu küresel bilgisayar ağları sistemi",*[105] *"merkezi ve hiyerarşik bir yapısı bulunmayan, geniş seviyede planlanmış, global bir ağ yapısı",*[106] *"dünya üzerinde bulunan bilişim ağlarının ve bilgisayarların birbiri ile bağlanarak belli esaslar dâhilinde kendine özgü bir dille iletişimlerinin sağlanması",*[107] *"dünya üzerine yayılmış milyonlarla ifade edilen sayıdaki bilgisayarların birbirine bağlanması ile oluşan ağların yine birbirine bağlanması ile oluşan çok geniş yapıdaki bir ağ",*[108] *"günümüzde bilgiye en kolay, hızlı ve ucuz bir şekilde ulaşmanın yolu",*[109] *"bilgisayarlar arasında kurulmuş bir haberleşme ağı",*[110] "*telefon hatları ve TCP/IP protokolüyle bütün dünyadaki bilgisayar sistemlerinin birbirine bağlanmasıyla oluşturulan entegre bir yapıya sahip olan ve her katılımla geometrik hızla büyüyen bir ağ",*[111] *"birden fazla*

---

[102] Eralp, *Bilişim Terimleri Sözlüğü,* s.74.

[103] Özen-Baştürk, s.13.

[104] Tulum, s.11.

[105] Çekiç, s.34.

[106] Ali Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Genişletilmiş ve Gözden Geçirilmiş 2.B., Ankara, Seçkin Yayınevi, Mayıs 2009, s.36.

[107] Yenidünya-Değirmenci, s.36-37.

[108] Dülger, *Bilişim Suçları*, s.50.

[109] Sınar, s.21.

[110] Yasin Beceni, www. hukukcu. com/ bilimsel/kitaplar /indeks.htm.*"Siber Suçlar"*, (çevrimiçi), (Erişim; 16.3.2011).

[111] Kurt, s.41.

haberleşme ağının, birlikte meydana getirdikleri bir iletişim platformu",[112] ve *"dünya üzerinde bulunan ağların veya bilgisayarların TCP/IP denilen yöntemle birbirine bağlanmasıyla oluşan, yeryüzündeki en büyük insan ve makine birliğini sağlayan ağ"*[113] şeklindedir.

Kuşkusuz yukarıda yer verilen tanımlar, yüzlerce tanımın sadece bir kısmıdır. Ancak her biri internetin farklı bir yönünü de ifade etmektedir. Bu tanımlar ışığında internet'i; *"belirli bir merkezi ve hiyerarşik bir yapısı olmayan ve çok geniş seviyede planlanmış, milyarlarca bilgisayar ve milyonlarca bilgisayar sisteminin oluşturduğu ağların, kendine özgü bir dille belirlenen protokolleri kullanarak, yine birbirine bağlanması ile oluşarak, yeryüzündeki en büyük insan ve makine birliğini sağlayan, kolay, hızlı ve ucuz bir şekilde ulaşılabilen, üretilen bilgiyi saklama/paylaşma ve ona kolayca ulaşma imkânı veren, her katılımla geometrik bir hızla sürekli büyüyen iletişim ve bilgi portalıdır"* şeklinde tanımlayabiliriz.

Bu tanımda dikkat edilmesi gereken husus internetin dünyadaki bilgi ağlarının tamamı olmadığı, internet dışında da bazı ülkelerin, çeşitli kurumların (askeri birlikler, üniversiteler vb.) kendi aralarında iletişim sağladıkları ağların da (LAN ve MAN) bulunduğudur.[114]

İnternet ilk başlarda sınırlı olarak askeri alanda ve askeri haberleşmelerde kullanılırken; dünyadaki tüm ülke ve insanlar tarafından kullanılmaya başlanmasıyla birlikte günümüzde neredeyse işlevlerinin sınırı çizilemeyen konuma gelmiştir. Günümüzde internetle dünyanın dört bir tarafıyla hızlı ve ucuz bir şekilde iletişim kurulup, karşılıklı bilgi alışverişinde bulunulabilmekte, istenen her konuda araştırma yapılabilmekte, bu süreç içinde gerekli görülen bilgi ve dokümanlar bilgisayara yüklenebilmekte, kullanıcının yerinden kalkmasına gerek kalmadan, alışveriş yapılabilmekte, müze ve sergiler gezilebilmekte, müzik dinleyip film izlenebilinmekte, ticaretle uğraşanlar, yurt dışı bağlantılarını ve ticari işlemleri en kısa sürede gerçekleştirilebilmektedir.

---

[112] İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* 1.B, Ankara, Adalet Yayınevi, Eylül 2008, s.7.

[113] Alaca, s.16.

[114] a.g.e. s.7.

İnternet aracılığıyla, özellikle 2011 yılında "Arap Baharı" olarak nitelendirilen Tunus, Libya ve Mısır gibi ülkelerin yönetimlerinin değiştirilmesi sürecinde facebook ve twitter gibi sosyal ağların oynadığı rol düşünüldüğünde ülke yönetimlerinin değiştirilmesinde söz sahibi dahi olunabilmektedir.

1.2.5.2. İnternetle İlgili Teknik Terimler

Kapsam ve özellikleri sayılamayacak kadar çok olan interneti daha iyi kavrayabilmek ve dolayısıyla bilişim suçları açısından daha detaylı bir değerlendirme yapabilmek için internetin alt yapısını oluşturan; TCP/IP Protokolü, IP Adresi, Alan Adı, İnternet Servis, Erişim ve İçerik Sağlayıcılar, Server ve Host gibi teknik terimlerin anlam ve işlevlerinin bilinmesine ihtiyaç vardır. Aşağıda bu terimler sırasıyla incelenmiştir.

1.2.5.2.1. TCP/IP Protokolü (Transmission Control Protocol / İnternet Protocol)

İnternet ağı içerisinde yer alan bilgisayarların sorunsuz olarak iletişimde bulunabilmeleri bazı kurallara uymalarına bağlıdır. Bu kuralların genel adına kısaca "TCP/IP Protokolleri" denir.[115] TCP/IP protokolleri dört katmandan ve yüzlerce farklı protokolden oluşan protokol ailesine/kümelerine verilen addır.[116] Bu protokollerin en önemlileri TCP (Transmission Control Protocol – İletim Kontrol Protokolü) ve IP (İnternet Protocol – İnternet Protokolü) protokolleri olduğu için bu protokollere genel olarak TCP/IP protokolleri adı verilmiştir.

İnternet hizmetlerini kullanabilmek için gerekli programlar ve bağlantı programlarını içeren TCP/IP Protokolü sayesinde dünyadaki tüm bilgisayarlar ortak bir anlaşma dili oluşturarak sağlıklı bir iletişim kurabilmektedirler. Bu protokoller

---

[115] "*İnternette, TCP/IP protokolünün dışında, ortak anlaşma dili olarak başka protokoller de kullanılmaktadır. Ancak bu protokoller pek rağbet görmedikleri ve yaygın olarak kullanılmadıkları için, şu an internet ağında evrensel olarak benimsenmiş tek genel geçer ortak anlaşma dili TCP/IP protokolüdür.*" Sınar, s.24.

[116] Bu katmanlardan bazıları; 1. *Donanım katmanındaki bazı protokoller*; **ARP** (Adres Çözümleme Protokolü), **RARP** (Ters ARP protokolü) 2. *IP katmanındaki bazı protokoller*; **ICMP** (İnternet Yönetim Mesajlaşması Protokolü), **RIP** (Router Bilgi Protokolü), **OSPF** (İlk Açık Yöne Öncelik), **IGMP** (İnternet Grup Mesajlaşma Protokolü), **DHCP** (Dinamik Cihaz Ayar Protokolü) 3. *Taşıma katmanındaki bazı protokoller*; **UDP** (Kullanıcı Veri Protokolü), **TCP** (İletim Kontrol Protokolü) 4. *Uygulama katmanındaki bazı protokoller*; **DNS** (Alan Adı Sistemi), **HTTP** (Hiper Metin Yollama Protokolü), **HTTPS** (Güvenli HTTP), **POP3** (Postahane Protokolü 3), **SMTP** (Basit Mektup Gönderme Protokolü), **FTP** (Dosya Gönderme Protokolü) ve **FTPS** (Güvenli FTP)'dir. www.ip-adres.com/tcp-ip-protokolleri.php (çevrimiçi), (Erişim; 17.04.2012).

birbirleriyle iletişim içinde bulunan tüm donanım ve yazılım birimleri arasında geçerlidir. Bu nedenle iletişimin gerçekleşebilmesi için her ögenin bu protokolü kabul etmiş ve uyguluyor olması gerekir. TCP/IP protokolü diğer iletişim ağlarında da kullanılabilir. Özellikle pek çok bilgisayarı ve/veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı oldukça yaygındır.[117]

1.2.5.2.2. IP Adresi (İnternet Protocol Adres)

IP adresi (numarası); belli bir ağa bağlanmak isteyen bilgisayarların ağa girebilmek için aldıkları sıra numarasıdır. İnternete bağlanan her bilgisayara, o anda sadece kendisine ait olan ve o bilgisayarı tanımlayan özel bir IP adresi numarası verilmektedir. Bu numara her bağlantıda değişmektedir.[118]

Söz konusu adresler 32 bitlik bir sayıdan oluştuğundan internete teorik olarak yaklaşık olarak 4 milyar bilgisayar bağlanabilir. IP adresleri; gösterimi, yazımı ve ağ yönetiminin kolay olması amacıyla, her biri 8 bit'lik olan ve noktalarla birbirinden ayrılan, 163.72.194.50 gibi dört rakam kümesine bölünmüştür. Bu adresleme sisteminde her rakam daha alt birimleri gösterecek şekilde hiyerarşik bir yapı kullanılmaktadır.[119] Adreslemenin ilk kısmı alan adını, son kısmı ise cihazın "host" numarasını verir.

IP adresleri, kullanım şekli itibariyle; dinamik (değişen) ve statik (sabit) adresler olmak üzere ikiye ayrılırlar. Dinamik IP adreslerinin her bağlantıda belli kısımları değişirken, statik IP adresleri ise değişmez. Dinamik IP adresleri telefon ile internete bağlanan kullanıcılara verilirken, statik IP adresleri ise sunucu görevi gören bilgisayarlara verilir.[120]

1.2.5.2.3. Alan Adı Sistemi (Domain Name System)

Alan Adı Sistemi (DNS-Domain Name System); hatırlanması zor olan IP numaralarının yazılarak, internete bağlanılması yerine, okunması ve akılda tutulması

---

[117] Özgür Eralp, http://www.ozgureralp.av.tr/makaleler/İP *"Bilişim Suçlusuna Giden Yol – IP"*, (çevrimiçi), (Erişim; 17.04.2012).

[118] Tulum, s.14; Ergün, "*Siber Suçların Cezalandırılması..."*, s.9.

[119] Ali Osman Özdilek, *(Uygulamadan Örnek Olaylarla) Bilişim Suçları ve Hukuku,* 1.B. İstanbul, Vedat Kitapçılık, Eylül 2006, s.2.

[120] Çekiç, s.39.

çok daha kolay olan ve genelde irtibata geçilmek istenen adreslerle ilişkilendirilebilen simgesel isimlerle yapılan bir adresleme sistemidir.[121]

Teknik bir anlatımla Alan Adı Sistemi (DNS); genel amaçlı dağıtılmış (Distributed), kopyalanmış (Replicated), veri sorgulama (Data Query) hizmeti ve internete bağlanan bilgisayarların isimlerinin IP adresine dönüştürülme yoludur.[122] IP adresleri telefon numaraları gibi düşünülebilir. Bu numaralar yazıldığı zaman ulaşılmak istenen sayfanın bulunduğu sunucuya bağlanılmaktadır. Örneğin 179.23.45.20 numaralı IP adresine simgesel olarak "cankaya.edu.tr" adı verilirse bunu akılda tutmak ve dolayısıyla bağlanmak çok daha kolay olacaktır.

Alan Adı Sistemi; isim sunucuları ve çözümleyicilerinden oluşur. İsim sunucuları, IP adres bilgilerini tutarlar. Çözümleyiciler ise DNS istemcilerdir. DNS istemcilerde, DNS sunucuların adresleri bulunur. Bir DNS istemci irtibat kurmak istediği bilgisayarın ismine karşılık gelen alan adını yazarak isim sunucuya başvurur. İsim sunucu (DNS sunucu) da eğer kendi veritabanında öyle bir isim varsa, bu isme karşılık gelen IP adresini istemciye gönderir ve bu yolla irtibat sağlanır.[123]

DNS isimleri, belli bir kurala göre gittikçe detaylanan bir yapıya uygun olarak genelden özele doğru (tersten) sırasıyla; ülke, kurum, kurum içi kullanıcı şeklinde verilmektedir. Örneğin; "www.cankaya.edu.tr adresinde; "tr" Türkiye'yi, "edu" alt alanın bir eğitim kurumu olduğu, "cankaya" ise bu eğitim kurumunu, "www" başlangıç terimi olarak interneti, göstermektedir.[124]

Alan adlarını ve ülke kodlarını gösteren .com, .tr, .co, uk, gibi simgeleri o ülkelerde yetkilendirilen kuruluşlar yapmaktadır. Dünyada tüm internet kayıt işlemlerini ABD'de bulunan (Global İnternet Registry – Global İnternet Kaydedici)

---

[121] Özdilek, s.2.

[122] Eralp, *Bilişim Terimleri Sözlüğü,* s.51.

[123] Özdilek, s.2; Çekiç, s.39.

[124] Örneğin ülke kodu olarak; "de" Almanya'yı, "uk" İngiltere'yi gösterir. İnternet ve benzeri uygulamaları bulan ülke ABD olduğundan ABD için bir ülke takısı kullanılmamaktadır. İnternet adresleri ülkelere ayrıldıktan sonra .com, .edu, .gov gibi daha alt bölümlere ayrılır. Bu ifadeler DNS'de üst düzey (top level) alan adlarına karşılık gelir. Bazı üst düzey alan ad ve anlamları şöyledir. **com**; ticari kuruluş, **org**; ticari olmayan kurum, **edu**; eğitim kurumu, **net**; internet omurgası işlevini üstlenen ağ, **gov**; hükümete bağlı kurum ve **mil**; askeri kurumları gösterir.

yapmaktadır. Bu kurum Avrupa'da IP numarası dağıtım işini (Reseaux IP Europens Network Coordination Center – RIPE NCC) organizasyonuna vermiştir. RIPE NCC, Türkiye'de IP numarası tahsisi yetkisini Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM)'ne vermiştir. Türkiye'de alan adı tahsis işlemleri ODTÜ, ULAKBİM ve TTnet tarafından yapılmaktadır.[125]

10.11.2008 tarihinde yürürlüğe giren 5809 sayılı Elektronik Haberleşme Kanunu'nun 35. maddesinde *alan adlarının* tahsisinin Ulaştırma Bakanlığı tarafından yapılacağı hüküm altına alınmıştır. Bu kanuna dayanarak Ulaştırma Bakanlığı'nca 06.10.2010 tarihine kadar "*İnternet Alan Adları Yönetmeliği*" hazırlanması gerekiyordu. Ancak bu yönetmelik henüz çıkarılmadığından TRABİS (.tr ağ bilgi sistemi) faaliyete geçmemiştir. TRABİS faaliyete geçtikten sonra alan adları konusunda ODTÜ, ULAKBİM ve TTnet'in görev ve yetkileri sona erecektir.

1.2.5.2.4. İnternet Servis Sağlayıcılar - ISS (İnternet Service Providers)

İnternet Servis Sağlayıcılar (ISS); internete bağlanmak isteyen kullanıcılara, kendi bilgisayarlarını internete genellikle bir giriş kapısı olarak sunan, ticari amaçlı, aracı kuruluşlardır.[126] Ticari kuruluşların dışında öğretim üyelerini ve öğrencileri internete ücretsiz eriştiren kuruluşlar da vardır.[127] İnternete bağlanmak için tüm yazılım ve donanımı hazır olan bir kullanıcı, herhangi bir İnternet Servis Sağlayıcı kuruluş olmadan internet ağına dâhil olamamaktadır. İnternet Servis Sağlayıcıları (İSS); servis sağlama işlevini, her kullanıcıya bir kullanıcı adı ve şifre vererek yaparlar. Genellikle ücretsiz bir e-posta adresi hizmeti de sağlarlar. ISS'ler internete erişim olanağı sağlamanın yanı sıra; kendilerinin hazırladığı ya da başka ISS'ler tarafından hazırlanmış olan içeriği, kendi sunucularında depolayabilme ve doğrudan internet bağlantılarını kullanarak bu içeriği internet üzerinden kullanıcılarına erişilebilir kılabilme özelliğini de sahip bulunmaktadırlar.[128]

---

[125] Ergün, *Siber Suçların Cezalandırılması...*, s.9.

[126] "Herkes İçin Bilgisayar Ansiklopedisi", *İnternet Araçları,* Vogel Yayıncılık, S.1, (İnternet Bölümü), İstanbul, s.7; Tulum, s.15.

[127] Yıldız, s.37.

[128] Seher Ergüç, *"Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku",* Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, İşletme Bölümü (MBA), Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2008, s.7; Çekiç, s.55.

1.2.5.2.5. İnternet Erişim Sağlayıcılar - İES (İnternet Access Providers)

İnternet Erişim Sağlayıcılar (İES); kullanıcıların internet ağına doğrudan erişmelerini sağlayan, başkalarına ait içeriklere ulaşılmasına aracılık eden kuruluşlardır.[129]

İnternet Erişim Sağlayıcı (İES)'ların doğrudan internet hizmeti vermenin dışında ayrıca ISS'lar gibi başkalarına ait bilgileri kendi sunucularında depolayarak bu bilgileri internet üzerinden erişilebilir kılma gibi bir hizmetleri yoktur.[130] Son kullanıcı ile İnternet Servis Sağlayıcıları arasında bağlantı (köprü) görevi gören erişim sağlayıcıların sistemlerinde, bilgiler saniyeden çok daha kısa sürelerde kalır ve hemen internet kullanıcılarına iletilir. İES'lere Türkiye'de örnek olarak en büyük erişim sağlayıcısı olan, Türk Telekom A.Ş.'i verebiliriz.[131]

1.2.5.2.6. İnternet İçerik Sağlayıcılar - İİS (İnternet Content Providers)

İnternet İçerik Sağlayıcılar (İİS); internet üzerinde yayınlanan bir bilgi, belge, yayın veya sitenin internet ortamında yayınlanacak şekilde içeriğini bizzat üreten/hazırlayan kişi ya da kuruluşlardır. Başka bir anlatımla "bir dosya ya da bilgiyi kullanıcıların kendi bilgisayarlarına yükleme hizmeti verenler içerik sağlayıcılardır."[132] Bir web sayfasının/sitesinin içeriğini hazırlayıp, İSS'lar aracılığı ile internette yayınlayan kişi internet içerik sağlayıcısıdır. Bir gazetenin, derginin, internet üzerinde yayınlanan sayfalarını hazırlayan, yayınlanacak haberleri seçerek yayınlayan editörler de içerik sağlayıcıdır. Forumlarda ise, başkaları tarafından gönderilebilen mesajları yazan ve gerek gördüğünde kendisine ait mesajları silebilme veya düzeltebilme, değiştirebilme imkânına sahip olan kişiler de içerik sağlayıcısıdır.[133]

---

[129] Tulum, s.15; Ergüç, s.7.

[130] Yıldız, s.36.

[131] Çekiç, s.55; Ergüç, s.7; Tulum, s.16.

[132] Yıldız, s.37; Ergüç, s.8.

[133] Tulum, s.6; Çekiç, s.56.

1.2.5.2.7. Server ve Hosting

İSS'lerin servis hizmetini sağladıkları sunuculara *server* adı verilmektedir. Sunucu bir bilgisayar ya da program olabilir. Özel veya tüzel kişiye ait olabilir. İSS'nin ya da özel bir sunucunun, başkasına ait olan bilgiyi kendi bilgisayarında depolayarak internette yayınlaması işlemine ise; *hosting* adı verilmektedir.[134] Bir web sitesinin yayına başlayabilmesi için domain adı ve hosting ücreti ödenir. Domain adı için başlangıçta bir kez ücret ödenirken, hosting için her yıl ödeme yapmak gerekmektedir.

1.3. TARİHSEL SÜREÇ

Bilişim sistemlerinin temel yapısını kuşkusuz bilgisayarlar oluşturmaktadır. Bilgisayarlar, XX. yüzyılın ilk yarısının sonlarına doğru mekanik ve elektro-mekanik yapılardan kurtulup, günümüz anlamında elektronik devre elemanlarından yararlanılarak üretilmeye başlanmıştır. Üretimin elektronik devre elemanları kullanılarak yapılması bilgisayar teknolojisindeki gelişmelere çok büyük ivme kazandırmıştır. Anılan gelişmeler sonucunda bir bakıma "elektronik çağ" başlamıştır. İnternetin bulunması ve elektronikle birleşmesinden sonra çok kısa (20-25 yıl) süren "elektronik çağ" sona ermiş ve "bilişim çağı" başlamıştır. Bilgisayarla internetin buluşmasıyla ortaya çıkan bu yeniçağ, aslında bilgisayarın da modern çağıdır.

Doktrinde bilgisayarın tarihi gelişimi çeşitli dönemlere ayrılmıştır. Dikkatle incelendiğinde bu dönemleri birbirinden ayıran etkenler bilgisayarlarda kullanılan elektronik devre elemanlarının niteliği, hafızalarının türü ve kapasitesi gibi etkenlerdir. Bu sınıflandırmalar teknolojik gelişmelere göre yapıldığından doğal olarak dönem sayısı ve tarihleri arasında fikir birliği oluşmamış, farklı değerlendirmeler yapılmıştır.[135] Bu sınıflandırmaların son dönemi, ağırlıklı olarak

---

[134] Yıldız, s.36.

[135] Örneğin; Birinci Dönem (1946-1958), İkinci Dönem (1958-1964), Üçüncü Dönem (1964-1970), Dördüncü Dönem (1970-Günümüze kadar) Akbulut, *Türk Ceza Hukukunda Bilişim Suçları*; s.6-10; Birinci Dönem (1940-1958), İkinci Dönem (1958-1964), Üçüncü Dönem (1965-1971), Dördüncü Dönem (1971- Günümüze kadar) Dülger, s.57-59, Kızıltan, s.28-29 ve Yazıcıoğlu, *Bilgisayar Suçları*, s.34; Birinci Nesil Bilgisayarlar (1945-1956), İkinci Nesil Bilgisayarlar (1956-1963), Üçüncü Nesil Bilgisayarlar (1963-1971), Dördüncü Nesil Bilgisayarlar (1971- Günümüze kadar) Çekiç, s.24-29; bu sınıflandırmaya 5. Nesil olarak (Günümüz ve Gelecek)'i ekleyen de vardır. Güngör, s.25-30; Birinci Dönem (1940-1959), İkinci Dönem (1960-1964), Üçüncü Dönem (1965-1971), Dördüncü Dönem (1971-Günümüze kadar) Demircan, s.15-16.

"1970 yılından günümüze" şeklindedir. 1970'li yıllarda internet yaygınlaşmaya başladığından aslında bilgisayarın tarihi gelişim sürecinde "1970 ve sonrası dönem" olarak ifade edilen bu dönem, aynı zamanda internetin ilk dönemi olmuştur. Açıklanan nedenlerle, bilgisayarın tarihsel süreci dönemlere ayrılmadan ve 1970 sonrası internetin tarihsel gelişimi olarak incelenmiştir.

1.3.1. Bilgisayarın Tarihsel Gelişimi

İnsanlığın bilgiyi elde etme, saklama ve bilgiye en kısa sürede ulaşma ihtiyacı ve çalışmaları çok eskilere dayanır. Ama bu çalışmalar binlerce yıl boyunca çok basit düzeneklere sahip ve karmaşık işlemleri yapamayan mekanik aletlerden öteye geçememiştir. Günümüz anlamında bilgisayar teknolojisinin başlangıcı 1940'lı yıllara dayanır. Başka bir anlatımla, toplumları büyük bir hızla dönüştüren/değiştiren gelişmelere neden olan bilgisayarların 50 - 60 yıllık kısa bir geçmişi vardır.

II. Dünya Savaşı'ndan sonra bazı ülkeler arasında özellikle silah ve savunma teknolojilerinde öne geçme ve bu yolla hasım ülkelere karşı üstünlük elde etme ve bu üstünlüğü devam ettirme yarışı başladı. Bu amaçla teknolojik araştırmalar için ayrılan kaynaklar artırıldı. Nihayet bu çalışmalar ciddi anlamdaki ilk meyvesini 1946 yılında ABD'de verdi.[136] 1946 yılında, askeri amaçla topçu atış hesaplarını yapabilmek için, Pennsylvania Üniversitesinden iki fizikçi ve ekibi tarafından günümüz anlamında ilk bilgisayar olan ENIAC (Electronic Numerical Integrator and Calculator - Elektronik Sayısal Entegreli Hesaplayıcı) üretildi. ENIAC, elektro-mekanik bilgisayarlardan elektronik bilgisayarlara geçişin ilk örneğiydi.[137]

---

[136] ENIAC'tan önce üretilen makineler, mekanik parçalardan oluşan cihazlardı. ENIAC'a en yakın cihaz Amerikalı H. H. Aiken tarafından 1937'de üretilen ve Mark 1 adını verdiği bilgisayardı. Delikli kart sistemiyle çalışan Mark 1, daha önceki benzerlerinden farklı olarak, logaritma ve trigonometrik fonksiyonlar da yapabilmekteydi. Ancak Mark 1; mekanik sayıcılarından oluştuğu için bugünkü anlamda elektronik bilgisayar olarak kabul edilmemiştir (Ö. Turhan, Bütün Yönleriyle Bilgisayar, İstanbul, Beta Basım Yayım Dağıtım A. Ş. 1994, s. 16)'dan aktaran Akbulut, ...*Bilişim Suçları,* s.7.

[137] ENIAC; Amerikalı, Jr. John W. Mauchly ve J. Presper Eckert tarafından geliştirilen, 500.000 dolar maliyetinde, 30 ton ağırlığında, 167m^2 yer kaplayan, yapımında 70.000 direnç, 10.000 kondansatör, 6.000 anahtar, 18.000 elektron lambası, 1.500 röle kullanılan bir cihazdı. ENIAC, saatte yaklaşık 180KW elektrik harcayan, saniyede 5.000 işlem yapabilen, ekranı bulunmayan ve öncekilere göre çok daha hızlı bir bilgisayardı. Yenidünya-Değirmenci, s.13; Çekiç, s.25; Yazıcıoğlu, *Bilgisayar Suçları,* s.34-35.

ENIAC'ın ardından kısa bir süre sonra EDVAC (Electronic Discrete Variable Automatic Computer – Kesikli Değişkenli Otomatik Elektronik Bilgisayar) adı verilen bilgisayar üretildi.[138] EDVAC'ın özelliği, belirli bir hafızasının olması ve ilk kez belleğine program yüklenebilmesiydi.[139]

EDVAC'tan sonra satışa sunulan ilk ticari bilgisayar olan UNIVAC (UNIVersal Automatic Computer –UNIVAC- Evrensel Otomatik Bilgisayar) ve UNIVAC-1 üretildi.[140] Bu sıralarda yarı iletken transistörlerin bulunması bilgisayarların gelişimine önemli katkılar yaptı.[141] Transistörler, daha hızlıydı ve daha az elektriğe ihtiyaç duyuyordu. Transistörün bulunması sonucu, International Business Machine (IBM) şirketi, önemli derecede boyut ve enerji tasarrufu sağlayan ilk ticari bilgisayarı üretti.[142] Bu dönemin genel özelliği temel devre elemanı olarak elektron lambalarının, bellek için manyetik ortamların (manyetik teyp, manyetik disk) kullanılması ve anılan bilgisayarların ayrı bir programlama dillerinin olmaması ve hâlâ makine dilleri ile işlem yapabilmesiydi.[143] Bu eksiklik ayrı programlama dilleri olan FORTRAN (FORmula TRANslator - Çevirici)'ın 1951'de ve ALGOL (ALGOrithmic Language – Dil)'un 1961'de geliştirilmesiyle aşıldı. Daha sonra bu dillerle makinenin donanımı arasında bir köprü işlevi gören işletim sistemleri oluşturuldu. Bilgisayarlar birden çok kişi tarafından kullanılabilecek hale getirildi.[144]

1960'lı yılların ikinci yarısında yarı iletken devre elamanları transistörler geliştirilerek, yüzlerce transistörü içinde barındıran çok küçük boyutlarda entegre (tümleşik) devreler kullanılmaya başladı. Bilgisayarlar sadece bilgi-işlem

---

[138] AnaBritannica Ansiklopedisi, Bilgisayar Programı, C.XIX, s.318.

[139] Yazıcıoğlu, *Bilgisayar Suçları,* s.35; Çekiç, s.25; Güngör, s.26.

[140] Yaycı, s.12; Alaca, s.12; Kızıltan, s.13; Yazıcıoğlu, *Bilgisayar Suçları,* s.36; Çekiç, s.25; UNIVAC-1'in bellekleri 7 adet cıva tankı ve 18 çift kristal transformatörden oluşuyordu. Demircan, s.15.

[141] Yazıcıoğlu, *Bilgisayar Suçları,* s.36; Akbulut, *Türk Ceza Hukukunda Bilişim Suçları,* s.7; Çekiç, s.25.

[142] Bu bilgisayarın IBM-7090 (Yazıcıoğlu, *Bilgisayar Suçları,* s.36) veya IBM-650 ve 700 olduğu ifade edilmektedir. (Akbulut, ...*Bilişim Suçları*, s.7.)

[143] Yazıcıoğlu, *Bilgisayar Suçları,* s.36; Akbulut, ...*Bilişim Suçları,* s.7.

[144] Dülger *Bilişim Suçları,* s.57; Alaca, s.13; Kızıltan, s.14; Yazıcıoğlu, *Bilgisayar Suçları,* s.36; Akbulut, ...*Bilişim Suçları,* s.7; Çekiç, s.26; Güngör, s.26; Demircan, s.16.

merkezlerinde kullanılan makineler olmaktan çıkıp kişisel kullanıma açıldı. ABD'de ilk bilişim suçunun işlendiğine dair bir iddia gazetelere yansıdı.[145]

Programlama dillerine PL/I, BASIC, COBOL gibi yeni diller eklendi. 1975 yılında INTEL firması (0.5cm. yüksekliğinde) ilk mikroişlem birimini imal etti.[146] Bu yıllarda yazılım alanında büyük gelişmeler yaşandı. Paket programlar yaygınlaşarak yoğun şekilde kullanılır oldu. Yaşamın her alanına ait paket programları bulmak olası hale geldi. IBM firmasının 1981 yılında ilk PC'yi üretmesi üzerine o zamana kadar "mikro bilgisayar" olarak adlandırılan bu tür bilgisayarların ismi PC (Personal Computer - Kişisel Bilgisayar) olarak değiştirildi.

Donanım ve fiziksel özellikleri yönünden kişisel bilgisayarların gelişimi ise şöyle olmuştur. 1980'li yıllardan itibaren kişisel bazda yaygın olarak kullanılan bilgisayarların ilk şekli masaüstü bilgisayarları idi. Masaüstü bilgisayarlar, kasa ve içindeki donanımlarla birlikte monitör, hoparlör, klavye ve fareden oluşuyordu. 1990'lı yıllarda kullanılmaya başlayan notebook'larda masaüstü bilgisayarlardan farklı olarak tüm donanımlar tek bir cihazda toplanırken, artık kullanıcılar bilgisayarını yanında taşıyabiliyordu.

Notebook'ların ardından içerisinde, optik sürücü (CD/DVD sürücü) yer almayan nispeten daha zayıf sistem özelliklerine sahip olan ancak daha hafif, daha ucuz ve daha az yer kaplayan netbook'lar (mini notebook) 2007 yılından itibaren kullanılmaya başlandı. Netbook'lar 2007 yılından sonra yaygınlaşmaya başlasa da, yerini yavaş yavaş ultrabook'lara bırakmaya başladı bile. 2012 yılı itibariyle satışa sunulan ultrabook'lar, netbook'lara göre çok daha ince ve hafif bir yapıya sahiptir. Ultrabook'lar netbook'lara göre daha geniş bir ekrana sahip olmasına rağmen, donanımsal özellikleri açısından netbook'lardan üstündürler. Ultrabook'lar henüz yeni bir ürün olduğundan şu sıralar fiyatları da 2 bin liradan başlıyor. Ayrıca 2010 yılında satışa sunulan iPad'ler ile birlikte tablet bilgisayarlar da ikinci baharını yaşamaya başladı. iPad'ler bugün için notebook'ların birebir alternatifi olmasa da,

---

[145] 18.10.1966 tarihinde Minneapolis Tribune gazetesinde "*bir bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor*" şeklinde bir haber çıkmıştır. Emin Doğan Aydın, *Bilişim Suçları ve Hukukuna Giriş,* Ankara, Doruk Yayınevi, Eylül 1992, s.13.

[146] Yazıcıoğlu, *Bilgisayar Suçları*, s.36.

kullanıcılar dokunmatik ekranı sayesinde internete giriyor, dergi ve gazeteleri yine tabletleri üzerinden görüntüleyebiliyorlar.[147]

Bu gelişmelerle bilgisayarların depolama kapasiteleri ve hızları arttı, ebatları küçüldü, fiyatları ucuzladı. İnternetin telefon hatları aracılığı ve bilgisayar yardımıyla kullanılmaya başlanması kişisel bilgisayar kullanımının patlamasına, kişisel bilgisayar sayısının 1975 yılında 300 bine, 1985'te 35 milyona ulaşmasına yol açtı.[148] Yukarıda da bahsedildiği üzere bilgisayarların internet ile buluşması sonrasında, bilgisayarların tarihsel gelişimini internetin tarihsel gelişimi içinde sürdürdüğünü ifade edebiliriz. Son olarak bu cümleye, Digital, Hewlett Packard, Honeywell, Nixodorf gibi dev yabancı şirketlerin yanında Vestel, Arçelik, Casper gibi Türk şirketlerinin de bilgisayar ürettiğini ekleyebiliriz.

1.3.2. İnternetin Tarihsel Gelişimi

Öncelikle bilgisayar ve sonrasında da İnternetin bulunup geliştirilmesi ve günlük hayatın her alanında yaygın olarak kullanılması, bilim adamlarının insanlık tarihi konusunda yapmış oldukları sınıflandırmaları değiştirmelerine dahi yol açtı.[149] Bu derece büyük gelişmeleri sağlayan en önemli olay, dünya çapında bilgisayar kullanımının yaygınlaşması değil, bütün bilgisayar ağlarını kapsayan genel bir ağ olan "internet"in bulunması oldu.

İnternet fikri, daha doğrusu öncelikle bilgisayar ağları fikri; bilgisayarın bulunması sürecine benzer bir gelişme ile yine İkinci Dünya Savaşı'ndan sonra, bazı ülkeler arasında özellikle silah ve savunma teknolojilerinde öne geçme, hasım ülkelere karşı üstünlük elde etme ve bu üstünlüğü devam ettirme yarışı neticesinde ortaya çıktı. İnternet ağlarının gelişmesini tetikleyen en önemli olay 1957 yılında Sovyetler Birliği'nin "Sputnik" adını verdiği aracı dünya yörüngesine göndermesi oldu. Bu gelişme üzerine, Amerika Birleşik Devletleri, hasmı olan Sovyetler Birliği tarafından yapılan bu hamleye cevap verebilmek için bir proje başlattı. Bu projede, nükleer savaş ve/veya büyük bir sosyal karışıklık halinde ülke yöneticilerinin

[147] www.hurriyet.com.tr. (çevrimiçi), (Erişim; 07.04.2012).

[148] Dülger *Bilişim Suçları,* s.57; Alaca, s.13; Kızıltan, s.14; Yazıcıoğlu, *Bilgisayar Suçları,* s.36; Çekiç, s.26; Güngör, s.26; Demircan, s.16.

[149] Bkz. Yuk. 97 numaralı dipnot. (Bu yeni sınıflandırmayı Alvin – Heidi Toffler çifti yapmıştır.)

birbiriyle ve savunma sistem yöneticileri arasında kurulan iletişimin, merkezi bir servis sağlayıcıya bağımlı kalmadan ve kesintisiz devam etmesi, bir bilgisayarın arızalanması halinde diğer bilgisayarlar üzerinden görüşmelerin devam etmesi öngörülüyordu. Anılan proje kapsamında araştırmalar yapmak üzere Savunma Bakanlığı bünyesinde, (1958 yılında) ARPA (Advanced Research Project Agency – İleri Araştırma Projeleri Ajansı) isimli bir daire kurmuştur.[150]

ARPA dairesinin çalışmaları sonucunda, California'dan üç, Utah'dan da bir merkez olmak üzere toplam dört düğüm noktasındaki bilgisayarlar arasında ilk bilgi transferi 1969 yılında gerçekleştirilmiştir.[151] Bu başarı sonucunda proje halinde olan ARPANET (ARPA-NETwork) resmen uygulamaya konulmuştur. Bu sistemden öncelikle ABD ordusu sonra da üniversiteleri yararlanmaya başlamıştır.

Bu ağın temel özelliği bir merkezi ve hiyerarşik bir yapısının olmamasıydı.[152] Bir süre sonra sistemin yaygınlaşması ve ARPANET'e farklı türde ve yapıda bilgisayarların bağlanmaya başlaması neticesinde bilgisayarlar arasında iletişim kurma sorunları baş göstermiştir. Bu sorunlar 1983 yılında TCP/IP protokolünün oluşturulması ve uygulanmasıyla aşılmıştır. İnternet üzerindeki iletişim bugün dahi TCP/IP protokolleri sayesinde sağlanmaktadır. Yine 1983 yılında ARPANET; MILNET (Military Network- Askeri Ağ) ve ARPANET olarak ikiye ayrıldı. MILNET ABD ordusunun kullanımına bırakılırken, ARPANET sivillerin kullanımına açıldı.

1986'da Amerikan Ulusal Araştırma Kurumu (National Science Foundation-NSF)'nun beş üniversitenin bilgisayarlarını bağlayarak NSFNET'i kurması ve bu yeni sistemin ARPANET'in yükünü hafifletmesiyle, sistem diğer ülkelerin de kullanımına açıldı. Sonraki yıllarda bu sisteme; Avustralya, Yeni Zelanda, İzlanda, İsrail, Brezilya, Hindistan ve Arjantin gibi ülkeler de katıldığından ağ dünyada yaygınlaşmaya başladı.[153]

---

[150] Sınar, s.22; Çekiç, s.35; Kurt, s.42; Ketizmen, s.20; Kızıltan, s.16.

[151] Daha detaylı bilgi için bkz. Dülger, *Bilişim Suçları,* s.60; Sınar, s.22; Çekiç, s.35; Kurt, s.42; Demircan, s.22; Alaca, s.17; Tulum, s.17; Ketizmen, s.20; Kızıltan, s.16; Güngör, s.35.

[152] Ketizmen, s.21.

[153] Bu yıllarda ABD dışında ilk olarak İngiltere'de **JANET** (**J**oint **A**cademic **Net**work) isimli ağ olmak üzere bazı Batı Avrupa ülkelerinde ve Japonya'da da çeşitli ağ sistemleri oluşturulmuştur. Dülger, *Bilişim Suçları,* s.60.

İsviçre'nin Cenevre şehrindeki CERN (Conseil Europeen Pour La Researche Nucleaire – Avrupa Nükleer Araştırma Merkezi)'de geliştirilen www (World Wide Web – Dünya Çapında Ağ) teknolojisi ve bu teknolojinin dayandığı en temel dosya transfer protokolü olan HTTP (Hyper Text Transfer Protokol - İnternet Sayfaları Transfer Protokolü)'nin, 1989 yılında bulunması ve ertesi yıl kullanıcıların hizmetine sunulmasıyla önce ARPANET kaldırılmış, ardından 1994 yılında bütün ağ omurgalarının tek bir yapı altında birleştirilmesi ve kişisel kullanıma açılmasıyla da İNTERNET devreye girmiştir.[154]

İnternetin tüm dünyada kullanıma açılmasıyla birkaç milyar insanın aynı anda çok kolay, hızlı ve ucuz bilgiye eriştiren yapı kurulmuştur. Sözkonusu ağ, insanlık tarihi açısından çok kısa süren geçmişine rağmen tüm dünyada yaygın olarak kullanılmaya başlamıştır. Örneğin; 50 milyon kullanıcı sayısına radyolar 38 yılda, televizyon 13 yılda ulaşırken, internet ise sadece 4 yılda ulaşmıştır.[155]

Türkiye'de ise internet konusunda ilk çalışmalar 1987 yılında Ege Üniversitesi öncülüğünde kurulan TÜVAKA (Türkiye Üniversite ve Araştırma Kurumları Ağı) ile başlamasına rağmen, ilk internet bağlantısı TÜBİTAK tarafından desteklenen bir proje kapsamında kiralanan bir hat aracılığıyla, ODTÜ Bilgi İşlem Daire Başkanlığı'nca 12 Nisan 1993 tarihinde, Washington NSFNET üzerinden gerçekleştirilmiştir.[156] Bu hat bir yıl kadar Türkiye'nin tek internet bağlantısı olmuştur. Bu bağlantıyı sırasıyla, 1994 yılı başlarında Ege Üniversitesi, 1995 yılı Eylül ayında Bilkent Üniversitesi, 1995 yılı Kasım ayında Boğaziçi Üniversitesi ve 1996 yılında İstanbul Teknik Üniversitesi'nin internet bağlantıları takip etmiştir.[157]

Bu gelişmelere paralel olarak 1996 yılı Haziran ayında TÜBİTAK bünyesinde ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) kurulmuştur. ULAKBİM'in

---

[154] Sınar, s.23; Dülger, *Bilişim Suçları,* s.61; Kızıltan, s.17, Demircan, s.23.

[155] Demircan, s.21.

[156] Güngör, s.36; Dülger, *Bilişim Suçları,* s.61; Şaban Cankat Taşkın, (2008), *Bilişim Suçları,* 1. Baskı, Bursa, Beta Yayınevi, s.14; Çekiç, s.35; Kızıltan, s.17; Yenidünya-Değirmenci, s.39; Sınar, s.111.

[157] Kayıhan İçel, *Kitle Haberleşme Hukuku*, Basın Radyo Televizyon Sinema, İnternet, Beta Yayım A.Ş. 4.B. 47 numaralı dipnot, 1998, s.415'ten aktaran Akbulut, ... *Bilişim Suçları,* s.17; Sınar, s.111.

görevi Türkiye'deki tüm araştırma ve kuruluşlarını birbirine bağlayacak olan ULAKNET (Ulusal Akademik Ağ) isimli iletişim ağını kurmak ve bu ağ ile ilgili gereken hizmeti vermek idi. ULAKNET 1997 yılında kurularak anılan kuruluşlara o yıldan itibaren ağ hizmeti vermeye başlamıştır.

Günümüzde akademik kuruluşlar ve ilgili birimlerin internet bağlantıları ULAKBİM tarafından; ticari kullanıcılar ve kişisel kullanıcıların bağlantıları ise genellikle TTnet omurgası üzerinden yapılmaktadır.[158] TTnet'in sayısına ulaşamasa da, bazı özel şirketler ve ülkemizde faaliyet gösteren üç GSM şirketi (Turkcell, Avea ve Vodafone) de kablosuz internet bağlantı hizmeti vermektedir. Ülkemizde akademik çalışmalar nedeniyle önce üniversiteler ve akademisyenlerce kullanılan internet, kısa sürede kişisel kullanım açısından da yaygın olarak kullanılmaya başlanmıştır.

2010 yılı Haziran ayı itibariyle Avrupa kıtasında toplam 367,6 milyon internet kullanıcısı vardır. Türkiye 36,5 milyon kullanıcı sayısı ile Avrupa'da 5., dünyada ise 15. sıradadır. Dünyada en fazla internet kullanıcısı 513 milyon adet ile Çin'dedir, Çin'i ABD, Hindistan ve Japonya takip etmektedir.[159] Avrupa kıtasında Türkiye'nin önünde Almanya 65,1 milyon, Rusya 59,7 milyon, İngiltere 51,4 milyon ve Fransa 44,6 milyon internet kullanıcısı sayısı ile yer almaktadırlar.[160] İnternetle ilgili (2012 yılı Nisan ayı itibariyle) diğer sayısal veriler ise şöyledir; Türkiye'de, internete kayıtlı 4 milyon dolayında bilgisayar ve .tr alan adı altında 250 bin alan adı (Domain Name) vardır. Türkiye'de düzenli internet kullananlar nüfusun %25'i civarında iken, TÜİK (Türkiye İstatistik Kurumu) verilerine göre interneti hiç kullanmayanlar toplam nüfusun %58'i civarındadır. İnterneti hiç kullanmayan kadınların oranı kırsal kesimde %85'e kadar yükselmektedir.[161] Dünya genelinde ise; Asya kıtasında 888,3 milyon, Avrupa kıtasında 475,1 milyon, Amerika kıtasında 470,9 milyon, Avustralya

[158] Sınar, s.111-112.

[159] Uluslararası Telekomünikasyon Birliği ve Nielsen Online araştırma şirketi verileri, Hürriyet Gazetesi Ankara eki, 11.06.2012, s.5.

[160] Hüseyin Akarslan, *Bilişim Suçları,* Seçkin Yayıncılık, 1.B. Ankara, Şubat 2012, s.30.

[161]İnternet Teknolojileri Derneği Başkanı Mustafa Akgül'ün açıklamaları, www. teknoloji. bugun. com.tr/internet-18-yasinda-150120-haberi.aspx (çevrimiçi), (Erişim; 11.04.2012).

kıtasında 21,3 milyon[162] olmak üzere toplam, 2 milyara yakın internet kullanıcısı; internete kayıtlı 778 milyon bilgisayar, 313 milyon web sitesi ve 205 milyon alan adı vardır.[163]

1.4. BİLİŞİM SUÇLARI KAVRAM VE TANIMI

Bilişim kavramı, son yarım asırda, temelinde bilgisayar ve internetin yer aldığı teknolojik gelişmelerde çok sık kullanılan temel kavramlardandır. Teknolojinin baş döndüren bir hızla gelişip yayılmasıyla birlikte bu alanda da kötüye kullanımlar ortaya çıkmıştır. Bu tür kötü niyetli kullanımların önüne geçilebilmesi amacıyla, çeşitli ülkelerde ceza hukuku alanında çeşitli yaptırımlar düşünülmüş ve uygulamaya konulmuştur. Ancak bilişim suçları hala tartışılan kendisine özgü özellikleri dolayısıyla henüz üzerinde uzlaşı sağlanamayan bir kavramdır.

Geleneksel suç türleri; nelerin suç olup olmadığı konusunda üzerinde uzlaşının olduğu, belirli bir zaman dilimi, coğrafi ve sosyal sınırlar içinde icra edilen eylemlerdir. Bilişim suçları ise; geleneksel suç türlerinden zaman ve mekân sınırlarının kolayca belirlenememesi, kanun terminolojisi açısından oldukça dikkate değer teknik bilgi gerektirmesi ve nelerin bilişim suçu olup olmadığı konusunda henüz uzlaşı olmaması yönlerinden ayrılmaktadır.[164]

Başlangıçta bilişim suçları, geleneksel suçların bilgisayar yoluyla işlenmesi olarak kabul edilirken, zamanla ayrı kavramlar ve tanımlar yapılmaya çalışılmıştır. Ancak teknolojiye paralel olarak hızla gelişen bilişim suçu tiplerindeki çeşitlilik ve süreklilik; kriminologlar, yasa koyucular, doktrin ve uygulayıcılar arasında üzerinde konsensüs sağlanan bir bilişim suçu tanımının yapılmasına engel olmuştur. Konunun kavranabilmesi daha detaylı incelenme gerektirdiğinden, aşağıda önce "bilişim suçu" kavramı ve sonrasında tanımı üzerinde durulacaktır.

---

[162] Akarslan, s.30.

[163] İnternet Teknolojileri Derneği Başkanı Doç. Dr. Mustafa Akgül'ün açıklamaları, http://www.teknoloji.bugun.com.tr/internet - 18- yasinda - 150120-haberi.aspx (çevrimiçi), (Erişim; 11.04.2012).

[164] M. Niyazi Tanılır, *İnternet Suçları ve Bireysel Mahremiyet,* 1.B., Ankara, Liberte Yayınevi, Ocak 2002, s.14.

1.4.1. Kavram

"Bilişim suçları", bilişim teknolojisindeki gelişmelere paralel olarak ortaya çıkan ve kendine özgü nitelikleri nedeniyle ceza hukuku alanında sürekli tartışılan bir suç türü olduğundan bu suçu ifade edebilmek için birçok kavram ortaya atılmıştır.

Bilişim alanında suç olarak tanımlanan bu ihlaller; "*Bilgisayar Suçu*", "*Bilgisayar Suçları*",[165] "*Bilgisayarla İlgili Suç*", "*Bilgisayar Suçluluğu*", "*Bilgisayar Aracılığıyla İşlenen Suçlar*", *Bilgisayarla İşlenen Suç (Computer Assisted Crime)*", *Bilgisayara Karşı İşlenen Suç (Crimes Against Computer)*",[166] "*Bilgisayar Bağlantılı Suçlar (Computer Related Crime)",*[167] "*İnternet Suçları*",[168] "*Siber Suç (Cyber Crime)*",[169] "Sayısal *Suç*", "Sanal Suç",[170] "*Elektronik Suç (Electronic Crime)*", "*Dijital Suç (Digital Crime)",*[171] "*Siber Uzay Suçları*"[172] ve "*Bilişim İhlali*" gibi çeşitli kavramlarla ifade edilmektedir. Son zamanlarda, "*Yüksek Teknoloji Suçu (Hi - Tech Crime / e-crime)*" kavramı da kullanılmaktadır.

Bu konuda en değişik nitelemelerden birisi ise "Ç*ok Yargısal Suçlar*" (*Multi - Jurisdictional Crime)* kavramıdır.[173] Ancak doktrin ve uygulamada çoğunlukla

---

[165] Yazıcıoğlu, s.135-136.

[166] Dülger, *Bilişim Suçları,* s.63.

[167] Yazıcıoğlu s.126.

[168] Feridun Yenisey, *İnternet Suçlarının Yeni İşleniş Biçimleri*, Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayını, (21-22 Mayıs 2001), s.447; Veli Özer Özbek, *"İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları",* **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, İzmir, C.IV, S.1, 2002, s.106-107.

[169] Ergün, *Siber Suçların Cezalandırılması Ve Türkiye'de Durum,* s.14-15; Beceni, *Siber Suçlar*, 16.03.2011; Hüseyin Çeken, *Amerika Birleşik Devletlerinde İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası,* http://archiv.jura.i-saarland.de/turkish/HCeken1.html. (çevrimiçi), (Erişim; 16.03.2011); Tanılır, s.13.

[170] Reşat Yılmaz Yazıcıoğlu, "*Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı",* Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayını, 21-22 Mayıs 2001, s.452; Beceni, *Siber Suçlar,* 16.03.2011.

[171] Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* s.35.

[172] Ergün, *Siber Suçların Cezalandırılması ...,* s.13.

[173] Barbara Etter, Leadreship in the Hi-Tech Crime Environment, Australasian Centre For Policing Research To 2/2002 Pelp At the Aipm Sydney, 14 August 2002, s.1.'den aktaran Karagülmez, s.35. Bu kavram, bilişim suçlarıyla dünya çapında mücadele edebilmek için çok sayıda ülke ve yargı yeri gerektiği için kullanılmıştır.

"*Bilişim Suçu*"[174] kavramı kullanılmaktadır. Günümüzde az sayıda hukukçu/yazar tarafından hala "*bilgisayar suçu*" veya "siber suç" kavramları kullanılsa da özellikle eski ve yeni ceza yasalarımızdaki "Bilişim Alanında Suçlar" kavramının kullanılmasından sonra ülkemizde hemen hemen "bilişim suçu" kavramı üzerinde uzlaşı sağlanmıştır diyebiliriz.

"Bilişim suçu" kavramı, bilgisayarı ve bilgisayar ağlarını (LAN ve WAN) da içine alan ve diğer kavramlara göre daha geniş kapsamlı bir kavram olduğu için bu çalışmada da "bilişim suçu" kavramı kullanılmıştır. Ülkemizde bilişim alanında işlenen suçları ifade etmek amacıyla kullanılan kavramları bu şekilde inceledikten sonra uluslararası alanda, önde gelen ülkelerin doktrin ve uygulamalarında bu suç türüyle ilgili hangi kavramların kullanıldığını inceleyelim.

Uluslararası alanda genel olarak bilişim suçlarıyla ilgili yasal bir tanım yapılmayıp[175] tanım yerine belirli kavramların kullanıldığını görmekteyiz. Bilgisayarların ilk olarak bulunup kullanılmaya başlandığı ABD'de doğal olarak bilgisayarla ilgili suç oluşturan davranışlara da ilk kez rastlanmış ve bu tür suçlar için doktrinde ve uygulamada "*Bilgisayar Suçu*" (Computer Crime) kavramı

---

[174] Doğan Soyaslan, *Ceza Hukuku Özel Hükümler,* 8.B., Ankara, Yetkin Yayınevi, 2010, s.155; Yenidünya - Değirmenci, s.31; Akbulut, *Türk Ceza Hukukunda Bilişim Suçları*, s.35; Kurt, s.49; Osman Yaşar, Hasan Tahsin Gökcan, Mustafa Artuç, *Yorumlu Uygulamalı Türk Ceza Kanunu,* Ankara, Adalet Yayınevi, C.V, 2010, s.6733; Taşdemir, s.244; Karagülmez, *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, s.35-36;* Ersoy, s.153; Cevat Özel, *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı,* (Derleyen Yeşim M. Atamer), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1.B., İstanbul, İstanbul Bilgi Üniversitesi Yayınları, No:51, s.341; Taşkın, *Bilişim Suçları,* s.12; Mustafa Yücel, *"Bilişim Suçları",* **Ankara Barosu Dergisi**, Yıl:49, S.4, Ankara, 1992, s.505; Alaca, s.21; İlker Çiçek, *"Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları"*, Haliç Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yönetim Bilişim Sistemleri, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2008, s.3; Olgun Değirmenci, *2004 Türk Ceza Kanunu'nun Bilişim Suçları Bakımından Değerlendirilmesi,* **Türkiye Barolar Birliği Dergisi**, S.58, 2005, 195-196; Hikmet Dijle, *"Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı"*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Elektronik-Bilgisayar Eğitimi Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara, Mayıs 2006, s.20-22; Ali İhsan Erdağ, *"Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda)",* **Gazi Üniversitesi Hukuk Fakültesi Dergisi**, C.XIV, S.2. Ankara, 2010, s.275; Aydın, s.12; Pallı, s.40; İlbaş, s.2; Tulum, s.19; Nacar, s.6; Yaycı, s.23; Demircan, s.25-26.

[175] "Bilişim Suçları" konusunda, tanım yapmak bu alanın sınırlarını çizmek demektir. Devletlerin yasa metinlerine, bilişim suçunun tanımını koymamasının nedeni, bu alanda yeni gelişebilecek bazı suçları tanım dışında (yaptırımsız) bırakmama düşüncesi olabilir. (F.G.)

kullanılmaya başlanmıştır. Doktrinde Almanya'da bu kavramı karşılamak üzere "Bilgisayar Suçları (Computerkriminalitat)" İtalya'da, "Enformatik Suç (Dolo İnformatica)", "Elektronik Suçlar (I Reati Elettronici)", "Bilgisayar Kullanımı Vasıtasıyla İşlenen Suçlar (I Reati Commessi Con I'uso Del Computer)", "Bilişim Suçluluğu (La Criminalita)" Fransa'da, "Bilişim Ceza Hukuku (Le Droit Penal İnformatique)", "Bilişim Suçluluğu (La Criminalite İnformatique)" ve " Bilişim Suçları (La Fraude Informatique)" kavramları kullanılmaktadır.[176]

Bu ülkelerin yasa metinlerine bakılacak olursa; "Bilişim Suçu" kavramının karşılığı olarak önceki Fransız Ceza Kanunu'nda "Bilişim İhlâli (La Fraude İnformatique)" yeni yürürlüğe giren Fransız Ceza Kanunu'nda ise "Verileri Otomatik İşleme Tabi Tutan Sistemlere Karşı İşlenen Suçlar (Des Atteintes Aux Sytemes De Traite Automatise De Donnees)" [177] İtalyan Ceza Kanunu ve Ceza Usul Kanunlarında "Bilişim Suçluluğu (La Criminalità İnformatica)" kavramı kullanılırken, Alman Ceza Kanunu, suçun işlendiği verileri esas aldığından bu tür suçlar için belirli bir kavram kullanmamıştır.[178]

Bilişim suçunu ifade etmek için kullanılan kavramlardan bazılarına doktrinde haklı olarak çeşitli eleştiriler yöneltilmektedir. Örneğin; "Bilgisayar Suçu" kavramının bilgisayarı suçun faili gibi gösterdiği, bilgisayarın suç işleyemeyeceği, bu kavramla kastedilenin aslında bilgisayar aracılığıyla işlenen suçlar olduğu ama bu durumda da nasıl tabanca aracılığıyla işlenen suçlara "tabanca suçları", suçun işlendiği yer açısından, apartmanda işlenen suçlara "apartman suçları" denemiyorsa, bilgisayar ile işlenen suçlara da "bilgisayar suçları" denemeyeceği; "internet suçu" kavramının ise, internet dışındaki ağlar üzerinde işlenen yerel (LAN) ve şehirsel (MAN) ağları kapsamadığı; "Siber Suç" ve Türkçedeki karşılığı olan "Sanal Suç" kavramıyla ilgili ise; işlenen suçların gerçek olması, sanal olmaması, bu tür suçların elektronik ağlar üzerinde işlenmesinin fiziki gerçekliği ortadan kaldırmadığı yönünde, bizim de katıldığımız haklı eleştiriler vardır.[179]

---

[176] Akbulut, ...*Bilişim Suçları,* s.34; Dülger, *Bilişim Suçları,* s.64.

[177] 765 sayılı ETCK'ndaki "Bilgileri Otomatik İşleme Tabi Tutan Sistem Kavramı" Yeni Fransız Ceza Kanunu tasarısından alınmıştır. Yazıcıoğlu, *Bilgisayar Suçları,* s.129.

[178] Akbulut, ...*Bilişim Suçları,* s.34; Özen – Baştürk, s.12; Dülger, *Bilişim Suçları*, s.64.

[179] Yenidünya–Değirmenci, s.31-33; Dülger, *Bilişim Suçları,* s.64-65.

1.4.2. Tanım

Bilişim suçlarının kendine özgü nitelikleri nedeniyle bir tanım yapabilmek için kimi hukukçular tarafından bazı kriterler tespit edilmiştir. Bu kriterler üzerinde uzlaşı sağlanamadığı için, bilişim suçunun tanımı üzerinde bir konsensüs sağlanabildiğini söylemek güçtür. Doktrin ve uygulamada kullanılan çeşitli "bilişim suçu" tanımları şöyledir; "*elektronik bilgi işlem kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtlara girilmesi veyahut bilgi tecavüzü için hazırlık yapılması*",[180] "*bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sisteme yasaya ve ahlaka aykırı olarak yetki dışında yapılan müdahale*",[181] "*bilgisayarı da kapsayan ancak daha geniş olan bilişim araçları ile işlenen veya bilişim araçlarına karşı işlenen suçlar*"[182] ve "*verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alanında işlenen, bir bilgisayar ya da ağına yönelik olarak ya da onları kullanarak icra edilen her türlü yasadışı haksız eylem*"dir şeklinde tanımlanmıştır.[183]

Tanımlamalarda kullanılan bazı kriterler; "*bilişim araçlarına karşı, bilişim sistemleri aracılığıyla veya bilişim sistemlerine karşı işlenen suçlar*",[184] "*bilgisayarın amaç veya araç olarak kullanılması, bilişim sistemleriyle bağlantılı olması, suçta bilgisayar kullanılması* kriterleri, *bilişim suçlarını sadece malvarlığı ihlaliyle sınırlandıranlar* ve bu konuda *tanım yapmayanlar"*[185] ya da bilişim suçlarını "e*konomik suçlar (beyaz yaka suçları) olarak değerlendirerek faili esas alan kriter*"[186] şeklindedir. Ceza hukukunda klasik suç tiplerine uygulanan çeşitli hükümlerin, kendine özgü nitelikler taşıyan bilişim suçlarında uygulama imkânı

[180] Aydın, s.27.

[181] Sinan Esen, *Malvarlığına karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar,* Ankara, Adalet Yayınevi, Eylül 2007, s.625.

[182] Ersoy, s.151.

[183] Kurt, s.53.

[184] Ersoy, s.160-161.

[185] Akbulut, ...*Bilişim Suçları,* s.36-45.

[186] Yazıcıoğlu, *Bilgisayar Suçları*, s.140-141.

olmaması nedeniyle, bilişim suçlarının klasik suç tiplerinden farkını ortaya koyabilmek için ileri sürülen bu kriterlere doktrinde çeşitli eleştiriler yöneltilmiştir.

Bilişim suçlarının ilk çıktığı dönemlerden beri, bilgisayar veya bilişimle bağlantısı olan bütün suçlar bilişim suçu olarak kabul edilmiş veya belirli kriterler kullanılarak, kriterlere uymayan her suç türü bilişim suçu kapsamı dışında bırakılmıştır.[187] Bu iki uygulamanın dışında bir yol bulunarak ceza kanunlarında yer alan geleneksel suç tiplerinden herhangi bir farkı olmayan bir suçu sırf bilgisayara karşı veya bilgisayarla işlendi diye bilişim suçu kabul etmemeli, öte yandan bilişim sistemiyle veya bilişim sistemine karşı işlenen bazı fiilleri de çeşitli kriterlere uymadı diye bilişim suçu dışında bırakmamalıyız. Örneğin, donanım unsurlarına fiziksel olarak yapılan bir saldırı sonucunda; yazıcı, monitör, klavye, fare gibi çeşitli unsurların kırılması, tahrip edilmesi ama verilerin veya veri işlemin zarar görmemesi halinde, klasik suç tiplerinden hiçbir farkı olmayan, yalnız "*mala zarar*" niteliği taşıyan bu fiili sırf bilgisayara karşı yapıldı diye veya internet üzerinden yapılan hakaret fiilini de sırf "*internet aracılığıyla*" yapıldı diye bilişim suçu olarak değerlendirmemeliyiz.[188] Öte yandan bilişim sistemine herhangi bir zarar vermeksizin "*bilişim sistemine girme*" ve yine herhangi bir zarar vermeden ayrılma fiilini de klasik suç tiplerine uymadığı, herhangi bir malvarlığı zararının oluşmadığı gerekçesiyle de bilişim suçu kapsamı dışında bırakmamalıyız.[189]

Yukarıda verilen örneklerin de ortaya koyduğu gibi, bilişim suçu tanımı için yalnız "*malvarlığına zarar verme*" kriteri yetersiz kalmaktadır. Diğer bir kriter olan "*faili esas alan kriter*"de yetersizdir. Çünkü bilgisayar ve bilişim sistemlerinin ortaya ilk çıktığı dönemlerde bu sistemlerden menfaat elde edebilmek için herkesin sahip olamayacağı teknik bilgiye ihtiyaç vardı ve bilişim sistemleri günümüzdeki kadar yaygınlaşmamıştı. Belki failin özelliği anılan ilk dönemlerde önemliydi. Ancak günümüzde bilişim sistemleri çok yaygınlaştığından, bu tür suçları işleyebilmek için

---

[187] "Cep telefonu ve fax gibi iletişim teknolojileri ile işlenen suçlar yanında, korsan CD satımı, lisanssız bilgisayar programı kullanma gibi suçlarında bilişim suçu olduğu" ileri sürülmektedir. Örneğin; Önder Ayhan, *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar*, İstanbul, Filiz Kitabevi, 1994, s.2.

[188] Akbulut, ...*Bilişim Suçları*, s.44. Bu arada yazarın bahsettiği bilgisayar aracılığıyla öldürme fiilinin nasıl bir suç olduğu anlaşılamamaktadır.

[189] TCK. m.243/1'de bu fiil "Bilişim sistemine girme" başlığı altında yaptırıma bağlanmıştır.

gereken bilgilere isteyen herkes kolaylıkla ulaşabilmektedir. Dolayısıyla bu tür suçlar için failin özelliği kalmamıştır. Ayrıca bu kriter kabul edilirse, bilgi sahibi olmadan, hatayla, yanlışlıkla büyük bir şirketin sistemine zarar vererek verilerin silinmesine neden olan failin eylemi de bilişim suçu olarak değerlendirilemeyecektir.[190] "*Bilgisayarın amaç veya araç olması", "bilişim sistemleriyle herhangi bir şekilde bağlantılı olma" ve "bilgisayar kullanımı",* "*ekonomik suç"* kriterleri de, özellikle zarar verilmeden sisteme girilmesi veya sadece donanım unsurlarına zarar veren eylemleri, bilişim suçu kapsamı dışına bıraktığından yetersiz kalmaktadır.

Sonuç olarak yukarıda açıklanan nedenlerle bilişim suçlarını kısa bir şekilde "*verilere ve/veya veri işlemle bağlantısı olan sistemlere karşı, doğrudan veya bilişim sistemleri aracılığıyla işlenen suçlar*" şeklinde tanımlamamız mümkündür.[191] Bu tanımlama, doğrudan veya dolaylı (dar veya geniş) anlamda kabul edilen bilişim suçlarını kapsamaktadır. Bilişim sistemine izinsiz veya yetkisiz erişimler ve girişler ve bu bağlamda sistemin yetkisiz kullanılması ve/veya verilerin ele geçirilmesi, veri sahtekârlığı, bilişim dolandırıcılığı ve verilere veya veri işleme zarar verilmesi fiilleri girmektedir. Burada önemli olan fiilin verilerle veya veri işlemle ilgili olması ve bilgisayar veya bilişim sistemlerinden faydalanılmak suretiyle gerçekleştirilmiş olmasıdır.[192]

Bilişim suçları tanımındaki "*doğrudan"* kelimesini; bilişim sistemi aracılığı olmadan, doğrudan doğruya "girilmek istenen bilişim sistemi önüne oturularak, sistemin (fiziksel olarak) açılıp üzerinde işlem yapılması" şeklindeki bazı fiillerin bilişim suçu kapsamı dışında kalmaması amacıyla kullandım. Tanımda kullanılan "*verilere ve/veya veri işlemle bağlantısı olan sistemlere karşı*" ifadesi; failin, bilişim sisteminde bulunan verileri, programları veya veri işlemle bağlantısı olan diğer herhangi bir unsuru ele geçirmeyi amaçladığı durumlarda, suç bilişim sistemlerine karşı işlenmiş olacağı için kullanılmıştır.

Daha öncede ifade edildiği üzere bilişim ve bilişim suçları alanı sürekli genişleyen dinamik bir alandır. Aslında bilişim suçları, dünyada herhangi bir

---

[190] Akbulut, ...*Bilişim Suçları*, s.44.

[191] a.g.e. s.44; Taşdemir, s.244; Dülger, *Bilişim Suçları*, s.67.

[192] Akbulut, ...*Bilişim Suçları*, s.45.

bilgisayar kullanıcısına veya sisteme karşı, herhangi bir ülkeden işlenebildiği için bilişim suçlarına bir çerçeve çizmekte oldukça zordur. Zaten bu nedenle bilişim suçlarına, "*çizgisiz çerçeveli suçlar*" da denilmektedir.[193] "Bilişim Suçları" konusunda, tanım yapmak bu alanın sınırlarını çizmek demektir. Oysa bu tür suçlar "çizgisiz çerçeveli suçlar" olduğu için tam bir tanımını yapmak da mümkün değildir. Bu nedenle belki de bilişim suçlarının çerçevesinin çizilememesi nedeniyle uluslararası mevzuatta, yasa metinlerinde, bilişim suçunun tanımı yapılmamıştır. Ancak devletlerden bir üst kurum olan Avrupa Topluluğu, bilgisayar suçları olarak ifade ettiği bilişim suçlarını 1983 yılı Mayıs ayındaki Paris toplantısında "*bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemle gayri kanuni, gayri ahlakî veya yetki dışı gerçekleştirilen her türlü davranış*"tır şeklinde tanımlamıştır."[194] Ülkemiz mevzuatında bilişim suçlarının bir tanımı yapılmamıştır. Bu bağlamda TCK'da da tanım yapılmayıp tanım yerine "bilişim sistemleri" kavramı kullanılmıştır.

1.5. BİLİŞİM SUÇLARININ TASNİFİ

Bilişim suçlarının tasnifi için bilişim suçlarının tanımlarına bakmanın yardımcı olabileceği düşünülebilir. Ancak üzerinde uzlaşılmış ortak bir tanım olmadığı için bu yolla bilişim suçlarının tek bir çeşit tasnifini yapabilmek mümkün değildir. Bunun yerine tanımlardan yola çıkarak bilişim suçu olarak değerlendirilen durumları ve bilişim suçlarını birbirinden ayırmak için kullanılan çeşitli kriterleri incelemek yerinde olacaktır.

Bilgisayar ve internetin ilk kullanıldığı ülke olan Amerika Birleşik Devletleri doktrininde, bilişim suçları üç ana başlık halinde sınıflandırılmıştır. Bu başlıklar; fikir haklarına karşı tecavüzler (programlar ve veriler dâhil), bilgisayar donanımına ve gereçlerine karşı işlenen suçlar ve bilgisayar kullanıcılarına karşı işlenen suçlar şeklindedir.[195] Amerika Birleşik Devletleri'nde daha ayrıntılı olarak yapılan başka

---

[193] Mustafa Karabal, www.turkhukuksitesi.com *"Bilişim Suçları ve Türk Polis Teşkilatı",* (çevrimiçi), (Erişim; 24.04.2012).

[194] Reşat Yılmaz Yazıcıoğlu, *Bilgisayar ve Bilgisayar Şebekeleri İlgili Suçlar Konusunda TCK 2000 Tasarısı,* Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Paneli, Bursa, 24.03.2001, s.71; Eralp, *Bilişim Terimleri Sözlüğü*, s.31.

[195] Aydın, s.28-29; ABD'de bilişim suçlarının dört ana başlık halinde sınıflandırıldığını söyleyen de vardır. Bu başlıklar; vandalizm, (*bilgisizlik ya da zevk için kasten kamu veya*

bir tasnifte ise on iki ayrı kategori tespit edilmiştir. Bu kategoriler; mülkiyete karşı hırsızlıklar, verilere veya hizmetlere karşı gerçekleştirilen hırsızlıklar, giriş ihlalleri, veri sahtekârlığı, insan hataları neticesi oluşan ihlaller, gasp, sır aleyhine ihlaller, sabotajlar, maddi kısımlara yönelik hırsızlıklar, evraklarda gerçekleştirilen sahtekârlıklar, ATM kartları konusundaki hırsızlıklar ve manyetik kartların şifreleri hususunda gerçekleştirilen fiiller şeklindedir.[196]

Amerika Birleşik Devletleri Adalet Bakanlığı, bilişim suçlarında bilgisayarı baz alarak üçlü bir sınıflandırma yapmıştır. Bu ayrıma göre bilişim suçları; Bilgisayarın hedef alındığı suçlar, bilgisayarın fail olduğu suçlar ve bilgisayarın suçun işlenmesinde kullanıldığı suçlar şeklindedir. Bilgisayarın hedef alındığı suçlar; bir bilgisayara veya ağ bağlantısına izinsiz erişim, veri ve/veya bilgilerine yapılan saldırılar veya elektronik kimlik hırsızlığı şeklinde gerçekleştirilmektedir. Bilgisayarın suçun faili olduğu suçlar suçun fiziki işlenme yerinin bilgisayar olması ve mağdurun mal kaybı söz konusu olan; bilgisayar korsanlığı, virüs, solucan, yazılım bombaları veya trojanların bulaştırılması gibi durumlarda geçerlidir. Bilgisayarın suçun işlenmesinde aracı olarak kullanıldığı suç türü ise; bir bilgisayarın kredi kartı bilgilerini çalma veya saklama, çocuk pornografisi veya buna benzer kötü içerikli görüntülerin yayılması amacıyla kullanılması durumunda söz konusu olabilir.[197]

Avrupa Birliği (o zamanki adı Avrupa Ekonomik Topluluğu) ise aldığı bir tavsiye kararında bilişim suçlarını beş ayrı sınıflandırmaya tabi tutmuştur. Bu sınıflandırmaya göre bilişim suçları; bilgisayar verilerini transfer etmek için veya bir sahtekârlık yapmak için ya da bilgisayar sistemlerinin çalışmasını engellemek için; verileri ele geçirmek, bozmak, silmek veya yok etmek, ticari amaçla bir bilgisayar

---

sanat yapılarına zararlar vermek, yıkmak ve bu eylemleri kendi başına bir amaç durumuna getirmektir. Burada veri ve programlara bilgisizlik, heyecan yaşamak veya zevk için zarar vermek amacında kullanılmıştır. F.G.) veri ve programlara karşı gerçekleştirilen hırsızlık veya dolandırıcılıklar, mali ihlaller ve hizmet hırsızlıkları şeklindedir. Yazıcıoğlu, *Bilgisayar Suçları*, s.148-149.

[196] Yazıcıoğlu, *Bilgisayar Suçları*, s.149; Kurt, s.77-78; Ergün, s.28-29.

[197] Rizgar Muhammed Kadir, *"The Scope And The Nature Of Computer Crimes Statutes A Critical Comperative Study",* German Law Journal, June 2010, s.616'dan aktaran Yavuz Erdoğan, *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle)*, 1.B., İstanbul, Legal Yayıncılık, Şubat 2012, s.96.

programının yasal sahibinin haklarını zarara uğratmak ve bilgisayar sistemi sorumlusunun izni olmaksızın emniyet tedbirlerini aşıp sisteme girerek müdahalede bulunmak şeklindedir.[198]

Birleşmiş Milletler ve Avrupa Birliği'nin 11.06.1999 tarihinde hazırladığı "Bilişim Suçları" raporunda ise bilişim suçları altı sınıfa ayrılmıştır. Bunlar; bilgisayar sistemlerine ve servislerine yetkisiz erişim ve dinleme, bilgisayar sabotajı, bilgisayar aracılığıyla dolandırıcılık veya sahtecilik, yasayla korunmuş yazılımların izinsiz kullanımı ve diğer suçlar şeklindedir. Diğer suçlar başlığı altında kanundışı veya pornografik yayınlar, hakaret ve sövme fiilleri vardır.[199] Birleşmiş Milletler'in düzenlemiş olduğu 10. Kongrede bilişim suçları ikili bir tasnife tabi tutulmuştur. Bu sınıflandırmalar; bilgisayar sisteminin güvenliğini veya veri işlemini hedef alan eylemleri niteleyen "*dar anlamda bilişim suçları*" ve bilgisayar sistemi ve ağı aracılığıyla veya bu sistem ve/veya ağda gerçekleştirilen hukuka aykırı eylemleri niteleyen *geniş anlamda bilişim suçları*dır.[200]

Avrupa Konseyi Siber Suç Sözleşmesinde ise bilişim suçları dörde ayrılmıştır. Bu sınıflandırmalar; bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarla bağlantılı suçlar, içerikle bağlantılı suçlar ve telif hakları ve benzer bağlantılı hakların ihlâline ilişkin suçlar şeklindedir. Bunlardan birinci grup olan "bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanıma açık bulunmasına yönelik suçlar", yasadışı erişim ve müdahale, verilere ve sistemlere müdahale ve cihazları kötüye kullanma suçlarıdır. İkinci gruptaki "bilgisayar bağlantılı suçlar", bilgisayar bağlantılı sahtekârlık ve bilgisayar bağlantılı dolandırıcılıklardır. Üçüncü grubu oluşturan "içerikle bağlantılı suçları" çocuk pornografisi ile bağlantılı suçlar oluşturmaktadır. Son gruplandırma

---

[198] Cevat Özel, *Bilişim Suçlarının Türk Ceza Kanunu ve Tasarı'daki Hükümler Yönünden Mukayeseli Değerlendirilmesi - Öneriler,* (Derleyen; Mete Tevetoğlu), Türkiye II. Bilişim Hukuku Sempozyumu, Bilişim Hukuku Toplantıları, İstanbul, Kadir Has Üniversitesi Yayınları, Aralık 2006, s.86; Yazıcıoğlu, *Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı,* s.71; Kızıltan, s.23-24; Akarslan, *Bilişim Suçları,* s.39; Kurt, s.78.

[199] Muhittin Kaya, Ankara Barosu Uluslararası Hukuk Kurultayı Adli Bilişim Oturumu Konuşma Metni, Ankara, Ankara Barosu Yayınları, C.II. (05.01.2008 - 11.01.2008), s.93.

[200] Yazıcıoğlu, R.Y. *Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı,* 2002, s.460.

ise "telif hakları ve benzer bağlantılı hakların ihlâline ilişkin suçları" oluşturmaktadır.[201]

Türk doktrininde ise, "bilişim sistemlerine/şebekelerine karşı işlenen suçlar ve bilişim sistemleri/şebekeleri ile işlenen suçlar şeklinde ikili ayrım",[202] ile "bilgisayar araç olarak kullanılarak; malvarlığına karşı işlenen suçlar, kişiye karşı suçlar ve bilgisayarın araç olarak kullanılması suretiyle topluma ait haklar üzerinde işlenen suçlar",[203] "bilgisayarın suçun maddi konusunu oluşturduğu suçlar, bilgisayar aracılığıyla işlenen suçlar ve bilgisayar ortamında işlenen suçlar",[204] "bilgisayarın fiziksel yapısına zarar veren eylemler, bilgisayarın işletme sistemine karşı eylemler ve bilgisayar ağlarına yönelen eylemler" şeklinde üçlü ayrımlar yapılmaktadır.[205]

Bilişim suçlarını, doğrudan (dar anlamda – gerçek anlamda) bilişim suçları ve dolayısıyla (geniş anlamda) bilişim suçları şeklinde ikiye ayırmak mümkündür.[206] Şöyle ki; doğrudan bilişim suçları, klasik suçların dışında, bilgisayar ve bilişim ağları ortaya çıkmadan önce işlenmeyen, görülmeyen ve bu nedenle de klasik ceza hükümleri tarafından tam anlamıyla yaptırıma bağlanamayan suç türleridir. Bu tür suçlara; bilişim sistemlerine yetkisiz, izinsiz erişim, verilere ve bilişim ağlarına yönelik eylemleri sayabiliriz. Dolayısıyla (geniş anlamda) bilişim suçları ise, klasik suçların bilişim sistemi unsurları vasıta olarak kullanılarak işlenmesidir. TCK'da bu sınıflandırma kabul edilmiş ve bu yönde düzenlemeler yapılmıştır.[207]

---

[201] Kızıltan, s.24; Erdoğan; s.98.

[202] Sulhi Dönmezer, *Bilgisayar Suçları,* IGUL Ceza Hukukunun Güncel Kaynakları, Hocaların Hocası Ord. Prof.Dr. Dr. H.c. mult. Sulhi Dönmezer Özel Bölüm, Promat Basım Yayın Sanayi ve Tic. A. Ş. İstanbul, Temmuz 2004, s.97; Şaban Cankat Taşkın, *"Bilişim Hukuku Uluslararası Uyuşmazlıklar"*, **Türkiye Barolar Birliği Dergisi**, Ankara, S.85, 2009, s.335; Haluk İnanıcı, *"Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü",* **İstanbul Barosu Dergisi**, C.LXX, S.7-8-9, 1996, s.514; Kurt, s.79; Olgun Değirmenci, *"Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi",* **Legal Hukuk Dergisi**, İstanbul, C.I, S.11, 2003, s.2750.

[203] Önder, s.505.

[204] Ersoy, s.160.

[205] Karagülmez, *Bilişim Suçları...,* s.53.

[206] Ergün, *Siber Suçlar...* s.27-43.

[207] "*Bilişim suçları, öğretide ve uygulamada öncelikle; a) Doğrudan bilişim suçu (gerçek bilişim suçları) b)Dolayısıyla bilişim suçu (bilişim bağlantılı suçlar) biçiminde tasnife tabi tutulmuştur. TCK'da da bu sistem kabul edilmiştir.*" YCGK, E.2009/11-193, K.2009/268,

1.6. BİLİŞİM SUÇLARININ İŞLENME YÖNTEMLERİ

1.6.1. Genel Olarak

Bilişim suçlarını klasik suç tiplerinden ayıran özelliği işlenme şekillerinin farklılığıdır. Klasik (dolandırıcılık, hırsızlık, yaralama, gasp, cinayet gibi) suçların maddi unsurunu oluşturan eylemler failin yoğun ve etkili fiziki hareketleri sonucu ortaya çıkmaktadır. Bilişim suçlarında ise failin; bilgisayarın klavyesine, fare (mouse)'nin tuşuna veya gelişmiş bazı cep telefonları veya tabletlerin ekranına dokunması dışında fiziksel bir eylemi yoktur. Ancak çok basit bu fiziksel eylemle mağdurlara klasik suçlarla verilebilecek zararlardan çok daha fazla zarar verilebilmektedir.[208]

Bilgi ve iletişim teknolojileri sayesinde bilginin ani, hızlı ve çok sayıda üretilmesi, iletilmesi ve kullanılması, bu sistemlerin insanların hayatını kolaylaştırmasına ve dolayısıyla hayatın her alanına yayılmasına, ulusal ve evrensel düzeyde etkisinin sürekli artmasına yol açmaktadır.

Bilişim sistemleri artık günlük hayatımızın olmazsa olmazları arasındadır. Bilişim sistemlerinin hayatımızın her alanını kaplaması, bu sistemlerin hayatımızı kolaylaştırmasının yanında kötü niyetle kullanılmasının yolunu da açmıştır. Kötü niyetle kullanım halinde bilişim suçlarını önlemenin ve tespitinin zor, suistimalinin de bir o kadar kolay olması bu suç türünün sürekli yayılmasına yol açmaktadır. Bu bağlamda bilişim suçlarının faili olan kişilerin ve her ölçekteki organizasyonun bilişim teknolojilerinin sunduğu imkânları ve bilişim sistemlerinin açıklarını kullanma yönünde her gün yeni yöntemler kullandıkları da dikkat çekmektedir.

Bu yöntemler, bankamatik şifresini kopyalamak gibi basit bir eylemden başlayıp toplumdaki güven duygusunu zedelemeye, terörist eylemlere, hedef ülkenin bilişim sistemlerine çeşitli gruplar vasıtasıyla saldırmaya varıncaya kadar değişik hedeflere karşı işlenmektedir.[209]

17.11.2009) ve (11. CD. E.2009/1616, K.2009/11328, 07.10. 2009), (Kaynak; Kazancı İçtihat Programı, 19.06.2012).

[208] Dülger, *Bilişim Suçları,* s.69.

[209] Örneğin, ülkemiz Başbakanlığına ABD ve Çin'den yapılan siber saldırıları, Başbakanlıkta görevli 5 bilişim güvenliği uzmanının püskürtmesi, saldırının ardından önlemleri artıran Başbakanlığın Türk mühendislerinin hazırladığı yerli yazılım bir güvenlik duvarı kurması. www.sabah.com.tr., (çevrimiçi), (Erişim; 07.03.2012), Bilgi Teknolojileri ve İletişim

Bilişim Sistemlerini hukuka aykırı olarak kullanma amaçları bilgisayar bilgisini ölçme, eğlence, heyecan,[210] intikam, suç işleme, siyasi çıkar sağlama, maddi menfaat temini, bilgi toplama, rakip firma bilgilerini ele geçirme, terörizm, ülkeler arası psikolojik harekât, saldırı veya savunma olmak üzere çeşitlilik göstermektedir. Bu durum bize bilişim suçlarının fail ve mağdur yelpazesinin giderek genişlediğini göstermektedir. Bilişim suçları bu kadar çeşitlenince mağdurlar da kişiler, yöneticiler, şirketler, muhalifler, hükümetler ve devletler olabilmektedir.[211] Bilişim suçlarının icra aşaması klavyeye, fareye, tuşa basılmak veya ekrana dokunmakla başlatılırken, suç konusu işi asıl olarak bu amacı yerine getirmeye yönelik olarak üretilmiş birçok değişik program yapmaktadır. Uygulamada bilişim suçlarını işlemek için üretilmiş zarar verici bu tür programlara "vandalware" (yıkıcı yazılımlar) adı verilmektedir.[212] Bilişim suçlarının sistemi hedef alanları; sistemi yavaşlatmak, aksatmak, durdurmak, bozmak şeklinde ortaya çıkabildiği gibi, bilgiye ulaşmayı hedefleyenler ise; bilgiye ulaşma, bilgiyi yayma, değiştirme, bozma, çalma ve saklama şeklinde ortaya çıkabilmektedir.[213] Aşağıda açıklamaya çalıştığım suç işleme şekilleri sadece tespit edilebilmiş ve nasıl yapıldığı ortaya çıkarılmış bazı örneklerden ibarettir, çünkü bilişim teknolojisinin gelişmesine paralel olarak her geçen gün yeni bir bilişim suçu işleme şekli ortaya çıkmaktadır ve bu hıza yetişmek mümkün değildir.[214] Bu nedenle "yazılıma dayalı bilişim suçları" konusunu kısmen

---

Kurumu'nun (BTK), Anonymous grubu tarafından hack'lenmesi ve elde edilen verilerin internette yayınlanması. www.sabah.com.tr. (çevrimiçi), (Erişim; 14.02.2012).

210 "Bilgi Teknolojileri ve İletişim Kurumu (BTK) Başkanı Tayfun Acarer, *siber saldırı* başlatan Anonymous (Anonim) adlı hacker grubuna yönelik operasyonda göz altına alınanların *bu işe ya heyecan olsun diye ya da bilmeden bulaşan gençler olduklarını* belirtti." www.milliyet.com.tr. (çevrimiçi), (Erişim; 11.06.2011).

211 Örneğin; "Filistinli siber korsanlar, ABD'deki en büyük Yahudi lobi kuruluşlarından *The American-Israeli Public Affairs Committee (Aipac)'in sitesini çökerterek Yahudi işadamlarının bilgi ve belgelerine ulaşmışlardır"* haberi ve "*ABD'nin önde gelen siber gruplarından L0pht, Chaos Computer Club ve the Cult of the Dead Cow'u da bünyesinde toplayan LoU ekibi, Irak'taki her türlü bilgi ve enformasyon ağına saldırı başlattı*," haberi www.hurriyet.com.tr. (çevrimiçi), (Erişim; 25.10.2002).

212 Akbulut, ...*Bilişim suçları,* s.53.

213 Öztürk, s.8.

214 Alev Akkoyunlu, "*2011 yılı sonunda dünyadaki zararlı yazılım sayısının 50 milyon adedi geçmiş olacağını tahmin ediyoruz*" şeklinde bir açıklama yapmıştır. **TBD Bilişim Kültürü Dergisi**, Yıl 40, S.141, Mart 2012, s.18-19.

sınırlandırarak yazılıma dayalı *bazı* bilişim suçları" başlığı altında incelemeye çalıştım.

1.6.2. Kullanıcı Hatasına Bağlı Bilişim Suçu Yöntemleri

Kullanıcı tabanlı siber ihlal yöntemleri, bilişim sistemlerine herhangi bir saldırgan yazılım veya sistemdeki güvenlik açıkları gibi teknik unsurlar kullanmadan doğrudan kullanıcıların dikkatsizlik, dalgınlık veya tecrübesizlik gibi zayıf yönlerini dikkate alarak uygulanan erişim tekniklerdir.[215]

1.6.2.1. Şifre ve Gizli Soru Tahmini

Bilişim sistemleri genellikle, kullanıcılarının sisteme giriş şifrelerini unutmaları durumunda yedek olarak kullanılmak üzere (en sevilen arkadaş veya en sevilen hayvan gibi) gizli bir soru ve yanıt ikilisinin, doğru bir şekilde cevaplanmasını istemektedir. İşte sisteme yetkisiz olarak girmek amacıyla en yaygın olarak kullanılan bu yöntem, şifreye erişim için kullanılan gizli soru cevabının tahmin edilmesine dayanmaktadır.

Günümüzde telefon bankacılığı işlemlerinde banka görevlileri tarafından güvenlik amacıyla sorulan anne kızlık soyadı, gizli soru ve yanıt ilişkisinin en çok kullanılan örneğidir. [Bu bağlamda bazı sosyal paylaşım sitelerinde (facebook gibi); kullanıcının dayısı ve soyadının yer alması, anne kızlık soyadının tespitini sağladığından faillerin işini çok kolaylaştırmaktadır.]

1.6.2.2. Omuz Sörfü

Kullanıcıların bilişim sistemlerine giriş şifrelerini yazarken görülmesi, gizlice izlenmesi, masa takvimi, ajanda, post-it, not kâğıtları, databank, cep telefonu gibi şifre yazılabilecek kaynakların incelenerek şifrelerin öğrenilmesine dayanan bir yöntemdir.[216]

1.6.3. Yazılıma Dayalı Bazı Bilişim Suçu Yöntemleri

Çeşitli amaçlarla üretilen ve neredeyse her gün geliştirilen yeni yazılımlarla bilişim sistemlerinin güvenlik açıklarının tespit edilerek, sistemlere girilmesine

[215] İlbaş, s.28.

[216] a.g.e. s.29.

hukuka aykırı menfaatler elde edilmesine ve/veya zarar verilmesine aracılık eden yöntemlerdir.

1.6.3.1. Bilgisayar Virüsleri (Computer Viruses)

Bilgisayar virüsleri, yerleştikleri bilişim sisteminde çeşitli dosyalara kendi program kodunu eklemek (kopyalamak) suretiyle çoğalan ve yazılımdan yazılıma, dosyadan dosyaya, sistemden sisteme kolaylıkla yayılabilen, sistem dosyalarına ve verilere en çok zarar veren programlardır.[217] Virüs programları genellikle "assembler" isimli az yer tutan alt düzey programlarda geliştirilebildikleri için çok kısa programlardır. Biyolojik virüslere çoğalıp bulaşabilme (yayılabilme) ve sistemi hasta edebilme özelliği benzediği için bu zararlı programlara "virüs" adı verilmiştir.[218] Günümüzde bilgisayar virüsleri; eğlence, heyecan, hırs, bilgisayar ağlarının performanslarını düşürmek, bilgi toplamak, sistemi kullanılamaz hale getirmek veya antivirüs programı satarak kazanç sağlamak gibi çeşitli amaçlarla üretilmektedirler. Bilgisayar virüsleri; çoğu kez bir e-postayla sisteme yerleşip insanların farkında bile olmadığı günlük işlemleri sonucunda, sistemde hızla yayılırlar. Bulaşma şekillerine, zarar seviyelerine veya hedeflerine göre tasnif edilebilen bilişim virüslerinin oluşturdukları suç unsuru, bilişim sisteminin işleyişini engellemek ve/veya bilgi çalmak olarak değişebilmektedir.[219] Bilgisayar virüsleri, bilgisayarda yerleştikleri yerlere göre genellikle "boot (ön yükleme) virüsleri", "dosya (file) virüsleri" ve "makro (ön ek) / mail virüsleri" olmak üzere üç gruba ayrılmaktadır.[220]

Boot virüsleri, disketlerin ve sabit belleklerin boot (ön yükleme) kısmına yerleştiklerinden bu adı almışlardır. Bilgisayarların çalışabilmesi için ihtiyaç duyduğu sistemlerin yüklenmesi gerekir. Sistemlerin yüklenmesi de bir disket, sabit disk veya bir ROM yongası (entegre devresi) aracılığıyla yapılır. Uygulamada ana

---

[217] Türkay Henkoğlu *Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi*, 1.B. İstanbul, Pusula Yayıncılık, Eylül 2011, s.20.

[218] Yazıcıoğlu, *Bilgisayar Suçları,* s.161; Sacit Yılmaz, (2011), *5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar,* **Türkiye Barolar Birliği Dergisi**, Ocak-Şubat 2011, Y:23, Ankara, S.92, s.76.

[219] Öztürk, s.13.

[220] Kızıltan, s.26.

sistem disketleri, genellikle boot edilebilir (ön yükleme yapılabilir) disketler olarak düşünülür ve bir bilgisayarı açma işlemi boot etme (booting up) olarak tanımlanır. Sistemin açılışı sırasında boot edilebilir diskler yüklenmeden bilgisayardaki herhangi bir programın çalıştırılamaz. Bu dosyalar bilgisayara verilecek tüm komutların nasıl yerine getirileceğini gösterirler.

Boot virüsleri, boot (ön yükleme) kısmına yerleştiklerinden bilgisayarlar her açıldığında veya sıfırlandığında (reset'lendiğinde) otomatik olarak çalışarak yüklenecek programın komut akışını değiştirir ve kendilerini de yüklerler. Bu virüsler, bilgisayarlar kapatılıncaya kadar yayılmaya ve kendi kendilerini çoğaltmaya devam etmektedirler. Boot virüslerine Brain, Crazy Boot Ver. 1.0, Ping Pong gibi virüsler örnek olarak verilebilir.[221]

"Dosya (file) virüsleri; uzantısı .bat, .exe veya .com olan çalıştırılabilir bir program sonuna yerleştikten sonra girdikleri programda değişiklik yaparak dosya çalıştırıldığı anda kendisini RAM belleğe yerleştirir."[222] Dosya virüsleri bilgisayar açık kaldığı müddetçe bellekte kalarak bu sırada çalıştırılan her dosyaya kendisini bulaştırır. Joker, Disk Killer, Walker virüsleri bu tipe örnek olarak gösterilebilir.[223]

Makro (ön ek) / mail virüsleri ise; Microsoft firmasının makro komutları yazmak için programlama dili olan "Word Basic"i geliştirmesinden sonra ortaya çıktılar, makro (ön ek) çalıştırma özelliği olan dosyalara bulaşmaktadırlar.[224] Makro/mail virüsleri Microsoft Office programlarına özellikle Word, Excel dosyalarına bulaşmaktadırlar. W97M/Class, W97M/Ethan virüsleri makro virüslerine örnek olarak verilebilir. Dosya virüslerinin en çok rastlanan türü olan mail virüsleri, kısa sürede binlerce bilgisayara bulaşma özellikleri yönüyle diğer dosya virüslerinden daha çok zarar vermektedirler.[225] Örneğin Filipinli bir bilgisayar öğrencisi tarafından 2001 yılında yazılan "Love Bug" isimli virüs programı 18 saat

---

[221] Kurt, s.71.

[222] Alaca, s.192; Yaycı, s.32.

[223] Alaca, s.64.

[224] Ergün, *Siber Suçların Cezalandırılması ...,* s.27.

[225] Mahmut Karslıoğlu, "Virüs mü kaptınız? Geçmiş olsun", CHIP Mayıs 2000 sayısı s.183'den aktaran Kızıltan, s.26; Alaca, s.64; Çekiç, s.73.

içinde 100 milyon bilgisayara bulaşmıştır.[226] Bilgisayar virüsleri; aslında *Ağ Solucanları*, *Truva Atı* gibi programların bir üst yapısını oluşturmaktadır. Virüsler; ağ solucanlarından dosya ve yazılımlar aracılığıyla yayılabilmeleri ve sisteme zarar vererek dolaşmaları yönlerinden; Truva Atı'ndan ise, sisteme izinsiz girmeleri yönünden ayrılırlar.

1.6.3.2. Ağ Solucanları (Network Worms)

Bilişim sistemine girdikten sonra, kullanıcının haberi olmadan hızlı bir şekilde kendini kopyalayarak çoğalan, genellikle e-posta aracılığıyla yayılan, girdiği sistemde donanıma veya yazılıma zarar vermeden bilgisayardan bilgisayara dolaşabilen ve sayısı aşırı artınca sistemleri çökerten zararlı yazılımlardır.[227]

Ağ solucanları, genellikle iyi oluşturulmamış güvenlik duvarlarını aşıp bilişim sistemine girerek eylemlerine başlamaktadırlar.[228] Solucanlar; disket, CD, internet ve e-posta gibi çeşitli yolları kullanarak bilgisayarlara bulaşırlar. Sisteme girdikten sonra ilk önce RAM (Read Access Memory - Rastgele Okunan Bellek) bellek'te kendine bir yer bularak kendini oraya kopyalarlar, daha sonra ise yeni kopyasını üretir ve çalıştırırlar. Sisteme yerleşen ağ solucanı otomatik olarak ve sürekli ilk üretilen kopyasını üretmeye devam eder. Başka bir ifade ile kopya solucandan kopyalama yapılamaz, kopyalama sadece orijinal solucandan yapılır. Kopyalama işlemi, sistemin hafızası doluncaya kadar devam eder, hafızada yer kalmayınca bilgisayar bazen yavaşlayarak veya yavaşlamadan çöker.[229] Ağ solucanları yerleştiği bilişim sistemiyle yetinmeyip başka bilgisayarlara da yayılmak isterler. Başka bilişim ağına ulaşıp o sistemin güvenlik duvarıyla karşılaştıklarında, kolayca tahmin edilen şifreleri ve verileri kullanıp, en çok kullanılan şifreleri ve ürettikleri değişik anahtarları deneyerek, güvenlik duvarını aşmaya çalışırlar.[230] Ağ solucanları, bu tür yöntemlerle bilişim sisteminin güvenlik duvarını aştıktan sonra

---

[226] Ergün, *Siber Suçların Cezalandırılması ...,* s.27.

[227] Aydın, s.53; Yılmaz, *...Bilişim Alanındaki Suçlar,* s.76.

[228] Kızıltan s.26.

[229] Halil İbrahim Dilek, *"Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri"*, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır, 2007, s.46.

[230] Kızıltan, s.26.

sistemin içine yerleşir, sistemde serbestçe dolaşırken ya sistemde bulunan yazılımlara zarar vermekte ya da üzerinde taşımış olduğu bir "Truva Atı" yazılımını sisteme bırakmaktadırlar. Sistem içinde bu eylemleri gerçekleştiren ağ solucanları genellikle hareketlerine ilişkin izleri de silmekte ve bulunmalarını nerdeyse imkânsız hale getirmektedirler.[231]

Kendilerini otomatik olarak çabuk ve çok sayıda çoğaltma becerileri olan solucanlar e-posta adres defterlerinde kayıtlı herkese kopyalarını gönderebilir ve sonra aynı şeyi gittiği yeni bilgisayarlarda da yapabilir. Girdikleri iletişim ağında çok gizli bir şekilde dolaşan solucanların, sisteme yerleştirdikleri *Truva Atı* yazılımı ile o sistem hakkında bilgi toplanabilirler.[232] Hatta bilgisayarlar, sisteme ağ solucanını yerleştirenlerin kontrolüne de geçebilir.[233] (Bu şekilde başkasının kontrolüne geçen bilgisayarlara "zombi bilgisayar" adı verilmektedir.) Yazılımdan yazılıma, dosyadan dosyaya kendisini kopyalama imkânı olmayan solucanlar girdikleri sistem kullanıcısının herhangi bir işlem ya da müdahalesine veya başka bir dosyaya ihtiyaç duymadan çalışabilmektedirler.[234]

Ağ solucanlarının varlığı ilk olarak 2 Kasım 1988 tarihinde ABD'de gerçekleştirilen bilişim sistemine saldırı olayıyla ortaya çıkmıştır. Söz konusu tarihte o günkü veri iletişim ağı olan ARPANET'e yüklenen bir yazılım bir anda ülkenin tüm önde gelen bilim kurumlarına ve askeri araştırma merkezlerinin bilişim sistemlerine bulaşmış ve inanılmaz bir hızla kendisini kopyalayarak sistemleri kullanılamaz hale getirmiştir. Bu saldırı sonucunda yapılan incelemede 2 bin bilgisayara bu solucanların bulaştığı ve 150 bin dolarlık zarara yol açtığı görülmüştür.[235]

1.6.3.3. Bilgi-Veri Aldatmacası (Data Diddling)

Veri aldatmacası; bilgi sistemine girilecek verilerin, bilerek yanlış girilmesi veya bazı verilerin eksik bırakılması gibi yollarla, verileri değiştirme yetkisi olan ya

---

231 Yaycı, s.35.

232 Akbulut, ...*Bilişim Suçları,* s.57.

233 Alaca, s.63.

234 Henkoğlu, s.183.

235 Aydın, s.48; Yazıcıoğlu, *Bilgisayar Suçları,* s.152; Kurt, s.62.

da yetkisiz kişilerce sonradan değiştirilmesi yöntemidir. Sisteme bu yöntemle veri yerleştiren veya değerleri değiştiren fail, mevcut veriler üzerinde istediği değişikliği yapma veya sistemi istediği gibi kullanma imkânına kavuşur.[236] Bu yöntem bilişim suçları içerisinde uygulanabilmesinin kolay olması, işlemden sonra tespiti ve ortaya çıkarılmasının zor olması nedenleriyle en çok tercih edilen yöntemlerden biridir.[237]

Veri aldatmacası yöntemi; veri-işlem belgelerinin değiştirilmesi, manyetik bant, disk veya disket gibi veri saklama birimlerinde saklanan verilerin özel olarak hazırlanmış araçlar ile değiştirilmesi, sisteme veri eklenmesi, bazı kayıtların iptali veya kontrol süreçlerinden kaçırılması şekillerinde uygulanabilir. Bu yöntem doğal olarak bilişim sistemlerine müdahale yetkisi olan kişilerce işlenebileceği gibi yetkisiz kişilerce de işlenebilir. Bu failler; verileri oluşturan, kaydeden, işlenmeye nezaret eden, nakleden, kontrol eden, şifreleyen kişiler olabileceği gibi, bu kişilerin dışından mevcut bir ağ üzerinden bilişim sistemlerine ulaşabilen kişiler de olabilmektedir.[238]

1.6.3.4. Bukalemun (Chameleon)

Adını aldığı canlıdan da anlaşılabileceği gibi, bukalemun yazılımı, yasalara uygun hazırlanmış programların her hareketini taklit ederek kullanıcıları kandırıp bilişim sistemlerine girer. Sistemi kullanan bir veya birden fazla kullanıcının ad ve şifrelerini gizli bir dosyaya kaydeder.[239] Kullanıcı adı ve şifrelerini kaydettikten sonra sistemin geçici bir süre ile kapatılması gerektiği mesajını verir. Sistem kapatılınca bukalemun yazılımının üreticisi, elde ettiği kullanıcı ad ve şifrelerini kullanarak sisteme girip yasadışı isteklerini gerçekleştirir.[240]

---

[236] Aydın, s.48; Kurt, s.62; Alaca, s.57; Güngör, s.60; Nacar, s.9.

[237] Veri aldatmacasına dünyadan ABD'de bir şirketin müdür yardımcısının kayıtlara girme yetkisini kullanarak, adına hisse senedi alım-satım hesabı açması, bu hesaptan kredi alıp borçlandırma işlemleri gerçekleştirmesi, bu durumun ortaya çıkmaması için tek nüsha kredi makbuzları düzenlemesi gibi işlemlerle 5 yıl içinde 50 bin ABD doları haksız kazanç elde etmesi örnek olarak gösterilebilir. Türkiye'den ise 1996 yılında bir banka çalışanının bankasının bilgisayar sistemine girerek kısa sürede yaptığı hilelerle 300 milyar TL tutarındaki hazine bonolarını üç ayrı bankada açtığı hesaplara transfer etmesi, sanığın arkadaşlarının da bu paraları çekip kaçmaları örnek olarak gösterilebilir. Yazıcıoğlu, *Bilgisayar Suçları,* s.151-153.

[238] Ergün, *Siber Suçların Cezalandırılması...,* s.20.

[239] Aydın, s.51; Kurt, s.75.

[240] Akbulut, ...*Bilişim Suçları,* s.58; Aydın, s.51; Dülger, *Bilişim Suçları,* s.74; Kurt, s.75; Ergün, *Siber Suçların Cezalandırılması...,* s.25; Çekiç, s.77.

1.6.3.5. Casus Yazılımlar (Spyware)

Casus yazılımlar kullanıcının yüklediği oyunlar, programlar, yardımcı araçlar gibi yollarla farkında olmadan bilgisayar sistemine giren yazılımlardır. Casus yazılımlar; girdiği bilgisayarlardaki verileri, gezilen siteleri, bilgisayar içeriğindeki bilgilerin işe yarayan, ya da istenen kısımlarını (şifreleri, gizli bilgileri) belli bir hedefe (üreticisine) göndermekte veya bilgisayarda istenmeyen reklamların çıkmasına, internetten reklam indirilmesine yol açmaktadırlar.[241]

Casus yazılımlar virüs olmadığından anti-virüs programları ile silinmeleri mümkün değildir. Bu tür programlar "Casus Yazılım Temizleme Programları" sayesinde bilgisayarlardan silinebilmektedirler. Bu tür zararlı yazılımlara karşı internet onayı gerektiren sitelerde "Evet-Yes"'e basılmaması, bilinmeyen programların yüklenmemesi, firewall (Koruma Duvarı) kullanılması, anti-casus programlarının kullanılması ve devamlı güncelleştirilmesi gerekir.[242]

1.6.3.6. Atık Toplama, Çöpe Dalma (Scavenging)

"Çöpe Dalma" ya da "Atık Toplama" olarak adlandırılan bu suç türü adından da anlaşılabileceği gibi bilgisayara veri olarak girilen bilgilerin çıktısının veya bilgisayarda bıraktığı izlerin toplanması yoluyla işlenmektedir.[243]

Bu bilgilere, bilgisayardan çıktısı alınan kâğıdın veya çıktının fiziki olarak elde edilmesi gibi basit bir yöntemle ulaşılabileceği gibi; bilgisayarda işlem görüp silinmiş, kayıtları yok edilmeye çalışılmış bilgilerin, bilişim sistemine doğrudan veya ağ ile ulaşılması yolu gibi gelişmiş teknik bilgi gerektiren işlemler sonucunda bazı programlar yardımıyla da ulaşılabilir.[244]

İkinci olarak ifade edilen bilişim sistemine doğrudan veya ağ ile ulaşılması yönteminin temeli bilgisayar diskine kaydolan verinin manyetik band üzerinde

---

[241] Dilek, s.43; Henkoğlu, s.183.

[242] "*Bir programın casus yazılımı olup olmadığı "Casus Yazılımlar Listesi " (Genel olarak Gator, Kazaa, Imesh, DC++, Alexa, Google Toolbar, Tüm Toolbarlar [All Tollbars], Cute FTP, Getright, Flashget) gibi kaynaklardan anlaşılabilir."* Dilek, s.45.

[243] Çekiç, s.63; Ergün, *Siber Suçların Cezalandırılması ...*, s.21; Pallı, s.57.

[244] Kurt, s.62.

bıraktığı izlerin (silmemize rağmen) silinmemesi, kaybolmaması ilkesine dayanmaktadır.[245]

1.6.3.7. Ekran Kaydetme ve Tuş Kaydetme

Ekran Kaydedici (Screenlogger) yazılımlar yerleştikleri bilişim sisteminde ekran görüntülerini kaydederek yazılımı üreten kişilere gönderen bir yazılım türüdür. Bu programlar sanal klavyeden şifre girilirken kaydedilen ekran görüntülerini ve sistem kullanıcılarının yaptıkları her işlemi anlık resimler veya film gibi hareketli şekilde kaydederek yazılımı tasarlayanlara gönderir bu yolla bu kişiler bilgisayarda kayıtlı tüm bilgilere erişim imkânına kavuşurlar. Bu yöntemin özellikle "internet cafe" gibi çok sayıda kişinin ortak kullandığı ve yeterli güvenlik önlemi alınmamış bilgisayarlarda kullanılma olasılığı yüksektir.[246]

Tuş Kaydedici (Keylogger) yazılımları; ekran kaydedicilerle aynı yöntemle sisteme girer ve aynı yöntemle çalışır. Bu yöntemde kullanıcının klavye'de basmış olduğu tuşları, basım sırasına göre; fare ile yaptığı hareket ve tıklamalar ise farenin ekranda durduğu nokta büyüklüğündeki bir grafik şeklinde olmak üzere bir metin dosyasına kaydedilir. Daha sonra kaydedilen bu veriler e-posta ya da uzaktan erişim yöntemiyle yazılımı üreten kişiye ulaşırlar.[247] Ekran Kaydetme ve Tuş Kaydetme yöntemleri ile işletim sistemlerinde tespit edilen açıklardan sisteme uzaktan girilip, sisteme dosya aktarma, aktarılan dosyayı çalıştırma gibi işlemlerle kullanıcılar takip edilebilmektedir.[248] Ekran kaydedicinin tuş kaydediciden farkı sadece klavyede basılan tuşların değil ekran görüntüsünün de naklini sağlamasıdır.[249]

---

[245] Örnek; "1980'lerde ABD'li Pat Riddle; ABD Hava Kuvvetleri bilgisayarları, Pentagon ve Beyaz Saray'ın bilgisayarlarına telefon şirketlerinin arkasında bulduğu, telefon sistemi kitapçıkları ve şirket içi notlarını elde ederek girmiştir." Mungo P. - Clough B. Approaching Zero, Data Crime and the Computer Underworld, *Sıfıra Doğru, Veri Suçları ve Bilgisayar Yeraltı Dünyası* (Çev: Kurma, E.) İstanbul, 1999. s.79'ndan aktaran Yazıcıoğlu, *Bilgisayar Suçları,* s.159, Alaca, s.56; Çekiç, s.63.

[246] Ergüç, s.19; Yazıcıoğlu, *Bilgisayar Suçları,* s.172-175.

[247] İlbaş, s.29.

[248] Dilek, s.41.

[249] a.g.e. s.43.

1.6.3.8. Gizlice Dinleme (Eavesdropping)

Bilgisayar sistemlerinde veri naklinde kullanılan ağlara girilerek veya bilgisayarın az da olsa yaydığı elektromanyetik dalgaların yakalanıp verilerin elde edilmesi tekniğidir.[250] Gizlice dinleme, olarak adlandırılan bu yöntemde aslında dinleme yapılmamakta, ses kaydedici cihazlar kullanılmamaktadır. Bu yöntem bilişim ağına fiziksel yolla girme veya bilişim ağındaki elektromanyetik dalgaların hassas alıcılarla algılanması esasına dayanmaktadır.[251] Fiziksel müdahale yönteminde veri iletişimine aracılık eden bilgisayar ağlarına fiziksel yolla (telefon hatlarındaki gibi) girilerek ağ üzerinde nakledilen bilgilere ulaşılmaktadır. Elektromanyetik algılama olarak niteleyebileceğimiz ikinci yöntemde ise, veri alışveriş bilgileri, sistemin yakınlarına yerleştirilecek hassas elektromanyetik dalga alıcıları vasıtasıyla tespit edilmektedir.[252]

1.6.3.9. Gizli Kapılar veya Hile Kapıları (Trap Doors)

Bilgisayar programcılarının, ileride bilgisayar sistemlerine normal yollardan girememe gibi sorunlar çıkması halinde, sisteme farklı yollardan girip arızaları giderebilmek veya yeni program yükleyebilmek amacıyla işletim sistemleri içine yerleştirdikleri gizli kapıların kullanılarak sisteme hukuka aykırı olarak girilmesi yöntemidir.[253] Bilgisayar programcıları bu yolla değişikliğe kapalı olan programları ortaya çıkan yeni şartlara göre onarma ve sistemi kurtarma olanağı oluşturmak istemişlerdir.[254]

İşletim sistemleri normal şartlarda yetkisiz girişe veya herhangi bir program veya kod çalıştırılmasına veya değiştirilmesine izin verilmeyecek şekilde tasarlanırlar. Ancak bilgisayar programcıları, ileride ortaya çıkabilecek sorunlu

---

[250] Oğuz Turhan, *"Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)",* Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Yayımlanmamış Planlama Uzmanlığı Tezi, Ankara, Nisan 2006, s.51.

[251] Ergün, *Siber Suçların Cezalandırılması ...,* s.21; Çekiç, s.64.

[252] Elektromanyetik dalgaların kirliliği ve kontrollü kullanım hakkında detaylı bilgi için bkz. Fazıl Gürler, *"Tehlikenin Farkında mısınız?"* **Ankara Barosu Bilişim ve Hukuk Dergisi**, S.5, Ankara, 2007, s.38-43.

[253] Kurt, s.67.

[254] Yazıcıoğlu, *Bilgisayar Suçları,* s.157.

durumlara karşı kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programa istendiğinde, "trap doors" adı verilen durma programları eklerler. Bu programları yükleyen programcıların bu gizli kapıları kullanarak, sisteme veya sistemin kullandığı bilgisayara uzaktan erişim yoluyla girmesi mümkündür.[255]

Bu gizli kapıların hatalar giderildikten sonra temizlenmesi gerekir. Ancak bazı durumlarda hatayla ya da ileride kullanılmak amacıyla gizli kapılar kapatılmaz. Ancak kötü niyetli kişilerin de bu kapıları kullanarak sisteme girmesi ve dolayısıyla bilişim suçlarını işlemesi mümkündür. Sık olmasa da kullanıcı kimlik denetimi (kullanıcı adı ve şifre) şeklinde de gizli kapı uygulaması mümkündür.[256]

1.6.3.10. Hukuka Aykırı İçerik Sunma

Hukuka aykırı; ırkçı, ayrımcı, bölücü, terörü ve şiddeti teşvik eden, kişilik haklarına aykırı, insan ticareti veya çocuk pornografisi vb. nitelikteki içeriklerin, web sayfaları, forumlar, elektronik postalar ve dosya paylaşımı gibi veri iletim ağları aracılığı ile diğer kullanıcıların erişimine sunulmasıdır.[257] Bilişim suçlarının son yıllarda sık karşılaşılan bir işlenme şeklidir. Özellikle çocuk pornografisiyle ilgili içeriklerin paylaşımı yaygınlaştığından birçok ülke ve uluslararası kuruluş bu içeriklerin bulundurulması, yayılması ve takibini önlemeye yönelik önlemler uygulamaya başlamıştır.[258]

1.6.3.11. İstem Dışı Alınan Elektronik Postalar (Spam)

İstem dışı alınan iletiler veya yığın ileti; aynı iletinin çok sayıdaki kopyasının, (ticari olan veya ticari olmayan amaçlarla) bilişim ağları üzerinden bu mesajı alma

---

[255] "İngiliz veri ve bilgi hizmeti kurumu olan Prestel'in sistemine girebilmek için kullanıcılar, kendi ID ve parolalarını tuşlamak zorundaydılar. Bu bilgiler kişiye özel ve yalnızca kullanıcı tarafından bilinen on karakterli bir harf ve numara dizisi olan ID ile dört haneli paroladan oluşmaktaydı. Prestel'in numarasını çeviren bir hacker deneme olarak on defa 2s girdi ve *doğru* mesajını aldı. Parola için de basitçe "1234" rakamlarını denedi ve Prestel'in test için bırakılmış gizli kapısından sisteme girdi." Çekiç, s.70.

[256] Pallı, s.55; Alaca, s.62; Çekiç, s.70.

[257] Yaycı, s.33; Alaca, s.71; Dülger, *Bilişim Suçları*, s.78; Öztürk, s.23.

[258] 2001 yılında İngiltere kaynaklı çocuk pornografisine ilişkin içerik bulundurarak bunları diğer kişilerin erişimine açan bir grup izlenmeye alınmış ve aralarında Türkiye'nin de bulunduğu on dokuz ülkenin güvenlik kuvvetleri ile işbirliği yapılarak bu kişiler yakalanmıştır. Volkan Sırabaşı, *İnternet ve Radyo-Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi),* Adalet Yayınevi, 2003, s.127'den aktaran; Yaycı, s.33; Dülger, *Bilişim Suçları*, s.79; Çekiç, s.81.

talebinde bulunmamış kişilere veya kurumlara gönderilmesidir.[259] Bu mesajlar ticari amacı (reklam, pazarlama) olan veya ticari amacı olmayan (siyasal, sosyal) amaçlarla gönderilmiş olabilir.[260]

İstem dışı alınan ileti veya yığın ileti olarak kullandığımız kavram yerine uluslararası literatürde SPAM (Spiced Pork And Ham) kavramı kullanılmaktadır.[261] Spam ilk olarak internette bir sohbet odasında, bir mesajın arka arkaya gönderilmesi olarak kullanılmaya başlamıştır. Spam adı verilen elektronik postaları gönderen kişiye *spammer*, elektronik posta gönderme işlemine ise *Spamming* denilmektedir. Spammer adı verilen kişiler forumlar, e-posta adresi satışları, posta listeleri, haber grupları, usenet, yeniden iletilen elektronik postalar (forward) ve web sayfalarından çalınan adresler, sohbet odaları gibi ortamları elektronik posta adresi elde etmek için kullanarak, buradan elde ettikleri e-posta adreslerine belirli amaçlarla mesaj iletmek, reklam yapmak, kamuoyu oluşturmak isteyen kişi veya kuruluşlara büyük paralar karşılığında satmakta veya bu adreslere bizzat kendileri mesajları atmaktadırlar.[262]

Diğer bilişim suçları kadar ciddi görülmeseler de istem dışı alınan iletiler kişilere rahatsızlık vermekte, özellikle İnternet Servis Sağlayıcıları'nın kaynaklarını israf etmekte, kullanıcılarına daha iyi hizmet sunmak için milyonlarca dolar daha fazla yatırım yapmalarına neden olmaktadır. Örneğin, spam'lerin 2004 yılı itibariyle Amerika Birleşik Devletleri'nde verdiği zararın 10 milyar dolar, Avrupa şirketleri

---

[259] Kurt, s.72; Dülger, *Bilişim Suçları,* s.77.

[260] Uluslararası Ticaret Örgütü'nün 1996 yılında yayınlamış olduğu "ICC Guidelinies on Interactive Marketing Comminication"'da spam; "*bir bülten veya haber grubu üzerinden ticari amaç taşımayan bu forum konuları ile ilgili olmayan ve gönderilmesine açıkça izin verilmeyen reklamlar*" şeklinde tanımlanıp ticari olmama vurgusu yapılırken, Fransız Ulusal Enformasyon ve Özgürlük Komisyonu (Commission Nationale de l'Informatique et des Libertés)'nda spam " *hiçbir temas olmaksızın tartışma forumlarından, dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının talebi olmaksızın ara-sıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalar"*dır şeklinde tanımlanarak *ticari* amaca vurgu yapılmıştır. Ben her iki unsuru da dâhil ederek tanımı yapmaya çalıştım.

[261] SPAM kelimesi, ilk defa bir firma tarafından Amerika'da kullanılmıştır. Anılan kelime bu firmanın baharatlı domuz eti ve jambon için kullandığı bir kısaltmadır**. *S*piced *p*ork *a*nd ha*m*** kelimelerinin baş harflerinden oluşmaktadır. Şimdiye kadar da bilgisayarlar için hiç kullanılmamıştır. Sonraları e-posta yolu ile kitlelere reklam yapılmasında kullanılmaya başlanmıştır. Tekin Memiş, *"Hukuki Açıdan Kitlelere E-Posta Gönderilmesi"*, **Atatürk Üniversitesi Hukuk Fakültesi Dergisi**, Erzincan, C.V. S.1-4, 2001, s.432.

[262] Alaca, s.67; Kurt, s.72; Memiş, s.432.

için ise yıllık 2,5 milyar Euro olduğu açıklanmıştır.[263] Amerikan internet şirketi AOL (Amerika Online) spam iletilerini mahkeme kararıyla durduruncaya kadar günde 1,8 milyon spam almaktaydı. Bu yoğunluktaki spam'in bir tanesini tespit etmek ve silmek için 10sn. zaman harcansa AOL şirketinin bir günlük istenmeyen spam'leri temizlemesi için 5.000 saat (yaklaşık 208 gün) bağlantı yapması ve bu işe personel ayırması gerekmektedir. Yine AOL şirketinin belirttiğine göre, günlük olarak işlem gören 15 milyon elektronik postanın %40'ını Spam'ler oluşturmaktadır. Bazen bir spammer bir dakikada 40.000 ila 50.000 adet elektronik posta alma kapasitesindeki bir sistemi çökertebilmektedir.[264] Türkiye spam gönderilmesinde dünyada 18. sırada yer almaktadır. Bir araştırmada 2009 yılı Mart – Haziran ayları arasında Türkiye'de 17 milyondan fazla spam gönderildiği tespit edilmiştir.[265]

ABD, Avusturya ve Avustralya'da spam göndermek kanunen yasaklanmıştır. Türk hukuku içinde spam'i yasaklayan bir hüküm olmamasına karşılık, engelleyebilecek hükümlerin var olduğu görülmektedir. Gönderilen spam'in içeriğine göre Tüketicinin Korunması Kanunu'na veya MK.'nun m.24 ve devamı hükümlerine göre veya e-postanın içeriğinde tehdit, hakaret gibi yasal olmayan unsurlar varsa bu takdirde de ayrıca ceza kanunu hükümlerine başvurulabilir.[266]

İstem dışı alınan elektronik postalar, sistemi engelleyecek boyuta ulaşırsa TCK'nın 244. maddesinde düzenlenen "bilişim sisteminin engellenmesi" kapsamında değerlendirilebilecektir. Ancak bu dolaylı engelleme çabaları yerine e-posta sahiplerini spam'a karşı koruyabilecek en etkin yolun yasal bir düzenleme ve yasaklama olduğu ortadadır.[267]

---

[263] Olgun Değirmenci, "*Bilişim Suçları*" Marmara Üniversitesi Sosyal Bilimler Enstitüsü Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2002 s.77'den aktaran Çekiç, s.64.

[264] "Bir adet CD'ye 80 milyondan fazla e-posta adresi sığmaktadır. Spammer'lar 1 milyon adrese e-posta gönderimi için haftalık yaklaşık 40 dolar almaktadırlar." Memiş, s.432.

[265] Henkoğlu, s.184.

[266] Yaycı, s.34; Kızıltan, s.27; Örneğin; "bir üniversitemizde idari görevleri de olan bir öğretim üyesine, hakaret ve tehdit içeren bir elektronik posta gönderilmiştir. Mesajda, öğretim üyesinin Ankara'da bulunan bir yakınının takip edildiği ve hareketlerini düzeltmediği takdirde yakınına zarar verileceği şeklinde tehdit bulunmaktadır. E-posta üzerinde yapılan teknik inceleme ile elektronik izler takip edilmiş ve fail yakalanarak mahkemeye sevk edilmiştir." Alaca, s.71-72.

[267] Kurt, s.73; Memiş, s.444.

1.6.3.12. Kredi Kartı Sahtekârlıkları

Bilişim suçu işlenme yöntemlerinden biri olan kredi kartı sahtekârlıklarında; sahte müracaat, sahte kart üretimi, hacking (sistemi kırarak bilgilerini alma), pfishing (balık avlama), web link ve wireless network (kablosuz ağ) hırsızlığı gibi usuller kullanılmaktadır.[268] *Sahte müracaat* yönteminde; gerçek kişilerin kimlik bilgileri elde edilip o şahıslar adına bankalara müracaat edilerek kredi kartı çıkartılıp kullanılmaktadır. *Sahte kart üretimi* ise*;* limiti yüksek kredi kartları ve şifre bilgileri; yasadışı hacking (sistem şifresinin kırılması), banka adına gönderilen sahte mailler (pfishing), bankalar adına sahte internet sitesi açılması (web link) ve internete girmek için kablosuz ağı (wireless network) kullananlardan bilgi hırsızlığı gibi yollarla elde edilip, bu bilgilerle sahte kredi kartı üretilmesi şeklinde yapılmaktadır.[269]

1.6.3.13. Truva Atı (Trojan Horse)

Truva Atı yöntemi; kullanıcılar tarafından yararlı ve lisanslı olduğu için internetten indirilen bazı programların içine gizlice yüklenen, yüklendiği bilgisayar çalıştırılınca o bilgisayarın kaynaklarına uzaktan erişim ve kullanılma imkânı sağlayan yazılım türüdür.[270]

Bu tür programlar genellikle internette ücretsiz yazılım sağlayan web sitelerinden, elektronik posta yoluyla, yardımcı programlarla, resim, video, müzik, animasyon veya ekran koruyucularla ya da arkadaşların birbirine şakalaşmak amacıyla gönderdiği programlara gizlice eklemlenerek sisteme girerler. Başka bir anlatımla trojan tarzı programlar, kullanıcı izin vermedikçe bilgisayarına giremezler. Kendiliğinden çalışma özelliği bulunmayan trojan programı, kullanıcının bahsedilen program veya fotoğrafı görmek maksadıyla çalıştırması halinde aktifleşip kullanıcı bilgisayarında bir açığa yol açarak, sistemi uzaktan erişim için uygun hale getirir. Kullanıcının açtığı program normal şekilde çalışmaktadır ancak arka planda sisteme yerleşen trojan programıyla fail, yine gönderdiği trojan'a uygun bir başka programı

---

[268] Kurt, s.77.

[269] Cevat Özel, *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı,* s.341-361.

[270] Daha detaylı bilgi için bkz. Kızıltan, s.25; İlbaş, s.30; Dülger, *Bilişim Suçları,* s.70; Yıldız, s.71; Yaycı, s.30; Öztürk, s.14; Kurt, s.63; Yazıcıoğlu, *Bilgisayar Suçları,* s.153; Akbulut, *Türk Ceza Hukukunda Bilişim Suçları,* s.56; Aydın, s.49; Ergüç, s.14; Alaca, s.58; Dilek, s.47; Pallı, s.53; Turhan, s.47 ve Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.75.

kullanarak hedefindeki sistemi kendi bilgisayarını kullanıyormuş gibi kullanabilmeye, tüm verilere ulaşabilmeye başlamaktadır.[271] Trojan programları genellikle internet üzerinden gönderilen ve/veya indirilen (.ini, .exe, .msi, .com uzantılı) dosyalara eklenirler. Trojan programları kendi kendilerine çoğalamamaları ve zararsız yazılım gibi görünmeleri yönlerinden virüslerden ayrılmaktadırlar.[272]

Truva Atı yazılımları, adını aldığı mitolojideki Truva Atı (bir armağan/yararlı yazılım) gibi görünüp kaleyi (bilgisayarı) ele geçirme mantığı ile çalışan programlarıdır. Her Truva Atı programı üretilme amacına uygun olarak farklı farklı işlemler yaparlar. Bazı trojan programlarıyla bilgisayar ve CD-ROM sürücüsü açılıp kapatılabilir, bilgisayar ekranına çeşitli mesajlar gönderebilir, bilgisayarın sabit diskine göz atabilir, bir dosya silinebilir, çalınabilir, yeni bir dosya yüklenebilir, sistemin giriş şifresi, kredi kartı şifresi gibi önemli bilgiler elde edilebilir.[273] Bugün internet üzerinde "Rottler, Silk Rope, Girlfriend, Netbus, Boo, Subseven, Back Orifice 2000" gibi trojan programları yaygın olarak kullanılmaktadır. 2009 yılında TrendLabs şirketi tarafından yapılan bir araştırmaya göre veri hırsızlığı yapılan yazılımların 2007 yılında %52'si, 2008 yılında %87'si ve 2009 yılının ilk altı ayında %93'ü Truva atları programları aracılığıyla yapılmıştır.[274]

Bilinen ilk Truva Atı programı 9 Aralık 1987'de Almanya'da "IBM Christmas Tree" adıyla üniversite öğrencilerine e-posta ile gönderilen bir programdı. Bu program 6 gün gibi kısa sürede (15 Aralık 1987'ye kadar) IBM şirketinin posta ağı VNET'i durma noktasına getirmişti.[275] Bilişim suçlarının hemen hemen hepsi bu yazılım yolu ile işlenebilmektedir.[276] Bankaların bilişim sistemine girilerek hukuka aykırı yarar sağlanması eylemleri[277] ya da devletlerin, bilimsel veya askeri

---

[271] Henkoğlu, s.182; Çekiç, s.65.

[272] Ergün, *Siber Suçların Cezalandırılması ...*, s.18.

[273] Alaca, s.58.

[274] Henkoğlu, s.182.

[275] a.g.e. s.182; Çekiç, s.66.

[276] Akbulut, ... *Bilişim Suçları,* s.56.

[277] Bir Kuveyt bankasında çalışan Thompson adında bir İngiliz, ülkesine dönmeden önce sisteme, banka hesaplarında uzun zamandır işlem görmemesi nedeniyle kapatılacak hesapların faizlerinin kendi adına açtığı bir hesaba transferini sağlayan bir Truva Atı

kuruluşların bilişim sistemlerine sızılarak milli güvenlik ve istihbarat bilgilerinin çalınması gibi casusluk eylemleri genellikle Truva Atı programlarıyla yapılmaktadır.[278] Trojan programlarının; kurumsal sistem yöneticilerinin sorumlulukları altındaki bilgisayarda oluşan arızayı giderebilmek amacıyla bilgisayarın yanına gitme imkânı olmadığında, arızalı bilgisayara trojan programı gönderip bu program sayesinde bilgisayarın arızasını öğrenmesi ve gidermesi gibi faydalı yönde de kullanılması da mümkündür.[279]

1.6.3.14. Bombalar (Bombs)

Bilişim sistemlerine zarar vermek isteyen kişi veya kişilerce önceden belirlenen koşullar gerçekleştiğinde bomba gibi patlayarak sisteme zarar vermek üzere üretilmiş programlardır.[280]

Bilişim sistemlerine azami zarar vermek üzere üretilen bombalar (bombs), *Mantık Bombaları (Logic Bombs), Saatli Bombalar (Time Bombs) ve Yazılım Bombaları (Software Bombs)* gibi farklı alt bölümlere ayrılırlar. Bombalar genellikle patlamak için programlandığı özel durumların gerçekleşmesini bekleyen yazılımlardır. Sisteme giren bombalar beklenen duruma kadar, faydalı bir programmış gibi davranarak sistemde kalır. Koşul gerçekleşince yapılan işlemin tersi yönünde veya mantık dışı komutlar vererek sistemi yıkarlar.[281]

---

programı yerleştirmiş ve bu yolla 45 bin sterlin haksız kazanç elde ettiği tespit edilmiştir. Yazıcıoğlu, *Bilgisayar Suçları,* s.155; Ersoy, s.172.

[278] ABD ve İsrail, ana belleğinde "promis" adlı Truva Atı yazılımını içeren bilişim sistemlerini Ürdün'e satarak, Ürdün'ün elinde Filistin hakkında bulunan bilgi ve dosyaları ele geçirmişlerdir. Odabaşı, A. "*Bilgi Toplumu mu? Gözetim Toplumu mu?*" **Bilim ve Ütopya Dergisi**, S.62 İstanbul, 1999, s.29'dan aktaran Yaycı, s.30; Dülger, *Bilişim Suçları,* s.70. İsrail gizli servisi, Suriye Devlet Başkanı Beşar Esad ile eşi Esma Esad'ın internet yazışmalarını bir Truva Atı programı vasıtasıyla ele geçirmiştir. (çevrimiçi) www.sabah.com.tr. (Erişim, 06.06.2005). Esma Esad'ın eşi Suriye Devlet Başkanı Beşar Esad ile internet üzerinden e-posta yoluyla yapmış olduğu kişisel yazışmalar 15 Mart 2012 tarihinde İngiliz Guardian gazetesinde yayımlanmıştır. www.sabah.com.tr. (çevrimiçi), (Erişim; 15.03.2012).

[279] Ergün, *Siber Suçların Cezalandırılması ...*, s.18.

[280] Akbulut, ...*Bilişim Suçları,* s.58.

[281] a.g.e. s.25; Kurt, s.73; Dülger, *Bilişim Suçları,* s.75; Akbulut, ...*Bilişim Suçları,* s.58; Yaycı, s.32; Pallı, s.56; Yıldız, s.75.

Belirli bir zamanda veya saatte aktifleşerek sisteme zarar veren yazılım bombalarına saatli bombalar (Time bombs) adı verilir. Bomba adı verilen yazılımların mantık bombaları ve saatli bombaların dışında *Yazılım Bombaları (Software Bombs)* denilen türü de vardır. Yazılım bombaları sisteme zarar vermek için herhangi bir şartın gerçekleşmesini beklemez. Sisteme girer girmez herhangi bir uyarı veya belirti vermeden verilere çarparak sistemi çökertirler.[282]

Bir mantık bombasının devreye girmesi için beklenen durum; bu programı yazan kişinin maaşının düşmesi, işten çıkarılma,[283] istenen fidyenin ödenmemesi,[284] satılmak istenen programın alınmaması,[285] eğlence, belirli bir tarih veya saat olabilir.[286]

1.6.3.15. Oltalama (Phishing) ve Sahte İleti (Fake Mail)

Olta Saldırıları (Phishing Attacks); faillerin sosyal mühendislik ve teknik hileler kullanarak internet kullanıcılarının kişisel bilgilerini (şifrelerini, kullanıcı adlarını vs.) ve banka hesap erişim bilgilerini (online bankacılık ve kredi kartı numarası, güvenlik kodları vs.) elde etmeye yarayan, zararlı yazılımlardır.[287]

İngilizce "balık tutma" anlamına gelen "fishing" kelimesinden üretilmiş olan phishing yöntemi, balık tutma işlemi ile aynı mantıkla işlediğinden bu adı almıştır. Bu yöntemde hedefte olan binlerce bilgisayar kullanıcısına, içeriği kandırmaya

---

[282] Akbulut, ...*Bilişim Suçları,* s.58.

[283] Bir Amerikan şirketinde çalışan görevlilerden biri işten çıkarılınca şirketin (kendisi dâhil) bütün çalışanlarının kimlik bilgilerini de içeren önemli manyetik arşiv bilgilerini yazılım bombası aracılığıyla silmiştir. Aydın, s.52; Yazıcıoğlu, *Bilgisayar Suçları,* s.157.

[284] Dilek, s.31.

[285] ABD'de isteyen kullanıcılara ticari amaçla deneme maksatlı paket programlar verilir. Deneme süresi sonunda paket programları beğenenler programı satın alacak, beğenmeyenler almayacaktır.Bu paket programı satın almayanların bilgisayarları kilitlenip dosyaları silinmeye ve arızalanmaya başlamıştır. Akbulut, ... *Bilişim Suçları,* s.59.

[286] (CIH) Çernobil virüsü adı verilen virüs her ayın 26'sında aktif hale geçip sistemlere zarar vermekteydi. Bu virüs virüsü yazan tarafından bir bilişim konferansında faydalı yazılım olduğu ifade edilerek konferansa katılanlara dağıtılmıştır. Bu virüs kısa sürede ABD, Rusya, İngiltere gibi ülkeler başta olmak üzere dünyanın birçok ülkesine yayılmıştır. 26.04.2009 tarihinden sonra da ülkemizde de etkili olmuştur. Çekiç, s.75; Dülger, *Bilişim Suçları,* s.75; Alaca, s.66; Yıldız, s.75; Kızıltan, s.26.

[287] Henkoğlu, s.183; Alaca, s.68; Ergüç, s.23; Dilek, s.33.

yönelik olarak hazırlanmış ve çalıştığı kurumdan veya sanki gerçek sahibinden geliyormuş gibi görünen, müşteri bilgilerinin güncellenmesi, kullanıcı adı ve şifresinin süre aşımına uğradığı, şifrelerin değiştirilmesi gerektiği, yarışma olduğu, ödül veya hediye kazandığı kişisel bilgilerini vermesi gerektiği, konulu sahte (fake mail) ileti yem olarak gönderilir.[288]

*Sahte İleti (Fake Mail)'*ye aldanıp cevap verenler ve/veya işlem yapanlar bankanın internet sitesini taklit eden siteye yönlendirilir. Bu sayfalarda kullanıcıdan elde edilmek istenen bilgilerin doldurulmasını gerektiren formlar vardır, kullanıcı bu formları banka için doldurduğunu düşünerek doldurunca kişisel bilgileri (şifreler, kullanıcı adları vs.) ve finansal hesap erişim bilgilerini (online bankacılık ve kredi kartı numaraları, güvenlik kodları) yazılımı hazırlayanların eline geçmiş olur. Failler bu bilgilerle bilgisayar kullanıcısının banka hesabına girerek her türlü bankacılık işlemlerini yapma imkânına kavuşurlar.[289] Phishing metodunda yüksek miktarlarda kolay ve haksız para kazanma ihtimali olduğu için dünya ile birlikte Türkiye'de de gün geçtikçe yaygınlaşmaktadır.[290]

1.6.3.16. Rootkit Tekniği

Rootkit tekniği; genellikle bilişim sistemlerine yerleştirilmiş tuş kaydedici (Keylogger) ve ekran kaydedici (Screenlogger) gibi bilgi çalmaya yönelik yazılımları

---

[288] Kurt, s.76.

[289] Ergüç, s.23; Dilek, s.33.

[290] Örneğin; ülkemizde Merkez Bankası logosu da kullanılarak, "*Merkez Bankası Genel Güncelleme Formu*" başlığıyla gönderilen sahte e-posta mesajlarının MB ile hiçbir ilgisi olmadığını açıklandı. Açıklamada, "*e-posta yoluyla başka web adreslerine yönlendirilen ve kişisel bilgilerin girilmesinin istendiği formların asla doldurulmaması gerektiği Merkez Bankasının e-posta yoluyla işlem yaptırmak ya da bilgi toplamak gibi uygulamasının olmadığı*" da hatırlatıldı. www.milliyet.com.tr. (Çevrimiçi), (Erişim, 8.2.2005).

Başka bir olay; Cihan Haber Ajansı, MB adına sahte olarak gönderilen mesajı MB yetkililerine sordu. "*Yetkililer, konuyla ilgili vatandaşlardan da telefonlar geldiğini belirterek, bizim vatandaşlara böyle bir çağrımız olmadı. Eğer olsa bunu resmi bir açıklamayla yaparız. Zaten mesajlardaki gibi makinenin polis çağırması teknolojik olarak mümkün değil*" açıklaması yaptı. İşte O sahte mesaj; "*T.C. Merkez Bankası'ndan bir uyarı.. Dağarcığınızda bulunsun... Eğer bir gün ATM Makinelerinden bir soyguncu tarafından para çekmeye zorlanırsanız PIN kodunuzu ters girmeniz halinde (Örn. 1234 yerine 4321 gibi). Makine parayı veriyor ancak bu arada polis de çağırıyor. Bu konuyu çok nadir kişi bildiği için, mümkün olduğunca çok kişiye bildirelim. T.C. MERKEZ BANKASI*". www.sabah.com.tr. (Çevrimiçi), (Erişim, 14.01.2009). Ayrıca; "2005 yılında İstanbul'da phishing yöntemi ile banka müşterilerine ait bilgileri elde ederek dolandırıcılık yapan, biri kadın dört kişi yakalanmıştır." Turhan, s.57.

gizlemek amacıyla kullanılır. Bu yazılımlar Linux ve Unix işletim sistemlerinde etkilidirler. Bu işletim sistemlerinde en yetkili lokal kullanıcı "root" kullanıcısıdır. Bu yazılım en yetkili lokal kullanıcıya erişip zararlı yazılımların tespitine mani olmaya çalıştığı için bu yazılıma "rootkit" adı verilmiştir.[291]

1.6.3.17. Salam Tekniği (Salami Technique)

Bu teknik çok fazla kaynaktan (banka hesabından), maddi değeri çok az, fark edilemeyecek kadar küçük değerlerin istenen kaynağa (belli bir hesaba) transferi ile hukuka aykırı menfaat elde etme yöntemidir.[292] Tanımdan da anlaşılabileceği gibi salam tekniği genellikle banka veya finans kurumlarına karşı ya da banka veya finans kurumları aracılığıyla işlenen bir bilişim suçu metodudur.[293]

Salam tekniği, çok sayıda banka hesabı, ücret veya maaş ödemelerindeki fark edilemeyecek kadar küçük meblağların (kuruş küsuratının) belli bir hesaba transferi ile hukuka aykırı yarar sağlama yöntemidir.[294] Transfer edilen meblağ çok küçük olduğundan (birkaç kuruş) hesabından para transfer edilen hesap sahipleri veya banka yöneticileri, yetkisiz hareketleri fark edemezler.[295]

Transfer işlemi bilişim suçlusu tarafından direkt olarak hesaba girilerek yapılabileceği gibi, bankaların mudilerine ödeme yapacağı zaman belirli bir küsurat miktarının yukarı veya aşağı yuvarlanması sonucu oluşan değerin özel açtığı

---

[291] Henkoğlu, s.184.

[292] Kızıltan, s.25; Alaca, s.61.

[293] Yaycı, s.31; Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.75.

[294] Dilek, s.31.

[295] Örneğin; "ABD'de bir banka çalışanının, bankanın tuttuğu mevduat hesaplarının dört ayda bir yapılan faiz ödemelerinden kendi hesabına küçük miktarda meblağlar aktarması örnek olarak gösterilebilir. Bankanın hesap sistemi bir yazılımla, bir doların 0.0075 kadar üstünde olan her rakamı bir üst sente yuvarlamakta ve bu fark hesap sahibine ödenmektedir. Bu rakamın altında olan rakamlar ise aşağı yuvarlanmakta ve bankanın hesabına eklenmektedir. Banka memuru, sistemin yaptığı işlemi bir yazılımla değiştirip, aşağı yuvarlanarak bankanın hesabına gitmesi gereken meblağın kendi açtığı özel bir hesaba gitmesini sağlamıştır. Banka memurunun bu fiili 3 yıl boyunca fark edilmediğinden, fail milyonlarca dolar hukuka aykırı yarar sağlamıştır." Mungo P. - Clough B. s.79'dan aktaran Dülger, *Bilişim Suçları,* s.71;

Başka bir örnek; "ABD'de bir banka programcısı, faiz hesaplarının müşteriler tarafından kontrol edilmeyeceğini düşünerek geliştirdiği özel bir program aracılığıyla tutarı 50 doları geçen her faiz miktarından 1 doları kendi hesabını aktararak önemli miktarda menfaat sağlamıştır." Akbulut, ...*Bilişim Suçları,* s.53.

hesabına transferi yönünde sisteme verilecek bir talimatla da yapılabilmektedir.[296] Çok değersiz gibi gözüken bu küçük miktarlar yapılan milyonlarca işlem sonunda çok büyük rakamlara ulaşmaktadır.[297] Bu tekniğin gerçekleştirilmesi için çoğunlukla Truva Atı yazılımının çeşitleri veya benzer çalışma yöntemine sahip yazılımlar kullanılmaktadır.[298] Bu yöntem daha çok sisteme erişim yetkisi bulunan kurum personelinin yetkisiz müdahaleleriyle ortaya çıkmaktadır.

1.6.3.18. Sistemin Kırılıp İçine Girilmesi (Hacking)

Bu suç türünde hedef bilişim sistemine girmek isteyen kişiler amaçlarına sistemlerin (açık kapılarını bularak) şifrelerini kırıp, koruma duvarlarını (firewall) aşmak yoluyla ulaşırlar.[299]

Önceleri bilişim sistemlerine iyi niyetle girerek sistemin açıklarını bularak düzeltilmesini isteyen kişilere "hacker" adı verilirken, sisteme girme işlemine "hacking" denilmekteydi. Ayrıca ilk başlarda kötü niyetli olarak bilişim sistemine girme veya zarar vermeye "crack" eylemi ve eylemi yapanlara ise "cracker" adı veriliyordu. Ancak zamanla bu detayı bilmeyen kamuoyunda crack ve hacking eylemi ile cracker ve hacker kavramları özdeşleşti. Sisteme girme niyetine bakılmaksızın (kötü niyetle girme anlamında) hacking ve hacker kavramları kullanılmaya başlandı.[300] Hacker teriminin karşılığı olarak Türkçede "bilişim korsanı" terimi kullanılmaya başlandı.[301] Sistem güvenliğinin kırılıp sisteme girilmesi fiilinin diğer bilişim suçlarından en önemli farkı genellikle sisteme giriş sırasında yardımcı yazılımlar kullanılmaması ve fiilin bilişim korsanı (hacker) veya korsanları tarafından gerçekleştirilmesidir.[302] Bazı hallerde güvenlik kodlarının

---

[296] Alaca, s.61.

[297] Yazıcıoğlu, *Bilgisayar Suçları,* s.155.

[298] Kurt, s.67; Çekiç, s.69.

[299] Dülger, *Bilişim Suçları*, s.71; Yaycı, s.31; Alaca, s.61.

[300] Akbulut, ...*Bilişim Suçları,* s.54.

[301] Yaycı, s.32.

[302] Redhack korsan grubu, İçişleri Bakanlığı Sitesi'ni 20.04.2012 tarihinde "hack"ledikten sonra siteye Bakan aleyhinde sözler yerleştirdi. (Vatan Gazetesi birinci sayfa, 21.04.2012).

çözülmesi için olasılık ve kombinasyon hesaplarını hızla yapan yazılımlar kullanılsa da sistem içinde gezme ve verileri ele geçirme eylemleri hacker'lar tarafından yapılmaktadır.[303]

1.6.3.19. Sistem Kaynaklarını Tüketme (DDOS)

Hizmeti Engelleme (DDOS) adı da verilen bu yöntemde; hedef olarak seçilen bilgisayarın ağ trafiğine bir sunucunun baş edemeyeceği kadar çok sayıda işlem talep edilmek veya e-posta göndermek suretiyle, hedef bilgisayarın dosya akışı ve web hizmetleri engellenir.[304] Başka bir ifade ile hedef bilgisayarın kaynağının tüketilmesi, kaynağı kullanamaması söz konusu olmaktadır. Bazı saldırılar hedef sistemi yavaşlatmak bazıları ise hedef sistemi çökertmek için planlanırlar. Bu saldırıları düzenleyenler kimliklerinin ortaya çıkmaması için "zombi" adı verilen bilgisayarlar üzerinden bu saldırıları gerçekleştirirler.[305]

Sistem kaynaklarını tüketmeye bir müşterinin bir otelde her seferinde sahte isim ve bilgilerle tekrar tekrar yer ayırtarak otel odalarının başkalarınca kullanılmasına mani olması örnek gösterilebilir.[306]

1.6.3.20. Süper Darbe (Super Zapping)

Süper darbe (Super Zapping), bilgisayar sistemlerinin çeşitli nedenlerle çalışamaz duruma gelmesi, kilitlenmesi halinde kısa bir süre içerisinde sistemin yeniden çalışmasını sağlamak üzere güvenlik kontrollerini aşıp sistemde değişiklik yapılabilmesi için geliştirilmiş bir programdır.[307]

---

[303] Dülger, *Bilişim Suçları,* s.72; Alaca, s.62.

[304] Pallı, s.67; Henkoğlu, s.182.

[305] Dilek, s.47.

[306] Örneğin; Türkiye'deki kamu kurumlarının internet sitelerine siber saldırı düzenleyeceğini duyuran Anonymous bünyesinde hareket eden hackerlar, 27.04.2012 günü saat 20.00 sıralarında Adalet, İçişleri ve Dışişleri bakanlıklarıyla Emniyet Genel Müdürlüğü bünyesindeki web sitelerine "*DDOS*" adı verilen internet erişimini engellemek için harekete geçti. Bir süre önce TİB bünyesinde siber tehditlere karşı kurulan Teknik İşletme Daire Başkanlığı siber savunmada aktif rol üstlendi. Başta internet servis sağlayıcıları olmak üzere tüm güvenlik birimleri ve bakanlıklarla gece yarısına kadar siber güvenlik için başarılı bir koordinasyon sağlandığını kaydeden TİB Teknik İşletme Daire Başkanı Dr. Barış Yaslan, siber saldırının devlete ait yaklaşık 20 web sitesine karşı yapıldığını söyleyerek, TÜBİTAK'ın da desteğiyle saldırının etkisiz kaldığını belirtti." www.star.com.tr (çevrimiçi), (Erişim; 28.04.2012).

[307] Turhan, s.52; Kurt, s.66; Yazıcıoğlu, *Bilgisayar Suçları,* s.156.

Süper darbe yazılımları, kilitlenen sisteme müdahale edebilmek amacıyla IBM-PC uyumlu bilgisayarlarda programın disketten diskete kopyalanmasını önleyen "kopya koruma" programlarını atlatan bir yazılım olarak ortaya çıkmıştır.[308] Bilişim sistemi programları belirli bir kullanıcı yetkisi ile çalışmaktadır. Ancak normal kullanıcı yetkisi ile çalıştırılabilen programlarla sistemdeki her veriye müdahale edilemez. Sistemdeki arızalara normal kullanıcı tarafından müdahale edilemeyince bu hataları gidermek için zaman zaman süper yetkili olarak çalışan programlara ihtiyaç duyulmaktadır.[309] Bu nedenle "Super Zap" adı verilen programlar yardımıyla bilişim sistemi "güvenli mod"da çalıştırılarak hatalara müdahale edilir.[310] Bilişim sisteminin kilitlenme hatası bu yöntemle düzeltilirken, kötü niyetli kimseler de bu yöntemle sistem üzerinde istedikleri değişiklikleri yapılabilmektedir.[311]

1.6.3.21. Tarama (Scanning)

Tarama, sıralı bir dizinin her seferinde, diziden bir numara artırılacak şekilde değişen verilerle bilişim sistemlerine girilmeye çalışılmak suretiyle sistemin olumlu cevap verdiği durumların tespitini yapan teknik bir işlemdir. Tarama programları bir IP numarasından başlayarak sırasıyla arama yapar, eğer aranan numara bir bilişim sistemine bağlı ise o numaraya bağlantı sinyali gönderir. İşlemler çok kısa sürelerde her seferinde bir numara artırılarak tekrar edilir. Bu yöntemle belirli bir aralıkta bulunan telefon numaralarına bağlı bilişim sistemleri tespit edilmiş olur.[312]

Tarama işlemi ile bilişim sistemlerinin telefon numaraları tespit edilebildiği gibi, numarası belli olan ancak bir şifre ile girişin engellendiği sistemlerin geçerli

---

[308] Alaca, s.60.

[309] "*1996 yılında New York'un başlıca servis sağlayıcısı Panix ve birkaç gün sonrada New York Times gazetesi hackerlar'ca süper darbe yöntemiyle erişime engellenmiştir."* PALLI, s.67.

[310] Çekiç, s.60.

[311] "Programın bu yönünü fark eden Bir Amerikan bankası veri-işlem görevlisi, sistemde meydana gelen bir hatayı düzeltmek için kullandığı süper zap programını kullanarak veri dosyalarında iz bırakmadan 128.000 doları hesabına transfer etmiştir. Olay bir banka müşterisinin hesabındaki azalmayı fark etmesi sonucunda ortaya çıkmıştır." Aydın, s.49; Pallı, s.55; Ergün, *Siber Suçların Cezalandırılması ...,* s.22.

[312] Alaca, s.59.

giriş şifresi ile internete bağlı sistemlerin IP numarası da tespit edilebilir.[313] Tarama işlemi deneme yanılma yöntemi ile yapıldığından milyarlarca ihtimali çok kısa sürelerde deneyebilmek için tarama programlarına ihtiyaç vardır. İnternetten kolaylıkla ulaşılabilen tarama programları sistemde tespit edilen açıkları kapatmak amacıyla kullanılabileceği gibi, bu açıklar kullanılarak sisteme girmek amacıyla da kullanılabilir.[314]

1.6.3.22. Tavşanlar (Rabbits)

Tavşanlar (Rabbits) olarak isimlendirilen zararlı yazılımlar çok kullanıcılı ve çok görevli sistemlerde bilişim sistemine girdikten sonra çok hızlı (tavşanlar gibi üreyerek) sürekli ve gereksiz işler yapması için komut vererek ağ trafiğini bozarak ve sistem kaynaklarını azaltarak yok etme işlevini görürler.[315]

Tavşanlar virüslerden farklı olarak kullanıcı veri kütüklerinin son kısımlarına eklenirler ve başka program veya verilere bulaşmazlar. Tavşanların aktifleşebilmesi için bulaştığı dosyanın çalıştırılmasına veya açılmasına gerek yoktur. Kendi kendilerine aktifleşen tavşanlar bulundukları bellek veya diski kendi kopyaları ya da kendi ürettikleri bilgilerle doldurarak sistemin bilgi işlem gücünü yok ederler.[316]

1.6.3.23. Web Sayfası Hırsızlığı ve Yönlendirmesi

Web sayfası hırsızlığı ve web sayfası yönlendirme yöntemine son yıllarda daha sık rastlanmaktadır. Web sayfası hırsızlığı yönteminde; kendisine web sitesi almak isteyen ve müracaatını yapmış kişi veya kurumlardan daha hızlı davranarak fail tarafından web siteleri satın alınmakta ve müracaatı yapan kişi veya kurumlara

---

[313] Kurt, s.65.

[314] Çekiç, s.68.

[315] Akbulut, ...*Bilişim Suçları,* s.58; Henkoğlu, s.184; Çekiç, s.76; Kurt, s.75; Ergün, *Siber Suçların Cezalandırılması ...,* s.24.

[316] 19 Şubat 1988 de İngiltere'de bir fail Queen Marry Üniversitesi bilgisayarlarına ulaşıp bilgisayarlara gereksiz işlemler yaptırarak sistemi işlemez hale getirmiştir. Çekiç, s.76; Henkoğlu, s.184. Başka bir olay; büyük bir şirkette işten atılan bir programcı bu duruma kızdığı için intikam amacıyla eskiden çalıştığı şirketin bilgisayarına giderken, 400 byte'lık yer kaplayan ve tek işlevi kendisinin 24 saat içinde tam bir kopyasını yapmak olan "Sarmaşık" adlı bir Tavşan programı yükler. Bu program 24 saat sonra kendini kopyalayınca 800 byte'lık, 48 saat sonra 1.600 byte'lık bir alan kaplar. Her 24 saatte ikiye katlanarak kopyalama işlemi yapıldığı için iki hafta sonunda bilgisayarda 16.384 "sarmaşık" olmuş ve bilgisayarda bazı hatalar olmaya başlamıştır. 20 gün sonra ise bilgisayarda "yarım milyondan fazla" sarmaşık programı olduğu için bilgisayar hiçbir iş yapamaz hale gelmiş ve sistem çökmüştür. Ergün, *Siber Suçların Cezalandırılması ...,* s.24.

yüksek bedellerle satılmaktadır. Web sayfası yönlendirme yöntemi ise, girilmek istenen sitenin IP adresinin değiştirilerek kullanıcıların istediklerinden başka sitelere girmesinin sağlanmasıdır.[317]

Web sayfası hırsızlığı; İnternet Servis Sağlayıcılarının (ISS), kendilerine yapılan internet müracaatına ait bilgileri, kötü niyetli üçüncü kişilere sızdırması veya İnternet Servis Sağlayıcısının sistemlerine, bilgisayar korsanlarının girerek bilgilere ulaşması şeklinde icra edilebilir.[318]

Kanaatimce, tam olarak hırsızlık sayılmasa da meşhur insanların (siyasetçi, sanatçı, futbolcu vb.) adlarına önceden web sitesi satın alınması, bu kişiler web sitesi açmak istediklerinde de bu sitelerin satılmak istenmesi de bu kapsamda değerlendirilebilecek başka bir eylemdir.

Web sayfası yönlendirmeye ise şu örneği verebiliriz. Çankaya Üniversitesinin web sayfasına ulaşmak için alan adı olan www.cankaya.edu.tr adresi web tarayıcısına girilmelidir. www.cankaya.edu.tr alan adı Türkiye'de "tr" uzantılı alan adı vermeye yetkili kuruluşlardan olan ODTÜ tarafından Çankaya Üniversitesi'ne tahsis edilmiştir.[319] Kullanıcıların Çankaya Üniversitesi web sitesine erişmek için üniversitenin IP adresini bilmesine gerek yoktur, tarayıcıya www.cankaya.edu.tr yazmaları yeterlidir. Ancak bilişim korsanları (hacker'lar) tarafından Çankaya Üniversitesinin DNS kaydının sisteme sızarak değiştirilmesi halinde www.cankaya.edu.tr yazsalar da başka siteye yönlendirilirler.

Başka bir web sayfası yönlendirme tekniği ise *typing error hijacking* (*yanlış yazanları kaçırma*) olarak isimlendirilen bir tekniktir. Bu teknikte bilişim korsanları web sayfası adı yazılırken yapılması muhtemel yanlışları dikkate alarak, kullanıcıları kendi sayfasına yönlendirirler. Örneğin ABD Başkanlık sarayının internet adresi

---

[317] Kurt, s.73; Turhan, s.56; Pallı, s.64; Çekiç, s.79; Alaca, s.70.

[318] Alman Bremen Üniversitesi Enformatik Teknoloji Merkezi'nin beş adet bilgisayarı için almak istediği internet adresi Berlin'de bir internet servis sağlayıcısında ayrılmış olmasına rağmen, başvuru sürecinde Teknoloji Merkezi'nin bilgileri kimliği belirlenemeyen kişilerce öğrenilmiş ve daha hızlı davranılarak adreslerin dört tanesi başkaları adına kaydedilmiştir. Aylin Sırımcıyan, "*Domain Hırsızları*" **CHIP Dergisi**, Mart 2000, s.258'den aktaran Çekiç, s.90; Alaca, s.70.

[319] "*.tr ağ bilgi sistemi – TRABİS*" faaliyete geçtiğinde ODTÜ, ULAKBİM ve TTnet'in bu görevi sona erecektir.

www.whitehouse.gov olmasına rağmen birçok kullanıcı eksik bilgi veya hata sonucu www.whitehouse.com adresinden bu siteye erişmeye çalışmaktadır. Bilişim korsanları bu hatayı değerlendirerek, www.whitehouse.com adresini alan adı olarak kaydettirmiş ve hatalı adres yazanları kendi sitesine yönlendirmiştir.[320]

1.6.3.24. Yerine Geçme (Masquerading)

Ağa bağlı olan bilgisayarların ağa erişim olanakları çeşitli sınıflara ayrılmıştır. Bazı bilgisayarlara daha geniş ulaşım imkânı tanınırken diğer bazı bilgisayarlar için bu olanak sınırlandırılabilir. Bu gibi durumlarda, herkesin ulaşım hakkı/yetkisi, erişim kodu, parola veya belirlenmiş herhangi bir ayırıcı unsurla belirlenir. Bu unsurların tespit edilerek erişim hakkı hiç olmayan ya da sınırlı olan şahısların yerine erişim hakkı/yetkisi olanın adıyla sisteme girilmesi yöntemine *yerine geçme (Masquerading)* yöntemi adı verilmektedir.[321]

Yerine geçme yöntemi kullanılırken Spam, Oltalama (Phishing) ve Elektronik Adres Yanıltması (Spoofing attack) tekniklerinden de yararlanılmaktadır.[322] Örneğin, bir banka adına müşteriye sahte olarak gönderilen e-mailde, bankadaki hesaptan para çekme girişiminin olduğu, belirtilen linke tıklanması halinde dolandırıcılık departmanının sorunu çözeceği belirtilerek telkinde bulunulur. Belirtilen link bankanın gerçek web sitesi olmayıp saldırganın (hacker'ın) kontrolünde olan başka bir sitedir ve link tıklandığında banka olduğu düşüncesiyle mağdur kendi eliyle şifre ve kart bilgilerini vermektedir. Bu yöntemle işlenen bilişim suçlarını önlemek için 2005 yılında ABD'de ve 2006 yılında İngiltere'de yasal düzenlemeler yapılmıştır.[323]

---

[320] Alaca, s.71; Çekiç, s.81. (Ayrıca www.whitehouse.com adresinin "tr" uzantılı halinde 02.04.2012 tarihi itibariyle bir bayan giyim firmasının ürünlerinin reklamı yapılmaktadır.)

[321] Kurt, s.74; Turhan, s.50; Pallı, s.65; Çekiç, s.76.

[322] "*1980'li yıllarda Triludan Warrior adlı bir hacker, İngiliz Prestel şirketinin bilgisayarlarına yerine geçme yöntemini kullanarak girmiş ve sistem yöneticisi olmuştur*." Çekiç, s.76.

[323] "ABD'de çıkartılan yasa *Anti-Phishing Act of 2005*, İngiltere'de çıkartılan yasa ise *Fraud Act 2006'*dır." Pallı, s.65.

İKİNCİ BÖLÜM

TÜRK CEZA KANUNU'NDAKİ BİLİŞİM ALANINDA SUÇLAR

2.1. GENEL OLARAK

5237 Sayılı TCK'da "Bilişim Alanında Suçlar" başlığı altında yapılan düzenlemelerin genel olarak kaynağı 23.11.2001 tarihinde Macaristan'ın başkenti Budapeşte'de imzalanan "Convention On Cyber Crimes" yani "Avrupa Konseyi Siber Suç Sözleşmesi" oluşturmaktadır.[324] TCK'da yapılan bu düzenlemelerin Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS) hükümlerini genel olarak karşıladığını ifade edebiliriz.

Ceza Yasamızda "Bilişim Alanında Suçlar" başlığı altında yer alan söz konusu düzenlemeleri, doğrudan (dar anlamda – gerçek anlamda) bilişim suçları ve dolayısıyla (geniş anlamda) bilişim suçları olarak ikiye ayırmak mümkündür.[325]

Bu bağlamda **Doğrudan bilişim suçları**, *bilgisayar ve bilişim ağları ortaya çıkmadan önce işlenmeyen/işlenemeyen ve klasik yöntemlerle işlenemediğinden ceza yasalarıyla da yaptırıma bağlanmamış suç türleri*dir. Bu tür dar anlamdaki suçlara; bilişim sistemlerine hukuka aykırı olarak yetkisiz ve izinsiz erişme, sistemi engelleme, bozma, verileri değiştirme, yok etme veya bilişim ağ ya da sistemlerini doğrudan hedef alan fiilleri sayabiliriz.

Dolayısıyla (geniş anlamda) bilişim suçları ise, *klasik suç işleme yöntemlerinin bilişim sistemi unsurlarının aracı olarak kullanılarak işlenmesiyle oluşan, bilişim bağlantılı suç türleri*dir. Örneğin bilişim sistemleri aracılığıyla hırsızlık (m.142/2-e) veya dolandırıcılık (m.158/1-f) fiilleri bilişim sistemlerinin doğrudan amaç olmadığı, hukuka aykırı menfaat elde etmek için bilişim sistemi

[324] Demircan, s.8.

[325] Aynı yönde görüş; Ergün, *Siber Suçların Cezalandırılması ...*, s.27-43.

unsurlarının aracı olarak kullanıldığı klasik suçlardır. TCK'da bilişim sistemi unsurları aracı olarak kullanılabilecek dolayısıyla (geniş anlamda) bilişim suçları; Eğitim ve Öğretimin Engellenmesi (m. 112), Kamu Kurumu veya Kamu Kurumu Niteliğindeki Meslek Kuruluşlarının Faaliyetinin Engellenmesi (m.113), Hakaret (m.125), Haberleşmenin Gizliliğinin İhlali (m.132), Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (m.133), Özel Hayatın Gizliliğini İhlal (m.134), Kişisel Verilerin Kaydedilmesi (m.135), Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme (m.136), Verileri Yok Etmeme (m.138), Halk Arasında Korku ve Panik Yaratmak Amacıyla Tehdit (m.213), Suç İşlemeye Tahrik (m.214), Suçu ve Suçluyu Övme (m.215), Halkı Kin ve Düşmanlığa Tahrik veya Aşağılama (m.216), Kanunlara Uymamaya Tahrik (m.217), Müstehcenlik (m.226) ve Kumar Oynanması İçin Yer ve İmkân Sağlama (m.228) gibi suçlardır.

Bilişim suçlarını, doktrin ve uygulamada da; gerçek bilişim suçları ve bilişim bağlantılı suçlar olmak üzere ikili bir tasnife tutanlar vardır.[326] Türk Ceza Kanunu'nda da genel olarak bu sınıflandırma kabul edilmiş ve bu yönde düzenlemeler yapılmıştır.[327] Bu bağlamda Türk Ceza Kanunu'ndaki 243. ve 244. maddelerin suç fiilinde bilişim sistemlerinin amaç olarak kullanılması halindeki "gerçek bilişim suçlarını" yaptırıma bağladığını, diğer düzenlemelerin ise bilişim sistemlerinin başka bir suç için araç olarak kullanıldığı ihlalleri, dolayısıyla/geniş anlamda bilişim suçlarını, yaptırıma bağladığını söyleyebiliriz. Bu çalışmamda incelediğim 245. maddedeki "banka veya kredi kartlarının kötüye kullanılması" suçu da bilişim sistemlerinin başka suçlar için aracı olarak kullanıldığı suç türüdür. Ancak Ceza Yasamızın İkinci Kitap, Üçüncü Kısım, "Bilişim Alanında Suçlar" başlığı altındaki Onuncu Bölümde banka veya kredi kartlarının kötüye kullanılması fiilleri konusunda da düzenleme yapıldığından, "banka veya kredi kartlarının kötüye kullanılması" fiilleri dar/gerçek anlamda bilişim suçu olmamasına ve koruma altına aldığı hukuki yararının da 243 ve 244. maddelerden farklı olmasına rağmen yasadaki düzenleme nedeniyle 245. maddeyi de çalışmamın kapsamına aldım.

---

[326] (YCGK E.2009/11-193 - K.2009/268, 17.11.2009), (Kaynak; Kazancı İçtihat Programı).

[327] "*Bilişim suçları, öğretide ve uygulamada öncelikle; a) Doğrudan bilişim suçu (gerçek bilişim suçları) b)Dolayısıyla bilişim suçu (bilişim bağlantılı suçlar) biçiminde tasnife tabi tutulmuştur. Türk Ceza Kanununda da bu sistem kabul edilmiştir.*" (11. CD. E.2009/1616, K.2009/11328, 07.10. 2009), (Kaynak; Kazancı İçtihat Programı).

Birleşmiş Milletler teşkilatının, düzenlemiş olduğu 10. Kongre'de de bilişim suçları yukarıda ifade ettiğim şekilde ikili bir tasnife tabi tutulmuştur. Bu sınıflandırmalar; bilgisayar sisteminin güvenliğini veya veri işlemini hedef alan eylemleri tanımlayan "dar anlamda bilişim suçları" ve bilgisayar sistemi ve ağı aracılığıyla veya bu sistem ve/veya ağda gerçekleştirilen hukuka aykırı eylemleri tanımlayan "*geniş anlamda bilişim suçları*" şeklindedir.[328] Çalışmamda bu bölümde "*gerçek bilişim suçları*" olarak ifade ettiğim alana yönelik olarak Türk Ceza Kanununda yapılmış olan düzenlemeleri ve bu düzenlemelerin Yargıtay uygulamalarına yansımalarını inceleyeceğim.

2.2. BİLİŞİM SİSTEMİNE GİRME VE ORADA KALMA SUÇU (m. 243)

2.2.1. Genel Olarak

243. maddedeki düzenlemeyle bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme ve orada kalma fiili suç haline getirilmiştir. Bu maddede yapılan düzenleme ile ETCK m.525a/1 de sadece "veri veya diğer herhangi bir unsuru ele geçirmeyi" yaptırıma bağlayan; veriler ele geçirilmeksizin, yetkisiz ve hukuka aykırı olarak sisteme girmeyi cezasız bırakan düzenlemeye yöneltilen eleştiriler giderilmek istenmiştir.[329] Bu düzenlemeyle hukuka aykırı olarak bilişim sistemine girme fiilleri hukuk sistemimizde ilk defa ceza yaptırımına bağlanmıştır.[330] 243. maddedeki düzenlemeyle AKSSS'nin "Kanunsuz Erişim" başlıklı 2. maddesinde[331] öngörülen yükümlülük karşılanmaya çalışılmıştır.[332] Ancak birinci

---

[328] Yılmaz Yazıcıoğlu, *Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı,* 2002, s.460.

[329] Yaycı, s.70; Murat Volkan Dülger, *"Bilişim Suçları ve Yeni Türk Ceza Kanunu",* **Kazancı Hukuk İşletme ve Maliye Bilimleri Dergisi**, S.5, s.115; Yaşar-Gökcan-Artuç, s.6738.

[330] Hakan Karakehya, *Türk Ceza Kanununda Bilişim Sistemine Girme Suçu,* **Türkiye Barolar Birliği Dergisi**, Ankara, S.81, 2009, s.6; Ali Parlar, (Ocak 2011), *Türk Ceza Hukukunda Bilişim Suçları,* 1. Baskı, Ankara, Bilge Basım Yayınevi, s.15.

[331] AKSSS m.2; "*Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı, gerekli önlemleri almalıdır*."

[332] Kurt, s.147; Aslı Bayındır, *Türk Ceza Hukukunda Düzenlenen Bilişim Suçları,* **Suç ve Ceza Dergisi**, İstanbul, S.2., Ekim 2010, s.60; Parlar, s.15; Yaycı, s.71; Demircan, s.83; Dülger, *Bilişim Suçları*, s.213; R. Yılmaz Yazıcıoğlu, *"Bilişim Suçları Konusunda 2001*

fıkrada "veya" bağlacı yerine "ve" bağlacının kullanılması nedeniyle sisteme girmenin yanında sistemde kalmanın da aranıyor olması nedeniyle AKSSS'nin "Kanunsuz Erişim" başlıklı 2. maddesindeki düzenlemenin karşılanmadığını ileri sürenlerde vardır.[333] Bu görüşün tamamen haksız olduğunu söylemek mümkün değildir. Aslında bilişim sistemine girmek, aynı zamanda farklı sürelerde de olsa da sistemde kalmayı da gerektirdiğinden "ve orada kalmaya devam eden" ibaresine gerek yoktu.[334] Ancak maddenin son haliyle AKSSS'nin "Kanunsuz Erişim" başlıklı 2. maddesindeki düzenlemeyi hiç karşılamadığını da söylemek mümkün olmaz.

243. maddenin birinci fıkrasında "*bir bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak girme ve orada kalma*" fiili yaptırıma bağlanırken; ikinci fıkrada "*bedeli karşılığında yararlanılabilen*" sistemlere hukuka aykırı girme bir indirim nedeni olarak düzenlenmiş; üçüncü fıkrada ise "*sistemin içerdiği verilerin yok olması veya değişmesi*" ağırlaştırıcı nitelikli hal olarak düzenlenip bu hale daha fazla ceza yaptırımı öngörülmüştür.

Karşılaştırmalı hukukta genellikle verilerin ele geçirilmesi suçuyla birlikte bu suç tipine de yer verilmektedir. Örneğin İngiltere, ABD, Yunanistan, Kanada ve Finlandiya gibi ülkelerle,[335] "Fransa (CK m.323/1), Almanya (CK m.202/a), Danimarka (CK m.193), Norveç (CK m.142/2), İtalya (CK m.616/2, 617 quarter, 617 quinquies), Lüksemburg (CK m.309) gibi ülkeler bu yönde düzenlemeler yapmışlardır."[336]

2.2.2. Korunan Hukuki Değer

Türk doktrininde bu düzenlemenin birden fazla hukuki değeri koruduğu, bu nedenle karma nitelik taşıdığı yönündeki görüş ağırlık kazanmıştır. Ancak korunan

---

Türk Ceza Kanunu Tasarısının Değerlendirilmesi", **Hukuk ve Adalet Eleştirel Hukuk Dergisi**, Y:1, S.1, Ocak-Mart 2004, s.177; Taşdemir, s.154.

[333] İlker Tepe, "Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları*"*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Antalya, 2009, s.277; Taşkın, *Bilişim Suçları*, s.21; Karagülmez, s.169.

[334] Soyaslan, *B.A. Suçlar,* s.1566; Mehmet Emin Artuk, Ahmet Gökçen, A. Caner Yenidünya, *Ceza Hukuku Özel Hükümler,* 10.B., Ankara, Turhan Kitapevi, 2010, s.698.

[335] Taşkın, *Bilişim Suçları*, s.21-22.

[336] Dülger, *Bilişim Suçları, s.213;* Soyaslan, ...*Özel Hükümler,* s.608; Yaycı, s.71; Karakehya, s.7; Parlar, s.15.

hukuki değerler konusunda farklı değerlendirmeler vardır. Doktrinde ifade edilen bu değerlendirmeler şöyledir;

Özel hayatın dokunulmazlığı/gizliliği ve verilerin güvenlik içinde muhafazası; bilişim sistemine hukuka aykırı olarak erişim ve orada kalma fiiliyle Anayasa'nın 20. maddesinde ifadesini bulan "Özel Hayatın Gizliliği" güvence altına alınmıştır. Gerçektende bilişim sistemine erişen (kanunun ifadesiyle giren) ve orada kalan kişi, başkalarına ilişkin bilinmesi istenmeyen veri veya bilgilere ulaşmakla özel hayatın gizliliğini/dokunulmazlığını ve verilerin gizliliği ve güvenlik içinde muhafazası değerlerini ihlal etmektedir.[337] Bu konuda aksi yönde görüş beyan ederek verilerin ve özel hayatın gizliliğinin koruma altına alınma amacı olmadığını ifade edenlerde vardır.[338] Bu görüşteki hukukçular anılan sonuca, *"...bazı ülkelerde bu suçun oluşumu için açıkça verilerin ele geçirilmesi düzenlenmiş iken bizim kanunumuzda böyle bir düzenleme yapılmammış olmasından*" ve kişisel verilerin ele geçirilmesi ile ilgili TCK m.136'da ayrı bir düzenleme yapılmasından ulaştıklarını ifade etmektedirler. Ancak bu şekilde düşünürsek TCK'nın dokuzuncu bölümünde **"**Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenen; m.132'deki "Haberleşmenin Gizliliğini İhlâl", m.133'deki "Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması", m.134'deki "Özel Hayatın Gizliliğini İhlâl", m.135'deki "Kişisel Verilerin Kaydedilmesi" ve m.136'daki "Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme" suçlarındaki düzenlemelerin tamamının "Bilişim Alanında Suçlar" başlığı altındaki düzenlemelerle çakıştığı ve ceza yasamızda bir suç fiili ile ilgili birden fazla hüküm olduğunu kabul etmemiz gerekecektir. Kanaatimce bu görüş yerinde değildir. Çünkü 243. ve sonraki maddelerde yapılan düzenlemelerin suç fiilinde bilişim sistemlerinin amaç olarak kullanılması halindeki ihlalleri (doğrudan bilişim suçlarını) yaptırıma bağladığını, TCK'nın dokuzuncu bölümünde **"**Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında yapılan düzenlemelerin ise bir yönüyle bilişim sistemlerinin başka bir suç için araç olarak kullanıldığı ihlalleri (dolayısıyla bilişim suçlarını) yaptırıma bağladığını düşünüyorum.

---

[337] Soyaslan, *B.A. Suçlar,* s.1566; Necati Meran, *(Yeni Türk Ceza Kanununda) Sahtecilik - Malvarlığı ve Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar,* 1.B. Ankara, Seçkin Yayınevi, Eylül 2005, s.363; Parlar, s.15; Akarslan, s.41; Kızıltan, s.61-62; Yaycı, s.71.

[338] Erdoğan, s.123; Ketizmen, s.93.

Kullanıcı ve sistem sahibinin çıkarları; yetkisiz erişimler aynı zamanda, sistemlerin, resmi veya özel kurumların bilişim sistemlerinin ulaşılmazlığını aşarak sistemin iyi çalışmadığını da göstermektedir. Bu durum ise banka, devlet kurumu gibi kurumların maddi ve manevi çıkarlarını zedelediği gibi, banka veya kurumlarda çeşitli bilgileri bulunan şahısların çıkarlarına da maddi veya manevi anlamda zararlar verme ihtimalini de barındırmaktadır.[339]

Olası başka suçların işlenmesinin önlenmesi; bilişim sistemine girme, daha sonra işlenmesi olası (verileri bozma, yok etme, değiştirme, dolandırıcılık, sahtekârlık gibi) suçlar için uygun bir ortam oluşturmakta bu suç türleri için aracı olan bir suç türü de olabilmektedir.[340] Yetkisiz girişin dahi cezalandırılması, bilişim sistemleri aracı olarak kullanılarak işlenebilecek başka suç eylemlerinin hazırlık hareketlerini de önlemiş olacağından caydırıcı olabilecektir. Bu bakımdan da hukuka aykırı erişimin cezalandırılması, daha sonra işlenebilecek suçları da engelleyici bir hüviyet kazanmaktadır.[341]

Bilişim sisteminin güvenliği; de korunan hukuki yararlar arasındadır. Bu hususun 243. madde kabul edilirken TBMM Genel Kurulu'nda yapılan değişiklikten önce daha çok önem arz eden bir hukuksal değer olduğunu ifade edebiliriz.[342] Şöyle ki; TBMM Genel Kurulu'nda; "hata ile sisteme girmeyi" yaptırım dışında bırakmak amacıyla yapılan bir değişiklikle, birinci fıkrada kullanılan "veya" kelimesi yerine "ve" kelimesi kullanılmıştır. Bu değişiklik sonucu, 243. maddedeki suçun oluşması için "bilişim sistemine yetkisiz girme" fiili yetersiz kalmış "ve" kelimesi nedeniyle ayrıca ek olarak "orada kalma" fiili de aranır olmuştur. Bunun sonucu olarak ta bilişim sistemine sadece girme nedeniyle ihlal edilecek olan "bilişim sisteminin güvenliği", "orada kalma" fiili nedeniyle "öncelikle" korunan hukuki yarar olmaktan çıkmıştır. Ancak bu yeni durumun da "bilişim sisteminin güvenliğini" büsbütün korunan değerler arasından çıkardığını söylemek mümkün değildir. Başka bir

[339] Parlar, s.15; Esen, s.628; Erdoğan, s.122; . Meran, s.363.

[340] Taşdemir, s.256; Kızıltan, s.62.

[341] Aksi yönde görüş, Erdoğan, s.122.

[342] Karagülmez, s.166-167; Parlar, s.15; Bayındır, s.60; Ergün, s.88; Dülger, *Bilişim Suçları*, s.213-214; Kızıltan, s.62; Demircan, s.83-84, Artuk-Gökçen-Yenidünya, s.696.

ifadeyle "bilişim sisteminin güvenliği" de öncelikli olmasa da korunan hukuksal değerler arasındadır.[343]

Mülkiyet hakkı; 243. maddenin ilk iki fıkrasında veri veya bilgilerin ele geçirilmesi, değiştirilmesi veya yok edilmesi konusunda bir düzenleme olmadığından mülkiyet hakkının koruma altına alındığını söyleyemeyiz. Üçüncü fıkrasında ise verilerin yok olması veya değiştirilmesi hüküm altına alındığından, üçüncü fıkra uyarınca mülkiyet hakkının da korunan hukuki değer olduğunu ifade edebiliriz.[344]

Bu hususlardan başka bilişim alanında suçların "topluma karşı suçlar" başlığı arasında yer alması nedeniyle bu maddeyle toplum düzeninin de korunduğu da ifade edilmektedir. Bu görüşe katılmak mümkün değildir. Çünkü öncelikli olarak bilişim alanındaki suçların "topluma karşı suçlar" arasında değil de kişilere karşı suçlar arasında yer alması daha doğru olurdu. Çünkü bilişim alanında işlenen suçlar kişilere karşı işlenmektedir.[345] İkinci olarak ceza yasasındaki bütün düzenlemeler geniş bir açıdan bakıldığında zaten topluma karşı işlenen suç olarak değerlendirilebilecektir. Bu açıdan 243. maddede özel bir amaç yoktur. Son eleştiri ise anılan eylemin ilgililerin rızasının hukuka uygun hale getirmesidir, bu durumda fiil suç olmaktan çıkacaktır. Bu madde ile toplum düzeninin de öncelikli amaç olarak korunduğu kabul edilirse, ilgili kişinin toplum adına karar verme yetkisine sahip olduğunu kabul etmemiz gerekecektir ki, bu durumun kabul edilmesi mümkün değildir[346]

Sonuç olarak 243. maddedeki düzenlemeyle özel hayatın dokunulmazlığı/gizliliği ve verilerin güvenlik içinde muhafazası, kullanıcı ve sistem sahibinin çıkarları, olası başka suçların işlenmesinin önlenmesi, bilişim sisteminin güvenliği ve 3. fıkra ile de mülkiyet hakkının koruma altına alındığını söyleyebiliriz.

2.2.3. Suçun Konusu

Suçun konusu, üzerinde suçun meydana geldiği, yasada ifade edilen hareketin kendisine yöneldiği eşya veya şahıstır.[347] Bu bağlamda 243. maddenin birinci

---

[343] Karşı yönde görüş için bkz. Taşkın, s.23; Bayındır, s.60; Karagülmez, s.167.

[344] Kurt, s.148.

[345] Zeki Hafızoğulları, Devrim Güngör, (2007), *Türk Ceza Hukukunda Suçların Tasnifi,* **Türkiye Barolar Birliği Dergisi**, S.69, Ankara, s.39; Soyaslan, *B.A. Suçlar,* s.1563.

[346] Ketizmen, s.67.

[347] Dülger, *Bilişim Suçları*, s.217; Erdoğan, s.146; Taşkın, *Bilişim Suçları*, s.24.

fıkrasında düzenlenen suçun konusu; hukuka aykırı olarak içine girilen ve orada kalmaya devam edilen "*bilişim sisteminin soyut varlığı*", ikinci fıkrasında düzenlenen suçun konusu "*bedeli karşılığında yararlanılan bilişim sistemi*" ve üçüncü fıkrasında düzenlenen suçun konusu ise, değişen veya silinen "*bilişim sisteminin içerdiği veriler"*dir.[348]

Bu suçun konusu, yasa metninde de ifade edildiği üzere bilişim sisteminin bütünü veya bir kısmı olabilir. Suç konusunu oluşturan eşya gerçek bir kişinin evinde kullanılan kişisel bilgisayar olabileceği gibi, bir kamu kurumunda kullanılan bir bilgisayar veya bilişim sistemi de olabilecektir.[349]

2.2.4. Fail

Madde metninde, *bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ... kimse* den bahsedildiği için fail için aranan farklı bir özellik yoktur. Bu nedenle anılan suçun faili herkes olabilir.[350] Bilgisayarların ve bilişim sistemlerinin dünyada ve ülkemizde ilk kullanılmaya başlandığı dönemlerde bilişim suçları sadece belirli özelliklere sahip bazı meslek gruplarınca işlenebilecek bir suç türü (beyaz yaka suçları - white color crimes)[351] olarak, konumuz açısından ise bilişimden anlayan, bilgisayar alanında belirli bilgi seviyesine ulaşmış, temel bilişim sistemi bilgilerinden daha fazla bilgiye sahip[352] sadece hacker'ların işleyebileceği bir suç türü olarak görülüyordu. Bu nedenle 765 sayılı ETCK 525a/1 maddesine göre, verilerin ele geçirilmesi suçunun işlenebilmesi için failin temel bilgisayar bilgisinin çok üzerinde bir bilgi seviyesi bulunmalıydı. Bu bilgilere ise ancak bilişim korsanı/hacker olarak tanımlanan failler sahip olabilirdi.[353] Ancak günümüzde bilişim sistemlerine evlerde, işyerlerinde, okullarda, üniversitelerde, umuma açık

---

[348] Meran, s.364; Yaşar-Gökcan-Artuç, s.6745; Erdoğan, s.146-147.

[349] Erdoğan, s.147.

[350] Kızıltan, s.62; Turgay Şahin, *Türk Ceza Kanunu, (Açıklamalı ve İçtihatlı)*, Afyonkarahisar, Afyonkarahisar Barosu Yayını, Mart 2006, s.601.

[351] "Beyaz yaka suçları (white color crimes); bazı meslek gruplarının (mimar, mühendis vb.) mesleği dolayısıyla sahip olduğu bilgileri, sosyal statüsünü ve kendisine duyulan güveni kötüye kullanarak işlenebilecek suç türlerini ifade etmektedir." Erdoğan, s.143.

[352] Taşkın, *Bilişim Suçları*, s.23.

[353] Dülger, *Bilişim Suçları*, s.215; Aydın, s.30; Ersoy, s.167.

internet cafe'lerde, cep telefonlarında ve her alanda ulaşmanın mümkün hale gelmesi, internet üzerinden kolaylıkla bulunabilen çeşitli yardımcı yazılımlarla bu suçun işlenmesinin kolaylaşması gibi nedenlerle bu suç türü hemen herkes tarafından işlenebilecek bir suç türü olmuştur.[354] Bu nedenle 243/1. fıkrada suçun faili için "kimse" ifadesinin kullanılması yerinde olmuştur.

Tüzel kişilerin fiil ehliyetleri olmadığından, kusur ehliyetleri de yoktur, dolayısıyla bu suçun faili olamazlar. Tüzel kişi yararına işlenen suçlarda ceza sorumluluğu öncelikle tüzel kişi adına hareket eden gerçek kişiye aittir. Tüzel kişi yararına haksız menfaat temin edilmişse ceza sorumluluğunun şahsiliği gereği tüzel kişi suç faili sayılmasa da, tüzel kişi aleyhine TCK m.60'da öngörülen; faaliyet izninin iptali, suçta kullanılan vasıtaların ve/veya elde edilen kazancın müsaderesi gibi güvenlik tedbirleri uygulanacaktır.[355]

2.2.5. Mağdur

Bu suçun mağduru; suçtan zarar görme tehlikesine maruz kalan veya suçtan zarar gören hak veya menfaati ihlal edilen gerçek veya tüzel kişilerdir.[356]

Gerçek veya tüzel kişiler aynı anda da mağdur olabilirler. Hatta suçla elde edilecek maddi menfaat düşünüldüğünde gerçek kişilerle birlikte onlardan daha çok tüzel kişiler bu suçun mağduru durumunda olacaklardır. Örneğin bir bankanın bilişim sistemine girilerek müşteri bilgilerinin incelenmesinde, bankanın ticari itibarı ve sisteminin güvenliği de zedelenmektedir. Bu örnekte ticari bankanın uğradığı hak ve menfaat kaybının gerçek kişinin kaybından daha çok olduğunun söyleyebiliriz.[357]

2.2.6. Maddi Unsurlar

Suçun maddi unsuru olarak üzerinde durulması gereken hususlar, o suçun işlenmesinde başvurulan hareketler, bu hareketler sonucu ortaya çıkan netice ile hareket ve netice arasındaki illiyet bağıdır.[358]

---

[354] Çekiç, s.89.

[355] Yaycı, s.74; Çekiç, s.90; Karagülmez, s.171.

[356] Soyaslan, *B.A. Suçlar,* s.1567; Esen, *Malvarlığına Karşı Suçlar,* s.628; Ali Parlar, Muzaffer Hatipoğlu, *(Açıklamalı Yeni İçtihatlarla) 5237 Sayılı Türk Ceza Kanunu Yorumu (141-345. Md.),* Ankara, C.II, 2007, s.1695; Meran, s.364.

[357] Yaşar-Gökcan-Artuç, s.6739; Erdoğan, s.145.

[358] Doğan Soyaslan, *Ceza Hukuku Genel Hükümler,* Güncelleştirilmiş 3.B., Ankara, Yetkin Yayınevi, 2005, s.220.

2.2.6.1. Hareket

243. maddenin 1. fıkrasının eylemi; hangi yolla olursa olsun bir bilişim sisteminin bir kısmına veya tamamına erişilmesi/girilmesi ve orada bir süre kalınması hareketleridir.[359] Başka bir anlatımla; bu suçun oluşması için icrai nitelikteki girme eylemine, ihmali nitelikteki sistemde kalmaya devam etme eyleminin eklenmesi (birleşik hareket) gerekmektedir.[360]

Sisteme her girme eylemi aynı zamanda çok kısa sürelerde olsa dahi kalma eylemini de içermektedir. Dolayısıyla suç mütemadi (kesintisiz) bir suçtur, seçimlik hareketli bir suç türü değildir.[361] Madde yasalaşmadan önce Adalet Komisyonu'nda geçerli olan metin, bilişim sistemine "giren veya orada kalmaya devam eden" şeklinde idi. Yasa metni TBMM'de bu haliyle iken yasalaşsa idi "sisteme girme" veya "sistemde kalmaya devam etme" hareketleri seçimlik hareketli suçlar olacaktı.[362] Yasa maddesinin başlığı "bilişim sistemine girme" olmasına ve madde gerekçesinde "sisteme hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiillerinin" suç olarak düzenlenmiş olduğundan bahsedilmesine rağmen, TBMM'de birinci fıkradaki "*veya*" kelimesi yerine "*ve*" bağlacının yasa metninde yer alması sonucu artık ortada seçimlik hareketli bir suçtan bahsetmek mümkün değildir. Yani artık suç hareketi olarak sisteme girme yeterli olmamakta buna ek olarak sistemde kalma hareketi de aranmaktadır.[363] Bu değişiklikle sistemde kalmaya devam edilmesi bu suçun tamamlayıcı unsuru haline getirilmiştir.

TBMM'de yapılan değişikliği savunanlar olduğu gibi karşı çıkanlar da vardır. Değişikliğin yerinde olduğunu savunan hukukçular veya-ve bağlaçları değişikliği ile "sistemde kalmaya devam etmek" fiilinin suçun tamamlayıcı unsuru haline getirilmesi, kötü niyetli olmayıp da hatayla, yanlışlıkla, bilgisizlik vb. nedenler ile

---

[359] Soyaslan, *B.A.Suçlar*, s.1567; Parlar, s.16.

[360] Erdoğan, s.125; Taşkın, Bilişim Suçları, s.26; Dülger, s. 218; Soyaslan, ...*Özel Hükümler*, s.610; Artuk-Gökçen-Yenidünya, s.699; Yaşar-Gökcan-Artuç, s.6745.

[361] Soyaslan, ...*Özel Hükümler,* s.608; Parlar, s.17; Karagülmez, s.169.

[362] Genel kabulün aksine; bu suçun seçimlik hareketli bir suç olduğu, bilişim sistemine girilmesi veya sistemde kalmaya devam edilmesi fiillerinden birinin gerçekleştirilmesiyle suçun gerçekleşmiş olacağını ifade edenlerde vardır. Dülger, *Bilişim Suçları,* s.217.

[363] Parlar, s.16.

sisteme kısa süreliğine giriş yapanların, sisteme girme eylemlerini de çok katı bir düzenleme ile münhasıran suç saymama düşüncesinden kaynaklandığından isabetli olmuştur, şeklinde değerlendirmelerde bulunmuşlardır.[364]

Değişikliğin doğru olmadığını daha güçlü argümanlarla savunan hukukçular ise; *birinci olarak*, madde başlığının "Bilişim Sistemine Girme" olması, *ikinci olarak* madde gerekçesinde bir "*bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiillerinin*" anılan suçu oluşturduğundan bahsetmesi ve bu hareketlerin seçimlik hareketler olması, *üçüncü olarak* ise aslında bilişim sistemine girilmekle (değişen sürelerde) orada kalma fiili de gerçekleştiğinden "ve orada kalmaya devam eden" ibaresine gerek olmadığını ifade etmektedirler.[365]

Son olarak ise Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)'nde sözleşmeye taraf ülkeler için sisteme yasa dışı erişim/girme konusunda yasal düzenleme yapılması tavsiye edilmektedir. AKSSS'nin Maddi Ceza Hukuku başlığı altındaki 2. maddesinde "Yasadışı Erişim" konusunda yapılan düzenlemede yasadışı erişimin suç olarak düzenlenmesi tavsiye edilirken "sistemde kalma" veya "kalmaya devam etme" gibi bir husus vurgulanmamıştır.[366] 243. maddenin bu madde hükmünü yerine getirmek amacıyla düzenlendiği düşünüldüğünde yapılan bu değişikliğin tavsiye edilen düzenleme kapsamını tam olarak karşılamadığını ifade edebiliriz.[367] Bu doğrultuda düzenleme yapan çeşitli ülkelerde de "sistemde kalma" gibi bir düzenlemeye yer verilmemiştir. Tüm bu nedenlerle veya-ve bağlacı değişikliğinin uygun olmadığını söyleyebiliriz.

Bilişim sistemine girme ve orada kalma fiili herhangi bir amaçla gerçekleştirilebilir. Fail sisteme veri elde etmek, sistem güvenliğini kırmak, heyecan

---

364 Kurt, s.148; Taşkın, *Bilişim Suçları,* s.25.

365 Soyaslan, *B.A.Suçlar*, s.1566.

366 AKSSS'nin "Maddi Ceza Hukuku" başlığı altındaki 2. m. 1. fıkrası; "*Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına kasıtlı ve haksız bir şekilde erişim yapıldığında, bu fiilin kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır*" şeklindedir.

367 Yazıcıoğlu, *Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi*, s.183; B. Zakir Avşar, Gürsel Öngören, *Bilişim Hukuku,* İstanbul, Türkiye Bankalar Birliği Yayını, Yayın No:270, Haziran 2010, s.133; Erdoğan, s.120.

yaşamak, kendini ispat etmek gibi çeşitli amaçlarla girebilir. Suç failinin bilişim sistemine kendi adına veya başka şahıslar adına girmiş olmasının suçun oluşması için herhangi bir önemi yoktur. Fail her iki durumda da sorumlu olacaktır. Anılan suçun tüzel kişiler lehine işlenmesi mümkündür, böyle bir durumda fail ile birlikte tüzel kişiler de sorumlu olduğundan tüzel kişilere de emniyet tedbirleri uygulanabilecektir.[368] Ayrıca failin sorumluluğu açısından, kendi bilişim sisteminden veya başkalarına ait bilişim sistemlerinden mağdurların bilişim sistemlerine girmiş olmasının da bir önemi yoktur.[369]

Girme ve orada kalma hareketi bilişim sisteminin yazılım unsurlarının tamamına veya bir kısmına erişme anlamındadır. Bu erişme bizzat bir bilgisayarın başında cihazın açılıp sisteme girilmesi ve içindeki veri ve bilgilere ulaşılması yoluyla olabileceği gibi, bir ağ üzerinden bilişim sisteminde oturum açılması veya açık olan oturuma girilmesi yoluyla da olabilir. Girme yöntemi önemli değildir. Bilişim sistemine girilmesinde kablolu veya kablosuz ağların kullanılması veya yakın veya uzak mesafeden erişimin sağlanması arasında da fark yoktur.[370] Ancak mağdur tarafından monitörde açılmış olan bilgilerin başkaları tarafından görülerek elde edilmesi durumunda bu suç oluşmaz. Çünkü fail tarafından hukuka aykırı olarak bilişim sistemine girme eylemi gerçekleşmemiştir. Ayrıca mağdurun çalışır halde bıraktığı bilgisayarda bulunan bilgilere, failin mouse veya klavye kullanarak ulaşması eylemi 243. madde kapsamında değerlendirilecektir.[371]

Bilişim sisteminde kalmak için elbette önce sisteme erişmek/girmek gerekir. Sisteme girildikten sonra içindeki bilgiler öğrenilebileceği gibi öğrenilmeyebilir de. Suçun oluşumu için bu hususlar herhangi bir farklılık arz etmemektedir.[372]

---

[368] İsmail Malkoç, *Açıklamalı İçtihatlı 5237 Sayılı Türk Ceza Kanunu (m. 188-345),* Malkoç Kitapevi, C.II, 2007, s.1668; Soyaslan, ...*Özel Hükümler*, s.609.

[369] "*Sanığın sahibi olduğu, internet cafe'de 70 adet bilgisayarın gözetimi ve denetimi için gerekli hassasiyeti göstermemesi sebebiyle kusurlu olduğu gerekçesiyle cezalandırılmasına karar verilmiş ise de adı geçen* ***iş yerindeki İP numarası … olan bilgisayardan müştekinin e-posta adresine girilmesinden*** **(işyeri sahibi)** ***sanığın sorumluluğu"*** yoktur. (11. CD. E.2009/23397 - K.2010/6054, 14.05.2010), (Kaynak; Erdoğan, s.126).

[370] Haydar Erol, *Türk Ceza Kanunu,* Ankara, Yayım Matbaacılık ve Ticaret İşletmesi Yayını, 2003, s.2533; Meran, s.365; Yaşar-Gökcan-Artuç, s.6745.

[371] Artuk-Gökçen-Yenidünya, s.699-700.

[372] Soyaslan, *B.A.Suçlar,* s.1567; Erdoğan, s.126.

Genel olarak başka bir bilişim sistemine, ya hedef bilişim sisteminde var olan açıklardan yararlanılarak ya da hedef sistemde açıklar oluşturularak girilebilir.[373] Hedef sistemde var olan açıklardan yararlanarak sisteme; sistemin kırılıp içine girilmesi (hacking), tarama (scanning) gibi yöntemlerle girilebilir. Hedef sistemde; ağ solucanları (network worms), bukalemun (chameleon), casus yazılımlar (spyware), istem dışı alınan elektronik postalar (spam), truva atı (trojan horse) ve tavşanlar (rabbits) gibi yöntemler aracılığıyla açıklar oluşturarak ta sisteme girilebilir. Bilgisayar virüsleri (computer viruses) ve bombalar (bombs) gibi yöntemler ise sisteme girildikten sonra kullanılabilirler.

Sistemde kalma süresi ile ilgili yasada herhangi bir düzenleme yapılmaması eleştirilmektedir. "*Orada kalmaya devam eden*" ibaresi "*kalan*" kelimesine göre daha uzun, daha geniş bir zaman dilimini ifade etmektedir. 243. madde metninde sisteme "*giren ve kalan*" ibaresi yerine, sisteme "*giren ve orada kalmaya devam eden*" ifadesi kullanılmıştır. Ancak "kalan" kelimesine nazaran daha uzun bir zamanı ifade eden "kalmaya devam eden" ibaresi için bir süre öngörülmemiştir. Objektif olarak tüm olaylara uyacak bir sürenin önceden belirlenmesi de mümkün değildir. Her bilişim sisteminin kendine ait güvenlik yapısı ve özellikleri ile sisteme hukuka aykırı giriş yapan failin becerisi ve hızı farklıdır. Dolayısıyla her somut olay için sistemde kalmaya devam etme (temadi) süresinin yeterli olup olmadığı hâkim tarafından araştırılıp belirlenmelidir.[374]

2.2.6.2. Netice

Madde metninde suçun neticesi ile ilgili bir ifade yoktur. Bu durumdan suçun tamamlanmış olması için kanunen bir koşul aranmadığı sonucuna ulaşılır. Başka bir ifade ile maddeye göre suç bir bilişim sistemine hukuka aykırı bir yolla girmekle tamamlanmış olur. Zaten girme/erişme fiili ile aynı zamanda orada (değişik sürelerde olsa da) kalınmış olunmaktadır.[375] Ancak bu durumda failin başkasının bilişim sistemine hatayla, yanlışlıkla, istemeden girmesi ve başkasının bilişim sistemine girdiğini anladığı anda hemen çıkması durumunda suçun oluşmayacağı istisnai bir durum olarak gözden uzak tutulmamalıdır.

---

[373] Akıncı-Alıç-Er, s.175-176.

[374] Parlar, s.16; Karagülmez, s.170.

[375] Soyaslan, ... *Özel Hükümler*, s.609; Karagülmez, s.169-170; Parlar-Hatipoğlu, s.1696.

Söz konusu suç bu özelliği yönünden konut veya işyeri dokunulmazlığının ihlali suçuna benzemektedir. Hatayla, yanlışlıkla istemeden başkasının bilişim sistemine girme durumlarında, suçun oluşumu için başkasının bilişim sistemine girildiği anlaşılmasına rağmen, kalmaya da devam etmek gerekmektedir.[376] Bu husus dikkate alınmazsa örneğin bilgisizlik, hata veya yanılgı ile başkasının bilişim sistemine girip, hemen çıkanların da cezalandırılması gerekir ki bu durum kanunun amacı dışındadır.[377] Madde gerekçesinde suçun oluşumu için "*sisteme, ...kasten girilmiş olması*" şartı konularak bu husus vurgulanmıştır.

Bu maddede netice aranmadığından, neticesi harekete bitişik suç/[378]birleşik hareketli suç/[379]sırf hareket suçu söz konusudur.[380] Sisteme girme orada kalmayı da getirdiğinden, bu suçun tamamlanmış olması için, sistemde bulunulan verilerin ele geçirilmesi, öğrenilmiş olması, değiştirilmesi veya verilere zarar verilmesi aranmaz. Yargıtay uygulamaları da bu yöndedir.[381] Fiilin yaptırıma uğraması için bilişim sistemi veya verilerine herhangi bir zarar verilmesi aranmamaktadır. Bilişim sistemine hukuka aykırı girilmesi fiili ile verilere/bilgilere zarar verme riski/tehlikesi oluşturduğundan birinci fıkradaki suç bir tehlike suçudur.[382] Eğer suç fiili sonucu, failin kastı olmaksızın bilişim sisteminin içerdiği veriler değişmiş veya silinmişse bu durum, ağırlatıcı neden olduğundan faile 243. maddenin 3. fıkrası uygulanacaktır.

Bu suçun oluşması için bir bilişim sistemine *girme ve orada kalma* unsurları arandığından, suç kesintisiz (mütemadi) bir suç niteliğindedir. Suç temadinin

---

[376] Yaşar-Gökcan-Artuç, s.6744; Meran, s.565.

[377] Kurt, s.148; Karakehya, s.14.

[378] Taşkın, *Bilişim Suçları,* s.26; Dülger, s. 218.

[379] Soyaslan, *...Özel Hükümler*, s.610.

[380] Artuk-Gökçen-Yenidünya, s.699; Yaşar-Gökcan-Artuç, s.6745.

[381] "*Sanığın, katılanın yetkilisi olduğu tekstil şirketinin .. Bankası .., Şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında,* ***sanığın eyleminin 5237 sayılı TCK'nın 243/1. maddesinde düzenlenen suçu oluşturduğu gözetilmeden*** *yazılı şekilde 5237 s. TCK'nın 244/4, 35/2 maddeleri gereğince hüküm tesisi…*" bozma sebebi yapılmıştır. (11. CD. E.2009/18190 - K.2009/3058, 26.03.2009), (Kaynak; Yaşar-Gökcan-Artuç, 1115 sıra numaralı, dipnot, s.6744.)

[382] Kurt, s.152; Parlar-Hatipoğlu, *TCK Yorumu*, s.1696; Yaşar-Gökcan-Artuç, s.6745.

kesilmesi ile sona erecektir. Temadi; failin iradesi ile fiiline son vermesi, suçüstü yakalanması, sistemdeki bir arıza, ya da elektrik kesilmesi gibi nedenlerle sona erebilmektedir.[383]

2.2.7. Manevi Unsur

Madde metninde özel kast, özel amaç ya da saiki işaret eden bir ifade olmadığı için suç genel kastla işlenebilir. Buradaki genel kast, failin kendisine yasak olan başkasının bilişim sisteminin bir kısmına veya bütününe hukuka aykırı olduğunu bilerek ve isteyerek girmesi ve orada kalmaya devam etmesidir.[384] Failin özel bir amacının olmasının, zarar verme kastı olup olmamasının, merak, heyecan, eğlence, kendini kanıtlama, reklam, sistem güvenliğini deneme veya oyun saikiyle hareket edip etmemesinin suçun oluşumu bakımından önemi yoktur.

Genel kastla işlenen bir suç olduğundan suçun taksirle işlenmesi mümkün değildir. Maddedeki düzenlemenin bu suçları sadece kasten işlenmesi halinde yaptırıma bağlaması AKSSS'ne uygun bir düzenleme olmuştur.[385] Ancak fiil sonucunda istemeden sistemin içerdiği verilerin silinmesi ya da değişmesi hali, 3. fıkrada ağırlaştırıcı neden olarak öngörülmüştür.[386] Failin başkasının bilişim sistemine hatayla, yanlışlıkla, istemeden girmesi ve başkasının bilişim sistemine girdiğini anladığı anda hemen çıkması durumunda suçun oluşmayacağı yukarıda da ifade edilmişti.[387] Bu durumda suçun oluşumu için başkasının bilişim sistemine girildiği anlaşılmasına rağmen, kalmaya da devam etmek gerekmektedir, bu halde "sonradan oluşan kast" nedeniyle suçun manevi unsuru gerçekleşmiş olacaktır.[388]

---

[383] Ahmet Gündel, *Yeni Türk Ceza Kanunu Açıklaması (m.207-345)*, C.IV. 2009, Ankara, s.4626; Yaşar-Gökcan-Artuç, s.6744.

[384] Soyaslan, *B.A.Suçlar*, s.1569; Yaşar-Gökcan-Artuç, s.6745; Erdoğan, s.145; Esen, *Malvarlığına Karşı Suçlar,* s.629; Parlar-Hatipoğlu, *TCK Yorumu*, s.1696; Meran, s.367; Dülger, *Bilişim Suçları*, s.220; Taşkın, *Bilişim Suçları*, s.28; Kurt, s.159; Karakehya, s.15; Bayındır, s.65; Karagülmez, s.172.

[385] Erdoğan, s.145.

[386] Taşkın, *Bilişim Suçları*, s.28; Çekiç, s.94.

[387] Yaşar-Gökcan-Artuç, s.6744; Meran, s.565.

[388] Yaşar-Gökcan-Artuç, s.6745-6746.

2.2.8. Hukuka Aykırılık Unsuru

Tüm suçların temel unsuru olan "hukuka aykırılık" unsuru TCK 91/2, 109, 120, 124, 262 gibi bazı maddelerle birlikte bilişim sistemine girme ve sistemde kalma fiilini yaptırıma bağlayan 243. maddede de ayrıca vurgulanmıştır. Bu tür vurgulama ile suç tipinde hukuka aykırılığın ayrıca belirtilmesine doktrinde "hukuka özel aykırılık" denilmektedir. Bu yöntemle yasa koyucu failin suç konusu eylemlerinin tamamında hukuka aykırı şekilde hareket ettiği bilinci içerisinde bulunması gerektiğini vurgulamıştır. Dolayısıyla hâkim karar verebilmek için her somut olayda failin ayrıca bu özel aykırılığı da bilerek hareket edip etmediğini de araştırmalıdır.[389] Çeşitli ülkelerde de bilişim sistemine girme ve orada kalma suçu ile ilgili "hukuka özel aykırılık" unsurunu ifade eden kelimelerle özel vurgulama yapılmıştır. Örneğin; Belçika CK (Ceza Kanunu), (m.550/b) "*yetkisiz olarak*", Kanada CK (m.342.1) "*açık bir hakkı olmaksızın*", Şili, Otomatik Bilgi İşlem Suçları Kanunu (m.2) "*hukuka aykırı olarak*", Danimarka CK (m.263) "*hukuka aykırı*" ibareleriyle hukuka özel aykırılık vurgulanmıştır.[390]

Mağdurun rızası (m.26/2), kanun hükmünün icrası (bilişim sistemi, bilgisayar programı ve verilerine el koyma - CMK m.134, İletişimin tespiti, dinlenmesi kayda alınması CMK m.135), amirin emrini yerine getirme (m.24) gibi çeşitli hukuka uygunluk nedenlerinin varlığı halinde hukuka aykırılık kalktığından bu suç oluşmayacaktır.

Mağdurun rızası ile (sistemin test edilmesi, bakım yapma, program yükleme veya arıza giderme gibi amaçlarla) bilişim sistemine girilip, işlem bitmesine, rıza kalkmasına rağmen sistemde kalmaya devam edilmesi halinde de suç gerçekleşecektir.[391]

2.2.9. Suçu Etkileyen Nedenler

2.2.9.1. Daha Az Cezayı Gerektiren Hal

243. maddenin ikinci fıkrası ile bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etme fiillerinin "*bedeli karşılığı yararlanılabilen sistemler*"

---

[389] Demircan, s.91; Çekiç, s.93; Kurt, s.158; Bayındır, s.65.

[390] Artuk-Gökçen-Yenidünya, s.714.

[391] Aynı yönde görüş, Parlar-Hatipoğlu, *TCK Yorumu*, s.1697; Demircan, s.91; Kurt, s.156; Bayındır, s.65; Parlar, s.18. Aksi yönde görüş için bkz. Ketizmen, s.107-108; Erdoğan, s.160.

hakkında işlenmesi hali, nitelikli hal kabul edilerek, bu suç açısından cezanın yarı oranda indirileceği hükme bağlanmıştır.

Böyle bir ceza indiriminin kabul edilmesi korunan hukuksal menfaatle ilgilidir.[392] 243. maddedeki düzenlemeyle özel hayatın dokunulmazlığı/gizliliği, verilerin güvenlik içinde muhafazası, kullanıcı ve sistem sahibinin çıkarları, olası başka suçların işlenmesinin önlenmesi ve bilişim sisteminin güvenliği gibi hukuksal değerlerin korunmasının amaçlandığı yukarıda ifade edilmeye çalışılmıştı. İkinci fıkradaki düzenlemeyle, birinci fıkrayla korunan bu hukuksal değerlerin dışındaki "ekonomik menfaat" ihlalinin bir indirim nedeni yapıldığını söylemek mümkündür.[393]

Yasa koyucu bu düzenlemeyle; bilişim sistemi sahiplerinin bedelini ödeyenlere açtığı bazı veri ve bilgilere, herhangi bir bedel ödemeyenlerin ulaşması halinde oluşan ihlalin, kamuoyuna hiç açılmamış veri ve bilgilere ulaşılması halinde oluşan zarardan, daha hafif olacağı düşüncesindedir diyebiliriz. Başka bir anlatımla yasa koyucu özel hayatın mahremiyeti, verilerin korunması gibi değerlere, malvarlığı ve ekonomik değerlerden daha fazla önem vermiştir diyebiliriz.

Yasa koyucu ceza yasamızda ilk kez yer alan "bedeli karşılığında yararlanılabilen sistemler" kavramı ile ilgili olarak yasa metninde ya da gerekçesinde herhangi bir tanımlama veya açıklama yapmamıştır. Ancak bu sistemlerin elektronik arşiv merkezleri, elektronik gazeteler, elektronik kütüphaneler, sanal kitaplar, sanal ortamda yayın yapan dershaneler, bireylere kişilik testi yapıp onların karakterleri hakkında tahmin sunan, belirli bilgisayar oyunları oynanmasına imkân veren ya da tamamen şifreli kullanıma açık benzer[394] "bilişim sistemleri" olduğu açıktır. Bu bağlamda "bedeli karşılığında yararlanılabilen sistemler" kavramından belirli bir ücret veya bedel karşılığında, kablolu veya kablosuz bir ağ üzerinden ya da çeşitli frekanslardan yayın yaparak; veri, bilgi ve haber gibi hizmetleri sunan internet siteleri ve yayınlar kastedilmiştir diyebiliriz.[395]

---

[392] Artuk-Gökçen-Yenidünya, s.712.

[393] Yaşar-Gökcan-Artuç, s.6749, Artuk-Gökçen-Yenidünya, s.712; Taşdemir, s.262.

[394] Parlar-Hatipoğlu, *TCK Yorumu*, s.1698; Erdoğan, s.148; Karakehya, s.17; Karagülmez, s.173-174; Yaycı, s.83; Esen, s.630.

[395] Bayındır, s.68.

Otomatlar; farklı program yüklenememeleri, yüklenebilecek bu programlara göre otomatik olarak değişik işlemler yapamamaları nedeniyle bilişim sistemi sayılmadıklarından bu madde kapsamına girmezler. "Dekoderler"[396] ise bilişim sistemi kapsamında değerlendirilebilirler.[397] Ancak TCK 163/2'nci fıkradaki dekoderleri de kapsayan ve daha özel olan "karşılıksız yararlanma" düzenlemesi nedeniyle bu madde kapsamına girmezler.[398]

İnternet cafe'ler bu fıkra kapsamına girmezler.[399] Yasada korunan, internet içinde bedel karşılığında sunulan elektronik hizmetlerdir, hizmetin verildiği yer değildir.[400] İnternet cafe'ler aracılığıyla bilişim sistemlerine ulaşma imkânı sağlanmaktadır. Eğer internet cafe'lerde "bilişim sistemleri kiralanıyor olsaydı"[401] bilişim sistemlerinin asıl sahiplerine de ayrıca bir ücret ödenmesi gerekirdi.

2.2.9.2. Netice Sebebiyle Ağırlaşmış Hal

243 maddenin 3. fıkrasında "bilişim sistemine girme ve orada kalma" fiili sonucunda "bilişim sistemin içerdiği verilerin yok olması veya değişmesi" ağırlaştırıcı nitelikli hal olarak düzenlenmiştir. Bu fiilin neticesinde faile birinci fıkradaki cezanın iki katına kadar yaptırım uygulanabilecektir.

"*Sistemin içerdiği verilerin yok olması veya değişmesi*" fiilinin bu fıkra kapsamına girebilmesi için fail bu sonuca istemeden yol açmış olmalıdır.[402] Başka bir ifade ile netice itibariyle ağırlaşmış bir hal söz konusudur. Örneğin; bir başkasının şifreli bilgisayarına, şifresini çözerek giren failin, şifre kırma çalışmaları sırasında

---

[396] Dekoderler; kendilerine kablolu veya kablosuz yollar aracılığıyla iletilen şifreli sinyalleri aldıktan sonra, bu sinyalleri üzerinde yüklü programlar vasıtası ile çözerek alıcılara ileten, cihazlardır.

[397] Erdoğan, s.149; Artuk-Gökçen-Yenidünya, s.712.

[398] TCK m.163/2 "*Telefon hatları ile frekanslarından veya elektromanyetik dalgalarla yapılan şifreli veya şifresiz yayınlardan sahibinin veya zilyedinin rızası olmadan yararlanan kişi*"nin cezalandırılmasını düzenlemiştir.

[399] Aynı yönde görüş için bkz. Erdoğan, s.149. Aksi yönde görüş için bkz. Artuk-Gökçen-Yenidünya, s.712; Yaşar-Gökcan-Artuç, s.6749; Karagülmez, s.174.

[400] Erdoğan, s.148.

[401] Artuk-Gökçen-Yenidünya, s.712.

[402] Akarslan, s.43; Karagülmez, 176; Bayındır, s.69; Karakehya, s.18; Dülger, *Bilişim Suçları*, s.228; Parlar-Hatipoğlu, *TCK Yorumu*, s.1698.

hedef bilgisayardaki veriler bozulur veya kaybolursa bu fıkra kapsamında ağırlaştırıcı hal oluşmuş olacaktır.[403] Eğer fail anılan zarara isteyerek yol açmışsa bu sefer fiil 244/2. madde kapsamında değerlendirilecektir.

2.2.10. Suçun Özel Görünüş Biçimleri

2.2.10.1. Teşebbüs

Teşebbüs; failin bir suçu gerçekleştirmek için elverişli hareketlerle icraya başlayıp ta elinde olmayan nedenlerle tamamlayamadığı durumlarda söz konusudur. 243. maddedeki suçun teşebbüse elverişli olup olmadığı konusunda doktrinde farklı görüşler mevcuttur.

Bu maddede düzenlenen suç türüne teşebbüsün mümkün olmadığını söyleyen hukukçular; bilişim sistemine girme ve kalma suçu birden fazla hareketli bir suçtur. Girme fiili aynı zamanda kalma fiilini de içerdiğinden, sisteme girme ve kalma hareketleri birbirinden ayrılamamakta, mütemadi niteliğinden dolayı bu suç parçalara bölünememektedir. Bu konuda her somut olaya göre hâkimler karar vereceğinden çeşitli yorum farkları nedeniyle bazı fiillere teşebbüsten ceza verilirken, aynı tür bazı fiillere de tamamlanmış fiilden ceza verilebileceğinden bu suça teşebbüsten ceza vermek mümkün değildir, demişlerdir.[404]

Çoğunluğu oluşturan, benim de katıldığım diğer görüş sahibi hukukçular ise; bu suça teşebbüsün mümkün olabileceğini ifade etmektedirler.[405] Bu görüşe göre; uygun icra hareketleriyle sisteme girildiği anda elektrik kesilmesi, sistemin kilitlenmesi, sistemin kullanıcısı tarafından kapatılması veya bilişim sistemin koruma programlarının önlemesi nedeniyle, orada kalma durumu gerçekleşmemişse fiil tamamlanmadığından fail anılan suça teşebbüsten sorumlu olur.

2.2.10.2. İştirak

Bilişim sistemine girme ve orada kalma suçu iştirak açısından farklı bir özellik taşımamaktadır. Bu nedenle faillik (m37), azmettirme (m.38), yardım etme

---

[403] Karakehya, s.18.

[404] Ketizmen, s.108; Taşkın, *Bilişim Suçları*, s.30; Parlar, s.18.

[405] Soyaslan, ...*Özel Hükümler,* s.611; Yaycı, s.80; Esen, s.631; Parlar-Hatipoğlu, *TCK Yorumu,* s.1698; Erdoğan, s.163-167; Demircan, s.94; Yaşar-Gökcan-Artuç, s.6750-6751; Karagülmez, s.171-172; Bayındır, s.66-67; Karakehya, s.19; Dülger, *Bilişim Suçları*, 221-222; Taşdemir, s.260; Çekiç, s.91; Meran, s.367; Artuk-Gökçen-Yenidünya, 715; Malkoç, *5237 Sayılı Türk Ceza Kanunu,* s.1669.

(m.39) ve bağlılık kuralı (m.40) düzenlemeleri ışığında somut olay değerlendirilerek karar verilecektir.[406] Bilişim sistemine girme ve orada kalma suçu mütemadi bir suç olduğu için, temadi sona erinceye kadar anılan suça iştirak etmek mümkündür. Bu suç bakımından, (suça iştirak iradesiyle olmak şartıyla) suçun işlenmesi için gereken bilgisayar ve unsurlarını temin etmek, teknik destek vermek, teşvik etmek, azmettirmek gibi fiilleri örnek olarak verebiliriz.[407]

2.2.10.3. İçtima

Ceza hukukunda kural olarak "kaç tane fiil varsa o kadar suç, kaç tane suç varsa o kadar ceza vardır." TCK'nın genel gerekçesinde de ifade edilen bu kuralın istisnasını ceza yasamızda düzenlenmiş olan içtima hükümleri (bileşik suç m.42, zincirleme suç m.43 ve fikri içtima, m.44) oluşturmaktadır.[408] İçtima hükümleri açısından konumuz olan bilişim sistemine girme ve orada kalma suçu farklı bir özellik taşımamaktadır.

Bilişim sistemine girme ve orada kalma suçu birleşik hareketli bir suçtur. Bu nedenle anılan suçun oluşması için hem sisteme girilmiş hem de sistemde kalınmış olması gerekir. Bu suç mütemadi/kesintisiz bir suç olduğu için temadi sona ermediği (sistemde kalınmaya devam edildiği) sürece tek suç var demektir. Suçun sona ermesi temadinin kesildiği andır. Failin bir bilişim sisteminde uzun sürelerde kalması ayrı bir suç oluşturmaz. Bu durumda sistemde kalınan süre temel cezanın belirlenmesinde (m.61) bir ölçüt olarak kullanılacaktır.[409]

Zincirleme suçun oluşabilmesi için failin aynı suç işleme kararı kapsamında, aynı mağdurun bilişim sistemine, değişik zamanlarda girmiş ve orada kalmış olması gerekir.[410] Bu durumda faile zincirleme suç düzenlemesi nedeniyle (m.43/1) tek bir

---

[406] Soyaslan, *B.A.Suçlar,* s.1569; Karakehya, s.20; Dülger, *Bilişim Suçları*, 222-224; Parlar, s.18; Yaycı, s.80; Demircan, s.95; Erdoğan, s.167-168; Yaşar-Gökcan-Artuç, s.6751.

[407] Erdoğan, s.168.

[408] Yaycı, s.80; Erdoğan, s.168; Çekiç, 96-97.

[409] Erdoğan, s.169; Yaşar-Gökcan-Artuç, s.6751.

[410] Bir Yargıtay kararında "*Sanığın oluşa uygun olarak sübutu kabul edilen* ***bilişim suçlarının mağdur sayısınca oluştuğu gözetilmeden,*** *zincirleme işlendiğinden bahisle yazılı şekilde 765 sayılı TCK'nın 80. maddesi ile uygulama yapılması ...*" ifadeleriyle bu suç açısından zincirleme suç hükümlerinin uygulanabileceğine vurgu yapılmıştır. (11. CD. E. 2007/9369, K.2010/6092, 18.05.2010), (Kaynak; Erdoğan, 648 numaralı dipnot, s.169).

suçtan ceza verilecek ancak cezasında artırıma gidilecektir.[411] Bu fiil farklı kişilere karşı işlenirse, mağdur sayısınca ayrı suç oluşacaktır. Failin girdiği bilişim sisteminde kendisinin dışında başkalarının da bilgi ve dosyalarının bulunması halinde mağdur sayısı birden fazla olacağından bu durumda diğer koşulları da varsa (m. 43/2) uyarınca yine zincirleme suç hükümleri uygulanabilecektir.[412]

Türk Ceza Kanunu'nda bilişim alanında düzenlenen "bir bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme" (m. 244), "banka veya kredi kartlarının kötüye kullanılması" (m. 245) suçları ile "haberleşmenin engellenmesi" (m.124), "haberleşmenin gizliliğini ihlal" (m.132) gibi diğer suçların işlenebilmesi için bilişim sistemine girme ve orada kalma fiilinin gerçekleştirilmesi gerekmektedir. Bu gibi durumlarda bilişim sistemine girme ve orada kalma suçu geçit suç rolü oynamaktadır.[413] Çünkü sonraki suçu işleyebilmek için bilişim sistemine girme suçunu önceden işlemek gerekmektedir. Bu durumlarda faile iki ayrı suçtan ceza yerine, fikri içtima (m.44) hükümleri uygulanarak daha ağır cezayı gerektiren maddenin uygulanması gerekmektedir.[414]

Biri diğerinin unsurunu veya ağırlaştırıcı nedenini oluşturan, dolayısıyla tek fiil sayılan suçlara bileşik suç denir (m.42). Bu tür suçlarda içtima hükümleri uygulanmaz. Örneğin "bilişim sistemi aracılığıyla hırsızlık" (m.142 2-e) ve "bilişim sistemi aracılığıyla dolandırıcılık" (md.158 1-f) gibi suçlarda bilişim sisteminin kullanılması anılan suçların ağırlaştırıcı nedenini oluşturduğu için içtima hükümleri yerine hırsızlık veya dolandırıcılık suçlarının ağırlaştırıcı yaptırımı uygulanır.[415]

2.3. BİLİŞİM SİSTEMİNİ ENGELLEME, BOZMA, VERİLERİ YOK ETME VEYA DEĞİŞTİRME SUÇLARI (m.244)

TCK'nın 244. maddesinde bilişim sistemi ve verilerine karşı yapılan her tür zarar verici eylem yaptırım altına alınmıştır. Bu fiiller bilişim sistemini engelleme,

---

[411] Esen, s.631; Parlar, s.18; Erdoğan, s.169; Bayındır, s.67; Karakehya, s.20; Meran, s.36; Artuk-Gökçen-Yenidünya, 716; Malkoç, *Açıklamalı İçtihatlı 5237 Sayılı Türk Ceza Kanunu,* s.1670; Taşkın, *Bilişim Suçları*, s.32.

[412] Artuk-Gökçen-Yenidünya, s.716; Erdoğan, s.169. Aksi yönde görüş için bkz. Yaşar-Gökcan-Artuç, s.6751.

[413] Soyaslan, ...*Özel Hükümler,* s.612.

[414] Erdoğan, s.169; Karakehya, s.21; Taşkın, *Bilişim Suçları*, s.33.

[415] Karakehya, s.22; Parlar, s.18; Taşkın, *Bilişim Suçları*, s.33.

bozma, verileri yok etme veya değiştirme gibi eylemlerdir. Söz konusu maddenin birinci fıkrası ile bilişim sisteminin işleyişini engelleme veya bozma fiilleri, ikinci fıkrasıyla; sistemde yer alan verileri bozma, yok etme, değiştirme, erişilmez kılma, sisteme veri yerleştirme ve verileri başka yere gönderme eylemleri yaptırım altına alınmıştır. Üçüncü fıkrada; bu fiillerin bir banka veya kredi kurum ve kuruluşunun bilişim sistemi üzerinde işlenmesi artırım nedeni olarak öngörülmüş ve son fıkra ile de failin bu eylemleri sonucunda kendisine veya başkasına haksız menfaat sağlaması durumu nitelikli hal sayılmıştır. Başka bir ifade ile 244. maddenin ilk üç fıkrası ile bilişim sistemi ile sistemdeki verilerin korunması amaçlanırken, dördüncü fıkrası ile bilişim sistemi kullanılarak haksız yarar sağlama fiili önlenmeye çalışılmıştır.

765 sayılı ETCK'da bu fiiller ile başkasına zarar verme amacı aranırken, TCK 244. maddede failde zarar verme amacı aranmamıştır. Bu maddenin 1. ve 2. fıkralarının kısmen ETCK'nın 525/b fıkrasının, 244/4. fıkrasının ise yine kısmen 525/c maddesinin karşılığı olduğunu söyleyebiliriz. Eski yasa döneminde olmayan 244/3. fıkrayla, suçun banka veya kredi kurumuna ya da bir kamu kurum ve kuruluşuna ait bilişim sistemi üzerinde işlenmesi artırım nedeni olarak düzenlenmiştir.[416]

Maddenin ilk fıkrası; Avrupa Konseyi Siber Suç Sözleşmesi (AKSSS)'nin 5. maddesindeki "*sistemlere müdahale*",[417] ikinci fıkrası; AKSSS'nin 4. maddesindeki "*verilere müdahale*",[418] başlıklı hükümleri karşılanmak için düzenlenmiştir.[419]

---

[416] Parlar, s.24; Yaşar-Gökcan-Artuç, s.6755.

[417] AKSSS m.5; *"Taraflardan her biri, bilgisayar verilerine yeni veriler ilave etmek, bilgisayar verilerini başka yerlere iletmek, tahrip etmek, silmek, bozmak, değiştirmek veya erişilemez kılmak suretiyle, bir bilgisayar sisteminin işleyişini ciddi ölçüde ve haksız şekilde engelleme fiilleri kasıtlı olarak işlendiğinde, bu fiillerin kendi ulusal mevzuatı kapsamında cezaî bir suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır."*

[418] AKSSS m.4/1; "*Taraflardan her biri, bilgisayar verilerinin haksız bir şekilde tahrip edilmesi, silinmesi, bozulması, değiştirilmesi veya erişilemez kılınması fiilleri, kasıtlı olarak yapıldıklarında, bu fiilleri kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır*."

[419] Taşkın, *Bilişim Suçları,* s.39-40; Parlar, s.24; Yaycı, s.86; Esen, s.633; Murat Volkan Dülger, *Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler,* **Çağın Polisi Dergisi**, C.IV, S.42, Haziran 2005, Ankara, s.3; Çekiç, s.102; Ergün, s.90.

Ayrıca haklı olarak AKSSS'nin "*bilgisayarla ilişkili sahtekârlık fiilleri*" başlıklı 8. maddesi[420] hükümlerinin de bu madde kapsamına girdiğini ifade edenler de vardır.[421]

Karşılaştırmalı hukukta da bu suç tipine yer verilmektedir. Örneğin Fransa (CK m.323/2), Almanya (CK m.303/a), Finlandiya (CK m.35/1), Danimarka (CK m.279/a), Norveç (CK m.151b), Avusturya (CK m.126/a1) ve Avustralya (CK m.76/c) gibi ülkeler bu yönde düzenlemeler yapmışlardır.[422]

2.3.1. BİLİŞİM SİSTEMİNİN İŞLEYİŞİNİ ENGELLEME VEYA BOZMA SUÇU (m. 244/1)

2.3.1.1. Korunan Hukuki Değer

244/1. fıkrada düzenlenen suç tipi AKSSS'nin açıklayıcı raporunda "bilgisayar sabotajı" olarak nitelendirilen eylemleri önlemeyi amaçlamaktadır.[423] AKSSS'nin gerekçe raporunda 4. maddeyle; "*bilgisayar verileri veya programlarına zarar verilmesi önlenerek programların doğru ve aksaksız çalışması"*nın, 5. maddeyle "*bilgisayar sabotajları önlenerek bilişim sisteminin sağlıklı şekilde kullanılması ve sisteme yönelecek haksız davranışların önlenmesi"*nin korunmaya çalışılan hukuksal değer olduğu açıklanmıştı.[424] TCK 244. maddenin gerekçesinde de AKSSS'nin 4. ve 5. maddeleri paralelinde düzenleme yapıldığı, *"Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir,"* şeklindeki ifadelerden anlaşılmaktadır. Gerekçedeki "*ızrar fiilleri özel bir suç haline getirilmiştir*" ifadesinden sisteme zarar verici fiillerin önlenmeye çalışıldığı anlaşılmaktadır.[425]

---

[420] AKSSS m.8; "*Taraflardan her biri, aşağıdaki faaliyetlerde bulunmak suretiyle bir başkasının mülkiyetinin ziyaına sebep olma fiili, kasıtlı ve haksız olarak yapıldığında, kendi ulusal mevzuatı kapsamında cezaî birer suç olarak tanımlanması için gerekli olabilecek yasama işlemlerini ve diğer işlemleri yapacaktır: Bu fiiller sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma; sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme fiilleridir.*"

[421] Taşdemir, s.266; Bayındır, s.70.

[422] Çekiç, s.102; Erdoğan, s.181.

[423] Artuk-Gökçen-Yenidünya, s.718.

[424] Şaban Cankat Taşkın, *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yüksek Lisans Tezi, İstanbul, 2008, s.48.

[425] Parlar, s.24.

244/1. fıkradaki düzenlemeyle genel olarak bilişim sisteminin hem donanımına hem de yazılımına zarar verici nitelikteki eylemler önlenmeye çalışılmıştır. Bu düzenlemenin ihdasıyla bilişim sistemlerinin doğru ve uygun şekilde çalışması ve devamı koruma altına alınmaya çalışılmıştır.[426] Bir başka açıdan da korunan hukuksal değerler arasında bilişim sistemine olan güven, sistem sahibi ve kullanıcısının maddi ve manevi çıkarları ve haberleşme özgürlüğünün de olduğunu ifade edebiliriz.[427] Doktrinde mülkiyet hakkı ve fikri mülkiyet hakkının da korunduğunu ifade edenler de vardır.[428]

Doktrinde ayrıca bir failin mala zarar vermek kastıyla mağdurun bilgisayarını kırması halinde, TCK 244/1. fıkra yerine, 151. maddedeki mala zarar verme yaptırımının uygulanması gerektiği ileri sürülmektedir.[429] İlk bakışta bu görüş doğru olarak gözükse de, kanaatime göre bilgisayarın bilişim sistemi unsuru olduğu dikkate alındığında, bilişim ağlarına bağlı veya kullanımda olan bir bilgisayarın donanım unsurlarına verilecek zararın yazılım unsurlarına da zarar vereceği görüleceğinden bu görüşe katılmak mümkün değildir. Bu durumda TCK 151. madde yerine 244/1. fıkranın uygulanması daha uygun olacaktır. Ancak bir ağa veya sisteme bağlı olmayan, henüz kullanılmayan bir bilgisayar için mala zarar verme fiilinden yaptırım uygulanabilir. Bu nedenle her somut olaya göre ortaya çıkan zarar belirlenip bu tespite göre karar verilmesi daha uygun olacaktır.

2.3.1.2. Suçun Konusu

Suçun konusu; işleyişi engellenen, bozulan bilişim sistemidir. Bilişim sistemi kavramı, bilişim sisteminin çalışabilmesi için ihtiyaç duyulan her türlü donanım ve yazılımları ifade etmektedir. Sistemin çalışabilmesi için gereken yazılım ve donanım unsurlarının bütünlüğü birlikte korunmuştur.[430]

---

[426] Artuk-Gökçen-Yenidünya, s.718.

[427] Yaşar-Gökcan-Artuç, s.6756; Erdoğan, s.184.

[428] Kurt, s.162.

[429] Soyaslan, ...*Özel Hükümler,* s.615; Dülger, *Bilişim Suçları,* s.231; Meran, s.633; Henkoğlu, s.192; Kızıltan, s.75.

[430] Taşkın, *Bilişim Suçları,* s.43; Çekiç, s.105; Artuk-Gökçen-Yenidünya, s.720; Soyaslan, *B.A.Suçlar,* s.1573; Kızıltan, s.77; Yaycı, s.93; Yaşar-Gökcan-Artuç, s.6757.

Suçun konusu; bilişim sistemi olduğu için maddenin uygulanmasında engellenen veya bozulan bilişim sisteminde sonradan yüklenen veri olup olmaması önemli değildir. Önemli olan, zarar gören bilişim sistemi unsurunun kullanılıyor olup olmamasıdır. Bu bakımdan herhangi bir bilişim sistemine bağlı olmayan, içinde veri bulunmayan ve bir mağaza vitrininde satılmak için sergilenen bir bilgisayara yönelik fiil TCK 244/1. madde kapsamına girmezken, aynı mağazada internete bağlı olan ve/veya bağlı olmadan kullanılan bilgisayara yönelik fiil 244/1 fıkra kapsamında değerlendirilecektir.[431]

2.3.1.3. Fail

243. maddenin incelenmesinde fail konusunda yapılan açıklamalar bu madde için de geçerlidir. Herkes bu suçun faili olabilir. Zira yasada bu konuda bir sınırlama getirilmemiştir.[432]

Tüzel kişi yararına haksız menfaat temin edilmişse ceza sorumluluğunun şahsiliği gereği tüzel kişi suç faili sayılmasa da, tüzel kişi aleyhine TCK m.60'da öngörülen; faaliyet izninin iptali, suçta kullanılan vasıtaların ve/veya elde edilen kazancın müsaderesi gibi güvenlik tedbirleri uygulanacaktır.[433]

2.3.1.4. Mağdur

Bu suçun mağduru için diğer suçlardan farklı herhangi bir özellik aranmamaktadır. Mağdurlar; suçtan zarar gören, hak veya menfaati ihlal edilen gerçek veya tüzel kişiler olabilir.[434] Suç fili sonucunda zarar gören "*mağdurun*" belirlenebilmesi için suç fiiliyle bilişim sisteminin hangi unsurunun hedef alındığının belirlenmesi gereklidir.[435] Suçun hedefi; bilişim sistemi, sistemdeki veriler, hem bilişim sistemi hem de veriler olabileceği için, bu unsurlar üzerinde kullanım,

---

[431] Çekiç, s.105; Soyaslan, ...*Özel Hükümler*, s.616; Taşkın, *Bilişim Suçları,* s.44.

[432] Artuk-Gökçen-Yenidünya, s.720; Parlar-Hatipoğlu, *5237 Sayılı TCK'da Asliye Ceza Davaları,* s.857; Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.70.

[433] Soyaslan, ...*Özel Hükümler*, s.615; Yaycı, s.93; Çekiç, s.103.

[434] Esen, *Malvarlığına Karşı Suçlar,* s.634; Parlar, s.25; Meran, s.371.

[435] Dülger, *Bilişim Suçları* s.232 ve ondan alıntı yapan Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.70'te failin belirlenebilmesi için bilişim sistemi unsurlarının kullanım, mülkiyet ve tasarruf yetkisinin kimlere ait olduğunun tespiti gerektiğini ifade etmişlerse de, kanaatimce failden daha çok mağdurun tespiti için bilişim sistemi unsurlarının kullanım, mülkiyet ve tasarruf yetkisinin kimlere ait olduğunun belirlenmesi gerekir. Bu nedenle alıntı yaptığım metinlerdeki "fail" terimi yerine "mağdur" terimini kullandım.

mülkiyet ve tasarruf yetkisinin kimlere ait olduğu mağdur veya mağdurların tespiti açısından önemlidir.[436]

Gerçek veya tüzel kişiler ayrı ayrı mağdur olabilecekleri gibi aynı anda da mağdur olabilirler. Hatta suçla elde edilecek maddi menfaat düşünüldüğünde gerçek kişilerle birlikte onlardan daha fazla banka ve kredi kurumları gibi tüzel kişilerin (ekonomik zarar ve itibar kaybı nedeniyle) mağduriyeti söz konusudur. Suç konusu eylemler nedeniyle, bilişim sistemine erişemeyen, geç erişen ya da sistemi kullanamayan ve sistem üzerinde tasarruf yetkisine sahip olan herkes bu suçun mağduru olabilecektir.[437]

2.3.1.5. Maddi Unsurlar

TCK'nın 244. maddenin ilk fıkrasıyla bilişim sistemini engelleme veya bozma fiilleri suç olarak düzenlenmiştir.[438] Failin çeşitli fiilleri sistemin engellenmesi veya bozulması sonucunu doğuracağından anılan fiiller seçimlik hareketlidir, failin bu sonuca yol açan hareketlerden birini seçmesi ve icra etmesiyle netice de gerçekleşir. "Bu fiil açısından neticesi harekete bitişik suç tipi söz konusudur."[439]

2.3.1.5.1. Hareket

244 maddenin 1. fıkrasında bilişim sisteminin engellenmesi veya bozulması fiilleri düzenlenmiştir. Yasa metninde ve gerekçesinde engelleme ve bozma fiillerinin tanımına yer verilmemiştir. MEB sözlüğüne göre engelleme; "*önlemek, geciktirmek, engel meydana getirmek, bir şeyin gerçekleşmesine mani olmak*", bozmak ise; "*işlemez, kullanılamaz hale getirmek, zarar vermek*" anlamlarına gelmektedir.[440]

---

[436] "*Sanığın bilgisayar programı sayesinde katılana ait internet bankacılığı şifre bilgilerini ele geçirip, bu şifreyi kullanarak hesaplarından kendi hesabına para aktarması eylemlerinde gerçek kişiye yönelik bir hile ve desise bulunmadığından…"* (11. CD. E.2008/16570 – K.2009/101, 28.01.2009), (Kaynak; Corpus İçtihat Programı).

[437] Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.70; Dülger, *Bilişim Suçları* s.232; Kızıltan, s.76.

[438] Avşar-Öngören, s. 108.

[439] Bayındır, s.82; Soyaslan, ...*Özel Hükümler*, s.616; Çekiç, s.104.

[440] Örnekleriyle Türkçe Sözlük; C.I. s.837 ve s.381.

Bilişim sisteminin engellenmesi doktrinde; "*sisteme etkide bulunularak sistemin düzgün işlemesinden elde edilecek her türlü faydanın engellenmesi ve sistemin işlevlerini yerine getirememesi*",[441] "*sistemin geçici veya sürekli olarak çalışmasının herhangi bir şekilde kesintiye uğratılması*",[442] "*sistemin çalışmasının bir şekilde kesintiye uğratılması*",[443] "*sistemin çeşitli yöntemlerle sürekli ya da geçici olarak işlem görmesinin engellenmesi*",[444] "*sistem aracılığıyla veri işleme faaliyetinin engellenmesi*",[445] "*sisteme etkide bulunularak sistemin düzgün işlemesinden elde edilecek her türlü faydanın engellenmesi ve sistemin işlevlerini yerine getirememesi*",[446] "*sistemin gerektiği gibi çalışmasının önlenmesi, faaliyet ve kapasitesinin sınırlandırılması, sistemin işleyişinin yavaşlatılması ya da tamamen kilitlenme noktasına gelmesi*"[447] ve "*bilişim sisteminin varlık sebebi olan görevlerini yapamaz hale getirilmesi*" şeklinde tanımlanmıştır.[448]

Sistemin engellenmesinde dikkat edilmesi gereken husus bilişim sistemin işleyişinin yine devam ediyor olmasıdır. Fakat bilişim sistemi suç konusu fiile maruz kalmadan önceki gibi görevlerini yerine getirememektedir. Engelleme fiilinin geçici veya sürekli olmasının bir önemi yoktur. Engelleme fiilinin gerçekleştirilme şeklinin de herhangi bir önemi yoktur. Bu fiiller bilişim sisteminin somut donanım unsurlarına yönelik (bağlantısını kesmek, elektriğini kesmek gibi) fiillerle gerçekleştirilebileceği gibi, soyut yazılım unsurlarına yönelik (elektronik posta bombardımanı[449] spam, mantık bombası, tavşanlar[450] gibi zararlı yazılımların

---

[441] Ergün, s.92.

[442] Karagülmez, s.187.

[443] Parlar, s.25.

[444] Meran, s.371.

[445] Ketizmen, s.129.

[446] Dülger, *Bilişim Suçları*, s.235.

[447] Taşdemir, s. 268.

[448] Erdoğan, s.189.

[449] Kurt, s.164.

[450] Örnek için bkz. yuk. 70-80. sayfalar.

bulaştırılması gibi) fiillerle de gerçekleştirilebilir.[451] Hatta bilişim sistemi yoğun elektromanyetik dalgalara maruz bırakılarak ta çalışmasına engel olunabilir.[452]

Bilişim Sisteminin Bozulması doktrinde; "*bilişim sisteminin; kendisinden beklenilen işi yapamayacak duruma getirilmesi, düzeninin karıştırılması, zarar verilmesi, kötü duruma getirilmesi*",[453] "*sistemin geçici veya sürekli şekilde tamamen çalışamaz hale getirilmesi",*[454] "*sistemin veri işleme faaliyetini yapamayacak hale gelmesi*",[455] "*sistemin çökertilmesi, program akışının değiştirilmesi, bozulması, sistemin soyut unsurlarının işleyemez hale getirilmesi*",[456] "*sistemin olağan ve normal koşullarda yapması gereken işlevlerinin değişikliğe uğratılması*",[457] "*haksız müdahale ile sistemin sağlıklı işleyişinin geçici veya sürekli şekilde ortadan kaldırılması*",[458] "*kalıcı surette sistemden istifadenin engellenmesi*",[459] "*bilişim sisteminin veri işleme faaliyeti yapamayacak hale getirilmesi*",[460] "*sistemdeki unsurların kısmen veya tamamen işlev göremez hale getirilmesi",*[461] "*sistemin maddi yapısına vaki müdahalelerle, verilerin ve işleyişin düzenini bozan her tür hareket*"[462] ve "*bilişim sisteminin olağan koşullarda yapması gereken işlevlerin değişikliğe uğratılması*" şeklinde tanımlanmıştır.[463]

---

[451] Önder, s.509; Kubilay Taşdemir – Ramazan Özkepir, *Uygulamada - Öğretide Belgelerde Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar,* Adil Yayınevi, Ankara, s. 1115.

[452] Taşdemir, s.268; Artuk-Gökçen-Yenidünya, s.719.

[453] Dülger, *Bilişim Suçları*, s.235; Soyaslan, ...*Özel Hükümler*, s.616; Ergün, s.93.

[454] Parlar, s.25.

[455] Ketizmen, s.129.

[456] Kurt, s.164; Taşkın, *Bilişim Suçları*, s.45.

[457] Meran, s.371.

[458] Karagülmez, s.188.

[459] Artuk-Gökçen-Yenidünya, s.719.

[460] Erdoğan, s.189.

[461] Gündel, s.4633.

[462] Malkoç, ...*Türk Ceza Kanunu,* s.1679.

[463] Taşdemir, s.268.

Sistemin bozulmasında dikkat edilmesi gereken husus bu maddeyle korunmak istenen bilişim sisteminin artık ya hiç işlememesi veya hatalı işlem yapıyor olmasıdır. Bozma fiilinin nasıl gerçekleştirildiği suçun oluşumu açısından önemli değildir. Sistemin işleyişi; bilişim sistemleri kullanılarak sistemin tümüne veya bir kısmına (sistemde yer alan verilere[464] veya diğer unsurlarına) yapılacak müdahaleler ile bozulabileceği gibi, sisteme yönelik fiziksel müdahalelerle de bozulabilir.[465] Bilişim sisteminin yanında DVD, CD, Flash bellek, yedek harddisk gibi veri taşıma araçları ile sistemin sağlıklı çalışmasına engel olacak diğer unsurları da madde kapsamındadır. Kısmen bozmanın veya sistemin diğer unsurlarının bozulmasının bu madde kapsamına girebilmesi için bozulan kısım nedeniyle bilişim sisteminin bir daha kullanılamaz hale gelmesi gerekmektedir.[466]

2.3.1.5.2. Netice

Maddenin birinci fıkrasındaki suçun neticesi "bilişim sisteminin işleyişinin engellenmesi, bozulmasıdır."[467] Bu tür suçlar neticesi harekete bağlı suçlar olduğundan netice, hareket yapıldığı anda gerçekleşir. Netice hareketten ayrılamamaktadır. Buradaki engelleme veya bozma fiilleri seçimlik hareketli suçlardır. Bu hareketlerden bir tanesinin yapılması neticenin gerçekleşmesi demektir.

---

[464] Örneğin; "*Onaltılık (Hex) editör programı aracılığıyla, bir word belgesinin program kodundaki üç satırın değiştirilmesi (yani Object ID kodu yerine Exploid Code yazılması) durumunda, program kodu değiştirilmiş bu word belgesinin açılması o bilgisayarın word programının çökmesine neden olmaktadır*." **CHIP Dergisi** 2004 Nisan sayısı, *Hacker Raporu*, s.52'den aktaran Ergün, s.94.

[465] Artuk-Gökçen-Yenidünya, s.720; Soyaslan, *B.A.Suçlar,* s.1574; Karagülmez, s.188; Dülger, *Bilişim Suçları*, s.235; Taşdemir, s.269; Meran, s.371; Hayati Pallı, *"Türk Ceza Kanununda Yer Alan Başlıca Bilişim Suçları",* Adalet Bakanlığı, **Adalet Dergisi**, S.33, Ankara, Ocak 2009, s.92.

[466] Soyaslan, ...*Özel Hükümler*, s.617; Yaşar-Gökcan-Artuç, s.6759; Kurt, s.165; Taşkın, *Bilişim Suçları*, s.45; Parlar, s.25; Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.72; Çekiç, s.106.

[467] "*Sanıkların, oluşa uygun olarak sübutu kabul edilen önceden hazırladıkları tertibatla* ***şikayetçilere ait bankamatik kartlarının ATM makinesine sıkışmasını sağlayıp****, yine ATM kabinine monte ettikleri, içinde cep telefonu bulunan duvar tipi telefonu arayıp, kendisini banka görevlisi olarak tanıtıp kartı iptal edeceği bahanesi ile bankamatik kartının şifresini de öğrenip, ATM makinesinden ayrılmalarını müteakip hile ve desiselerle ele geçirip şifresini öğrendikleri bankamatik kartlarıyla para çekmekten ibaret eylemlerinin 765 Sayılı TCK.nun 504/3.* ***(5237 Sayılı TCK.nun 244/1) maddesinde yazılı suçu oluşturduğu gözetilmeden, ...****"* (11. CD. E.2006/2696 – K.2006/7334, 20.09.2006), (Kaynak; Yaşar-Gökcan-Artuç, s.6793).

Hareketlerin tamamlanmasıyla ortaya çıkan neticeler aynı zamanda zararı da oluştururlar.[468] Ayrıca bilişim sistemine karşı yapılan eylemler ile sistemin engellenmesi veya bozulması arasında uygun bir illiyet bağı da bulunmalıdır.

2.3.1.6. Manevi Unsur

244/1. fıkra açısından suçun manevi unsuru, bilerek ve isteyerek genel suç işleme kastıdır, özel kast aranmaz. Kast doğrudan kast olabileceği gibi olası kast da olabilir. Fail 1. fıkrada yer alan seçimlik iki fiili gerçekleştirirken eylemleri neticesinde bir zararın meydana gelmesini de istemelidir. Failin veya faillerin hangi saikle hareket ettiğinin bir önemi yoktur.[469]

2.3.1.7. Hukuka Aykırılık Unsuru

Birinci fıkrada düzenlenmiş olan suçlar da ancak hukuka aykırı bir fiille gerçekleştiğinde cezalandırılabilmektedir. Bu suç türünde bilişim sistemi ve/veya verileri üzerinde tasarruf yetkisi olan hak sahibi kişinin rızasının olması anılan fiilleri suç olmaktan çıkartır. Hak sahibinin rızası doğrultusunda bilişim sisteminin yapılandırılması, sistem güvenliği için internete erişimi engelleyen bir program yerleştirilmesi, verileri kurtarabilmek için bazı sistem dosyalarını silmek veya format atarak tüm verileri silmek gibi fiiller, hukuka aykırı olmadıkları için suç oluşturmayacaklardır.[470] Suç şikâyete bağlı olmayan, re'sen soruşturulan bir suç türü olduğu için hak sahibinin rızası fiilden önce olmalıdır. Fiil gerçekleştirildikten sonra hak sahibinin rızası, onaylaması, şikâyetçi olmaması fiilin soruşturulması ve kovuşturulmasını engellemez.[471]

Birinci fıkra açısından CMK'nın 134. maddesinde düzenlenen "Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma", 135. maddesinde düzenlenen "İletişimin Tespiti, Dinlenmesi ve Kayda

---

[468] Esen, s.635; Meran, s.372; Soyaslan, ...*Özel Hükümler*, s.621.

[469] Dülger, *Bilişim Suçları*, s.240-241; Taşdemir, s.270; Karagülmez, s.190; Soyaslan, *B.A.Suçlar*, 1579; Parlar, s.27; Bayındır, s.75; Esen, s.635; Meran, s.375; Kurt, s.175; Erdoğan, s.230; Yaşar-Gökcan-Artuç, s.6766.

[470] Taşdemir, s.269; Kurt, s.174; Erdoğan, s.200-201; Akıncı, F. S. "*Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi",* İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İnternet Özel Bölümü, C.LIX, S.1-2, 2001, s.19; Bayındır, s.75-76.

[471] Malkoç, ...*Türk Ceza Kanunu,* s.1667; Erdoğan, s.200, Dülger*, Bilişim Suçları*, s.240.

Alınması" ve 140. maddesinde düzenlenen "Teknik Araçlarla İzleme" koruma tedbirlerinin yasada gösterilen koşullara uygun olarak uygulanması halinde, yasa hükmünün icrası nedeniyle de bu suç oluşmayacaktır.[472]

2.3.1.8. Suçun Özel Görünüş Biçimleri

2.3.1.8.1. Teşebbüs

244. maddedeki suçun teşebbüs halinde kalması mümkündür. Birinci fıkra açısından fail, bilişim sisteminin işleyişini *bozmak* veya *engellemek* amacıyla sisteme girip kendi iradesi dışında amacına ulaşamazsa ve herhangi bir zarar meydana gelmemişse suç teşebbüs aşamasında kalmış demektir.[473]

Örneğin; bir bilişim sistemini engellemek veya bozmak amacıyla bilişim sistemine yerleştirilen virüs veya mantık bombasının harekete geçme zamanından önce fark edilerek etkisiz kılınması, sisteme veri yerleştirilirken elektriklerin kesilmesi,[474] sistemin kırılıp içine girmeye çalışılması (hacking) veya DDOS saldırıları ile sistem kaynaklarının tüketilip hizmetin engellenmeye çalışılması ama sistemin hizmet vermesinin engellenememesi gibi durumlarında suç teşebbüs aşamasında kalmış olacaktır.[475]

2.3.1.8.2. İştirak

244/1. fıkrada düzenlenen suç iştirak ile uyuşabilir. İştirak açısından farklı bir özelliği yoktur. TCK; m.37 (faillik), m.38 (azmettirme), m.39 (yardım etme) ve m.40 (bağlılık kuralı)'ta ifade edilen hükümler olaya uygulanarak suça iştirak olup olmadığının değerlendirilmesi hâkim tarafından yapılacaktır.[476]

2.3.1.8.3. İçtima

Bu suçun, aynı suç işleme kararıyla, farklı kısa zaman aralıklarıyla aynı kişi veya kuruma karşı birden fazla zincirleme şekilde işlenmesi mümkündür. Bu tür

---

[472] Erdoğan, s.201.

[473] Yaşar-Gökcan-Artuç, s.6767-6768; Soyaslan, ...*Özel Hükümler*, s.622; Bayındır, s.76; Taşkın, *Bilişim Suçları,* s.53-54; Parlar, s.27.

[474] Soyaslan, *B.A.Suçlar*, s.1583.

[475] Dülger, *Bilişim Suçları*, s.241.

[476] Esen, s.636; Erdoğan, s.202.

fiiller uygulamada sık sık kısa zaman aralıklarıyla bilişim sisteminin çalışmasının engellenmesi şeklinde görülmektedir.[477]

244. maddenin birinci fıkrasında düzenlenen engelleme ve bozma fiilleri seçimlik hareketli suçlardır. Dolayısıyla bilişim sisteminin engellenmesi veya bozulmasıyla suç oluşur. Örneğin bilişim sistemi önce engellenip sonrada bozulursa bu iki farklı eylem suç çokluğuna neden olmaz, eyleme tek suç nedeniyle yaptırım uygulanır.[478]

Fail TCK m.243/1 ile m.244/1 hükümlerini aynı anda ihlal ederse, başka bir ifade ile bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girip, orada kalmaya devam eden fail, aynı zamanda bilişim sisteminin işleyişini engeller veya bozarsa, fikri içtima hükümleri gereği faile 244/1. fıkra hükümleri uygulanmalıdır.[479]

Failin bilişim sistemini engellemesi veya bozmasındaki asıl amacının dördüncü fıkrada düzenlenen haksız çıkar sağlamak olduğu belirlenmişse faile dördüncü fıkradaki yaptırım uygulanır. Bu durumda faile ayrıca birinci fıkra hükümleri uygulanmaz.[480]

2.3.2. BİLİŞİM SİSTEMİNDEKİ VERİLERE ZARAR VERME SUÇU (m.244/2)

2.3.2.1. Korunan Hukuki Değer

TCK 244/2 fıkrada ifade edilen bir bilişim sistemindeki verilerin fail tarafından bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması, sisteme veri yerleştirilmesi, var olan verilerin başka bir yere gönderilmesi gibi 6 tür fiil sonucunda mağdurların pek çok hukuksal değeri ihlal edilebilecektir. Dolayısıyla 244/2. fıkrada pek çok değerin korunduğunu ifade edebiliriz.

Bu fıkra ile genel olarak bilişim sistemindeki verilerin gizliliği ve dokunulmazlığının korunan hukuki değer olduğunu söyleyebiliriz. Bunun dışında

---

[477] Taşkın, *Bilişim Suçları*, s.54; Bayındır, s.76; Artuk-Gökçen-Yenidünya, s.727.

[478] Yaşar-Gökcan-Artuç, s.6768 – 6769.

[479] Erdoğan, s.202-203.

[480] Yaşar-Gökcan-Artuç, s.6769.

ihlal edilen hukuksal değeri sistemde yer alan verilerin ve verilere yapılan hukuka aykırı fiilin niteliği belirleyecektir. Bu anlamdaki veriler bilişim sisteminin çalışmasını sağlayan dolayısıyla 244/2. fıkrada koruma altına alınan veriler değildir. 244/2 kapsamındaki veriler bilişim sistemi kullanıcısı tarafından, faal haldeki bilişim sistemine sonradan yüklenmiş, sonradan oluşturulmuş veya başka taraftan gönderilmiş olabilir. Bu verilerin sistemin çalışmasına etkisi yoktur. Söz konusu verilere yapılan müdahaleyle sistemin çalışması engellenip sistemin bozulması mümkün olmaz. Eğer hukuka aykırı fiille sistem engellenip bozuluyorsa, o fiile 244/2. fıkra hükümleri değil 244/1. fıkra hükümleri uygulanmalıdır.[481]

244/2. fıkra kapsamında korunan hukuksal değeri hukuka aykırı işlem yapılan verilerin niteliği ve verilere yapılan işlemin belirleyeceğini ifade etmiştim. Örneğin yasaya aykırı müdahalede bulunulan veya başka yere gönderilen veri özel hayata ilişkin ise "*özel hayatın gizliliği*", haberleşmeye ilişkin ise "*haberleşme özgürlüğü*" ihlal edilmiş olacaktır.[482] Müdahale edilen veri; bir şiir, roman, müzik eseri, kitap gibi çalışmalar olabileceği gibi yeni bir buluş içeren teknik bir çalışmada olabilir, bu durumda ise hukuken korunan değerin "*fikri mülkiyet hakkı*" olduğunu söyleyebiliriz.[483]

2.3.2.2. Suçun Konusu

Suçun konusu; değiştirilen, erişilmez kılınan, sisteme yerleştirilen veya yok edilen bilişim sistemindeki soyut verilerdir.[484] Veriler bilişim sistemine göre tali nitelikte, daha az değerde gibi gözükse de aslında öyle değildir. Çoğu zaman bilişim sisteminin çok üzerinde maddi değere sahiptirler. Örneğin bir avukatın dava ve icra dosyaları, bir muhasebecinin kayıtları veya bir şirketin yazışma ve evraklarının kayıtlı olduğu soyut veriler, bilişim sisteminin somut değerinin çok üzerinde bir maddi değere sahiptirler. 2012 yılında televizyondaki bir haber bülteninde İstanbul'da işyerinde kullandığı dizüstü bilgisayarı çalınan işyeri sahibinin, hırsıza önemli bilgilerinin kayıtlı olduğu bilgisayarını geri getirmesi halinde, hem 100 bin

---

[481] Erdoğan, s.215.

[482] A.g.e. 799 numaralı dipnot, s.214; Artuk-Gökcen-Yenidünya, s.722; Bayındır, s.71.

[483] Erdoğan, s.216; Bayındır, s.71.

[484] Taşkın, *Bilişim Suçları,* s.43; Çekiç, s.105; Artuk-Gökçen-Yenidünya, s.720; Soyaslan, *B.A.Suçlar,* s.1573; Kızıltan, s.77; Yaycı, s.93; Yaşar-Gökcan-Artuç, s.6757.

TL ödül vermeyi ve hem de herhangi bir hukuksal işlem yapmamayı taahhüt etmesi bu tespitimi teyit etmektedir.

Suçun konusu; bilişim sistemindeki veriler olduğu için maddenin uygulanmasında bilişim sisteminde veri yüklü olup olmaması, bu verilerin kullanımda olup olmaması önemlidir. Üzerinde veri bulunmayan bilişim istemine verilen zarar 244/2 kapsamı dışındadır. Duruma göre mala zarar verme veya 244/1. fıkra hükümleri uygulanabilir. 244/2. fıkradaki suç verilere zarar verilmesiyle tamamlandığından 243. maddeden farklı olarak bir tehlike suçu değil zarar suçudur.[485]

2.3.2.3. Fail ve Mağdur

Yasa metninde herhangi bir özellik veya sınırlama belirtilmediğinden suçun fail ve mağduru herkes olabilir.[486] Tüzel kişi yararına haksız menfaat temin edilmişse ceza sorumluluğunun şahsiliği gereği tüzel kişi suç faili sayılmasa da, tüzel kişi aleyhine güvenlik tedbirleri uygulanacaktır.[487]

Genel olarak suçun fail ve mağdurunun tespit edilebilmesi için suç fiilinin bilişim sisteminin hangi unsuruna yöneldiği belirlenmelidir. 244/2. fıkra kapsamında verilere karşı eylem yapıldığını düşünürsek verilerin kullanım, mülkiyet ve tasarruf yetkisinin kim veya kimler ise suçun mağduru da onlar olacaktır.[488]

2.3.2.4. Maddi Unsurlar

2.3.2.4.1. Hareket

244. maddenin ikinci fıkrasında düzenlenen suç tipini, birinci fıkrada düzenlenen bilişim sisteminin engellenmesi ve bozulması fiilinden ayıran unsur, suçların konusudur. Birinci fıkradaki suçun konusu "bilişim sistemi" iken, ikinci fıkradaki suçun konusu bilişim sisteminde yer alan verilerdir.[489]

---

[485] Yaşar-Gökcan-Artuç, s.6757.

[486] Artuk-Gökçen-Yenidünya, s.720; Parlar-Hatipoğlu, *5237 Sayılı TCK'da Asliye Ceza Davaları,* s.857; Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.70.

[487] Soyaslan, ...*Özel Hükümler*, s.615; Yaycı, s.93; Çekiç, s.103.

[488] Taşkın, *Bilişim Suçları,* s.14;

[489] Yaşar-Gökcan-Artuç, s.6759.

Bilişim sistemindeki verileri bozmak fiili; bilişim sisteminde yer alan verilerin, bilişim temelli bir hareketle veya veri yüklü sabit diskin ya da çeşitli veri taşıma araçlarının fiziken kırılması yoluyla, veriler yok edilmeden, verilerin tamamen veya kısmen işe yaramaz hale getirilmesini ifade eder. Anılan hareketler sonucunda veriler bozulmuş, bulunamaz veya ulaşılamaz hale gelmiştir.[490]

Verilerin bozulması veya yok edilmesinin sistemin genel çalışmasının bozulmasından çok daha ciddi bir kayıp olduğu göz önüne alındığında, sistemin işleyişinin bozulmasına göre, verilere yönelik zararlı eylemlerin daha ağır yaptırıma bağlanması uygun olmuştur.[491]

Verileri yok etmek fiili; verilerin ortadan kaldırılmasını ifade etmektedir. Bu anlamda yok etme verilerin silinmesini de içermektedir. Bilişim alanında verilerin silinmesi kurşun kalemle deftere yazılmış bilgilerin silinmesi gibi değildir. Buradaki silinme fiziki değil bilişim terimi olarak mantıki bir silinme, verilere normal yollardan ulaşılamaması demektir. Yoksa bir bilgisayar uzmanı tarafından yapılacak çeşitli teknik işlemlerle anılan verilere bazen ulaşılması mümkündür. Bunun dışında DVD, CD, Flash bellek, yedek hard disk gibi veri taşıma araçlarının fiziksel olarak kırılmasıyla da veriler yok edilmiş olur. Bu fiildeki verilere artık ulaşmak mümkün değildir. Gerçek anlamda veriler yok edilmiştir. Ancak söz konusu bu fiilde verilerin yok edilmesi fiili ikinci fıkra kapsamındadır.[492]

Verileri değiştirmek fiili; verilere başka bir görünüm kazandırma, başka bir şekle sokmadır. Bu yolla eski orijinal bilgilere ulaşılma olanağı ortadan kaldırılarak, değiştirilmiş hatalı bilgilere ulaşılma olanağı sağlanmış olur. Değiştirme işlemi bir bilgi notunun, öğrencinin dersten aldığı notun, resim ya da grafiğin değiştirilmesi şeklinde olabileceği gibi, verilerden oluşan (word, excel veya power point programları gibi) bir uygulama yazılımının değiştirilmesi şeklinde de olabilir.[493]

---

[490] a.g.e. s.6759-6760; Soyaslan, *B.A.Suçlar,* s.1575; Ergün, s.95.

[491] Akıncı-Alıç-Er, s.268.

[492] Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.73; Dülger, *Bilişim Suçları*, s.236-237; Taşdemir, s.271.

[493] Yılmaz, ...*Bilişim Alanındaki Suçlar,* s.74; İsmail Malkoç, Mahmut Güler, (*Uygulamada) Türk Ceza Kanunu Özel Hükümleri - IV,* Adil Yayınevi, Ankara, (t.y.), s.4762; Taşdemir-Özkepir, s.1115; Örneğin; "*Hacettepe Üniversitesine giriş sınavını kazanamadığı halde,*

Verileri erişilmez kılmak fiili; verilerin muhafaza edildiği bilişim sistemi veya bilgisayara ya da veri taşıma araçlarına erişim ve tasarruf hakkı olan bir kişinin verilere ulaşmasını önleyen veya erişimi sona erdiren herhangi bir eylem anlamındadır. Başka bir anlatımla, istendiği zaman istenen verilere ulaşılmasının engellenmesidir.[494]

Fiil, verilere ulaşmaya yarayan anahtar sözcüğün değiştirilmesi yoluyla,[495] şifresi olmayan bilişim sistemine şifre yerleştirerek veya verileri kullanan veya verilere malik olan kişinin istediği zaman istenen verilere erişmesinin engellenmesi gibi yollarla gerçekleştirilebilir.[496] Verilerin erişilmez kılınması fiilinin geçici süreli ya da sürekli olması suçun oluşumunu etkilememektedir.[497]

Bilişim sistemine veri yerleştirmek fiili; sistem maliki, sistem kullanıcısı veya ilgili kişilerin bilgisi ve onayı dışında, sistemde yer alan verilere herhangi bir zarar vermeden, onlara ulaşma imkânını ortadan kaldırmadan, sistemin orijinalinde daha önce mevcut olmayan ek birtakım verinin, dışarıdan bilişim sistemine ya da veri taşıma araçlarına, kaydedilmesi, eklenmesi veya yüklenerek yerleştirilmesidir.[498]

Suçun oluşumu için failde sisteme zarar verme kastı olması gerekmez. Yerleştirme fiili, DVD, CD, Flash bellek, yedek hard disk gibi veri taşıma araçlarıyla doğrudan doğruya sisteme fiziksel olarak veri aktararak yapılabileceği gibi, internet

---

bilgileri otomatik işleme tabi tutulmuş sistemi değiştiren kişiler vasıtası ile kendisine yarar sağlayan sanık U.Z.K.'nın eyleminin TCK 525/b-son maddesine uyduğu gözetilmeden…" (6.CD. E.1994/9297, K.1994/9639, 20.10.1994), (Kaynak; Vural Savaş, Sadık Mollamahmutoğlu, *Türk Ceza Kanunu'nun Yorumu,* Seçkin Yayınevi, 3.B. Ankara, Mayıs, 1999, s.5864.) ve "*Sanık tarafından bilgisayar kayıtlarındaki sayaç çarpanlarının değiştirilerek eksik fatura düzenlenmesiyle 15 milyar lira eksik tahakkuk ve tahsilâta neden olma eylemi 765 sayılı TCK 525/b maddesi kapsamında değerlendirilmelidir.*" (4.CD. E.2000/1068 - K.2000/1771, 28.02.2000), (Kaynak; Taşkın, *Bilişim Hukuku Uluslararası Uyuşmazlıklar*, s.340.)

[494] Ö. Umut Eker, *"Türk Ceza Kanununda Bilişim Suçları" Eski TCK Bağlamında Hukukumuzda Yer Alan İlk Düzenlemeler ve 5237 Sayılı Yeni Türk Ceza Kanunu'nun İlgili Hükümlerinin Yorumu,* **Türkiye Barolar Birliği Dergisi**, S.62, Ankara, 2006, s.126.

[495] Kurt, s.170.

[496] Taşkın, *Bilişim Suçları*, s.48.

[497] Dülger, *Bilişim Suçları*, s.235; Soyaslan, *B.A.Suçlar,* s.1576.

[498] Taşkın, *Bilişim Hukuku Uluslararası Uyuşmazlıklar*, s.341; Artuk-Gökçen-Yenidünya, s.725; Eker, s.125; Parlar-Hatipoğlu, *...Asliye Ceza Davaları,* s.859.

veya diğer bilişim ağları vasıtasıyla da yapılabilir. Fiilin oluşumu bakımından, bilişim sistemine failin hukuka uygun ya da aykırı bir şekilde girmiş olmasının önemi yoktur. Önemli olan sistem maliki, sistem kullanıcısı veya ilgili kişilerin bilgisi ve onayı dışında yükleme işleminin yapılmış olmasıdır.[499]

Bu bağlamda örneğin, facebook gibi bazı sosyal paylaşım sitelerine, sayfa sahibinin rızası olmadan çeşitli resim, yazı veya veri yüklenebilir. Ya da sisteme yerleştirilen "key logger" programıyla kullanıcının yaptığı bütün işlemler, programı yerleştirene iletilebilir, "virüs" programlarıyla sistem erişilemez ya da işlemez hale getirilebilir veya "Truva atı" yazılımı ile sistem her tür saldırıya açık hale getirilebilir.[500] Tabii bu durumda, 244/2. fıkradaki yaptırımın dışında, verileri başka bir yere göndermek, sistemi bozmak ya da erişilmez kılmak ya da özel hayatın ihlali veya verileri hukuka aykırı olarak ele geçirme gibi fiillerle başka ceza normu ihlallerinin de olduğu gözden uzak tutulmamalıdır.

Bilişim sistemindeki verileri başka bir yere göndermek fiili; doktrinde genel olarak, "*bilişim sisteminde bulunan verilerin, başka bir bilişim sistemine veya veri taşıma aracına transfer edilmesi, kaydedilmesi ya da kopyalanması*" şeklinde tanımlanmıştır.[501] Yine doktrinde kanun metninde herhangi bir sınırlama olmadığından bu tanıma ek olarak "*mağdurun bilişim sisteminde bulunan verilerin, yine mağdurun bilişim sistemindeki başka bir klasör veya dosyaya gönderilmesi halinde*" de anılan suçun oluşacağı haklı olarak ifade edilmiştir.[502]

Verileri göndermek fiili, DVD, CD, Flash bellek, yedek hard disk gibi veri taşıma araçlarıyla doğrudan doğruya sistemden fiziksel olarak veri kopyalama, aktarma yoluyla yapılabileceği gibi, internet veya diğer bilişim ağları vasıtasıyla da sistem içine veya dışına veri gönderilmesi yoluyla da yapılabilir.

---

[499] İsmail Ergün, *"Yeni Türk Ceza Kanunu'nda Bilişim Suçları",* **Çağın Polisi Dergisi**, C.IV. S.44, Ankara, Ağustos 2005, s.12; Yaycı, s.92; Demircan, s.109-110; Kızıltan, s.83; Erdoğan, s.226; Soyaslan, ...*Özel Hükümler*, s.620.

[500] Çekiç, s.109.

[501] Taşdemir, s.271-272; Meran, s.372; Dülger, *Bilişim Suçları*, s.238; Soyaslan, *B.A.Suçlar,* s.1577-1578; Parlar, s.27; Eker, s.125; Ergün, s.58.

[502] Ketizmen, s.142; Artuk-Gökçen-Yenidünya, s.725; Erdoğan, s.227; Yaşar-Gökcan-Artuç, s.6761.

Bu fiillere örnek olarak; bir üniversite öğrencisinin bilişim sistemindeki sınav sorularını kopyalaması,[503] bir bilişim sistemindeki özel fotoğraf, grafik veya çeşitli belgelerin yazıcıdan çıktı yoluyla alınması,[504] sisteme yerleştirilen Truva atı programının sistemdeki verileri daha önceden tanımlanan bilgisayara göndermesi[505] veya devletlerin güvenliğine ilişkin önemli bilgilerin ele geçirilmesi, kişilerin özel bilgi ve resimlerinin kopyalanması, ekonomik menfaat temin etmek veya başka amaçlarla üçüncü kişilerin eserlerini haksız olarak ele geçirmek gibi fiilleri sayabiliriz.[506]

2.3.2.4.2. Netice

İkinci fıkradaki suçun neticesi, bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılınması, bilişim sistemine veri yerleştirilmesi veya bilişim sistemindeki verilerin başka bir gönderilmesi anında gerçekleşmiş olur.[507] Anılan fiiller yapıldığı anda suç gerçekleşmiş olur. Bu nedenle 244/2. fıkrada neticesi harekete bitişik bir suç tipi vardır.[508] Ayrıca bilişim sistemindeki verilere karşı yapılan eylemler ile verilerin uğradığı zarar arasında uygun bir illiyet bağı da bulunması gerekir.

2.3.2.5. Manevi Unsur

244/2. fıkrada düzenlenen verilere zarar verme suçu kasten işlenebilen bir suç türüdür. Genel kasıt yeterlidir. Failde özel bir amacın bulunmasına gerek yoktur. Fail gerçekleştirdiği fiilin sonuçlarını da istemelidir.[509]

---

[503] Parlar, s.27.

[504] Erdoğan, s.228.

[505] Ergün, s.58.

[506] Bayındır, s.74-75.

[507] *"İddianamede açıklanan ve suç oluşturduğu ileri sürülen fiil bilişim sistemine girilmek suretiyle bilgileri değiştirmekten ibaret olup, anılan suç gerek 765 sayılı TCY, gerekse 5237 sayılı TCY'nda Asliye Ceza Mahkemesinin görevi alanında bulunmaktadır.* ***Konusu bilişim sistemine girilmek suretiyle bilgileri değiştirmek olan*** *iddianame dışına çıkılarak, davaya konu edilmeyen ve bağımsız bir diğer suç teşkil eden başka bir eylemden dolayı yargılama yapılması ve sahtecilikten açılmayan davadan hüküm kurulabileceğinin düşünülerek görevsizlik kararı verilmesinin önerilmesi yasal olarak olanaklı değildir."* (YCGK. E.2007/11-44 – K.2007/200, 09.10.2007), (Kaynak; Kazancı İçtihat Programı).

[508] Soyaslan, *B.A.Suçlar*, s.1578.

[509] Taşkın, *Bilişim Suçları*, s.28; Taşdemir, s.274.

Verilere zarar verme suçunun taksirle işlemesi mümkündür.[510] Örneğin bilişim sisteminin bakımını yapan teknik hizmet görevlilerinin, bakım yaparken hatayla, istemeden sistemdeki verileri bozması mümkündür. Ancak yasa metninde fiilin taksirli hali için yaptırım öngörülmediğinden, TCK 22/1 (taksirle işlenen fiillerin açıkça belirtilmesi hususu) gereğince de bu örnekteki fiil dolayısıyla teknik hizmet görevlilerine herhangi bir ceza verilemeyecektir.

2.3.2.6. Hukuka Aykırılık Unsuru

244/2. fıkrada düzenlenmiş olan suçlar hukuka aykırı bir fiille gerçekleştiğinde cezalandırılabilmektedir. Bu suç türünde hukuka uygunluk nedenlerinden; veriler üzerinde tasarruf yetkisi olan hak sahibi kişinin rızası, yasa hükmünü icra ve yetkili amirin emrini icra sözkonusu fiilleri suç olmaktan çıkartır.[511]

Hak sahibinin rızası doğrultusunda, bilişim sisteminin yapılandırılması, sistem güvenliği için internete erişimi engelleyen bir program yerleştirilmesi, verileri kurtarabilmek için bazı sistem dosyalarını silmek veya format atarak tüm verileri silmek gibi fiiller, hukuka aykırı olmadıkları için suç oluşturmayacaklardır.[512] Yasa hükmünü icra olarak hâkim kararıyla "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" işlemi kapsamında şüphelinin iletişim, e-posta kayıtlarının kayda alınması ve bu işlemi amirinin emriyle yerine yetiren görevlinin faaliyetleri suç oluşturmayacaktır.[513]

2.3.2.7. Suçu Etkileyen Neden / Daha Ağır Cezayı Gerektiren Hal

244. maddede herhangi bir ceza indirimi öngörülmezken, *maddenin 3. fıkrasında*, ilk iki fıkrada tanımlanan fiillerin "*bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali*" bir ağırlatıcı sebep olarak kabul edilmiş ve verilecek cezanın artırılması öngörülmüştür.

Kişisel bir bilgisayarın saldırıya uğrayıp belirli bir süre çalışmaması ile bir kamu kurumuna ait bir sistemin belirli bir süre çalışmaması sonucu ortaya çıkan

---

[510] Aksi yönde görüş, Soyaslan, ...*Özel Hükümler*, s.622, Yaşar-Gökcan-Artuç, s.6766.

[511] Kızıltan, s.85; Taşkın, *Bilişim Suçları,* s.50-52.

[512] Taşdemir, s.269; Kurt, s.174; Bayındır, s.75-76.

[513] Erdoğan, s.201; Yaşar-Gökcan-Artuç, s.6767.

zararlar arasında ciddi farklar olacaktır. Adalet Bakanlığı'nın UYAP (Ulusal Yargı Ağı Projesi), Nüfus ve Vatandaşlık Genel Müdürlüğü'nün MERNİS (Merkezi Nüfus ve İdare Sistemi), Tapu ve Kadastro Genel Müdürlüğü'nün TAKBİS (Tapu Kayıt ve Bilgi Sistemi) gibi kamuya ait sistemlerin ve bankacılık işlemlerinin aksatılması toplumun çok sayıda ferdini olumsuz olarak etkileyeceğinden, bu hallerde uygulanacak yaptırımda artırım yapılması yerinde olmuştur. Bu bağlamda bazı özel yasalarda da 244'ncü maddeye atıf yapılmıştır.[514]

2.3.2.8. Suçun Özel Görünüş Biçimleri

2.3.2.8.1. Teşebbüs

İkinci fıkra açısından, fail bilişim sistemindeki *verileri bozmak, yok etmek, değiştirmek veya erişilmez kılmak, sisteme veri yerleştirmek, verileri başka bir yere göndermek* amacıyla harekete geçip kendi iradesi dışında amacına ulaşamazsa ve herhangi bir zarar meydana gelmemişse suç teşebbüs aşamasında kalmış demektir.[515]

Bu fıkrada seçimlik 6 fiil sözkonusu olduğu için yasada öngörülen fiillerden birinin neticelenmesi halinde diğer fiiller teşebbüs aşamasında kalsa dahi suç tamamlanmış olacağı[516] için faile yaptırım uygulanacaktır.[517]

2.3.2.8.2. İştirak

Fıkra kapsamındaki suçlar iştirak açısından farklı bir özellik göstermez. Ceza yasamızda öngörülen iştirak çeşitleri (m.37 - 40) somut olaya göre uygulanacaktır.

2.3.2.8.3. İçtima

İkinci fıkradaki suçun, aynı suç işleme kararıyla, farklı kısa zaman aralıklarıyla aynı kişi veya kuruma karşı birden fazla zincirleme şekilde işlenmesi

---

[514] Örneğin, 5411 sayılı Bankacılık Kanunu'nun 157. maddesinde Bankacılık Kanunu'na tabi kuruluşların bilişim sisteminin engellenmesi, bozulması, verilerinin yok edilmesi veya değiştirilmesi suçları açısından TCK 244. maddesi kapsamında olduğu ifade edilmiştir.

[515] Yaşar-Gökcan-Artuç, s.6767-6768; Soyaslan, ...*Özel Hükümler*, s.622; Bayındır, s.76; Taşkın, *Bilişim Suçları,* s.53-54; Parlar, s.27.

[516] "*Bilişim sistemindeki* ***verileri değiştirmek suretiyle*** *haksız menfaat elde edilmesi suçunun* ***sanık tarafından EFT'nin şikâyetçi şirketin hesabından sahte olarak açtırmış olduğu hesaba intikali anında tamamlandığı gözetilmeyerek*** *eylemin teşebbüs aşamasında kaldığından bahisle eksik ceza tayini aleyhe temyiz olmadığından bozma sebebi sayılmamıştır.*" (11.CD. E.2007/2168 - K.2007/4372, 25.06.2007), (Kaynak; Yılmaz, ...*Bilişim Alanındaki Suçlar,* 47 numaralı dipnot, s.79.)

[517] Kızıltan, s.86.

mümkündür.[518] 244. maddenin ikinci fıkrasında düzenlenen verilere yönelik eylemlerden birisinin yapılmasıyla suç oluşur. Sözkonusu bu eylemlerin birden fazlasının gerçekleştirilmesi suç çokluğuna neden olmaz, eyleme tek suç nedeniyle yaptırım uygulanır.[519]

Fail TCK m.243/1 ile m.244/2 hükümlerini aynı anda ihlal ederse, başka bir ifade ile bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girerek, orada kalmaya devam eden fail, aynı zamanda bilişim sistemindeki verilere de zarar verirse, fikri içtima hükümleri gereği faile 244/2. hükümleri uygulanmalıdır.[520]

Failin ikinci fıkradaki hareketleri yapmakla asıl amacının dördüncü fıkrada düzenlenen haksız çıkar elde etmek olduğu belirlenmişse faile dördüncü fıkradaki yaptırım uygulanır. Bu durumlarda faile ayrıca ikinci fıkra hükümleri uygulanmaz.[521]

2.3.3. BİLİŞİM SİSTEMİNİ KULLANARAK HAKSIZ YARAR SAĞLAMA SUÇU (m.244/4)

244. maddenin dördüncü fıkrasında, bir kimsenin bir bilişim sisteminin işleyişini engellemesi veya bozması ya da bir bilişim sistemindeki verileri bozması, yok etmesi, değiştirmesi, erişilmez kılması, sisteme veri yerleştirmesi, var olan verileri başka bir yere göndermesi yoluyla, kendisine veya başkasının yararına *haksız bir çıkar sağlaması durumunda fiilin başka bir suçu oluşturmaması haline yönelik bir yaptırım* düzenlenmiştir. Burada önemli olan husus fiilin 244/4. fıkra kapsamına girebilmesi için, anılan fiile başka bir maddede ceza öngörülmemiş olmasıdır. Bu nedenle bu fıkra hükmü tali norm niteliğindedir.[522] Bu hükmün uygulanabilmesi için fiil başka bir suç oluşturmamalıdır. 244/4. fıkra ile birlikte uygulanma ihtimali olan suçlar; zimmet, dolandırıcılık, hırsızlık ve güveni kötüye kullanma gibi suç

[518] Taşkın, *Bilişim Suçları*, s.54; Bayındır, s.76; Artuk-Gökçen-Yenidünya, s.727.

[519] Yaşar-Gökcan-Artuç, s.6768 – 6769.

[520] Erdoğan, s.202-203.

[521] Yaşar-Gökcan-Artuç, s.6769.

[522] Yılmaz, *...Bilişim Alanında Suçlar*, s.86.

türleridir.[523] Bu fıkra 765 sayılı ETCK'nın 525/b-2. fıkrasını karşılamak üzere düzenlenmiştir.[524]

Dördüncü fıkra, 244. maddenin ilk iki fıkrasında belirtilen eylemlerin bazı geleneksel suç biçimleriyle karşılanamayacak olması halinde, boşluk yaratmamak ve anılan fiillerin cezasız kalmaması için düzenlemiştir.[525] Fıkradaki fiilin başka bir suça vücut vermesi halinde bu hükmün tatbik edilmeyeceği düzenlemesiyle yasa koyucu bağımsız bir suç türü oluşturmuştur. Bu düzenleme başka bir suçun ağırlaştırıcı hali de değildir.[526]

Sözkonusu düzenleme ile AKSSS'nin 8. maddesinde *"Sahtekârlık yoluyla **kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme** veya erişilemez kılma"* şeklinde ifade edilerek yaptırıma bağlanması istenen eylemler ceza yasamıza 244/4. fıkra olarak girip iç hukukumuzda yaptırıma bağlanmıştır.[527]

Bu fıkra kapsamına girebilecek suça örnek olarak; internet ortamında yapılan açık artırmaya müdahale edilerek haksız menfaat temin edilmesi, bankada hesabı olan mağdurun internet şifresi ele geçirilerek menfaat temin edilmesi gibi eylemler gösterilebilir.[528]

2.3.3.1. Korunan Hukuki Değer

244. maddenin 4. fıkrasındaki suçun oluşabilmesi için mağdur aleyhine bir zarar meydana gelmiş olmalıdır.[529] Bu zarar maddi zarar olabileceği gibi manevi

---

[523] Soyaslan, ...*Özel Hükümler*, s.624.

[524] Ergün, s.99; Bayındır, s.78;

[525] Eker, s.127.

[526] Erdoğan, s.246-247.

[527] Artuk-Gökcen-Yenidünya, s.728.

[528] Bayındır, s. 79.

[529] "*Gerçek bir kişiyle karşı karşıya gelmeden, yüz yüze veya telefon, bilgisayar, bilgi geçer gibi bir başka vasıta kullanılarak görüşmeden, konuşmadan, hileli davranışlarla gerçek kişiler dolandırılmadan **sadece bilişim sistemi kullanılarak doğrudan doğruya çıkar sağlanması halinde bilişim sistemine girerek haksız çıkar sağlama suçu gerçekleşecektir.** ... Somut olayda oluşa uygun kabule göre; Kayseri PTT Müdürlüğü Otomasyon Bölümünde bilgisayar teknisyeni olarak görev yapan sanık M.Ö.Ö ile Kayseri'de bulunan özel bir*

zarar da olabilir. Bu nedenle korunan hukuki değer özel hayatın gizliliğinden malvarlığı haklarına kadar geniş bir yelpazede mağdurların maddi ve manevi haklarıdır.[530]

2.3.3.2. Suçun Konusu

Dördüncü fıkrada düzenlenen kendisinin veya başkasının lehine hukuka aykırı haksız bir çıkar sağlanması suçunun konusu *haksız yarar* elde edilmesidir. Bu *haksız çıkar* bilişim sistemi veya sistemdeki veriler üzerinde bulunan maddi veya manevi[531] nitelikte her tür çıkar olabilir.[532]

2.3.3.3. Fail ve Mağdur

Herkes bu suçun fail ve mağduru olabilir.[533] Mağdur failin müdahalede bulunarak haksız menfaat sağladığı bilişim sistemi veya sistemdeki veriler üzerinde hak sahibi olan kimse veya kimselerdir.[534] Üzerinde işlem yapılan bilişim sisteminin maliki ile hak sahibi her zaman aynı kişiler olmayacağı için sistem malikinin rızasına rağmen, hak sahibi mağdur olabilir. Örneğin aldığı izinle bir üniversitenin bilişim sistemine giren failin, aralarında husumet olduğu bir akademisyenin sistemde tek nüsha halinde yüklü bulunan doktora tezi çalışmasını kasten yok ederek manevi bir yarar sağlaması durumunda bilişim sisteminin maliki sistemden zarar görmediği için

---

dershanede öğretmen olan diğer sanık A... K...'nın fikir ve eylem birliği içersinde hareket ederek, ... PTT on-line sistemi veri tabanına girilmek suretiyle rakam ilave edilerek ödeme merkezlerince, gerçekte havale edilenden 10 veya 100 kat fazla tutarda ödeme yapılmasını sağlayarak ***haksız menfaat temin eden sanıkların eylemlerinin tamamen bilişim ortamında gerçekleştirilmiş olması, gerçek kişiye karşı yöneltilen her hangi hileli bir davranışın bulunmaması nedeniyle*** *765 sayılı TCK.nun 525/b-2 maddesindeki* ***(5237 sayılı TCK.nun 244/4 md) bilişim suçunu oluşturacağı gözetilmeden*** *yazılı şekilde hüküm kurulması ...*" (11.CD. E.2008/11060 - K. 2009/11936, 12.10.2009) (Kaynak; Akarslan, H., http://www. bilgisayarpolisi.com/index.php?sayfa=makaleoku & kategori= "*Bilişim Suçu Kavramı"*, çevrimiçi, Erişim; 07.03.2011).

[530] Ali Parlar, Muzaffer Hatipoğlu, *5237 Sayılı TCK'da Özel ve Genel Hükümler Açısından Asliye Ceza Davaları,* Ankara, Adalet Yayınevi, 2008, s.857; Çekiç, s.115.

[531] Örneğin bir kimsenin bilişim sistemi aracılığıyla reyting ölçen alete girerek kendi programının reytingini olduğundan yüksek göstermesi durumunda manevi yarar da vardır. Yaşar-Gökcan-Artuç, s.6763.

[532] Yılmaz, *...Bilişim Alanında Suçlar*, s.87; Soyaslan, *B.A.Suçlar*, s.1582; Erdoğan, s.255.

[533] Artuk-Gökçen-Yenidünya, s.729; Parlar-Hatipoğlu, *...Asliye Ceza Davaları,* s.857.

[534] Erdoğan, s.253.

mağdur olmazken, doktora tezinin sahibi olan kişi mağdur olabilecektir.[535] Tüzel kişi yararına haksız menfaat temin edilmişse tüzel kişi aleyhine güvenlik tedbirleri uygulanacaktır.[536]

2.3.3.4. Maddi Unsurlar

2.3.3.4.1. Hareket

Fiilin bu fıkra kapsamına girebilmesi için ikisi olumlu, biri olumsuz olan üç hususun aynı anda gerçekleşmiş olması gerekir. Bu hususlardan ilki, 244. maddenin birinci ve ikinci fıkrasında sayılan sekiz adet fiilden birinin fail tarafından gerçekleştirilmiş olmasıdır. Bu fiiller seçimlik hareketli suçlardır. Failin sözkonusu fiillerin birini veya birkaçını birden işlemesinin önemi yoktur.

İkinci olarak failin bu eylemleriyle kendisine veya bir başkasına haksız bir çıkar elde etmiş olması gerekmektedir. Bu çıkar maddi veya manevi bir çıkar olabilir.

Son olarak anılan fiillerin birisi veya birkaçı ile haksız çıkar elde edilmiş olsa dahi, anılan fiil ile bir başka suç gerçekleşmemiş olmalıdır. Anılan fiiller sonucunda haksız bir menfaat edilmiş olsa bile bu fiille dolandırıcılık, zimmet, güveni kötüye kullanma ve hırsızlık gibi başka bir suç oluşmuşsa bu fıkra uygulanmayacak, fail o suçun düzenlendiği madde uyarınca cezalandırılacaktır.[537]

2.3.3.4.2. Netice

Dördüncü fıkra açısından neticenin gerçekleşmesi için hukuka aykırı haksız maddi veya manevi nitelikte bir yarar sağlanmış olmalıdır. Failin elde ettiği yararı kimin için elde ettiğinin önemi yoktur.[538] Fail bir yarar elde ederken, mağdurda herhangi bir zarar oluşması şart değildir. Fakat bilişim sistem ve/veya verilerine karşı yapılan eylemler ile elde edilen haksız menfaat arasında uygun bir illiyet bağı da bulunması gerekir.[539]

---

[535] Çekiç, s.118.

[536] Yaycı, s.93; Çekiç, s.103.

[537] Meran, s.373-374; Ergün, s.98-99; Dülger, s.246; Yaşar-Gökcan-Artuç, s.6763-6764; Bayındır, s.78-79.

[538] Meran, s.374; Soyaslan, ...*Özel Hükümler*, 625-626.

[539] Erdoğan, s.253.

2.3.3.5. Manevi Unsur

244/4. fıkranın manevi unsuru olarak doktrinde bizim de katıldığımız ağırlıklı görüş "genel suç işleme kastının yeterli olduğudur."[540] Ancak "failin haksız menfaat elde etme özel amacıyla hareket etmesi gerektiğini ifade edenler de vardır."[541] Fail suç oluşturan eylemleri bilerek yapmalı, sağladığı çıkarın haksız olduğunu bilmelidir. Fiilin taksir sonucu meydana gelmesi halinde faile ceza verilmez.[542]

2.3.3.6. Hukuka Aykırılık Unsuru

Dördüncü fıkradaki düzenlemede suç konusu fiiller için ilk üç fıkraya atıf yapıldığı için yukarıda 244/1. ve 2. fıkralarda hukuka aykırılık unsuru konusunda ifade edilen hususlar burada da geçerlidir.

İlk iki fıkrada ifade edilen sekiz fiilde ancak hukuka aykırı olarak gerçekleştiğinde cezalandırılabilecektir. Bu suç türünde hukuka uygunluk nedenlerinden; veriler üzerinde tasarruf yetkisi olan hak sahibi kişinin rızası, yasa hükmünü icra ve yetkili amirin emrini icra sözkonusu fiilleri suç olmaktan çıkartır.[543] Bilişim sistemi sahibi ile hak sahibi kişinin rızasının farklı olduğu hususu dikkate alınarak her somut olayda hukuka uygunluk için rızayı mağdur kişinin vermiş olması aranmalıdır.[544]

2.3.3.7. Suçun Özel Görünüş Biçimleri

2.3.3.7.1. Teşebbüs

244. maddenin ilk fıkrasında ifade edilen "bilişim sisteminin engellenmesi, bozulması" ve ikinci fıkrasında düzenlenen "bilişim sistemindeki verilere zarar verilmesi" fiilleri sonucunda failin iradesine rağmen bir menfaat edememesi durumunda 244/4. fıkra açısından fiil tamamlanmamış teşebbüs aşamasında kalmış demektir. Failin uygun icra hareketlerini yapmasına rağmen hukuka aykırı yarar elde edememesi halinde fiil teşebbüs aşamasında kalmış demektir. Fıkra konusu fiiller

---

[540] Taşdemir, s.279; Soyaslan, ...*Özel Hükümler*, s.626; Esen, s.635; Meran, s.375; Erdoğan, s.256-258; Yaşar-Gökcan-Artuç, s.6766.

[541] Dülger, *Bilişim Suçları*, s.248; Parlar, s.27; Yılmaz, ...*Bilişim Alanında Suçlar*, s.89.

[542] Artuk-Gökçen-Yenidünya, s.731.

[543] Kızıltan, s.85; Taşkın, *Bilişim Suçları,* s.50-52.

[544] bkz. yuk. s.127, fail ve mağdur konusu.

seçimlik olduğu için bir fiilin tamamlanmış olmasıyla diğer fiiller teşebbüs aşamasında kalmış olsa dahi faile tamamlanmış suçtan yaptırım uygulanır.[545]

2.3.3.7.2. İştirak

Fıkra kapsamındaki suçlar iştirak açısından farklı bir özellik göstermediğinden ceza yasamızda öngörülen iştirak çeşitleri (m.37-40) somut olaya göre uygulanacaktır.

2.3.3.7.3. İçtima

Dördüncü fıkradaki suçun aynı suç işleme kararıyla, farklı kısa zaman aralıklarıyla aynı kişi veya kuruma karşı birden fazla zincirleme şekilde işlenmesi mümkündür.[546] 244. maddenin ilk iki fıkrasında düzenlenen bilişim sistemine ve verilere yönelik eylemlerden birisinin yapılmasıyla suç oluşur. Sözkonusu bu eylemlerin birden fazlasının gerçekleştirilmesi suç çokluğuna neden olmaz, eyleme tek suç nedeniyle yaptırım uygulanır.[547]

Fail TCK m.243/1 ile m.244/2 hükümlerini aynı anda ihlal ederse, fikri içtima hükümleri gereği faile 244/2 hükümleri uygulanmalıdır.[548] Failin birinci ve ikinci fıkradaki hareketleri yapmakla asıl amacının dördüncü fıkrada düzenlenen haksız çıkar sağlamak olduğu belirlenmişse faile dördüncü fıkradaki yaptırım uygulanır. Bu durumlarda faile ayrıca bir ve ikinci fıkra hükümleri uygulanmaz.[549]

Yargıtay Ceza Daireleri, önceleri somut olaylarda 244. maddenin 4. fıkrası ile hırsızlık (142/2-e), dolandırıcılık (158/1-f) gibi suçların bilişim sistemleri kullanılarak işlenmesi hallerinde birbirinden farklı kararlar vermekteydiler. Yargıtay 6. Ceza Dairesi bu tür olaylarda hırsızlık suçunun bilişim yoluyla gerçekleştirildiğini ifade ederek (142/2-e)'deki nitelikli hırsızlık suçunun oluştuğunu kabul ederken,[550]

---

[545] Çekiç, s.118; Yılmaz, *...Bilişim Alanında Suçlar*, s.89; Erdoğan, s.259-262.

[546] Taşkın, *Bilişim Suçları*, s.54; Bayındır, s.76; Artuk-Gökçen-Yenidünya, s.727.

[547] Yaşar-Gökcan-Artuç, s.6768 – 6769.

[548] Erdoğan, s.202-203.

[549] Yaşar-Gökcan-Artuç, s.6769.

[550] "*Bilişim sisteminin kullanılması suretiyle işlenen **hırsızlık suçunun**, sanık tarafından yakınanın hesabından paranın başkası hesabına havale edilmesi anında **tamamlandığı gözetilmelidir.**"* (6. CD. E.2008/555 – K.2008/12249, 02.06.2008), (Kaynak; Kazancı İçtihat Programı).

benzer olaylarda 11. Ceza Dairesi, bilişim unsurları kullanılarak haksız çıkar elde edildiği düşüncesiyle 244. maddenin 4. fıkrasının uygulanması gerektiği yönünde kararlar veriyordu.[551]

Neticede, Yargıtay Ceza Genel Kurulu 17.11.2009 tarihinde, *genel olarak bilişim sistemi kullanılarak çeşitli hesaplardan para çekilmesi olaylarında TCK'nın 142/2-e'deki nitelikli hırsızlık suçu hükümlerinin uygulanması gerektiğine* karar vererek Yargıtay Ceza Daireleri arasındaki yorum farklılığını gidermiştir.[552]

Anılan olayda 142/2. fıkra hükümlerinin uygulanacağı yönünde karar verilince, 244/4. fıkrada ifade edilen "*haksız bir çıkar sağlanması halinin başka bir suçu oluşturmaması şartı nedeniyle*" artık bu tür olaylarda 244/4. fıkranın uygulanmayacağı ortadadır. Dolayısıyla bu suç ile benzer hukuki değerleri koruyan diğer suç tipleri arasında fikri içtima hükümlerinin uygulanması mümkün değildir.[553] Başka oluşan suçun cezasının daha ağır ya da daha hafif olmasının bir önemi yoktur. Bu durumda 244/4. fıkra hükümleri değil, yasa metnindeki ifade nedeniyle diğer oluşan suçun hükümleri olaya uygulanacaktır.

---

[551] "*Sanığın, katılan MS'nin kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A.Bank A.Ş'nin Y. .. Şubesinde hesap açtırarak diğer katılan M Ç'nin bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan M Ç'ye yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle* ***5237 SY TCK'nın 244/4 maddesine uyan suçu oluşturduğu gözetilmeden,*** *vasıflandırmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması, bozmayı gerektirmiştir*." (11. CD. E.2007/8423 - K.2008/117, 22.01.2008), (11. CD. E.2008/22 – K.2008/1141, 28.02.2008), (11. CD. E.2008/23 – K.2008/1160, 28.02.2008), (11. CD. E.2007/5875 – K.2007/7637, 26.03.2007), (Kaynak; Yaşar-Gökcan-Artuç, s.6770-6783.)

[552] *"Sanığın; firari diğer sanık ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın internet bankacılık şifresini kullanmak suretiyle, banka şubesindeki hesabından 10.750 YTL 'yi, kendi adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylem, 5237 sayılı TCY'nın 142/2-e maddesinde düzenlenmiş bulunan* ***bilişim sistemi kullanılmak suretiyle hırsızlık*** *suçunu oluşturur."* (YCGK. E.2009/11-193, K.2009/268, 17.11.2009), (Kaynak; Yaşar-Gökcan-Artuç, s.6770-6783).

[553] Çekiç, s.120; Soyaslan, ...*Özel Hükümler*, s.627; Yaşar-Gökcan-Artuç, s.6769.

2.4. BANKA VEYA KREDİ KARTLARININ KÖTÜYE KULLANILMASI SUÇU (m.245)

Ülkemizde bilişim alanında en çok rastlanan suç türü olan banka veya kredi kartlarının kötüye kullanılması suçuna yönelik ETCK'da bir düzenleme yoktu.[554] ETCK döneminde mahkemeler tarafından banka veya kredi kartıyla işlenen suçlar hakkında hırsızlık, dolandırıcılık gibi farklı kararlar veriliyordu. Bu sorun YCGK'nun 10.04.2001 tarih ve E.2001/6-30- K.2001/57 sıra numarasıyla, bu tür fiiller sonucunda ETCK'nın 525b/2 maddesindeki "bilişim *sistemleri aracılığıyla hukuka aykırı yarar elde etme*" suçu oluşacağı yönündeki içtihadıyla giderilmeye çalışıldı.[555] Ancak bu kez de suçta kullanılan kartın "ele geçiriliş" ve "kullanılış" şekline göre klasik "dolandırıcılık"[556] suçunun mu ya da "bilişim sistemleri aracılığıyla hukuka aykırı yarar elde etme" suçunun mu oluştuğu yönünde tartışmalar başlamıştır.[557] Söz konusu içtihattan sonra banka veya kredi kartının kötüye kullanılması fiilleri mahkemeler önüne o kadar çok geldi ki neredeyse 525b/2 maddesi başka bir fiil için kullanılmaz oldu. Bu nedenle uygulamada çok sık karşılaşılan bu fiiller için yeni TCK'da ayrı bir düzenleme yapılarak bu sorun giderilmeye çalışılmıştır. Yeni TCK'da bu alanda yapılan düzenlemeden sonra 1 yıl içinde alt derece mahkemelerinde 2102 dava açılmıştır.[558] Madde gerekçesinde de

---

554 ***"1990-2011 yılları arasında ülkemizde işlenen tüm bilişim suçlarının %57'si yaklaşık olarak 41.715'i banka ve kredi kartları aracılığıyla işlenmiş suçlardır."*** Çığır İlbaş, Mehmet Ali Köksal, "*Türkiye Bilişim Suçları Raporu",* İzmir II. Uluslararası Bilişim Hukuku Kurultayı, 17-19 Kasım 2011, Bildiriler Kitabı, (Editör, Tekin Memiş) İzmir, Aralık 2011, s.170; Kurt, *Bilişim Suçları,* s.181.

555 "*Sanığın haksız olarak ele geçirdiği bir başkasına ait kart ve şifreyi kullanarak bir bankanın iki farklı şubesindeki ATM makinesinden para çekip hukuka aykırı yarar sağlaması eyleminin, TCK.nun 493/2. maddesindeki* (nitelikli hırsızlık) *suçunu değil aynı Yasanın 525/b-2. madde ve fıkrasında düzenlenen,* ***bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu oluşturduğu***". (YCGK. E.2001/6-30 - K.2001/57, 10.04.2001), (Kaynak; Kazancı İçtihat Programı).

556 "*Bankanın maddi varlığı olan şikâyetçiye ait bankamatik kartının ATM makinesinde sıkışmasını sağlayıp banka görevlisiyle konuşturuyormuş gibi diğer sanık ile görüştürüp hileli hareketlerle öğrendiği şifresini kullanmak suretiyle işlenen* ***dolandırıcılık suçu*** *765 sayılı TCK'nun 504/3 maddesine uyar."* (11.CD E.2007/8430 - K.2007/8690, 03.12.2007), (Kaynak; Taşdemir, s.312).

557 Murat Volkan Dülger, *Bilişim Suçları ve Yeni Türk Ceza Kanunu,* **Kazancı Hukuk İşletme ve Maliye Bilimleri Dergisi**, S.5, Ocak 2005, s.116.

558 "*TCK 245. maddeye aykırı hareketlerden dolayı 01 Eylül 2007 ile 01 Eylül 2008 tarihleri arasında açılan dava sayısıdır.*" Budak, s.ii.

ifade edildiği üzere bu maddedeki düzenlemeler ile ağırlıklı olarak kişilerin malvarlığına ait eylemler yaptırıma bağlanmıştır. Bu nedenle bu suç türlerinin ceza yasamızda "topluma karşı suçlar" kısmında değil de "kişilere karşı suçlar" kısmında yer alması ceza yasamızın sistematiği açısından daha uygun olurdu.[559]

245. maddede ceza yasası yürürlüğe girdikten sonra iki değişiklik yapılmıştır. İlk değişiklikle yasanın yürürlüğe girmesinden hemen sonra 29.06.2005 tarihinde 5377 sayılı yasa ile metne 2. ve 4. fıkralar eklenmiştir. İkinci değişiklik ise uygulamada ortaya çıkan sorunları gidermek amacıyla, 06.12.2006 tarihinde 5560 sayılı kanun ile maddeye 5. fıkra eklenerek yapılmıştır.

Maddenin birinci fıkrasında "*başkasına ait banka veya kredi kartını ele geçiren kişilerin, anılan kartı, sahibinin rızası dışında kullanarak veya kullandırarak kendisi veya başkası lehine yarar sağlaması*" hali, ikinci fıkrasında; "*başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretilmesi, devredilmesi, satılması, satın alınması, kabul edilmesi*" hali; üçüncü fıkrasında "*sahte oluşturulan veya sahtecilik yapılan banka veya kredi kartı kullanılarak menfaat sağlanması*" hali suç olarak düzenlenerek yaptırıma bağlanmıştır. Maddenin dördüncü fıkrasıyla *"yakın akrabalar arasında bu suçun işlenmesi şahsi cezasızlık hali"* olarak öngörülürken, son maddesiyle birinci fıkra kapsamındaki suçlar için "*etkin pişmanlık*" imkânı getirilmiştir. 245. maddedeki düzenlemenin daha iyi anlaşılabilmesi için, anılan maddede suç vasıtası olarak gösterilen banka ve kredi kartları üzerinde durmakta yarar vardır.

Banka ve kredi kartları; 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun "Tanımlar" başlığını taşıyan 3. maddesinin d fıkrasında **Banka kartı;** "*mevduat hesabı veya özel cari hesapların kullanımı dâhil bankacılık hizmetlerinden yararlanmayı sağlayan karttır*" şeklinde tanımlanmıştır.

Banka kartları ülkemizde ilk kullanılmaya başlandığı 1987 yılında, sadece ATM'ler üzerinden hesap bakiyesi kadar para çekme imkânı verirken artık alışverişlerde hizmet ve mal alımı gibi işlemlerde de kullanılabilmektedir.[560] Bu bakımdan 01.03.2006 tarihinde yürürlüğe giren 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu (BKKKK)'ndaki banka kartı tanımının gelişen teknolojiyle birlikte

[559] Soyaslan, *B.A.Suçlar,* s.1586; Dülger, *Bilişim Suçları*, s.252.

[560] **Pano Dergisi**, Bankalararası Kart Merkezi (BKM), İstanbul, S.1. Ağustos 1997, s.2.

artık yetersiz kaldığını söylemek mümkündür. Dolayısıyla banka kartını; "*Mülkiyeti bir banka veya finans kurumuna ait olan, anılan kurumdaki vadesiz hesaba ulaşarak, hesap bakiyesi kadar POS cihazları (Satış Noktası Terminalleri, POS - Point of Sale) veya internet aracılığıyla mal veya hizmet alma olanağı veren, ATM'lerden para çekme, bakiye inceleme gibi hizmetlerde kullanılabilen bir karttır*" şeklinde tanımlayabiliriz.

Kredi kartı; Banka Kartları ve Kredi Kartları Kanunu'nun 3. maddesinin e fıkrasında "*Nakit kullanımı gerekmeksizin mal ve hizmet alımı veya nakit çekme olanağı sağlayan basılı kartı veya fiziki varlığı bulunmayan kart numarasını*" ifade eder şeklinde tanımlanmıştır.

Banka Kartları ve Kredi Kartları olarak uygulamada plastikten üretilmiş, fiziki varlığı olan kartlar kullanılmaktadır. Kredi kartını; "*Mülkiyeti bir banka veya finans kurumuna ait olan, kendisine kart verilen kişiyle anılan kurum arasında yapılan sözleşme gereğince, müşterilerine belirli bir kredi limiti dâhilinde üye işyerlerinden veya internet üzerinden mal veya hizmet satın alma veya ATM'lerden nakit çekme işlemlerinde kullanılabilen bir karttır*" şeklinde tanımlamamızın daha uygun olacağını düşünüyorum.

Banka ve kredi kartlarının fiziksel özellikleri ise şöyledir; kartların ön yüzünde; kart kullanıcısının adı ve soyadı, kartı çıkaran banka veya finans kuruluşunun logosu ve ismi ile kartın geçerlilik süresinin yanında sadece o karta ait olan 16 rakamlı kart numarası ve kartın irtibatlı olduğu hesap numarası bulunur. Kartların arka yüzünde ise bilgileri muhafaza eden manyetik şerit, imza bandı ve banka veya finans kuruluşuna ait telefon ve adres bilgileri yer alır.

Genel olarak kredi kartı ile banka kartının farkları şöyledir; kredi kartı, kart sahibine peşin para ödemeden alışveriş tarihi ile kredi kartı faturasının son ödeme tarihi arasında faizsiz kredi kullanma, borçlarını taksitle ödeme, ihtiyaç halinde nakit avans çekme veya sanal alanda alışveriş imkânı sunarken; banka kartı, aynı işlemleri kart sahibine hesabındaki bakiye ile sınırlı olarak sunmaktadır.[561] Son yıllarda banka kartlarına da nakit avans çekme imkânı verilmesiyle banka kartları ile kredi kartları arasındaki farklar çok azalmıştır. Kartların fiziksel farkları ise, banka kartları üzerindeki kart numarası, son kullanma tarihi ve kart sahibinin adının düz olmasına

[561] Taşdemir, s.314.

rağmen, kredi kartlarında bu bilgilerin kabartmalı olarak yazılmış olmasıdır. Ayrıca günümüzde üretilen kredi kartlarının üzerinde cep telefon sim kartlarına benzeyen küçük bir çip bulunmaktadır. Bu çip daha fazla bilgi muhafaza etmesinin yanında kredi kartı sahibine daha güvenli alışveriş için şifre kullanma avantajı da sağlamaktadır.[562]

Fail kendi kartını başka hesaplar ile ilişkilendirilerek maddede düzenlenen fiilleri gerçekleştirirse bu suç 245. madde kapsamında değerlendirilemez. Banka veya kredi kartı dışında kalan telefon kartı,[563] mağaza kartı, doğalgaz kartı, su kartı gibi kartlar üzerinde işlenen suçlar için de 245. madde hükümleri uygulanmaz.[564] Yargıtay Ceza Daireleri, telefon kartları ile işlenen suçların öncelikle "*hırsızlık*", sonrasında da "*karşılıksız yararlanma*" suçu kapsamına girdiği şeklinde birbirinden farklı kararlar verirken Yargıtay Ceza Genel Kurulu 19.06.2007 gün ve E.2007/6-136, K.2007/150 sayılı kararı ile telefon kartıyla işlenen bu tür fiillerin "*bilişim suçu*" olduğu ve 244/4. fıkranın kapsamına girdiği, dolayısıyla da 245. madde kapsamına girmediği yolunda içtihat oluşturmuştur.[565]

---

[562] Ahi, *Kredi Kartları Sahteciliği,* s.18.

[563] Veli Özer Özbek, (2007), "*Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m.245)",* **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, İzmir, C. IX, Özel sayı, s.1026.

[564] Yaşar-Gökcan-Artuç, s.6802.

[565] "*Sanıkların PTT'ye ait kullanılmış telefon kartlarının manyetik şerit bölümüne bant yapıştırıp yeniden konuşma yaptıklarının anlaşılması karşısında eylemlerinin TCK'nun 491/1* (**hırsızlık**) *maddesine uyduğunun gözetilmemesi*", (6. CD. E.2003/19684 - K.2005/7583, 15.09.2005), (Kaynak; Kazancı İçtihat Programı); "*Sanığın daha önceden yapmış olduğu eski ve görüşülmüş telefon kartlarının üzerindeki manyetik bölümlerine teyp bantları (şeffaf) yapıştırmak suretiyle bedava görüşme yaptığı, dolayısıyla Telekom Müdürlüğünü zarara soktuğu, kendi lehine menfaat sağladığı ... Sanığın eyleminin 765 Sayılı TCK. nun 521/b maddesindeki* ***karşılıksız yararlanma*** *suçunu oluşturduğu*," (11. CD. E.2005/7734, K.2006/8338, 19.10.2006), (Kaynak; Özbek, *...Kartların Kötüye Kullanılma Suçu*, 19 numaralı dipnot, s.1027);

"*Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasasının 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren* ***5237 sayılı Türk Ceza Yasasının 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır.***" (YCGK E.2007/6-136 - K.2007/150, 19.06.2007), (Kaynak; Kazancı İçtihat Programı).

2.4.1. GERÇEK BİR BANKA VEYA KREDİ KARTINI KÖTÜYE KULLANARAK HAKSIZ YARAR SAĞLAMA SUÇU (m.245/1)

2.4.1.1. Korunan Hukuki Değer

245. madde gerekçesinde bu düzenlemenin hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik fiillerinin tüm unsurlarını içermesine rağmen uygulamadaki duraksamalar ve içtihat farklılıklarını önlemek üzere bağımsız bir suç türü oluşturulduğu ifade edilmiştir.[566] Bu nedenle 245. madde ile genel olarak birçok hukuki değer korunmaya çalışıldığından, korunan hukuki değer karma nitelik taşımaktadır. Örneğin madde kapsamına giren hırsızlık, dolandırıcılık fiillerine karşı malvarlığı değerleri; sahtecilik fiillerine karşı kamunun belge ve kartlara olan güveni; güveni kötüye kullanma fiiline karşı da bilişim sisteminin sağlıklı ve güvenli bir şekilde işleyişi korunmaya çalışılmıştır.[567] Ticaret hayatı ve kamu güvenliği de korunan değerler arasındadır.[568]

2.4.1.2. Suçun Konusu

Suçun hukuki konusu banka kartları ya da kredi kartlarıdır.[569] Doktrinde bu madde kapsamındaki suçun hukuki konusunun "failin sağladığı hukuki yarar" olduğunu ileri sürenler de vardır.[570] Suçun konusu; üzerinde suçun oluştuğu, suç hareketinin kendisine yöneldiği ve ceza normunda belirtilen kişi veya şey iken, korunan hukuki değer suç tipinin oluşturulmasıyla korunmak istenen değerdir.[571] 245. madde düzenlemesiyle malvarlığı değerleri ve kamunun güveni korunmaya çalışılmaktadır. Bu nedenle 245/1. fıkranın konusunun banka ve kredi kartları olduğu

---

[566] Bayındır, s.85.

[567] Kurt, s.177-178; Taşdemir, s.318; Çekiç, s.121-122; Artuk-Gökçen-Yenidünya, s.734; Taşkın, *Bilişim Suçları*, s.83; Yaşar-Gökcan-Artuç, s.6798.

[568] Özbek, ...*Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1025; Erdoğan, s.300-301.

[569] Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1025; Artuk-Gökçen-Yenidünya, s.738; Meran, s.379; Erdoğan, s.309; Yaşar-Gökcan-Artuç, s.6799.

[570] Bu görüş için bkz. Dülger, *Bilişim Suçları*, s.253; Soyaslan, *B.A.Suçlar*, s.1586; Taşkın, *Bilişim Suçları*, s.65; Çekiç, s.123.

[571] Erdoğan, s.146.

kanaatindeyim. Ayrıca suç konusunun hem banka ve kredi kartları hemde para ve menkul değerler olduğunu ileri sürenler de vardır.[572]

2.4.1.3. Fail ve Mağdur

245/1. fıkrada düzenlenen suç türü açısından fail herkes olabilir. Yasada fail açısından farklı bir özellik öngörülmemiştir.[573]

Birinci fıkrada incelenen suç türü mağdur bakımından da farklı bir özellik göstermez. Herkes bu suçun mağduru olabilecektir. Suç fiili sonucunda malvarlığında azalma olan kişi mağdur durumdadır. Banka veya kredi kuruluşları ise oluşan suç nedeniyle bilişim sistemlerinin ve kartlarının güvenilirliği ile genel olarak ticari itibarları zarar gördüğünden mağdur sıfatıyla değil suçtan zarar gören sıfatıyla davalara katılabilirler.

Maddenin 1. fıkrasında birbirinden farklı olarak "kart sahibinden" ve "kartın kendisine verilmesi gereken kişi"den bahsedilerek mağduriyet açısından bir farklılık oluşturulmuştur. Kartların mülkiyeti banka, finans veya kredi kurumlarına ait olduğundan bu fıkrada mağdur kastedilerek kullanılan "kart sahibi" ifadesi uygun olmamıştır. Aslında burada "kart hamili" ifadesi kullanılsaydı ayrı ayrı "kart sahibi" ve "kartın kendisine verilmesi gereken kişiden" bahsedilmesine gerek olmazdı. Nitekim ceza yasamızdan sonra 01.03.2006 tarihinde yürürlüğe giren ve daha özel olan 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun "Tanımlar" başlıklı 3. maddesinin j fıkrasında ve yasa metninde "kart hamili" ifadesi kullanılmış ve Kart Hamili; "*Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişi*" olarak tanımlanmıştır.

Burada da ifade edildiği gibi "kart hamili" kartın sahibi değil yararlanıcısıdır. Zaten "kart kendisine verilmesi gereken kişi" de kartın hamilidir.[574] Ayrıca "kart hamili" ifadesiyle banka veya kredi kartından tüzel kişilerin de yararlanması halinde, tüzel kişiler de mağdur sıfatıyla CMK'nın tanıdığı haklardan yararlanabileceklerdir.

---

[572] Esen, s.643.

[573] Parlar-Hatipoğlu, s.1705.

[574] Erdoğan, s.306; Taşdemir, s.319; Bayındır, s.87.

2.4.1.4. Maddi Unsurlar

2.4.1.4.1. Hareket

245. maddenin ilk fıkrasında yaptırıma bağlanan fiil; başkasına ait banka veya kredi kartını, eline geçiren ya da elinde bulunduran kişinin, kart sahibinin veya kartın verilmesi gereken kişinin rızası olmaksızın kartı kullanması ya da başkalarına kullandırtması sonucu hukuka aykırı bir yarar sağlanmasıdır.

Madde metnindeki sıralamaya göre fiili inceleyelim. **Sahte olmayan bir kredi kartının kullanılması**; bu fıkrada ifade edilen suçtan söz edebilmek için fail tarafından gerçek bir kredi kartı kullanılmış olmalıdır. Eğer suç fiilinde kullanılan banka veya kredi kartı sahte ise, bu durumda bu fıkra değil duruma göre 245. maddenin ikinci veya üçüncü fıkralarının uygulanması söz konusu olabilecektir.[575]

Başkasına ait bir banka veya kredi kartı; fail tarafından kullanılan kart başkasına ait bir banka veya kredi kartı olmalıdır. Bir kimsenin kendisine ait banka veya kredi kartını bankanın bilgisi dışında alıp kullanması bu suçu oluşturmaz.[576]

Her ne suretle olursa olsun; ifadesiyle kastedilen suçun oluşumu açısından kartın ele geçiriliş, elde ediliş yönteminin önemli olmadığıdır. Banka veya kredi kartının fail tarafından nasıl ele geçirildiğinin bir önemi yoktur. Ele geçirme kart hamilinin rızasıyla olabileceği gibi, rızası dışında unutma, kaybedilen kartın ele geçirilmesi, hırsızlık, yardım etme bahanesi, kaybolma, çalınma, hileyle ele geçirme veya gasp şeklinde de olabilir. Neticede bu tür fiillerin hepsi bilişim suçu olarak değerlendirilecektir.[577]

"*Her ne suretle olursa olsun*" ifadesiyle, 765 sayılı ETCK döneminde Yargıtay tarafından kartın ele geçiriliş yöntemine göre bu suç türü için hırsızlık, dolandırıcılık ya da bilişim suçu oluştuğu şeklinde birbirinden farklı verilen

---

[575] Yaşar-Gökcan-Artuç, s.6802.

[576] a.g.e. s.6802.

[577] "*Sanığın misafir olarak gittiği* ***yakınanın evinde, çantasından çaldığı kredi kartı*** *ile değişik işyerlerinden alışveriş yapması"* (6.CD. E.2004/1306 – K.2006/9962, 17.10.2006), (Kaynak; Yaşar-Gökcan-Artuç, s.6804); "*Sanığın, yakınanın* ***ATM cihazında unuttuğu bankamatik kartıyla iki defa*** ... (nakit para) *çekip, günlük para çekme limitinin bu şekilde dolmasından sonra* (bir miktar parayı) *da kendi hesabına havale etmesi* " (6. CD. E.2003/18198 - K.2005/8516, 04.10.2005) gibi eylemler Yargıtay tarafından bilişim suçu sayılmaktadır. (Kaynak; Corpus İçtihat Programı).

kararların önüne geçilmek istenmiştir.[578] Ayrıca teknolojinin gelişmesiyle birlikte anılan suçun şu ana kadar işlenen şekillerinden farklı işleniş şekilleri de ortaya çıkabilecektir. Bu nedenle madde metninde yer alan "*her ne suretle olursa olsun"* ifadesiyle ortaya çıkabilecek yeni suç şekilleri de madde kapsamına gireceğinden sınırlama yapılmaması isabetli olmuştur.

Kartı ele geçirme ya da elinde bulundurma; ifadesiyle ele geçirme fiiliyle kart sahibinin haberi ve rızası olmadan, kartı bularak, çalarak, hile veya dolandırıcılıkla ya da yetkisi olmadan kartların elde edilmesi ifade edilmektedir. Elinde bulundurma ise ağırlıklı olarak ele geçirmeden sonraki süreci anlatmakla birlikte, kart sahibinin bilgisi ve izni dâhilinde[579] ya da yasal yetkilere uygun olarak kartları elinde bulundurmayı ifade eder. Bir bankada kartları teslim etmekle görevli olan personelde teslim edilecek kartların bulunması veya posta, kargo gibi yollarla kartları teslim edecek görevlide kartların bulunması bu durumlara örnek oluşturur.[580]

Kartın fiziki olarak ele geçmesi değerlendirildiğinde, genel olarak kartın fiziksel olarak ele geçirilmesinin gerekmediği görülmektedir.[581] Yargıtay'a intikal

---

[578] Taşkın, *Bilişim Suçları*, s.66; Artuk-Gökçen-Yenidünya, s.735, Örneğin; "*Müştekiye ait kredi kartını ele geçiren sanığın, bu kartı kullanarak 2 gün ara ile ATM'den para çekmesi eylemi, TCK.nun 493/2.* (**hırsızlık**) *ve 80. maddelerindeki suçu oluşturur".* (6. CD. E.1998/10848 - K.1998/10939, 26.11.1998), (Kaynak; YKD. Şubat-1999, s.268); "*Sanığın ... şikayetçinin bankamatik kartının ATM cihazına sıkışmasını sağlayıp yardım etmek bahanesiyle yaklaşarak bankaya ait izlenimini verdiği duvara monte ettiği telefonla banka görevlisi görüşüyormuş gibi ...arkadaşını arayıp ....banka görevlisi olduğunu söylediği arkadaşı ile telefonla görüştürerek bu kişi vasıtasıyla şifresini öğrendiği, ...sanığın arkadaşının kartın bloke edildiğini söylemesi üzerine şikayetçinin ATM cihazından ayrılmasından sonra, sanığın sıkışan kartı çıkartarak şikayetçinin hesabından ... para çektiğinin anlaşılmasına ...ve kabul edilmesine göre; sanığın şikayetçiye ait bankamatik kartını ve şifresinin hile ve desise yaparak öğrenmesi, telefon ve bankayı vasıta kılarak şikayetçinin zararına, kendi yararına haksız menfaat sağlaması nedeniyle eylemin TCK. nun 504/3. maddesine uygun* ***dolandırıcılık*** *suçunu oluşturduğu gözetilmeden*" (11. CD. E.2003/8507 - K.2004/5914, 29.06.2004), (Kaynak; Corpus İçtihat Programı); "*Sanığın sabit olan bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak yarar sağlama eylemi, TCK.nun 522/b-2* (**bilişim suçu**) *maddesinde öngörülen suçu oluşturur.*" (11. CD. E.1999/5477 - K.1999/8485, 06.12.1999), (Kaynak; YKD. Mart-2000, s.489).

[579] *"Üye işyeri sahibi olan sanığın,* ***şikayetçi tarafından hesap ödemek için verilen kredi kartı ile*** *alışveriş yapılmış gibi slip çekerek haksız yarar sağladığının anlaşılması karşısında; eylem, bir bütün halinde, suç tarihinde yürürlükte bulunan ve lehe olan 765 sayılı TCK'nın 525/b-2 (5237 sayılı TCK'nın 245/1) maddesinde öngörülen bilişim suçunu oluşturur."* (11. CD. E.2009/8505 - K.2011/685, 09.02.2011), (Kaynak; Corpus İçtihat Programı).

[580] Karagülmez, *Bilişim Suçları*, s.204-205.

[581] Aksi yönde görüş "*Bu suçun oluşması için kartın fiziksel olarak kullanılması zorunludur.*

eden bir olayda, kart fiziksel olarak ele geçirilmeden kredi kartı bilgilerinin kullanılmasıyla da anılan suçun oluştuğu kanaatine varılmıştır.[582] 11. Ceza Dairesi anılan kararında, BKKKK'nın 3/e maddesindeki kredi kartı tanımına atıf yaparak, tanımdaki "*basılı kartı veya fiziki varlığı bulunmayan kart numarası*" ifadelerine vurgulama yapmıştır. Gerçekten de bu tanımdan kredi kartına ait kart numarasının da kredi kartı olarak kabul edileceği ortadadır. Ancak BKKKK'daki banka kartı tanımında banka kartının "fiziki varlığının olmasından" bahsedilmemiştir. Bu durumda fiziksel olarak ele geçirilmeyen banka kartlarının 245. madde kapsamına girmeyeceği ileri sürülmüştür.[583] Ancak BKKKK'nın yürürlüğe girmesinden sonra bilişim teknolojilerindeki gelişmeler ve banka kartıyla hizmet ve mal satın alınmasının yanında, bu kartlara hesapta bakiye olmamasına rağmen avans kredi kullanma imkânının getirilmesiyle banka kartı ile kredi kartı arasında pek fark kalmamıştır. Dolayısıyla banka kartı fiziksel olarak ele geçirilmeden işlenen fiiller de 245. madde kapsamında değerlendirilmelidir.

Kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın kartın kullanılması; ifadesinde "kart sahibi" ibaresiyle kastedilen kartın hamili veya yararlanıcısıdır. Çünkü banka veya kredi kartlarının sahibi, kartı çıkaran banka, finans veya kredi kurumlarıdır. Nitekim BKKKK'da bu kart kullanıcıları için "kart hamili" ifadesi kullanılmıştır.[584]

Kartın kendine verilmesi gereken kişi ifadesiyle kredi kartı edinme talebine olumlu cevap verilerek adına kart üretilen, ancak kartı kendisine henüz ulaşmamış

Hükümde yer alan kartın kullanılması ya da kullandırılması *sadece karta ilişkin bilgilerin değil, bizatihi kartın kullanılması şeklinde anlaşılmalıdır."* Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, s. 1029.

[582] *"Sanıkların* ***yakınana ait kredi kartını fiziki olarak ele geçirmeden sadece kredi kartı numarasını kullanarak*** *bilişim sistemi üzerinden kontör satın alınması aynı sistem üzerinden başkalarına kontörlerin satılması eylemleri nedeniyle dava açıldığının anlaşılması karşısında; fiilin ... TCK.nun 245/1 ve 43. m.lerinde öngörülen zincirleme suretiyle banka ve kredi kartlarının kötüye kullanılması suçunu oluşturacağı ve eylemde sahte oluşturulmuş veya üzerinde sahtecilik yapılmış bir banka veya kredi kartından söz edilemeyeceği gözetilmeden, aynı maddenin 3. fıkrası ile uygulama yapılması"* bozma nedeni sayılmıştır. (11.CD. E.2008/12914 - K.2008/8887, 17.09.2008), (Kaynak; YKD Mayıs-2009, s.998).

[583] Yaşar-Gökcan-Artuç, s.6804.

[584] BKKKK m.3/J "*Kart hamili: Banka kartı veya kredi kartı hizmetlerinden yararlanan gerçek veya tüzel kişidir."*

kişi kastedilmektedir. Yasa koyucu, madde metnindeki "*kartın kendisine verilmesi gereken kişi*" ifadesiyle, kredi kartlarının hamiline ulaşmadan fail tarafından elde edilerek kullanılması fiillerini de bilişim suçu kapsamına dâhil edilerek tartışmalara son vermek istemiştir.[585]

Zira Yargıtay bu tür fiilleri bazen dolandırıcılık bazen bilişim suçu ve bazen de hem dolandırıcılık hem de bilişim suçu olarak değerlendiriyordu.[586] Dolandırıcılık olarak niteleme yapıldığında[587] suçtan zarar gören bankanın özel veya kamu bankası olup olmamasına göre olaya uyguladığı madde değişiyordu.[588] Banka personeli kartın tesliminde görevli değilse, suç dolandırıcılık olarak değerlendirilerek, mağdur kamu bankası ise ETCK md. 504/7 (nitelikli dolandırıcılık), özel banka ise ETCK md. 503/1 (basit dolandırıcılık) hükümleri uygulanmaktaydı. Banka personeli veya kargo personeli kartın tesliminde görevliyse, faile aynı zamanda güveni kötüye kullanma fiilinden de işlem yapılıyordu.[589]

Kartın ele geçirilmesi/elde edilmesi hamilin rızasıyla olabileceği gibi rızası dışında da olabilir. Mağdurun rızası, madde metninde de yer alan suçun kurucu unsurlarındandır.[590] Mağdurun rızası sakatlanarak gasp, hırsızlık, güveni kötüye

---

[585] Dülger, *Bilişim Suçları*, s.255; Kurt, *Bilişim Suçları*, s.185.

[586] *"... Bankası Saruhanlı Şubesinde güvenlik görevlisi olarak görev yapan sanığın şikayetçi adına düzenlenen kredi kartını ve şifresini haksız olarak ele geçirerek ATM'den bir kez para çektiği ve aynı kredi kartı ile iki kez de alışveriş yaptığı anlaşılmasına göre, ATM'den para çekme eyleminin TCK. nun 525/b-2 maddesindeki **bilişim suçunu**, kendisine ait olduğunu bildirerek kredi kartıyla iki kez alışveriş yapma eyleminin de aynı yasanın 504/3 ve 80. maddelerindeki **zincirleme dolandırıcılık suçunu oluşturduğu**, suç tarihi itibariyle bilişim suçunda 4616 sayılı Yasanın uygulanması ve dolandırıcılık suçundan da mahkumiyetine karar verilmesi gerektiği gözetilmeden*" (11. CD. E.2002/11255 - K.2002/8921, 13.11.2002), (Kaynak; Corpus İçtihat Programı).

[587] "*Özel tüzel kişi banka tarafından düzenlenen kredi kartlarının, adlarına düzenlenen kişilere teslim edilmeden, dağıtımını üstlenen kişi tarafından kullanılması **eylemi, doğrudan bankaya yönelik olması nedeniyle TCK 503/1 maddesindeki dolandırıcılık suçu**nu oluşturur.*" (6.CD. E.1999/2418, K.1999/2370, 26.04.1999), (Kaynak; Seza Reisoğlu, "*Banka Kredi Kartları ve Uygulama Sorunları",* **Bankacılar Dergisi**, Yıl 15, S.49, İstanbul, Haziran 2004, s.116.)

[589] Serkan Sazak, *Ceza Hukukunda Banka ve Kredi Kartlarının Kötüye Kullanılması,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, 2008, s.52; Dülger, *Bilişim Suçları*, s.257.

[590] Yaşar-Gökcan-Artuç, s.6804; Özbek, *...Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1031.

kullanma, dolandırıcılık gibi eylemler sonucu kartın ele geçirilme eylemi başka bir suçu da oluşturuyor ise failin bu suçtan da ayrıca cezalandırılacağı açıktır.[591]

Kartın fail tarafından kullanılarak veya kullandırılarak, kendisine veya başkasına yarar sağlanması; sadece banka veya kredi kartının ele geçirilmesi veya elde bulundurulmasıyla bu fıkradaki suç oluşmaz. Suçun tamamlanabilmesi için kart veya kart bilgileri kullanılarak ya da kullandırılarak hukuka aykırı maddi ekonomik bir yarar elde edilmesi gerekmektedir.[592] Madde metninde kullanmak veya kullandırmanın ne şekilde olacağı belirtilmediği, sınırlandırılmadığı için suç serbest hareketli bir suçtur. Suçun oluşumu açısından banka veya kredi kartının kullanılması işleminin fail veya anlaştığı/görevlendirdiği bir başka kişi tarafından yapılmasının farkı yoktur.[593]

Öte yandan kartı kaybolmadığı veya çalınmadığı halde, kartın hamili tarafından kartı çıkaran kurum aranarak ilgili kurum tarafından kart kullanıma kapatılıncaya kadar geçen kısa sürede, kart hamili fail veya anlaştığı bir başka kişi tarafından alışveriş veya nakit çekimi yapılması gibi durumlarda m. 245 hükümleri değil, dolandırıcılık hükümleri uygulanmalıdır.[594] Çünkü bu durumda eylemin kart hamilinin rızası doğrultusunda yapılması, bu fiili 245. madde kapsamından çıkarır.

---

[591] Sacit Yılmaz, "*...Kredi Kartlarının Kötüye Kullanılma Suçu",* **Türkiye Barolar Birliği Dergisi**, Y:22, S.87, Ankara, 2010, s.272-273; Yaşar-Gökcan-Artuç, s.6804; Esen, s.644.

[592] Yaşar-Gökcan-Artuç, s.6805; Erdoğan, s.306;

[593] *"Somut olayda; sanıkların aralarında anlaşarak sanık UA'nın işyerindeki Y. ve İ. bankasına ait POS cihazlarından,* ***sanık MK.'nın tanıdığı olan sanık FH. tarafından temin edilen yabancı bankalara ait sahte kredi kartlarının geçirilmesi suretiyle*** *alışveriş yapılmadığı halde yapılmış gibi gerçeğe aykırı bir biçimde sanık FH'nu borçlu, sanık UA'yı alacaklı olarak gösterip, sanık UA'nın Y. bankasındaki hesabına geçen ... lirayı aldığı, ...anlaşılıp kabul edilmesine göre, işyeri sahibi UA'nın da diğer sanıklarla birlikte bu suçu işlemesi nedeniyle kendisine yönelen bir hile ve desiseden söz edilemeyeceği, dolandırıcılık suçunun yasal unsurlarının oluşmadığı, sanıkların eylemlerinin bir bütün halinde TCK. nun 525/b-2, 80. maddelerinde öngörülen* ***bilişim suçunu oluşturduğu gözetilmeden****, bankaları dolandırmak hususunda anlaştıklarından bahisle, aynı kanunun 504/3. maddesinde yer alan banka vasıta kılınmak suretiyle dolandırıcılık suçundan hüküm kurulması, kanuna aykırı ... olduğundan hükmün bozulmasına"* (11. CD. E.2002/10428 - K.2002 /10395, 25.12.2002), (Kaynak; Corpus İçtihat Programı).

[594] Dülger, *Bilişim Suçları*, s.256; Özbek, ...*Kartların Kötüye Kullanılma Suçu*, s.1033; Yılmaz, ...*Kartların Kötüye Kullanılma Suçu*, s.273; Soyaslan, ...*Özel Hükümler*, s.631.

Nitekim Yargıtay uygulamaları da bu yöndedir.[595] 01.03.2006 tarihinde yürürlüğe giren 5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 37. maddesinde de bu tür fiiller için yaptırım öngörülmüştür.[596] Bu daha yeni ve daha özel yasa maddesi nedeniyle artık BKKKK sonrasında bu eylemlerin dolandırıcılık olarak değerlendirilemeyeceği düşüncesindeyim.[597]

2.4.1.4.2. Netice

Birinci fıkradaki fiilin neticesi; başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlamaktır. Kartın fail tarafından nasıl ele geçirildiğinin önemli olmadığı "*her ne suretle olursa olsun*" ibaresiyle belirtilmiştir. Fail tarafından kart mağdurun rızası dışında veya rızası ile de elde edilmiş olabilir. Ama sonuçta kartın kullanımı ile bir haksız bir menfaat elde edilmiş ve bir zarar ortaya çıkmış olmalıdır.[598] Zarar ile failin hareketleri arasında uygun illiyet bağı da olmalıdır. Zararın ortaya çıkması için fail tarafından, menfaatin bizzat elde edilmiş olmasına gerek yoktur. Örneğin, failin belirlediği hesaba, mağdurun hesabından havale işlemi yapıldığı anda, para failin hâkimiyeti altına girdiğinden suç tamamlanmış olur.[599]

2.4.1.5. Manevi Unsur

245/1. fıkrada ifadesini bulan gerçek bir banka veya kredi kartının kötüye kullanılması suçu için özel kast aranmadığından genel kastla işlenebilen bir suç

---

[595] *"Sanık hakkında Y... bankasından verilen K.K.'ya ait kredi kartlarıyla E.banktan verilen S.Ö'ye ait kredi kartını ele geçirerek çeşitli yerlerde kullanmaktan dolayı dava ikame edildiği anlaşılmaktadır. Kart sahibi K.K. 21.05.1997 tarihinde kartının kaybolduğunu ve Y. bankasına bildirmiş olması karşısında bildirdiği saat araştırılıp belirlenerek* ***alışverişlerin*** *bildirimden önce yapıldığının tespiti halinde, eylemin TCK'nın 504/3, 80. maddelerinin* ***sonra yapılmış olması halinde ise Y. Bankasının özel kuruluş olması karşısında TCK'nın 503/1, 80. maddelerinin uygulanması gerekeceği****nin gözetilmemesi karşısında*" (6. CD. E.1998/11178 – K.1998/11223, 03.12.1998.), (Kaynak; Dülger, *Bilişim Suçları,* 508 numaralı dipnot, s.256).

[596] BKKKK m.37. "*Banka kartı veya* ***kredi kartını kaybettiği ya da çaldırdığı yolunda gerçeğe aykırı beyanda bulunarak kartı bizzat kullanan veya başkasına kullandıran kart hamilleri ile bunları bilerek kullananlar*** *bir yıldan üç yıla kadar...*"

[597] Aynı yönde görüş için bkz. Taşkın, *Bilişim Suçları*, s.71; Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1033.

[598] Soyaslan, ...*Özel Hükümler*, s.630; Yaycı, s.114.

[599] "...***paranın açılan hesaplara transferiyle suçun tamamlanacağı gözetilmeden",*** (11. CD. E.2009/3700 – K.2009/6207, 12.05.2009), (Kaynak, Yaşar-Gökcan-Artuç, s.6792).

türüdür. Failin yasal düzenlemedeki unsurları bilerek ve isteyerek hareket etmesi yeterlidir.[600] Madde metninde yer almadığından fiilin taksirle işlenmesi mümkün değildir.

2.4.1.6. Hukuka Aykırılık Unsuru

Maddenin birinci fıkrasında öngörülen düzenlemedeki suçun oluşabilmesi için, banka veya kredi kartının failin rızası dışında kullanılması gerekir. Bu rıza, kart hamilinin veya kart kendisine teslim edilmesi gereken kişinin rızasıdır. Söz konusu rıza sadece kartın teslimi değil, kullanımı konusunda da olmalıdır.[601] Bu şartları taşıyan rıza fiili suç olmaktan çıkarır. Bazı durumlarda zorunluluk hali de, kusurluluğu ortadan kaldıracağı için fiili hukuka uygun hale getirir.[602] Örneğin; arkadaşlarıyla yurtdışı seyahate giden failin, uçağı kaçırıp ülkeye dönememesi ve üzerinde hiç para ve başka imkân kalmadığından, bir şekilde üzerinde kalmış olan bir arkadaşının kartını kullanarak ülkemize dönmesi durumunda ıztırar hali kusurluluğu ortadan kaldırır.[603]

2.4.1.7. Suçun Özel Görünüş Biçimleri

2.4.1.7.1. Teşebbüs

Birinci fıkrada tanımlanan suçların daha zarar ortaya çıkmadan teşebbüs aşamasında kalması mümkündür. Başkasına ait banka veya kredi kartını eline geçiren fail, söz konusu kartı kullanarak sonucu gerçekleştirmeye uygun hareketlerle icraya başlayıp elinde olmayan nedenlerle bir çıkar elde edemezse fiili teşebbüs aşamasında kalmış olur. Örneğin başkasına ait kredi kartını bir şekilde elde etmiş olan failin, kartla ATM cihazından para çekmeye çalışması ama başarılı olamaması veya bu sırada banka görevlilerince yapılan müdahale sonucu parayı çekememesi, söz konusu kartla mal ya da hizmet satın almaya çalışırken POS makinesinde işlem yapılmadan

---

[600] Taşdemir, 320-321; Meran, 382-383; Esen, s.648; Bayındır, s.91-92; Artuk-Gökçen Yenidünya, s.739; aksi yönde görüş Karagülmez, s.225; Dülger, *Bilişim Suçları*, s.262.

[601] Soyaslan, ...*Özel Hükümler*, s.635; Bayındır, s.92; Esen, s.649.

[602] Parlar, s.54; Kurt, s.194.

[603] Kurt, s.194-195.

durumun fark edilmesi gibi durumlarda zarar ortaya çıkmadığından suç tamamlanmış olmaz. Bu nedenle faile sadece 245/1 hükümleri teşebbüs yönünden uygulanır.[604]

2.4.1.7.2. İştirak

Birinci fıkranın suça iştirak açısından farklı bir özelliği yoktur.[605] Ceza Yasası'nın birlikte faillik (m.37), azmettirme (m.38), yardım etme (m.39) ve bağlılık kuralı (m.40) hükümleri çerçevesinde her somut olaya göre ayrı ayrı değerlendirme mahkemeler tarafından yapılacaktır.[606]

2.4.1.7.3. İçtima

Banka veya kredi kartlarının kötüye kullanılması fiillerinin içtima açısından farklı bir özelliği yoktur. TCK'da da tanımlandığı şekilde failin bir suç işleme kararaıyla, değişik zamanlarda aynı kişiye karşı fıkranın hükümlerini birden fazla işlemesi halinde, faile gerçekleşen zincirleme suç gereğince ceza verilir ve verilen cezada 1/4–3/4 oranları arasında artırım yapılır.[607] Failin birden fazla eylemi sonucunda her suç tamamlanmış olabileceği gibi, suçun biri tamamlanmış diğeri teşebbüs aşamasında kalmış veya iki suç ta teşebbüs aşamasında kalmış olabilir.[608]

Birinci fıkra açısından, failin ele geçirmiş olduğu kart birden fazla ise ve kartları ayrı ayrı bir seferden çok kullanmışsa her kart için kendi içinde zincirleme suç hükümleri uygulanacaktır.[609] Yargıtay uygulamaları da bu yöndedir ve her kart için ayrı bir suç işlendiği yorumuyla hükümler kurulmaktadır.[610]

---

[604] Erdoğan, s.319-320; Dülger, *Bilişim Suçları*, s.263; Bayındır, s.93; Taşdemir, s.321.

[605] Yaşar-Gökcan-Artuç, s.6817, Bayındır, s.91-92; Dülger, *Bilişim Suçları* s.263.

[606] "*Sanık A.M. ile M. K.'nın başkasına ait kredi kartını birden fazla iş yerinde kullanarak çıkar sağlamaları nedeniyle haklarında TCK'nun 43. maddesinin uygulanmaması, sanık H.F.'nin suçun işlenmesindeki rolü suça olan katkısı, fiilin işlenişi üzerinde kurduğu hakimiyet dikkate alındığında* ***müşterek fail olduğu gözetilmeden, yazılı şekilde suça yardım eden olarak kabulüyle eksik ceza tayini*** *karşı temyiz olmadığından bozma nedeni yapılmamıştır."* (11. CD. E. 2006/5011 - K. 2006/9392, 22.11.2006), (Kaynak; Esen, s.657).

[607] "*Suça konu kredi kartı* ***birden fazla işyerinde kullanılarak*** *haksız çıkar sağlandığı halde TCK 43. maddesinin uygulanmaması*," (11. CD E.2008/14622 - K.12423, 25.11.2008), (Kaynak; Yılmaz, ...*Kredi Kartlarının Kötüye Kullanılması Suçu,* 68 numaralı dipnot, s.285).

[608] Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* s.285.

[609] Yaşar-Gökcan-Artuç, s.6818.

[610] "*Hukuka aykırı kullanılarak banka veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek amacıyla 5237 sayılı Yasa'da düzenlenen* ***banka veya kredi kartlarının kötüye kullanılması suçu*** *hükmün, düzenleme amacı ve düzenleniş biçimi ile*

Fail başkalarının banka veya kredi kartını hırsızlık, dolandırıcılık, güveni kötüye kullanma ve yağma gibi suçları işleyerek ele geçirmişse bu durumda gerçek içtima sözkonusu olur ve faile hem kartı ele geçirme işlemi sırasında işlediği suçtan ve hem de 245/1. fıkradan yaptırım uygulanır.[611]

2.4.2. BAŞKA HESAPLARLA İLİŞKİLİ SAHTE BANKA VEYA KREDİ KARTI ÜRETMEK, SATMAK, DEVRETMEK VEYA KABUL ETMEK SUÇU (245/2)

2.4.2.1. Korunan Hukuki Değer

245/2. fıkradaki düzenlemeyle de birçok hukuki değer korunmaya çalışıldığından, korunan hukuki değer karma nitelik taşımaktadır. Fıkra ile malvarlığı değerleri, kamunun belge ve kartlara olan güveni, bilişim sisteminin sağlıklı ve güvenli bir şekilde işleyişi korunmaya çalışılmıştır.[612] Fıkrada sahtecilik suçları özellikleri de bulunduğu için kamuya duyulan güven ve itibar da korunmaktadır.[613]

2.4.2.2. Suçun Konusu

Suçun hukuki konusu ikinci fıkra açısından da banka kartları ya da kredi kartlarıdır.[614] Ancak bu kartlar başka banka hesaplarıyla ilişkilendirilmiş sahte banka veya kredi kartlarıdır. Kartlar gerçek ise bu fıkra değil birinci fıkra hükümleri uygulanır.[615]

---

korunan hukuki menfaat gözetildiğinde ***kart sayısınca oluştuğu halde*** *yazılı şekilde TCK.nun 245. maddesi ile bir kez uygulama yapılarak eksik ceza tayini…",* (11. CD. E.2006/5243 - K.2006/7374, 20.09.2006), (Kaynak; Nazif Kaçak, *Yeni İçtihatlarla Yeni Türk Ceza Kanunu,* Ankara, Seçkin Yayınevi, 2007, s. 620-621).

[611] "***Sanığın misafir olarak gittiği yakınanın evinde, çantasından çaldığı kredi kartı ile değişik işyerlerinden alışveriş yaptığının anlaşılması karşısında****; yakınana ait kredi kartını çalma eyleminin 765 sayılı TCY.nın 491/3.* ***(5237 sayılı Yasanın 142/1-b) maddesine uyan hırsızlık suçunu ve bu kartla değişik işyerlerinden alışveriş yapma eyleminin aynı Yasanın 504/3, 80. (5237 sayılı Yasanın 245/1) maddelerine uyan suçu oluşturup oluşturmadığına ilişkin*** *kanıtları takdir ve değerlendirmenin üst dereceli Ağır Ceza Mahkemesine ait olduğu gözetilmeyerek, görevsizlik kararı yerine, duruşmaya devamla yazılı biçimde karar verilmesi*", (6. CD. E.2004/1306 – K.2006/9962, 17.10.2006), (Kaynak; Yaşar-Gökcan-Artuç, 1249 numaralı dipnot, s.6819).

[612] Soyaslan, *Ceza Hukuku Özel Hükümler*, s.629; Artuk-Gökçen-Yenidünya, s.735.

[613] Bayındır, s.85; Taşkın, *Bilişim Suçları* (Tez), s.74.

[614] Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1025; Artuk-Gökçen-Yenidünya, s.738; Meran, s.379; Erdoğan, s.309; Yaşar-Gökcan-Artuç, s.6799.

[615] Erdoğan, s.338.

2.4.2.3. Fail ve Mağdur

245. maddenin ikinci fıkrası için fail ve mağdur açısından farklı bir özellik yoktur. Suçun fail ve mağduru herkes olabilir. "Sahte banka veya kredi kartı üretimi ve diğer fiillerde" anılan kartlar henüz kullanılmadığından bu fıkra açısından suçun mağdurunun hesap sahibi kişi olmayıp, banka veya kredi kartını çıkartma yetkisine sahip banka veya kredi kuruluşlarının olacağı yönünde Yargıtay kararları mevcuttur.[616]

2.4.2.4. Maddi Unsurlar

2.4.2.4.1. Hareket

245. maddenin ikinci fıkrası TCK'nın ilk halinde yer almamış ve 5377 sayılı kanunla 29.06.2005 tarihinde eklenmiştir. Bu ek maddedeki düzenlenmenin amacı TBMM Adalet Komisyonu raporunda; "*Başkalarına ait banka hesaplarıyla ilişkilendirilerek üretilen sahte banka veya kredi kartlarının ticari amaçlı olarak piyasaya sürülmesi karşısında, bu fiilleri yaptırıma bağlamak amacıyla maddeye yeni ikinci fıkra eklenmiştir*" şeklinde belirtilmiştir.[617] Bu fıkrada birinci fıkradan farklı olarak gerçek banka veya kredi kartı değil, başkalarının hesabıyla ilişkilendirilmiş sahte kartların üretimi, kopyalanması, satılması, devredilmesi, satın alınması, kabul edilmesi yaptırıma bağlanmıştır. Yasa koyucu bu ek düzenlemeyle sahte kart üretimi ve kullanılması için gereken dört aşamanın üçünü yaptırıma bağlamıştır. "İlk aşama kartın sahte olarak üretilmesi veya kopyalanması",[618] ikincisi

---

[616] "*5237 sayılı TCK'nun 245/2. maddesinde tanımlanan suçun mağdurunun, kartın henüz kullanılmamış olması nedeniyle hesap sahibi olmayıp banka veya kredi kartını çıkartma yetkisine haiz banka olacağı… nazara alınmadan*" (11. CD. 20.02.2008, E.2007/8458 - K.2008/915), (Kaynak; Taşdemir, s.392.)

Aynı yönde başka bir karar; "*5237 sayılı TCK.nun 245/2. maddesinde tanımlanan suçun mağdurunun, kartın henüz kullanılmamış olması nedeniyle hesap sahibi olmayıp banka veya kredi kartını çıkarma yetkisine haiz banka olacağı …gözetilmelidir*" (11. CD. E.2009/630 - K.2009/4067, 09.04.2009), (Kaynak; Yaşar-Gökcan-Artuç, s.6799.)

[617] Karagülmez, s.218.

[618] "*Somut olayda; Katılan YK. Bankasının tüm elektronik ihtiyaçlarını karşılamak üzere faaliyet gösteren, bankanın yönetim ve denetimine sahip olduğu … A.Ş de analist olarak görev yapan sanığın, kredi kartları sistemleri konusuyla ilgili serviste 1997 yılının Şubat ayından 1999 yılının Ağustos ayına kadar toplam 69 müşterinin kredi kartı numara ve şifrelerini ele geçirerek bu bilgileri evinde ele geçirilen, para çekme eylemlerinde kullanılan boş manyetik bantlı beyaz kartlara yüklemesi işleminde kullanılan* ***ENCODER isimli cihaz vasıtasıyla*** *boş beyaz kartlar üzerindeki manyetik şerit üzerine* ***kopyalayarak,*** *bu kartlar ile değişik zamanlarda farklı ATM cihazlarından para çekmesi şeklinde oluşan eylemlerinde gerçek kredi kartı sahiplerine yönelen bir hile ve desiseden söz edilemeyeceği, sanığın*

satılması veya devredilmesi, üçüncüsü satın alınması veya devralınmasıdır. Dördüncü aşama olan sahte kart kullanılarak hukuka aykırı menfaat temini ise üçüncü fıkrada yaptırıma bağlanmıştır.[619]

Bu fıkrada yaptırıma bağlanan fiiller; başkalarına ait banka hesaplarıyla ilişkilendirilerek, sahte banka veya kredi kartını üretmek, satmak, devretmek, satın almak veya kabul etmek fiilleridir.

Türk Dil Kurumu Sözlüğünde anılan eylemlerden **üretmek**; oluşturmak, meydana getirmek; **satmak**; bir değer karşılığında bir malı alıcıya vermek, **devretmek**; bir malın mülkiyetini, bir mal üzerindeki hakkı başkasına geçirmek, **satın almak**; bir nesneyi belirlenen fiyatını ödeyerek kendine mal etmek anlamlarına gelmektedir.[620] **Kabul etmek** fiilinin ise kendisine sunulan, verilen bir şeyi almak anlamına geldiğini ifade edebiliriz.

Bu fiiller maddede düzenlenen suçun hareket unsurunu oluşturmaktadır. Madde metninde "üretme" fiiliyle karşılanabilecek olan "kopyalama" fiilinin de ayrıca bu fiiller arasında sayılması daha yerinde olurdu.

Kopyalama fiili; kredi kartları hizmet veya mal alımı gibi yasal bir işlem sırasında kullanılırken kart bilgilerinin çalınması işlemidir. Elde edilen bilgiler sahte üretilmiş kredi kartına aktarılarak kullanılmaktadır. Bu durumda başkasına ait hesapla ilişkilendirilmiş sahte kredi kartı üretimi olduğu için gerçekleşen suç 245/2 kapsamına girer. Mağdura ait bilgiler ve şifre, sahte bir kart üretilmeden sanal ortamda alış-veriş yapmak amacıyla kullanılırsa oluşan suç için duruma göre 244/2 veya 244/3 hükümleri uygulanmalıdır.[621]

---

eyleminin bir bütün halinde TCK. nun 525/b-2, 80 maddelerinde öngörülen zincirleme bilişim suçunu oluşturduğu gözetilmeden suçun nitelemesinde hata sonucu yazılı şekilde karar verilmesi, Yasaya aykırı, ... olduğundan bozulmasına" (11. CD. E.2003/13869 - K.2004/2773, 01.04.2004), (Kaynak; Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, s.104).

[619] Dülger, "*Banka veya Kredi Kartlarının Kötüye Kullanılması Suçunda 5377 Sayılı Yasayla Yapılan Değişikliğin Değerlendirilmesi",* **Güncel Hukuk Dergisi**, İstanbul, S.23, Kasım 2005, s.29.

[620] TDK internet sitesi, www.tdk.gov.tr (çevrimiçi), (Erişim; 23.12.2012).

[621] Özbek, ...*Kartların Kötüye Kullanılma Suçu*, s.1032. Ayrıca bu yönde *"Somut olayda; sanığın, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri)*

İkinci fıkradaki suç, seçimlik hareketli olarak düzenlenmiştir. Bu seçimlik hareketlerden biri ya da birkaçının gerçekleştirilmesiyle tek suç işlenmiş olmaktadır.[622] Ancak birden fazla kart için sahtecilik yapılmışsa, bu durumda kart sayısınca suç oluşacaktır.[623]

Sahte olarak üretilen, kopyalanan kartların anılan suçu oluşturabilmesi için başkalarına ait geçerli bir banka hesabıyla ilişkilendirilmiş olması gereklidir.[624] Başkalarına ait hesaplarla irtibatlandırılma hususu gerçekleşmemişse işlenen suç bu madde kapsamına girmez. Örneğin, kredi borçlarını ödemediğinden dolayı bankaların kara listesinde olan bir kişinin, kendisine kredi kartı verilmemesi gerekçesiyle, kendi hesabıyla ilişkilendirerek sahte kart üretmesi durumunda madde kapsamındaki suç oluşmaz.[625]

---

sahte kimliklerle açtırdığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtırdığı hesaplara intikaline kadar gerçek kişilere yöneltilmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştirildiğinden, her bir mağdura karşı işlenmiş ayrı ayrı 5237 sayılı TCK. nun 244/4 maddesine uyan suçu oluşturduğu" (9. CD. E.2007/6709 - K.2007/6012, 27.09.2007), (Kaynak; Kazancı İçtihat Programı).

[622] Malkoç, ...*Türk Ceza Kanunu (m. 188-345),* s.1688; Özbek, ... *Kredi Kartlarının Kötüye Kullanılması Suçu*, s.1048;

"*Sanık M'in mağdurlara ait banka veya kredi kartlarını reader denilen bir cihazı kullanarak* ***kopyalayıp satmaktan ibaret eyleminin*** *TCK 245/2 maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması*", (11. CD. E.2006/7420 – K.2007/1026, 21.02.2007), (Kaynak; B. Zakir Avşar, Gürsel Öngören, *İnternet Hukuku*, Türkiye Odalar ve Borsalar Birliği Yayını, Ankara, Mart 2009, s.115).

[623] *"Sanığın adına düzenlenen sahte pasaport içerisinde iki adet kredi kartının ele geçirildiği, Bankalararası Kart Merkezi (BKM)'nin düzenlediği raporda, her iki kartın da başka hamillere ait manyetik şerit bilgilerinin kopyalanması suretiyle üretildiğinin belirtilmesi karşısında; sahte kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçunun unsurları, sahte oluşturulan kredi kartını kullanmak suçunun yasal tanımında yer almadığı gibi, nitelikli hali olarak da düzenlenmediği, kullanma suçunun oluşması için üretme, satın alma veya kabul etme suçunun işlenmesinin şart olmadığı ve* ***kredi kartının kötüye kullanılması suçunun sahte üretilen kart sayısınca oluşacağı gözetilerek*** *TCK 245/2 madde ve fıkrası uyarınca iki kez hüküm kurulması*" (11. CD. E. 2009/3281 – K. 2009/2673, 08.04.2009), (Kaynak; Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* 45 numaralı dipnot, s.278).

[624] "*Sanık M.B.'ın mağdurlara ait banka veya kredi kartlarını* ***reader denilen bir cihazı kullanarak kopyalayıp*** *satmaktan ibaret eyleminin TCK. nun 245/2. maddesinde düzenlenen sahte kredi kartı üretmek suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması",* (11. CD. E.2006/7420 – K.2007/1026, 21.02.2007), (Kaynak; Yaşar-Gökcan-Artuç, 1228 numaralı dipnot, s.6807).

[625] Yaşar-Gökcan-Artuç, s.6806.

Suçun oluşumu için sahtecilik yapılan kartın kullanılmasına, bir zararın oluşmasına gerek yoktur. Kartın failin üzerinde bulunmasıyla suç tamamlandığından anılan suç bir tehlike suçudur.[626] Bu düzenleme ile mağdurun zarara uğrama tehlikesi yaptırıma bağlanmıştır. Aynı zamanda neticesi harekete bitişik bir suçtur.[627]

Başkasına ait hesaplarla ilişkilendirilen kartın üretilmesi, kartın manyetik şerit bilgilerinin silinerek başka hesap sahibine ait bilgilerin yüklenmesi veya gerçek bir kartın kopyalanması şeklinde olabileceği gibi, kart üzerinde yapılacak kısmi oynamalar, kabartma yazı ve numaraların yeniden basılması, arka yüzdeki manyetik şerit bilgilerinin değiştirilmesi gibi tahrifatlarla da yapılabilmektedir.[628]

Banka veya kredi kartıyla hukuka aykırı menfaat elde etme fiilleri arasında sahte kredi kartı üretimi veya var olan kart üzerinde sahtecilik yapma eylemleri önemli yer tutmaktadır. Bu amaca ulaşabilmek için çeşitli yöntemler kullanılmaktadır. Bu yöntemleri analiz edebilmek için, öncelikle karşımıza çıkabilecek olan bazı teknik terim ve cihazlar ve kötü niyetle kullanım şekilleri üzerinde durmakta yarar vardır.

İmprinter cihazı; üye işyerlerinin kredi kartı ile ödeme kabul ederken kullandığı mekanik cihazlardır. Hizmet veya mal sunan işyerleri, bu cihazı kullanarak kredi kartının ön yüzündeki kabartma bilgileri harcama belgesi (slip) üzerine geçirir. Harcama belgesine, satış tutarı ve işlem tarihi gibi bilgiler de yazılır. Bu belge daha sonra kart hamiline imzalatılarak alış-veriş işlemi tamamlanmış olur.[629] Günümüzde POS cihazlarının yaygın olarak kullanılması ve imza işleminin kaldırılmasıyla artık bu cihazlar pek kullanılmamaktadır.

---

[626] "*Sanıklardan M. **üzerinde ele geçen, alışverişlerde kullanılmayan sahte üretilmiş kredi kartını bulundurmanın TCK 245/2 maddesine temas eden suçu oluşturacağı** gözetilmeden beraatine karar verilmesi, aleyhe temyiz olmadığından bozma nedeni yapılmamıştır*." (11. CD. E.2006/7193 – K.2006/10572, 27.12.2006), (Kaynak; Yılmaz, ...*Kredi Kartlarının Kötüye Kullanılması Suçu*, 46 numaralı dipnot, s.278).

[627] Ali Parlar, Muzaffer Hatipoğlu, *5237 Sayılı TCK'da Özel ve Genel Hükümler Açısından Asliye Ceza Davaları,* Ankara, Adalet Yayınevi, 2008, s.874; Yaşar-Gökcan-Artuç, s.6806; Budak, s.69.

[628] Olgun Değirmenci, *"Ceza Hukuku Açısından Kredi ve Banka Kartları"*, **Legal Hukuk Dergisi**, İstanbul, C.I, S.3, 2003, s.604; Bayındır, s.89; Taşdemir, s.329.

[629] Sazak, s.5.

POS Cihazı (Point Of Sale Terminal - Satış Noktası Terminali); üye işyerlerinin kredi kartı ile ödeme kabul ederken kullandığı elektronik cihazdır. POS cihazı ile kartın arka yüzündeki manyetik şerit bilgileri elektronik olarak okunmaktadır. Ödeme işlemi, banka ile bağlantı kurularak (online) ya da belirli limitler dâhilinde banka ile bağlantı kurulmadan (offline) yapılır.[630] İmprinter cihazlarıyla, POS cihazları arasındaki fark; imprinter cihazının mekanik olması ve kart bilgilerinin ön yüzündeki kabartma bilgileri okumasına karşılık, POS cihazının elektronik olması ve kartın arka yüzündeki manyetik şerit bilgilerini okumasıdır.

Reader/Encoder (Okuyucu/Kodlayıcı) cihazı; alış-verişte kullanılan kartların arka yüzündeki manyetik şerit bilgisini okuyarak elde ettiği bilgileri bağlantılı olduğu bilgisayarın hard diskine aktarır.[631] Bilgisayara aktarılan bilgiler kötü niyetli olarak yine bu cihaz vasıtası ile sahte kartın manyetik şeridine kodlanabilir.[632]

Card printer (Yazıcı) cihazı; kredi kartı üretiminde kullanılan boş beyaz plastik üzerine desen, yazı ve şekil basımında kullanılmaktadır.

Embosser (Kabartma baskı) cihazı; kart bilgilerinin boş plastiklerin üzerine kabartma olarak basılmasında kullanılan cihazdır. Sahte oluşturulacak kredi kartını kullanacak kişinin bilgilerini karta basmak amacıyla kullanılan bir cihazdır.

Tipper (Renklendirici) cihazı kopyalanan beyaz plastik karta kabartma olarak yazılan kart bilgilerinin renklendirilmesi için kullanılır.[633] Bu cihazla bankaların renkli olan isim, amblem ve logolarının renklendirme işlemi yapılmaktadır.

Skimmer cihazı; kart hamili tarafından alış-veriş veya para çekme işlemi için kart kullanıldığı sırada kart bilgilerini elde etmeye yarayan küçük elektronik bir

---

[630] Sazak, s.6.

[631] Budak, s.21.

[632] "*Sanığın komşuları bulunan ... ve ..'ye bankalardan gelen hesap bildirim cetvellerini ele geçirerek bu belgelerdeki bilgilerden yararlanıp, evinde bulunan* ***encoder cihazı*** *ile kendisine ait kredi kartının manyetik şeridini yeniden kodlamak sureti ile*..." (6. CD. E.2000/4851 - K.2000/8874, 29.11.2000), (Kaynak; Değirmenci, *Ceza Hukuku Açısından Kredi ve Banka Kartları*, 46 numaralı dipnot, s.604).

[633] Budak, s.22-24.

cihazdır. Kredi kartı alış-veriş için kullanıldığında, kart hamiline fark ettirmeden skimmer cihazından da geçirilerek bilgiler kopyalanabileceği gibi, ATM'lerden para çekilme işleminde ise kart yuvasına yerleştirilen skimmer cihazı ile bilgiler kopyalanmaktadır. Uygulamada kartların arka yüzündeki şerit bilgilerini elde eden encoder veya skimmer cihazı ile yapılan kopyalama işlemine **skimming** adı verilmektedir.[634] Ancak en son teknolojiye sahip yeni ATM cihazları bu tür suçlara karşı genelde kart yuvasının ve klavyenin neye benzemesi gerektiğini arka plan resmi olarak vermektedirler. Böylece kart hamili fazladan bağlanmış yabancı bir cihazı tespit edebilmektedir.

Sahte kredi kartı üretimi veya kopyalanması amacıyla yaygın olarak kullanılan bilişim suçu işlenme yöntemleri ise şöyledir; **hacking**; sistem koruma şifresinin kırılarak, sistemde mevcut kart ve müşteri bilgilerini alma, **phishing (oltaya alma)**; banka adına sahte olarak gönderilen maillerle (fake mail), şifre ve kart bilgilerini güncelleme bahanesiyle mağdurdan kart bilgilerine ulaşma, **web link;** bankalar adına, banka sitesine çok benzeyen sahte siteler oluşturup mağdura bu sitelerde işlem yaptırarak bilgi edinme, **wireless network**; internete girmek için kablosuz ağı kullananlardan manyetik ortamdaki bilgilere ulaşma, **screenlogger (ekran kaydedici)** sisteme yerleştirilecek virüsler yardımıyla ekranda yazılanların veya **keylogger (tuş kaydedici)** tuş ve klavyeyle yazılanların kaydedilerek şifre ve kart bilgilerine ulaşma gibi yöntemler kullanılmaktadır.[635]

Doktrinde 245/2. madde kapsamındaki sahteciliğin banka kartlarının üretilmesi ve kopyalanması fiillerine yönelik olduğunu, bu fiillerin dışındaki kartın bankadan temini için verilen belgelerdeki sahteciliğin madde kapsamında olmadığı ifade edilmektedir.[636] Ancak Yargıtay bu tür sahteciliğin sadece kart alınıncaya kadar BKKKK yasasına tabi olduğu kart alındıktan sonra ise 245/2 veya duruma göre 3. maddenin uygulanacağı görüşündedir. 01.03.2006 tarihinde yürürlüğe giren 5464 sayılı BKKKK'nın 37. maddesinin ikinci fıkrasında "*Kredi kartı veya üye işyeri*

---

[634] Taşdemir, s.329.

[635] Gökhan Ahi, "*Kredi Kartları Sahteciliği",* **Bilişim ve Hukuk Dergisi**, S.4, Ankara, 2007, s.20-21; Daha detaylı bilgi için çalışmamızda bkz. yuk. "*Bilişim Suçlarının İşlenme Yöntemleri*" bölümü.

[636] Erdoğan, s.337; Özbek, ...*Kartların Kötüye Kullanılma Suçu*, s.1048; Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* s.279.

sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla ***sahte belge ibraz edenler***" için yaptırım öngörülmüştür. Yargıtay da BKKKK'nın 37/2. maddesindeki düzenlemenin sözleşmeye kadar olan safhada uygulanabileceği, sahte; nüfus cüzdanı, maaş bordrosu, ikamet ilmühaberi gibi belgelerle yapılan başvuruda belgelerin sahte olduğu anlaşılır ve başvuran adına kart çıkartılmazsa BKKKK m. 37/2. fıkrası; verilen evrakların sahteliği anlaşılmayarak faile kredi kartı teslim edilmiş ve fail tarafından kart henüz kullanılamamış veya kullanılmasına rağmen elde olmayan nedenlerden dolayı bir yarar sağlanamamış ise, 245/3'e teşebbüs aşamasında kaldığı, kart kullanılarak bir yarar sağlanmış ise, TCK md. 245/3'teki fiilin tamamlanmış hali hükümlerinin uygulanacağı yönünde kararlar vermektedir.[637]

Doktrinde güçlü gerekçelerle eleştiri konusu yapılan bir husus; sahte banka veya kredi kartlarının elde bulundurulması ve/veya haksız menfaat elde etme girişiminde bulunulmasına rağmen bir menfaat elde edilememesi durumlarında uygulanacak hükümlerin ceza adaleti yönünden olumsuz sonuçlar ortaya çıkarmasıdır. Şöyle ki; birinci durumda sahte banka veya kredi kartı fail üzerinde yakalanırsa TCK 245/2. fıkra hükümleri gereğince faile en az 3 yıl (36 ay) hapis cezası verilmektedir. İkinci durumda fail eline geçirdiği sahte banka veya kredi kartı ile haksız menfaat elde etme girişiminde bulunup elinde olmayan nedenlerle eylemi başarısızlıkla sonuçlanır ve yakalanırsa fiil teşebbüs aşamasında kaldığından TCK 245/3. ve 35. maddeleri gereğince en az 12 ay ceza alacaktır. Başka bir anlatımla fail ele geçirdiği sahte banka veya kredi kartıyla haksız menfaat elde etme girişiminde de bulunup başarısız olduğunda eylemi teşebbüs aşamasında kaldığından 12 ay gibi bir ceza alacakken, aynı fail kart üzerinde iken herhangi bir eylem yapmadan ya da eylem düşüncesinde dahi değilken yakalanırsa en az 3 kat daha fazla (3 yıl - 36 ay)

---

[637] "*5464 sayılı Banka Kartları ve Kredi Kartları Kanunu'nun 01.03.2006 tarihinde yürürlüğe girdiği ve anılan Kanun'un 37/2. maddesindeki kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler ile* ***ilgili düzenlemenin sözleşmeye kadar olan safhada uygulanabileceği****, kredi kartı* ***sözleşmesinin düzenlenmesinden sonra kartın üretilmesi halinde 5237 sayılı TCK'nın 245/2., üretilmeden sahteciliğin anlaşılması halinde bu suça 245/2'ye teşebbüs*** *ve* ***sahte üretilen bu kart kullanılarak menfaat temin edilmesi halinde ise ayrıca 245/3. maddesine temas eden suçu oluşturacağı****,*" (11. CD. E. 2010/639 - K. 2010/9199, 19.07.2010), (Kaynak; Kazancı İçtihat Programı).

ceza alacaktır. Bu durumu ceza adaleti açısından adil bir ceza uygulaması olarak görmek mümkün değildir.[638]

2.4.2.4.2. Netice

İkinci fıkrada fiilin neticesi belirtilmemiştir. Başkasına ait hesaplarla ilişkilendirilmiş banka veya kredi kartlarıyla fıkradaki seçimlik hareketlerin birisinin yapılmasıyla suç tamamlanmış olur.[639] Dolayısıyla anılan suç neticesi harekete bitişik bir suçtur.[640] Neticenin ortaya çıkması için sahtecilik yapılan kartın kullanılmasına, bir zararın ortaya çıkmasına gerek yoktur.[641] Bu fıkradaki suç kartın

---

[638] Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılma Suçu,* s. 281.

[639] *"Sanığın adına düzenlenen sahte pasaport içerisinde iki adet kredi kartının ele geçirildiği, Bankalararası Kart Merkezinin düzenlediği raporda,* ***her iki kartın da başka hamillere ait manyetik şerit bilgilerinin kopyalanması suretiyle üretildiğinin belirtilmesi karşısında****; sahte kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçunun unsurları, sahte oluşturulan kredi kartını kullanmak suçunun yasal tanımında yer almadığı gibi nitelikli hali olarak da düzenlenmediği,* ***kullanma suçunun oluşması için üretme, satın alma veya kabul etme suçunun işlenmesinin şart olmadığı*** *ve kredi kartının kötüye kullanılması suçunun sahte üretilen kart sayısınca oluşacağı gözetilerek TCK 245/2 madde ve fıkrası uyarınca iki kez hüküm kurulması"* (11. CD. E.2009/3281 – K.2009/2673, 08.04.2009) ve "*Sanıklardan Musa üzerinde ele geçen* ***alışverişlerde kullanılmayan sahte üretilmiş kredi kartını bulundurmanın TCK 245/2 maddesine temas eden suçu oluşturacağı gözetilmeden beraatine karar verilmesi****, aleyhe temyiz olmadığından bozma nedeni yapılmamıştır."* (11. CD. E.2006/7193 – K.2006/10572, 27.12.2006), (Kaynak, Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* 45 ve 46 numaralı dipnotlar, s.278.)

[640] Ali Parlar, Muzaffer Hatipoğlu, *5237 Sayılı TCK'da Özel ve Genel Hükümler Açısından Asliye Ceza Davaları,* Ankara, Adalet Yayınevi, 2008, s.874; Yaşar-Gökcan-Artuç, s.6806; Budak, s.69; Erdoğan, s.333.

[641] *"Somut olayda; sanıkların fikir ve eylem birliği içerisinde; düzenledikleri gerçeğe aykırı nüfus cüzdanları ile katılan bankalardan sahte kredi kartları alıp harcamalar yapmak suretiyle yarar sağladıkları ve bir kısım kartları da kullanmadan yakalandıkları tarihten sonraki eylemlerinde; farklı kimlik bilgileriyle bir bankanın aynı veya değişik şubelerinden birden fazla kredi kartı alıp kullanmak şeklindeki kullanılan kartlarla ilgili eylemlerinin her bir bankaya karşı kendi içinde teselsül eden 5237 sayılı TCK'nın 245. maddesinin 2. ve 3. fıkralarındaki suçların,* ***kullanılmayan kartlar yönünden ise anılan maddenin 2. fıkrasındaki suçun oluşacağı gözetilmeden,*** *sahte kart sayısınca ve suç vasfında hataya düşürülerek uygulama yeri bulunmayan anılan yasanın 158/1-j maddesindeki dolandırıcılık, kullanılmayan kartlar yönünden ise suç tarihleri kesin olarak tespit edilmeden ve 01.06.2005 tarihinden önce işlenen eylemler yönünden 765 sayılı TCK'nın 504/1. maddesindeki dolandırıcılığa teşebbüs suçunun oluşacağı da nazara alınmadan karar verilmesi, yasaya aykırıdır."* **(**11. CD. E.2009/15793 - K.2010/4885, 29.04.2010), (Kaynak; Kazancı İçtihat Programı**)**.

failin üzerinde bulunmasıyla tamamlandığından anılan suç bir tehlike suçudur.[642] Bu düzenleme ile mağdurun zarara uğrama tehlikesi yaptırıma bağlanmıştır.

2.4.2.5. Manevi Unsur

Bu suç kasten işlenebilen bir suçtur. İkinci fıkra açısından kast, suç konusu banka veya kredi kartının başkasının hesabıyla ilişkilendirildiğinin bilinciyle sahte olarak üretilmesi, satılması, devredilmesi, satın alınması ve kabul edilmesi gibi eylemleri bilerek isteyerek gerçekleştirmektir.[643] Fıkra metninde öngörülmediğinden fiilin taksirle işlenmesi mümkün değildir.

2.4.2.6. Hukuka Aykırılık

Bu suç bakımından genel olarak banka ve kredi kartlarının sadece banka, finans veya kredi kuruluşları tarafından üretilebileceği öngörülerek hukuka uygunluk nedeni olmayacağı ifade edilmektedir.[644] Doktrinde bu tespitin aksine, organize bir suç örgütünün ortaya çıkartılması amacıyla gizli soruşturmacının kullanabilmesi için banka veya kredi kartı üretilmesinin, bir hukuka uygunluk nedeni olduğunu ifade eden de vardır.[645]

2.4.2.7. Suçun Özel Görünüş Biçimleri

2.4.2.7.1. Teşebbüs

245. maddenin ikinci fıkrasındaki suç bir tehlike suçu olarak düzenlenmiştir. Suçun tamamlanması için kartın kullanılması gerekmemektedir. Sahte banka veya kredi kartının failin üzerinde bulunmasıyla suç tamamlanmış olur. Fakat 245/2. fıkrada düzenlenen suça teşebbüs mümkündür.[646]

---

[642] "*Sanıklardan M. **üzerinde ele geçen, alışverişlerde kullanılmayan sahte üretilmiş kredi kartını bulundurmanın TCK 245/2 maddesine temas eden suçu oluşturacağı** gözetilmeden beraatine karar verilmesi, aleyhe temyiz olmadığından bozma nedeni yapılmamıştır*." (11. CD. E.2006/7193 – K.2006/10572, 27.12.2006), (Kaynak; Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, 46 numaralı dipnot, s.278).

[643] Yaşar-Gökcan-Artuç, s.6809; Taşdemir, 320-321; Meran, 382-383; Esen, s.648; Bayındır, s.91-92; Artuk-Gökçen Yenidünya, s.739.

[644] Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1049.

[645] Erdoğan, s.339.

[646] Parlar-Hatipoğlu, s.1707; Budak, s.74; Erdoğan, s.339-340; Meran, s.383; Dülger, *Bilişim Suçları*, s.263; Karagülmez, 227; Bayındır, s.94; Yaşar-Gökcan-Artuç, s.6815-6816.

Doktrinde büyük çoğunluk 245/2'ye teşebbüsün mümkün olduğunu kabul etmektedir.[647] Örneğin, "*başkalarına ait kredi veya banka kartı bilgileri bilgisayarında ve sahte kart üretiminde kullanılan cihaz ve materyalleri de evinde bulunduran bir kimse açısından"*[648] ya da *" kart üretimini gerçekleştiren makinede meydana gelen bir arıza nedeniyle üretim fiili gerçekleşmemiş ise*" söz konusu suç teşebbüs aşamasında kalmış olur.[649] Yargıtay sahte belgelerle kredi kartı müracaatı yapan faille banka arasında, sözleşme imzalandıktan sonra sahtecilik anlaşılarak faile kredi kartı verilmemesi durumunda faile 245/2'de düzenlenen suça teşebbüs hükümlerinin uygulanması gerektiğine karar vermiştir.[650]

2.4.2.7.2. İştirak

İkinci fıkranın suça iştirak açısından farklı bir özelliği yoktur.[651] Ceza Yasası'nın birlikte faillik, azmettirme, yardım etme ve bağlılık kuralı hükümleri çerçevesinde her somut olaya göre mahkemeler tarafından ayrı ayrı değerlendirme yapılacaktır.

Örneğin; üç kişi birbiriyle önceden anlaşarak, sahte banka veya kredi kartını birisi üretse, birisi satsa, bir başkası satın alsa TCK m.37 gereği birlikte faillikten sorumlu olurlar. Bu üç kişi birbirinden habersiz olarak biri kartı üretse, diğerine satsa, bir başkası ise bu kartı satın alsa bu durumda her bir failin eylemi bağımsız olduğu için her üçüne de ayrı ayrı m.245/2'den yaptırım uygulanmalıdır.[652]

---

[647] 245/2'ye teşebbüsün mümkün olmadığını söyleyenler de vardır. Örn. Esen, s.650.

[648] Sazak, s.66.

[649] Budak, s.74.

[650] "*Sanığın katılan A.bank'a müracaat ederek kredi kartı talebinde bulunduğu ancak başvurunun sahte kimlikle yapıldığı ihbarı üzerine sanığa herhangi bir teslimat yapılmadığından ve kredi kartı henüz kullanılmadığından ... eylemin TCK.nun 245/3. maddesindeki sahte kredi kartını kullanmaya teşebbüs suçunu oluşturmayacağı,* ***kredi kartı sözleşmesi imzalandıktan sonra kredi kartı düzenlenmiş ise fiilin TCK.nun 245/2. madde ve fıkrasında öngörülen suçu oluşturacağı, sözleşme imzalandıktan (sonra) fakat kartın düzenlenmemesi halinde ise TCK.nun 245/2. madde ve fıkrasında öngörülen suçun teşebbüs aşamasında kalacağı gözetilerek,*** *sanığın hukuki durumunun takdiri gerektiği*", (11. CD. E.2010/9643 - K.2010/9400, 20.09.2010), (Kaynak; Kazancı İçtihat Programı).

[651] Yaşar-Gökcan-Artuç, s.6817, Bayındır, s.91-92; Dülger, *Bilişim Suçları* s.263.

[652] Özbek, ... *Kredi Kartlarının Kötüye Kullanılması Suçu*, s.105; Erdoğan, s.341.

2.4.2.7.3. İçtima

Banka veya kredi kartlarının kötüye kullanılması fiillerinin içtima açısından farklı bir özelliği yoktur. TCK'da da tanımlandığı şekilde failin bir suç işleme kastıyla, değişik zamanlarda aynı kişiye karşı 245/2. fıkranın aynı hükümlerini birden fazla işlemesi halinde, faile gerçekleşen zincirleme suç (m.42.) gereğince ceza verilir.[653]

İkinci fıkra açısından failin fiilleri, kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek olmaktadır. Fail söz konusu filleri tek kart için yapmışsa, örneğin bir kartı sahte olarak hem üretip hem satmışsa tek bir suç oluşacaktır. Fıkrada ifade edilen eylemlerin mağduru bankadır. Bu nedenle birden fazla bankaya ait kart üretilmişse banka kartı sayısınca ayrı suç oluşacaktır.[654] Fail birden çok kimsenin bilgileriyle sahte kart üretmişse mağdur adedince suçun varlığı kabul edilerek, gerçek içtima kuralları uygulanacaktır.[655]

2.4.3. SAHTE BANKA VEYA KREDİ KARTINI KULLANARAK HUKUKA AYKIRI HAKSIZ YARAR SAĞLAMAK SUÇU (m.245/3)

2.4.3.1. Korunan Hukuki Değer

Bu fıkradaki düzenlemeyle de birçok hukuki değer korunmaya çalışıldığından, korunan hukuki değer karma nitelik taşımaktadır. Fıkra ile malvarlığı değerleri; kamunun belge ve kartlara olan güveni, bilişim sisteminin sağlıklı ve güvenli bir şekilde işleyişi korunmaya çalışılmıştır.[656] Bu fıkrada sahtecilik suçları

---

[653] "*Suça konu kredi kartı **birden fazla işyerinde kullanılarak** haksız çıkar sağlandığı halde TCK 43. maddesinin uygulanmaması*," (11. CD E.2008/14622 - K.12423, 25.11.2008), (Kaynak; Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* 68 numaralı dipnot, s.285).

[654] "***5237 sayılı TCK. nun 245/2. maddesinde tanımlanan suçun mağdurunun, kartın henüz kullanılmamış olması nedeniyle hesap sahibi olmayıp banka veya kredi kartını çıkarma yetkisine haiz banka olacağı*** *ve Bankalar Arası Kart Merkezi'nin 07.02.2008 günlü yazısında suça konu kopyalanmış kartların AE-US ve E KG adlı iki ayrı bankaya ait olduğunun tespit edilmesi karşısında **sanığın eyleminin teselsül eden iki ayrı suç oluşturduğu gözetilmeden** yazılı şekilde tek suçtan hüküm kurulması aleyhe temyiz olmadığından bozma nedeni yapılmamıştır.*" (11. CD. E.2009/630 – K.2009/4067, 09.04.2009), (Kaynak; Yaşar-Gökcan-Artuç, 1250 numaralı dipnot, s.6819)

[655] Sazak, s.68.

[656] Soyaslan, ... *Özel Hükümler*, s.629; Artuk-Gökçen-Yenidünya, s.735; Yaşar-Gökcan-Artuç, s.6798.

özellikleri de bulunduğu için korunan değer aynı zamanda kamuya duyulan güven ve itibardır.[657]

2.4.3.2. Suçun Konusu

245/3. fıkranın hukuki konusu sahte oluşturulan veya üzerinde sahtecilik yapılan banka kartları ya da kredi kartlarıdır.[658] Birinci fıkrada gerçek bir banka veya kredi kartı sözkonusu iken, bu fıkrada sahte oluşturulan veya üzerinde sahtecilik yapılan kartlar söz konusudur. Fail kendi kartını başka hesaplar ile ilişkilendirerek maddede düzenlenen fiilleri gerçekleştirirse bu suç 245. madde kapsamında değerlendirilemez. Banka veya kredi kartı dışında kalan telefon kartı,[659] mağaza kartı, doğalgaz kartı, su kartı gibi kartlar üzerinde işlenen suçlar için de 245. madde hükümleri uygulanmaz.[660]

Yargıtay Ceza Daireleri, telefon kartları ile işlenen suçların öncelikle "*hırsızlık*", sonrasında da "*karşılıksız yararlanma*" suçu kapsamına girdiği şeklinde birbirinden farklı kararlar verirken Yargıtay Ceza Genel Kurulu 19.06.2007 gün ve E. 2007/6-136, K. 2007/150 sayılı kararı ile telefon kartıyla işlenen bu tür fiillerin "*bilişim suçu*" olduğu ve 244/4 maddenin kapsamına girdiği, dolayısıyla da 245. madde kapsamına girmediği yolunda içtihat oluşturmuştur.[661]

---

[657] Bayındır, s.85; Taşkın, *Bilişim Suçları* (Tez), s.74.

[658] Aynı görüş için bkz. Özbek, ... *Kredi Kartlarının Kötüye Kullanılması Suçu,* s.1025; Artuk-Gökçen-Yenidünya, s.738; Meran, s.379; Erdoğan, s.309; Yaşar-Gökcan-Artuç, s.6799.

[659] Özbek, ... *Kredi Kartlarının Kötüye Kullanılması Suçu (TCK m. 245), s.1026.*

[660] Yaşar-Gökcan-Artuç, s.6802.

[661] "*Sanıkların PTT'ye ait kullanılmış telefon kartlarının manyetik şerit bölümüne bant yapıştırıp yeniden konuşma yaptıklarının anlaşılması karşısında eylemlerinin TCK'nun 491/1* (**hırsızlık**) *maddesine uyduğunun gözetilmemesi*", (6. CD. E.2003/19684 - K.2005/7583, 15.09.2005), (Kaynak; Kazancı İçtihat Programı); "*Sanığın daha önceden yapmış olduğu eski ve görüşülmüş telefon kartlarının üzerindeki manyetik bölümlerine teyp bantları (şeffaf) yapıştırmak suretiyle bedava görüşme yaptığı, dolayısıyla Telekom Müdürlüğünü zarara soktuğu, kendi lehine menfaat sağladığı ... Sanığın eyleminin 765 Sayılı TCK. nun 521/b maddesindeki* ***karşılıksız yararlanma*** *suçunu oluşturduğu*," (11. CD. E.2005/7734, K.2006/8338, 19.10.2006), (Kaynak; Özbek, a.g.e. 19 numaralı dipnot, s.1027);

"*Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişikliklerle, sistemin verileri farklı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklenmesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan*

2.4.3.3. Fail ve Mağdur

245. maddenin üçüncü fıkrasında fail için bir farklılık öngörülmediğinden suçun faili herkes olabilir. Fail sahte kartı kullanarak kendisine veya başkalarına menfaat sağlayan kişidir. Ancak suçun öncelikli mağduru sahte olarak üretilen veya üzerinde sahtecilik yapılan banka veya kredi kartlarını çıkaran banka, finans veya kredi kuruluşlarıdır.[662] Anılan eylem dolayısıyla malvarlığında azalma meydana gelen kişiler de bu suçun mağdurudurlar.[663]

2.4.3.4. Maddi Unsurlar

2.4.3.4.1. Hareket

245/3. fıkrada düzenlemesi yapılan suçun fiili, tamamen sahte olarak oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartının kullanılmasıdır. Suçun tamamlanması için failin veya başkasının yarar sağlamış olması gerekir. Fail veya faillere bu madde hükmünün uygulanabilmesi için fiil daha ağır cezayı gerektiren başka bir suçu da oluşturmamalıdır.[664]

Madde metnindeki "*sahte oluşturulan*" ifadesiyle banka veya kredi kartının tamamen sahte olması,[665] gerçek olmaması hali, "*üzerinde sahtecilik yapılan*" ifadesiyle ise mevcut ve geçerli olan bir banka veya kredi kartı üzerinde aldatma

---

*765 sayılı Türk Ceza Yasasının 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan sonra yürürlüğe giren **5237 sayılı Türk Ceza Yasasının 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır.***" (YCGK E.2007/6-136 - K.2007/150, 19.06.2007), (Kaynak; Kazancı İçtihat Programı).

[662] Dülger, *Bilişim Suçları*, s.253; Taşkın, *Bilişim Suçları*, s.64.

[663] Erdoğan, s.350.

[664] Özbek; ...*Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1053; Sazak, s.60; Budak, s.79; Yılmaz, ..*Kredi Kartlarının Kötüye Kullanılma Suçu,* s.280; Artuk-Gökçen-Yenidünya, s.738; Parlar-Hatipoğlu, *Asliye Ceza Davaları,* s.874; Meran, s.381; Akarslan, s.51; Erdoğan; s.348-349; Bayındır, s.90; Yaşar-Gökcan-Artuç, s.6808.

[665] "***Sanığın kendine ait POS cihazlarından sahte kredi kartları ile işlem yaptığı**nın iddia ve kabul olunması karşısında, gerçek kişiye yöneltilen hile ve desise bulunmadığından yüklenen fiilin suç tarihinde yürürlükte bulunan 765 sayılı TCK 525/b-2 (5237 sayılı TCK 245/3) maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden yazılı şekilde hüküm kurulması*" (11. CD. E.2009/5813 – K.2309, 11.03.2009), (Kaynak; Yılmaz, ...*Kredi Kartlarının Kötüye Kullanılma Suçu*, 50 numaralı dipnot, s.279).

kastıyla oynamalar, değişiklikler yapılmasıyla gayri sahih hale getirilmesi kastedilmektedir.[666]

Madde metnindeki "kullanmak fiili", banka veya kredi kartının ATM'lerde, internet üzerinden online ödeme işlemlerinde (SET, Open Market, Cyber Cash, Brokat), WAP (Wireless Application Protocol) bankacılığında, POS cihazlarında ve sanal POS cihazlarında kullanılmasını ifade eder.[667] Kartın bu kullanımı sonucunda failin kendisinin veya başkasının lehine bir yarar sağlaması gerekmektedir.[668] Yarar sağlanması suçun kurucu unsurudur. Eğer bir yarar sağlanmamışsa anılan suç oluşmaz.

Haksız ve hukuka aykırı menfaat elde edilen banka veya kredi kartı gerçek ise 245/1, bir hesapla bağlantılı olarak sahte olarak üretilmişse 245/2 veya 245/3 bir hesapla bağlantısı olmadan üretilmişse sadece 245/3 oluşur.[669] 245/3'te düzenlenen suç icrai hareketlerle icra edilebilir, ihmal ile bu suç işlenemez. Neticesi hareketten ayrılabilen bir suçtur. Netice bir zararın oluşmasıdır. Bu zarar mağdur aleyhine, fail veya üçüncü kişi lehine olmalıdır. Yararın fiilen elde edilmesi şart değildir. Yararın failin veya başkasının tasarruf alanına girmesi yeterlidir.[670] Örneğin failin, sahte kredi kartıyla mağdurun hesabındaki parayı, kendi tasarrufu altındaki hesaba havale

---

[666] Eker, s.129.

[667] Pallı, ...*Bilişim Suçları,* s.98.

[668] "*Hükümlü T.P'ın, hükmü temyiz eden katılan banka müşterilerine ait* ***kredi kartlarındaki bilgileri kopyalamak suretiyle sahte olarak ürettiği kartları kullanarak banka zararına ve kendi yararına menfaat sağladığı*** *iddia ve kabul olunması karşısında; fiilin, 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu'nun 245. maddesinde tanımlanan banka veya kredi kartlarının kötüye kullanılması suçunu oluşturduğu gözetilmeden, 5252 sayılı yasanın 9. maddesi hükmü doğrultusunda karşılaştırmanın anılan madde yerine 158/1-f maddesi nazara alınarak yapılması bozma nedeni yapılmıştır.*" (2. CD. E.2007/9046 – K.2007/2945, 01.05.2007), (Kazancı İçtihat Programı).

[669] "*Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçlarının* ***birbirinden bağımsız iki ayrı suç oluşturduğu*** *gözetilmeyerek fikri içtima kurallarının uygulanması gerektiğinden bahisle tek suç kabulü ile eksik ceza tayini aleyhe temyiz olmadığından bozma nedeni yapılmamıştır."* (11. CD. E.2007/2538 – K.2007/3738, 29.05.2007), (Kaynak, Yaşar-Gökcan-Artuç, 1234 nolu dipnot, s.6808).

[670] Soyaslan, ...*Özel Hükümler*, s.640; Özbek, ... *Kredi Kartlarının Kötüye kullanılma Suçu*, s.1054; Erdoğan, s.349.

ettiği anda veya sahte kartla internet üzerinden sipariş verdiği anda suç tamamlanmış olur. Failin parayı eline alması veya siparişini teslim alması şart değildir.[671]

765 sayılı ETCK döneminde tamamen sahte üretilen banka veya kredi kartları kullanılarak menfaat temin edilmesi durumunda, fiilin işleniş şekline göre faile, dolandırıcılık veya bilişim suçu hükümleri uygulanmaktaydı.[672] Ancak kredi kartı almak için sahte belgelerle müracaat edip ilgili kurum tarafından verilen gerçek kartın kullanılması halinde 504/1'deki "*banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak maksadıyla*" dolandırıcılık suçunun oluştuğu kabul edilerek hüküm kurulmaktaydı.[673]

Bu maddenin TCK'daki karşılığı *"banka veya diğer kredi kurumlarınca tahsis edilmemesi gereken bir kredinin açılmasını sağlamak,*" şeklinde ifade edilen nitelikli dolandırıcılık (158/1-j) maddesidir.[674] Ancak yeni TCK'da banka veya kredi kartlarının kötüye kullanması ayrı bir suç türü olarak düzenlendiğinden 158/1-j maddesi yerine 245/2-3 hükümleri uygulanacaktır. Ayrıca daha sonra yürürlüğe giren ve daha özel olan 5464 sayılı BKKKK 37/2 maddesi de anılan durumlar için uygulama imkânı bulabilecektir. Yukarıda da ifade edildiği üzere Yargıtay TCK

---

[671] "*Sanıkların, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdıkları hesaba bilişim sistemi aracılığıyla göndererek yine sahte kimliklerle çekmek istemesinden ibaret eylemlerinin* ***paranın açılan hesaplara transferiyle suçun tamamlanacağı gözetilmeden*** *paranın çekilmemesi nedeniyle teşebbüs aşamasında kaldığından bahisle eksik ceza tayini isabetsizdir.*" (11. CD. E.2009/3700 – K.2009/6207, 12.05.2009), (Kaynak, Yaşar-Gökcan-Artuç, s.6792).

[672] *"Sanığın, komşuları adına bankadan gelen hesap bildirim cetvellerini ele geçirerek, bu belgelerdeki bilgilerden yararlanıp, evinde bulunan encodem* (Encoder) *cihazı ile kendisine ait kredi kartının manyetik şeridini yeniden kodlamak suretiyle ve internet yoluyla yurt dışındaki şirketlerden mal siparişinde bulunduğu ileri sürüldüğüne göre, öncelikle bu işlerde bilgi ve uzmanlığı bulunan üç kişilik bilirkişi kurulu oluşturularak, TCK.nun 525/a-b maddesinde gösterilen durumlardan bir veya birkaçının bulunup bulunmadığı, kesin olarak belirlenmeli ve sonucuna göre sanığın hukuki durumunun takdiri gerektiği gözetilmelidir"* (6. CD. E.2000/4851 - K.2000/8874, 29.11.2000), (Kaynak; Kazancı İçtihat Programı).

[673] *"... Sanık AB'nin TK, sanık OÖ'nün ise MKÇ sahte kimlikleriyle kredi kartı alıp kullanmaları biçiminde gerçekleşen eylemlerinin; gerçek kişi olan TK ve MKÇ'yı bankayı aracı kılıp dolandırmak değil, TCK'nun 504/1. maddesi kapsamındaki hak etmedikleri krediyi almak suçlarını oluşturacağı gözetilmeden yazılı biçimde hüküm kurulması, bozmayı gerektirdiğinden*" (6. CD. E.2003/6249 - K.2004/1797, 23.02.2004), (Kaynak; Corpus İçtihat Programı).

[674] Budak, s.82.

245/2-3 hükümleriyle, BKKKK 37/2 hükümlerinin aynı anda uygulanma ihtimalini failin suç fiilinde geldiği aşamayı dikkate aldığı içtihatlarıyla çözmeye çalışmıştır.[675]

Sahte belgelerin, kredi kartı için değil de tüketici veya ticari kredi temini için sunulması durumunda ise, nitelikli dolandırıcılık suçu oluşacağından TCK 158/1. maddesi (j) fıkrası hükümleri uygulanır.[676]

Doktrinde 245. madde 3. fıkrayla ilgili olarak benim de katıldığım haklı bir eleştiri yapılmaktadır. Bu eleştiri; madde hükmünün *"fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde"* uygulanacağı ifadesidir. İnceleme konumuz olan m.245/3'ün yaptırımı 4-8 yıl arası; bilişim sistemleri kullanılmak suretiyle **hırsızlık, (**m.142/2-e) suçunun yaptırımı 3-7 yıl arası; bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle **dolandırıcılık, (**m.158/1-f) suçunun yaptırımı 3-7 yıl; **güveni kötüye kullanma** (m.155) 1-7 yıl arası, kredi kartı müracaatı için sahte belge düzenleyip sunma suçu açısından, **özel belgede sahtecilik** (m.207/1) 1-3 yıl, **resmî evrakta sahtecilik suçu** (m. 204/1) 2-5 yıl arası, ayrıca sahte resmî veya özel belgenin bir başka suçun işlenmesi sırasında kullanılması hâlinde, sahtecilik ve ilgili suçtan dolayı ayrı ayrı cezaya hükmolunacağı bu cezalarında ayrı ayrı 245/3 hükmünden az olacağı ortadadır. Tüm bu açıklamalardan da anlaşılacağı üzere bilişim sistemleri aracılığıyla işlenebilecek diğer suçların yaptırımı, 245/3. madde kapsamındaki suçlar için 4 yıldan 8 yıla kadar olacağı öngörülen hapis cezasından daha azdır. Başka bir anlatımla bilişim sistemleri doğrudan veya aracı olarak kullanılarak bu fıkradaki fiilden daha ağır cezayı

---

[675] Aksi yönde görüş; bu halde maddedeki *"sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartı olmadığından,* bu halde öncelikle evrakta sahtecilik ve TCK m.158'de yer alan nitelikli dolandırıcılık ve daha sonra yürürlüğe giren 5464 sayılı BKKKK hükümleri uygulanmalıdır." Özbek, ... *Kredi Kartlarının Kötüye kullanılma Suçu*, s.1055.

[676] *"Sanığın, 09.01.2006 tarihinde F.Bank Antalya şubesine kredi kartı almak için sahte M.B.O. kimliği ile başvurmasına rağmen katılanın şikayeti üzerine Bankalar Birliği'nce yazılan yazı nedeniyle kredi kartının verilmemesi şeklinde oluşan eylemi hakkında mahkemece suç tarihinden sonra 23.02.2006 tarihinde yürürlüğe giren 5464 Sayılı Banka ve Kredi Kartları Yasası md. 37/2 hükümleri olaya uygulanarak cezalandırılmasına karar verilmiş ise de; suç tarihinde yürürlükte bulunan ve eylemine uyan **5237 Sayılı Yasanın 158/1-j ve 35.maddelerindeki düzenlemeler** ile 5464 Sayılı Yasanın 37/2. maddesi olaya uygulanıp ortaya çıkan sonuçların denetime imkan verecek şekilde gösterilip birbiriyle karşılaştırılması suretiyle lehe olan yasa belirlenip sonucuna göre hüküm kurulması gerektiğinin gözetilmemesi"* (11. CD. E.2007/5158 – K.2007/6701, 15.10.2007), (Kaynak; Budak, s.84).

gerektirir bir suçu işlemek mümkün görünmemektedir. Bu nedenle *"fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde"* bu madde hükmünün uygulanacağı yönündeki ifade yersiz ve gereksiz olmuştur.[677]

2.4.3.4.2. Netice

Üçüncü fıkradaki suç ta birinci fıkradaki gibi bir zarar suçudur. Suçun tamamlanabilmesi için bir zarar ortaya çıkmalıdır. Suçun hareket kısmı sahte kartı kullanmak, netice kısmı ise hukuka aykırı yarar elde etmektir. Dolayısıyla bu suç neticesi harekete bitişik bir suç değildir.[678] Birinci fıkra hükmünden farklı olarak bu fıkrada başkalarının hesaplarıyla ilişkilendirilmiş kartların yerine başkalarının hesaplarıyla ilişkilendirilmemiş banka veya kredi kartının kullanılması söz konusudur. Üretilen kartlar ya tamamen sahtedir ya da üzerinde sahtecilik yapılmıştır. Fail, söz konusu kartı kullanarak kendisine veya başkasına yarar sağladığı anda suç tamamlanmış olur.[679]

2.4.3.5. Manevi Unsur

245/3. fıkrada banka veya kredi kartlarının kötüye kullanılması suçu için özel kast aranmadığından genel kastla işlenebilen bir suç türüdür. Failin yasal düzenlemedeki unsurları bilerek ve isteyerek hareket etmesi yeterlidir.[680] Madde metninde yer almadığından fiilin taksirle işlenmesi mümkün değildir.[681]

2.4.3.6. Hukuka Aykırılık Unsuru

Bu suç bakımından genel olarak banka ve kredi kartlarının sadece banka, finans veya kredi kuruluşları tarafından üretilebileceği öngörülerek hukuka uygunluk nedeni olmayacağı kabul edilmektedir.[682] Ancak bir organize suç örgütünün ortaya

---

[677] Kurt, s.191.

[678] Özbek, ... *Kredi Kartlarının Kötüye Kullanılma Suçları*, s.1053; Erdoğan, s.349.

[679] Erdoğan, s.348-349.

[680] Taşdemir, 320-321; Meran, 382-383; Esen, s.648; Bayındır, s.91-92; Artuk-Gökçen Yenidünya, s.739; aksi yönde görüş Karagülmez, s.225; Dülger, *Bilişim Suçları*, s.262.

[681] Yaşar-Gökcan-Artuç, s.6809-6810.

[682] Özbek, ...*Kredi Kartlarının Kötüye Kullanılma Suçu*, s.1049.

çıkartılması amacıyla gizli soruşturmacının kullanabilmesi için banka veya kredi kartı üretilmesinin, bir hukuka uygunluk nedeni olduğunu ifade eden de vardır.[683]

2.4.3.7. Suçu Etkileyen Nedenler

2.4.3.7.1 Şahsi Cezasızlık Hali (m.245/4)

245. maddenin ilk halinde yer almayan şahsi cezasızlık hali 29.06.2005 tarihinde 5377 sayılı kanun ile madde metnine dördüncü fıkra olarak eklenmiştir. Söz konusu fıkrada; birinci fıkrada yer alan suç için, belli akrabalık ilişkilerinin varlığı şahsi cezasızlık hali olarak düzenlenmiştir. Bu akrabalık bağları; *haklarında ayrılık kararı verilmemiş eşler, üstsoy veya altsoy veya bu derecede kayın hısımlarından biri, evlat edinen veya evlâtlık, aynı konutta beraber yaşayan kardeşlerden biri*dir. Sözkonusu kişiler birbirinin aleyhine, diğerinin banka veya kredi kartını kullanarak bir menfaat temin ederlerse, bu akrabalık bağları nedeniyle fail hakkında birinci fıkra hükümleri uygulanmaz. Bu fıkradaki akrabalık ilişkisine sahip olanlara birinci fıkradaki fiili işlemesi halinde hiç ceza uygulanmaz.

Doktrinde bu düzenleme genel olarak olumlu olarak değerlendirilmektedir. Ancak maddenin daha özenle hazırlanarak en azından bu suçun soruşturulması ve kovuşturulmasının şikâyete bağlı olması daha uygun olurdu.[684] Örneğin avukat olarak önüme gelen bir olayda; bir işte çalışan mağdure evli kadın, eşinden fiziksel şiddet görmüş ve kadın sığınma evine sığınmıştır. Akabinde kocasına karşı boşanma davası açmıştır. Ancak eşyalarını alamadığı için evinde kalan ve maaşını aldığı banka kartı kendisine şiddet uygulayan eşi tarafından kullanılarak son maaşı eşi tarafından çekilmiştir. Böylece zaten mağdur olan kadın 245/4 hükmü gereği daha da mağdur olmuştur. Bu nedenle bu fıkrada düzenlenen suç, en azından şikâyete bağlı hale getirilerek mağdura bazı hallerde, failin cezalandırılmasını isteme hakkı verilmelidir.

2.4.3.7.2. Etkin Pişmanlık (m.245/5)

Beşinci fıkra madde metnine, Resmi Gazetede 06.12.2006 tarihinde yayımlanan 5560 sayılı kanunla eklenmiştir. Eklenen bent hükmüyle; "birinci fıkra

[683] Erdoğan, s.339.

[684] a.g.e., s.311.

kapsamına giren fiillerle ilgili olarak ceza kanununun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanacağı" öngörülmüştür.[685]

Bu düzenlemeyle 245/1. fıkra kapsamına giren fiilleri işleyen failler hakkında TCK'nın malvarlığına ilişkin etkin pişmanlık hükümleri (m.168) uygulanacaktır. Yasa koyucu söz konusu düzenlemeyle Anayasa'nın 10. maddesindeki eşitlik ilkesine uygun bir değişiklik yapmıştır.[686]

2.4.3.8. Suçun Özel Görünüş Biçimleri

2.4.3.8.1. Teşebbüs

245. maddenin üçüncü fıkrasındaki suç bir zarar suçudur. Suç failin sahte olarak üretilen veya üzerinde sahtecilik yapılan banka veya kredi kartını kullanarak bir menfaat elde etmesiyle tamamlanmış olur. Ancak fail tüm icra hareketlerine rağmen, elinde olmayan nedenlerle ve iradesi dışında menfaat temin edememişse suç teşebbüs aşamasında kalmış olur. 245/3 açısından hareket ve netice birbirinden ayrılabildiğinden doktrinde teşebbüs olmadığına dair görüş yoktur. Yargıtay uygulamaları da bu yöndedir.[687]

---

[685] "*Yargılama boyunca gerek sözleriyle, gerekse bir takım davranışlarıyla pişmanlığını ortaya koymuş ancak herhangi bir ödemede bulunmamış olan* ***hükümlünün****, 5237 sayılı Yasanın 245. maddesinde 19.12.2006 tarihli Resmi Gazetede yayımlanarak yürürlüğe giren 5560 sayılı Yasanın 11. maddesiyle yapılan değişiklik nedeniyle* (eklenen 245/5 fıkra*) hakkında 5237 sayılı Yasanın 168. maddesindeki etkin pişmanlık hükümlerinin uygulanma olasılığının ortaya çıkması üzerine,* ***ailesini harekete geçirmek suretiyle ödemenin yapılmasını sağladığı anlaşılmakla, hükümlü hakkında 5237 sayılı Yasanın 168. maddesinde düzenlenmiş bulunan etkin pişmanlık hükümlerinin uygulanmasına bir engel bulunmamaktadır.*****"** (YCGK. E.2008/11-127 - K.2008/147, 27.05.2008), (Kaynak; Kazancı İçtihat Programı).

"*5237 Sayılı Yasayla 245. maddeye eklenen Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun mal varlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır hükmüne göre* ***mağdurun zararının tazmin edilip edilmediği araştırılarak sonucuna göre etkin pişmanlık hükmünün uygulama olanağının değerlendirilmesi gerekir***." (11. CD. E. 2006/367 - K. 2008/574, 06.02.2008), (Kaynak; Kazancı İçtihat Programı).

[686] Parlar-Hatipoğlu, s.875.

[687] *"Sanığın, haksız şekilde ele geçirdiği katılan Engin'e ait kimlik bilgileri ile düzenlediği sahte nüfus cüzdanını kullanmak suretiyle aynı suç işleme kararı altında değişik zamanlarda F ... bank A.Ş., T.V ... Bankası T.A.O. ve Y ... ve K ... Bankası A.Ş.'lerin Fethiye şubelerinde sahte vadesiz mevduat hesabı açtırıp, bu bankalardan banka hesap cüzdanları almasının kül halinde 5237 sayılı TCK'nın 204/1 ve 43. maddelerinde öngörülen zincirleme suretiyle resmi belgede sahtecilik, ayrıca F ... bank A.Ş. Fethiye Şubesi'nde açtırdığı söz konusu hesapla bağlantılı olarak üretilen sahte bankamatik kartını teslim aldıktan sonra, kendisine veya başkasına herhangi bir yarar sağlamadan üstünde yakalanması ile aynı sahte kimlik*

Burada yukarıda da üzerinde durduğumuz sahte belgelerle banka veya kredi kartı müracaatı yapılması halinde hangi hükümlerin uygulanacağını yinelemekte yarar vardır. Böyle durumlarda Yargıtay, kart müracaatında kullanılan evrakın sahteliği anlaşılmayarak faile kredi kartı teslim edilmiş ise 245/2. fıkrası, alınan kart fail tarafından kullanılmasına rağmen elinde olmayan nedenlerden dolayı bir yarar sağlayamamışsa 245/3'e teşebbüs; kart kullanılarak bir yarar sağlanmış ise TCK 245/3. fıkrası hükümleri uygulanmalıdır.[688]

2.4.3.8.2. İştirak

Üçüncü fıkranın suça iştirak açısından farklı bir özelliği yoktur.[689] Ceza Yasası'nın birlikte faillik (m.37), azmettirme (m.38), yardım etme (m.39) ve bağlılık kuralı (m.40) hükümleri çerçevesinde mahkemeler tarafından her somut olaya göre ayrı ayrı değerlendirme yapılacaktır.[690]

---

bilgilerini kullanarak internet üzerinden H ... Bank A.Ş.'ye yaptığı kredi kartı başvurusu sonucu üretilen sahte kredi kartının, başvurunun gerçeğe aykırı olduğunun tespiti üzerine bankaca teslim edilmeden iptal edilmesi ***eylemlerinin de ayrı ayrı teşebbüs aşamasında kalan 5237 sayılı TCK'nın 245/3. maddesinde öngörülen banka veya kredi kartlarının kötüye kullanılması suçunu oluşturacağı gözetilmeden***" (11. CD. E.2008/8860 - K.2008/9215, 24.09.2008), (Kaynak; Kazancı İçtihat Programı).

[688] "*Sanığın katılan A.bank'a müracaat ederek kredi kartı talebinde bulunduğu ancak başvurunun sahte kimlikle yapıldığı ihbarı üzerine sanığa herhangi bir teslimat yapılmadığından ve kredi kartı henüz kullanılmadığından* ***eylemin TCK.nun 245/3. maddesindeki sahte kredi kartını kullanmaya teşebbüs suçunu oluşturmayacağı, kredi kartı sözleşmesi imzalandıktan sonra kredi kartı düzenlenmiş ise fiilin TCK.nun 245/2. madde ve fıkrasında öngörülen suçu oluşturacağı, sözleşme imzalandıktan fakat kartın düzenlenmemesi halinde ise TCK.nun 245/2. madde ve fıkrasında öngörülen suçun "teşebbüs aşamasında" kalacağı gözetilerek,*** *sanığın hukuki durumunun takdiri gerektiği*", (11. CD. E.2010/9643 - K.2010/9400, 20.09.2010), (Kaynak; Kazancı İçtihat Programı).

"*5237 sayılı Yasanın 245/3 maddesinde düzenlenen sahte banka kartını kullanmak suretiyle çıkar sağlama suçunun teşebbüs aşamasında kalması için suçun icra hareketlerine başlanması ve sanığın elinde olmayan engel nedenlerle sonucuna ulaşamaması gerektiği cihetle; kartı veren bankanın 13.02.2008 günlü yazısında, sanığın 13.09.2007 tarihinde hesap açtırarak bankamatik kartı aldığı, ancak bu kartı herhangi bir alış verişte kullanmadığı ve hesaba ait hiçbir hareket olmadığının belirtilmesi ve sanığın bu kartı kullanarak çıkar sağlamaya yönelik bir eylemde bulunduğuna dair iddia ve delil bulunmaması nedeniyle, Ceza Genel Kurulunun 27.05.2008 gün ve 87/150 sayılı kararında açıklandığı üzere,* ***sanığın sahte kimlikle banka kartını temin etmekten ibaret eyleminin 5237 sayılı Yasanın 245/2 maddesinde öngörülen suçu oluşturduğu gözetilmeden aynı Yasanın 245/3, 35 maddeleriyle hüküm kurulması, karşı temyiz olmadığından bozma nedeni yapılmamış***," (11. CD. E.2008/20909 - K.2009/5303, 06.05.2009), (Kaynak; Kazancı İçtihat Programı).

[689] Yaşar-Gökcan-Artuç, s.6817, Bayındır, s.91-92; Dülger, *Bilişim Suçları* s.263.

[690] *"... Olayın başlangıcından beri fikir ve eylem birliği içerisinde olan sanıklar S., F. ve*

2.4.3.8.3. İçtima

Üçüncü fıkra açısından suçun zincirleme suç şeklinde işlenmesi mümkündür. Sahte üretilen veya üzerinde sahtecilik yapılan kart birden fazla kullanılarak haksız menfaat elde edilirse, bu kartla işlenen suçlar açısından zincirleme suç hükümleri uygulanabilecektir.[691] Bu fıkradaki suçlar kart sayısınca oluşacaktır. Kartların hamilinin aynı kişi veya farklı kişiler olmasının suçun oluşumu açısından bir farkı yoktur.[692]

245/3. fıkra metninde geçen *"... fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde*" ifadesi nedeniyle m.44'teki fikri içtima hükümlerinin uygulanması söz konusu olamayacaktır.[693] TCK m.44 hükmü nedeniyle zaten birden fazla suçun oluşması halinde daha ağır cezayı gerektiren suçun cezası verileceğinden *"... fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde*" ifadesi gereksiz bir ifade olmuştur.

Yargıtay suç sayısının belirlenmesi açısından, kart hamilini değil de kart sayısını kriter olarak almaktadır.[694] Ancak anılan kriter ağır sonuçlar getirdiği, için

---

*B.'ın adlarına oluşturulmuş kredi kartlarının kullanılması suretiyle haksız menfaat temini sırasında birbirlerinin yanında bulunmak suretiyle birbirlerinin fiillerine iştirak ederek **5237 sayılı TCK'nın 245/3. maddesinde düzenlenen kredi kartının kötüye kullanılması suçunu işledikleri,** bu suçun yapılan alışveriş sayısınca değil, **haksız olarak kullanılan kart sayısınca oluştuğu***", (11. CD. E.2006/5208 - K.2006/8493, 30.10.2006), (Kaynak; Artuk-Gökçen-Yenidünya, s.740).

[691] "*Sahte oluşturulmuş bir kredi kartıyla kısa süre içerisinde **değişik işyerlerinde alışveriş yapılması eylemlerinin, TCK md. 43'ün uygulanmasını gerektirir zincirleme suçu oluşturduğu gözetilerek**, sanık Feyzullah'ın sahte kredi kartıyla mağdur H.Ç.'nin işyerindeki **alışveriş eyleminin tamamlandığı**, mağdur **F.Ö.'ye ait işyerindeki eyleminin ise teşebbüs aşamasında kaldığı anlaşıldığından**, bu iki eylemi yönünden tamamlanmış suçtan hüküm kurularak **cezanın TCK md. 43 uyarınca artırılması gerektiği gözetilmeden,** her bir işyerine karşı işlenen fiillerin bağımsız suçlar olarak kabul edilmesi suretiyle fazla ceza tayini*", (11. CD. E.2006/6678 - K.2006/9711, 30.11.2006), (Kaynak; Budak, s.86).

[692] Yaşar-Gökcan-Artuç, s.6819-6820.

[693] Sazak, s.68.

[694] *"... 5237 sayılı TCK'nın 245/1. maddesinde öngörülen banka veya kredi kartlarının kötüye kullanılması suçunun,...**kart sayısınca oluşacağı ve zincirleme suç hükmünün de aynı kartın farklı zamanlarda birden fazla kullanılması halinde uygulanacağı gözetilmeden** aynı şikayetçinin farklı bankalara ait birden fazla kredi kartının hukuka aykırı şekilde kullanılması eyleminde zincirleme suç hükümleri uygulanmak suretiyle tek **mahkumiyet kararı verilerek eksik cezaya hükmolunması** ...",* (11. CD. E.2007/7255 - K.2007/7837, 12.11.2007), (Kaynak; Özbek, ...*Kredi Kartlarının Kötüye Kullanılması Suçu* 44 numaralı dipnot, s.1042).

"kart sayısı" yerine mağdur olan "hamil sayısının" kriter yapılması gerektiği yönünde doktrinde haklı eleştiriler de vardır.[695]

Son olarak sahte olarak üretilen kartla 245/2. fıkra ve aynı kartla haksız menfaat elde edilerek 245/3. fıkra hükümlerinin aynı anda ihlal edilmesi durumunda hangi hükümlerin uygulanacağı üzerinde durmakta yarar vardır. Yargıtay bu tür durumlarda iki ayrı suçun oluştuğu görüşündedir.[696] Ancak doktrinde benimde katıldığım ikinci fıkradaki suçun üçüncü fıkra için geçit suç olduğu ve sahte kartla menfaat sağlanması halinde sadece 245/3. fıkra hükümlerinin uygulanacağı yönünde görüşler mevcuttur.[697] Çünkü üçüncü fıkradaki suçu işleyebilmek için ikinci fıkradaki suçu işlemek zorunludur. Bir başka anlatımla sahte kredi kartıyla menfaat elde edebilmek için zorunlu olarak öncelikle sahte bir banka veya kredi kartı üretilmesi veya elde edilmesi gerekmektedir.

2.5. BİLİŞİM SUÇLARININ TÜZEL KİŞİ YARARINA İŞLENMESİ (m. 246)

243, 244 ve 245. maddelerde anılan fiiller fail tarafından bir tüzel kişi yararına işlenmiş ve tüzel kişiler haksız bir menfaat elde etmişse bu durumda anılan tüzel kişiler aleyhine TCK (m.60) da öngörülen faaliyet izninin iptali ve elde edilen kazancın müsaderesi gibi güvenlik tedbirleri uygulanacaktır.

---

[695] Özbek, ... *Kredi Kartlarının Kötüye Kullanılması Suçu*, s.1042.

[696] *Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek ile sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlamak suçlarının* ***birbirinden bağımsız iki ayrı suçu oluşturduğu gözetilmeyerek*** *fikri içtima kurallarının uygulanması gerektiğinden bahisle tek suç kabulü ile eksik ceza tayini aleyhe temyiz olmadığından bozma nedeni yapılmamıştır."* (11. CD. E.2007/2538 – K.2007/3838, 29.05.2007), (Kaynak; Yılmaz, ... *Kredi Kartlarının Kötüye Kullanılması Suçu*, 54 numaralı dipnot, s.280-281.)

[697] Dülger, *Bilişim Suçları*, s.264; Tepe, s.286, Erdoğan, s.343 Esen, s.645. Soyaslan, ... *Özel Hükümler*, s.642.

SONUÇ

Çalışmamda, önce bilgisayarın daha sonra da bilgisayar ağları ve internetin bulunmasıyla, klasik ticaret ve iş hayatını, haberleşme yöntemlerini, sosyal hayatı ve toplumları, kısaca hayatın her alanını daha önceki dönemlerde yüzyıllar sonrasında ulaşabildiği dönüşüme, 20-30 yıl içinde ulaştıran bilişim teknolojilerini kötü niyetle kullanarak, haksız menfaat elde eden şahıslara karşı 5237 sayılı Türk Ceza Yasası'nda "Bilişim Alanında Suçlar" başlığı altında, 243-246. maddeleri arasında yapılan düzenlemeleri incelemeye çalıştım.

Bilişim suçlarının işlendiği bilişim alanı; sanal, özgür, çok hızlı ve sürekli genişleyen, sınır çizilemeyen, denetlenemeyen ama hayatın her alanını kolaylaştıran bir teknolojiyi, interneti de içinde barındıran bir alandır. Bu nedenle eğer sınırları belirlenmezse değişik açılardan onlarca tez veya doktora konusu olabilecek bu alanı sınırlayarak tez çalışmamı 5237 sayılı Türk Ceza Kanunu'nda "Bilişim Alanında Suçlar" başlığı altındaki suçlar ile sınırlı tuttum.

Bilişim suçları alanı, teknoloji kullanmadan suç işlenebilmesinin çok zor olduğu bir alandır. Bu nedenle çalışmamım yarısını bilişim suçlarını inceleyebilmek ve kavrayabilmek için gerekli olan bilişim sistemine, bilgisayar ve internet teknolojisine ait temel, teknik terim ve kavramlara ayırdım. Bu içerik doğrultusunda çalışmamın başlığını da "Teknik ve Hukuksal Yönleriyle Bilişim Alanında Suçlar" koydum.

Aslında bilişim suçlarının doğrudan (dar anlamda, gerçek) bilişim suçları ve dolayısıyla (geniş anlamda) bilişim suçları olarak ikiye ayrılması gerektiğini düşünüyorum. Yeri geldiğinde bu düşüncemi teyit eden Yargıtay kararları ve doktriner görüşler üzerinde de durdum. Doğrudan bilişim suçları bilgi çağı ile ortaya çıkan 30-40 yıl öncesinde olmayan, bilişim sistemlerine karşı veya bilişim sistemleri aracılığıyla işlenen soyut veri veya bilgilerin kullanıldığı yeni suç işlenme yöntemleridir. Dolayısıyla bilişim suçları ise (dolandırıcılık, zimmet, hakaret, tehdit gibi) klasik suçların, bilişim sistemleri aracılığıyla işlendiği suç yöntemleridir. Bu

bağlamda 243. ve 244. maddenin doğrudan bilişim suçu, 245. maddenin ise dolayısıyla bilişim suçu türü olduğunu ifade edebiliriz. Bu çalışmamı doğrudan bilişim suçları ve dolayısıyla bilişim suçları, sınıflandırması altında inceleyemedim ama ileride bu tür sınıflandırmalar yapılarak makaleler, tezler hazırlanacağını düşünüyorum.

Sonuç olarak bu tür suçları işleyenlerin cezasız kalmaması ve daha da önemlisi anılan suçların işlenmesinin önüne geçilebilmesi için alınabilecek bir kısım önlem ve önerilerimi şu şekilde sıralayabilirim;

1. Genel olarak;
    a. Bilişim teknolojisini kullanan suçlularla etkin mücadele edebilmek adına yapılan yasal denetimler, bireylerin iletişim özgürlüğüne ve özel yaşamına, bireysel mahremiyetine olabildiğince az müdahale etmelidir. Bu bağlamda yapılacak düzenlemelerde kamu güvenliği ve kamu düzeniyle, bireylerin temel hak ve özgürlükleri arasındaki denge iyi kurulmalıdır.
    b. Bilişim suçlarının özellikle yurtdışı bağlantılı olarak işlenmesi nedeniyle, uluslararası alanda diğer devletlerle koordineli olarak, anılan suçlar konusunda uygulanacak olan yetki ve usul hükümleri tereddüde yer bırakmayacak şekilde belirlenerek, bu tür suçları işleyen sanıkların cezasız kalmasının önüne geçilmelidir.
    c. Özellikle büyükşehirlerde birkaç yıldır uygulanan bilişim savcılığı ve emniyet bilişim şubeleri yaygınlaştırılarak, bu birimlerde görev yapan personel, uygun altyapı, eğitim, teçhizat ve yasal düzenlemelerle desteklenmelidir.
    d. Bilişim suçlularını yargılayacak özel ihtisas mahkemeleri kurulmalıdır.
2. Bilişim hukukunun eğitim ve öğretimi açısından;
    a. Hukuk fakültelerinde bilişim hukuku dersleri açılarak en azından yeni yetişecek hukukçuların bilişim sistem ve terminolojisine sahip olarak mesleğe başlamaları sağlanmalıdır.

b. Hukuk fakültelerinde bağımsız bilişim hukuku dalları açılarak bir kısım hukukçularında bilişim hukuku ve bilişim ceza hukuku alanlarında uzman olarak yetişmeleri sağlanmalıdır.

3. 5237 sayılı TCK'da bilişim alanında yer alan hükümlerin kaynağı Avrupa Konseyi Siber Suç Sözleşmesi'dir. Türkiye bu sözleşmeyi imzalamıştır. Ancak hukuksal prosedür tamamlanmadığı için sözleşme hükümleri iç hukuk normu niteliğinde değildir. Sözleşmenin bazı maddelerini karşılayacak düzenleme de yapılmış değildir. Bu nedenle bir an evvel çıkarılacak kanun ile Siber Sözleşme'nin uygunluğu onaylanarak, düzenleme yapılmamış olan hükümleri iç hukuk normu haline getirilmelidir.

   Avrupa Konseyi Siber Suç Sözleşmesi onaylandıktan sonra sözleşme hükümleriyle yetinilmemeli, sözleşme asgari bir model olarak değerlendirilerek, daha ileri ve daha güncel düzenlemelerle, bağımsız bir bilişim suçları ile mücadele kanunu çıkarılmalıdır.

4. Ceza yasamızda mevcut düzenlemeler açısından;
   a. 243. maddenin birinci fıkrasındaki bilişim sisteminin bütününe veya bir kısmına hukuka aykırı olarak "*giren **ve** orada kalmaya devam eden*" ifadesi yerine "*giren **veya** orada kalmaya devam eden*" ifadesi getirilerek hem anlam karmaşasına son verilmeli ve hem de suç fiilleri seçimlik ve belirli hale getirilmelidir.

   b. 244/4. fıkradaki haksız çıkar sağlamanın "*başka bir suç oluşturmaması halinde*" ifadesi yerine, gerekçedeki gibi, haksız çıkar sağlamanın "*daha ağır cezayı gerektiren başka bir suçu oluşturmaması halinde*" ifadesi eklenerek, fıkra işlevsel hale getirilmelidir.

   c. Banka veya kredi kartlarına yönelik suçları yaptırıma bağlayan 245. maddenin koruduğu hukuksal değer, malvarlığı olduğu için bu madde bilişim alanında suçlar arasında değil, kişilere karşı suçların düzenlendiği 2. Kısım 10. Bölümdeki malvarlığına ilişkin suçlar altında yer almalıdır. 06.12.2006 tarihinde 245. maddeye eklenen 5.

fıkrada, etkin pişmanlık açısından TCK m.168'e atıf yapılması bu görüşümüzü teyit etmektedir.

d. 245/2. fıkrada yer alan suç fiillerinin başına "*bilerek*", fıkradaki eylemler arasına da "*bulundurmak*" fiili eklenerek tesadüfî cezalandırılmaların önüne geçilmelidir.

e. 245/2. ve 245/3. fıkraların aynı suça yönelik oldukları, 2. fıkrada öngörülen fiillerin 3. fıkrada öngörülen suçu işleyebilmek için geçit suç olduğu dikkate alınarak her iki fıkra birleştirilip, 3. fıkra, 2. fıkranın nitelikli haline dönüştürülmeli ve ceza adaleti açısından sanıklara iki ayrı ceza verilmesinin önüne geçilmelidir.

f. 245/4. fıkrada öngörülen bazı yakın akrabalar arasındaki şahsi cezasızlık hali zorunlu olarak uygulanmamalı, mağdur açısından cezalandırmayı isteyebilecek şekilde şikâyete tabi kılınmalıdır.

Son olarak; sadece yasal düzenlemelerle anılan suçların önüne geçilemeyeceği göz önünde bulundurularak, üzerine sorumluluk düşen tüm bireyler, tüzel kişiler ve devlet kurumları ile yasaları uygulayanların da sorumlu ve hassas hareket etmesinin bilişim suçlarının ve diğer tüm suçların da en aza inmesini sağlayacağını da unutmamalıyız.

KAYNAKÇA

[1] Ahi, G., (2007), *Kredi Kartları Sahteciliği,* Bilişim ve Hukuk Dergisi, Ankara, S.4, s.18-22.

[2] Akarslan, H., http://www. bilgisayarpolisi.com/ index.php?sayfa=makaleoku& kategori= "*Bilişim Suçu Kavramı"*, (çevrimiçi), (Erişim; 07.03.2011).

[3] Akarslan, H., (Şubat 2012), *Bilişim Suçları,* 1. Baskı, Ankara, Seçkin Yayıncılık.

[4] Akıncı, F. S., (2001), *Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi* İnternet Özel Bölümü, İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, İstanbul, C.LIX, S.1-2, s.11-38.

[5] Akıncı, H., Alıç, E., Er, C., (Ocak 2004), *Türk Ceza Kanunu ve Bilişim Suçları,* (Derleyen; Atamer, Y. M.), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1. Baskı, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, No: 51, s.157-275.

[6] Akbulut, B. B., (1999), *Türk Ceza Hukukunda Bilişim Suçları*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Ceza ve Ceza Usul Hukuku Bilim Dalı, Yayımlanmamış Doktora Tezi, Konya.

[7] Akbulut, B. B., (2000), *Bilişim Suçları*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, Milenyum Armağanı, Konya, C. VIII, S.1-2, s.545-555.

[8] Akkoyunlu, A., (Mart 2012), TBD Bilişim Kültürü Dergisi (Ropörtaj), Y:40, S. 141, s. 18-19.

[9] Alaca, B., (2008), *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile),* Ankara Üniversitesi Sosyal Bilimler

Enstitüsü, Antropoloji (Sosyal Antropoloji) Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[10] AnaBritannica Genel Kültür Ansiklopedisi, (1987), Ana Yayıncılık ve Sanat Ürünleri Pazarlama A. Ş. Yayını, C. IV. İstanbul.

[11] Artuk, M. E., Gökçen, A., Yenidünya, C., (2010), *Ceza Hukuku Özel Hükümler*, 10. Baskı, Ankara, Turhan Kitapevi.

[12] Avşar, B. Z., Öngören, G., (Mart 2009), *İnternet Hukuku*, Ankara, Türkiye Odalar ve Borsalar Birliği Yayını.

[13] Avşar, B. Z., Öngören, G., (2010), *Bilişim Hukuku*, İstanbul, Türkiye Bankalar Birliği Yayını, Yayın No: 270.

[14] Aydın, E. D., (Eylül 1992), *Bilişim Suçları ve Hukukuna Giriş,* Ankara, Doruk Yayınevi.

[15] Bayındır, A., (Ekim 2010), *Türk Ceza Hukukunda Düzenlenen Bilişim Suçları,* Suç ve Ceza Dergisi, İstanbul, S.2, s.55-106.

[16] Beasant P., (1999), *Elektronik,* (Çeviren; Tunalı, E.), 2. Baskı, Ankara, Nurol Matbaacılık, TUBİTAK Popüler Bilim Kitapları 103, Gençlik Kitaplığı 20.

[17] Beceni, Y., (2003), http:// www. hukukcu. com/bilimsel /kitaplar/ yasin beceni/ indeks. htm. *Siber Suçlar*, (çevrimiçi), (Erişim; 16.03.2011).

[18] Budak, M., (2009), *Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu,* Polis Akademisi, Güvenlik Bilimleri Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[19] Büyük Larousse, Sözlük Ve Ansiklopedisi (1986), Milliyet Yayını, Baskı Milliyet Gazetecilik A. Ş., C.IV. İstanbul.

[20] Çeken, H., http://archiv.jura.uni-saarland.de/turkish/HCeken1.html *Amerika Birleşik Devletlerinde İnternet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası,* (çevrimiçi), (Erişim; 16.03.2011).

[21] Çekiç, B., (2006), *İnternet Aracılığıyla İşlenen Suçlar,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[22] Çiçek, İ., (2008), *Ülkemizde Adli Bilişim Laboratuarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları*, Haliç Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Yönetim Bilişim Sistemleri, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[23] Değirmenci, O., (2003), *Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi,* Legal Hukuk Dergisi, İstanbul, C. I, S.11, s.2750-2758.

[24] Değirmenci, O., (2003), *Ceza Hukuku Açısından Kredi ve Banka Kartları*, Legal Hukuk Dergisi, İstanbul, C.I, S.3, s.592-609.

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

[26] Demircan, T., (2007), *Bilişim Alanında Suçlar*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Konya.

[27] Dijle, H., (Mayıs 2006), *Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Elektronik-Bilgisayar Eğitimi Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[28] Dilek, H. İ., (2007), *Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri*, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Diyarbakır.

[29] Dönmezer S. (Temmuz 2004), *Bilgisayar Suçları,* IGUL Ceza Hukukunun Güncel Kaynakları, Hocaların Hocası Ord. Prof.Dr. Dr. H.c. mult. Sulhi Dönmezer Özel Bölüm, Promat Basım Yayın Sanayi ve Tic. A. Ş. İstanbul, 96-100.

[30] Dülger, M. V., (Kasım 2004), *Bilişim Suçları,* 1. Baskı, Ankara, Seçkin Yayınevi.

[31] Dülger, M. V., (Ocak 2005), *Bilişim Suçları ve Yeni Türk Ceza Kanunu,* Kazancı Hukuk, İşletme ve Maliye Bilimleri Dergisi, S.5, s.114-120.

[32] Dülger, M. V., (Haziran 2005), *Yeni Türk Ceza Kanunu'nda Düzenlenen Bilişim Suçları ve Bu Suçlarla Mücadelede Alınması Gereken Önlemler,* Çağın Polisi Dergisi, Ankara, C. IV, S.42, s.3-8.

[33] Dülger, M. V., (Kasım 2005), *Banka veya Kredi Kartlarının Kötüye Kullanılması Suçunda 5377 Sayılı Yasayla Yapılan Değişikliğin Değerlendirilmesi,* Güncel Hukuk Dergisi, İstanbul, S.23, s.28-30.

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

[35] Er, C., (2004), *Bilişim Suçları*, İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, İstanbul, s. numarası yok.

[36] Eralp, Ö., (Mart 2004), www.ozgureralp. av.tr/makaleler/İP *Bilişim Suçlusuna Giden Yol – IP*, (çevrimiçi), (Erişim; 28.03.2011).

[37] Eralp, Ö., (Haziran 2007), *Hukukçular için Bilişim Terimleri Sözlüğü,* 1.Baskı, Bodrum, Muğla, Eralp Kitap Basım Yayıncılık.

[38] Erdağ, A. İ., (2010), *Bilişim Alanında Suçlar (Türk ve Alman Ceza Hukukunda),* Gazi Üniversitesi Hukuk Fakültesi Dergisi, Ankara, C. XIV, S.2., s.75-303.

[39] Erdağ, A. İ., http://www.temyiz.net/forum/22-ceza-hukuku/ 613–yard-doc-dr-ali-ihsan-erdag-ekonomi-sanayi–ve–ticarete–iliskin-suclar–bilisim-alaninda–suclar–tck-9-ve-10-bolumler.html. Bilişim Suçları, (çevrimiçi). (Erişim; 11.04.2012)

[40] Erdoğan, Y. (Şubat 2012), *Türk Ceza Kanunu'nda Bilişim Suçları (Avrupa Konseyi Siber Suç Sözleşmesi ve Yargıtay Kararları İle),* 1.Baskı, İstanbul, Legal Yayıncılık.

[41] Ergüç, S., (2008), *Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar ve Bilişim Suçları Hukuku,* Kadir Has Üniversitesi Sosyal

Bilimler Enstitüsü, İşletme Bölümü (MBA), Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[42] Ergün, İ., (Ağustos 2005), *Yeni Türk Ceza Kanunu'nda Bilişim Suçları,* Çağın Polisi Dergisi, Ankara, C. IV, S.44, s.8-15.

[43] Ergün, İ., (Eylül 2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum,* 1.Baskı, Ankara, Adalet Yayınevi.

[44] Erol, H., (2003), *Türk Ceza Kanunu,* Ankara, Yayım Matbaacılık ve Ticaret İşletmesi Yayını.

[45] Ersoy, Y., (Haziran 1994), *Genel Hukuki Koruma Çerçevesinde Bilişim Suçları*, Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, Ankara, C. XLIX, S.3-4. s.150-180.

[46] Esen, S., (Eylül 2007), *Malvarlığına karşı Suçlar, Belgelerde Sahtecilik ve Bilişim Alanında Suçlar,* Ankara, Adalet Yayınevi.

[47] Gümüş, Ç., (2008), *Bilişim Suçlarıyla Mücadelede Polisin Eğitimi*, Fırat Üniversitesi Sosyal Bilimler Enstitüsü, Eğitim Bilimleri Anabilim Dalı, Yayımlanmamış Doktora Tezi, Elazığ.

[48] Gündel, A., (2009), *Yeni Türk Ceza Kanunu Açıklaması (m.207-345),* Ankara, (Yayınevi Yok), C.IV.

[49] Güngör N. M., (2007), "*Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları"*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[50] Gürler, F., (2007), *Tehlikenin Farkında mısınız?,* Ankara Barosu Bilişim ve Hukuk Dergisi, Ankara, S.5, s.38-43.

[51] Hafızoğulları, Z., Güngör, D. (2007), *Türk Ceza Hukukunda Suçların Tasnifi,* Türkiye Barolar Birliği Dergisi, S.69, Ankara, 21-49.

[52] Havuz, S., (2007), *Avrupa Konseyi Siber Suçlar Sözleşmesi Kapsamında Türkiye'nin Güvenliği*, Genelkurmay Başkanlığı Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü, Uluslararası İlişkiler Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[53] Henkoğlu, T., (Eylül 2011), *Adli Bilişim, Dijital Delillerin Elde Edilmesi ve Analizi*, 1. Baskı, İstanbul, Pusula Yayıncılık.

[54] Herkes İçin Bilgisayar Ansiklopedisi, *İnternet Araçları,* İnternet Bölümü, S.1. İstanbul, Vogel Yayıncılık.

[55] İlbaş, Ç., (2009), *Bilişim Suçlarının Sosyo-Kültürel Seviyelere Göre Algı Analizi*, Başkent Üniversitesi Fen Bilimleri Enstitüsü, İstatistik ve Bilgisayar Bilimleri Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[56] İlbaş, Ç., Köksal, M. A., (Aralık 2011), *Türkiye Bilişim Suçları Raporu*, (Editörler; Memiş, T. vd.), İzmir II. Uluslararası Bilişim Hukuku Kurultayı, 17-19 Kasım 2011, Bildiriler Kitabı, İzmir, s.163-171.

[57] İnanıcı, H., (1996), *Bilişim ve Yazılım Hukuku Uygulama İçinden Görünüşü,* İstanbul Barosu Dergisi, C. LXX, S.7-8-9, s.510-537.

[58] Kaçak N., (2007), *Yeni içtihatlarla Yeni Türk Ceza Kanunu*, Ankara, Seçkin Yayınevi, s.620-621.

[59] Karabal, M., (2005), http://www.Turk hukuksitesi.com.tr. *Bilişim Suçları ve Türk Polis Teşkilatı*, (çevrimiçi), (Erişim; 12.04.2012)

[60] Karagülmez, A., (Mayıs 2009), *Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri,* Genişletilmiş ve Gözden Geçirilmiş 2. Baskı, Ankara, Seçkin Yayınevi.

[61] Karakehya, H., (2009), *Türk Ceza Kanununda Bilişim Sistemine Girme Suçu,* Türkiye Barolar Birliği Dergisi, Ankara, S.81, s.1-24.

[62] Kaya, M., (2008), Ankara Barosu Uluslararası Hukuk Kurultayı (05.01.2008-11.01.2008), Adli Bilişim Oturumu Konuşma Metni, C.II. Ankara Barosu Yayını.

[63] Ketizmen, M., (Ocak 2008), *Türk Ceza Hukukunda Bilişim Suçları*, 1.Baskı, Ankara, Adalet Yayınevi.

[64] Kızıltan M. B., (2007), *5237 sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme ve Bozma Suçları,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[65] Kuplay, Ö., (Haziran 2007), *Bilişim Suçları ve Hukuku,* Çağın Polisi Dergisi, Y: 6, Ankara, S.66, s.42-51.

[66] Kurt, L., (Eylül 2005), *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* 1.Baskı, Ankara, Seçkin Yayınevi.

[67] Malkoç, İ., (2007), *Açıklamalı İçtihatlı 5237 Sayılı Türk Ceza Kanunu (m. 188-345),* C.II. Malkoç Kitapevi.

[68] Malkoç, İ., Güler, M., t.y., (*Uygulamada) Türk Ceza Kanunu Özel Hükümleri - IV,* Ankara, Adil Yayınevi.

[69] Memiş, T., (2001), *Hukuki Açıdan Kitlelere E-Posta Gönderilmesi*, Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi, Erzincan, C.V, S.1-4, s.431-444.

[70] Meran, N., (Eylül 2005), *(Yeni Türk Ceza Kanununda) Sahtecilik - Malvarlığı ve Bilişim Suçları ile Ekonomi ve Ticaret Alanında Suçlar,* 1. Baskı, Ankara, Seçkin Yayınevi.

[71] Nacar, F. B., (2010), *Avrupa Birliği Ülkeleri ve Türkiye'de Bilişim Suçlarının Ceza Hukukundaki Uygulamaları*, Atılım Üniversitesi Sosyal Bilimler Enstitüsü, Avrupa Birliği Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[72] Önder, A., (1994), *Şahıslara ve Mala Karşı Cürümler ve Bilişim Alanında Suçlar,* İstanbul, Filiz Kitabevi.

[73] Örnekleriyle Türkçe Sözlük (2000), İstanbul, Milli Eğitim Bakanlığı Yayını, C.II. Milli Eğitim Basımevi.

[74] Özbek, V. Ö., (2002), *İnternet Kullanımında Ortaya Çıkabilecek Bazı Ceza Hukuku Sorunları,* Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C.IV. İzmir, S.1, s.101-158.

[75] Özbek, V. Ö., (2007), *Banka veya Kredi kartlarının Kötüye Kullanılması Suçu (TCK m. 245),* Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, C. IX, Özel sayı, İzmir, s.1019-1063.

[76] Özdilek, A. O., (Eylül 2006), *(Uygulamadan Örnek Olaylarla) Bilişim Suçları ve Hukuku,* 1. Baskı, İstanbul, Vedat Kitapçılık.

[77] Özel, C., (Ocak 2004), *Bilişim Suçları İle İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı,* (Derleyen; Yeşim M. Atamer), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1. Baskı, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, No:51, s.341-361.

[78] Özel, C., (Aralık 2006), *Bilişim Suçlarının Türk Ceza Kanunu ve Tasarı'daki Hükümler Yönünden Mukayeseli Değerlendirilmesi - Öneriler,* (Derleyen; Tevetoğlu, M.), Türkiye II. Bilişim Hukuku Sempozyumu, Bilişim Hukuku Toplantıları, İstanbul, Kadir Has Üniversitesi Yayınları, s.85-91.

[79] Özen, M., Baştürk İ., (Ekim 2011), *Temel Hak ve Özgürlükler Bağlamında Bilişim – İnternet ve Ceza Hukuku*, 1. Baskı, Ankara, Adalet Yayınevi.

[80] Özkul, D., (Ocak-Haziran 2002), *Bilişim Sistemi Kavramı ve Bilişim Sistemlerinin Denetimi,* Sayıştay Dergisi, Ankara, S.44-45, s.11-34.

[81] Öztürk, M. İ., (2007), *Bilişim Cihazlarındaki Delillerin Tespiti ve Değerlendirilmesinde İş Akış Modelleri,* Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Disiplinler arası Adli Tıp Ana Bilim Dalı, Fizik İncelemeler ve Kriminalistik Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[82] Pallı, H., (Kasım 2008), *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Kayseri.

[83] Pallı, H., (Ocak 2009), *Türk Ceza Kanununda Yer Alan Başlıca Bilişim Suçları,* Adalet Bakanlığı, Ankara, Adalet Dergisi, S.33, s.83-104.

[84] Pamuk, S., (1999), *Dünya Parmağınızın Ucunda,* (Bilgisayarın Temelleri), Ankara, Meridyen Bilişim Yayını.

[85] Pano Dergisi, (Ağustos 1997), Bankalararası Kart Merkezi (BKM), S.1. İstanbul.

[86] Parlar, A., Hatipoğlu, M., (2007), *(Açıklamalı Yeni İçtihatlarla) 5237 Sayılı Türk Ceza Kanunu Yorumu (141-345. Md.),* C.II. Ankara.

[87] Parlar, A., Hatipoğlu, M., (2008), *5237 Sayılı TCK'da Özel ve Genel Hükümler Açısından Asliye Ceza Davaları,* Ankara, Adalet Yayınevi.

[88] Parlar, A., (Ocak 2011), *Türk Ceza Hukukunda Bilişim Suçları,* 1. Baskı, Ankara, Bilge Basım Yayınevi.

[89] Reisoğlu, S., (Haziran 2004), *Banka Kredi Kartları ve Uygulama Sorunları,* Bankacılar Dergisi, Yıl:15, İstanbul, S.49, s.100-123.

[90] Savaş, V., Mollamahmutoğlu, S., (Mayıs 1999), *Türk Ceza Kanunu'nun Yorumu,* 3. Baskı, Ankara, Seçkin Yayınevi.

[91] Sazak, S., (2008), *Ceza Hukukunda Banka ve Kredi Kartlarının Kötüye Kullanılması,* İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

[92] Sınar, H., (24 Mart 2001), *İnternet ve Ceza Hukuku,* 1. Baskı, İstanbul, Beta Yayınevi.

[93] Soyaslan, D., (2005), *Ceza Hukuku Genel Hükümler,* Güncelleştirilmiş 3. Baskı, Ankara, Yetkin Yayınevi.

[94] Soyaslan, D., (2009), *Bilişim Alanında Suçlar,* Prof. Dr. Mualla Öncel'e Armağan, Ankara, Ankara Üniversitesi Hukuk Fakültesi Yayını, No:243, s.1563-1597.

[95] Soyaslan, D., (2010), *Ceza Hukuku Özel Hükümler,* 8. Baskı, Ankara, Yetkin Yayınevi.

[96] Tanılır, M. N., (Ocak 2002), *İnternet Suçları ve Bireysel Mahremiyet,* 1. Baskı, Ankara, Liberte Yayınevi.

[97] Tanşu, O., (Ocak 2004), *Bilişim Çağı, Yeni Tanımlamalar ve Hukuki Düzenlemeler,* (Derleyen; Yeşim M. Atamer), İnternet ve Hukuk, Bilişim Üzerine Yazılar, İnternet ve Ceza Hukuku (Panel), Bilişim Hukukuna İlişkin Hukuki Metinler, 1. Baskı, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, No:51, s.139-154.

[98] Taşdemir, K., *Yargıtay Uygulamalarında İnternet Suçları,* (Hazırlayan Müslüm Saylı, D. Akdeniz), Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Sempozyumu, Bursa, 24.03.2001, s.57-65.

[99] Taşdemir, K., (Temmuz 2009), *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları,* İstanbul, Ütopyagrafik Yayınevi.

[100] Taşdemir K., Özkepir, R., *Uygulamada - Öğretide Belgelerde Sahtecilik, Mala Karşı Suçlar ve Bilişim Alanında Suçlar,* Ankara, Adil Yayınevi.

[101] Taşkın Ş. C., (2008), *Bilişim Suçları,* 1. Baskı, Bursa, Beta Yayınevi.

[102] Taşkın Ş. C., (2008), *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları,* Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Ana Bilim Dalı, Kamu Hukuku Bilim Dalı, Yüksek Lisans Tezi, İstanbul.

[103] Taşkın Ş. C. (2009), *Bilişim Hukuku Uluslararası Uyuşmazlıklar*, Türkiye Barolar Birliği Dergisi, S.85, Ankara, s.334-364.

[104] Türk Dil Kurumu internet sitesi, www.tdk.gov.tr/index.php? option =com _gts &arama (çevrimiçi), (Erişim; 04.04.2012).

[105] Tepe, İ., (2009), *Modern Ceza Hukuku Anlayışında İnternet Suçluluğu ve Türk Ceza Hukukundaki Yansımaları*, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Antalya.

[106] Turhan, O., (Nisan 2006), *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar),* Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Yayımlanmamış Planlama Uzmanlığı Tezi, Ankara.

[107] Tulum, İ., (2006) *Bilişim Suçları İle Mücadele,* Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Yönetimi Ana Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Isparta.

[108] Vatan Gazetesi, Birinci sayfa haberi 21.04.2012.

[109] www.bilgisayardefteri.com/ibd_disket_surucu.php. Bilgisayar Defteri, (Disket nedir?), (Çevrimiçi), (Erişim; 12.04. 2012).

[110] www. bilgisayar dershanesi.com /modemler.html Bilgisayar Dershanesi, (Modem nedir?), (çevrimiçi) (Erişim; 11.04. 2012).

[111] www.bilgisayarnedir.com.BilgisayarNedir?, (Çevrimiçi), (Erişim; 11.04.2012).

[112] www.bilisimakademi.net/kbOku.asp?kbID=31 Bilişim Akademi, (Bilişim Nedir?), (Çevrimiçi), (Erişim; 11.04. 2012).

[113] www.harddisknedir.com/ (Çevrimiçi), (Erişim; 11.04.2012).

[114] www.hurriyet.com.tr., (Çevrimiçi), (Erişim; 07.04.2012).

[115] www.ip-adres.com/tcp-ip-protokolleri.php (Çevrimiçi), (Erişim; 17.04.2012).

[116] www.Milliyet.com.tr. (Çevrimiçi), (Erişim; 11.04.2012).

[117] www.pcnet.com.tr/forum/windows-ipuclari/130519-tarayici-nedir-ogrenmek-isteyenler-icin.html (Çevrimiçi), (Erişim; 11.04.2012).

[118] www.sabah.com.tr (Çevrimiçi), (Erişim; 14.02. 2012).

[119] www.sessiztr.com/donanim/9022-mouse-fare-nedir.html.MouseNedir? (Çevrimiçi), (Erişim; 11.04.2012).

[120] www.stargazete.com.tr (Çevrimiçi), (Erişim; 28.04.2012).

[121] www.teknoloji.bugun.com.tr/internet-18-yasinda-150120-haberi.aspx (Çevrimiçi), (Erişim; 11.04.2012).

[122] www.tr.wikipedia.org/wiki. Wikipedia, (Çevrimiçi), (Erişim; 11.04.2012).

[123] www.turkeyforum.com/satforum/archive/index.TurkeyForum,(Bilişim), (Çevrimiçi), (Erişim; 13.02.2012).

[124] www.usbvitrini.com/?&Bid=1180873&/USB-BELLEK-ED%CUsbVitrini, (Usb Bellek Nedir?), (Çevrimiçi), (Erişim; 12.04.2012).

[125] www.veteknoloji.com/bilgibank.php?id=100 Teknoloji, (Çevrimiçi), (Erişim; 11.04. 2012).

[126] Yaycı, E., (2007), *Bilişim Suçları,* Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Ceza ve Ceza Usulü Hukuku Bilim Dalı, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

[127] Yazıcıoğlu, Y., (1997), *Bilgisayar Suçları, (Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile)*, 1. Baskı, İstanbul, Alfa Yayınları.

[128] Yazıcıoğlu, R. Y., (24.03.2001), *Bilgisayar ve Bilgisayar Şebekeleri İle İlgili Suçlar Konusunda TCK 2000 Tasarısı,* Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Paneli, Bursa, s.70-81.

[129] Yazıcıoğlu, R. Y., (2002), *Bilgisayar Ağları İle İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı,* Uluslararası İnternet Hukuku Sempozyumu, (21-22 Mayıs 2001), İzmir, Dokuz Eylül Üniversitesi Yayını, s.451-470.

[130] Yazıcıoğlu, R. Y., (2004), *Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi*, Hukuk ve Adalet Eleştirel Hukuk Dergisi, Y:1, S. 1, Ocak-Mart 2004, s.172-185.

[131] Yenidünya, A. C., Değirmenci O., (Nisan 2003), *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları,* 1. Baskı, İstanbul, Legal Yayıncılık.

[132] Yenisey, F., (2002), *İnternet Suçlarının Yeni İşleniş Biçimleri*, Uluslararası İnternet Hukuku Sempozyumu, İzmir, Dokuz Eylül Üniversitesi Yayını, (21-22 Mayıs 2001), s.447-450.

[133] Yıldız, S., (2007), *Suçta Araç Olarak İnternetin Teknik ve Hukuki Yönden İncelenmesi,* Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Yayımlanmamış Doktora Tezi, Konya.

[134] Yılmaz, S., (2010), *Banka veya Kredi Kartlarının Kötüye Kullanılma Suçu,* Türkiye Barolar Birliği Dergisi, Ankara, Y:22, S.87, s.262-298.

[135] Yılmaz, S., (2011), *5237 Sayılı TCK'nın 244. Maddesinde Düzenlenen Bilişim Alanındaki Suçlar,* Türkiye Barolar Birliği Dergisi, Ocak-Şubat 2011, Y:23, Ankara, S.92, s.62-100.

[136] Yücel, T. M., (1992), *Bilişim Suçları,* Ankara Barosu Dergisi, Yıl:49, Ankara, S.4, s.505-512.

EK-1

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Soyadı, Adı **: GÜRLER Fazıl**
Uyruğu **: Türkiye Cumhuriyeti**
Doğum Tarihi ve Yeri **: 23.09.1965 ANKARA**
Medeni Hali **: Evli, (3 çocuk babası)**
Tel **: 0 533 739 20 32**
E-Posta **: fazilgurler@hotmail.com**

EĞİTİM

DERECE	KURUM	MEZUNİYET TARİHİ
Lisans	Ankara Üniv. Hukuk Fak. Anadolu Üniv. İşl. Fak.	2000 2012
Lise	Elekt.Astsb.Haz.Okl./ANKARA	1983

İŞ DENEYİMİ

YIL	YER	POZİSYON
1983-2005 **(1998-2005)**	Türk Silahlı Kuvvetleri KKK.lığı MEBS Okulu	Mu.Tekns.Astsb. Öğretmen
2005 - 2006	Ankara Barosu	Stajyer Avukat
2006 – devam ediyor	Ankara Barosu	Serbest Avukat

YABANCI DİL İngilizce – Orta seviyede

HOBİLER Çiçek yetiştirmek, kitap okumak, belgesel izlemek, spor yapmak