T.C.
BAŞBAKANLIK
DEVLET PLANLAMA TEŞKİLATI MÜSTEŞARLIĞI
HUKUK MÜŞAVİRLİĞİ

BİLGİSAYAR AĞLARI İLE İLGİLİ SUÇLAR
(SİBER SUÇLAR)

Planlama Uzmanlığı Tezi

OĞUZ TURHAN

Nisan 2006
Ankara

ÖZET

Planlama Uzmanlığı Tezi

BİLGİSAYAR AĞLARI YOLUYLA İŞLENEN SUÇLAR (SİBER SUÇLAR)

Oğuz TURHAN

Bilgisayar ağları yoluyla işlenen suçların Dünya'da gittikçe artması ve toplum hayatını olumsuz etkilemesi nedeniyle, bu suçlarla mücadele edebilmenin yolları aranmaya başlanmıştır. Bu konuda ilk çalışmalar ve düzenlemeler, söz konusu suçlardan en çok müzdarip olan gelişmiş ülkeler tarafından yapılmıştır. Ülkemizde ise bu konu biraz geç ele alınmıştır. Bunun sebebi kurumsal ve kişisel bilgisayar kullanımının geç yaygınlaşması sonucunda, siber suçlar konusunun ceza hukuku açısından büyük bir problem teşkil etmemiş olmasıdır.

Çalışmanın genel olarak amacı, siber suçlarla mücadele konusunda uluslararası alanda ve Avrupa Birliğinde yapılan çalışmaların incelenmesi, konuyla ilgili ülkemizde mevcut olan düzenlemelerin yeterliliğinin değerlendirilmesi ve siber suç olgusunun hukuk alanında yaratmış olduğu sorunlara çözüm önerilerinde bulunmaktır.

Siber suçlar uluslararası boyutu da olan suçlardır. Bu suçları işleyenler, hukuk sistemlerindeki boşluklardan yararlanarak tutuklanma ve/veya kovuşturmadan kaçabilmektedirler. Bu nedenle, siber suçlarla mücadele edebilmek için her ülkenin, kendi hukuk sistemi içerisinde gerekli düzenlemeleri yaparak, bu suçları işleyenleri cezasız bırakmaması gerekmektedir. Ancak şu da bir gerçektir ki, sadece milli kanunlarda yapılan düzenlemeler, bu suçlarla mücadelede tek başlarına yeterli olamamaktadırlar. Siber suçlarla etkin bir mücadele yapabilmek için devletlerin ortak bir bilinçle hareket etmeleri gerekmektedir. Bu sebeple, ülkemizin de üyesi olduğu Avrupa Konseyi tarafından hazırlanan Siber Suç Sözleşmesi'nin bir an önce kabul edilmesi ve milli mevzuatımızın bu sözleşmeye uygun hale getirilmesi gerekmektedir.

Anahtar Kelimeler

Siber Suçlar, İnternet suçları, Bilişim Suçları, Bilgisayar Suçları.

ABSTRACT

Planning Expertise Thesis

CRIMES COMMITED BY MEANS OF COMPUTER NETWORK (CYBER CRIMES)

Oğuz TURHAN

Because of the gradual increase in the number of crimes commited by means of computer network and their negative effects on the community life, various ways have begun to be sought to fight such crimes. The first regulations on this matter were made by countries which suffer the most from these crimes. However, the issue was handled with delay in our country. The reason for the delay was that cyber crimes were not much of a problem in terms of our criminal law since the use of computers by corporations and individuals became widespread in our country later than it did in those countries.

The aim of this study is to analyse the existing studies which were made by other countries and especially by the European Union members on the issue of fighting cyber crime; to evaluate the sufficiency of the regulations in our country on this matter and to offer solutions to the problems caused by cyber crimes in the field of law.

Cyber crimes also have an international dimension. People who commit these crimes can evade being arrested and/or prosecuted because of the gaps in the law system. Thus, in order to be able to fight cyber crimes, each country should make the necessary regulations in its own law system and punish the ones who commit these crimes. However, it is also a fact that regulations made only in national laws can never be sufficient in fighting such crimes. All countries must act with a collective consciousness to pursue an efficient fight against cyber crimes. Therefore Convention on Cybercrime which is prepared by the Council of Europe should be accepted as soon as possible and our national legislation should be brought into consonance with this convention.

Key Words

Cyber Crimes, Internet Crimes, Information Technologies Crimes, Computer Crimes

İÇİNDEKİLER

KISALTMALAR

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ACLU	: American Civil Liberties Union
ARPA	: Advanced Research Project Agency
AT	: Avrupa Topluluğu
ATAD	: Avrupa Toplulukları Adalet Divanı
BK	: Borçlar Kanunu
BKKK	: Banka Kartları ve Kredi Kartları Kanunu
bkz.	: Bakınız
BM	: Birleşmiş Milletler
DDOS	: Distributed Denial Of Service
DNS	: Domain Name Server
EARN	: European Academic and Research Network
EC	: European Commission
ETCK	: Eski Türk Ceza Kanunu
EU	: European Union
FBI	: Federal Bureau of Investigation
FSEK	: Fikir ve Sanat Eserleri Kanunu
FTP	: File Transfer Protocol
IRC	: Internet Relay Chat
ISO	: International Standards Organization
İSS	: İnternet servis sağlayıcı
LAN	: Local Area Networks
m.	: Madde
MILNET	: Military Network
NAP	: Network Access Point
NSF	: National Science Foundation
ODTÜ	: Orta Doğu Teknik Üniversitesi
OECD	: Organization for Economic Co-operation and Development
pp.	: Page to page

RG	: Resmi Gazete
ss.	: Sayfadan sayfaya
TBMM	: Türkiye Büyük Millet Meclisi
TCK	: Türk Ceza Kanunu
TCP/IP	: Transmission Control Protocol/İnternet Protocol,
TRIPS	: Agreement on Trade-Related Aspects of Intellectual Property Rights
TÜBİTAK	: Türkiye Bilimsel ve Teknik Araştırma Kurumu
TUENA	: Türkiye Ulusal Enformasyon Altyapısı Projesi
TÜVAKA	: Türkiye Üniversiteler ve Araştırma Kurumları Ağı
vd.	: ve devamı
ve ark.	: ve arkadaşları
WAN	: Wide Area Network
YCGK	: Yargitay Ceza Genel Kurulu
YTCK	: Yeni Türk Ceza Kanunu

GİRİŞ

Son yıllardaki hızlı gelişimi göz önüne alındığında, bilişim teknolojisinin önümüzdeki yıllarda önemini artırarak insan hayatında yer almaya devam edeceği düşünülmektedir. Hatta bilişim teknolojilerindeki gelişmeler sanayi devrimi ile mukayese edilmektedir.

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi ve bu teknolojilerin en önemli uygulama alanı olan İnternet'in de buna bağlı olarak uygulama ve etki alanını genişletmesi sonucunda İnternet, kendi dilini, söylemini, hukukunu ve yaşam modunu oluşturmaya başlamıştır.

Her yeni teknolojide olduğu gibi, İnternet'de insanlara sağlamış olduğu faydaların yanında, toplumu katlanmaya mecbur bıraktığı bir çok zararlı eylem ve davranışı da beraberinde getirmiştir. Kötü niyetli insanların varlığı ve İnternet çalışma prensiplerinin yetersizliği, siber suçların oluşmasına ve hızla yayılmasına sebebiyet vermiştir. Gelişen bilişim teknolojisi yeni suç ortamları yarattığı için, siber suçlar, bilinen suçların bilgisayar ağları ortamında işlenmesinin yanısıra, bilgisayar ağlarına ve İnternet'e özgü yeni suçları da kapsamaktadır. Günümüzde bilgisayar kavramı, sadece hayatımızı kolaylaştıran bir yenilik olmaktan çıkmış, suç kavramı ile birlikte anılan bir araç haline de gelmiştir.

İnternet'i iletişim, bilgi edinme ve paylaşım gibi iyi amaçlarla kullanan kullanıcıların varlığına karşılık, teknolojinin yaramaz çocukları olarak adlandırılan; intikam alma duygusu, güce sahip olma, aç gözlülük, şehvet, macera gibi geleneksel olarak bireyleri suç işlemeye götüren nedenlerle hareket eden, sabotaj veya kaos yaratmak amacıyla çeşitli sistemlerin açıklarını bularak bu sistemlere atak yapan ve sisteme izinsiz girerek çeşitli hasarlar yaratan programcılar veya bilgisayar ile uğraşan bilgisayar korsanlarının (hackerların) ortaya çıkması, bilişim teknolojisinden faydalanarak İnternet'teki yerini almak isteyen "terör örgütleri"nin faaliyetlerini bu ortama taşıması, "hırsızlık" ve "dolandırıcılık" gibi suçların bu ortamda işlenmeye başlanması, İnternet'te izinsiz yayınlanan film, müzik ve oyunların oluşturduğu "lisans hakları ihlalleri" şeklindeki suçların genişlemesi, hakaret amaçlı sitelerin kurulması ve son olarak, bilgisayar orijinli resimler yoluyla yeni müstehcenlik

biçimlerinin oluşturulması ile sübyancı olarak adlandırılan kimselerin sapkın düşüncelerini yaşama geçirmeleri sonucu "pornografi" ve "çocuk pornografisi" gibi yasadışı yayınların giderek artması, İnternet'in kötü amaçla kullanılabileceğini açıkça gözler önüne sermiştir.

Bilgisayar ağları aracılığıyla gerçekleştirilen suçun oluşmasına sebep olan fiillerin gerek nitelik gerek nicelik olarak artan bir öneme sahip olması, bu konunun üzerinde dikkatle durulmasını gerektirmektedir. Gerçekten bilgisayar ağları üzerinden yapılan bir yayının ulusal sınırların da ötesine geçerek diğer kitle iletişim araçlarına nazaran daha geniş bir çevreye ulaşması sebebiyle daha etkili olduğu görülmektedir. Böyle bir gücün kötüye kullanılması durumunda suç içerikli materyallerin aynı hız ve etkiyle dünyaya yayılması son derece ciddi ve tehlikeli bir sonuç çıkarmaktadır. Bunun sonucunda da suç işlemeye meyilli insanlar için bilgisayar ağları çok cazip bir araç haline gelmektedir.

Yukarıda belirtilen sebeplerden dolayı kanun koyucular siber uzayda işlenen suçların önüne geçmek ve orada işlenen suçları cezasız bırakmamak için mevzuatlarında düzenleme yapma ihtiyacı duymuşlardır. Bu kanuni düzenleme çalışmalarında hızlı bir şekilde hareket edilmesi, ülkelerin gelişmişlik düzeyleriyle doğru orantılı olmuştur. Bugün için siber uzay alanında yapılması gereken hukuki düzenlemelerin, çoğu ülke tarafından geç olsa da yapılmış olması sevindirici bir gelişmedir.

Ülkemizde bu konu biraz geç ele alınmıştır. Fakat, kurumsal ve kişisel bilgisayar kullanımının geç yaygınlaşmasından dolayı, siber suçlar konusu ceza hukuku açısından büyük bir problem teşkil etmemiştir.

Çalışmanın genel olarak amacı, ülkemizde bilgisayar ağları yoluyla işlenen suçların özellikle de Dünya'da en çok kullanılan ağ olan İnternet'in, ceza hukuku alanında yarattığı sorunların ciddi bir şekilde çalışılmaması, sınırlı bir çerçevede tartışılması ve ülkemizde İnternet'in hem teknik hem de hukuki alt yapısının acilen oluşturulmasının önemli hale gelmesi sebebiyle siber suç olgusunun hukuk alanında yarattığı sorunların ortaya çıkarılması ve değerlendirmesinin yapılmasıdır.

Çalışmamız genel olarak beş bölümden oluşmaktadır. Bu çerçevede birinci bölümde İnternet'in teknik özellikleri hakkında genel bilgiler verilmiş, bugün için geçerli olan fonksiyonları açıklanmaya çalışılmış ve son olarak da ülkemizdeki gelişim süreci incelenmiştir.

İkinci bölümde ise siber suç olgusu, siber suçun tarihçesi ve bu suçların işleniş şekilleri, siber suçları işleyen suçlular, internet servis sağlayıcılarının cezai sorumlulukları detaylı bir şekilde incelenmiştir.

Üçüncü bölümde uluslararası organizasyonların siber suçlarla ilgili yapmış oldukları çalışmalara yer verilmiş, yine karşılaştırmalı hukukta (Amerika Birleşik Devletleri, Almanya, Fransa, İngiltere, Japonya) gelişmiş ülkelerin siber suçları nasıl düzenledikleri incelenmiştir.

Dördüncü bölümde, siber suçlarla mücadelede ülkelerin başarılı olabilmeleri için uluslararası işbirliğine gidilmesinin bir mecburiyet teşkil etmesi nedeniyle, bu yönde yapılan çalışmaların sonucu olarak siber suçları düzenleyen uluslararası tek belge olan "Avrupa Konseyi Siber Suç Sözleşmesi"nin hükümleri incelenmiştir.

Çalışmamızın son bölümünde ise Türk hukukunda siber suçlar incelenmiş, yeni ceza kanununda siber suçlarla ilgili düzenlemelere değinilmiş ve eski ceza kanunu ile yeni ceza kanununun bu suçlar bakımından mukayesesi yapılmıştır.

Sonuç ve öneriler bölümünde ise bütün bu inceleme ve analizlerin ışığında yapılması gereken düzenlemeler, alınması gereken tedbirler ve uygulanması gereken programlar sunulmuştur.

1. BİLGİSAYAR AĞLARI VE İNTERNET KAVRAMI – İNTERNET'İN TARİHÇESİ – UNSURLARI - İŞLEVLERİ

1.1. Bilgisayar ağları kavramı

Teknolojinin hızlı bir şekilde gelişmesiyle bilgi paylaşımı önemli hale gelmiştir. Bunun sonucunda, kişisel bilgisayarların, diğer bilgisayarlarla bağlantı sağlayarak kendi aralarında haberleşmelerine ve bilgi alış verişinde bulunmalarına ihtiyaç duyulması üzerine, bilgisayarların birbirine bağlanması sağlanmış ve buna bilgisayar ağları denmiştir.

Bir bilgisayar ağında en az iki bilgisayar yer alır. Bu bilgisayarlar yan yana duran iki bilgisayar olabileceği gibi, tüm dünyaya yayılmış binlerce bilgisayar da olabilir. Bilgisayarlar arasında genellikle kablo ile bağlantı sağlanırken, kablo bağlantısının mümkün olmadığı durumlarda mikro dalgalar ve uydular aracılığıyla da ağ içindeki iletişim kurulabilir[1].

Bilgisayar ağlarının ilk uygulamaları 1960'lı yılların sonlarında başlamış olmasına rağmen yerel bilgisayar ağlarının yaygınlaşmasının 1980'li yıllarda gerçekleşmesi ve yine kişisel bilgisayarların bu yıllarda çoğalması, bilgisayar ve iletişim teknolojilerinde önemli gelişmeler kaydedilmesi, bilgisayar ağlarının daha yararlı olmasını sağlamıştır.

Bilgisayar ağı, birbirine bağlı birden çok bağımsız bilgisayar anlamına gelir. İki bilgisayarın birbirinin kaynaklarını (diskini ya da diskinde yer alan bilgilerini) paylaşabilmesi ve birbiriyle konuşabilmesi onların birbirine bağlı olduğunu gösterir.

Bilgisayar ağları genel olarak üç grupta incelenebilir. Bunlardan birincisi, iki bilgisayardan bir kampüs büyüklüğüne kadar olan bilgisayar ağlarını kapsayan ağlardır. Bu ağlara "Yerel Bilgisayar Ağları" (LAN, Local Area Networks) adı verilir.

[1] Tuncel, Mustafa, Kişisel web sayfası. 16 ARALIK 2004. 14 OCAK 2005. http://www.mtuncel.com/bilgisayaraglari.htm

Yerel ağ içinde bilgisayarlar, yazıcılar, çiziciler, cd-rom sürücüleri ve diğer çevre birimleri yer alabilir. LAN, bilgisayar kullanıcılarına; uygulamalara ve cihazlara ulaşım, bağlı kullanıcılar arasında dosya değişimi, elektronik posta ve diğer uygulamalar yoluyla haberleşme gibi çeşitli avantajlar sağlarlar.

Burada belirtilmesi gereken önemli bir konuda, İntranet ve LAN'ın birbirlerinden ayrı tutulamayan iki kavram olduğudur. Eğer bir LAN şirket içinde kurulmuşsa ve şirket personelinin kullanımına açık ise "intranet" adını alır.

LAN; yazıcı, cd-rom gibi pahalı donanımlar, uygulama programları ve daha önemlisi kullanıcıların işlerini yapmaları için gerekli bilgi gibi hayati kaynakların elektronik olarak paylaşımına olanak sağladığı için kısa sürede popüler hale gelmiştir.

İkinci bilgisayar ağına ise "Geniş Alan Bilgisayar Ağları" (WAN, Wide Area Network) adı verilmiştir. Bu ağlar, bir ülke ya da Dünya çapında yüzlerce veya binlerce kilometre mesafe arasında iletişimi sağlayan ağlardır. WAN, coğrafi olarak birbirinden uzak yerlerdeki (şehirlerarası/ülkelerarası) bilgisayar sistemlerinin veya yerel bilgisayar ağlarının birbirlerine bağlanmasıyla oluşturulur. Genellikle kablo ya da uydular aracılığı ile uzak yerleşimlerle iletişimin kurulabildiği bu ağlarda çok sayıda iş istasyonu kullanılır. WAN üzerinde on binlerce kullanıcı ve bilgisayar çalışabilir.

Son bilgisayar ağına verilen isim ise "Şehirsel Bilgisayar Ağları"dır. (MAN, Metropolitan Area Network) Bu ağlar, LAN'ın kapsadığı alandan daha geniş, fakat WAN'ın kapsadığından daha dar mesafeler arası iletişimi sağlayan ağlardır. Genellikle şehiriçi bilgisayar sistemlerinin birbirleriyle bağlanmasıyla oluşturulur.

Bilgisayar ağlarının temel amacı, ağ içindeki kullanıcılar arasında iletişimi sağlamaktır. Bilgisayar ağları kullanıcılarına birçok olanak da sunar; kullanıcılar bilgisayar ağlarına girerek, yeni yazılımlar elde edebilirler. Yine bilgisayar destekli eğitimde ya da üniversiteler arası bilgi alışverişlerinde bilgisayar ağları çok etkin bir eğitim ortamı sağlar. Diğer bir olanak da uzak veri tabanlarına erişimdir. Bir bilgisayar kullanıcısı kendi bilgisayarından uzak veri tabanlarına girerek kendisine bir uçak bileti alabileceği gibi sermaye piyasası hakkında da bilgi sahibi olabilir.

1.2. İnternet'in Tanımı

"İnternational" ve "network" kelimelerinin birleştirilmesinden türetilen İnternet[2], "Ağların ağı" olarak da ifade edilmekte olup, bunun dışında da birçok tanımı yapılmıştır. Aşağıda bunlardan bir kaçı belirtilmiştir.

"İnternet, dünya üzerindeki milyonlarca bilgisayarın birbirlerine bağlanmaları ile oluşan global bir bilgisayar ağını ifade etmektedir[3]."

"İnternet, birden fazla haberleşme ağının birlikte meydana getirdikleri; metin, resim, müzik, grafik vb. dosyaları ile bilgisayar programlarının kısaca tüm insanlık bilgisinin paylaşıldığı ve karşılıklı olarak iletildiği, bilgisayarlar arasında kurulmuş bir ağdır[4]."

"İnternet, Dünya üzerinde bulunan bilişim ağlarının ve bilgisayarların birbirleri ile bağlantılandırılarak belli esaslar dahilinde, kendine özgü bir dille iletişimlerinin sağlandırılmasıdır[5]."

ABD Yüksek Mahkemesi vermiş olduğu bir kararda İnternet'i; "İnternet birbirleri ile bağlı bulunan bilgisayarlardan oluşan uluslararası ağdır. ...İnternet, bireylerin Dünya çapında haberleşmesi için tamamen yeni ve benzeri olmayan bir ortamdır." şeklinde ifade etmiştir[6].

Tüm yukarıdaki tanımlar dikkate alınarak İnternet'i, dünyadaki milyonlarca bilgisayarın (ki bu bilgisayarlar evde, okulda, üniversitede, devlet dairesinde veya özel sektörde olabilir) birbirine bağlanmasıyla, bilginin bir bilgisayardan diğerine, günün 24 saatinin istenilen her anında gönderilebildiği, herkese açık bir iletişim ağı olarak tanımlamak mümkündür.

1.3. İnternet'in tarihçesi

İnternet gibi bir sistemin oluşturulabileceği fikrini ilk ortaya atan kişi kimsenin beklemediği bir alanda uzman olan psikolog Joseph Carl Rebnett

[2] Sarıhan (1995:10)'a göre İnternet kelimesi özel isim olduğundan ilk harfi büyük olarak yazılmalıdır. Eğer küçük harfle yazılırsa birden çok ağı birleştiren bağlantıları ifade etmektedir.
[3] Boğaç ve Songür, 1999:282.
[4] Özdilek, 2002:13.
[5] Yenidünya ve Değirmenci, 2003:36.
[6] Özdilek, 2002:13.

Licklider'dir[7]. Masachussets Institude of Techology (MIT) de çalışmaya başlayan Licklider, Ağustos 1962'de yazmaya başladığı "Galaktik Ağ" (Galactic Network) notlarında, herkesin veri ve programlara basit bir şekilde ulaşabildiği, birbiriyle bağlantılı bir bilgisayar kümesi öngördü[8].

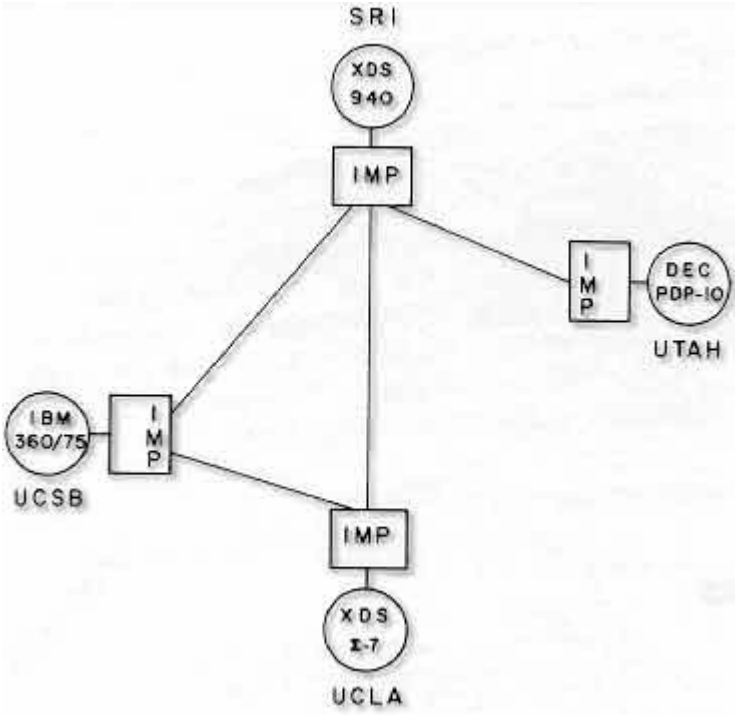
Amerika Birleşik Devletleri ile Sovyet Sosyalist Cumhuriyetler Birliği, İkinci Dünya Savaşı sonrası, soğuk savaş yıllarında birbirleriyle her alanda kıyasıya rekabet halindeydiler. Bu rekabet kendini daha çok silahlanma ve Uzay ile ilgili çalışmalarda göstermekteydi. Tam bu rekabetin ortasında Sovyetler Birliği'nin 1957 yılında Sputnik adlı ilk yapay uyduyu Uzay'a göndermesi, Amerika Savunma Teşkilatında büyük bir korku ve şaşkınlık yarattı[9]. Buna karşılık olarak Amerika da, savunma sanayinde ve bilim ve teknoloji alanında liderliği ele geçirebilmek için yapmış olduğu çalışmaları hızlandırarak, Savunma Bakanlığı'nın himayesinde İleri Savunma Araştırma Projeleri Kurulu'nu (Advanced Research Project Agency – ARPA)[10], bir savaş durumda askeri iletişimin kopmadan devam edebilmesini sağlamak yani herhangi bir bilgisayarda bulunan bilgileri bir diğer bilgisayara aktarabilmek amacıyla kurdu ve başına bu fikri ilk ortaya atan kişi olan Licklider'i getirdi.

ARPA kuruluş amacına uygun olarak çalışmaya ve projeler üretmeye başladı. Bu projelerden bir tanesinin amacı Los Angeles'taki Kaliforniya Üniversitesi (University of California, Los Angeles/UCLA), Santa Barbara'daki Kaliforniya Üniversitesi (University of California, Santa Barbara/UCSB), Stanford'daki Stanford Araştırma Enstitüsü (Stanford Research Institute/SRI) ve Salt Lake City'deki Utah Üniversitesi'nde (the University of Utah, Salt Lake City) bulunan dört büyük bilgisayar arasında veri iletişimini yani bir bilgisayarda bulunan verilerin diğerine aktarımı sağlayabilmekti. 1969 yılında dört bilgisayar arasında veri aktarımı gerçekleştirildi. ARPA'dan araştırma desteği alan bilim adamlarının birbirleriyle iletişimlerini sağlamak amacıyla kurulan deneme amaçlı ağ daha sonra geliştirilerek

[7] Özdilek, 2002:18
[8] Bila, 2001:78.
[9] Lloyd, 2000:8.
[10] Leiner, M.Berry at al., *A Brief History of the Internet*, Internet Society. 31 EKİM 2003. 26 ARALIK 2005. http://www.isoc.org/internet-history/brief.html, İleri Araştırma Projeleri Kurumu (ARPA) ismini 1971'de Savunma İleri Araştırma Projeleri Kurumu'na (DARPA), 1993'te tekrar ARPA'ya ve 1996'da tekrar DARPA'ya çevirmiştir.

ARPANET adını aldı[11]. Bundan sonra daha fazla bilgisayar ağa bağlanmaya başladı ve Aralık 1971'de ARPANET'te 23 host bilgisayar birbirine bağlandı[12].

Şekil 1: ARPANET (1969)



Kaynak : http://www.let.leidenuniv.nl/history/ivh/chap2.htm

ARPANET'e bağlı olan bilgisayarların, aynı tip ve özellikte olmamalarından kaynaklanan bazı sorunların ortaya çıkması sebebiyle, ARPA mühendisleri bu sorunları ortadan kaldırmak amacı ile çalışmaya başladılar. Stanford'daki uzmanlarla yapmış oldukları ortak çalışmaların sonucunda, farklı şebekelerin birbirleri ile iletişimlerine izin veren ortak bir dil geliştirdiler ve geliştirdikleri bu dile, İletim Kontrol Protokolü/İnternet Protokolü, genel olarakda İnternet Protokolleri (A Transmission Control Protocol/İnternet Protocol- TCP/IP) adını verdiler. 1980'lerde ARPA, araştırma ağına bağlı bilgisayarlarını TCP/IP protokolüne dönüştürmeye

[11] Sarıhan, 1995:16.
[12]Griffiths, T. Richard. *The Creation of ARPANET.* Leiden University. 11 EKİM 2002. 06 EYLÜL 2004. http://www.let.leidenuniv.nl/history/ivh/chap2.htm

başladı. 1983'te ARPANET'in beklenenden daha fazla büyümesi sonucunda, askeri bölümün ayrılması düşünüldü. Bu düşünce sonucunda ARPANET araştırma ve askeri amaçlı olarak ikiye ayrıldı ve araştırma amaçlı kısım ARPANET adıyla devam ederken, askeri amaçlı kurulan yeni ağa ise MİLNET ismi verildi[13].

ARPANET'e giderek küçük ağların ve diğer kullanıcıların da bağlanması sonucu kontrol edilemez bir büyüme meydana geldi. Bunun üzerine Ulusal Bilim Vakfı (National Science Foundation - NSF), İnternet'te kamu kullanımı için beş süper bilgisayarı devreye soktu. Bu bilgisayarlar zamanın en gelişmiş bilgisayarlarıydı, fakat bir süre sonra bu bilgisayarlar da yetersiz olmaya başladı. NSF bunun üzerine yeni bir ağ kurmaya karar verdi ve kurdukları bu yeni ağa NSFNET adı verildi. NSFNET uzun bir müddet Amerika'da kullanıldı ve giderek büyüdü. ARPANET'in bütün bağlantıları NSFNET'e aktarıldı. ARPANET, Haziran 1990'da kullanımdan kaldırıldı. Yerini ABD, Avrupa, Japonya ve Pasifik ülkelerinde ticari ve hükümet işletimindeki omurgalar[14] (backbone) aldı.

ARPANET'in kaldırılmasına rağmen, İnternet Protokolleri kullanılmaya devam etti ve geliştirildi.

İnternet 1994'ten sonra büyük bir hızla artan yeni ağların katılımıyla bütün Dünya'ya yayılarak günümüzdeki şeklini aldı[15]. İstatistikler[16] gösteriyor ki İnternet hızla yaygınlaşmakta ve insan hayatında daha fazla yer alarak hayatın vazgeçilmez parçalarından biri olma yolunda ilerlemektedir.

1.4. İnternet'in teknik altyapısı

1.4.1. İnternet protokolleri (TCP/IP)

Bilgisayarların da insanlar gibi düzgün ve doğru bir iletişim sağlayabilmeleri için kendi aralarında ortak bir dil kullanmaları gerekmektedir. Yani model ve markadan bağımsız olmak üzere (kişisel tabanlı bilgisayarlardan büyük sistemlere

[13] Bila, 2001:87.
[14] Bilgisayar ağlarındaki çok yüksek kapasiteli hat ya da seri bağlantı yollarına verilen addır. Omurgalar, şehirleri, ülkeleri ya da kıtaları internet üzerinde birbirine bağlar.
[15] Sınar, 2001:23.
[16] Türkiye'de 2002 yılında 4 milyon İnternet kullanıcısı varken, bu sayı 2005 yılında 15 milyona çıkmıştır (2004 Yılı Yıllık Programı s.205; 2005 Yılı Yıllık Programı:213)

kadar) farklı bilgisayarlar arasında ağ üzerinde iletişim kurulabilmesi için ortak bir dile ihtiyaç vardır.

Bilgisayarların birbirleri ile İnternet veya başka bir ağ aracılığıyla iletişim sağlayabilmeleri, veri paylaşımını düzgün bir şekilde gerçekleştirebilmeleri amacıyla geliştirilen bu ortak dile "İnternet protokolleri" ya da TCP/IP protokoller ailesi denir.

Bir başka ifadeyle "İnternet protokolleri", bilgisayarlar ile veri iletme ve alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini mümkün kılan pek çok veri iletişim protokolünün genel adıdır[17].

İnternet'in günümüzde bu kadar yaygın olarak kullanılması, TCP/IP adı verilen ve çeşitli protokollerden oluşan bu protokol sayesinde olmuştur. Bu protokollere örnek olarak, dosya alma ve gönderme protokolü (FTP, File Transfer Protocol), elektronik posta iletişim protokolü (SMTP - Simple Mail Transfer Protocol), TELNET protokolü verilebilir. Adını sıkça duyduğumuz "www" ortamında birbirine link objelerin iletilmesini sağlayan protokol ise Hiper-Metin Transfer Protokolü (HTTP - Hyper Text Transfer Protocol) olarak adlandırılmaktadır[18]. TCP/IP protokolü özel iletişim ağlarında da (intranet, extranet vs.) kullanılabilir. Özellikle pek çok farklı tipte bilgisayarı veya iş istasyonlarını birbirine bağlayan yerel ağlarda (LAN) kullanımı yaygındır[19].

İnternet'te kullanılmakta olan tek protokol ailesi TCP/IP olmamakla birlikte, diğer protokollerin çok fazla kullanılmaması sebebiyle günümüzde İnternet ortamında kabul edilen evrensel dil TCP/IP protokol ailesidir.

1.4.2. Dünyayı saran ağ (Web-www)

İnternet, genellikle Dünyayı Saran Ağ ile bir tutulmasına rağmen aynı şey değildir. Dünyayı Saran Ağ, genel olarak ağ üzerinde bir bilgi kümesi iken İnternet, ağın fiziksel yönünü yani bilgisayarlar, kablolar ve bağlantılar kümesini ifade eder[20].

---

[17] Gökçol, Orhan. *TCP/IP Nedir?*. Orta Doğu Teknik Üniversitesi. 16 KASIM 1997. 25 MART 2005. http://www.po.metu.edu.tr/links/inf/css25/bolum1.html

[18] *TCP/IP*. TechTarget. 16 HAZİRAN 2005. 03 AĞUSTOS 2005. http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci214173,00.html

[19] Gökçol, Orhan. *TCP/IP Nedir?*. Orta Doğu Teknik Üniversitesi. 16 KASIM 1997. 25 MART 2005. http://www.po.metu.edu.tr/links/inf/css25/bolum1.html

[20] Bila, 2001:115

Dünyayı Saran Ağ, yerel ve genel ağlar üzerinden bilgilere ulaşmayı ve onların paylaşımını sağlayan bir metottur. Dünyayı Saran Ağ, küresel ve bağımsız bir çevredir. İnternet'teki bilgilere (yazı, şekil, ses, video, hesap servisleri) standart adlandırma ve erişim anlaşmaları kullanılarak ulaşmamızı sağlayan bir çoklu hiper ortam sistemi ve İnternet teknolojisidir.

Dünyayı Saran Ağ sayesinde kullanıcılar, renkli resimler ve yazıların iç içe olduğu, animasyonların kullanıldığı sayfalara erişirler. Her sayfanın bir adresi vardır. Bu adreslere URL (uniform resource locator, tekdüze kaynak yer-belirleyici) denir. Dünyayı Saran Ağ sayfaları arasında, bağlantılar (link) tanımlanarak birinden diğerine geçiş mümkün hale gelmektedir. Dünyayı Saran Ağ sayfaları, İnternet'te bilgi aktarımını olanaklı kılan mekanizmalardır. İnsanlar, web gözatıcısı (browser) adı verilen bilgisayar programlarıyla, bu tipte hazırlanmış bilgi sayfalarına, bu sayfaların adreslerini yazarak bağlanabilirler ve tüm bu entegre bilgileri görebilirler.

1.5. İnternet'in altyapısı

İnternet üzerinden veri iletişimi, İnternet omurgası (backbone) ismi verilen ana iletişim hatları üzerinden sağlanır. İnternet teknolojisini ilk kullanan ve geliştiren Amerika'da kurulan İnternet omurgası başlangıçta Ulusal Bilim Vakfı (National Science Foundation-NFS) tarafından işletilirken, Mayıs 1993'den itibaren teknolojinin yeterince olgunlaştığı gerekçesiyle tümüyle özel sektöre devredilmiştir. Günümüzde, İnternet omurgası işletmek isteyen özel sektör kuruluşları, bu alanda belirlenen kurallara uygun olarak yatırım yaparak İnternet omurgası işletebilme hakkına sahip olabilmektedirler. ABD'de kurulan İnternet omurgaları önce dört daha sonra on bir Ağ Erişim Noktası (Network Access Point – NAP) aracılığı ile birbirlerine bağlanarak, bir omurgadaki veri trafiğinin bir diğer omurgaya aktarabilmesini sağlamışlardır. ABD omurgalarında en önemli nokta, yeni kurulan ya da kurulacak olan bir omurganın trafiğinin ya yeni bir NAP ile ya da varolan NAP'ların aracılığı ile tüm diğer NAP'lara doğrudan aktarılma zorunluluğudur.

Devletler genellikle İnternet alt yapısını ülkenin enformasyon alt yapısı içinde ele alarak, eylem planlarını buna göre yapmaktadırlar[21]. Ülkemizde Ulaştırma

[21] İÇEL, 2000:413.

Bakanlığı tarafından yürütülen Türkiye Ulusal Enformasyon Altyapısı Projesi (TUENA) kapsamında, uluslararası boyutta araştırma ve incelemeler yapılmakta ve ulusal enformasyon altyapısının geliştirilmesi için alınacak önlemler üzerinde durulmaktadır. TUENA projesi, ülkemizin enformasyon ve iletişim teknolojisi alanındaki eksikliklerinin giderilmesi açısından büyük önem taşıdığından, söz konusu projeye destek vermek ülkemiz açısından bir zorunluluk teşkil etmektedir[22].

1.6.İnternet'in İşlevi

İnternet, bilgisayarlar arasında veri iletişimini güvenli ve kesintisiz bir şekilde sürdürebilmek için düşünülmüş ve tasarlanmıştır. Bu sebeple İnternet'in ana işlevinin ağ içerisinde çift yönlü bilgi aktarımını sağlamak olduğu söylenebilir. İnternet'in bu işlevi sayesinde İnternet erişimi olan bir kullanıcı, eğer kendisine yetki verilmişse, İnternet'e bağlı diğer herhangi bir bilgisayardaki bilgilere erişebilir, onları kendi bilgisayarına aktarabilir, kendi bilgisayarından da İnternet erişimi olan başka bir bilgisayara bilgi gönderebilir[23].

İnternet'in sunduğu hizmetlerin çeşitliliğini örneklerle somutlaştırmak gerekirse, eğer bir akedemisyen iseniz İnternet vasıtasıyla hemen hemen Dünya'daki tüm kütüphanelerde araştırma yapabilir, yine konunuzla ilgili dergileri ve bilimsel yayınları inceleyebilirsiniz. Eğer iyi bir sinemasever iseniz, henüz vizyona girmemiş filmlerin tanıtımını izleyebilir ve önceden yerinizi ayırtabilirsiniz. Alışveriş yapmayı çok seven ve modayı takip eden biriyseniz, tüm dünyadaki ürünleri görebilir ve beğendiklerinizi sipariş edebilirsiniz. Ucu açık bir dünya olan İnternet aracılığıyla yapılabilecek şeylerin sayısı her geçen gün artmaktadır.

İnternet'in en çok kullanılan işlevsel özellikleri elektronik posta, posta listeleri ve haber grupları, tartışma öbekleri (usenet), İnternet'te sohbet, dosya aktarma protokolü ve telnettir. Aşağıda kısaca bunlardan bahsedilecektir.

---

[22] Sınar, 2001:29.
[23] Ankara Ticaret Odası Yayınları. *Elektronik Ticaret ve İnternet.* Yayın No:08. 01 HAZİRAN 1999. s.21. 28 MART 2005. http://195.155.145.1/turkce/index10.html.

1.6.1. Elektronik posta (e-mail, e-posta, ileti)

E-posta veya ileti Dünya'da en çok kullanılan İnternet faaliyetidir[24]. 2000 yılında günde 10 milyar ileti gönderilirken, 2005 yılında bu rakamın günde yaklaşık olarak 35 milyar ileti olacağı tahmin edilmekteydi[25]. İnternet'in bu en çok kullanılan unsurunu, İnternet kullanıcılarının siber uzayda mesaj ya da daha genel anlamıyla bilgi alış verişini sağlayan bir posta sistemi olarak tanımlayabiliriz.

E-posta, baslangıçta sadece düz yazı içeren mesajlar göndermek amacıyla geliştirilmişken, 1995'li yıllardan sonra geliştirilen tekniklerle, e-posta içinde kompozit yapıların (resim, ses, video, html dokümanları, çalışabilir program vb.) kullanımı mümkün hale gelmiştir. Artık günümüzde hemen hemen her türlü e-posta programları bu formatları desteklemektedir.

E-postalar, geleneksel postalar gibi adresleme sistemine ihtiyaç duyarlar. E-posta adresleri, kullanıcılara erişim sağladıkları servis sağlayıcılar aracılığıyla verilebileceği gibi, İnternet üzerinde bulunan çok sayıdaki e-posta sistemlerinden de ücretsiz olarak temin edilebilir.

E-posta günümüz iletişim araçlarının en hızlısı ve ucuzu olması sebebiyle gün geçtikçe daha fazla insan tarafından kullanılmaktadır. Şu an bazı güvenlik zaafiyetleri olsa bile ticari kullanımının da artmasıyla beraber bu zaafiyetlerin ortadan kaldırılması için yapılan çalışmaların yakın bir zamanda sonuca ulaşacağı düşünülmektedir.

1.6.2. Posta listeleri ve haber grupları

Posta listeleri, belirli konularla ilgilinen kişilerin, İnternet üzerinden belirledikleri konu hakkında e-posta yoluyla görüş alış verişinde bulunmak için oluşturdukları bir araçtır. Posta listeleri, aynı konuyla ilgilenen kişilerin e-posta adreslerinden oluşan bir listedir. Oluşturulan bu liste sayesinde, katılımcılardan birinin göndermiş olduğu e-posta, listeye kayıtlı diğer tüm katılımcılara aynı zamanda ulaşır ve listeye üye olanlardan aldıkları e-posta konusunda görüş beyan etmek isteyenler görüşünü tüm gruba gönderebilirler. Posta listelerinin sağlamış

[24] Collins, 2001:19.
[25] Collins, 2001:19.

olduğu bu olanak sayesinde birbirini hiç tanımayan ancak ilgi alanları kesişen kullanıcılar, aynı konu hakkında görüş bildirebilirler ve tartışma yapmak suretiyle yeni fikirlerin üretilmesine katkı sağlamış olurlar[26].

Haber gruplarının posta listelerinden farkı, bu gruplara üye olmanın gerekli olmamasıdır. Haber grupları, internet ağı üzerinden tartışmaların yapılabildiği bölümlere verilen isimdir[27]. Haber grupları bir gazete ya da dergiye yazı göndermek olarak düşünülebilir. Herkes gönderilen mesajı okuyabilir ve gönderen kişiye özel ya da açık bir cevap yazma hakkına sahiptir[28].

Haber grupları, akedemik tartışmalardan fıkralara kadar değişen bir yelpaze ortaya koymaktadırlar. Haber gruplarına verilen isimler gruptaki tartışmaları çağrıştıracak şekilde takılsa da binlerce haber grubu içerisinde aranan haberlere ulaşmak zor bir iştir. Bu sebeple haber grupları alt gruplara bölünmüştür[29].

1.6.3. Tartışma öbekleri (Usenet)

Tartışma öbekleri, dünya üzerindeki milyonlarca ağ kullanıcısının (internet/bitnet vb) çok değişik konularda haberler, yazılar gönderdiği bir tartışma platformudur[30]. Tartışma öbeklerinden haber almak veya göndermek için İnternet'in kullanılması şart değildir. Yani tartışma öbekleri İnternet'e özgü değildir. Kişiler diğer farklı bilgisayar ağlarına bağlı olarak da tartışma öbeklerinden haber alabilir veya gönderebilir.

Bu öbekler, konularına göre belirli bir hiyerarşide oluşturulmuş tartışma öbeklerinden (news group, haber grubu) oluşur. Kullanıcı, iletisini içerik olarak en uygun öbeğe gönderir. Kullanıcıların gönderdiği postalar (haber, değişik konularda yazı vb.) İnternet için, Ağ Haberleri Transfer Protokolü (Network News Transfer Protocol-NNTP) isimli bir internet protokolu kullanılarak iletilir.

---

[26] Akçam, 1999:89.
[27] Sınar, 2001:36.
[28] Stonebank, Michael. *What is Usenet* News?. University of Surrey Guildford. 28 EKİM 1994. 30 MART 2005. http://www.eps.surrey.ac.uk/FAQ/usenet.html
[29] Bila, 2001:110
[30] Gökçol, Orhan. *Usunet Nedir?*. Orta Doğu Teknik Üniversitesi. 16 KASIM 1997. 31 MART 2005. www.po.metu.edu.tr/links/inf/css25/bolum4.html

Tartışma öbeklerinde, haber akışını kontrol eden üst bir otorite yoktur. Sadece, yerel tartışma öbeği servis sağlayıcıları, bünyelerinde bulundurdukları öbek sayılarını kontrol edebilmekte ve bazı öbekleri kendi listelerinden çıkarabilmektedirler.

Genelikle tartışma öbeği grupları, bir yerel sorumlu (servis sağlayıcının bulunduğu yerdeki yerel sorumlu- usunet işleteni) tarafından yönetilirler. Yani iletiler haber grubundan sorumlu bir kişiye gönderilir ve o kişi bu iletileri toplu olarak dağıtıma sokar. İşte bu haber grubunun bağlı olduğu sunucudan sorumlu olan kişiye tartışma öbeği işleteni denmektedir. Bu sistem sayesinde iletiler hukuka ve gruba uygunluk gibi yönlerden bir denetime tabi tutulmuş olur.

1.6.4. İnternet'te sohbet

İnternet'te sohbet, Dünya üzerindeki değişik kullanıcıların İnternet'e bağlı oldukları ve aynı sunucuyu ya da birbirine bağlı sunucuların şebekesini seçtiklerinde, birbirleri ile iletişim kurmalarını sağlayan bir ortamdır. Daha açık bir ifade ile, Dünya'nın farklı yerlerindeki kullanıcılar, İnternet'te sohbet vasıtası ile İnternet üzerinden eş zamanlı olarak sohbet etme imkanına sahip olmaktadırlar[31].

IRC kullanıcıları genellikle gerçek isimlerini kullanmazlar bunun nedeni, IRC'nin bir veya birden fazla takma isim (rumuz ya da nick name) kullanılmasına ve değiştirilmesine imkan tanımasıdır[32].

IRC olarak nitelenen sohbet faaliyetlerinin, sadece İnternet'in bir eğlence aracı olarak kullanıldığını düşünmek pek doğru değildir. Zira İnternet sohbetleri, Dünya'nın dört bir yanındaki farklı ülkelerden katılan insanları, aynı anda tek bir kanalın içerisine toplamasıyla, bugüne kadar eşi görülmemiş bir iletişim zenginliği gerçekleştirmekte ve geleceğe dönük yeni iletişim modellerine de öncülük etmektedir[33].

[31] Bila, 2001:128.
[32] Bila, 2001:128.
[33] Sınar, 2001:38.

1.6.5. Dosya aktarma protokolü

Dosya aktarma protokolü, ilk geliştirilen İnternet protokollerinden birisidir. İnternet'e bağlı bir bilgisayardan, diğerine (her iki yönde de) dosya aktarımı yapmak için geliştirilen bir internet protokolüdür.

Dosya aktarma protokolü ile bir bilgisayardan diğer bir bilgisayara dosya aktarımı yapılırken, o bilgisayar ile etkileşimli olarak aynı anda (on-line) bağlantı kurulur ve protokol ile sağlanan bir dizi komutlar yardımıyla iki bilgisayar arasında dosya alma/gönderme işlemleri yapılır.

1.6.6. Telnet

Telnet, İnternet yoluyla bir bilgisayardan diğerine bağlanılarak, bağlanılan bilgisayar programlarının uzaktan çalıştırılabilmesini sağlayan sisteme verilen isimdir. Bağlanılan makineye girebilmek için orada bir kullanıcı isminin olması gerekir. Telnet yapmak diye bilinen deyim, telnet protokolü kullanan bir program ile İnternet üzerindeki bir makineye bağlanmayı ifade eder[34].

Telnet sistemi, bilgiye daha kolay ve hızlı bir şekilde ulaşabilme gereksinimin bir sonucu olarak ortaya çıkmıştır[35].

Ayrıca, telnet yazı tabanlı olması ve bazı UNIX işletme sistem komutları bilgisini gerektirmesi nedeniyle, web'in gerisinde kalmıştır. Fakat bu durum bilgisayar korsanları için tersidir. Yani telnet, bilgisayar korsanlarının amaçlarını gerçekleştirebilmeleri için için hala kullanışlı bir araçtır. Bunu bir örnekle açıklamak gerekirse, bir bilgisayar korsanı başka bir bilgisayara izinsiz giriş yapar ve daha sonra bu bilgisayardan diğer bir bilgisayara girer ve bu böyle devam eder. Bu sayede kendi izini saklayabilir. Bu durum, kanun uygulayıcılarının bir bilgisayar korsanının izini sürmesini ve yakalamasını zorlaştırmakta olup, yine mahkemede suçun kim tarafından işlendiğinin belirlenmesini ve geçerli kanıtların toplanmasını oldukça güçleştirmektedir[36].

---

[34]Bugman. *Telnet Nedir?*. PCnet - Bilgisayar ve İnternet Dergisi. 22 EKİM 2002. 01 NİSAN 2005. http://www.pcnet.com.tr/modules.php?name=Forums&file=viewtopic&p=116314

[35] Sınar, 2001:40.

[36] Gringras, 1997:8.

1.7. İnternet işlevlerinin yerine getirilmesi

İnternet'in çok yönlü işlevlerinin kullanıcıların hizmetine sunulabilmesi görevi, İnternet alanında faaliyet gösteren özneler tarafından yerine getirilir[37]. Bunlara, "İnternet'in hukuk özneleri", "İnternet işlevlerini yerine getiren özneler" ya da kısaca "İnternet özneleri" denmektedir. Altı tane İnternet öznesi bulunmaktadır. Bunlar telefon/telekomünikasyon idareleri, İnternet servis sağlayıcıları, sunucular, içerik sağlayıcılar, barındırıcılar ve erişim sağlayıcılarıdır.

1.7.1. Telefon/Telekomünikasyon idareleri

İnternet, kullanıcılara genel haberleşme kanallarından yararlanarak bilgi iletişimi sağlayan bir sistemdir ve bu iletişim sağlanırken kullanılan kanallar, her ülkenin ilgili mevzuatı çerçevesinde, fakat genellikle de ulusal telefon/telekomünikasyon idarelerinin sahip olduğu ve kontrolü altında tuttuğu telefon hatlarıdır[38].

Bu nedenle, İnternet servis sağlayıcı (İSS) hizmeti görmek isteyen bir girişimci, İnternet'e bağlantı sağlamak için kullanacağı hatları elde etmek üzere önce telefon/telekomünikasyon kuruluşu ile bir anlaşma imzalamak zorundadır. Telefon/telekomünikasyon işletmelerinin fonksiyonu tamamen teknik olup, zorunlu iletişim altyapısının, belli şartlar altında, İSS girişimcisine tahsis edilmesinden ibarettir[39].

Bu teknik ilişki açısından bakıldığı zaman, telefon/ telekomünikasyon işletmeleri, İnternet sistemi içinde birinci özne olarak karşımıza çıkmaktadır.

1.7.2. İnternet servis sağlayıcıları (İSS)

İnternet servis sağlayıcıları (İSS), bireylerin (özel kişilerin ve özel hukuk veya kamu hukuku tüzel kişilerinin) İnternet'e bağlanmalarını, İnternet üzerinden iletişim kurmalarını sağlayan ve İnternet'in sağladığı olanakları kullanmalarına

[37] Sırabaşı, 2002:114.
[38] Güran ve ark., 2000:17.
[39] Güran ve ark., 2000:17.

aracılık eden gerçek veya tüzel kişilerdir[40]. Yani, İnternet'e geçiş İSS'ler aracılığı ile olur. Şu halde, İnternet'in anahtarını elinde tutan özne İSS'lerdir[41].

İSS'lerin vermiş oldukları hizmeti farklı ve önemli kılan şey, İSS'lerin başkaları tarafından hazırlanan içeriği kendi "sunucularında" (server) stoklayabilme imkanına sahip olması ve stokladıklarını internet bağlantılarını kullanarak siber dünyaya aktarabilme yeteneğine sahip olmalarıdır.

İnternet sistemi içinde birinci derecede önem taşıyan aktör ve dinamik hüviyetteki hukuk öznesi İSS işletmelerdir. Türk mevzuatı bakımından, İSS olabilmek için özel hüküm yoktur. Ancak, İSS'lerin faaliyette bulunabilmeleri için "Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği"[42]nde belirtilen belli şartları yerine getirmeleri gerekmektedir. Öncelikle 406 sayılı Telgraf ve Telefon Kanununun Ek 18'inci maddesi kapsamında yer alan telekomünikasyon hizmetleri ve/veya kurulacak ve işletilecek telekomünikasyon altyapıları, Telekomünikasyon Kurumu tarafından verilen 2'nci Tip Telekomünikasyon Ruhsatı ile yürütülebilmektedir. İSS'lerin faaliyetlerinin de bu kapsamda olması sebebiyle, kendilerini Telekomünikasyon Kurumunda "genel izin"[43] kapsamında kayıt ettirmeleri gerekmektedir.[44]

---

[40] Özdilek, 2002:93.

[41] Güran ve ark., 2000:12.

[42] Söz konusu yönetmeliğe http://www.tk.gov.tr/Duzenlemeler/Hukuki/yonetmelikler/thayy.pdf adresinden ulaşabilmek mümkündür. (12.12.2005)

[43] Genel İzin, Bir telekomünikasyon hizmetinin yürütülmesi için, Telekomünikasyon Kurumu tarafından işletmecileri belirli genel şartlara ve Telekomünikasyon Kurum'u nezdinde kayıt yaptırılmasına tabi olarak yetkilendiren genel düzenleyici işleme denmektedir.

[44]Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği'nin 28'inci maddesine göre, Genel İzin kapsamında kayıtlanmak için Kuruma başvuru yapan sermaye şirketinde aşağıdaki şartlar aranmaktadır :

a) Türkiye Cumhuriyeti Kanunlarına göre, yalnızca yetkilendirmeye tabi faaliyetleri yürütmek üzere anonim veya limited şirket statüsünde kurulmuş olması,

b) Şirketin tescil ve ilan olduğu Ticaret Sicil Gazetesinde yer alan ana sözleşmesinde faaliyet alanı kapsamında "telekomünikasyon hizmeti verilmesi ve/veya altyapısı kurulması ve işletilmesi" ifadesine veya yetkilendirilmeyi talep ettiği telekomünikasyon faaliyetine yer verilmiş olması,

c) Şirket hisselerinden en az yüzde beş (%5)'ine sahip ortaklar ve tüzel kişiliği idare ve temsile yetkili kişilerin Türk Ceza Kanununun İkinci Kitap Birinci Babında yer alan Devletin şahsiyetine karşı işlenen suçlarla, Terörle Mücadele Kanununda yazılı suçlardan hürriyeti bağlayıcı ceza ile hüküm giymiş olmaması. Ayrıca, 2. Tip TR başvuruları için, söz konusu kişilerin bu koşulun yanı sıra; taksirli suçlar hariç olmak üzere affa uğramış olsa dahi, 4389 sayılı Bankalar Kanununun 22nci maddesi ile 2499 sayılı Sermaye Piyasası Kanunu hükümlerine muhalefet, yahut basit ve nitelikli zimmet, irtikap, rüşvet, hırsızlık, dolandırıcılık, sahtecilik, inancı kötüye kullanma, hileli iflas ve konkordato, kaçakçılık suçları, resmi ihale ve alım-satımlara fesat karıştırma, kara para aklama, vergi

Görüldüğü üzere ülkemizde İSS olarak faaliyette bulunabilmek için genel izin için aranan şartları yerine getirip başvuruda bulunmak yeterlidir.

İSS'lerin cezai sorumluluğu aşağıda ayrı bir başlık olarak incelenecektir.

1.7.3. Sunucu (Server)

Sunucu belli kapasitesi olan ve diğer bilgisayarlara hizmet sağlayan bir bilgisayar veya bir programdır. Sunucu aynı zamanda dijital bilgilerin saklandığı bir manyetik ortamdır[45]. İSS'ler, üstlendikleri çeşitli hizmetleri yerine getirebilmek için sunucuları kullanırlar. Herhangi bir özel veya tüzel kişinin kendi başına sunucu hizmeti vermesi de mümkündür. Diğer bir deyişle, bir özel veya tüzel kişi, kendisine ait bilgileri bir manyetik ortamda saklayarak sunucu fonksiyonunu görebilir. Ancak sunucu işlevinin ana unsuru, gerçek veya tüzel kişinin başkalarına ait bilgilerin manyetik bir ortamda depolanmasını sağlamasında ortaya çıkar. Eğer başkalarına ait bilgileri saklayan gerçek veya tüzel kişi aynı zamanda kendisi de İnternet'e bağlantı kurma özelliğine de sahipse, bu gerçek ve tüzel kişi artık İSS statüsüne girer ve İSS'lerın tabi olduğu hukuki rejime tabi olur[46].

1.7.4. İçerik sağlayıcılar

İçerik sağlayıcı, İnternet kullanıcıları tarafından erişilebilen herhangi bir İnternet yayınının içeriğini hazırlayan veya bilgiyi bizzat üreten İnternet öznesidir. Örneğin, bir web sayfasının içeriğini hazırlayan ve İnternet'e yükleme işlemini de İSS'nin aracılığıyla gerçekleştiren İnternet öznesine, içerik sağlayıcı denir[47].

1.7.5. Barındırıcı (Host)

İnternet uygulamalarının elektronik ortamda iletilebilmesi için gerekli uç birim görevini gören her bilgisayara barındırıcı (host), bu hizmetin sunulmasına ise

---

kaçakçılığı veya vergi kaçakçılığına teşebbüs ya da iştirak suçlarından dolayı hüküm giymiş olmaması.
d) Bu Yönetmeliğin hizmete özel eklerinde belirtilecek diğer şartların sağlanması.

[45] Güran ve ark., 2000:13.
[46] Sınar, 2001:41.
[47] Sınar, 2001:41

barındırma (hosting) denir[48]. İnternet ortamında her barındırıcının bir IP adresi ile ilişkilendirilmiş alan adı (domain name) vardır. Akılda kalabilir ve kullanımı kolay alan adları, İnternet'in kamuya açık bir yapı olmasını desteklemek amacıyla ortaya çıkmış ve DNS (Domain Name Server) aracılığı ile IP adresleri ile ilişkilendirilerek kullanılmaya başlanmıştır[49].

İSS'nin, bir abonesine ait web sayfasını kendi bilgisayarlarında saklaması ve bu sayfaya İnternet'ten girilmesine olanak vermesi barındırmadır. Reklam verenlerin reklamlarının manyetik ortamda tutulması keza barındırma işlemidir[50].

1.7.6. Erişim sağlayıcı

Erişim sağlayıcı, kullanıcıların İnternet ağına erişmelerini sağlayan, başka bir ifadeyle başkalarına ait içeriklere ulaşılmasına yalnızca aracılık eden İnternet öznesine verilen isimdir[51]. Erişim sağlayıcı, İSS'de olduğu gibi başkalarına ait bilgiler depolanmaz, bir kaç salisede bilgiler kullanıcıya ulaştırılır.

1.8. Türkiye'de İnternet

1.8.1. İnternet'in Türkiye'de gelişim süreci

Türkiye'de İnternet'in gelişim sürecini dört bölüme ayırarak inceleyebiliriz. Birinci dönemi, 1986-1993 yılları arasında İnternet öncesi akademik ağlar dönemi, ikinci dönemi, 1993-1995 yılları arasında akademik ağ olarak İnternet dönemi, üçüncü dönemi, 1996-2002 yılları arasında İnternet'te İSS'ler dönemi ve son olarak da 2002'den günümüze kadar olan dönemi ise İnternet krizi ve sonrası olarak ayırmamız mümkündür.

Birinci dönemde, yani 1986 yılında, üniversitelerin önderliğinde Türkiye'de İnternet öncesi ilk geniş alan bilgisayar ağı kurulmuştur. Türkiye Üniversiteler ve Araştırma Kurumları Ağı (TÜVAKA) ismi ile kurulan bu ağ, başlangıçta European Academic and Research Network'ün (EARN) Türkiye uzantısı durumundaydı.

[48] Güngör ve Evren. *İnternet Sektörü ve Türkiye İncelemeleri.* Telekomünikasyon Kurumu. 13 MAYIS 2002:8. 27 NİSAN 2005. http://www.tk.gov.tr/yayin/Raporlar/pdf/internetraporu.pdf
[49] Güngör ve Evren, 2002:8.
[50] Güran ve ark., 2000:13.
[51] Sınar, 2001:42

Kurulduğu günlerde, sadece üniversiteler ve araştırma kurumları tarafından kullanılan ve finanse edilen TÜVAKA, 1989 yılında tıkanmaya başlamış ve teknolojik gelişmeler karşısında yetersiz kalması nedeniyle bu ağın geliştirilmesi için, Orta Doğu Teknik Üniversitesi (ODTÜ) ve Türkiye Bilimsel ve Teknik Araştırma Kurumu (TÜBİTAK) tarafından yeni ağ teknolojilerinin kullanılması gerektiği öngörüsü ile ortak bir proje (TR-NET) başlatılmıştır[52].

EARN ağına ilk önce Aralık 1986 tarihinde Ege üniversitesi bağlanmış, daha sonra da 1987 yılı içinde sırası ile Anadolu, Yıldız, İstanbul Teknik, Boğaziçi, Fırat, Orta Doğu Teknik, Bilkent ve İstanbul üniversitelerinin bağlantıları gerçekleştirilmiştir.

İkinci dönemde ise, TR-NET (Türkiye İnternet Proje Grubu) adını alan TÜBİTAK destekli proje çalışmaları sonucunda, 12 Nisan 1993 tarihinde 64 Kbps hızındaki ODTÜ-Washington (NSF) hattı kullanıma açılarak, İnternet servisi başlatılmıştır. Aynı yıl, Ege Üniversitesi de, TÜVAKA kapsamında kullanılan 64 Kbps hızındaki uluslararası hat üzerinden Bonn bağlantılı İnternet hizmetini kullanıma açmıştır[53].

1993'de İnternet bağlantısının kullanıma açılması ile başlayan sürecin ilk aşamasının en önemli görünümü, İnternet ağında akademik kesimin egemenliğidir. Türkiye'de İnternet ağının, üniversitelerin ve TÜBİTAK'ın başlıca aktör olduğu bir biçimde kurulması, uluslararası gelişmelerle de uyum içindedir. Çünkü aynı dönemde İnternet alanındaki uluslararası gelişmelere baktığımızda, farklılıkların eğilim düzeyinde var olduğunu, ancak İnternet'in genel görünümünün bir akademik ağ olarak tanımlanabileceğini görmekteyiz[54].

TÜVAKA'dan başlatabileceğimiz, üniversitelerin, özellikle de ODTÜ'nün TÜBİTAK ile birlikte başlıca aktörler olarak kurdukları, şekillendirdikleri, sınırlı da olsa kurallarını belirledikleri İnternet'in kuruluş dönemi, 1995 yılının Kasım ayında

---

[52] Başaran, Funda ve Özdemir, Önder. *Türkiye'de İnternet'in Dünü, Bugünü*. Hacettepe Üniversitesi. 01 ARALIK 2003:2. 12 NİSAN 2005. http://www.hacettepekamu.org/forum_posts.asp?

[53] Akgül, Mustafa. *Türkiye İnterneti'nin ve İnternet Kurulunun Kısa Tarihi*. Türkiye Bilişim Derneği. 20 AĞUSTOS 2001:1. 22 AĞUSTOS 2004. http://dergi.tbd.org.tr/yazarlar/20082001/mustafa_akgul.htm

[54] Akgül, 2001:2.

TURNET omurgası ihalesinin sonuçlanması ile birlikte sona ermiştir. Türk Telekom tarafından Türkiye İnternet altyapı işleticiliği yapmak üzere planlanan TURNET omurgasının kuruluşu; yeni aktörlerin ortaya çıktığı, İnternet'in daha yaygınlaştığı, düzenleme tartışmalarına ve ana planlara konu olduğu, öte yandan özel sektörün büyük beklentilerle ciddi yatırımlar gerçekleştirdiği yeni bir dönemi başlatmıştır[55].

Özel sektörün aktif bir biçimde rol aldığı bu yeni dönemde ise, ticari İnternet kullanımına yönelik olarak kurulan ilk omurga olan TURNET'in hizmete girmesinin ardından oluşmaya başlayan Türkiye İnternet pazarı kısa süre içerisinde kurulan çok sayıda İSS ile beraber kişisel bağlantı isteklerinin artması ve TURNET çıkışlarının bu talepler karşısında yetersiz kalması sonucunda 1999 yılında yeni bir oluşum (TTNet) faaliyete sokulmuş ve yeni bir altyapı çalışmasına başlamıştır[56]. TTNet devreye girdiğinde kişisel bağlantı talepleri karşılanabilmiştir.

Dördüncü dönemde ise, yani 2000 yılının sonundan itibaren, Türkiye'de İnternet pazarı daralmaya başlamış, tüm İSS'ler tarafından, Türkiye'de telefon hatları ile İnternet'e bağlanan kullanıcı sayısında 2000 yılına göre, 2001 yılı Şubat ayında yaşanan finansal krizinde etkisiyle %30 oranında bir azalma olmuştur[57]. Bunun sonucunda büyük sermaye gruplarının İnternet şirketleri sadece grup faaliyetlerine yönelerek küçülmeyi tercih etmişlerdir. Kişisel erişim yatırımlarını durdurup, öncelikle gruba ait diğer şirketlerin veri trafiklerini taşıyarak ayakta kalmak, daha sonra ise kurumsal aboneye yönelerek krizden çıkmaya çalışmak bu firmaların başlıca hedefi olmuştur.

Türkiye'nin içinde olduğu ekonomik krizle birleşen bu süreç Türkiye'deki İSS'ler arasında hızlı bir yeniden yapılanmayı da beraberinde getirmiştir.

1.8.2. İnternet'i Türkiye'de yönlendiren kuruluşlar

Türkiye'de İnternet çalışmalarını yönlendirmek, İnternet'in altyapı çalışmalarının yapılmasında yol gösterici olmak ve İnternet'in kısa, orta, uzun vadeli hedeflerini belirlemek ve Ulaştırma Bakanlığı'na danışmanlık yapmak için kurulan İnternet Üst Kurulunu, Türkiye'de İnternet'i yönlendiren en önemli kuruluş olarak

[55] Başaran ve Özdemir, 2003:3.
[56] Sınar, 2001:113
[57] Başaran ve Özdemir, 2003:4.

gösterebiliriz. Bu sebeple aşağıda İnternet Üst Kurulu hakkında temel bilgiler verilmiştir[58].

Türkiye'de İnternet'in altyapıdan başlayarak tüm boyutları ile kısa, orta ve uzun vadeli hedeflerini belirlemek, bu hedeflere erişmek için gerekli stratejik ve taktik ulusal kararların alınması ve uygulanması sürecinde danışmanlık görevini yürütmek, uygulamada gözlenen aksaklıkları belirlemek ve giderilmesi için öneriler oluşturmak, konu ile ilgili birimler arasında eşgüdüm sağlamak, gelişme, yaygınlaştırma, hizmet üretimi konularında düzenleyici öneriler oluşturmak, ve uluslararası gelişmeleri yakından izleyerek ülke çıkarlarını korumak amaçları ile, Ulaştırma Bakanlığı tarafından "İnternet Kurulu" oluşturulmuştur.

Kurulun belli başlı görevleri şunlardır:

1. Kurul, İnternet'in Türkiye'de sağlıklı gelişmesi ve toplumsal yarar üretilmesi için temel öneriler oluşturmak amacıyla ulusal İnternet altyapısının kısa, orta ve uzun vadeli gelişme planları konusunda, ulusal İnternet altyapısı üzerinde sunulabilecek hizmetler ve sektörel yapılanmalar konusunda görüş oluşturarak, İnternet altyapısı ve diğer hizmetler konusunda ilgili kuruluşlarca uygulanmak üzere düzenleyici önerilerde bulunmak,
2. Türkiye'de ulusal İnternet'in sağlıklı gelişmesi amacıyla, ilgili tüm kuruluşların (üniversite, kamu, özel ve sivil toplum) İnternet'e ilişkin etkinliklerinin eşgüdüm içerisinde yürütülmesine katkıda bulunmak,
3. Türkiye'de İnternet gelişiminin nitel ve nicel olarak değerlendirilebilmesi amacıyla, ilgili kuruluşlardan veri toplamak ve yayınlamak. Türkiye'de İnternet kullanıcılarının görüş ve önerilerini toplamak ve değerlendirmek,
4. Türkiye'de İnternet üzerinden bilimsel yöntemlerle ölçümler yapmak ve sonuçlarını yayınlamak,
5. Türkiye'de İnternet'in sağlıklı gelişmesi amacıyla, gerektiğinde; Türkiye İnterneti'nin çeşitli katmanlarında yer alan ve hizmet veren kuruluşlara

[58] İnternet Kurulu hakkındaki bilgiler, kurulun resmi sitesi olan http://kurul.ubak.gov.tr adresinden derlenmiştir.

hizmete ilişkin önerilerde bulunmak, İnternet Teknolojileri üreticisi ve satıcısı kesimlere önerilerde bulunmak,

6. Kamuoyu görüşlerinin toplanarak değerlendirilmesi için mekanizmalar oluşturmak,
7. Dünyadaki gelişmeleri izlemek,
8. Uluslararası platformlarda ülke çıkarlarını korumak,
9. İnternet'e ilişkin uluslararası toplantı ve konferanslara ülke çıkarlarının korunması ve bilgi alışverişinin sağlanması için katılmak ve uluslararası platformlarda ülkemizin görüşlerinin doğru dile getirilebilmesi için gerekli çabayı göstererek öneriler oluşturmak,
10. İnternet ve ilgili teknolojilerin ulusal platformda gelişimini sağlamak ve önünü açmak amacıyla, bu konularda düzenleyici erke ve diğer ilgili kuruluşlara iletilmek üzere öneriler oluşturmak,
11. Eğitim etkinlikleri düzenlemek,
12. İnternet ve ilgili teknolojileri ile ilgili bilgi ve deneyim birikimine katkıda bulunmak üzere seminer, konferans vb. etkinlikler düzenlemek, düzenlenmesine katkıda bulunmak; teknolojilerin akılcı kullanımını sağlayacak eğitsel yöndeki çabalara destek olmak, Ulaştırma Bakanlığı'nın verdiği diğer görevleri yapmak,

İnternet Kurulu, yukarıda belirtilen görevleri tam anlamıyla yerine getirebilmesi durumunda, ülkemizde İnternet'in sağlıklı gelişmesine büyük bir katkı sağlayacaktır.

İnternet'i yönlendiren bir başka kurum ise Telekomünikasyon Üst Kurulu'dur. Bu kurum İnternet'le ilgili düzenlemeleri yapmaktadır. Ayrıca İnternet Servis Sağlayıcılar, Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği kapsamında genel izin almak suretiyle yetkilendirilmekteler. Söz konusu genel izin Telekomünikasyon Üst Kurulu tarafından verilmektedir.

2.SİBER SUÇLAR – SINIFLANDIRILMASI - SUÇLULAR - İŞLENİŞ ŞEKİLLERİ - ÖZELLİKLERİ - SORUMLULUK REJİMİ

2.1. Siber Suçlar

2.1.1.Genel olarak

Bilişim teknolojisinin son yıllardaki hızlı gelişimi göz önüne alındığında, önümüzdeki bin yıla damgasını vuracak teknolojilerden biri olacağı açıktır. Nitekim, bilgisayar ve iletişim teknolojilerindeki gelişmeler günümüzde insanlık tarihi açısından çok önemli bir gelişme olarak görülmekte, sanayi devrimi ile mukayese edilmektedir[59].

İnternet'in; gündelik iş yaşamından devlet kurumlarına, ekonomiden ticarete, bankalardan hastanelere, medyadan adliyelere, daha adını sayamayacağımız kadar geniş bir alana yayılmış olması ve bilginin bu sayede insanlara artık bir klavye tuşu kadar yakın olması, bu iletişim aracının kullanıcı sayısını her geçen gün daha da artırmaktadır. İnternet'in toplum yaşamında giderek daha fazla yer alması ve kullanım alanının günden güne genişlemesi, doğal olarak bazı hukuki sorunları da beraberinde getirmektedir.

Gerçekten, İnternet'i iyi amaçlarla kullanan kullanıcıların varlığına karşılık, teknolojinin yaramaz çocukları olarak adlandırılan, sabotaj veya kaos yaratmak amacıyla çeşitli sistemlerin açıklarını bularak bu sistemlere saldıran ve sisteme izinsiz girerek çeşitli hasarlar veren programcılar veya bilgisayar ile uğraşan bilgisayar korsanlarının ortaya çıkması, bilişim teknolojisinden faydalanmak isteyen "terör örgütleri"nin faaliyetlerini bu ortama taşıması, "hırsızlık" ve "dolandırıcılık" gibi suçların bu ortamda işlenmeye başlanması, İnternet'te izinsiz yayınlanan film, müzik ve oyunların oluşturduğu "lisans hakları ihlalleri" şeklindeki suçların genişlemesi, hakaret amaçlı sitelerin kurulması ve son olarak, bilgisayar orijinli resimler yoluyla yeni müstehcenlik biçimlerinin oluşturulması ile sübyancı olarak adlandırılan kimselerin sapkın düşüncelerini yaşama geçirmeleri sonucu "pornografi"

[59] Dokurer, Semih. *Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri*, Emniyet Genel Müdürlüğü. 10 ARALIK 2003. 24 MART 2004. www.egm.gov.tr/docs/inet-tr2001Metni.pdf

ve "çocuk pornografisi" gibi yasadışı yayınların giderek artması, İnternet'in kötü amaçla kullanılabileceğini açıkça gözler önüne sermiştir.

Bilgisayar ağları yoluyla yukarıda belirtilen suçların daha ucuz ve kolay biçimde işlenebilmesi nedeniyle, ileride bu suç tiplerinin yaygınlaşacağı ve çoğunlukla dijital ortamda işleneceği muhakkaktır.

2.1.2. Siber suç olgusu

Birinci bölümde İnternet'in tüm yönleriyle anlatılmaya çalışılmasının nedeni, suçun işlendiği ortamın nasıl bir ortam olduğunun gösterilmesi ve bunun asıl konu olan siber suçların nasıl işlendiğinin daha iyi anlaşılmasına yardımcı olacağının düşünülmesidir.

Siber suçun tanımını yapmadan önce, neden "İnternet suçu" değil de "siber suç" kavramının kullanıldığına da kısaca değinmek gerekmektedir. Siber uzay ve İnternet kavramları genellikle eş anlamlı olarak kullanılmalarına rağmen, gerçekte eş anlamlı değillerdir. Siber uzay kavramı, sadece İnternet'i değil, intranet[60] ve benzer diğer ağ (network) sistemlerini de kapsayan bir üst kavramdır. Yani intranet ortamında eğer bir suç işlenirse, söz konusu suç, siber uzayda işlenmiş bir siber suçtur fakat bu suç İnternet suçu değildir. Bu sebeple siber suç, İnternet suçunu da kapsayan bir kavramdır. Bir başka deyişle, her İnternet suçu bir siber suçtur ancak her siber suç İnternet suçunu oluşturmaz[61]. Fakat şu da bir gerçektir ki siber suçların büyük bir bölümü İnternet aracılığıyla işlenmektedir. Bunun sebebi de İnternet'in diğer siber suç araçlarından daha yaygın olması ve daha çok insan tarafından kullanılmasıdır.

2.1.3. Siber suçun tarihsel gelişimi

Siber suçların tarihsel gelişimini ve tanımını yapmadan önce, siber suçların işlendiği ortam olan ve siber uzay adı verilen kavramdan bahsetmek gerekmektedir.

---

[60] İntranet özellikle çok yönlü büyük şirketlerin, çalışanları ve departmanları arasında veri alışverişinin sağlanabilmesine yönelen özel bir iletişim ağıdır. Bu niteliği ile intranet, internet'in özel bir şirkete özgülenmiş şekli olarak tanımlanabilir. İntranet, Tüm web özelliklerini sağlamanın yanında, şirketlerin yapıları ile paralel olarak hangi kullanıcının nereye, ne oranda ve nasıl erişebileceğini de kontrol edebilen bir sistemi ifade etmektedir.

[61] Sınar, 2001:69

Siber uzay (Cyberspace) kavramı ilk defa bilim kurgu yazarı William Gibson tarafından "Neuromancer" isimli kitabında kullanılmıştır[62]. Gibson kitabında kısaca, küresel bilgi altyapısının yaygınlaşması sonucunda bilginin paradan daha önemli bir konuma gelmesiyle, hükümetlerin yerini almış büyük kuruluşlara, güvenli verilere ve bilgilere savaş açan bilgisayar kovboylarının mücadelesini anlatmaktadır[63]. Gibson, siber uzayı, "bilginin elektromanyetik formda oluşturulması ile başlayıp dünyanın dört bir yanını kuşatan çeşitli sistemler vasıtasıyla (örneğin ağ sistemleri, telefon hatları ve uydular gibi) bilgiye erişimin sağlandığı sanal ortamın bütünü" olarak tanımlamıştır[64].

Bilgisayar ve İnternet kullanıcıları, İnternet üzerinden iletişimlerini sağlamak, bilgi alış verişinde bulunmak, alış veriş yapmak, sinema filmleri seyretmek... vs. için oluşturdukları ortama Gibson'nın kitabından da ilham alarak, siber uzay adını vermişlerdir.

Bilgisayar ve İnternet alanında işlenen suçların tarihi 1960'lara kadar gitmektedir. Bu yıllarda bazı gazete ve bilimsel dergilerde yayımlanan makale ve inceleme yazılarında "bilgisayar suçu" (computer crime) veya "bilgisayarla ilgili suç" (computer-related crime) terimlerinin telaffuz edilmeye başlanması ile birlikte Penoloji[65] ve Kriminoloji[66] bilimlerinin ilgileneceği yeni bir kavram daha ortaya çıkmıştır[67].

İnternet'in anavatanı olan ABD, İnternet ve bilgisayar dünyasındaki tüm olumlu gelişmelerin öncülüğünü yapmasının yanında, İnternet'in bir suç vasıtası olarak kullanılmasında ve bu suçlara ilişkin düzenlemelerin yapılmasında da öncülüğü kimseye bırakmamıştır.

---

[62]Beceni, 2004:3.
[63] Çeken, 2003:4.
[64] Beceni, 2004:3; Gibson, 1984:8.
[65] Penoloji: Cezaların ve emniyet tedbirlerinin içeriklerini, gelişmesini ve ne derece etkili olduklarını inceleyen bir bilim dalıdır.
[66] Kriminoloji: Suç denilen insan eylemlerini, suçun varlığını kanıtlayacak deliller bulunmasını, suçun sebep ve faktörlerini ve suça karşı korunmayı içeren birçok disiplini kapsayan bir bilim dalıdır.
[67]Sieber, Ulrich. *Legal Aspects of Computer-Related Crime in the Information Society COMCRIME-Study*. Eurpean Commission Information Society. 1 OCAK 1998:19. 17 AĞUSTOS 2004. http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html

Bilgisayarlar ve İnternet konusunda 1970'li yılların ortalarına kadar karşılaşılan ve suç teşkil eden eylemler, bugün için nispeten basit sayılabilecek düzeyde, bilgisayarların çeşitli şekillerde sabote edilmesi, bilgisayar sisteminin yasa dışı olarak kullanılması ve bilgisayar casusluğu şeklinde ortaya çıkmaktayken, zaman ilerledikçe, bilgisayar ve İnternet teknolojisinin de gelişmesiyle -ki bu teknoloji çok hızlı bir şekilde gelişmektedir- beraber, İnternet kullanımının da yaygınlaşması sonucunda bilgisayar ve İnternet vasıtasıyla işlenen suçların sayıları artmış ve daha karmaşık hale gelmeye başlamıştır[68].

Bilgisayarlar yoluyla işlenen suçlar üzerine yapılan ilk çalışmalar, 1970'li yıllarda başlamıştır. Gerçekten, bu yıllarda ortaya çıkan Amerikan Eşitlik Fonu (Am. Equity Fund), Alman Herstatt ve İsviçre Volvo davaları bu çalışmaları tetikleyen ilk davalardır. Söz konusu çalışmalar sınırlı sayıda siber suçu açığa çıkarmıştır. Fakat adli mercilere bildirilmeyen veya soruşturulmayan yüksek miktarda bilgisayar suçu olduğuda tahmin edilmektedir[69].

1980'li yıllardan sonra, iş hayatında ve günlük hayatta bilgisayar ve İnternet kullanımının yaygınlaşması ile birlikte, nitelik ve nicelik olarak değişikliğe uğrayan suç olgusu, bu sahanın da birtakım hukuki düzenlemelerle disipline edilmesi ihtiyacını ortaya çıkarmıştır. 1980'li yıllardan sonra, bilgisayar ve İnternet yoluyla işlenen suçların sadece ekonomik boyutlarının olmadığı ve bu tür suçların en az ekonomi kadar önemli, diğer bazı değerler aleyhine de işlenebileceği anlaşılmıştır. Bunun sonucu olarak da siber suç olgusu ortaya atılmış ve bu suçların ayrı bir disiplin altında incelenmesi gereği ortaya çıkmıştır[70].

2.1.4. Siber suçun tanımı

Bilişim teknolojilerinin gelişmesiyle birlikte, bu teknolojiye ait kavramlar da değişmektedir[71]. Bilişim ortamında işlenen suçları belirtmek için "bilgisayar suçları" (computer crimes), "bilgisayarla ilgili suç" (computer-related crime), "bilgisayar ihlalleri" (computer abuse), "yüksek teknoloji suçları" (high-tech crimes), "İnternet

[68] Sieber, 1998:19.
[69] Sieber, 1998:19.
[70] Çeken, 2002:2.
[71] Koca, 2003:787.

suçları" (internet crimes) gibi kavramlar kullanılmaktadır. Bu kavramlardaki çeşitlilik ve bu kavramların çoğunda geçen bilgisayar terimi, İnternet'in günümüzdeki gibi etkin olarak kullanılmadığı dönemlerde suçluluğun bilgisayar ve ona bağlı sistemler yolu ile ortaya çıkmasından kaynaklanmaktadır[72].

İlk zamanlarda bilgisayar suçu nedir? Neler bilgisayar suçudur? Bu suç ne şekilde müeyyide altına alınır? Nasıl yargılanır? Bunlarla mücadele ne şekilde yapılmalıdır? gibi sorulara cevap aranırken, bilişim teknolojilerinin büyük bir hızla ilerlemesiyle beraber, bilgisayar aracılığıyla işlenen suçlar yeni gelişmelere ayak uydurmuş ve gelişen teknoloji ve sağladığı olanaklar sayesinde oluşan yeni yarar sahalarına eş olarak, yeni ihlal tipleri ortaya çıkmıştır[73]. İşte hem bu yeni ihlal tiplerinin ortaya çıkması hem de bilgisayar ağlarının özellikle de bu ağlardan İnternet'in etkinliğini arttırarak bilişim dünyasında bilgisayarın yanında yer alması sonucunda bütün ihlalleri tek bir kavram altında toplama ihtiyacı duyulmuştur.

Bu ihtiyaca binaen uluslararası hukukta "cyber crime" denilen, ülkemizde ilk olarak "sanal suç"[74] olarak adlandırılan "siber suç" terimi, daha sonra uluslararası kullanıma paralel olarak bilişim teknolojileriyle işlenen suçlar için kullanılmaya başlanmıştır.

Türk yazınında hala bu suçlar için genel bir kavram kullanmak hususunda görüş birliği yoktur. Erem[75], Yazıcıoğlu[76] *Bilgisayar Suçları*; İçel[77] ve Yenisey[78]

---

[72]Beceni, Yasin. *Siber Suçlar*. 29 NİSAN 2004. s.17.
http://www.hukukcu.com/bilimsel/kitaplar/yasinbeceni/indeks.htm .

[73] Yazıcıoğlu, 2002:452.

[74] Yazıcıoğlu, (2002:452)'e göre, doğru tercihin "bilgisayar suçu" mu veya "yüksek teknoloji suçları" mı ya da "bilişim suçu" mu olduğu konusundaki isim sorunu, bilgisayar ağları ile ilgili suçlara "sanal suç", "internet suçu" veya "siber suç" kavramlarından hangisinin tercih edilmesi gerektiğinde de çıkmaktadır. Şöyle ki, sanal kelimesinin sözlük anlamı "gerçekte yeri olmayıp zihinde tasarlanan, mevhum, farazi, tahmini" anlamında iken bilgisayar ağları, bu ağlar arasındaki bağlantılar, iletişim ve yine bu ortamda gerçekleştirilen suçlar farazi değil gerçektir; diğer taraftan "internet suçu" deyimi de bilgisayar ağları ile ilgili suçları tam olarak karşılamamaktadır. Çünkü siber uzay terimi internet sözcüğünden daha geniş bir anlamı vardır. Bu nedenle "internet suçu" terimi, nispeten daha dar anlamı nedeniyle problemi tam olarak tanımlayamaz. Yine internet bilgisayar ağlarından bir tanesidir ve bugün için en yaygın olarak kullanılanıdır. Çok hızlı gelişen ve değişen siber uzayda ismi "internet suçu" olarak belirlemek başka bir bilgisayar ağında işlenen veya yarın daha yaygın olarak kullanılmaya başlanabilecek başka bir ağda şuçları ifade edebilmek veya karşılayabilmek bakımından çeşitli sorunlar doğurabilecektir. Bu nedenledir ki dünyada bilgisayar ağlarında işlenen suçlara (crimes related to computer networks) siber suçlar (cyber crime) kavramı kullanılmaktadır.

[75] Erem, 1993:727vd.

[76] Yazıcıoğlu, 1997:53 vd.

[77] İçel, 2000:414.

İnternet'te İşlenen Suçlar; Önder[79] *Bilişim Alanında Suçlar;* Koca[80], Sınar[81] ve Çeken[82] *Siber Suçlar*; Ünver[83] *İnternet Alanında Suçlar;* Bayraktar[84], Ersoy[85], Yenidünya/Değirmenci[86], Dülger[87] ve Karagülmez[88] *Bilişim Suçları* kavramlarını kullanmaktadırlar.

Yukarıdan da anlaşılacağı gibi Türk yazınında ortak bir kullanımın söz konusu olmaması nedeniyle çalışmamızda anılan suçlar için uluslararası hukukta yaygın olarak kullanılan ve bu konuda Dünya'daki tek düzenleme olan Avrupa Konseyi Siber Suç Sözleşmesi'nin de adına uygun olarak "siber suç" kavramını kullanmanın uygun olacağı düşüncesiyle siber suçlar kavramı kullanılmıştır.

Bilgisayar ağları ile ilgili suçların, yani siber suçların tanımını yapmadan önce kısaca bilgisayar suçu kavramından da bahsetmek gerekmektedir.

Bilgisayar suçunun herkesin üzerinde fikir birliği sağladığı ortak bir tanımı yapılamamıştır[89]. Hatta uluslararası örgütler bile hazırlamış oldukları raporlarda resmi bir tanım yapmaktan kaçınarak eylemlere göre bir sınıflandırma yapmışlardır. Avrupa Topluluğu uzmanlar komisyonu bilgisayar suçlarını "bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde kanuna, ahlaka aykırı olarak veya yetki dışı gerçekleştirilen her türlü davranış" olarak tanımlarken (Mayıs 1983 Paris); Birleşmiş Milletler de 2000 yılında Brüksel'deki 10'uncu kongresinde bilgisayar suçlarını, "bilgisayarların güvenliğine ve işlevlerine zarar verme amaçlı herhangi bir fiil" olarak tanımlamıştır.

Bilişim teknolojisinin hızla gelişmesi ve bilgisayarın insan hayatının her alanına girmesiyle birlikte homojen bir bilgisayar suçundan bahsetmenin mümkün

---

[78] Yenisey, 2001: 447.
[79] Önder, 1994:504.
[80] Koca, 2003:787.
[81] Sınar, 2001:69.
[82]Çeken, 2002:2.
[83] Ünver, 2001:59.
[84] Bayraktar, 2000:202.
[85] Ersoy, 1994:166.
[86] Yenidünya ve Değirmenci, 2003:27.
[87] Dülger, 2004:63vd.
[88] Karagülmez, 2005:37.
[89] "Bilgisayar Suçu" kavramının farklı tanımları için bkz. Yazıcıoğlu, 1997:136 vd.

olmaması nedeniyle, bilgisayar suçu kavramının kullanılmasından vazgeçilmiş ve siber suç kavramı kullanılmaya başlanmıştır[90].

Siber suç, en geç ve belkide en karmaşık problem olarak siber dünyada yerini almıştır. Bu sebeple siber suçun tanımını yapmak oldukça güçtür. En basit şekliyle siber suç, siber uzayda işlenen suç olarak tanımlanabilir. Fakat bu tanımlama, siber suçların tasnifine ilişkin olup, siber suçun niteliğini ortaya koymamaktadır. Siber suç terimi, esasen bir bilgisayar sistemi veya ağı aracılığıyla bir bilgisayar sistemi veya ağında veya bir bilgisayar sistemi veya ağına karşı gerçekleştirilen eylemler anlamına gelmektedir. Bu yönü dikkate alındığında siber suç ile bilgisayar suçu arasında bir fark görülmemektedir. Avrupa Birliği'nin bir bildirisinde de bilgisayar suçunun geniş anlamda tanımlandığı ve aynı anlama gelen yüksek teknoloji suçu ve siber suçun da kullanıldığı belirtilmiştir[91].

Yine Birleşmiş Milletler 10 uncu Kongresinde siber suçlar, bilgisayar ağlarında veya ağlarına karşı gerçekleştiren her türlü fiil olarak tanımlanmakta ve dar anlamda ve geniş anlamda siber suçlar olarak ikiye ayrılarak incelenmektedir. Dar anlamda siber suçları, bilgisayar sisteminin güvenliğini veya veri işlemini hedef alan eylemler olarak tanımlanırken; geniş anlamda ise bilgisayar sistemi ve ağı aracılığıyla veya bu sistem veya ağda gerçekleşen herhangi kanun dışı eylem olarak tanımlanmaktadır[92].

Yukarıda yapılan açıklamaların ışığında siber suçun tanımını yapmak gerekirse; siber suç, bilgisayar veya bilgisayar ağlarının siber uzayda yapılan kanunsuz bir davranışın aracı veya amacı ya da her ikisi olarak kullanılmasıdır. Diğer bir ifade ile herhangi bir suçun elektronik ortam içersinde işlenebilme imkanı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçlara siber suçlar denir[93].

[90] Koca, 2003:788.
[91] Koca, 2003:789.
[92] Yazıcıoğlu, 2002:460.
[93] Beceni, s.18.

2.1.5. Siber suçların özellikleri

Bilgisayar ağlarının tüm dünyayı sarmasıyla beraber, İnternet kullanımı yaygınlaşmış ve siber uzay olarak adlandırılan sanal dünyada bir takım hukuka aykırı eylemlerin gerçekleştirilmesinde bir vasıta olarak kullanılmaya başlanmıştır. Bu sebeple, siber uzayda işlenen siber suçların, hukuk düzeni tarafından tanımlanması ve ceza hukukunda mevcut olan kurallar karşısındaki konumlarının belirlenmesi gerekliliği ortaya çıkmıştır. Bu gereklilik sonucunda öncelikli olarak incelenmesi gereken konu, siber suç ile klasik anlamdaki suç kavramı arasındaki ilişkidir. Siber suçlar klasik anlamdaki suçların siber uzayın bir vasıta olarak kullanılmasıyla işlenen suçlar mıdır? Yoksa siber suç klasik anlamdaki suç kavramından ayrı bağımsız bir suç kategorisi midir? Siber suç, klasik suç ayrımı bu görüşler çerçevesinde incelenecektir.

2.1.5.1. Siber suçların klasik suçların bir görünümü olduğunu savunan görüş

Bu görüşün savunucuları, siber uzayda gerçekleştirilen suçlar ile gerçek dünyada işlenen suçlar arasında suçun temel unsurları bakımından bir fark olmadığı esasından yola çıkmakta ve her iki suç arasında tek farkın "fiziksel gerçeklik" noktasında ortaya çıktığı görüşünü ileri sürmektedirler.

Onlara göre, gerçek dünyada işlenen suçlar fiziksel bir gerçekliğe sahiptir. Siber suçların işlendiği siber uzay ortamı ise, gerçek dünyanın yanında ancak ondan ayrı bir varlık olarak yer almaktadır. Ancak fiziksel bir gerçeklikten yoksun olması, gerçek dünyada uygulanan ceza hukuku ilke ve normlarının siber suçlar hakkında uygulanamayacağı anlamına gelmez. Siber suçlar ile klasik suçlar arasında temel unsurlar bakımından bir fark bulunmamakta, siber suçlarda, klasik suçlardan farklı olarak siber uzay ortamı suçun gerçekleştirilmesinde bir araç olarak kullanılmaktadır. Örneğin telefon, radyo ve televizyonun bulunuşu, sahtekarlık cürümlerini işlemekte olan kişilerin bu aletleri kullanarak çok daha yeni şekillerde bu suçu işlemeleri için kendilerine eşsiz olanaklar tanımıştır. Ancak bu durum, sahtekarlık suçunun

yüzyıllardır kanundışı sayılmasını ve bu suçların yüzyıllardır işlenmekte olduğu gerçeğini değiştirmemektedir[94].

Siber suçların klasik suçların bir görünümü olduğunu savunanlar, eğer siber uzay ortamı sadece geleneksel suçların işlendiği bir ortam ise, siber suçları tanımlamak için ayrı bir kategori yaratmaya, özel hukuki düzenleme yoluna gitmeye gerek bulunmadığını savunmakta ve mevcut hukuk kurallarının bu konuda yeterli olduğunu ileri sürmektedir[95]. İddialarını güçlendirmek için gerçek dünyada işlenen bazı geleneksel suçlar ile bu suçlara temel unsurlar yönünden benzeyen siber suçları karşılaştırarak incelemektedirler.

Söz konusu görüşü savunanlar bu karşılaştırmalarının birinde hırsızlık suçunu ele alıp, bu suç ile siber uzay ortamında gerçekleştirilen siber hırsızlık suçunu karşılaştırarak her iki grup arasında bir farklılığın olup olmadığını belirlemeye çalışmıştır.

Söz konusu karşılaştırmada siber hırsızlık terimi, bir bütün olarak, siber uzay ortamının kullanılması yoluyla gerçekleştirilen bilgi hırsızlığı, -bilgisayar yazılımlarını da kapsar biçimde- para veya mal hırsızlığı ile hizmet hırsızlığı fiillerini de içine alan bir manada kullanılmaktadır[96].

Gerçek dünyada hırsızlık basitçe, başkasına ait taşınabilir bir malın sahibinin rızası olmaksızın faydalanmak kastı ile bulunduğu yerden alınması şeklinde tanımlanabilir. Mal terimi sadece para, mücevher, giysi gibi maddi şeyleri değil elektrik, dijital veriler gibi fiziksel varlığı olmayan şeyleri de kapsar. Klasik anlamda hırsızlık suçunun gerçekleşebilmesi için Anglo Amerikan hukuk geleneğine göre dört unsurun gerçekleşmesi gereklidir[97]. Buna göre maddi unsur; bir başkasının mal varlığında bulunan bir malı alarak fiili hakimiyet alanına dahil edilmesidir. Manevi unsur; failin bu eylemi kasten gerçekleştirmesidir. Hukuka aykırılık unsuru; failin suç konusu malı almak veya fiili hakimiyet alanına dahil etmek konusunda hukuken

[94] Brenner, W. Susan. *Is There Such a Thing as "Virtual Crime"?*. Computer Crime Research Center. 1999:1. 13 EYLÜL 2004. http://www.crime-research.org/library/Susan.htm
[95] Brenner, 1999:1.
[96] Brenner. 1999: 2; Sınar, 2001:71,
[97] Sınar, 2001:72:La Fave and Scott'dan, 1972:7 vd.

korunan bir yararının olmamasıdır. Zarar unsuru ise; mağdurun mal varlığında bulunan maldan yoksun kalmasıdır.

Klasik anlamda hırsızlık suçunun oluşabilmesi için gerekli olan bu unsurlar siber hırsızlık suçunun gerçekleşmesi ve ceza sorumluluğunu doğurabilmesi açısından da uygulanabilir niteliktedir. Buna örnek olarak siber uzayın bir para veya mal hırsızlığı amacıyla kullanılması verilebilir. Bir siber suç failinin, siber uzay ortamını kullanarak kendi bilgisayarından bir finans kuruluşunun sistemine girdiğini ve bu finans kuruluşunun fonlarında bulunan paraları kendisine ait hesaplara geçirdiğini düşünürsek, siber suçun faili başkasına ait olduğunu bildiği parayı hukuka aykırı olarak kendi fiili hakimiyet alanına geçirmekte ve o paraya hukuken sahip olan kişileri zarara uğratmaktadır. Siber hırsızlık ile gerçek dünyadaki hırsızlık arasındaki tek fark, burada failin gerçek dünyada fiziksel güç harcayarak gerçekleştirebildiği bir eylemi bilgisayar ve siber uzay ortamını kullanarak gerçekleştirmesidir. Suçun failleri, hırsızlık suçunu gerçekleştirmek için farklı metotlar kullanmakta fakat bu metotlar suçun yapısal unsurları üzerinde bir değişiklik meydana getirmemektedir.

Başkasının arazisine tecavüz, ev içinde hırsızlık, sahtekarlık, dolandırıcılık, pornografi ve müstehcenlik, tehdit, hırsızlık, zimmet, başkasının malına zarar verme, teşebbüs, yasa dışı para toplama, komplo, ihkak-ı hak ve terörizim gibi suçlar hem sanal dünyada hem de gerçek dünyada işlenmesi mümkün olan suçlardır. Bu suçların değişik işlenme şekillerinde dahi bilinen suçlara ait ceza sorumluluğu prensipleri uygulanabilmektedir. Bunları bu özelliklerinden dolayı kısaca siber suç benzerleri olarak isimlendirebiliriz[98].

Sonuç olarak bu görüşü savunanlar, siber suçun işlenebilmesi için siber uzay ortamının kullanılmasının gerekli olduğunu fakat bu gerekliliğin suç oluşturan eylemi yeni ve bağımsız bir suçluluk biçimine dönüştürmediğini ifade etmektedirler. Ceza hukukunun mevcut normları, siber uzay ortamında gerçekleştirilen yeni suç biçimine de uygulanabilmektedir. O halde yukarıda örnekte verilen siber hırsızlığın ve benzeri İnternet suçlarının yeni ve bağımsız bir kategori olarak nitelendirilmesi mümkün değildir. Bu suçlar için özel bir hukuki düzenleme rejimi geliştirilmesine de gereksinim bulunmamaktadır.

[98] Çeken, 2002:4.

Bu görüşü esas alan devletler, siber suçlar bakımından gerek suç siyasetleri, gerek ceza kanunlarının oluşumunda esas teşkil eden suçla korunan hukuki yarar kıstasını muhafaza etme olgusu, gerek kanunlarında suç enflasyonuna yol açmamak ve gerekse yukarıda da belirtildiği gibi mevcut suçların zaten bilgisayar veya bilgisayar ağları marifetiyle işlenen suçları yaptırım altına almaya yettiği düşüncesiyle kanunlarını, mevcut suçların kapsamlarını bilgisayar veya bilgisayar ağı yoluyla işlenen fiilleri kapsayacak şekilde yeniden düzenlemekte ve bazı tanım ve kavramlara bilgisayar ve bilgisayar ağları kavramını da eklemektedir[99].

Bu usul, Almanların öncülük ettiği bir sistemdir ve Avusturya, Danimarka, Kanada, İsveç, İtalyan, Yunanistan, Japonya, İsviçre, Hollanda, Norveç ve İzlanda Ceza Kanunlarında bu usulü kullanmaktadır[100].

2.1.5.2. Sadece siber dünyada işlenebilecek suçların ayrı bir kategori olduğunu savunan görüş

Siber suçların klasik suçlardan bağımsız ve farklı bir kategoriyi oluşturduğunu savunan görüşe göre, yukarıda incelenen siber hırsızlık örneğinden de anlaşılacağı gibi bazı klasik suç tipleri siber uzay ortamının bir araç olarak kullanılması suretiyle işlenmekte olduğu ve bu gibi durumlarda siber uzayda işlenen suçların mevcut ceza hukuku genel ilkeleri ve normları ile çözüme kavuşturulmasında bir sakınca olmadığını söyleseler de, gerçek dünyada gerçekleştirilen suçlarla benzerlik gösteren bazı siber suçlar dışında, sadece siber uzay ortamında işlenebilen bir takım siber suçların var olduğunu, bu suçların ise gerçek dünyada işlenen suçlar ile bir benzerliği olmadığını ve mevcut ceza hukuku normları ile çözüme kavuşturulamadıklarını, bu nedenden ötürü bu suçların cezasız kalmaması için ayrı bir hukuki rejimin gerekliliğinin ortaya çıktığını ileri sürmektedirler[101].

[99] Yazıcıoğlu, 1997:172 vd.
[100] Yazıcıoğlu, 1997:173.
[101] Brenner, 1999:15

Siber uzaya özgü olan yani sadece siber uzayda işlenebilecek olan siber suçlar kategorisinin varlığını savunanlar, bu görüşlerini LambdaMOO isimli sanal bir ortamda yaşanan olayla örneklendirmektedir[102].

LambdaMOO, katılımcıların bir sohbet odasında olduğu gibi yazı aracılığıyla ve bir takma isim kullanarak iletişim kurdukları sanal bir topluluktur[103]. Diğer sohbet odalarından farklı olarak LambdaMOO'da katılımcılar kimlik bilgileri ile topluluğa üye olmakta ve sürekli olarak kullanılan bir sanal kimliğe sahip olmaktadırlar[104]. Mr. Bungle takma ismini kullanan bir LambdaMOO katılımcısı, voodoo doll ismi verilen ve kendisine istediği herhangi bir katılımcının yerine geçerek onun ağzından konuşabilme imkanı veren bir bilgisayar programını kullanarak, LambdaMOO'da bulunan bazı bayan katılımcıların yerlerine geçerek ve onların ağzından son derece aşağılayıcı ifadeler kullanarak, Mr. Bungle'nin kendilerine nasıl tecavüz ettiğini anlatıyormuş gibi bir izlenim yaratmıştır. Bu LambdaMOO üyesi bayan katılımcılar sanal ırza geçme suçunun mağdurları haline gelmişlerdir. Mr. Bungle'nin kendi karakterlerini aşağılayıcı bir şekilde kullanması ve kendilerinin O'nu durdurmak konusunda hiçbir şey yapamamış olmaları, bu eylemin mağdurlarında gerçek dünyada ırza geçme eyleminin mağdurlarında olduğu gibi bir travma hali yaratmıştır. Bu nedenle, LambdaMOO adlı sohbet odasında yaşananların "sanal ırza geçme" olarak nitelendirilmiştir[105].

Siber suçların bağımsız, klasik suçlardan farklı bir kategori olduğu görüşünü benimseyenler, LambdaMOO örneğini vererek bu sanal ırza geçme eylemini gerçek dünyada işlenen suçlarla yapısal unsurlar bakımından benzerlik göstermeyen saf siber suçlara örnek olarak göstermektedirler[106].

---

[102] Sınar, 2001:75.
[103] Dibel, Julian. Personel web site. *My Dinner With Catharine MacKinnon And Other Hazards of Theorizing Virtual Rape*. 26 NİSAN 1996:1. 14 MAYIS 2004. www.juliandibbell.com/texts/mydinner.html
[104] Dibel, 1996:2.
[105] Dibel, Julian. Personel web site. *A Rape in Cyberspace (Or TINYSOCIETY, and How to Make One)* 01 ARALIK 1998:4. 14 MAYIS 2004. http://www.juliandibbell.com/texts/bungle.html; "Virtual Rape". *Journal of Computer-Mediated Communication*. 04 MART 1997. 14 MAYIS 2004. http://jcmc.indiana.edu/vol2/issue4/mackinnon.html#abstract
[106] Brenner, 1999:17; Sınar, sf.75.

Sanal ırza geçme olarak isimlendirilen eylemi klasik manadaki ırza geçme suçuyla karşılaştırırsak, sanal ırza geçme suçunun gerçek dünyadaki ırza geçme suçundan, suçun oluşabilmesi için aranan unsurlar bakımından kesin olarak ayrıldığını görürüz. Gerçek dünyadaki ırza geçme suçunun meydana gelebilmesi için kanun koyucunun aramış olduğu en önemli unsur, mağdura fiziksel bir saldırının yapılmasıdır.

Siber suçların bağımsız, klasik suçlardan farklı bir kategori olduğu görüşünü benimseyenler, siber uzayda fiziksel bir saldırı yapılamayacağından, ırza geçme suçu sadece gerçek dünyada gerçekleşebileceğini Mr. Bungle'nin eylemi ise mağdurun fiziksel varlığına değil ruhsal varlığına yönelmekte olduğunu, böyle bir eylemin ancak siber ortamda gerçekleşebileceğini ileri sürerek, bu nedenle sanal ırza geçme eylemini, ırza geçme suçunu geniş yorumlayarak ve hatta suçun tanımında değişikliğe giderek cezalandırmasının mümkün olamayacağını belirtmektedirler[107].

Anılan görüşünü benimseyenler, siber uzay ortamını ihlal eden her eylemin, mevcut hukuk düzeninde yapılmış olan suç tanımlarının yeniden yorumlanması ve klasik ceza sorumluluğu ilkelerinin uygulanmasıyla bir sonuca ulaşılacağını beklemenin doğru olmayacağı söylemektedirler. Onlara göre, siber uzay ortamının gün geçtikçe biraz daha büyüdüğü ve hemen hemen gerçek dünyada yapılan her faaliyetin siber uzayda da yapılmaya başlandığı göz önüne alınarak, yeni ihlal tiplerinin ortaya çıkabileceği ve bu ihlallerin klasik suçlardan giderek ayrılacağı muhakkaktır. Bu nedenle siber suçların tanımlanması ve bunlara ilişkin ceza sorumluluğu kurallarının belirlenmesi için yeni yaklaşımlar geliştirilmelidir[108].

Siber suçların klasik suçlardan bağımsız ve farklı bir kategoriyi oluşturduğunu savunan görüş; sonuç olarak yapılması gerekenin siber suçları bağımsız bir alan olarak kabul ederek, bu alanda işlenen suçlar için yeni sorumluluk rejimi kuralları getirerek, burada işlenen suçların cezasız kalmamasının sağlanmasının gerekliliğini ileri sürmektedirler[109].

[107] Brenner; 1999.17
[108] Brenner; 1999:18; Sınar, 2001:75.
[109] Brenner; 1999:18.

2.1.5.3. Konuya ilişkin görüşümüz

Burada öncelikli olarak tartışılması gereken konu, siber uzay ortamında işlenen suçların cezalandırılmasında, mevcut ceza hukuku normlarının yeterli olup olmadığıdır. Eğer siber uzayda işlenen suçlar, gerçek dünyada işlenen suçlar bakımından suçun oluşabilmesine ilişkin unsurları taşıyorsa, yani mevcut ceza normlarıyla cezalandırılabiliyorsa, burada mevcut ceza normunun uygulanmasıyla sorun çözüme kavuşturulacaktır.

Siber uzay ortamında işlenen suç, unsurları bakımından klasik suç tiplerinden ayrışıyorsa, burada ceza hukuku ilkeleri göz önüne alınarak yeni suç tiplerinin tanımlanması gerekecektir.

Günümüzde ortaya çıkan siber suçlar incelendiğinde, bu suçların klasik manadaki suçlarla benzer olduğu görülmektedir. Bu sebeple bu suçlar mevcut ceza hukuku normlarıyla cezalandırılabilmektedir. Yani bugün siber suçların cezalandırılabilmesi konusunda bir problem yaşanmamaktadır. Yalnız, ileride siber uzayda yapılan ihlaller karşısında mevcut ceza hukuku normlarının yeterli olmaması durumunda, kanun koyucunun bu konuda yeni düzenlemeler yapması gerekecektir.

Siber dünyada işlenebilecek suçların ayrı bir kategori olduğunu savunan görüşün, görüşünü desteklemek için vermiş olduğu LambdaMOO örneği, bir siber uzay ihlali olmasına rağmen bu eylem suç yoğunluğu taşımamaktadır. Belki siber uzayda sövme ve hakaret suçu olduğu konusu tartışılabilir. Ama ırza geçme suçunun gerçekleşmediği de aşikardır. Bu ve buna benzer eylemlerin "netiquette" olarak adlandırılan, internet kullanım ahlakına aykırılık olarak değerlendirilmeleri daha doğru olacaktır[110].

2.2. Siber Suçların Sınıflandırılması

Siber suçların hayatımızda yeni yeni yer almaya başlaması ve bizleri rahatsız etmesiyle beraber, siber suçları çeşitli yönleriyle düzenleme ve sınıflandırma gereği ortaya çıkmıştır. Ceza Hukukunun temel ilkelerinden biri olan "kanunsuz suç ve ceza

[110] Sınar, 2001:78

olmaz" ilkesi uyarınca, kanun koyucularının bu suçlar için düzenlemeler yapması gerektiği ifade edilmiştir.

Ancak bu konuda bilgisayar ağları alanındaki sorunların ve özellikle İnternet'in tam olarak değerlendirilememesi, İnternet'in sürekli gelişmesi ve her geçen gün biraz daha fazla insan hayatına girmesi, bunun sonucunda yeni ihlal tiplerinin ortaya çıkması cezalandırılması düşünülecek fiillerin hangileri olduğunu saptamaya imkan vermemektedir. Bu nedenle siber suçları sınıflandırma çalışmaları farklılık arz etmektedir.

Siber suçların tarifini yaparken de gördüğümüz gibi herkesin uzlaşmış olduğu bir tanım bulunmamaktadır. Konu ile ilgilenen kimi uzmanlar bu kapsama girmesi muhtemel fiilleri saymakla yetinmekte ve gruplara ayırarak tasnife gerek görmemekte, bazı uzmanlar ise, bu suçları iki, üç ya da dört ana başlık altında incelemektedir.

Öncelikle doktrinde genel kabul gören McConnel International adlı Amerikan global politika ve teknoloji yönetimi danışmanlık firması tarafından yapılan sınıflandırmaya bakmak gerekir[111]. Bu sınıflandırmaya göre siber suçlar dört başlık altında incelenmiştir.

2.2.1. McConnel International'ın Yapmış Olduğu Sınıflandırma

2.2.1.1. Veri Suçları

Verilere karşı işlenebilecek suçlar üç alt başlık halinde düzenlenmiştir.

2.2.1.1.1. Verilere Müdahale Edilmesi

Siber uzayda veri transferine müdahale edilmesine ilişkin suçtur. Bu suçun gerçekleşmesi için, verilerin transferi sırasında üçüncü kişilerin bu transfere müdahale ederek veri naklini engellemesi, naklin rotasını değiştirmesi ve üçüncü kişilerin verileri ele geçirmesi gerekmektedir.

[111] Bu sınıflandırma için bkz. McConnell-International, Cyber Crime... and Punishment? www.mcconnellinternational.com (22.04.2005); Uçkan ve Beceni 2004:389; Değirmenci, 2002:123

2.2.1.1.2. Verilerin Değiştirilmesi

Bu suçun oluşabilmesi için verilerin saklı tutulduğu bir ortamda veya iletildiği sırada değiştirilmesi, kısmen veya tamamen tahrip edilmesi gerekmektedir. Buradan çıkan bir sonuçda aktarım sırasında verilerin değiştirilebilir, tahrip edilebilir veya silinebilir olmasıdır. Bu durum iki ayrı suçun işlenmesi durumunu ortaya çıkarır ve bu halde iki suç birleştirilerek tek bir ceza verilir.

2.2.1.1.3. Veri Hırsızlığı

Çalınan verilerin, veri sahibinin veya üçüncü bir kişinin aleyhine olacak şekilde kullanılması veya çalınan veriler sayesinde çalan veya başka biri lehine haksız bir kazanç sağlanması durumunda ortaya çıkan bir suçtur.

2.2.1.2. Ağ Suçları

Verilerin bir yerden başka bir yere iletilmesini sağlayan sisteme ağ sistemi[112]denmekte olup, ikinci suç grubunu oluşturmaktadır. Bu suçlar iki çeşittir.

2.2.1.2.1. Ağ Engellenmesi

Ağın tamamına veya bir kısmına erişimin engellenmesidir. Bu suç farklı şekillerde işlenebilmektedir. En sık karşılaşılan şekli web siteleri ve İSS üzerinden gönderilen veriler yüzünden erişimin engellenmesi ya da önlenmesidir. Buna DDOS (distributed denial of service) saldırıları denmektedir. DDOS saldırıları, "hack" edilen bilgisayarların yönlendirilmiş olduğu siteye, bilgisayara veya sisteme gönderilen veriler nedeniyle başkalarının o siteye, bilgisayara veya sisteme erişiminin engellenmesi veya önlenmesi olarak ifade edilmektedir.

2.2.1.2.2. Ağ Sabotajı

Ağın veya sistemin fiziki ve elektromanyetik olarak tahrip edilmesi veya değişikliğe uğratılmasıdır.

[112] Uçkan ve Beceni; (2004:390)'a göre, ağ sistemlerini üç ana başlık halinde inceleyebiliriz. Birinci ağ sistemi, belli teknik gereklilikleri sağlayan herkesin kullanabildiği açık ağ sistemi; ikincisi sadece tanımlanan kullanıcılar tarafından kullanılabilen intranet (iç ağ); son olarakta belli bir kurumun iletişimini sağlamak için oluşturulmuş kurum içi ağ sistemi extranet (dış ağ) tir.

2.2.1.3. Yetkisiz Erişim Suçları

Burada erişimden; sistemin bir kısmına ya da bütününe veya içerdiği verilere ulaşma kastedilmektedir. Bu suç grubunda iki çeşit suça yer verilmiştir.

2.2.1.3.1. Yetkisiz Erişim

Sistem içerisindeki mevcut olan bilgilere ulaşım hakkı, söz konusu bilgilere ulaşma yetkisi verilen kişilere aittir. Yetkili kişiler dışında sisteme girip bilgilere ulaşmak ve bunları başkalarıyla paylaşmak hemen hemen her ülkede suç olarak kabul edilmiştir. Bu suçun hedefi bir bilgisayar sistemi ya da ağıdır.

2.2.1.3.2. Virüs Yayılması

Bilişim sistemlerine ağ üzerinden veya manuel olarak CD ve disketler kullanılarak zarar vermek için gerçekleştirilen bir suç fiilidir.

2.2.1.4. İlgili Suçlar

Bu başlık altında incelenen husus Bilişim ve İletişim Teknolojileri alanında işlenen suçlarda iştirakin cezalandırılmasıdır. Mevcut ceza kanunlarında iştirak zaten cezalandırıldığından, bu suçlarda ayrıca düzenlemeye gitmenin gereği bulunmamaktadır. Bu başlık altında düzenlenen diğer iki suç türü şunlardır.

2.2.1.4.1. Bilgisayarla İlgili Sahtekarlıklar

Kendisine veya başkasına yasa dışı yollarla maddi menfaat sağlamak ve mağduru zarara uğratmak amacıyla, bilgisayar sistemlerinden yararlanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgelerde (formlar, raporlar, vs.) değişiklik yapmaktır. Dijital ortamda tutulan dokümanları değiştirmek sahtekarlığın bir çeşidi olup, bilgisayarda mevcut olan belgeler (İş akış programları, personel bilgileri vs) değiştirilerek insanlarda yanlış kanaatlar oluşturulabilmektedir.

2.2.1.4.2. Bilgisayarlarla İlgili Dolandırıcılık

Haksız fayda sağlamak amacıyla bilgisayar sistemlerine müdahale ederek veya sahte veri girerek veya mevcut bilgileri değiştirerek mağdura zarar verme eylemidir.

İkinci olarak İnternet Üst Kurulu'nun yapmış olduğu sınıflandırma incelenecektir. Bu sınıflandırma yapılırken, İnterpol Genel Sekreterliği'nin hazırlamış olduğu "İnterpol Bilgisayar Suçları El Kitabı" (Interpol Computer Crime Manual) esas olmak üzere, Birleşmiş Milletler'in hazırlamış olduğu "Birleşmiş Milletler Bilgisayar Suçlarını Kontrol ve Önleme" (United Nations on the Prevention and Control of Computer-Related Crime) kitapçığı ve Avustralya Polis Teşkilatı'nın hazırlamış olduğu "Bilgisayar Kaynaklı Suçların Soruşturulması için Asgari Şartlar" (Minimum Provisions for the Investigation of Computer Based Offences) kitapçıklarından istifade edilmiştir[113]. Söz konusu sınıflandırmaya göre siber suçlar şunlardır.

2.2.2. İnternet Üst Kurulu'nun Yapmış Olduğu Sınıflandırma

2.2.2.1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

2.2.2.1.1. Yetkisiz Erişim

Bir bilgisayar sistemine ya da bilgisayar ağına, bir kişinin yetkisi olmadan erişmesidir. Erişim, sistemin bir kısmına ya da bütününe veya programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Yetkisiz erişim, bir kişi tarafından bir bilgisayara doğrudan yakın bir yerden olabileceği gibi, uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilir.

2.2.2.1.2. Yetkisiz Dinleme

Bir bilgisayar veya ağ sistemi kullanılarak, iletişimin yetkisiz olarak sistem içinden yapılan teknik anlamda dinlenmedir. Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferinin teknik olarak takip edilmesi ve dinlenmesidir.

Teknik anlamda dinleme, iletişim içeriğinin izlenmesi, verilerin kapsamının ya doğrudan (bilgisayar sistemini kullanma ya da erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanma yoluyla) elde edilmesi ile ilgilidir.

[113] Daha geniş bilgi için bkz. http://www.tuena.ubak.gov.tr/m06.php# (27.03.2005)

Suçun oluşması için hareketin yetkisiz ve kasten işlenmesi gerekir. Uygun yasal şartlar çerçevesinde, soruşturma yetkililerinin yaptıkları dinleme bu kategoriye girmez.

2.2.2.1.3. Hesap İhlali

Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının bilgisayar sistemlerinden erişilebilen hesabını kanunsuz olarak kullanmaktır. Başka bir ifadeyle bir kişinin, İnternet, telefon veya benzer bir sistemdeki hesabının kişinin rızası olmaksızın, kanunsuz olarak kullanılmasıdır.

2.2.2.2. Bilgisayar Sabotajı

2.2.2.2.1. Mantıksal Bilgisayar Sabotajı

Bir bilgisayar ya da iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir. O halde mantıksal bilgisayar sabotajı, bir bilgisayar ya da iletişim sisteminin fonksiyonlarına zarar vermek amacı ile verilerin veya programların "zaman bombası", "truva atları", "virüsler", "solucanlar" gibi yazılımlar kullanılarak değiştirilmesi, silinmesi, ele geçirilmesi ya da çalışmaz hale getirilmesidir.

2.2.2.2.2. Fiziksel Bilgisayar Sabotajı

Bir bilgisayara ya da iletişim sistemini oluşturan parçalara, sistemin fonksiyonlarını yerine getirmemesi amacıyla fiziksel yollarla zarar verilmesidir.

2.2.2.3. Bilgisayar Yoluyla Dolandırıcılık

Bilgisayar ve iletişim teknolojileri kullanılarak verilerin alınması, değiştirilmesi ve silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek için mağdura zarar vermektir.

Suçlunun hedefi kendisine veya bir başkasına mali kazanç sağlamak ya da mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları, suçların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık gösterir.

2.2.2.3.1. Banka Kartı Dolandırıcılığı

Kartlı ödeme sistemleri kullanılarak yapılan dolandırıcılık ve hırsızlık suçlarıdır.

Kredi kartları, bankamatik kartları ve benzeri kartlarla yapılan dolandırıcılık suçlarıdır. Kart ödeme sistemleri (ATM-Automated Teller Machine) genelde bankalar veya benzer finans kuruluşları tarafından kullanılırlar. Erişim genellikle bir kişi tanımlama numarası (PIN-Personel Identification Number) girişi gerektiren, bir kart ya da benzeri bir sistem ile yapılmaktadır. Dolandırıcılık bu kartların çalınması, çoğaltılması, kopyalanması veya iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur.

2.2.2.3.2. Girdi/Çıktı/Program Hileleri

Bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden yanlış çıktı almak ya da sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır.

Bir bilgisayar veri tabanına yanlış veri girmek, yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistemde kullanılan yazılım programlarını da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

2.2.2.3.3. İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma

Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerini veya diğer bilgisayar sistemlerini hakkı olmadan kullanmaktır.

2.2.2.4. Bilgisayar Yoluyla Sahtecilik

Kendisine ve başkasına yasadışı ekonomik menfaat temin etmek ve mağdura zarar vermek maksadıyla, bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

2.2.2.5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı

Kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasadışı yöntemlerle elde edilen bilgisayar yazılımlarının satışını, kopyalanmasını, dağıtımını ve kullanımını ifade eder.

2.2.2.5.1. Lisans Sözleşmesine Aykırı Kullanma

Tek bir bilgisayar için alınan yazılımın, birden fazla bilgisayarda lisans haklarına aykırı olarak kullanılmasıdır.

Yazılım lisansları genellikle tek bir bilgisayarda kullanmak üzere tanzim edilir. Tek bir bilgisayar için alınan yazılımın lisans hakları çerçevesinde birden fazla bilgisayara kullanılmak üzere kopyalanması ve çalıştırılması yasaktır.

2.2.2.5.2. Lisans Haklarına Aykırı Çoğaltma

Lisans sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kanunsuz olarak kopyalanmasıdır. Genel itibariyle ödemeden kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılımın başka bir medya ortamına taşınmasıdır.

Burada söz konusu yazılımı kopyalayan da, kopyalatan da sözleşme ihlali yapmış sayılır. Bugün bir çok yerde satılan program, film ve oyun CD'leri bu şekildedir. Bu tür CD'lere bakıldığında üzerlerinde Kültür Bakanlığının bandrolü olmadığı, yazılabilir CD'lere kayıt edildiği ve orijinal kutularında olmadığı görülmektedir.

2.2.2.5.3. Lisans Haklarına Aykırı Kiralama

Değişik medyalar üzerine kayıtlı oyun, film ve yazılımların lisans haklarına aykırı olarak kiralanmasıdır. Başka bir deyişle, oyun, program ve filmleri kiralamaya yönelik özel bir lisansı bulunmadan kiralanmasıdır. Uygulamada daha çok film ve oyun cd'lerinin kiralanması olarak karşımıza çıkmaktadır.

2.2.2.6. Diğer Suçlar

2.2.2.6.1. Kişisel Verilerin Suiistimali

Ticari ya da mesleki sırları, kişisel bilgileri ya da değerli diğer verileri kişinin kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla, bu bilgileri kullanması, satması ve dağıtmasıdır. Daha açık bir ifadeyle, banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kişisel menfaat sağlamak veya başkasına zarar vermek amacıyla bu bilgilere sahip kişilerin rızası dışında kullanılmasıdır.

2.2.2.6.2. Sahte Kişilik Oluşturma ve Kişilik Taklidi

Hile yoluyla kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır.

Bu metotta, gerçek kişilere ait bilgileri kullanarak, o kişinin arkasına saklanılmakta ve o kişinin muhtemel bir suç durumunda sanık durumuna düşmesine neden olunmaktadır. Ayrıca kredi kartı numara oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgilerin, hayali kişiler oluşturulmasında kullanılmasıyla menfaat sağlanılmakta ve zarar verilmektedir.

2.2.2.6.3. Yasadışı Yayınlar

Yasadışı unsurların yayınlanması ve dağıtılması maksadı ile bilgisayar sistem ve ağlarının kullanılmasıdır.

Kanun tarafından yasaklanmış her türlü materyalin, web sayfaları, elektronik postalar, haber grupları ve optik medyalar gibi her türlü veri saklanabilecek dijital kayıt yapan sistemler vasıtasıyla saklanması dağıtılması ve yayınlanmasıdır.

Bir diğer sınıflandırma da Avrupa Konseyi tarafından hazırlanan 23 Kasım 2001 tarihli Siber Suçlar Sözleşmesinde yapılmıştır. Bu sözleşme ileride detaylı bir şekilde incelenecektir.

2.3. Siber suçların işleniş şekilleri (modus operandi)

2.3.1. Genel olarak

Siber suçları, diğer suçlardan yani geleneksel anlamdaki suçlardan ayıran özelliklerden en önemlisi, bu suçların işleniş şekillerinin (modus operandi) tespitinin zorluğudur. Siber suçların işlenmesine vasıta olan maddi hareket çok farklı şekillerde ortaya çıkabilir. Söz konusu suçlar, yepyeni ve çok farklı yollarla işlenebilir. İşin içine bilgisayar ve internet girdiğinde bir suç hem çok hızlı ve kolay bir şekilde işlenebilmekte hem de suçun tespit edilmesi zorlaşmaktadır. Yine suç tespit edilse bile suçun failinin yakalanması için zorlu bir uğraş verilmesi gerekmekte, bu uğraşa rağmen failin her zaman yakalanması mümkün olamamaktadır.

Yukarıda belirtilen nedenlerden ötürü, siber suçların meydana gelmesine sebep olan modus operandilerin tanımlanmasında ve tespit edilmesinde yarar görülmektedir. Bu tanımlama ve tespit işlemi sınırlayıcı değil, örnekleyicidir. Çünkü internet gibi bilgisayar ağlarında her geçen gün kendini yenileyen bu teknolojik gelişme karşısında kesin bir belirlemeye gitmek büyük bir hata olacak ve bu suçlarla mücadelede geri düşülmesine sebep olunacaktır[114]. Bu nedenle her yeni olay yeni bir modus operandi ortaya çıkarabildiğinden aşağıda incelenecek teknikler sadece şu ana kadar görülmüş modus operandilerdir.

2.3.2. Truva atı

Truva atı, Yunan mitolojisinde bir armağan gibi görünüp, aslında Truva kentini ele geçirme hedefi olan Yunanlı askerleri taşıyan tahta bir ata verilen addır. Bugün siber suçların işleniş şekillerinden biri olan truva atı; yararlı gibi görünen, bilgisayar programlarının, aslında arkasında gizli bir kodun da yer alması nedeniyle bilişim güvenliğine zarar veren, tehlikeye atan bir program olarak ifade edilebilir.

Truva atları, bilgisayarları uzaktan yönetmek için arka kapı açan programlardır. Lisanslı programların yasa dışı kopyalarının veya aktivasyon kodlarının dağıtıldığı "warez"[115] diye adlandırılan siteleri veya bedava mp3, oyun

[114] Yazıcıoğlu, 1997:151.
[115] Şifreli olarak kullanılan her türlü program veya verinin şifrelerinin kırılarak ücretsiz olarak dağıtıldığı sitelere verilen addır.

veya yetişkin içerik dağıtan siteleri ziyaret eden kullanıcılar, farkında olmadan yukarıda belirtilen programları bilgisayarlarına indirirken, aynı zamanda kötü niyetli programları da indirmiş olurlar. Bilgisayara kurulan bu programlar, arka plandan çalışarak, kullanıcının sistemine uzaktan erişim imkanı sağlar. Truva atlarıyla sisteme arka kapıdan ulaşan bilgisayar korsanları, bilgisayarın sistem yapılanmasını değiştirebilir, kullanıcının şifrelerine ve diğer kişisel bilgilerine ulaşma imkanına sahip olabilirler. Yani truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren taraf olan bilgisayar korsanının isteklerini yerine getirir[116].

Çeşitli truva atları mevcuttur. Bunların hepsi aynı amaca hizmet etmekle beraber, özellikleri bakımından birbirinden ayrılmaktadırlar. Truva atları altı grupta tasnif edilebilir. Bunlar; "uzaktan kontrol edilen truva atları", "parola truva atları", "imtiyazlı- yükselen truva atları", "anahtar kırıcı", "yıkıcı truva atları", ve "şaka programları"dır[117].

Truva atlarının en popüleri, uzaktan kontrol edilen truva atlarıdır. Bu truva atı türü bilgisayar korsanına, kullanıcının hard diskine erişimini sağlar ve kullanıcının bilgisayarında çeşitli hareketleri (cd-rom sürücüsünü açıp kapayabilir, sistem ekranına çeşitli mesajlar gönderebilir, sistemi kapatabilir vs.) yapmasına olanak verir ve bu durum çoğu kullanıcının korkmasına sebep olur.

Parola truva atı; bilgisayarı parola bulmak için tarar ve bulduğu parolaları ileti yoluyla bilgisayar korsanına gönderir.

İmtiyazlı-yükselen truva atı; sistem yöneticilerini aldatmak için kullanılır. Bu tip truva atları oldukça kullanışlı, ilgi çekici ve zararsız gibi görünen veya bir genel sistemin faydası için zorunlu olduğu düşünülen programların arkasında yer alırlar. Sistem yöneticisi bu programı çalıştırdığında, bu program bilgisayar korsanına sistem üzerinde birçok işi yapabilmesi için imtiyaz sağlar.

---

[116] Değirmenci, 2002:79

[117] Nagpal, Rohas. *What is a Trojan?*. Asian Schol of Cyber Laws. 2004:2-3. 11 KASIM 2005. www.asianlaws.org/cyberlaw/library/cc/what_trojan.htm .

Anahtar kırıcı adı verilen truva atı; kullanıcının klavye üzerindeki her dokunuşunu not eder ve daha sonra bunları ya bir dosyada saklar veya ileti vasıtasıyla belli aralıklarla bilgisayar korsanına gönderir.

Yıkıcı truva atı; kullanıcının tüm sabit diskini, şifresini ya da sadece önemli dosyalarını tahrip eden bir truva atıdır.

Şaka programları adlı truva atı ise, kullanıcının sistemine zarar veren, tahrip eden programlardan değildir. Şaka programlarıyla ya kullanıcının sabit diskine format atılıyor ya da tüm parolaları bazı bilgisayar korsanlarına gönderiliyor gibi gözükür fakat gerçekte hiçbir şey yapılmıyordur.

Şu anda İnternet üzerinde bir çok truva atı dolaşmaktadır. Bunlardan en yaygın olarak kullanılanlar ise "Rottler", "Silk Rope", "Back Office 2000", "Netbus" adlı truva atlarıdır.

Yukarıda da belirtmiş olduğumuz gibi bir truva atıyla bilgisayar korsanının yapabilecekleri, o truva atının program yapısına göre değişiklik arz etmektedir. Örneğin Back Office 2000 isimli truva atı programı ile

- CD-ROM sürücüsü açılıp kapatılabilir,
- Sistem ekranına çeşitli mesajlar gönderilebilir,
- Sistem kapatılabilir,
- Sabit diskteki istediğiniz dosyalar silinebilir,
- Bilgisayar korsanı, sabit diskten kendi bilgisayarına dosya transfer edebilir veya müdahale edilen bilgisayara istediği bir dosyayı yerleştirilebilir,
- Giriş şifresi, kredi kartı şifresi gibi önemli bilgiler ele geçirilebilir[118].

Truva atı programının kullanıldığı bir kaç olayı örnek vermek gerekirse; 06.06.2005 tarihli Sabah Gazetesinde çıkan bir haberde, İsrail gizli servisinin bilgisayar meraklısı olan Suriye First Leydisi Esma Esad'ın İnternet yazışmalarının

[118] Değirmenci, 2002:81.

incelendiğinin belirlendiği belirtilmiştir. Söz konusu eylemin bir truva atı aracılığıyla yapıldığı ve eşi Suriye Devlet Başkanı Beşar Esad ile yapmış olduğu yazışmaların tespit edildiği ve Esad hakkında bir rapor hazırlandığı haber sayfalarında yerini almıştır. Bu eylemde kullanılan truva atının özelliği, hedef bilgisayara casus bir yazılım gönderilerek, ardından bütün ileti ve dosyaların kopyalanması ve programın yönlendirildiği bir başka bilgisayara bu bilgilerin gönderilmesidir.

Bir başka çarpıcı örnek ise, Microsoft'un gizli bilgilerinin Rus Gizli Servisi tarafından "QAZ Truva Atı" adı verilen bir program vasıtası ile ele geçirilmesidir. Adı geçen program bir ileti ile hedef bilgisayara bulaştırılmıştır. Her hangi bir zararlı içerik barındırmıyormuş gibi gözüken bu ileti gerçekte "QAZ Truva Atı" programını barındırıyordu. İleti açılır açılmaz aktif hale gelen program, bilgisayar giriş kodlarını kırarak, Microsoft'un ABD Redmond'da bulunan ana bilgisayarını ele geçirerek, program şifre ve kodları ile bazı bilgileri St. Petersburg'a gönderirken, Microsoft'a ait olan bazı bilgileri de silmiştir. Bu program sayesinde Microsoft'un ana bilgisayarına üç ay boyunca girilmiştir. Çalınan bilgi ve dosyaları elinde bulunduran kişi, bu dosyalar ile Microsoft'un en önemli ürünü olan Windows yazılımının yüklendiği bilgisayarların şifrelerini kıracak virüsleri yazabileceği ve bu bilgisayarlara kolaylıkla girilebileceği ileri sürülmektedir[119].

2.3.3. Bukalemun

Normal bir program gibi çalışan "bukalemun", aslında bir takım hile ve aldatmalar uygulayarak çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklit yeteneği sayesinde gizli bir dosyaya kaydederek, sistemin bakım için geçici bir süre kapatılacağına ilişkin bir uyarı verir. Bu sırada bukalemun programını kullanan kişi, bu gizli dosyaya ulaşarak kullanıcı adlarını ve şifrelerini ele geçirir[120].

2.3.4. Yerine geçme

Bir ağa bağlı olan bilgisayarlara tanınan erişim imkanları sınıflara ayrılabilir. Bazı bilgisayarlara daha geniş erişim imkanı tanınırken diğer bilgisayarlar için bu imkan sınırlandırılabilir. Bu gibi durumlarda, herkesin erişim hakkı, erişim kodu ve

[119] Değirmenci (2002:81): Sabah Gazetesi, 30.10.2000, sf. 26.
[120] Aydın, 1992:51.

parolasıyla belirlenir. Ancak sistemde yapılacak ufak hilelerle erişim hakkı olmayan ya da sınırlı olan şahıslara erişim hakkı sağlanabilmektedir. Sistemde yapılan hile, erişim yetkisi olan bir kişinin parola veya erişim şifresinin yazılması yoluyla yapılıyorsa bu "yerine geçme" olarak isimlendirilmektedir[121].

2.3.5. Mantık bombaları

Truva atı metodunun bir çeşidi olan mantık bombaları, bilişim sisteminde veya ağında bulunan bir program kodunun bir parçasını taşıyan, bazı kötü niyetli hareketlerin yapılması için tasarlanan bir programdır[122]. Mantık bombası, bilgisayar sisteminde, kötü niyetli bir hareket gerçekleştirebilmek için uygun durumlarda veya sürekli olarak faaliyet gösteren bir program olup, bilgisayar sistemlerini bozmak, işlemez hale getirmek için tasarlanmaktadır[123].

2.3.6. Artık toplama

Bilgisayar sisteminin kullanılmasından sonra kalan bilgilerin toplanmasıdır. Yani bilgisayar sisteminin belleğinde mevcut olan ancak ihtiyaç kalmadığından silinen verilerin, gelişmiş teknikler kullanılarak tekrar elde edilmesidir.

2.3.7. Gizli dinleme

Bilgisayar sistemlerinde veri nakli yapılırken kullanılan ağlara girilerek veya bilgisayarın az da olsa yaydığı elektromanyetik dalgaların yakalanarak verilerin tekrar elde edilmesi tekniğidir.

2.3.8. Bilgi aldatmacası

Bilgi aldatmacası, bu tür eylemler arasında en çok tercih edilen basit ve güvenli bir modus operandidir. Bilgisayara veri girilirken yanlış girilmesi, veri saklama ortamında verilerin özel olarak hazırlanmış yöntemlerle değiştirilmesi, bazı kayıtların iptal edilmesi bu yöntem sayesinde rahatlıkla yapılabilmektedir.

---

[121] Değirmenci, 2002:103.
[122] The Information Security Glossary, Logic Bomb, 17 TEMMUZ 2005. http://www.yourwindow.to/information-security/gl_logicbomb.htm
[123] Yazıcıoğlu, 1997:157.

Bilgi aldatmacası ile ilgili olarak şu örnek ilgi çekicidir. Amerika'da yaşayan on beş yaşındaki bir çocuk, evdeki bilgisayarı ile Kaliforniya'daki bir hastanenin kayıtlarına ulaşarak, orada yatan bir hastanın, hastalığına ait geçmiş bilgileri ve ona bağlı olarak hastaya verilen reçetelere ait bilgileri eğlence amaçlı değiştirmiştir. Bu hareket sonucunda hasta alerjik bir reaksiyon sonucu şoka girmiştir[124].

2.3.9. Salam tekniği

Bu teknik genellikle bankacılık sektöründe kullanılmaktadır. Hesaplardaki virgülden sonraki küsuratların son rakamı veya son iki rakamı failin belirlediği bir hesaba aktarılarak orada biriktirilmektedir[125]. Bu durumda çok değersiz gibi görünen rakamlar başka bir hesapta toplandığı zaman büyük yekünler tutmaktadır.

2.3.10. Süper darbe

Süper darbe, bilgisayar sistemlerinin çeşitli sebeplerle işlemez hale gelmesi yani kilitlenmesi durumunda çok kısa bir süre içerisinde sistemin tekrar çalışmasını sağlamak üzere güvenlik kontrollerini aşarak sistemde değişiklik yapılabilmesi için geliştirilmiş bir programdır.

Bu program geliştirilme amacına uygun olarak kullanıldığında çok faydalı olmasına rağmen, kötü niyetli kişiler tarafından kötü amaçlara alet edildiğinde çok tehlikeli olabilmektedir.

Bir Amerikan bankası veri-işlem görevlisi, sistemde meydana gelen bir hatayı düzeltmek için kullandığı süper darbe programının güvenlik tedbirlerini ortadan kaldırdığının farkına varmış ve arkadaşlarının hesaplarına yüklü miktarlarda para aktarmıştır. Bu olay bir banka müşterisinin hesabında meydana gelen azalmayı fark etmesi sonucunda ortaya çıkmıştır[126].

2.3.11. Ağ solucanları

Ağ solucanları genellikle virüslerle karıştırılan, bilgisayar ağları arasında herhangi bir donanıma veya yazılıma zarar verme zorunluluğu olmadan dolaşan,

[124] Wrobleski and Hens, 1990:366.
[125] Yazıcıoğlu, 1997:155.
[126] Yazıcıoğlu, 1997:156: Castelli'den, 1986:27.

kullanıcı müdahalesine gerek kalmadan kendi kendini aktif hale getirebilen ve bir kopyasını ağa bağlı olan diğer bilgisayarlara bulaştırabilen bir programdır. Ağ üzerinde dolaşan bir ağ solucanı, bilgisayar sistemine bir virüs gibi davranarak yazılıma zarar verebileceği gibi bir truva atı da bırakabilir.

2.3.12. Bilgisayar virüsleri

Günümüzde bilgisayarların en büyük düşmanları olarak gösterilen virüsler, bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen kötü amaçlı programlardır. Teknik olarak bir bilgisayar programının virüs sayılması için kendi benzerini yapıp, bunu başka programlara bulaştırabilme yeteneğine sahip olması gerekmektedir.

Virüslerin bilgisayarların başlıca düşmanı olarak gösterilmesinin haklı gerekçeleri vardır. Gerçekten virüsler, bilgisayarla çalışmayı imkansız hale getirebilmekte, sistemde bulunan bilgilere zarar verebilmekte, sabit diskteki verileri silebilmektedir.

Virüsler baslıca üç bölümden meydana gelmişlerdir. Bunlar sırası ile kopyalama bölümü, gizleyici bölümü ve etki bölümüdür.

Kopyalama bölümü ile kendisini çalıştırılabilir dosyalara ilave eder.

Gizleyici bölümü, kendini gizleme görevi yapar. Daha ziyade anti-virüs programlarının gözünden kaçmak ve anti-virüs programını yanıltmak için oluşturulmuştur.

Etki bölümü ile asıl işlem yerine getirilir. Asıl işlemin yaptığı zararlı etkilere; verileri karıştırmak, programın bir kısmını silmek, disk veya disketin çalışmasını engellemek örnek olarak verilebilir.

Genel olarak virüsleri tahrip edici ve sisteme rahatsızlık verici olarak ikiye ayırmak mümkündür. Tahrip edici virüsler, verilerin veya programların bir kısmına veya tamamına zarar verip, sistemin çalışmasına mani olurken, sisteme rahatsızlık

verici virüsler ise geçici bir süre sistemin çalışmasına mani olan, ekranda garip mesajların görünmesine sebep olan virüslerdir[127].

Bilgisayar virüslerinin yol açtığı zararlar küçük gibi gözükse de toplamda çok büyük zararlara yol açabilmektedirler. 3 Mayıs 2000 günü tüm dünyada yayılan ve elektronik postaya ekli olarak gelen "I Love You" veya "Love Bug" virüsü olarak bilinen bir virüs, çok kısa zamanda 55 milyon bilgisayara ulaşmış ve bunlardan 2.5-3 milyonuna bulaşarak 8.7 milyar dolar zarara sebebiyet vermiştir[128].

2.3.13. İstem dışı alınan elektronik iletiler (SPAM)

İnternet'in yaygınlaşmasıyla birlikte ortaya çıkan yeni bir kavram olan SPAM, istem dışı alınan elektronik iletilere verilen isimdir. SPAM, Amerikan orijinli bir kelime olup, bir Amerikan firmasının baharatlı domuz eti ve jambon için kullandığı "Spiced Pork And Ham" kelimelerinin baş harflerinin alınması ile oluşturulmuştur[129].

SPAM, genellikle pazarlama, reklam veya sosyal içerikli olarak büyük kitlelere ulaştırılmak istenen mesajların kullanıcının isteği dışında kendisine İnternet ya da cep telefonu gibi teknolojiler aracılığı ile yollanmasına dayanır[130].

Fransız Ulusal Enformasyon ve Özgürlük Komisyonu (Commission Nationale de l'Informatique et des Libertés) SPAM'ı, hiçbir temas olmaksızın tartışma forumlarından, dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının talebi olmaksızın arasıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalar olarak tanımlamıştır[131].

Bireylerin özgür iradesine müdahale edici, bireysel ve ulusal kaynak israfına yol açıcı olması nedeniyle Ulaştırma Bakanlığı bünyesinde oluşturulan İnternet Üst

---

[127] Yazıcıoğlu, 1997:163
[128] Zetter, 2000:80 vd.
[129] Memiş, Tekin. *Hukuki Açıdan Kitlelere E-posta Gönderilmesi.* Saarbrücken Hukuki İnternet Projesi. 18 AĞUSTOS 2005. www.jura.uni-sb.de/turkish/TMemis1.html
[130] İnternet Üst Kurulu SPAM Bildirgesi. T.C. Ulaştırma Bakanlığı İnternet Üst Kurulu. 01 TEMMUZ 2000. 18 AĞUSTOS 2005. http://kurul.ubak.gov.tr/m08.php,
[131] Memiş, Tekin. *Hukuki Açıdan Kitlelere E-posta Gönderilmesi.* Saarbrücken Hukuki İnternet Projesi. 18 AĞUSTOS 2005. www.jura.uni-sb.de/turkish/TMemis1.html

Kurulu 12 Ocak 2000 tarihli "SPAM Bildirgesinde", SPAM'ın bir kamu suçu oluşturduğunu belirtmiştir[132].

SPAM'ın yarattığı en temel sakıncaları İnternet Üst Kurulu dört madde olarak sıralamıştır. Bunlar:

1) Kişi ve kuruluşların e-posta adresleri, cep telefon numaralarında olduğu gibi kişisel bilgileridir. Bu gibi bilgilerin kişisel izin olmaksızın ticarete konu olması kişilik haklarına açık bir saldırıdır.

2) SPAM iletileri bireysel İnternet kullanıcıları için en azından ek maliyet anlamına gelmektedir. Oluşan toplam kayıp ise ciddi bir ulusal kaynak israfına işaret etmektedir.

3) SPAM iletileri, yeni gelişmekte olan İnternet Servis Sağlayıcı kuruluşlarının kaynaklarını da israf etmekte, kullanıcılarına daha iyi servis vermelerini engellemektedir.

4) SPAM, yasadışı ürün ve servislerin tanıtımı için de kullanılabilmektedir.

Türk hukuku içinde SPAM'ı yasaklayan veya cezalandıran bir düzenleme bulunmamakla birlikte, SPAM ileti gönderilmesini engelleyebilecek hükümler bulunmaktadır. Bunlardan biri olan Tüketicinin Korunması Hakkında Kanun, sadece içeriği reklam olan e-postalara karşı bir yaptırıma sahipken, Medeni Kanunun 24 üncü maddesi ve devamı hükümleri, kitlelere gönderilen gayri ticari iletilere karşı en etkin korumayı sağlayan hükümler olarak görülmektedir.

E-posta sahiplerini SPAM'a karşı korumanın en etkili yolu, kanun koyucunun SPAM hakkında bir kanuni düzenleme yapmasıdır. Yapılacak olan kanuni düzenlemede iki yol tercih edilebilir. Bunlardan birincisinde, SPAM yapma konusunda herhangi bir yasaklama yoluna gidilmeyerek, sadece e-posta sahibinin reddi halinde bir daha SPAM yapılmaması; aksi halde cezalandırma yoluna gidilmesidir. İkincisinde ise SPAM yapan kimsenin önceden e-posta sahibinden izin almasıdır. Her iki kanuni düzenleme biçimi de 4.6.1997 tarihli "Mesafe Ötesi Sürüm

[132]İnternet Üst Kurulu Spam Bildirgesi. T.C. Ulaştırma Bakanlığı İnternet Üst Kurulu. 01 TEMMUZ 2000. 18 AĞUSTOS 2005. http://kurul.ubak.gov.tr/m08.php,

Sözleşmelerinde Tüketicinin Korunması Hakkında" ki Avrupa Birliği Direktifine uygundur[133].

SPAM'ın vermiş ve vermekte olduğu rahatsızlığın derecesini bir örnekle netleştirmek gerekirse, ABD'de görülen bir davada, İnternet'ten SPAM gönderen 3 şirket, şimdiye dek SPAM'cılara verilen en yüksek cezaya çarptırılmışlardır.

Iowa eyaletinde görülen davada federal yargıç, merkezi Arizona'da bulunan AMP Dollar Savings şirketini 720 milyon dolar, Florida'daki Cash Link Systems şirketini 360 milyon dolar ve yine Florida'da kurulu bir şirket olan TEI Marketing Group'u 140 bin dolar tazminat ödemeye mahkum etmiştir[134].

2.3.14. Web sayfası hırsızlığı ve web sayfası yönlendirme

Amerika ve Almanya'da çok sık görülen bu suç tipinde, kendisine bir İnternet adresi (domain name)[135] almak isteyen kişinin İnternet Servis Sağlayıcıya başvuruda bulunduğu sırada, sisteme müdahale eden bir bilgisayar korsanı veya bu bilgiye ulaşan bir İnternet servis sağlayıcı çalışanı tarafından kendileri veya üçüncü bir kişi adına daha hızlı davranılarak kaydettirilmesi ve daha sonra bu adresin yüksek ücretle satılması fiilidir[136].

Web sayfası yönlendirme ise, İnternet adreslerini dağıtmakla sorumlu olan organizasyonların[137] veri bankasında bulunan web sayfalarına, İnternet üzerinden nasıl erişilebileceğine dair "yönlendirme kuralları"nın yapılan müdahalelerle değiştirilerek, İnternet kullanıcılarının farklı İnternet adreslerine yönlendirilmesidir. Burada bilgisayar korsanı herhangi bir İnternet adresine ulaşmaya çalışan İnternet kullanıcısına, farklı bir IP numarası vererek, değişik bir bilgisayara yönlendirmektedir. İnternet kullanıcısı bir İnternet adresine ulaşmak için isim olarak yazar. Örneğin Devlet Planlama Teşkilatı Müsteşarlığının web sayfasına ulaşmak

---

[133] Memiş, 2005:1

[134] http://www.sabah.com.tr/2004/12/20/dun99.html (15.05.2005)

[135] Türkçe karşılığı internet adresi veya alan adı olan Domain Name, IP adresi denilen, bilgisayarların birbirini tanımasını sağlayan numara sisteminin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş halidir. Örneğin dpt.gov.tr alan adını adres barına yazıldığında Internet bu alan adını önce IP adresine çevirir, daha sonra IP adresine sahip bilgisayara yönlendirir.

[136] Değirmenci, 2002:99.

[137] Ülkemizde internet adreslerini dağıtmak ve kayıt etmekle sorumlu ve yetkili olan ODTÜ'nün bağlı bulunduğu "Resaux IP Europeens Network Coordination Center" (RIPE) gibi organizasyonlardır.

isteyen kullanıcı www.dpt.gov.tr yazar, fakat bu bilgi web sayfasının bulunduğu bilgisayara erişebilmek için kendi başına yeterli değildir, bunun yanında IP numarasının bilinmesine de gerek vardır. Alan Adı Sunucusu (Domain Name Server) bu IP numarasını diğer alan adı sunucularına sorar, bilgisayar korsanları işte bu noktada müdahale ederek "Alan Adı Sunucusu"na farklı bir IP numarası bulduarak istediği bilgisayara kullanıcıyı yönlendirir. Bu yöntem genellikle banka web sayfasına ulaşmak isteyen kullanıcılara uygulanır ve kullanıcıların yönlendirildiği bilgisayar kullanıcının gerçekte ulaşmak istediği web sayfasının benzer şekilde tasarlanan bir web sayfasıdır. Burada kullanıcı şifrelerini girdiğinde, bilgisayar korsanı bu şifreleri elde eder ve kötü niyetini gerçekleştirmek üzere kullanır.

Web sayfası yönlendirmede kullanılan diğer bir metot ise, "yanlış yazanları kaçırma" olarak adlandırılan ve oldukça basit olan bir tekniktir. Burada bilgisayar korsanı genellikle yapılan yanlışları dikkate alarak, bu yanlışları yapan kullanıcıları kendi sayfasına yönlendirir[138]. Örneğin, birçok kişi tarafından Amerika Başkanlık Sarayının internet adresi www.whitehouse.com olarak bilinir, fakat doğru adres www.whitehouse.gov'dur. Çok sık yapılan bu yanlışı göz önüne alan bir kişi, bu yanlışı değerlendirerek www.whitehouse.com İnternet adresini kendi adına kaydettirerek, Amerika Başkanlık Sarayının sitesine girmek isteyen kişileri porno sayfası haline getirdiği siteye çekmiştir[139].

2.3.15. Phishing

Phishing saldırıları; İnternet suçları arasında en yaygın ve tehlikeli olanlarından biridir. İngilizce "Balık tutma" anlamına gelen "Fishing" sözcüğünün "f" harfinin yerine "ph" harflerinin konulmasıyla türetilen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuştur.

Phishing; bir İnternet kullanıcısının müşterisi olduğu bankanın, e-posta veya bunun gibi bilgi girmeyi gerektiren bir kuruluşun web sayfasının bir kopyasının yapılarak söz konusu kullanıcının hesap bilgilerini çalmayı amaçlayan bir İnternet

[138] Değirmenci, 2002:100.
[139] Sırımcıyan, 2000:258.

dolandırıcılığıdır. Sahtekarlığı gerçekleştirecek kişi/kişiler; bir banka, kart şirketi veya finansal işlemler gerçekleştiren bir finans şirketinden geliyormuş gibi hazırladığı sahte e-postayı, elde edebildiği tüm e-posta adreslerine gönderir. E-posta'nın konusu; müşterilerin bilgilerinin güncellenmesi veya şifrelerin değiştirilmesi amacı içeren ifadelerden ve ilgili kurumların sayfalarının bire bir kopyası şeklinde görünen İnternet sayfalarına giden linklerden oluşmaktadır.

Bazı İnternet kullanıcıları, tehlikenin farkında olmadan, istenilen bilgileri doldurarak e-posta'lara cevap verirler. Bunun sonucunda, bu kişilerin kişisel bilgileri ve şifreleri dolandırıcılar tarafından çalınmış olur.

Phishing metodu ile yapılan online sahtekarlıkta çalınan bilgiler;

1. Kredi, Debit/ATM Kart Numaraları

2. Şifreler ve Parolalar

3. Hesap Numaraları

4. İnternet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleridir.

Phishing metodu dünyada gün geçtikçe yaygınlaşmakta olan bir metottur. Bunun nedeni ise bu metotla yüksek miktarlarda kolay ve haksız para kazanma ihtimalinin olmasıdır.

Söz konusu yöntem ile dolandırıcılık yapan bir şebeke de Türkiye'de ortaya çıkarılmıştır. İstanbul Şişli'de yapılan bir operasyonla, İnternet'te işlem yapan banka müşterilerine ait bilgileri elde ederek dolandırıcılık yaptıkları öne sürülen biri kadın dört kişi yakalanmıştır. Operasyonun ilgi çekici yanlarından biri ise, 17 yaşındaki bir bilgisayar korsanının bu şebeke içerisinde yer almasıdır[140].

2.4. Siber suçlular

Her kim bir bilgisayar sistemine yetkisi olmadan girerse veya bilgisayarı bir suç işlemek için kullanırsa, halk ve medya bu kişiye bilgisayar korsanı (hacker)

[140] 08.04.2005 tarihli Milliyet Gazetesinden alınmıştır.

ismini vermektedir[141]. Gerçekte ise bilgisayar korsanı terimini tanımlamak bu kadar kolay değildir.

Siber suçluların tanımı ve sınıflandırılması bugüne kadar çok farklı yollardan yapılmıştır[142]. Bu sınıflandırmalar yapılırken siber suçluların yetenekleri, davranış özellikleri ve suç işleme nedenleri esas alınmıştır.

2.4.1. Suç İşleme Nedenine Göre Siber Suçlular

Suç işleme nedenine göre yapılan sınıflandırmaya göre siber suçlular, idealistler, açgözlülükle hareket eden profesyonel suçlular ve siber teröristler olarak üç gruba ayrılarak incelenmiştir[143].

2.4.1.1. İdealistler

Bu gruptakiler genellikle suç geçmişi olmayan 12-19 yaş arası gençlerden oluşmaktadır. Bu yaş grubundaki insanlar "siber kültüre" toplumda en hızlı şekilde adapte olan gruptur. Bunun nedeni, İnternet'in onlara içinde bulundukları yaşta aradıkları özgürlüğü sağlamasıdır.

İdealistler olarak adlandırılan grubu siber suç işlemeye yönlendiren saikler genellikle medyanın ilgisini çekmek ve arkadaşlarına bu konudaki gücünü göstererek içinde bulunduğu toplumun hiyerarşisinde yukarı tırmanmaktır.

Bu tip siber suçluların topluma sıklıkla yardımı dokunduğu kabul edilmektedir. Şöyle ki, medyatik ve bireysel bazda zararsız eylemleri yoluyla, önemli suç örgütlerinin veya siber suçları maddi menfaat elde etmek amacıyla yapan diğer siber suçluların gerçek anlamda zarar vermek amacıyla kullanabilecekleri güvenlik açıklarının keşfedilmesine yardımcı olurlar.

İdealistlerin eylemlerinin suç ilan edilmesinin onları durdurmayacağı aksine tehlike ve heyecan istediklerinden bu durumun onları daha fazla kamçılayabileceği

---

[141] Quarantiello, 1997:16.
[142] Icove at al, 1995:61.
[143] Bu sınıflandırma için bkz. Magnin, J. Cedric, "The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?", 01 HAZİRAN 2001:7-14. 09 ARALIK 2004. http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf

son çalışmalarla belirlenmiştir[144]. Bu sebepten dolayı bu gençlerin ancak eğitim yoluyla bu tür suçları işlemeleri engellenebilecektir.

2.4.1.2. Profesyonel Siber Suçlular

Suç bilimcilere göre suç toplumun bir parçasıdır. Suç her zaman var olmuştur ve hep var olacaktır. Bu nedenle, profesyonel suçlular kendilerini teknoloji ile dolu yeni bir dünya olan siber dünyaya entegre etmekte çok gecikmemişlerdir.

Bu kategorideki siber suçlular, normal hayattaki suçlular gibi vicdan ve ahlaktan yoksun insan grubu olduğundan, onlara nakit sağladığı sürece herhangi bir suçu siber uzayda işlemekten çekinmeyeceklerinden dolayı tehlikelidirler. Çocuk pornografisinin kökeninde bile bunlar vardır.

Yine bu tip siber suçlular iyi organize olmuşlardır ve polisten nasıl kaçacaklarını bilirler. Karargahlarını da genellikle sıkı polis kontrolü olmayan yerlere kurarlar. Toplum için potansiyel olarak çok tehlikeli ve zarar vericidirler.

Maddi olarak vermiş oldukları hasarlar, idealist gençlerin bir virüs göndererek neden oldukları zarardan daha az görünse de, kurban başına zarar daha yüksek ve ekonomik olarak daha yıkıcıdır.

Bu tür siber suçlularla mücadele edebilmek için öncelikle bu suçluların kanundan kaçmasına neden olabilecek kanuni boşlukların doldurulması, uluslararası yasaların birbirine uyumlu hale getirilmesi ve ulusal güvenlik güçleri arasında koordinasyon ve yardımlaşmanın teşvik edilmesi gerekmektedir.

2.4.1.3. Siber Teröristler

Bu kategoride yer alan suçlular, siber dünyanın potansiyel olarak en tehlikeli suçlularıdır. Ana eylem amaçları sadece para değil, aynı zamanda savundukları görüşün de reklamını yapmaktır.

Siber terörün, yeni yüzyılda terörizmin yeni yüzü olarak karşımıza çıkacağı düşünülmektedir. Bunun nedeni artık insanların bilişim teknolojilerini daha fazla kullanmaya başlamaları ve gerçek hayatta yaptıkları bir çok şeyi siber uzayda da

[144]Chebium, Raju, *Experts Say More Laws Won't Stop Computer Hackers.* 08 MAYIS 2000. 17 ARALIK 2004. www.cnn.com/2000/LAW/05/05/love.bug/index.html

yapmaya başlamalarıdır. Bu durum terörist grupların ilgisini çekmekte gecikmemiştir ve bu alanda boy göstermek için çaba sarf etmeye başlamışlardır.

Zaten teröristlerin siber uzayda yapabileceklerine baktığımızda, amaçları toplum nezdinde kaos yaratmak olan bu grup için siber suçlar gayet caziptir. Siber uzayda yapabileceklerini örneklerle somutlaştırmak gerekirse; elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşme sistemine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını söndürebilecekleri, telefonları felç edebilecekleri, elektrik ve doğal gaz hatlarını kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri, bankacılık ve finans sektörünü çökertebilecekleri, acil yardım, polis, hastaneler ve itfaiyelerin çalışmasını engelleyebilecekleri, hükümet kurumlarını alt üst edebilecekleri, sistemin birden durmasına neden olabilecekleri ihtimaller dahilindedir[145].

2.4.2. Yeteneklerine Göre Siber Suçlular

Konunun bazı uzmanları[146], siber suçluları yeteneklerine göre sınıflandırmışlardır. Bu sınıflandırmaya göre siber suçlular; "kırıcılar", "bilgisayar korsanları" ve "kemirici"lerdir.

2.4.2.1. Kırıcılar (Crakers)

Siber suçlular içerisinde teknik bilgi ve donanım bakımından en ileri seviyede olan siber suçlulardır. Kötü niyetli olarak kendisine veya üçüncü bir şahsa çıkar sağlamak amacıyla, web sayfalarının veya sistemlerin güvenlik duvarlarının şifrelerini kırarak, web sayfalarına veya sistemlere zarar verilmesi eylemini gerçekleştiren suçlulara siber dünyada "kırıcı" adı verilmektedir[147]. Bu kişiler diğer suçlu tiplerine göre daha kötü niyetli ve yıkıcı faaliyetlerde bulunurlar.

Bilgisayar korsanı ile kırıcı (hacker – craker) kavramları sıklıkla birbirlerinin yerlerine kullanılmaktadırlar. Oysa yukarıda verilen tanımlardan da anlaşılacağı

---

[145]Özcan, Mehmet. *Yeni Milenyumda Yeni Tehdit: Siber Terör.* Uluslararası Stratejik Araştırma Kurumu. 28 EYLÜL 2004. 18 TEMMUZ 2005.
http://www.turkishweekly.net/turkce/makale.php?id=12 (18.07.2005)
[146] Yazıcıoğlu, 1997:120.
[147] Özdilek, 2002:166

üzere aralarında temel farklılıklar mevcuttur. Bilgisayar korsanları, bir sistemin güvenlik duvarını aşarak sisteme izinsiz girmek suretiyle her türlü bilgiye ulaşırlar; kırıcılar ise güvenlik duvarlarını kırarak sisteme girerler ve verileri yok etme, değiştirme, şifreleri kırma ve bunları dağıtma gibi fiillerle zarar verirler. Yani iki suçlu tipindeki temel fark birinin sisteme zarar vermesidir.

2.4.2.2. Bilgisayar korsanları (hackerlar)

İşletim sistemlerinde mevcut olan güvenlik açıklarını tespit ederek, bu açıkları kullanarak sisteme yetkisiz giriş yapan kişilere verilen isimdir.

2.4.2.3. Kemiriciler (Rodents)

Sisteme müdahale edenler arasında bilgi seviyesi en alt düzeyde olan kişilere rodents denmektedir. Söz konusu kişiler bu alanda oldukça yeni ve zararsız kişilerdir.

2.4.3. Davranış Şekillerine Göre Siber Suçlular

Siber suçlular davranış şekillerine görede üç grup olarak sınıflandırılmışlardır[148]. Bunlar; "gerçek uzmanlar", "siliciler", elektronik vandallar"dır.

2.4.3.1. Gerçek Uzmanlar

Emniyet önlemlerini ortadan kaldırarak, meraklarını giderebilmek maksadıyla sistematik ve düzenli bir çalışma ile sistemlere girmeye çalışanlara gerçek uzmanlar adı verilmektedir.

2.4.3.2. Siliciler

Oyun amaçlı veya elde ettikleri bilgileri değişim aracı olarak kullanabilmek için sistemlere giren kişilere verilen isimdir.

2.4.3.3. Tahrip Ediciler

Sisteme müdahale edenler arasında azınlık olan bu kişiler, sistemlere girme konusunda oldukça tecrübeli ve tehlikelidirler. Bunun nedeni ise girdikleri sisteme tahrik edici mesajlar bırakmaları veya zarar vermeleridir.

---

[148] Yazıcıoğlu, 1997:121:Samocıuk'dan, 1986:9.

2.5. İnternet İşlevlerini Yerine Getiren Öznelerin Ceza Sorumluluğu

İnternet'in kendine has karakteri sebebiyle herhangi bir sahibi yoktur. Günümüzde bu kadar yaygınlaşmasının sebebi hem birisinin mülkiyetinde olmaması hem de İnternet'e girebilmek için herhangi bir kurala uyulması ya da izne gerek bulunmamasıdır. Dünyadaki herhangi bir insan, eğer ülkesinde gerekli alt yapı mevcutsa ve İnternet'e ulaşabilmek için gerekli donanıma sahipse İnternet'e girebilir.

İnternet'in bir özgürlük dünyası olarak görülmesi nedeniyle İnternet'teki özgürlüğü kısıtlayacak herhangi bir düzenleme kamuoyunda çok büyük yankılar uyandırmaktadır. İnternet'in anavatanı olan ABD, bu önemli ve gittikçe etkisini arttıran kitle iletişim sisteminin zararlarından endişe duyarak, İnternet üzerindeki suç içerikli yayınların önlenmesi amacıyla, 1934 tarihli Telekomünikasyon Yasasına yeni hükümler getiren (Communications Decency Act – İletişim Ahlak Yasası) bir yasa tasarısı hazırlamış ve bu tasarı 8 Şubat 1996 tarihinde yürürlüğe girmiştir. Bu yasa ile İnternet üzerinde pornografik veya şiddet içerikli yayında bulunulması suç olarak düzenlenmiş ve bu yayını gerçekleştiren süjelerin iki yıla kadar hapis cezası ile 250.000 dolara kadar para cezası ile cezalandırılması öngörülmüştür. Fakat, tasarının kanunlaşmasından bir yıl sonra söz konusu yasanın Anayasaya aykırılığı iddia edilmiş, Amerikan Yüksek Mahkemeside hükmü anayasaya aykırı bularak iptal etmiştir[149]. Söz konusu mahkemenin bu kararı vermesindeki nedenlerinden biri de, İnternet'in sansüre uğramasına engel olmaktır.

Kuşkusuz İnternet'in, yasaların geçerli olmadığı, bireylerin ve kuruluşların haklarının korunmadığı bir ortam olarak algılanmaması gerekir. Toplumun faaliyet gösterdiği diğer alanlarda nasıl hukuk egemense, İnternet ortamında da hukukun egemen olacağı muhakkaktır. Bu sebeple İnternet ortamını hukuk şemsiyesi altına almak için kanun koyucular İnternet öznelerine belirli yasalarla sorumluluklar yüklemektedirler. Burada ülkelerin en çok üzerinde durdukları konu, bir İnternet yayını olarak ortaya çıkan siber suçlardan doğan ceza sorumluluğunun kime ait olacağı, bir başka deyişle içeriğinde suç unsuru bulunan yayınlardan kimin sorumlu tutulacağıdır[150].

[149] İçel, 2000:415
[150] Sınar, 2001:86

İnternet suçlarından dolayı ceza sorumluluğuna ilişkin esasların saptanması amacıyla karşılaştırmalı hukukta yapılan çalışmalar incelendiğinde, Almanya'da kabul edilen ve 13 Haziran 1997 tarihinde yürürlüğe giren Teleservisler Yasasının öne çıktığı gözlemlenmektedir[151]. Gelişen teknolojinin yarattığı çeşitli iletişim sistemlerine uygulanacak hukuki rejimi belirlemek için çıkartılan bu yasanın 5'inci paragrafında İnternet yayınlarından doğan ceza sorumluluğuna ilişkin esaslar belirlenmiştir.

Aşağıda Avrupa Konseyinin aldığı kararlardan da yararlanarak İnternet öznelerinin cezai sorumlulukları incelenecektir.

2.5.1. Telekomünikasyon idarelerinin cezai sorumluluğu

Haberleşme kanallarını ve dolayısıyla veri hatlarını kontrol altında tutan ve İSS'lere kiralayan kurumlar olarak İnternet sisteminin ilk özneleri Telefon/ Telekomünikasyon idareleri olmaktadır[152].

Telefon/ Telekomünikasyon idareleri var olan telefon hatlarından özel hatları İnternet bağlantısı hizmetine sunmaktadır. Bu hatlar İSS'lere tahsis edilmektedir.

Birçok ülkede telekomünikasyon alt yapısını kurma ve bunu işletme hakkı ya kamu kurumu niteliğindeki kuruluşlara ya da imtiyaz tanınan kuruluşlara verilmektedir.

Şu an ülkemizde İnternet haberleşmesinin sağlanmasında kullanılacak olan veri hatlarının kurulması hizmeti Türk Telekomünikasyon A.Ş. tarafından yapılmaktadır. Fakat veri hatları kurulması hizmeti Türk Telekomünikasyon A.Ş.'nin tekelinde değildir.

26 Haziran 2004 tarihli ve 25565 sayılı Resmi Gazete'de yayımlanan Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğine göre İSS'lerin faaliyet gösterebilmeleri için Telekomünikasyon Kurumundan genel izin almaları gerekmektedir. Yine 15 Kasım 2005 tarihli ve 25994 sayılı Resmi Gazete'de yayımlanan "Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik"in birinci

[151] İçel, 2000:415.
[152] Demir, 2002:474.

maddesi ile Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinin İnternet Servis Sağlayıcılığı Hizmetine ilişkin EK-A6 bölümü değiştirilmiş ve İSS'lerin hakları ve yükümlülükleri belirlenmiştir.

Bu Yönetmelik ile İSS'lerin anılan Yönetmeliğin ana metninde yer alan yükümlülüklerine ilaveten yerine getirmek zorunda olduğu bazı yükümlükler getirilmiştir. Bu yükümlülükler;

İşletmeci, yetkilendirme kapsamında kullanıcılara internet üzerinden telefon hizmetleri sunamaz.

İşletmeci, kullanıcılarının internet üzerindeki yetkisiz ve rahatsız edici girişimlerine meydan verilmemesi için gerekli tedbirleri almakla yükümlüdür.

İşletmeci, vereceği hizmete ve sisteminde kullanılacak cihazlara, yetkisiz kişilerin erişimi ve bozucu/değiştirici müdahalelerini önlemek amacıyla gerekli tedbirleri almakla yükümlüdür.

İşletmeci, her bir kullanıcı için, kullanıcı tarafından sisteme bağlı kalınan süre, trafik miktarı ve trafik yolu bilgilerini en az 6 (altı) ay süreyle muhafaza etmekle yükümlüdür.

İşletmeci, hizmetin kesintisiz olarak sunulması için gereken tedbirleri almakla yükümlüdür.

İşletmeci, internet servis sağlayıcılığı hizmetini tanıtmaya yönelik olarak "tr" uzantılı en az bir internet sitesi kurmakla yükümlüdür.

İşletmeci, internet servis sağlayıcılığı hizmetini, kendi adına vermekle yükümlü olup, söz konusu hizmeti internet servis sağlayıcılığı yetkisi olmayan kişi veya şirket adına sunulacak şekilde veremez. Ancak, gerçek veya tüzel kişiler, aldıkları internet erişim hizmetini, kişisel telekomünikasyon tesisi içerisinde halka açık olarak verebilir.

İşletmeci, erişim sistemini kullanıcılara internet erişim hizmeti verilmesi haricinde başka amaçlar için kullanamaz. Kişisel telekomünikasyon tesisi alanı dışında bu sistemler noktadan noktaya kablosuz veri iletim amacıyla kullanılamaz.

İşletmeci tarafından kurulacak erişim sistemindeki cihazlar enterferansa karşı korunmamış olup, tahsis ve tescil edilmiş frekanslardaki diğer telsiz sistemlerinin çalışmasından meydana gelecek enterferansı kabul eder ve söz konusu telsiz sistemlerini enterfere edemez.

Erişim sisteminin kurulacağı yer ile ilgili gerekli izinlerin alınması, sistemin tesis edilmesi ve kullanılmasından kaynaklanan her türlü sorumluluk işletmeciye aittir.

Erişim sisteminde kullanılacak cihazlar, Telsiz ve Telekomünikasyon Terminal Ekipmanları Yönetmeliğine, Kısa Mesafe Erişimli Telsiz Cihazlarının Kurma ve Kullanma Esasları Hakkında Yönetmeliğin 8 inci maddesinde belirlenen kriterlere ve Kurumun diğer düzenlemelerine uygun olacaktır.

Yukarıda belirtilen yükümlülüklere İSS'lerin uymamaları durumunda 406 sayılı Telgraf ve Telsiz Kanununun 2'nci maddesinin f bendine göre cezalandırılacaklardır[153].

2.5.2. İnternet servis sağlayıcıların cezai sorumluluğu (İSS)

Hukukumuz açısından İSS'lerin[154] faaliyet koşulları ile ilgili özel bir kanun hükmü bulunmamaktadır. Fakat, yukarıda da belirtildiği gibi 15/11/2005 tarihli ve 25994 sayılı Resmi Gazete'de yayımlanan "Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinde Değişiklik Yapılmasına Dair Yönetmelik"in birinci maddesi ile 26/8/2004 tarihli ve 25565 sayılı Resmi Gazete'de yayımlanan Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliğinin İnternet Servis Sağlayıcılığı Hizmetine ilişkin EK-A6 bölümü değiştirilmiş ve İSS'lerin hakları ve yükümlülükleri belirlenmiştir.

---

[153] 406 sayılı Kanunun 2'nci maddesinin f bendine göre "Kurum; Türk Telekom dahil işletmecilerle imzaladığı sözleşmelerin ve verdiği genel izin ve telekomünikasyon ruhsatlarının şartlarına uyulmasının sağlanması için gereken tedbirleri almaya, faaliyetlerin mevzuat ile görev ve imtiyaz sözleşmesi, telekomünikasyon ruhsatı veya genel izin şartlarına uygun yürütülmesini izleme ve denetlemeye, aykırılık halinde ilgili işletmecinin bir önceki takvim yılındaki cirosunun % 3'üne kadar idari para cezası uygulamaya, milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amaçlarıyla gerekli tedbirleri almaya, gerektiğinde tesisleri tazminat karşılığında devralmaya ya da ağır kusur halinde imtiyaz sözleşmesini, telekomünikasyon ruhsatını ya da genel izni iptal etmeye yetkilidir."

[154] İntrernet Servis Sağlayıcısının tanımı için bkz. sf.15-16.

Telekomünikasyon Hizmet ve Altyapılarına İlişkin Yetkilendirme Yönetmeliği'ne göre "İşletmeciler, İSS hizmetini Telekomünikasyon Kurumundan alacakları genel izin çerçevesinde yürütürler."

Karşılaştırmalı hukuka baktığımızda; Amerika Birleşik Devletlerinde İSS olabilmek için özel bir izin veya ruhsat alınması söz konusu değildir. 1996 tarihli Telekomünikasyon Kanununa göre, kamu hizmeti niteliğinde haberleşme faaliyetinde bulunan diğer kuruluşlara uygulanan rejime dahil edilmemişlerdir ve bunlara uygulanan izin ve ruhsat sisteminden muaf tutulmuşlardır[155].

Belçika'da İnternet servis sağlama faaliyeti "Data Switching Service" olarak nitelendirilmekte ve sadece ilgili resmi makama yapılacak bir beyan ile faaliyete geçilebilmektedir[156].

İngiltere'de 1992 yılında çıkarılmış bulunan "Telecommunication Services Licence" ile sınıf lisansı kriterleri belirlenmiş ve İnternet servis sağlama hizmeti vermek isteyenler, sınıf lisansında tespit edilen şartları gerçekleştirmekle yükümlü tutulmuşlardır. İnternet servis sağlama hizmeti vermek isteyenlerden, bunun dışında herhangi bir ruhsat veya beyan istenmemiştir[157]. Fakat, AB mevzuatı uyum çerçevesinde, 2003 tarihli Telekomünikasyon Kanunu ile, İSS'lerin sadece bildirimde bulunmak suretiyle faaliyete başlayabilecekleri düzenlenmiştir[158].

Almanya'da İnternet servis sağlama hizmetlerinin Deutsche Bundespost Telekom tekeline girmediği kabul edilmekte ve dolayısıyla İnternet servis sağlama hizmetleri serbest bırakılmış ve İSS'ler hiçbir ruhsata veya izne tabi tutulmamışlardır[159].

Görüldüğü üzere bütün AB ülkelerinde İSS'ler bildirim usulüyle faaliyet göstermektedirler. Şu an taslak halinde olan Elektronik Haberleşme Kanunu'nun

---

[155] Sevi, 2004:192.
[156] Özdilek, 2002:102
[157] Akdeniz, Yaman. *The Regulation of Pomography and Child Pomography on the Internet*. Cyber-rights & Cyber - Liberties. 01 Ocak 2001:4. 19 EYLÜL 2004. http://www.cyber-rights.org/documents/us_article.pdf; Özdilek, 2002:102,
[158] 15 - 17 Eylül 2003 tarihli 2155 sayılı İngiltere İletişim Kanunu (Communication Act 2003), Bölüm 33, www.legislation.hmso.gov.uk/si/si2003/20031900.htm. 13 MAYIS 2004.; Sevi, 2004:192.
[159] Sieber, 1997:25.

yasalaşması durumunda ülkemizde de İSS'ler bildirim usulüyle faaliyete geçeceklerdir.

AB düzenlemesine göre ise, "European Committee for the Regulation of Telecommunications" tarafından kurulmuş bulunan "European Telecommunication Office" bünyesinde, Avrupa'da ruhsat ve lisans rejimini düzenlemek amacıyla 30 Haziran 1994 tarihinde yapılan sözleşme ile, bir üye devlet vatandaşlarının bir başka üye devlette İnternet servis sağlama faaliyeti göstermek istemesi halinde başvurularını sadece söz konusu European Telecommunication Office'e yapma hakkı kabul edilmiştir[160].

2.5.2.1. İnternet servis sağlayıcılarının sağladığı hizmet türlerine göre sorumluluğu

İSS'ler farklı ülkelerde, farklı yapılarda olmasına rağmen, genel olarak salt İnternet erişimi (mere conduit - AB Direktif'i tanımı) sağlamaktadırlar. Ancak İSS'lerin erişim hizmeti dışında, sunucu kiralama, alan adı sağlama, sunucu barındırma, uygulama servis sağlayıcılığı, içerik (bilgi) sunma gibi hizmetleri de bulunmaktadır[161].

İSS'lerin genel yükümlükleri şunlardır;

a. Resmi Makamlarca yapılan talep doğrultusunda hukuka aykırı yayını sunumdan kaldırmak,

b. Resmi Makamlarca yapılan talep doğrultusunda erişimi engelleme-hizmet talebini reddetmek,

c. Resmi Makamlarca yapılan talep doğrultusunda bilgi sağlamak,

d. Şikayetleri değerlendirmek,

e. Herhangi bir surette haberdar olduğu hukuka aykırılığı yetkili mercilere bildirmek,

[160] Özdilek, 2002:103.
[161] Akgün ve ark., s.1, www.teknoturk.org/docking/yazilar/tt000086-yazi.htm, (07.04.2005)

f. İrtibat noktası tesis etmek ve kolayca ulaşılabilirliği sağlama konularında, her halükarda yükümlü olmalıdır[162].

Genel yükümlülüklere değinildikten sonra, İSS'lerin verdikleri hizmet türlerine göre sorumluluklarını kısaca incelemek gerekmektedir.

2.5.2.1.1. Erişim hizmeti

İSS'lerin ilk ve temel hizmeti, kullanıcıların İnternet'e bağlantısını sağlayan erişim hizmetidir[163]. İSS'ler ana hizmetleri olan erişimi sağlama açısından dağıtıcılara (distribütörlere) benzemektedirler. Bu yönleri ile İSS'ler erişim hizmetinde bulunurlarken bir köprü görevi üstlenmektedirler[164].

İSS doğrudan İnternet bağlantısına sahip fakat başkalarına ait verileri depolayacağı sunucuları olmayan İnternet özneleridir. Bu durumda İSS'leri bir dağıtıcı olarak düşünmek mümkündür. Geleneksel telefon haberleşmesi sağlayan kuruluşlardan farkı bulunmamaktadır. Belli bir kaynaktan gelip doğrudan yayınlanacak bilgilerden dolayı İSS'lerin kontrol ve denetim imkanı yoktur. Bu nedenden dolayı İSS'lerin sorumluluğu söz konusu olamaz. Salt erişim sağlayan İSS'lerin içeriğe müdahale etme imkanları yoktur. Saniyede binlerce kullanıcının aynı anda sunduğu bilgilerin incelenmesi de teknik olarak imkansızdır.

Federal Almanya'da 13 Haziran 1997 tarihinde yürürlüğe giren Teleservisler Yasası'nın (Teledienstegesetz-TDG) 5'inci maddesinin 3'üncü paragrafında erişim sağlayıcıların cezai sorumluluğu altında bulunmadıkları açıkça ifade edilmiştir[165]. Alman Hukukunda yer alan bu düzenlemeye göre, erişim hizmeti veren İSS'ler fonksiyonları gereğince sadece başkalarına ait verilere ulaşılmasına aracılık etmektedirler. Bu sebeple erişim hizmeti veren İSS'lerin herhangi bir cezai sorumluluklarının olmaması hukukun gereğidir.

---

[162] Sevi, (2004: 194)'e göre Avrupa Birliği Elektronik Ticaret Direktifi'nin, 45, 46, 47, 48 numaralı paragraflarında, "İSS'lerin Sağlamakla Yükümlü Olduğu Bilgiler" başlığı altında benzer yükümlülükler öngörülmektedir.

[163] Erişim, çeşitli kaynaklardan gelen bilgileri doğrudan yayınlama ve kullanıcılara sunma hizmetidir.

[164] T.C. Başbakanlık, "Bilgi Toplumuna Doğru", Türkiye Bilişim Şurası Taslak Raporu, 2002:447; Akgün ve ark.,s.2; Sevi, 2004:194

[165] Başbakanlık, 2002:449.

Yukarıda da belirtildiği gibi, erişim hizmeti veren İSS'lerin bilgisayarlarından gigabyte'larla ifade edilen veriler, saniyelerin kesirleri gibi sayılarla ifade edilebilen bir zamanda iletilmektedir. Bu verilerin erişimin sağlandığı esnada denetlenmesi zaten teknik olarak imkansızdır. Teknik olarak imkansız olan bir durumdan dolayı insanlara cezai sorumluluk yüklemek hakkaniyete aykırı olacaktır. Gerek karşılaştırmalı hukukta gerekse uluslararası düzenlemelerde erişim hizmeti sağlayan İSS'lerin sorumluluklarının bulunmadığı görülmektedir.

Avrupa Birliği'nin Elektronik Ticaret Direktifi'nin 12'nci maddesinde, İSS'lerin bir takım koşulların yerine gelmesinde bir katkısı yoksa, iletilen bilginin içeriğinden sorumlu olmayacağı düzenlenmiştir.

Söz konusu maddeye göre;

a- İletişim İSS'nin kendisi tarafından başlatılmamışsa (yani İSS iletişimde kaynak taraf değilse),

b- İletişimde yer alan kişinin karşı tarafı seçme yetkisi yoksa (yani alıcıyı seçemiyorsa),

c- İletişime konu olan bilgiyi seçmiyorsa ve onu değiştirmiyorsa (yeniden üretmiyorsa),

İSS'ler iletilen bilginin içeriğinden sorumlu olmayacaktır. Direktif'te, bu maddenin bir mahkeme veya idari makamın, üye devletlerin hukuk sistemlerine uygun olarak hizmet sunucusunun ihlali sona erdirmesini veya önlemesini talep etme imkanını etkilemeyeceği özellikle belirtilmiştir[166].

Aynı Direktif'te, teknik olarak önemli bir ayrıntı olan kaşeleme (caching) de düzenlenerek, İSS'nin bilgi iletişimini sağlamaktan sorumlu tutulmadan, bilgiyi makul bir süre için otomatik olarak depolayabileceği belirtilmiştir. Yine Direktif'te, geçici olarak depolanan bilginin, yetkili otorite ya da mahkeme tarafından kaldırılmasına karar verildiğinde, İSS tarafından derhal kaldırılacağı ya da bu bilgiye erişiminin engelleneceği de hüküm altına alınmıştır[167].

[166] Akgün ve ark., s.3.
[167] Akgün ve ark., s.3.

2.5.2.1.2. Barındırma (hosting)

İSS'lerin sunuculara vermiş oldukları hizmetlerden faydalanan gerçek ve tüzel kişilerin hazırlamış oldukları içeriklerden, kural olarak İSS'ler hukuki veya cezai olarak sorumlu tutulmamaktadırlar. İçerikle ilgili hukuki ve cezai sorumluluk bilgiyi sunucuya yerleştiren gerçek ve tüzel kişilere ait olmalıdır. Ancak İSS'ler yetkili makamlarca usulüne uygun olarak bilgiyi sunucuya koyan gerçek ve tüzel kişilere ulaşılmasını sağlayacak bilgiler istendiğinde, bu bilgileri vermekle yükümlü olmalı ve bu bilgileri verememesi durumunda ise sorumluluk İSS'ye ait olmalıdır.

AB'nin 2000/31/EC nolu Elektronik Ticaret Direktifinin 14'üncü maddesine[168] göre de, üye devletler; sunucu, kanun dışı faaliyet veya bilgiden haberdar değilse ve tazminat taleplerine ilişkin olarak da, kanun dışı faaliyet veya bilginin açığa çıkabileceği maddi vakıa ve şartları bilmiyorsa ya da bu bilgiyi edindiği durumun farkına vardığı anda, bilgiyi kaldırır, erişimini engellemekte özenli davranırsa, barındırma dolayısıyla İSS'nin sorumlu tutulamayacağı düzenlenmiştir.

Almanya Teleservisler Yasası'nn 5'inci maddesine göre ise;

1- Hizmet sunan kişiler genel yasalar çerçevesinde kullanıma açtıkları kendi bilgilerinden sorumludurlar.

2- Hizmet sunan kişiler hizmete açtıkları şahıslara ait bilgilerden, bu bilgilerin içeriğinden haberdar olmaları ve teknik olarak bu bilgileri bloke edebilme kapasitelerinin var olduğu durumların dışında sorumlu değildirler.

---

[168] 14 üncü maddenin tam metni "1) Üye devletler, hizmetin alıcısı tarafından sağlanan bir bilginin saklanmasından oluşan bir bilgi toplumu hizmetinin sunulması halinde, üye devletler hizmet sunucunun hizmet alıcısı tarafından talep edilen bilginin saklanmasından dolayı sorumlu tutulmamasını, aşağıdaki şartların gerçekleşmesi halinde, temin ederler :
(a) sunucu, yasadışı faaliyet veya bilgi hakkında bilgi sahibi değilse, tazminat talepleri açısından, yasadışı faaliyet veya bilginin anlaşılabileceği maddi vakıa ve şartlardan haberi bulunmuyorsa; veya sunucu bu bilgiyi edinmesi veya durumun farkına varması üzerine, bilgiyi kaldırır veya erişimini engellemekte özenli biçimde hareket ederse,
2) 1. Paragraf, hizmet alıcısının sunucunun yetkisi ve kontrolü dahilinde hareket etmesi halinde uygulanmaz.
3) Bu madde, bir mahkeme veya idari makamın, üye devletlerin hukuk sistemlerine uygun olarak, hizmet sunucunun ihlali sona erdirmesini veya önlemesini talep etme imkanını etkilemediği gibi, üye devletlerin bilginin kaldırılması ya da erişiminin engellenmesini düzenleyen prosedürler öngörmesi imkanını da etkilemez.

Söz konusu maddeye göre İSS'ler ancak sunucularında depoladığı başkalarına ait suç içerikli verilerin bu özelliğinden haberdar olması ve ayrıca bu verilerin İnternet üzerinden erişilebilir kılınmasını teknik olarak önleme olanağına sahip olması durumunda sorumlu olacaktır[169].

2.5.2.1.3. Elektronik posta

Elektronik postalarda hukuki ve cezai sorumluluk, elektronik postayı hazırlayan ve gönderen gerçek veya tüzel kişilere aittir. Ancak İSS'ler yetkili makamları tarafından usulüne uygun olarak talep edilen elektronik postayı hazırlayan ve/veya gönderene ulaşılması konusunda gerekli yardımı yapmakla yükümlü tutulmalıdırlar[170].

2.5.2.1.4. Haber grupları ve sohbet odaları

Haber gruplarının kamuya açık olmasından dolayı, İSS'lerin sorumluluğunun daha farklı olması gerektiği yolunda görüşler ortaya çıkmıştır. ABD'de dava konusu olan bir olayda[171], İSS'nin bir haber grubunun yönetimini üstlenmiş olduğu, yayıncı gibi davrandığı ve bu nedenle içeriğin editörlüğünü üstlenmesi gerektiği belirtilerek İSS'nin sorumluluğuna hükmedilmiştir. Söz konusu karara göre, eğer İSS'nin kontrollü bir denetimi yoksa, sorumluluğunun da olmayacağına karar verilmesidir. Bu durum hukuka aykırı içeriği önlemek için mücadele eden İSS'lerin, bu konuyla hiç ilgilenmeyen İSS'ler karşısında cezalandırılması anlamına gelmektedir.

2.5.2.2. Türk mevzuatına göre İSS'lerin sorumluluğu

Mevcut mevzuatımıza göre İSS'lerin sorumluluklarını düzenleyen özel bir kanun bulunmamakla birlikte, FSEK'te esere ilişkin ihlaller için bir düzenleme yapılmış ve yukarıda da belirtmiş olduğumuz gibi Telekomünikasyon Hizmetleri Yönetmeliğinde bu duruma kısaca değinilmiştir. Halihazırdaki mevzuatımıza göre, FSEK'de düzenlenen ihlaller dışında, ne İSS'lerin sorumluluğunun sınırı ne de

[169] Sieber, 1997:26.
[170] Akgün ve ark., s.2; Sevi; 2004:202.
[171] New York Eyalet Mahkemesi, Prody Vakası, 1995, 07 Mayıs 2004, www.phillipsnizer.com/library/cases/lib_case80.cfm

yaptırımlar konusunda bir hüküm bulunmaması sebebiyle genel hükümler çerçevesinde bir sonuca ulaşmak gerekmektedir.

FSEK'teki EK-4'üncü maddenin 3 ve 4'üncü fıkralarındaki düzenlemede, bu kanuna göre hakkı ihlal edilen hak sahibi, ilk önce ihlale konu olan durumun düzeltilmesi için içerik sağlayıcıya başvur, 3 gün içerisinde ihlal düzeltilmezse Cumhuriyet Savcısı, yapılan başvuru üzerine servis sağlayıcıya durumun düzeltilmesi için başvurur ve içerik sağlayıcının hizmetinin durdurulması istenir, ihlal sona erdikten sonra içerik sağlayıcıya tekrardan hizmet sağlanır. Servis sağlayıcıları ile bilgi içerik sağlayıcılar Bakanlıkça[172] istendiği takdirde her türlü bilgi ve belgeyi Bakanlığa vermekle yükümlü tutulmuşlardır. Söz konusu düzenleme AB düzenlemesine paralel bir düzenlemedir.

[172] Kültür Bakanlığı.

3. ULUSLARARASI ALANDA VE KARŞILAŞTIRMALI HUKUKTA SİBER SUÇLAR

3.1. Siber Suçlarla Mücadele Amacıyla Uluslararası Alanda Yapılan Çalışmalar

3.1.1. Genel Olarak

Bilgisayar ağları yoluyla işlenen suçlar, yapısı itibariyle bütün toplumları etkilemektedir. Bu suç türünün belli bir mekana, yani fiziki bir coğrafyaya bağlı olmadan bilgisayar ağ sistemlerinin alt yapısının var olduğu Dünya'nın herhangi bir yerinden başka bir yerine doğru işlenebilmesinin mümkün olmasından dolayı, siber suçlara karşı etkili bir şekilde mücadele edebilmek için devletlerin ortak hareket etmesi gerekmektedir. Bu durumun gerçekleştirilebilmesi için de uluslararası platformda sıkı bir işbirliğine gidilmesi gerekmektedir.

Siber suçlarla etkin bir şekilde mücadele edebilmek için devletlerin ortak hareket etmeleri gerekmekte ise de, bu durum bazen klasik bir takım sebeplerden bazen de bu suçluluk çeşidinin özelliğinden dolayı gerçekleşememektedir. Devletlerin siber suçlar konusunda ortak hareket edememelerinin sebepleri;

- Siber suçlarla ilgili hangi tipte yapısal düzenlemenin yapılması gerektiği konusunda uzlaşma sağlanamaması,
- Suç oluşturan fiillerin hukuki tanımlamalarının yapılmasında bir bütünlük sağlanamaması,
- Genel anlamda koğuşturma makamlarının ve zabıta organlarının bu alandaki tecrübe eksikliği,
- Ulusal düzeydeki usul yasalarındaki koğuşturma hükümlerinin farklılığı sebebiyle siber suçların koğuşturulmasında uyumun sağlanamaması,
- Siber suçların bir çoğunun uluslararası karakter arz etmesi,

- Suçluların iadesi ve karşılıklı yardım anlaşmalarındaki eksiklikler nedeniyle uluslararası işbirliğine izin veren koğuşturma mekanizmalarının uyumlu bir şekilde çalıştırılamaması,
- Devletlerin, egemenlik haklarında uluslararası organizasyonlar lehine tavizde bulunmak istememeleri[173] olarak gösterilebilir.

Devletlerin siber suçlarla mücadelede ortak hareket edememeleri nedeniyle oluşan boşluğu doldurabilmek için uluslararası organizasyonlar bu konu hakkında çalışmalar yapmışlardır.

Uluslararası ve uluslar üstü organizasyonlar, siber tehdidin bütün Dünya için bir tehdit oluşturduğuna erken farkına varmışlar ve siber suçlarla mücadele için uluslararası işbirliğine gidilmesine ve bu alanda yüksek seviyede bir hukuk düzenlemesi yapılmasına katkı sağlamak için çalışmalar yapmışlardır. Bu konuda önemli çalışmalar yapan uluslararası organizasyonlar, Birleşmiş Milletler (United Nations – UN), G-8 (The Group of Eight), OECD (The Organization for Economic Co-Operation and Development), Avrupa Konseyi (The Council of Europe – CoU) dir. Bu kuruluşlar yapmış oldukları çalışmalarla siber tehdide karşı uluslararası bir bilincin oluşmasında önemli rol oynamışlardır.

Bu bölümde sırasıyla G8, OECD, BM ve Avrupa Konseyi bünyesinde yapılan çalışmalar incelenecektir.

3.1. 2. G-8 TOPLULUĞU

G-8 Dünya üzerinde en gelişmiş sanayiye sahip sekiz ülkenin (ABD, İngiltere, Fransa, Almanya, İtalya, Japonya, Kanada ve Rusya ayrıca Avrupa Birliği de organizasyon bünyesinde kurumsal olarak yer almaktadır) oluşturduğu bir birliktir. Bu ülkelerin başkanları her yıl düzenli olarak toplanmaktadır. Toplantıların içeriği genellikle teknolojinin gelişme yolu, suç ve terörizm gibi dünya gündemini teşkil eden önemli problemlerdir.

1995'ten itibaren, G-8 Topluluğu siber suçlarla ilgili çalışmalar yapmaya başlamıştır. Bu konuyla ilgili çeşitli çalışma grupları oluşturulmuş, liderler tarafından

[173] Beceni, Siber S, s.31,32.

bir çok bildiri yayımlanmış ve üye ülkelerin adalet bakanları tarafından eylem planları hazırlanmıştır.

1995 yılında Kanada'da düzenlenen zirvede, Organize Suçlar Kıdemli Uzmanlar Grubu (Senior Experts Group on Organized Crime) oluşturulmuştur. Bu grup Nisan ayında "Ülkeler Arası Organize Suçlarla Mücadelede Tavsiyeler" adı altında bir rapor yayınlamıştır. Raporda şu hususlar dile getirilmiştir. "Ülkeler iç hukuklarını modern teknoloji ihlallerini cezai müeyyide ile karşılayacak şekilde yeniden düzenlemelidirler. Problemli konuların da (yetki, adliye makamları, soruşturma, eğitim, uluslararası işbirliğinin sağlanması...vs.) etraflıca tanımlanması gereklidir. Ülkeler bu alanda yapılacak çalışmaları teşvik etmeli, teknolojik suçlar ve soruşturmalar ile ilgili problemleri, anlaşmalar ve sözleşmeler yolu ile çözüme kavuşturmalıdır."[174].

Yine Haziran 1997'de, G-8 Topluluğu bünyesinde "İleri Teknoloji Suçları Alt Komitesi" oluşturulmuştur. Bu komite "Uluslararası Bilgi Ağlarının Kötü Kullanımı" (Misuse of International Data Networks) adında bir rapor hazırlamıştır[175].

Aralık 1997 yılında yapılan toplantıda ise "İleri Teknoloji Suçları" tartışılmıştır. Buna göre; bilgisayar sistemlerine yapılan ihlallerin cezai müeyyide ile karşılanması konusunda üye devletlerin iç hukuklarının gözden geçirilmesi ve ileri teknoloji suçlarının araştırılmasının geliştirilmesine yardımcı olunması, karşılıklı yardım anlaşmalarının ve düzenlemelerinin yapılmasının özendirilmesi, yerleri tespit edilemeyen verilerin bilgisayar yolu ile araştırılması ve sınırlar ötesi araştırma ve yardım için yerine getirilmesi önerilen delillerin muhafazası hususlarında çözüm üretiminin teşvik edilmesi kararlaştırılmıştır.

Mayıs 2000 tarihinde Paris'de yapılan toplantıda siber suçlarla ilgili bir takım tavsiye kararları alınmıştır. Toplantının sonuç bildirgesinde; "Elektronik bileşenleri içeren suçun kovuşturulması, araştırılması ve engel olunması için siber suçların değişik sistemler arasında tespit edilmesi ve tanımlanması gerekmektedir.

[174] Beceni, Siber S, s.33.
[175] Beceni, Siber S, s.33.

Katılımcılar aşağıda belirtilecek hususların referansında herhangi bir çözümün getirilmesi konusunda mutabakata varmışlardır[176]:

- Gizlilik ve bireysel özgürlüğün korunmasının sağlanması,
- İleri teknoloji suçlarıyla mücadele için hükümetlerin amaçlarının korunması,
- Çalışmaları kolaylaştıracak uygun araçların içerilmesi,
- Siber suçluluğu gösteren şeffaf ve kesin tanımlamaların yapılması,
- Serbest ve adil aktivitelerin sağlanması, özel sektörün gönüllü olarak belirlediği davranış kuralları ve standartların etkinliğinin desteklenmesi,
- Etkinlik ve sonuçlara değer biçilmesi.

G-8 Topluluğu, siber suçların gelecekte en fazla işlenecek suçlar olacağının farkına varması ve özellikle bu suçlardan daha çok G-8 Topluluğu üyelerinin etkileneceğini düşünmesi nedeniyle siber suçlarla nasıl mücadele edilmesi gerektiği ve alınması gereken güvenlik tedbirleri konusunda önemli çalışmalar yapmaktadır.

3.1.3. Birleşmiş Milletler

Birleşmiş Milletler[177], milletlerarası barış ve güvenliği sağlamak; milletlerarası dostane ilişkileri geliştirmek; ekonomik, sosyal, kültürel veya insani mahiyetteki problemlerin çözümü ve insan hak ve hürriyetlerine saygının geliştirilip teşvik edilmesi konusunda milletlerarası işbirliğini sağlamak; bu müşterek amaçları geliştirecek hareketlerin uyumlu hale getirilmesinde bir merkez görevi görmek amacıyla oluşturulmuş bir birliktir.

[176] Beceni, Siber S, s.36.

[177] Müttefiklerin oluşturduğu 26 ülke hükümeti, Amerika Birleşik Devletleri Başkanı Roosvelt'in önderliğinde ilk kez l Ocak 1942'de Birleşmiş Milletler adını kullanarak bu teşkilatın kuruluş çekirdeğini oluşturmuşlardır. 25 Nisan- 26 Haziran 1945 tarihleri arasında San Fransisco' da toplanan Birleşmiş Milletler Uluslar arası Konferansı , Birleşmiş Milletler'in ilk oluşumunu hazırlanmıştır. 24 Ekim 1945 tarihinde teşkilatın kuruluşuna 51 ülke imza atmışken, günümüzde üye ülke sayısı 17l'e ulaşmıştır. (www.icep.org.tr/turkish/bm/index.asp - 26k) (20 Eylül 2005)

Birleşmiş Milletler bünyesinde 1985 yılında düzenlenen " 7. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin ardından hazırlanan Milan Eylem Planının 42'nci ve 44'üncü paragrafları arasında Bilgisayar Suçları ele alınmıştır[178].

"8. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin hazırlık çalışmaları sırasında düzenlenen "Asya Pasifik Bölgesel Katılımcılar Toplantısında" teknolojik gelişimin etkileri ve bilgisayar suçlarının giderek arttığı belirtilmiştir[179].

"8. Suçtan Korunma ve Suçluların Rehabilitasyonu" kongresinin 13. toplantısında üye ülkeler tarafından, içerisinde bilgisayar suçlarıyla ilgili çözüm önerilerinin de bulunduğu bir taslak kabul edilmiştir. Bu taslak ile bilgisayar suçlarıyla mücadele konusunda önemli çalışmalar yapılması kararlaştırılmış olup, bu çalışmalar sırasında bazı konuların dikkate alınması tavsiye edilmiştir. Bu konular:

- Zabıta ve yargı organlarına ve vatandaşlara bilgisayar suçlarından korunmanın öneminin anlatılması,
- Zabıta ve yargı organlarının bu suçlarla mücadele konusunda eğitilmesi,
- İlgili organizasyonlarla işbirliğine gidilerek bilgisayar kullanımı ile ilgili etik kurallarının tespit edilmesi ve bu kuralların bilişim eğitiminin bir parçası olarak öğretilmesinin sağlanmasıdır.

İtalya'da düzenlenen "Sınırlar Ötesi Organize Suçlarla Mücadelenin Önemine İşaret Edilmesi" sempozyumunda siber suçlar tartışılmıştır ve çözüm önerileri üretilmeye çalışılmıştır[180]. Bu sempozyum bünyesinde 14 Aralık 2000 tarihinde düzenlenen panelde üye ülkelerin aşağıda belirtilen eylemleri cezai müeyyide ile karşılamaları önerilmiştir. Bu eylemler[181];

- Bilgisayar sistemlerine yetkisiz giriş

---

[178] "International Review of Criminal Policy – United Nations Manual on the prevention and control of the computer- related crime" s.6 http://www.uncjin.org/Documents/irpc4344.pdf (14.07.2005)

[179] http://www.uncjin.org/Documents/irpc4344.pdf (14.07.2005), sf.6

[180] Bu Konferansla ilgili ayrıntılı bilgi edinmek için Bkz. http://www.odccp.org/palermo/ (14.07.2005)

[181] Bkz "Syposium On The Occasion of The United Nations Convention Againts Transnational Organized Crime , "Panel On The Challenge of Borderless Cyber-Crime" ,"Introductory Remarks and Concluding Remarks by The Moderator of the Panel" ,CORELL Hans, s.1, Under-Secretary-General for Legal Affairs The Legal Counsel of The United Nations , Palermo,İtalya,Palazzo dei Normanni , 14 Aralık 2000, http://www.odccp.org/palermo/convmain.html,; Beceni Yasin, Siber S., s.38.

- Bilgisayar veya bilgisayar sistemlerinin hukuka uygun olarak kullanılmasına engel olunması
- Bilgisayar sistemleri içerisindeki verilerin yok edilmesi veya değiştirilmesi
- Gayri fiziki ekonomik değer taşıyan objelerin çalınması
- Aldatma yoluyla değer elde edilmesi (elektronik sistemleri içeren).

B.M.'nin panelinde önerilen hususlar ceza kanunumuzda suç olarak düzenlenmiştir. Bu konu Türk hukukunda siber suçlar bölümünde ayrıntılı olarak incelenmektedir.

3.1.4. Ekonomik Kalkınma ve İşbirliği Örgütü (The Organization for Economic Co-Operation and Development)

Uluslararası bir ekonomi örgütü olan OECD, üye ülkelerin ekonomik ve sosyal gelişimine katkı sağlamak, üyeleri arasında işbirliğini kuvvetlendirmek, global ölçekli sorunlara çözüm üretmek üzere kurulmuş bir organizasyondur.

Bilgisayar suçları hakkında ceza hukuku problemlerine ilişkin uluslararası anlamda ilk ayrıntılı çalışma OECD tarafından başlatılmıştır. 1983 yılından 1985 yılına kadar OECD'nin geçici komitesi, bilgisayarlarla ilgili ekonomik suçlarla mücadele konusunda bir uluslararası uyumlaştırmanın mümkün olup olmadığı hususunda tartışmıştır[182]. Eylül 1985'de komite, üye devletlere bilgisayar yoluyla işlenen suçlarda, ulusal ceza kanunlarının göz önüne alınması tavsiyesinde bulunmuştur.

OECD'nin Geçici Komitesi ve ICCP komitesi (International Computer and Communications Policy Committee), üye devletleri siber suçlarla ilgili olarak ortak bir hukuk paydası altında birleştirmek maksadıyla, üye ülkelerin hukuklarının karşılaştırılmasına dayanılarak hazırlanan kurallar listesine göre üye ülkelerin kanunlarında aşağıda yer alan fiilleri suç olarak düzenlemelerini önermişlerdir. Bir başka ifadeyle aşağıda sayılan ihlallerin cezai müeyyide ile karşılanması konusunda fikir birliğine varılması gerektiği bildirilmiştir. Bu ihlaller;

[182] Sieber, 1998:157.

(1) Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ve/veya sermaye veya diğer değerli varlıkların yasa dışı transferi suçunu işlemek kastıyla bilgisayar programları yapılması, (Bilgisayar yoluyla dolandırıcılık);

(2) Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ve/veya sahtecilik suçu işleme kastıyla bilgisayar programları yapılması, (Bilgisayar yoluyla sahtecilik);

(3) Giriş, değiştirme, silme ve/veya bilgisayar verilerinin bastırılması ya da telekomünikasyon sistemi ve/veya bilgisayar fonksiyonlarının kasten engellenmesi maksadıyla, bilgisayar sistemlerine müdahale edilmesi, (Bilgisayar program ve verilerinde değişiklik yapılması);

(4) Korunmakta olan, münhasıran bir şahsa ait bilgisayar programını ticari olarak istismar etmek veya piyasaya sürmek maksadıyla, kişilerin bireysel haklarının ihlal edilmesi, (Bilgisayar programlarının telif haklarına aykırı olarak kopyalanması,çoğaltılması ve dağıtılması);

(5) Güvenlik önlemlerinin ihlali ya da diğer aldatıcı ve zararlı niyetlerle, sistem hakkında yetkili kişinin izni olmadan, bir bilgisayar ve/veya telekomünikasyon sistemine girmenin ve kullanımının engellenmesi; (Telekomünikasyon sistemlerinin, bilgisayarın diğer fonksiyonlarının ve iletişimin değişikliğe uğratılması)[183].

1989 yılında OECD, bilgi sistemleri hakkındaki çalışmalarına özel bir önem vererek devam etmiştir. 26 Kasım 1992'de, OECD Konseyi, Bilgi Sistemleri Güvenliği Tavsiye Yönergesini kabul etmiştir. Yönerge, kamu ve özel sektörü ilgilendirmekte olup, bilgi sistemleri için minimum standartların uygulanması konusuna odaklanmaktadır. Ancak, bilgi sistemlerinin güvenliği konusunda, karşılıklı yardımlaşma, uluslararası alanda suçluların iadesi konularında olduğu gibi, bilgi sistemlerinin yanlış kullanılmasını önlemek amacıyla da yeterli cezai, idari veya diğer müeyyideler talep edilmektedir[184].

[183] Sieber, 1998:158
[184] Sieber, 1998:159

3.1.5. Avrupa Konseyi

Avrupa Konseyinin oluşturulması fikri, II. Dünya savaşından maddi ve manevi büyük zararlar gören Avrupa'nın, benzer trajedileri bir daha yaşamasını önlemek maksadıyla ortaya atılmış ve Avrupa'da tarih boyunca yaşanan gerginliğin ve çatışmaların yerini güven ve işbirliğinin alması hedeflenmiştir.

Bu ortamda 5 Mayıs 1949'da 10 Avrupa ülkesi, Belçika, Danimarka, Fransa, Hollanda, İngiltere, İrlanda, İsveç, İtalya, Lüksemburg ve Norveç Avrupa Konseyini kuran anlaşmayı imzalamışlardır.

Türkiye 13 Nisan 1950 tarihinde Avrupa Konseyi'ne üye olmuştur. Kuruluşun bugün 41 üyesi vardır.

Avrupa Konseyi savunma konuları dışında toplumları ilgilendiren tüm sorunlara çözüm üretmeye çalışan bir topluluktur. Bu sorunlara örnek olarak, sosyal güvenlik, hukuki işbirliği, insan hakları, yerel yönetimler, bölgesel planlama, medya, eğitim, kültür, spor, gençlik, sağlık, çevre, aile konuları verilebilir. Konseyin bu alanlardaki çalışmaları genellikle sözleşme ya da protokoller hazırlanması ile sonuçlanmaktadır. Sözleşme ve protokoller üye ülke mevzuatlarının uyumlaştırılması, bu suretle ortak normlar ve bir Avrupa Hukuk Düzeni oluşturulması amacına yöneliktir.

Avrupa Konseyi siber suçlar konusunda ilk çalışmalarını 80'li yılların sonlarına doğru gerçekleştirmiştir. Konsey, siber suçlarla ilgili çalışma yapmak üzere bir Uzmanlar Komitesi oluşturmuştur. Konseyin siber suçlarla ilgili olarak böyle bir çalışma başlatmasının hedefi bu suçlarla ilgili olarak ceza kanunlarında hangi fiillerin suç olarak kabul edilip cezalandırılması gerektiğini açık bir şekilde tespit etmek, sivil özgürlük ve güvenlik kavramları arasındaki uyuşmazlığın nasıl aşılacağı konusunda üye ülkelere yol göstermektir.

Uzmanlar Komitesi OECD'nin 1986 yılında yayınladığı raporunu[185] referans alarak burada belirlenen ihlallerin, üye ülkeler nezdinde cezai müeyyide altına alınmasını benimsemiş ve ayrıca bir takım prensiplere ve OECD'nin raporunda belirtilmeyen ihlallere de dikkatleri çekmiştir. Komite çalışmalarının sonucunda

[185] Bkz. s. 80-81.

OECD'nin raporunda belirlenen ihlallere ek olarak bilgisayarla bağlantılı suçlarla ilgili korunma, engellenme, mağdurlar, usulü bir takım kurallar örneğin uluslararası araştırmalar, veri bankalarına el konulması ve bilgisayar suçlarının soruşturulması ve kovuşturulmasında uluslararası işbirliğine gidilmesi hususlarının eklendiği bir taslak halinde sunulmuştur. Söz konusu taslak üye ülkelere yol gösterici niteliktedir. Daha sonra Avrupa Konseyi Bakanlar Komitesi tarafından 13 Eylül 1989 tarihinde yürürlüğe girmiştir.

Avrupa Konseyinin siber suçlarla ilgili son ve en önemli çalışması "Siber Suç Sözleşmesi" (Convention on Cyber Crime) dir. Avrupa Konseyi tarafından dört yılda hazırlanan Siber Suç Sözleşmesi hükümlerine yönelik çalışmalar, 1996 yılında Suç Sorunları Avrupa Komitesi'nin CDPC/103/211196 tarihli kararı ile siber suçla ilgili uzmanlardan oluşan bir komite kurulması sonucunda başlamıştır. 1997 yılında Avrupa Konseyi Bakanlar Komitesinin, uzmanlardan siber suç kapsamına giren konulara ilişkin bağlayıcı özelliğe sahip olacak hukuki bir metin hazırlanmasını talep etmesi ile sözleşme gündeme gelmiştir. Nisan 2000'de taslak metin İnternet'ten yayınlanmış, son halini ise Haziran 2001'de almıştır[186].

Avrupa Konseyi tarafından hazırlanan bu sözleşmenin amacı ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi ve uluslararası işbirliğinin geliştirilmesidir.

Sözleşme dördüncü bölümde detaylı bir şekilde incelenecektir.

3.2. Karşılaştırmalı Hukukta İnternet Suçları

3.2.1. Genel Olarak

Karşılaştırmalı hukukta siber suçlarla ilgili düzenlemeler farklı sistematikler kullanılarak meydana getirilmiştir. Günümüzde ülkeler, bu konuda ya ceza hukuku ile ilgili mevcut kanunlardan ayrı olarak özel düzenlemeler ihdas etmekte, ya da mevcut hükümlerde değişiklikler yaparak mevzuatlarını geliştirmektedirler. Siber suçları özel düzenlemeye tabi tutan ülkeler ceza kanunlarında iki farklı yöntem izlemişlerdir. Birinci yöntem, siber suçları ceza kanunundan ayrı bir kanun çıkarmak

[186] Helvecıoğlu, 2004:278.

suretiyle düzenleme altına alan yöntemdir. Özellikle Anglo-Sakson hukukuna tabi olan İngiltere, İrlanda ve ABD'de bu yöntem izlenmiştir[187]. İkinci yöntem ise Kara Avrupası ülkelerinde uygulanan yöntemdir ki, bu yöntemde siber suçlar ceza kanunları içerisinde ayrı bir fasılda düzenlenmektedirler. Bu yöntemi uygulayan ülkelere örnek olarak Fransa, Lüksemburg verilebilir[188]. Ülkemiz de bu yöntemi kendi mevzuatında tatbik etmiştir.

Siber suçları ceza kanunlarında dağınık olarak düzenleyen, sisteme öncülük eden ülke Almanya'dır. Bu sisteme göre, suç teşkil eden eylemler mevcut kanunlara göre incelenmektedir. Yani bu sistemde kanun koyucular ayrı fasıllar veya kanunlar oluşturmamakta, halihazırdaki hükümleri siber suçları da göz önüne alarak yeniden düzenlemektedirler. Örneğin, Alman Ceza Kanununun 303a maddesi bilgisayarlara girilmek suretiyle, mevcut programların bozulması tahrip edilmesi ve değiştirilmesi suçunu düzenlemektedir. Suçun ihdası ile korunan hukuki yarar eşya üzerindeki mülkiyet hakkı olduğundan suç temelde nas-ı ızrar suçudur. Bu sebeple, mal aleyhine işlenen suçları düzenleyen fasıl içinde yer almaktadır[189]. Bu sistemi benimseyen ülkelere örnek olarak İsveç, İtalya, Japonya gösterilebilir.

Sonuç olarak Anglosakson Hukuk Sistemini uygulayan ülkelerde siber suçlarla ilgili olarak Ceza Kanunlarının dışında özel düzenlemelere başvurulmaktadır. Kıta Avrupası Sistemi'ni uygulayan ülkelerin büyük kısmında da ceza kanunlarında yapılan değişikliklerle, siber suçlar alanında düzenlemeler yapılmaktadır.

3.2.2. Amerika Birleşik Devletleri

İnternet teknolojisinin icat edildiği yer olan Amerika Birleşik Devletleri'nde son on yıl içerisinde bilgisayar ve İnternet'in Amerikan yaşamının her alanında yerini almasıyla birlikte, suç işleyenlerin de bu durumu gözden kaçırmayarak, faaliyetlerini bu alana kaydırmaya başlamaları sonucunda siber suçlarla ilk defa karşılaşan ülke olmuştur.

---

[187] Yazıcıoğlu, 1997:170.
[188] Yazıcıoğlu, 1997:170.
[189] Değirmenci, 2002:119.

Anılan ülkede bilgisayar ağlarının ülke kalkınmasında önemli bir role sahip olması nedeniyle, bilişim sistemlerinin kullanılmasında güvenliği sağlamak, bu ülke için bir mecburiyet teşkil etmiştir. Ayrıca işlenen siber suçlar sebebiyle ABD'deki şirketler ekonomik olarak da büyük gelir kaybetmektedirler. Bilgisayar ağları yoluyla yapılan dolandırıcılık yüzünden ülkenin uğramış olduğu zarar tam olarak tespit edilemese de, Sertifikalı Dolandırıcılık Araştırma Uzmanlar Birliği (The Association of Certified Fraud Examiners) ABD şirketlerinin bu nedenle toplam yıllık kaybının en az 40 milyar Dolar olduğunu belirtmektedir[190]. Bu sebeplerden ötürü ABD, bilgisayar ağlarının suç aracı olarak kullanılması ve bu suçların düzenlenmesi konusunda da ilk çalışmaları yapan ülke olmuştur.

ABD'de siber suçlarla ilgili ilk düzenlemeler eyalet düzeyinde başlamıştır. 1984 yılında siber suçlarla ilgili ilk federal yasa olan "Computer Fraud and Abuse Act" yürürlüğe girdiğinde 47 eyalette siber suçlarla ilgili düzenlemeler bulunmaktaydı[191].

ABD'de çeşitli siber suç şekillerini düzenleyen birçok federal yasa kabul edilmiştir. Bunların en önemlileri aşağıda incelenmektedir.

3.2.2.1. Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası (Computer Fraud and Abuse Act)[192]

1984 yılında kabul edilen bu yasa, ABD'de artan siber eylemleri engellemek, en azından artmasını önlemek amacıyla düzenlenmiştir. Başlangıçta söz konusu yasanın kısa ve dar ölçekli olması amaçlanmıştır. Ancak bilgisayar güvenliğini tehdit eden eylemlerin her geçen gün artması ve yasanın yetersiz kalması nedeniyle 1988, 1989, 1990 ve 1994 yıllarında çeşitli değişiklikler yapılmış ve yasanın kapsamı genişletilmiştir. Bu yasa ile Federal Temel Yasa'nın 18'inci Bölümünün 1030'uncu maddesi değiştirilmiştir[193]. Yasa temel olarak, korumalı bir bilgisayara yetkisiz ve izinsiz erişimi yasaklamaktadır. Yasa ile kamuya ve özel sektöre ait tüm

[190] Şehitoğlu, 2004:258.
[191] Yazıcıoğlu, 1997:187; Değirmenci, 2002:133.
[192] Yasanın orjinal metnine www.panix.com/~eck/computer-fraud-act.html (20.12.2004) adresinden ulaşabilirsiniz.
[193] Çeken, 2002:3.

bilgisayarların yanında, kişisel bilgisayarlar da bu korumadan tam olarak istifade edebilmektedir. Yasa ile suç haline sokulan hareketler şunlardır[194]:

- ABD hükümetine zarar vermek veya herhangi bir yabancı ülkeye yarar sağlamak maksadıyla, tasnif edilmiş ve gizlilik dereceli savunma ve dış işleri konularına ilişkin enformasyona izinsiz olarak erişmek,
- Finansal bir kurum veya tüketici araştırma ajanslarından herhangi birinin bilgisayarlarındaki finansal kayıtlara izinsiz ve yetkisiz olarak erişmek,
- Kamu kuruluşlarından herhangi birinin kullandığı bir bilgisayara girerek, bu kuruluşların verdiği hizmeti aksatacak şekilde, burada bulunan bilgileri değiştirmek, bozmak veya ifşa etmek,
- Herhangi bir bilgisayara sahtekarlık veya hırsızlık yapmak maksadıyla izinsiz ve yetkisiz olarak girmek,
- Herhangi bir şekilde kasten veya ihmalen, korumalı bir bilgisayara erişmek, bu tip bir bilgisayara data veya program göndermek,
- Bilgisayar şifrelerini veya bilgisayarlara erişmekte kullanılabilecek herhangi bir bilgiyi dağıtmak, başkalarının kullanımına sunmak,
- Para veya para hükmünde olan herhangi bir değeri elde etmek maksadıyla, bir bilgisayar veya bilgisayar sistemine zarar verme yönünde tehditler savurmak.

Bu hareketlerden herhangi birinin suç olarak nitelendirilebilmesi için sanığın diğer bir bilgisayara yetkisiz veya mevcut yetkisini aşarak erişmiş olduğunun kanıtlanabilmesi gerekmektedir.

[194] Damon, W.D. Wright. "Cybercrimes". Venable LLP. 01 OCAK 2003. 18 MAYIS 2005. http://www.venable.com/docs/resources/ebookcybercrimes.cfm

3.2.2.2. Anti-Terörizm Yasası (USA_Patriot - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)[195]

11 Eylül 2001 tarihinde ABD'de bulunan Dünya Ticaret Merkezi'ne ait kulelere yapılan terörist saldırılardan sonra, Amerikan Kongresi tarafından 26 Ekim 2001 tarihinde yeni bir anti-terör yasası kabul edilmiştir. Yasa, İSS'lere eskiye nazaran, abonelerinin üye bilgilerini soruşturma makamlarına verme konusunda daha ağır yükümlülükler getirmekte, ulusal güvenliğin gerektirdiği hallerde, hakim kararı olmaksızın haberleşmenin denetlenebileceğini ve ulusal istihbarat örgütleri ile ulusal olmayan istihbarat örgütleri arasında bu yollardan elde edilen bilgilerin paylaşılabileceğini hükme bağlamaktadır[196].

Söz konusu yasa ile 1984'den beri yürürlükte olan Computer Fraud and Abuse Act'ın siber suç yaklaşımı genişletilmiştir. 1994 ve 1996 yıllarında yapılan değişikliklere kadar, ABD makamlarının uluslararası boyutlu bir siber suçu izleyebilmeleri ve kovuşturma yapabilmeleri için yasayla "korunmalı bilgisayar" olarak ifade edilen ve ABD sınırları içerisinde bulunan bir bilgisayar ya da şebekeye saldırıda bulunulması ve bu saldırının bir zarara sebebiyet vermesi gerekmekteyken, anılan yasa ile bu tanım genişletilerek saldırının ABD'de bulunan şebeke (network) sistemlerinden geçmesi yeterli sayılmıştır. Bunu bir örnekle somutlaştırmak gerekirse; İstanbul'da yaşayan bir bilgisayar korsanı, Trabzon'da bulunan bir bilgisayarı ya da sistemi çökerttiğinde ya da herhangi şüpheli bir eylemde bulunduğunda eğer bu eylem ABD'de bulunan şebekelerin biri üzerinden veri (data) paketi olarak geçmişse, Amerikan Federal Soruşturma Bürosu işe müdahil olabilmektedir. Bunun nedeni olarak savunulan görüş ise, Dünya İnternet trafiğinin %70'inin ABD şebekeleri üzerinden geçmesi olarak açıklanmaktadır[197].

---

[195]Yasanın orjinal metnine http://www.cybercrime.gov/PatriotAct.htm (17.01.2005) adresinden ulaşabilirsiniz.
[196] Çeken, 2002:11.
[197] "Avrupa Konseyi ve Siber Uzay Suçları". *Bilişim Kültürü Dergisi*. 01 EYLÜL 2001:14. 11. EYLÜL 2004. http://tbd.org.tr/sayi79_html/hukuk_kesmez.html

Yasanın siber suçlara ilişkin en önemli bölümü, Federal Temel Yasa'nın, daha önceden içeriği "Bilgisayar Sahtekarlığı ve Bilgisayarların Kötüye Kullanılması Yasası" ile belirlenen 1028[198] nci maddesinde yaptığı önemli değişikliklerdir[199].

Yeni yasa ile yapılan değişiklikler;

- 1028'inci maddede önceden belirlenen ceza miktarlarının arttırılması,
- ABD sınırları dışında bulunan bilgisayarlar kullanılarak gerçekleştirilen ve ABD ticaretini zarara uğratan faaliyetlerin de, 1028'inci madde kapsamına alınması,
- 1028'inci maddede sayılan fiillere teşebbüs edenlerin dahi, bu fiilleri tamamlamış gibi cezalandırılacaklarının belirtilmesi,
- Daha önceden, herhangi bir eyalet mahkemesi tarafından haklarında bilgisayarlar aracılığıyla işledikleri bu tür suçlardan biriyle mahkumiyet kararı verilenlerin, bu mahkumiyetlerinin, bu kişilerin daha sonradan, federal düzeyde işleyecekleri suçlarda tekerrüre esas sayılacağının ve bu durumda olanların cezalarının arttırılacağının hükme bağlanmasıdır.

Söz konusu yasada ayrıca siber terörizm suçu kategorisi yaratılmakta ve bu suç faillerinin fiilleri başkasının ölümüne sebep olmuşsa ömür boyu, olmamışsa 15 yıla kadar hapsedilmeleri hükme bağlanmıştır.

Yasa ile getirilen siber terörizm suçları:

- Milli güvenlik, milli savunma veya 1954 tarihli Atom Enerjisi Yasasının gereklerine göre erişilmesi yasak olan bilgisayarlara erişerek, buradaki bilgileri yetkili olmayan bir kimseye vermek veya Amerikan çıkarlarına aykırı olduğunu bile bile bir başka ülkenin kullanımına sunmak,

[198] Federal Temel Yasa'nın 18 nci Bölümünün 1028 nci Maddesi, (18 U.S.C. § 1028), bilgisayarlar da dahil olmak üzere, kimlik bilgilerinde oynamalar yapmak amacıyla kullanılabilecek herhangi bir cihazın üretilmesini, böyle bir cihaza sahip olunmasını veya nakledilmesini yasaklamaktadır.
[199] Çeken, 2002:11.

- Federal Temel Yasa'nın 1028'inci maddesinde belirtilen fiilleri gerçekleştirerek toplumun veya bireylerin sağlığına zarar vermek veya bunların sağlığını tehdit eden sonuçların ortaya çıkmasına neden olmak,
- Federal Temel Yasanın 1028'inci maddesinde belirtilen fiilleri gerçekleştirerek, bir federal yönetim organının veya adalet, mili savunma veya milli güvenlik idarelerinin bilgisayarlarına zarar vermek veya bunların zarara uğraması tehlikesine yol açmak[200].

Bu yasanın en çok eleştirilen yönü, bugüne kadar 11 Eylül saldırılarında herhangi bir siber katkının varlığı ispat edilmemişken, özellikle ABD vatandaşlarının temel hak ve özgürlüklerine getirdiği kısıtlamalar ve uluslararası hukuku ilgilendiren iletişimin izlenmesi, ele geçirilmesi ve siber suçların kovuşturulmasıyla ilgili hükümlerinin içerdiği boyutu olmaktadır.

Ancak bu Yasa ile getirilen kısıtlamalar 31 Aralık 2005 tarihine kadar geçerli olacakken ve bu tarihten sonra yasa gereği getirilen kısıtlamalar kendiliğinden ortadan kalkacakken, ABD Kongresi bu yasayı belirli periodlarla uzatmaktadır.

3.2.2.3.İletişim Ahlakı Yasası[201] (Communications Decency Act-CDA)

Bu yasa, İnternet kaynaklı sorunların çözümlenmesi amacıyla düzenlenen yasalardan birisi olup, getirmiş olduğu hükümler bakımından tarihi bir kilometre taşı olarak kabul edilmektedir[202].

Yasanın temel amacı, İnternet'te interaktif olarak yapılan pornografik içerikli yayınlardan çocukların korunmasıdır. Söz konusu yasaya göre İnternet üzerinden müstehcen içeriğe sahip resim, yazı, video, klip...vb., materyallerin yayınlanması ve iletilmesi ile şiddet içeren yayınların gerçekleştirilmesi suç olarak düzenlenmiştir. Bunun yanı sıra yasanın uygulanabilmesi için yetkili mercilere, İnternet

[200] Çeken, 2002:11; Değirmenci, 2002:128.
[201] Yasanın tam metni için bak. www.epic.org/free_speech/CDA/cda.html, (17.01.2005)
[202] Akdeniz, Yaman. *The Regulation of Pomography and Child Pomography on the Internet*. Cyber-rights & Cyber - Liberties. 01 Ocak 2001:4. 19 EYLÜL 2004. http://www.cyber-rights.org/documents/us_article.pdf

kullanıcılarının e-posta mesajlarının okunabilmesi ve haber gruplarındaki tartışmalar ile IRC üzerinden yapılan sohbetlerin izlenebilmesi olanağı sağlanmıştır[203].

Bu yasa ile yürürlüğe giren antidemokratik hükümlere karşı kamuoyunda büyük bir tepki meydana gelmiş ve sivil toplum örgütleri American Civil Liberties Union (ACLU- Amerikan Sivil Özgürlükler Birliği) önderliğinde anılan yasaya karşı muhalefet hareketine başlamışlar ve İletişim Ahlakı Yasası ile getirilen bazı hükümlerin Anayasanın 1'inci ekinde teminat altına alınan ifade özgürlüğünü ihlal eder nitelikte olduğu ve yasada yer alan "müstehcen yayın", "ahlaksız" gibi ifadelerin oldukça soyut ve geniş kavramlar olduğu ve bu durum ile ceza normunun belirliliğine ters düştüğü iddia edilerek, ACLU & Reno davası olarak literatüre geçen davayı açmışlardır[204]. Ayrıca bu gruplar yetişkinlerin kendi çocukları için neyin doğru neyin yanlış olduğuna kendilerinin karar verme yetkilerinin de ellerinden alındığını iddia etmişlerdir[205].

Söz konusu girişimlerin sonucunda Amerikan Federal Yüksek Mahkemesi İletişim Ahlakı Yasası ile getirilen hükümlerin Anayasa'nın 1'inci Eki'ne aykırı oldukları gerekçesiyle iptal edilmelerine karar vermiştir.

Federal Yüksek Mahkeme kararın gerekçesinde, "*Bir kitle iletişim aracı olarak İnternet'in hükümetlerin müdahalesine karşı korunması gerekmektedir. İnternet üzerindeki yayınlarla ilgili bir düzenlemenin bulunmaması kuşkusuz bir kaos yaratmıştır ancak unutmamak gerekir ki, İnternet'in gücü de bu kaostan kaynaklandığı gibi Anayasa'da belirlenen düşünceyi açıklama özgürlüğü de aynı kaosa dayanmaktadır*", ifadeleri kullanılmış ve ayrıca "Demokratik toplumda özgür fikir alışverişinin sağlayacağı toplumsal yarar, İntenet'te sansürün sağlayabileceği toplumsal yararla karşılaştırılamayacak kadar önemlidir." denmiştir[206].

---

[203] Sınar, 2001:93; Caden, Marc L.-LUCAS Stephanie E., Accidents On The İnformation Super Highway, *The Richmond Journal of Law and Technology*. 13 ŞUBAT 1996. 27 NİSAN 2005. www.law.richmond.edu/jolt/v2i1/caden_lucas.html

[204] Sınar, 2001:94

[205] Çeken, 2002:6; Akdeniz, Yaman. *Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach.* Cyber-rights & Cyber – Liberties. 01 OCAK 2000. 10 ARALIK 2004. http://www.cyber-rights.org/reports/governan.htm

[206] İçel, 2000:412; Sınar, 2001:94

Sonuç olarak, İletişim Ahlakı Yasası'nın gün ışığındaki yolculuğu Federal Yüksek Mahkeme'nin iptal kararıyla sona ermiştir. Bu yasa kanun koyuculara İnternet'le ilgili hukuki düzenlemelerin nasıl yapılmayacağına dair iyi bir örnek teşkil etmektedir.

3.2.2.4. Çocuk Pornografisinin Önlenmesi Yasası[207] (Child Pornography Prevention Act – CPPA)

Çocuk pornografisi, çocuğun gerçekte veya taklit suretiyle bariz cinsel faaliyetlerde bulunur şekilde herhangi bir yolla teşhir edilmesi veya çocuğun cinsel uzuvlarının, ağırlıklı olarak cinsel amaç güden bir şekilde gösterilmesidir[208]. 1996 yılında Amerikan Kongresi tarafından çocukların bu amaçla sömürülmesinin önüne geçmek amacıyla söz konusu yasa çıkarılmıştır.

Anılan yasa ile çocukların görüntülendiği pornografik yayın ve materyallerin elde bulundurulması veya İnternet'te yayınlanması ve bilgisayarlar veya e-posta yoluyla çocuk görüntülerinin bulunduğu cinsel materyallerin ticaret aracı olarak kullanılması yasaklanmıştır. Ayrıca suç teşkil eden çocuk görüntülerinden üç veya daha fazla adedini bizzat bilgisayarında bilerek muhafaza edenler cezalandırılmaktadır.

Yasada 1996 yılında yapılan bir değişiklikle, bilgisayarlar yoluyla oluşturulan çocuk görüntüleri de suç sayılmıştır. Bunun sebebi, gerçek görüntüler ile birtakım resim ve grafik programlarıyla oluşturulan görüntülerin birbirinden ayırt edilmesinin zorluğu gösterilmiştir[209].

3.2.2.5. Çocukların Online Yayınlardan Korunması Yasası[210] (Child Online Prevention Act - COPA)

Bu yasa çocukları pornografik ve müstehcen yayınlardan korumak amacıyla 1998 yılında çıkarılmıştır. Yasa ile normalde büyüklerin erişmesine izin verilen site ve materyallere küçüklerin erişmesinin kolaylaştırılması cezalandırılmaktadır[211].

---

[207] Yasanın tam metni için bkz.www.ojp.usdoj.gov, (17.01.2005)
[208] Tanım, Avrupa Konseyi Siber Suç Sözleşmesinden alınmıştır.
[209] Çeken, 2002:3-4.
[210] Yasanın tam metni için bkz. www.politechbot.com/docs/cppa.text.html, (17.01.2005)
[211] Çeken; 2002:3-4.

Amerikan Federal Mahkemesi 22 Haziran 2000 tarihinde Reno & ACLU II davasında verdiği kararda bu yasanın Anayasaya aykırı olduğuna karar vermiştir[212].

3.2.2.6. Elektronik Haberleşmenin Gizliliği Yasası (Electronic Communications Privacy Act- ECPA)

Bu yasa ile, radyo haberleşmesi, elektronik posta, özel haberleşme kanalları ve bilgisayar haberleşmesine ilişkin özgürlük ve gizlilik sınırları genişletilmiştir. Yasa ile, resmi makamlar tarafından olduğu kadar, resmi olmayan makamlarca da yapılmakta olan kanunsuz dinleme faaliyetlerinin önüne geçilmek istenmektedir[213].

3.2.2.7. İnternet'te Kumarın Önlenmesi Yasası[214] (Internet Gambling Prohibition Act)

Bu yasa ile ABD sınırları içerisinde (kumar oynamanın yasal sayıldığı Las Vegas ve Atlantic City gibi belirli yerler dışında), yasaklanmış bulunan çeşitli şans ve kumar oyunlarının İnternet siteleri aracılığıyla herkes için erişilebilir kılınması üzerine yasa koyucu bir düzenleme yapma ihtiyacı duymuş ve bu şekilde kumar oynatanların 2 yıla kadar hapis cezası ve 10.000 dolara kadar para cezası ile cezalandırılabilecekleri bir yasa çıkarılmıştır[215].

ABD'de yukarıda belirttiğimiz federal nitelikli düzenlemelerin yanında federe devletlerde de, bilgisayar ağları kaynaklı hukuki sorunlara çözüm bulunabilmesi amacıyla çeşitli yasal düzenlemelere gidildiğini belirleyebilmek mümkündür[216].

3.2.3. Almanya

Yukarıda da belirtmiş olduğumuz gibi Almanya'da siber suçlar için ayrı fasıllar veya kanunlar yapılmamakta, fiiller halihazırda kabul edilen suçlar bazında değerlendirilmektedir. Konuyu bir örnekle somutlaştırmak gerekirse, bilişim

---

[212] Sınar; 2001:95, dipnot 244.
[213] Çeken, 2002:8.
[214] Yasanın tam metni içinbkz. http://fto.loc.gov/pub/thomas/c105/s474.is.txt, (17.01.2005)
[215] Sınar; 2001:96.
[216] Damon, W.D. Wright. "Cybercrimes". Venable LLP. 01 OCAK 2003. 18 MAYIS 2005. http://www.venable.com/docs/resources/ebookcybercrimes.cfm

sistemlerine karşı nas-ı ızrar fiilini suç olarak düzenleyen Alman Ceza Kanununun 303a maddesi; nas-ı ızrar suçunu düzenleyen fasılda yer almaktadır[217].

Alman Ceza Kanununun 202a maddesinde verilerin depolandığı ve işlendiği bilgisayar ağlarına izinsiz olarak girilmesi ve verilerin ele geçirilmesi suç olarak düzenlenmiştir. Anılan suç, bilgisayar sistemlerinde saklanan verilere yönelik olması hasebiyle "sır aleyhine işlenen suçlar" arasında yer almaktadır. Alman Ceza Kanunu bilgisayar sistemlerine izinsiz girilmesini tek başına suç olarak kabul etmemekte, bunun yanında söz konusu suçun meydana gelebilmesi için verilerin de ele geçirilmesini aramaktadır. Kısaca fiil, kendisi veya üçüncü bir kişi lehine, kendisine ait olmayan ve sisteme girmesine izin verilmeyen, emniyete alınmış verilerin ele geçirilmesi halinde suç olarak sayılmaktadır[218].

Yine Alman Ceza Kanununun 263a maddesinde bilişim sistemlerinin kullanılmasıyla işlenen dolandırıcılık suçu hüküm altına alınmıştır. Bu maddeye göre dolandırıcılık suçunun oluşabilmesi için suçu işleyenin kendisi veya üçüncü bir şahıs için hukuka aykırı bir şekilde ekonomik fayda sağlamak amacıyla hareket etmesi gerekmektedir. Kısacası suçun oluşabilmesi için kanun özel kast aramaktadır. Söz konusu maddede dolandırıcılığa sebep olacak fiiller sayılmasına rağmen, bu fiiller tahdidi değildir. Yani sayılan fiiller dışındaki bir fiil ile de dolandırıcılık suçu işlendiğinde cezai müeyyide uygulanacaktır. Bu fiiller; yanlış programlarla, yanlış veya tamamlanmamış verileri kullanarak, verileri yetkili olmadan veya başka suretlerle bilgi işleme yetkisi olmadan müdahale ederek işlenmesidir. Madde metninde, suçun oluşması için verilerin meydana çıkmasını etkilemek suretiyle bir şahsın ekonomik zarara uğramasına sebep olmak da ayrıca ifade edilmiştir[219].

Bilişim sistemleri vasıtasıyla meydana gelen sahtekarlık fiilleri Alman Ceza Kanununun 269 ve 279'uncu maddelerinde düzenlenmiştir. Anılan maddelerde, sahtekarlık suçunun oluşması için, hukukça hükmü haiz bir belgenin bilişim sistemleri aracılığıyla sahte olarak düzenlenmesi veya üzerinde tahrifat yapılması ve bu belgelerin kullanılması yeterli görülmüştür.

---

[217] Değirmenci, 2002:143.
[218] Önder, 1994:505.
[219] Değirmenci, 2002:143

3.2.4. Fransa

İnternet'in ortaya çıkardığı hukuki sorunlarla ilgili olarak Fransa'daki mevzuat incelendiğinde İnternet'le ilgili olarak ceza hukuku alanında özel bir yasa olmadığı görülmektedir. Fransız yasa koyucular İnternet'le ilgili özel bir kanun hazırlamak yerine Fransız ceza mevzuatında İnternet'i de kapsamına alabilecek genel ifadelere yer vermişlerdir. Örneğin, 1994 tarihli Fransız Ceza Yasası ile küçüklere yönelik olmadığı sürece pornografinin suç teşkil etmeyeceği savunulmakla birlikte yasanın 227-24'üncü maddesi pornografik ve şiddet içerikli yayınların hangi araç ile olursa olsun küçükler tarafından erişilebilir kılınmasını suç olarak düzenlemiştir[220].

Yine Yasanın 227-23'üncü maddesi ise bir küçüğün pornografik nitelikteki resminin kaydedilmesi ve hangi araçla olursa olsun yayınlanması ve iletilmesi eylemlerini suç olarak düzenlemiştir[221].

Ayrıca Ceza Kanununun 226-8'inci maddesi rızası olmadan sözleri veya resmi üzerinde gerçekleştirilen montajın hangi yollarla olursa olsun yayınlanması eylemi suç olarak kabul edilmiştir[222].

Görüldüğü üzere Fransız Ceza Kanununda yer alan yukarıda belirtilen maddelerde geçen "hangi yollarla olursa olsun" ve "hangi araçlarla olursa olsun" ifadelerinin bilgisayar ağlarını ya da İnternet'i kapsadığı aşikardır.

Fransız hukukunda İnternet üzerindeki suç içerikli yayınlardan dolayı kimin sorumlu tutulacağı sorunu da tartışmalara konu olmuş ve mevcut kuralların gereksinimleri karşılamadığı düşüncesiyle 30 Eylül 1986 tarihli iletişim özgürlüğü Yasasında değişiklik yapan l Ağustos 2000 tarihli yeni bir yasa kabul edilmiştir. Bu yasa ile iletişim özgürlüğü Yasasının 2'nci babına "Link Üzerinde özel Haberleşme Dışındaki iletişim Servisleriyle ilgili Hükümler" şeklinde bir 4'üncü başlık eklenmiştir. Toplam 4 maddeden oluşan bu başlık altında İnternet öznelerinin sorumluluğuna ilişkin bir düzenleme rejimi geliştirilmiştir[223].

[220] Kangal, 2001:228.
[221] Kangal, 2001:228.
[222] Kangal, 2001:228.
[223] Sınar, 2002:666.

İSS'ler yönünden içerik sağlayıcının hazırlamış oldukları suç içerikli yayınlardan dolayı genel kurallara göre sorumlu olacağı kabul edilmektedir. Ayrıca webmaster[224], editör veya benzeri bir sıfatla suç içerikli verilerin yayına hazırlanmasında veya yayına konulmasında katkısı bulunan kişilerin de iştirak kuralları çerçevesinde sorumlu olacakları esası benimsenmektedir.

Erişim sağlayıcılar açısından ise, erişim sağlayıcının sadece bir taşıyıcı olmasından hareketle ceza sorumluluğu kabul edilmemiştir. Ancak erişim sağlayıcılara bazı hizmetleri ayıklamaya yarayan teknik olanakları kullanıcılara bildirme yükümlülüğü getirilmiştir.

İSS'lere ilişkin esaslar ise Yasanın 48-3'üncü maddesinde düzenlenmiştir. Servis sağlayıcıların sunucularında depoladıkları suç içerikli veriler nedeniyle bu durum kendilerine adli bir makam tarafından bildirilmesine rağmen harekete geçmemişlerse sorumlu tutulabilecekleri düzenlenmiştir. İSS'lere sunucularında barındırdıkları verilerle ilişkili olarak kesinlikle bir takip ve denetim yükümlülüğü öngörülmemiş, aksine servis sağlayıcının harekete geçmemiş olmasından dolayı sorumlu olabilmesini ancak bir yargı makamı tarafından kendisine bildirimde bulunulması şeklinde bir ön şarta bağlamaktadır[225].

3.2.5. İngiltere

İngiltere'de siber suçlar Anglo Sakson hukuk sistemine uygun olarak Amerika Birleşik Devletleri, İrlanda ve Portekiz'de olduğu gibi özel kanunlarla düzenlenmiştir.

İngiltere'de siber suçları düzenleyen kanun 29 Temmuz 1990 tarihinde yürürlüğe giren "Computer Misuse Act" adlı kanundur. Bu kanunun yürürlüğe sokulmasının amacı yetkisiz olarak bilgisayarlara girilmesinin veya değişiklik yapılmasının veyahut benzeri müdahalelerde bulunulmasının önlenmesidir.

[224] Bir web sitesinin yönetimini üstlenen kişiye "Webmaster" adı verilir. Webmaster'ın görevi Web sitesininin tasarımını yapmak ve güncelliğini korumaktır.
[225] Sınar, 2002:666.

Yine anılan kanunla üç tip suç belirlenmiştir[226]. Bu suçlar;

- Yetkisiz olarak bilişim cihazlarına, veri ve programlarına girilmesi,
- Başka bir suçun işlenmesini sağlamak veya kolaylaştırmak amacıyla yetkisiz olarak bilişim cihazına girilmesi,
- Yetkisiz olarak bir bilgisayarın içeriğinde değişikliğe neden olunmasıdır.

Görüldüğü üzere İngiltere'de yapılan siber suçlara ilişkin düzenleme Amerika Birleşik Devletleri'ndeki mevzuata benzemektedir.

İngiltere'de, İnternet öznelerinin ceza sorumluluğu, öz-düzenleme (self-regulation) yolu ile belirlenmiştir. Yani İSS'ler tabi olacakları hukuki rejimin ana ilkelerini kendileri belirlemektedirler. Bunu da kurmuş oldukları "Birleşik Krallık İnternet Servis Sağlayıcıları Derneği" (ISPA-UK - Internet Service Providers Association of United Kingdom) adlı bir örgüt çatısı altında bir araya gelerek yapmışlardır. İnternet servis sağlayıcıları kendi koymuş oldukları kuralların sağlıklı bir şekilde işleyip işlemediğini yine kendi oluşturdukları bir kontrol mekanizması ile denetlemektedirler[227].

3.2.6. Japonya

Japonya'nın teknolojiye olan yakın ilgisinin de etkisiyle, siber suçlar konusunun yaratabileceği tehlikelerin önceden farkına varılmış ve ceza hukukunda gerekli düzenlemeler erken bir zamanda yapılmıştır. Söz konusu düzenlemeler yapılmadan önce, bu düzenlemelerin nasıl yapılacağı konusu doktrinde tartışılmış ve siber suçlarla mücadelede, klasik ceza normlarının yeterli olamayacağı kabul edilerek, bu konuda yeni suç tiplerinin kabul edilmesi gerektiği konusunda uzlaşmaya varılmıştır. Bunun sonucunda 22 Haziran 1987 tarihinde yürürlüğe giren "Ceza Hukuku Alanında Bazı Hükümlerde Değişiklik Yapılmasına İlişkin Kanun"

---

[226] Akdeniz, Yaman. *Section 3 of the Computer Missuse Act 1990: an Antidote for Computer Viruses!*. Web Journal of Current Legal Issues. 01 OCAK 1996. 24 ARALIK 2005. http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html

[227] Akdeniz, Yaman. *Section 3 of the Computer Missuse Act 1990: an Antidote for Computer Viruses!*. Web Journal of Current Legal Issues. 01 OCAK 1996. 24 ARALIK 2005. http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html

ile Ceza Kanununa siber suçlarla ilgili yeni suç tipleri eklenmiştir. 1990'lı yıllarda ise, cyber-pornografik fiiller Ceza Kanunu'nun 175'inci maddesi kapsamında kabul edilmiştir[228].

Ayrıca 3 Şubat 2000 tarihinde yürürlüğe giren 1999/128 sayılı "Bilgisayarlara Yetkisiz Erişim Kanunu" (Unauthorized Computer Access Law) ile de, bilgisayar ağları yoluyla işlenen suçlar ayrıntılı bir şekilde düzenlenmiştir[229].

[228] Karagülmez, 2005:166; Dülger, 2004:121; Ünver, 2001:75,76.
[229] Karagülmez, 2005:121.

4. AVRUPA KONSEYİ SİBER SUÇ SÖZLEŞMESİ

4.1. Giriş

Ceza hukukunun ilk ve en önemli ilkesine göre, bir eylemin suç sayılması ve bu eylemi yapanın cezaya çarptırılabilmesi için, o eylemin işlendiği tarihte yürürlükte olan yasalarda suç olarak tanımlanmış olması gerekmektedir. Bu ilke, 01/06/2005 tarihi itibarıyla yürürlükten kaldırılan 706 sayılı Türk Ceza Kanunu'nun birinci maddesinde "Kanunun sarih olarak suç saymadığı bir fiil için kimseye ceza verilmez. Kanunda yazılı cezalardan başka bir ceza ile de kimse cezalandırılamaz" biçiminde ifade edilmişken, 5237 sayılı Yeni Türk Ceza Kanunu'nun ikinci maddesinin birinci bendinde "Kanunun açıkça suç saymadığı bir fiil için kimseye ceza verilemez ve güvenlik tedbiri uygulanamaz. Kanunda yazılı cezalardan ve güvenlik tedbirlerinden başka bir ceza ve güvenlik tedbirine hükmolunamaz." şeklinde ifade edilmiştir.

Yine gerçek dünyada suç sayılan yani ceza kanununda suç olarak kabul edilen bir eylemin, yeni bir görünüm veya biçimde siber uzayda karşımıza çıkması durumunda, bu suçun ceza kanununda yer alan bir suçun benzeri olduğunu söyleyip, o suça verilen cezayı yeni bir görünüm veya biçimde siber uzayda karşımıza çıkan suça veremeyiz. Çünkü ceza hukukunda kıyas geçerli değildir. 5237 sayılı Yeni Türk Ceza Kanunu'nun ikinci maddesinin üçüncü bendinde "Kanunların suç ve ceza içeren hükümlerinin uygulanmasında kıyas yapılamaz. Suç ve ceza içeren hükümler, kıyasa yol açacak biçimde geniş yorumlanamaz." denilerek, ceza hukuku açısından kıyas, kesin olarak yasaklanmıştır. Kısaca, ceza hukuku açısından bir eylemin suç sayılabilmesi için o eylemin bütün öğeleri ile yasada belirlenmiş ve suç olarak tanımlanmış olması gerekir.

Milli yasalar ve özellikle ceza yasaları, genel olarak sadece ülke sınırları içinde uygulanabilmektedir. Buna yasaların ülkeselliği (territoriality) ilkesi denmektedir. Oysa siber uzayda işlenen bir suçun hangi ülkede işlendiğinin

belirlenebilmesi için, bazı yeni hukuksal tanımların ve kabullerin yapılması ve üzerinde anlaşılması gerekmektedir[230].

Bazen bir yasadışı eylemin meydana geldiği ülke ile sanığın vatandaşlık bağı ile bağlı olduğu ülke farklı olabilmekte, hatta yasadışı eylemi işleyen kişi üçüncü bir ülkede yaşayabilmektedir. Bu durumda söz konusu eylemin "suç" olup olmadığı, hangi ülkenin yasasına göre belirleneceği ve yasadışı eylemle ilgili adli kovuşturma, yargılama ve cezalandırmanın hangi ülkede yapılacağı sorunları ortaya çıkmaktadır. Bu sorunların çözümü uluslararası hukukun alanına girmekte ve bu sorunlar çeşitli, çok taraflı veya iki taraflı uluslararası anlaşmalarda ele alınmaktadır. Yukarıda da belirtildiği gibi, siber uzayda işlenen suçlarda, çoğu kez, suçun işlendiği, suçlunun yaşadığı ve vatandaşı olduğu ülkeler ayrı ayrı ülkeler olabilmektedir.

Diğer taraftan yasadışı eylemin siber uzayda işlenmiş olması, bu fiilin kimin tarafından ve nerede yapıldığını ve sonuçlarının nerelerde etkili olduğunu saptamak bugünkü teknolojinin sağladığı araçlarla zor da olsa büyük ölçüde mümkün bulunmakla beraber, bunun için ilgili ülke makamlarının işbirliği yapmaları ihtiyacı ortaya çıkmaktadır[231].

Yukarıda belirtilen sorunların çözüme kavuşturulabilmesi için, bilgisayar ağlarının sınır ötesi yapısı gereği, siber uzay suçlarının hangi fiillerden oluştuğunun saptanması ve bu suçlarla mücadelede uluslararası müşterek bir ceza politikasının belirlenmesi gerekmektedir. Zira geleneksel ceza hukuku kuralları, siber uzay olanaklarının kötüye kullanımını engellemeye yetmemektedir. Gerçekten bilgisayar ağlarının ve bu ağlardan en çok kullanılmakta olan İnternet'in milyonlarca bilgisayar arasında iletişimi sağlaması, suçun ve suçlunun ortaya çıkartılması ve delillerin toplanmasında uluslararası dayanışmayı günümüzde hiç olmadığı kadar önemli ve gerekli kılmaktadır. Siber suçlarla mücadelede uluslararası dayanışmaya gereken önem verilmezse, çeşitli bölgelerin veya ülkelerin siber suç cenneti haline gelmesi kaçınılmaz olacaktır[232].

---

[230] "Avrupa Konseyi ve Siber Uzay Suçları". *Bilişim Kültürü Dergisi*. 01 EYLÜL 2001:1. 11. EYLÜL 2004. http://tbd.org.tr/sayi79_html/hukuk_kesmez.html

[231] "Avrupa Konseyi ve Siber Uzay Suçları". *Bilişim Kültürü Dergisi*. 01 EYLÜL 2001:2. 11. EYLÜL 2004. http://tbd.org.tr/sayi79_html/hukuk_kesmez.html

[232] Sieber, 1998:74

Sonuç olarak yukarıda zikredilen sorunların çözüme kavuşturulabilmesi için uluslararası işbirliğine gidilmesi gerekmektedir. Bu sebeple böyle bir sözleşmeye ihtiyaç duyulmuş ve siber suçlardan en çok müzdarip olan ABD'nin de katkı ve görüşleriyle Avrupa Konseyi Siber Suç Sözleşmesi[233] hazırlanmıştır. Siber suçlarla ilgili ilk ve tek uluslararası sözleşme olan Avrupa Konseyi Siber Suç Sözleşmesi bu tip suçlarla mücadelede büyük bir önem taşımaktadır.

4.2. Sözleşmenin amacı ve sistematiği

Avrupa Konseyi, 19 Eylül 2001 tarihinde siber suçlar hakkında uluslararası bir sözleşme taslağı üzerinde anlaşmaya varmış ve taslak sözleşme metnine yönelik nihai kararı 8 Kasım tarihinde bakanlar düzeyinde yapılan toplantıda ele alarak, sözleşmeyi 23 Kasım 2001 tarihinde imzaya açmıştır[234].

Sözleşmenin yürürlüğe girebilmesi için üçü Avrupa Konseyi üyesi olmak üzere beş ülkenin onaylaması gerekmektedir.

Sözleşme 48 maddeden oluşmakta olup, bu sözleşmeyle amaçlanan, sözleşmeye uygun ulusal düzenlemelerin yapılması, uluslararası işbirliğinin geliştirilmesi ve bu sözleşmeyi imzalayan tüm taraf devletlerde benzer suç tipleri tespit edilerek uluslararası yeknesaklık sağlanması ve böylece toplumun siber suçlara karşı korunması için ortak bir ceza politikasının oluşturulmasıdır.

Sözleşme buna uygun olarak dört bölümden oluşmaktadır. Birinci bölümde Terimler, ikinci bölümde Ulusal Düzeyde Alınacak Önlemler, üçüncü bölümde Uluslararası İşbirliği, dördüncü bölümde ise Diğer Hükümler başlıkları altında düzenlenmiştir.

---

[233] Council of Europe, *Convention on Cybercrime*, 23.11.2001, orjinal metin için bkz. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; Bu metnin çevirisi İnternet ve Hukuk Platformu – İvHP tarafından yapılmıştır. http://www.ivhp.org.tr

[234] 23 Kasım 2001 tarihinde Budapeşte'de yapılan toplantıda, Avrupa Konseyi üyelerinden Arnavutluk, Bosna-Hersek, Danimarka, Ermenistan, Avusturya, Belçika, Bulgaristan, Hırvatistan, Çek Cumhuriyeti, Estonya, Finlandiya, Fransa, Almanya, Yunanistan, Macaristan, İtalya, Lüksemburg, Letonya, Litvanya, Lüksenburg, Sırbistan Karadağ, Malta, Moldovya, Hollanda, Norveç, Polonya, Portekiz, Romanya, İrlanda, İspanya, İsveç, İzlanda, Makedonya, Slovakya, Slovenya, Güney Kıbrıs, Ukranya ve İngiltere, üye olmayan ülkelerden ise Kanada, Japonya, Güney Afrika, ve ABD sözleşmeyi imzalamışlardır.

4.3. Sözleşme'nin temel hükümlerinin incelenmesi

4.3.1. Sözleşmede yer alan terimler

Sözleşmede[235] bilgisayar sistemi, bilgisayar verisi, hizmet sağlayıcı ve trafik bilgisi tanımlarına yer verilmiştir. Anılan terimlere açıklık getirilmesi ve kapsamlarının net bir şekilde belirlenmesi, sözleşme hükümlerinin daha iyi anlaşılabilmesi ve etkin bir şekilde uygulanabilmesi bakımından büyük önem taşımaktadır. Avrupa Konseyi Siber Suç Sözleşmesi'nin bu alanda kabul edilen ilk uluslararası anlaşma olması, sözleşmede yer verilen terimlerle, ülkeler arasında işbirliğini hızlandırma ve kolaylaştırma görevini de yüklemektedir[236].

4.3.1.1. Bilgisayar sistemi

Bilgisayar sistemi, dijital verilerin otomatik olarak işlenmesi için geliştirilmiş donanım ve yazılımdan oluşan bir cihazdır. Bu tanım girdi, çıktı ve saklama özelliklerini de içine almaktadır. Sistem tek başına çalışabileceği gibi benzer cihazlardan oluşan bir ağa bağlı olarak da çalışabilir.

Ağdan anlaşılması gereken, bir veya daha fazla bilgisayar arasındaki ara bağlantıdır. Bu bağlantı kablo veya tel ile olabileceği gibi radyo, kızıl ötesi (infrare), veya uydu vasıtasıyla da olabilir. Ağ coğrafi bakımdan küçük bir alanla sınırlı olabileceği gibi (yerel ağ), geniş bir alan içerisinde de geçerli olabilmektedir.

Verinin işlenmesinden kastedilen bir bilgisayar programı tarafından işletilen bilgisayar sistemi içerisinde çalışan veridir. Otomatikten kastedilen ise, insan müdahalesinin olmamasıdır.

4.3.1.2. Bilgisayar verisi

Bilgisayar verisinin tanımı ISO'nun veri tanımına dayanmaktadır. Bu tanımda "işlenmeye uygun nitelikte" (suitable for processing) ifadesi kullanılmıştır Bu ifadeden anlaşılması gereken verilerin bilgisayar sistemi tarafından doğrudan

---

[235] Bu bölümdeki açıklamalar Avrupa Konseyi Siber Suç Sözleşmesinin Açıklayıcı Memorandumundan (Convention on Cybercrime Explanatory Report) faydanılarak oluşturulmuştur. http://conventions.coe.int/Treaty/en/Reports/Html/185.htm

[236] Helvecıoğlu, 2004:278.

işlenebilir biçimlerde bulunmasıdır. Sözleşmede bahsedilen verilerin elektronik ya da diğer doğrudan işlenebilir biçimlerde olduğunu açıkça belirtmek için "bilgisayar verisi" kavramı kullanılmıştır. Otomatik olarak işlenen bilgisayar verileri, bu Sözleşmede tanımlanan ceza hukukuna tabi suçlardan birinin hedefi ve bu Sözleşmede tanımlanan soruşturmaya yönelik önlemlerden birinin uygulanmasının nesnesi olabilir.

4.3.1.3. Hizmet sağlayıcı

Bilgisayar sistemlerindeki verilerin iletişiminde ya da işlenmesinde belirli bir role sahip kişilere yönelik olarak kullanılan, oldukça geniş bir kategoriyi içine alan bir terimdir.

Hizmet Sağlayıcı tanımı hem kamu hem de özel sektörü kapsamaktadır. Bu nedenle kullanıcıların kapalı bir grup oluşturması ya da sağlayıcının hizmetlerini kamuoyuna sunması, hizmetlerin bedava veya ücretli olmasının bir önemi bulunmamaktadır.

4.3.1.4. Trafik bilgileri

Özel bir hukuki rejime tabi olan bilgisayar verisi olup iletişim zincirinde, iletişimi başlangıcından varış noktasına kadar sürdüren bilgisayarlar tarafından oluşturulmaktadır.

Bir bilgisayar sistemi ile bağlantılı olarak işlenen ceza hukukuna tabi bir suçun soruşturulmasında, yeni deliller toplanması için bir başlangıç noktası ya da suçun delillerinin bir parçası olarak iletişimin kaynağının saptanması için trafik bilgilerine ihtiyaç bulunmaktadır.

Trafik bilgileri çok kısa süreli olarak tutuluyor olabilir; bu yüzden hemen koruma altına alınması gerekebilir. Dolayısıyla, silinmeden önce yeni deliller toplamak ya da şüpheliyi teşhis etmek üzere bir iletişimin izlediği yolu bulmak için bu bilgilerin hemen açıklanması gerekebilmektedir. Bu nedenle bilgisayar verilerinin toplanmasında ve açıklanmasında kullanılan normal usuller yetersiz kalabilir. Ayrıca bu verilerin toplanmasının ilke olarak özel hayatı daha az zedeleyici olduğu

düşünülmektedir. Çünkü bu durumda iletişimin daha hassas olduğu düşünülen içerik açığa vurulmamaktadır.

Trafik bilgilerinin içerisinde iletişimin başlangıç noktası, varış noktası, izlediği yol, saat, tarih, boyutlar, süre ve bu iletişimde kullanılan hizmet tipi (dosya transferi, e-posta gibi) bulunmaktadır.

4.3.2. Ulusal düzeyde alınacak önlemler

Sözleşmede ulusal düzeyde alınacak önlemler, iki kısma ayrılarak düzenlenmiştir. Birinci kısım "maddi ceza hukuku", ikinci kısım ise "usul hukuku" başlığını taşımaktadır. Maddi ceza hukuku başlığı altında düzenlenen kısımda, bilgisayar ya da bilgisayar ile ilgili suçlar alanında hem suç sayılacak eylemleri belirleyen hükümler, hem de bağlantılı diğer hükümler yer almaktadır.

Sözleşmenin maddi ceza hukuku kısmında suç olarak kabul edilen eylemler asgari bir uzlaşmayı temsil etmektedir, ulusal düzeydeki eklemeleri içermemektedir. Listede büyük ölçüde Avrupa Konseyi'nin bilgisayarla ilişkili suçlara ilişkin R(89)9 sayılı Tavsiyesiyle bağlantılı olarak geliştirilmiş olan talimatlara ve diğer kamusal ve özel uluslararası kuruluşların (OECD, BM,) çalışmaları esas alınmıştır.

Sözleşmede maddi ceza hukukuna ilişkin düzenlemeler 2-13'üncü maddeler arasında düzenlenmiştir.

Ulusal düzeyde alınacak önlemler kapsamında maddi ceza hukuku bölümü 5 başlık altında toplanmaktadır, ilk başlıkta bilgisayara ilişkin temel suçlar olan bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne, kullanıma açıklığına yönelik suçlar ele alınmıştır.

2, 3 ve 4'üncü başlıklar ise bilgisayar ile ilişkili diğer suçları kapsamaktadır. Bu suçlarda daha çok eylem öne çıkmakta, bilgisayar ve telekomünikasyon sistemleri mevcut ceza hukuku ile korunan menfaatlere saldırmada araç olarak kullanılmaktadır.

2'nci başlıkta bilgisayarla ilişkili sahtecilik ve sahtekarlık, 3'üncü başlıkta ise, bilgisayar sistemlerinin kullanılması ile çocuk pornografisinin kanunsuz olarak üretimine ve dağıtımına ilişkin eylemler yer almaktadır.

4'üncü başlıkta ise telif ve ilgili hakların ihlallerine ilişkin suçlar bulunmaktadır. Telif hakkı ihlallerinin bilgisayarlarla işlenen veya bilgisayarlarla ilişkili suçların en yaygın biçimlerinden biri olması ve bu ihlallerin artışının uluslararası düzeyde kaygıya yol açması nedeniyle sözleşmeye dahil edilmiştir.

Sözleşmede yer alan fillerin ortak özelliği, hak sahibi olmadan işlenmiş olmalarıdır. Fiillerin suç olarak kabul edilebilmesi için gerekli unsur da budur. Sözleşmeye konu olan filler rıza, meşru müdafaa veya zaruret hali gibi durumlarda suç kapsamı dışında bırakılacaktır. Dolayısıyla kamu düzenini sağlamak, ulusal güvenliği korumak veya suça konu filleri araştırmak ve soruşturmak amacıyla gerçekleştirilen eylemler suç kapsamı dışında kalmaktadır. Kısacası, sözleşmede ele alınan bütün suç tiplerinin kasıtlı olarak işlenmesi gereklidir. Örneğin, bilgisayarla dolandırıcılık suçunda (m. 8) ekonomik bir kazanç elde etmeye yönelik bir maksat aranmaktadır.

Sözleşmenin "Ulusal Düzeyde Alınacak Önlemler" başlıklı bölümünün ikinci kısmı ise yukarıda da belirtildiği gibi muhakeme hukukuna ayrılmıştır. Bu kısmın kapsamı, bir bilgisayar sistemi aracılığıyla işlenen ya da delilleri elektronik formda bulunan her türlü suç için geçerli olduğundan, I. Kısımda tanımlanan suçlardan daha geniştir. Yine bu kısımda öncelikli olarak usule ilişkin yetkiler için geçerli olan müşterek önlemler ve şartlar belirlenmekte, daha sonra ise usule ilişkin şu yetkiler belirtilmektedir;

- Saklanan bilgisayar verilerinin hızlı bir şekilde korunması,
- Trafik verilerinin hızlı bir şekilde korunması ve kısmen açıklanması,
- Üretim talimatı,
- Trafik verilerinin gerçek zamanlı olarak toplanması,
- İçerikle ilgili verilere müdahale edilmesi.

Sözleşmenin "Ulusal Düzeyde Alınacak Önlemler" başlıklı bölümünün sonunda ise yargı yetkisi ile ilgili hükümlere yer verilmiştir. Usule ilişkin

düzenlemeler sözleşmenin 14-21 inci maddeleri arasında düzenlenirken, yargı yetkisi de 22 inci maddede düzenlenmiştir.

Sözleşmenin 2 ila 10'uncu maddeleri arasında düzenlenen suçlar dört kategoriye ayrılmıştır. Bunlar; "Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve ulaşılabilirliğine yönelik suçlar", "Bilgisayar marifetiyle işlenen suçlar", "İçerikle ilgili suçlar", "Telif hakları ve bağlantılı hakların ihlali ile ilgili suçlar" olarak tasnif edilmiştir. Aşağıda bu suçlar kısaca incelenecektir.

4.3.2.1. Bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve ulaşılabilirliğine yönelik suçlar

Birinci kategoriyi oluşturan suçlar, "hukuka aykırı erişim" (m.2), "yasadışı müdahale" (m.3), "verilere müdahale" (m.4), "sisteme müdahale" (m.5) ve "cihazların kötüye kullanılması" (m.6) şeklinde adlandırılmıştır. Ceza hukukuna tabi suçlarla, bilgisayar sistem ve verilerinin gizliliğini, mahremiyetini, bütünlüğünü ve bunlara ulaşılabilmesini engelleyen fiillerden bilgisayar kullanıcılarını korumak amaçlanmıştır.

4.3.2.1.1. Hukuka aykırı erişim (m.2)

"Hukuka aykırı erişim" terimi bilgisayar sistem ve verilerinin güvenliğine (yani gizlilik, bütünlük ve ulaşılabilirlik) yönelik tehlikeli tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Koruma ihtiyacı, kuruluş ve kişilerin sistemlerini rahatsız edilmeden ve engellenmeden yönetme, işletme ve kontrol etme ihtiyaçlarını yansıtmaktadır[237]. Sadece izinsiz girme yani "hacking", "cracking" ya da "computer trespass" ilke olarak başlı başına yasadışı olmalıdır. Bu durum, sistemlerin ve verilerin meşru kullanıcılarının engellenmesine ve düzeltilmesi yüksek maliyet getiren değişiklik ve yıkıma yol açabilir. Bu tür izinsiz girmeler gizli verilere (şifreler, hedeflenen sistemle ilgili bilgiler dahil olmak üzere) ve sırlara erişilmesine, sistemin ücretsiz kullanılmasına yol açabilir, hatta bilgisayar korsanları bilgisayarla ilişkili sahtecilik ve sahtekarlık gibi daha tehlikeli bilgisayarla ilişkili suç türlerine teşvik edebilir.

[237] Akıncı, 2001:16.

İzinsiz erişimi önlemenin en etkin yolu hiç şüphesiz etkin güvenlik önlemlerinin geliştirilmesi ve uygulanmaya başlanmasıyla mümkündür. Ancak kapsamlı bir önlem paketi ceza hukukuna ilişkin önlemleri kullanma tehdidini ve bu önlemlerin kullanımını da içermelidir. İzinsiz erişimin ceza yoluyla engellenmesi sistem ve veriler için ek bir koruma getirebilir ve yukarıda sayılan tehlikelerin erken bir aşamada önlenmesini sağlayabilir.

"Erişim", bilgisayar sisteminin tamamına ya da bir parçasına (donanım, bileşenler, yüklenen sistemin saklanan verileri, dizinler, trafik ve içerikle ilişkili veriler) girilmesi anlamındadır. Ancak, sisteme sadece bir e-posta mesajı ya da dosya gönderilmesini kapsamaz. Erişim, kamusal telekomünikasyon ağları yoluyla ya da bir kuruluşun yerel ağı (LAN) ya da İntranet gibi bir ağ üzerindeki başka bir bilgisayar sistemine girmeyi kapsamaktadır. İletişim yöntemi (örneğin kablosuz bağlantılar da dahil olmak üzere uzaktan ya da yakın mesafeden) önemli değildir.

Bir çok ulusal mevzuatta halihazırda hacking suçlarıyla ilgili hükümler bulunmaktadır. Ancak kapsam ve hükümler konusunda aykırılıklar mevcuttur. 2' nci maddenin ilk cümlesindeki geniş suç olarak tanımlama yaklaşımı tartışmalara yol açmıştır. Yalnızca izinsiz girme fiilinin hiçbir tehlike yaratmadığı ve hatta hacking olaylarının sistemlerin güvenliğindeki boşluk veya zayıflıkların tespitini sağladığı durumlar farklı görüşlerin doğmasına yol açmıştır.

Sözleşme ülkelere çeşitli alternatifler de sunmaktadır. Taraflar geniş yaklaşımı benimseyerek madde 2'nin ilk cümlesine uygun biçimde sadece hacking fiilini de suç olarak tanımlayabilirler. Diğer bir seçenek tarafların güvenlik önlemlerinin ihlal edilmesi, bilgisayar verilerinin elde edilmesi amacı, ceza hukukuna tabi suç oluşturacak dürüst olmayan başka amaçlar, suçun uzaktaki başka bir bilgisayar sistemine bağlı bir bilgisayar sistemi ile ilişkili olarak işlenmiş olması gibi şartları kabul etmeleridir. Son seçenek olarak Tarafların bir kişinin başka bir bilgisayar sistemini kullanmaksızın bağımsız bir bilgisayara fiziksel erişimi kapsam dışı bırakmalarıdır.

4.3.2.1.2. Yasadışı müdahale (m.3)

Sözleşmenin 3'üncü maddesinde düzenlenen bu hükümle, verilere müdahale değil, verilerin iletimine müdahale edilmesi yasaklanmıştır. Bu suçla, iletişimin gizliliği hakkının korunması hedeflenmiştir. İletişimin gizliliği hakkı, Avrupa İnsan Hakları Konvansiyonunun 8'inci maddesinde kutsal bir hak olarak gösterilmiştir. Madde 3'te tanımlanan suç, bu ilkenin telefon, faks, e-posta ya da dosya transferi şeklindeki bütün elektronik veri transferi biçimlerine uygulanmasını kapsamaktadır.

Teknik yöntemler kullanarak müdahale, iletişimin içeriğinin dinlenmesi, denetlenmesi ya da izlenmesi ve verilerin içeriğinin bilgisayar sistemine erişim ve sistemin kullanımı yoluyla doğrudan ya da elektronik gizli dinleme cihazlarının yardımı ile dolaylı olarak elde edilmesi ile ilgilidir. Müdahaleyi kaydetmek de buna dahildir. Teknik yöntemler, iletim hatlarına takılan teknik cihazlarla birlikte kablosuz iletişimi elde etmekte ve kaydetmekte kullanılan cihazları da kapsar. Bu yöntemler yazılım, şifre ve kodların kullanımını da kapsayabilir. Teknik yöntemler kullanma şartı, gereğinden fazla fiili suç olarak tanımlamaktan kaçınmak için getirilmiş kısıtlayıcı bir şarttır.

Suç, kamuya açık olmayan bilgisayar verilerinin iletimi için geçerlidir. Kamuya açık olmayan terimi ile iletilen verilerin yapısı değil, iletişimin yapısı nitelendirilmektedir. Örneğin kamuya açık olan bir bilgi taraflarca gizlilik içerisinde iletilmek istenilebilir veya veri kablolu TV gibi, ticari amaçlar nedeniyle hizmet bedeli ödeninceye dek gizli tutulmak istenilebilir. Bu nedenle kamuya açık olmayan ifadesi kamu ağlarından yapılan iletişimler haricinde yapılan iletişimlerdir gibi bir genelleme yapılamayacaktır.

Bilgisayar verilerinin iletimi biçimindeki iletişim tek bir bilgisayar sisteminin içinde (örneğin merkezi işlem ünitesinden ekran ya da yazıcıya akış), aynı kişiye ait iki bilgisayar sistemi arasında, birbiriyle iletişim halindeki iki bilgisayar ya da bir bilgisayar ile bir kişi (örneğin klavye yoluyla) arasında olabilir.

Çalışanların aralarında yaptıkları, iş dışı konular dahil olmak üzere, bilgisayar verisinin kamuya açık olmayan yayını olarak kabul edilen iletişimler de bu kapsamda korunmaktadırlar.

Yasadışı müdahalenin kasıtlı olarak ve haksız biçimde gerçekleştirilmesi gereklidir. Eğer müdahale eden kişi, bunu yapma hakkına sahipse veya iletimi tarafların talimatları doğrultusunda ya da izinleriyle yapıyorsa ya da izleme ulusal güvenlik ya da soruşturma mercilerinin suçları araştırma çalışmaları çerçevesinde yasal yetkiyle gerçekleştiriliyorsa, haklıdır ve bu suçtan dolayı cezalandırılmaz.

4.3.2.1.3. Verilere müdahale (m.4)

Bu hükmün amacı, bilgisayar verilerinin ve bilgisayar programlarının kullanımına, bütünlüğüne ve tam olarak işleyişine karşı kasıtlı olarak zarar verme eylemlerinin engellenmesidir.

Tahrip etmek ve bozmak özellikle veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz biçimde değiştirilmesiyle ilişkilidir. Verilerin silinmesi, fiziksel bir cismin imhasıyla eşdeğerdir. Bilgisayar verilerinin erişilmez kılınmasıyla, verilerin saklandığı bilgisayara ya da veri taşıyıcısına erişimi olan bir kişinin verilere ulaşmasını önleyen ya da sona erdiren herhangi bir fiil kastedilmektedir. Değiştirme mevcut verilerin farklı bir hale getirilmesi anlamındadır.

Virüs ve Truva Atı gibi kötü amaçlı kodların sisteme sokulması da verilerin farklı bir hale getirmesi nedeniyle bu madde kapsamındadır.

Bu fiiller ancak haksız biçimde gerçekleştirilirse cezalandırılabilir. Ayrıca failin kasıtlı olarak hareket etmiş olması gerekmektedir.

4.3.2.1.4. Sistemlere müdahale (m.5)

Sisteme müdahale bilgisayar sabotajı olarak da nitelendirilmektedir. Anılan maddede yer alan hükümler, bilgisayar sistemlerinin yasal kullanımının kasıtlı olarak engellenmesini suç olarak kabul etmektedir. Yine söz konusu maddeye göre bilgisayar sisteminin tam olarak işleyişini engelleyecek her türlü müdahale suça yönelik fiil olarak değerlendirilmektedir. Ancak engellemenin ciddi olması gereklidir. Taraflardan her biri engellemenin ciddi sayılabilmesi için hangi ölçütlerin gerçekleşmesi gerektiğine kendisi karar verecektir.

Ticari ya da başka amaçlarla istenmeyen e-postaların gönderilmesi, özellikle büyük miktarlarda ve çok sık bir biçimde gerçekleştirildiğinde alıcıyı rahatsız

edebilir. Metni hazırlayanlara göre bu fiil, ancak iletişimi kasıtlı olarak ve ciddi ölçüde engellediğinde suç olarak tanımlanmalıdır.

Engelleme haksız biçimde yapılmış olmalıdır. Suç kasıtlı olarak işlenmiş olmalı yani fail ciddi ölçüde engelleme kastıyla hareket etmiş olmalıdır.

4.3.2.1.5. Cihazların kötüye kullanımı (m.6)

Sözleşmenin bu kategorisinin son maddesinde, taraf devletlere suç olarak kabul edilmesi için önerdiği bu hüküm ile aslında, 2 ila 5'inci maddelerde yer alan suçların işlenmesi için yapılan hazırlık hareketleri niteliğindeki fiilleri, suç kapsamına alınmaktadır[238]. Bu suçları işlemek için genellikle erişim araçlarının ya da başka araçların bulundurulması gerekmektedir. Ayrıca suçun kasıtlı olarak ve haksız biçimde işlenmiş olması gerekmektedir. Maddenin 2'nci paragrafında bir bilgisayar sisteminin izinli olarak test edilmesi veya korunması amacıyla yaratılan araçların hükmün kapsamı dışında olduğu açıklanmaktadır.

4.3.2.2. Bilgisayarlarla ilişkili suçlar

Sözleşmenin 7 ila 10'uncu maddeleri arasında, bir bilgisayar sistemi kullanılarak işlenen geleneksel suçlara ilişkin hükümler yer almaktadır. Çoğu ülke, sözleşmede düzenlenen klasik suçları, suç olarak tanımlamış durumdadır. Bu ülkelerin mevcut mevzuatı bilgisayar ağlarını içine alacak kadar geniş olabilir ya da olmayabilir (örneğin, bazı ülkelerin mevcut çocuk pornografisi yasaları elektronik görüntülere uygulanabilir değildir). Bu nedenle ülkeler, bu maddeleri uygulama sürecinde mevcut mevzuatlarını inceleyerek bilgisayar sistem ve ağlarının söz konusu olduğu durumlara uygulanıp uygulanamayacaklarına karar vermelidir. Mevcut suçlar halihazırda bu fiilleri içine alıyorsa, mevcut suçlar üzerinde değişiklik yapmak ya da yeni suçlar tesis etmek gerekli değildir.

[238] Koca, 2003:802.

4.3.2.2.1. Bilgisayarlarla ilişkili sahtecilik fiilleri (m.7)

7'nci maddedeki hükmün amacı, somut (maddi) belge sahteciliği ile paralel bir suç tesis ederek, ceza kanunlarında yer alan sahtecilikle ilgili geleneksel suçlar konusunda doğabilecek boşlukların doldurulmasıdır.

Bu hüküm, yasal geçerliliği olan kamusal ve özel belgenin eşdeğeri olan verileri ele almaktadır. Doğru veya yanlış verilerin izinsiz olarak ilave edilmesi, sahte bir belgenin üretilmesine karşılık gelmektedir. Daha sonraki değiştirmeler (farklı hale getirme, farklı biçimlerini üretme, kısmi değişiklik), silme (verilerin veri ortamından çıkarılması) ve erişilmez kılma (verilerin gizli tutulması, saklanması) genel olarak hakiki bir belgenin tahrifine karşılık gelmektedir.

Bilgisayarlarla ilişkili sahtecilik, verilerde içerilen bilgilerin doğruluğuna dayalı hukuki işlemler sırasında verilerin delil olarak değerlerini değiştirmek üzere izinsiz olarak veri yaratılması ya da saklanan verilerin değiştirilmesi yoluyla kandırmaya yöneliktir. Korunan yasal hak, hukuki ilişkiler açısından önemli olabilecek elektronik verilerin güvenliği ve güvenilirliliğidir.

4.3.2.2.2. Bilgisayarlarla ilişkili sahtekarlık fiilleri (m.8)

Bu maddeye göre, her kim sahtekarlık yoluyla kendisi veya üçüncü bir şahsa haksız maddi menfaat sağlamak maksadıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma veya sahtekarlık yoluyla kendisi veya üçüncü bir şahsa haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale etme fiillerinde bulunmak suretiyle, bir başkasının mülkiyetinin ziyanına sebep olursa cezalandırılmaktadır.

Suçluların, teknoloji devrimiyle birlikte, kredi kartı sahtekarlıkları da dahil olmak üzere, sahtekarlık gibi ekonomik suçları işleme fırsatları artmıştır. Bilgisayar sistemlerinde temsil edilen ya da yönetilen varlıklar (elektronik fonlar, banka parası) geleneksel mülkiyet biçimleri gibi manipülasyon hedefi haline gelmişlerdir. Bu suçların başlıcaları, bilgisayara yanlış verilerin girildiği veri ekleme manipülasyonları, program manipülasyonları ve veri işleme sürecine yapılan diğer

müdahalelerdir. Bu Maddenin amacı mülkiyeti yasadışı biçimde nakletmek amacıyla veri işleme sürecine yapılan kanunsuz manipülasyonları suç olarak tanımlamaktır.

Bilgisayar sahtekarlığı manipülasyonları başka bir kişinin mülkiyetinin doğrudan ekonomik ya da zilyetlik kaybına yol açıyorsa ve fail kendisi veya bir başkasına kanunsuz ekonomik kazanç sağlamayı amaçladıysa suç olarak tanımlanmaktadır. Mülkiyetin kaybı terimi paranın, ekonomik değeri olan maddi ve gayri maddi varlıkların kaybını kapsamaktadır.

4.3.2.2.3. Çocuk pornografisi ile ilişkili suçlar (m.9)

Sözleşmenin üçüncü kategorisinde yer verilen fiiller "İçerikle ilgili suçlar"dır (Content-related offences). Bu suçların başında çocuk pornografisine ilişkin fiiller gelmektedir. Sözleşmenin bu maddesinde çocuk pornografisi ele alınmaktadır. Maddenin amacı, çocukları özellikle cinsel sömürüden koruyacak önlemlerin güçlendirilmesi ve ceza hukukunun ilgili maddelerinin modernizasyonu ile çocuklara yönelik cinsel suçlarda bilgisayar sistemlerinin kullanılmasına karşı daha etkin hükümlerin oluşturulmasıdır.

Bu hükümle, çocuk pornografisinin elektronik üretimi, bulundurulması ve dağıtılması suç olarak tanımlanmaktadır. Çoğu ülkenin çocuk pornografisinin geleneksel üretimini ve fiziksel dağıtımını suç olarak tanımlamış durumda olmasına rağmen, bu tür malzemelerin alışverişinde başlıca araç olarak İnternet'in kullanımının giderek artması karşısında çocukların bu yeni cinsel sömürü ve tehdit biçimine karşı savunulması için uluslararası hukuki bir belgeye ve özel hükümlerin yerleştirilmesinin çok önemli olduğu ortaya çıkmıştır.

9'uncu maddenin 1'inci bendinde çocuk pornografisi ile ilgili fiillere yer verilmiştir. Bunlar:

> "a. Bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek,
>
> b. Bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak ya da çocuk pornografisine erişim sağlamak,

c. Bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ya da yaymak,

d. Kişinin bir bilgisayar sistemi üzerinden kendisi ya da başkası için çocuk pornografisi temin etmesi,

e. Bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak." tır.

Paragraf 1 (b)'de bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak suç olarak tanımlanmıştır. "Sunmak" kelimesi teklif etmek anlamında kullanılmaktadır. Ayrıca, çocuk pornografisi elde etmek amacıyla başka kişilere başvurmayı da kapsaması amaçlanmıştır. Bu malzemeyi sunan kişinin onu gerçekten sağlayabileceği anlamına gelmektedir. Erişim sağlamak ifadesinin, örneğin bir çocuk pornografisi sitesi oluşturarak, başkalarının kullanımı için çocuk pornografisini online sunmayı kapsaması amaçlanmıştır.

Paragraf 1 (c)'de bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak ve yaymak suç olarak tanımlanmıştır. Bir bilgisayar sistemi üzerinden başka bir kişiye çocuk pornografisi göndermek, çocuk pornografisi yayını olarak kabul edilecek ve bu suç kapsamına girecektir.

Paragraf 1 (d)'de "kendisi ya da başkası için temin etmek" terimi, örneğin bilgisayarına indirme (download) yoluyla aktif olarak çocuk pornografisi elde etmek anlamındadır. Bir bilgisayar sisteminde ya da bilgisayar verilerinin saklandığı başka cihazlarda, örneğin bir disket ya da CD-Rom'da, çocuk pornografisi bulundurmak, bu tür malzemeler için talebi canlandıracağından paragraf 1 (e)'de suç olarak tanımlanmıştır.

9'uncu maddenin 2'inci bendinde çocuk pornografisi terimi açıklanmaktadır. Sözleşmeye göre çocuk pornografisi aşağıdakileri görsel anlamda teşhir eden pornografik malzemeler anlamına gelmektedir.

a. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımı,

b. Cinsel anlamda müstehcen bir eyleme reşit görünmeyen bir kişinin katılımı,

c. Cinsel anlamda müstehcen bir eyleme reşit olmayan bir kişinin katılımını gösteren gerçekçi görüntüler.

Bir başka ifade ile çocuk pornografisi, cinsel amaçlı ve şehvet hissi ile, düzeyi ne olursa olsun, cinsel bir aktiviteyi gösteren materyallerdir. Günümüzde İnternet'ten çocuk pornografisi gönderilmesi oldukça yaygınlaşmıştır. Chat odaları ve web sayfaları anonimlik hakkından da istifade ederek, bu tür materyallerin kolayca kullanıldığı ortamlar haline gelmiştir[239].

2'nci bentteki "Pornografik Malzemeler" terimi malzemelerin müstehcen, kamu ahlakına aykırı ve benzer biçimde ahlak dışı şeklinde sınıflandırılması açısından ulusal standartlara tabi olacaktır. Bu nedenle sanatsal, tıbbi, bilimsel ya da benzer bir değeri olan malzemeler pornografik olmayan malzemeler olarak görülebilir. Görsel teşhir terimi, bilgisayar disketi ya da başka elektronik saklama ortamlarında saklanan görsel malzemeye dönüştürülebilen verileri de kapsamına almaktadır.

9'uncu maddenin 3'üncü paragrafında "reşit olmayan kişi"den bahsedilmektedir. "Reşit olmayan kişi" terimi 18 yaşından küçük kişiler anlamına gelmektedir. Söz konusu tanım Birleşmiş Milletler Çocuk Hakları Sözleşmesindeki "çocuk" tanımına uygun olarak düzenlenmiştir. Burada sözü edilen yaşın çocukların cinsel nesne olarak kullanılmasıyla ilgili olduğu ve cinsel ilişki için izin yaşından farklı olduğu göz önüne alınmıştır. Ancak belirli ülkelerin çocuk pornografisi ile ilgili ulusal mevzuatlarında bir alt yaş sınırı getirdiği göz önüne alınarak, 3'üncü paragrafın son cümlesinde tarafların, 16'dan küçük olmamak şartıyla, farklı bir yaş sınırı getirmelerine izin verilmiştir.

4.3.2.2.4. Telif haklarının ve bağlantılı hakların ihlaline ilişkin suçlar (m.10)

Fikri mülkiyet haklarının, özellikle de telif haklarının ihlali, İnternet'te en yaygın olarak işlenen suçlar arasındadır ve bu durum hem telif hakkı sahipleri hem de bilgisayar ağları üzerinde profesyonel olarak çalışan kişiler için rahatsızlık yaratmaktadır. Koruma altındaki eserlerin (edebiyat, fotoğraf, müzik eserleri, görsel-

[239] Damon, W.D. Wright. "Cybercrimes". Venable LLP. 01 OCAK 2003. 18 MAYIS 2005. http://www.venable.com/docs/resources/ebookcybercrimes.cfm; Çeken, 2002:7; Koca, 2003:806.

işitsel eserler ve diğer eserler), telif hakkı sahibinin onayı olmadan İnternet üzerinde yeniden üretimi ve yayımının son derece yaygın olması, dijital teknolojiler aracılığıyla izinsiz kopya çıkarmanın kolaylığı ve elektronik ağlarda yeniden üretim ve yayımının iyice artması sonucunda, bu ihlallerin önüne geçebilmek için, sözleşmeye ceza hukuku hükümlerinin eklenmesi ve bu alandaki uluslararası işbirliğinin genişletilmesi zorunlu hale gelmiştir.

Taraflardan her biri 10'uncu maddede sayılan uluslararası anlaşmalar, Edebi ve Sanatsal Eserlerin Korunmasına Yönelik Bern Konvansiyonu çerçevesindeki 24 Temmuz 1971 tarihli Paris Yasası, Fikri Mülkiyet Haklarının Ticari Yönlerine İlişkin Sözleşme (TRIPS) ve Dünya Fikri Mülkiyet Kuruluşu (WIPO) Telif Hakları Anlaşması, Oyuncuların, Fonograf Yapımcılarının ve Yayım Kuruluşlarının Korunması Hakkında Uluslararası Konvansiyon (Roma Konvansiyonu), uyarınca yüklendiği sorumluluklara uygun olarak kendi milli mevzuatında belirlediği telif haklarının ve bağlantılı hakların kötü niyetli ihlallerini, bir bilgisayar aracılığıyla ve ticari ölçekte yapıldığında suç olarak kabul etmek zorundadır. Ancak, sözleşmeye taraf devletin bu ihlalleri suç olarak kabul etme yükümlülüğü, söz konusu sözleşmeler tarafından verilen manevi haklar için geçerli değildir[240].

Söz konusu maddede "ticari ölçekte" ve "bir bilgisayar sistemi aracılığıyla" gerçekleştirilen ihlallere karşı cezai yaptırımlar getirilmesi amaçlanmıştır. Bu, telif hakları meselelerinde cezai yaptırımları yalnızca "ticari ölçekte korsanlık" durumunda şart koşan TRIPS Sözleşmesinin 61'inci maddesine de uyumludur.

[240] Koca, (2003:806)' a göre FSEK'nin eser sahibine tanıdığı mavi haklar şunlardır; Umuma arz salahiyeti (m.14), adın belirtilmesi salahiyeti (m.15), eserde değişiklik yapılmasını menetmek (m.16) ve eser sahibinin zilyet ve malike karşı hakları (m.17). FSEK'nin 71'inci maddesi ise manevi haklara tecavüzü suç olarak kabul etmektedir. Buna göre; 1- Alenileşmiş olsun veya olmasın, eser sahibi veya halefin yazılı izni olmadan bir eseri umuma arz eden veya yayımlayan, 2- Sahip veya halefin yazılı izni olmadan, bir esere veya çoğaltılmış nüshalara ad koyan, 3- Başkasının eserini kendi eseri veya kendisinin eserini başkasının eseri olarak gösteren veya 15'inci maddenin ikinci fıkrasına aykırı hareket eden, 4- 32, 33, 34, 35, 36, 37, 38, 39, 40'ıncı maddelerdeki hallerde kaynak gösterilmeyen veya yanlış yahut kifayetsiz veya aldatıcı kaynak gösteren, 5- Eser sahibinin yazılı izni olmaksızın bir eseri değiştiren kişiler hakkında dört yıldan altı yıla kadar hapis ve elli milyardan yüz elli milyara kadar ağır para cezası verilecektir. Sözleşmenin 10'nuncu maddesi ile FSEK'nin 71'inci maddesini birbirini karşılayan maddeler olarak görmek zordur. 71'inci maddenin, Sözleşmenin 10'nuncu maddesini ihlal etmemesi için, bu maddedeki eylemlerin ticari ölçekte de olsa, bilgisayar sistemi aracılığıyla işlenmesinin, suç teşkil etmeyeceğine ilişkin bir fıkranın eklenmesi gerekir ki, bu tip bir düzenlemede mantıksız olur.

Ancak Taraflar "ticari ölçek" eşiğini aşmayı ve başka tür telif hakkı ihlallerini de suç olarak tanımlamayı tercih edebilirler.

Telif haklarının ve bağlantılı hakların ihlaline ilişkin suçların oluşabilmesi için telif hakları ve bağlantılı haklara karşı yapılan ihlallerin "kötü niyetli olarak" yapılması gerekir.

4.3.2.3. Sözleşme kapsamında suç olarak kabul edilen diğer fiiller

4.3.2.3.1. İştirak ve teşebbüs (m.11)

Madde 11'e göre, sözleşmede yer alan suçlara ek olarak, teşebbüs, yardım ve yataklık etme fiillerinin de suç olarak değerlendirilmesi gerekmektedir.

Maddenin 1'inci paragrafında taraf devletlerden, sözleşmede tanımlanan suçların herhangi birisinin işlenmesine yardım ve yataklık edilmesi durumunu kendi mevzuatlarında cezai bir suç olarak tanımlamaları istenmektedir. Sözleşmede tanımlanan bir suçu işleyen birine yine suçun işlenmesine başka bir kişi tarafından yardım edilirse, yardım ve yataklık ile ilgili yükümlülük doğmaktadır. Örneğin, zararlı içerik verilerinin ya da kötü amaçlı kodların İnternet üzerinden iletimi taşıyıcı olarak hizmet sağlayıcılarının yardımını gerektirmekle birlikte, cezai niyet taşımayan bir hizmet sağlayıcısı yükümlülük altına girmeyecektir. Dolayısıyla bu hüküm çerçevesinde cezai sorumluluktan kaçınmak için içeriği aktif olarak denetlemek hizmet sağlayıcısının görevi değildir.

Maddenin 2'nci paragrafında sözleşmede tanımlanan bazı suçlar ya da bu suçların unsurları için teşebbüsün kavramsal olarak güç olduğu düşünülmüştür (örneğin çocuk pornografisini sunmak veya buna erişim sağlamak unsurları). Dolayısıyla sadece sözleşmenin 3, 4, 5, 7, 8, 9(l)(a) ve 9(l)(c) maddelerinde tanımlanan suçlarla ilgili olarak teşebbüsün suç olarak tanımlanmasının gerekliliğine vurgu yapılmıştır. Ancak taraflar teşebbüse ilişkin bu hükme kısmen ya da hiç uymama hakkına sahiptir[241].

[241] Koca, 2003:812

4.3.2.3.2. Kurumsal yükümlülük (m.12)

Madde 12, tüzel kişiliklerin yükümlülükleri ile ilgilidir. Kurumlar, dernekler ve benzer tüzel kişiliklerin de işlenen suçlardan sorumlu tutulabileceğini göstermektedir. Maddenin amacı, bir tüzel kişilikte yönetici konumunda olan bir kişinin, tüzel kişiliğe bir menfaat sağlamak amacıyla gerçekleştirmiş olduğu suçlar sebebiyle tüzel kişiliklere yükümlülük getirmektir.

Maddenin 1'inci paragrafına göre, yükümlülüğün ortaya çıkması için dört şartın gerçekleşmesi gerekmektedir. Bu şartlar;

1- Sözleşmede tanımlanan suçlardan birinin işlenmesi;

2- Suçun bir tüzel kişiliğin menfaatine işlenmiş olması;

3- Suçun yönetici konumunda olan bir kişi tarafından işlenmesi;

4- Yönetici konumundaki gerçek kişinin kendi yetkileri dahilinde hareket ettiğini gösteren bir yetkiye (temsil etme, karar alma veya kontrol etme yetkisi) dayanarak hareket etmiş olmasıdır.

Paragraf 2'de ise sadece yönetici konumundaki gerçek kişiyi değil, bu kişinin idaresi altında faaliyet gösteren bir çalışanı ya da vekili tarafından suçun işlenmesi durumunda, tüzel kişilik üzerine yükümlülük getirme yetkisi düzenlenmektedir. Yükümlülük doğması için şu şartlar sağlanmalıdır: 1- suç, tüzel kişiliğin bir çalışanı ya da vekili tarafından işlenmiş olmalıdır, 2- suç tüzel kişiliğin menfaatine işlenmiş olmalıdır; 3- suçun işlenmesi yönetici konumundaki kişinin çalışan ya da vekil üzerindeki gözetim görevini yerine getirmemiş olması sonucunda mümkün hale gelmiş olmalıdır.

4.3.2.3.3. Yaptırımlar ve önlemler (m.13)

Sözleşmenin 13'üncü maddesi, ceza hukuku çerçevesinde cezalandırılabilir hale getirilmesi gereken siber suçların veya siber suçlarla bağlantılı suçların tanımlandığı madde 2-11'le yakından bağlantılıdır. Bu maddelerde getirilen zorunluluklara uygun olarak düzenlenen bu hüküm, Sözleşmeyi imzalayan tarafların bu suçların ciddiyetiyle ilgili sonuçlar çıkararak "etkin, adil, caydırıcı" ve gerçek

kişiler söz konusu olduğunda hapis cezası olasılığını da içeren cezai yaptırımlar getirmelerini şart koşmaktadır.

Yine bu maddeye göre yükümlülükleri madde 12'de saptanmış olan tüzel kişilikler de cezai, idari ya da medeni nitelikte olabilecek "etkin, adil ve caydırıcı" yaptırımlara tabi olmalıdır. Sözleşmeyi imzalayan Taraflar, paragraf 2 çerçevesinde tüzel kişiliklere parasal yaptırımlar getirme olasılığını yaratmak zorundadırlar.

Maddede, suçların ciddiyetine bağlı olarak başka yaptırım ve önlem olasılıkları açık bırakılmaktadır. Örneğin, önlemler ihtiyati tedbir ve hakkın düşmesini de içerebilmektedir. Mevcut ulusal hukuk sistemleriyle uyumlu bir cezai suç ve yaptırımlar sistemi yaratmak konusunda takdir yetkisi taraflara bırakılmaktadır.

4.4. Usul Hukuku

Bu bölümde, 1'inci bölümde tanımlanan suçların cezai soruşturması, bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlar ve cezai bir suça ilişkin olarak elektronik ortamda delil toplanması amacıyla ulusal düzeyde alınacak usul tedbirleri açıklanmaktadır.

4.4.1. Usul hükümlerinin kapsamı (m. 14)

Söz konusu maddeye göre, taraf ülkelerden her biri, ulusal mevzuatlarına ve hukuki çerçevelerine uygun olarak, bu bölümde tanımlanan yetki ve usulleri tesis etmek için gerekli olabilecek, "özel cezai soruşturma veya takibat"larla ilgili yasama önlemlerini ve diğer önlemleri benimsemek zorundadır.

İki istisnai durum dışında, taraflardan her biri bu bölüme uygun olarak tesis edilen yetki ve usulleri: 1- Sözleşmenin 1'inci kısmı uyarınca tesis edilen cezai suçlara; 2- bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlara; ve 3- cezai bir suça ilişkin olarak elektronik ortamda delil toplanmasına ilişkin olarak uygulamaya koyacaktır. Bu durum, bu kısımda belirlenen yetkiler ve usuller yoluyla herhangi bir cezai suça ilişkin olarak elektronik ortamda delil elde edilebilmesini ve toplanmasını güvence altına almaktadır. Böylece bilgisayar verilerini elde etmek ve toplamak için de elektronik olmayan veriler için geleneksel yetkiler ve usuller

çerçevesinde mevcut olanlara eşdeğer ya da paralel imkanlar sağlanmaktadır. Yine Sözleşmede, tarafların, kovuşturulan cezai suçun niteliğinden bağımsız olarak, dijital ya da başka elektronik ortamlarda bulunan bilgilerin ceza davalarında delil olarak kullanılmasının mümkün olduğunu mevzuatlarına sokmak zorunda olduklarını açıkça belirtilmiştir.

Bu uygulama kapsamı için yukarıda da belirtildiği gibi iki istisnai durum mevcuttur. Birincisi, 21'inci maddede, içerik verilerine müdahale etme yetkisinin ulusal mevzuatın belirlediği bir dizi ciddi suçla sınırlı tutulması, ikincisi ise, tarafların madde 20'deki önlemleri (trafik verilerinin gerçek zamanlı olarak toplanması) uygulama haklarının, ancak hakkın saklı tutulmasıyla ilgili hükümde belirtilen suçlar ya da suç kategorileri için ve bu suç ya da kategori grubunun, madde 21'de söz edilen müdahale önlemlerini uyguladığı suç grubundan daha sınırlı olmaması şartıyla saklı tutabilmesidir.

4.4.2. Şartlar ve önlemler (m. 15)

Sözleşmenin 15'inci maddesine göre, bu bölümde belirtilen yetki ve usullerin tesis edilmesi, gerçekleştirilmesi ve uygulanması her bir tarafın ulusal mevzuatındaki şart ve önlemlere tabi olacaktır. Taraflar belli usul hukuku hükümlerini ulusal mevzuatlarına sokmak zorunda olmakla birlikte, bu yetki ve usulleri hukuk sistemlerinde tesis etme ve gerçekleştirme tarzları, yetki ve usullerin özel durumlara uygulanması, tarafların ulusal yasalarına ve usullerine bırakılmıştır.

Sözleşmeye taraf olan ülkelerin, çok farklı hukuk sistemlerine ve kültürlere sahip olmasından dolayı, her bir yetki ve usul için geçerli olabilecek şart ve önlemleri ayrıntılarıyla açıklamak mümkün değildir. Sözleşmeye taraf olan ülkelerin sadık kalmak zorunda oldukları bazı ortak standartlar ya da minimum önlemler mevcuttur. Bunlar, tarafların konuyla ilgili uluslararası insan hakları araçları çerçevesinde üstlendikleri yükümlülükler uyarınca ortaya çıkan standartları ve asgari önlemleri içermektedir.

Sözleşmeyle getirilen diğer bir husus da yetki ve usullerin "hakkaniyet ilkesinin tesis edilmesini" sağlayacak olmasıdır. Hakkaniyet her bir taraf ülke tarafından ulusal mevzuatlarındaki ilgili ilkeler uyarınca uygulanacaktır. Ayrıca,

madde 21'deki müdahale önlemleriyle ilgili zorunlulukların ulusal mevzuatın belirlediği bir dizi ciddi suçla ilişkili olması konusundaki açık sınırlama, hakkaniyet ilkesinin uygulanması için açık bir örnektir.

4.4.3. Saklanan bilgisayar verilerinin hızlı bir biçimde korunması (m.16)

Avrupa Konseyi Siber Suç Sözleşmesi'nin en önemli özelliği, uluslararası ortamda siber suçlara ilişkin müşterek bir yaklaşım belirlemesidir. Birçok ülkede verinin muhafaza edilmesi yeni bir kavram olmakla beraber, bilgisayarlara ilişkili suçlara yönelik soruşturmalarda önemli bir role sahiptir[242]. Bu kapsamda suça yönelik eylem ve suçun sahibini belirlemede, taraf ülkeler arasında müşterek bir tutum meydan getirilmesi amacıyla saklanan bilgisayar verilerinin hızlı bir biçimde korunması konusuna açıklık kazandırılmıştır.

Verinin muhafazası, halihazırda depolanmış olan verinin, kalitesini veya durumunu değiştirecek veya bozacak her türlü şeyden korunması anlamına gelmektedir. Verinin muhafaza edilmesi ifadesi, verinin güvenli bir şekilde depolanma işleminin sürdürülmesi için kullanılmaktadır.

Veri muhafazasını gerekli kılan üç temel neden bulunmaktadır, l- bilgisayar verilerinin kolaylıkla değiştirilebilmesi; 2- bilgisayarlarla ilişkili suçların büyük çoğunluğunun bilgisayar sistemleri aracılığıyla yapılan iletişim yayınlarından kaynaklanması; 3- yasadışı içerik veya suça yönelik fiilin kanıtını taşıyan iletişimin muhafazasının, soruşturmalarda da delil özelliği taşıması.

16'ncı maddede ulusal yetkili mercilerin, özel bir cezai soruşturma ya da takibatla bağlantılı belirli saklı bilgisayar verilerinin hızlı bir biçimde korunması yönünde talimat vermelerini ya da buna benzer bir şekilde temin etmelerini sağlamayı amaçlamaktadır.

Paragraf 2'de ilgili tarafın korumayı bir talimat yoluyla yürürlüğe sokması durumunda, koruma talimatının, talimatı alan kişinin mülkiyetinde ya da kontrolü altında bulunan, belirtilen saklı bilgisayar verileri ile ilişkili olmasının gerektiği belirtilmiştir. Talimatı alan kişi yetkili mercilerin bu bilgisayar verilerinin

[242] Helvecıoğlu, 2004:289

bütünlüğünü, asgari 90 gün olmak üzere, gereken süre boyunca korumak ve saklamak zorundadır.

Paragraf 3'te ise ulusal mevzuatta belirlenecek bir süre için korunacak verilerin koruyucusuna ya da verileri koruma talimatı alan kişiye, koruma usullerini yerine getirmekle ilgili bir gizlilik yükümlülüğü getirilmektedir. İcra mercilerinin bu önlemi soruşturmanın şüphelisinin soruşturmadan haberdar olmaması ihtiyacını ve bireylerin gizlilik ihtiyacını karşılamaktadır.

4.4.4.Trafik verilerinin hızlı bir biçimde korunması ve kısmen ifşası (m.17)

Madde 17 ile, 16'ncı madde kapsamında trafik verilerinin korunmasıyla ilgili özel zorunluluklar getirilmekte ve belirlenen iletişimlerin yayınında diğer hizmet sağlayıcılarının katılıp katılmadığını belirlemek için bazı trafik verilerinin hızlı bir biçimde ifşasının sağlanması hedeflenmektedir.

Trafik bilgileri, özel bir hukuki rejime tabi olan bilgisayar verisi olup iletişim zincirinde, iletişimi başlangıcından varış noktasına kadar sürdüren bilgisayarlar tarafından oluşturulmaktadır. Trafik bilgilerinin içerisinde iletişimin başlangıç noktası, varış noktası, izlediği yol, saat, tarih, boyutlar, süre ve bu iletişimde kullanılan hizmet tipi (dosya transferi, e-posta gibi) bulunmaktadır.

Geçmişteki iletişimlerle ilgili saklı trafik verilerinin elde edilmesi, geçmişteki bir iletişimin kaynağını ya da varış noktasını belirlemek açısından büyük önem taşımaktadır. Bu bilgiler örneğin çocuk pornografisi dağıtan veya bilgisayar virüsü dağıtan kişileri saptamak açısından önemlidir.

Çoğu zaman bir iletişimin yayınlanmasında, birden fazla hizmet sağlayıcı yer almaktadır. Bu gibi durumlarda, her bir hizmet sağlayıcı, trafik bilgisinin bir kısmına sahip olabilir. Madde 17 ile birden fazla hizmet sağlayıcının, iletişimin yayınında yer aldığı durumlarda, bütün trafik verilerinin hızlı bir biçimde korunmasının tüm hizmet sağlayıcıları için geçerli olacağı ifade edilmektedir. Ancak maddede bu korumanın nasıl sağlanacağı belirtilmemekte olup, hukuk ve ekonomi sistemiyle uyumlu bir yol seçmek ulusal mevzuatlara bırakılmaktadır. Yetkili idareler tercih ederlerse her hizmet sağlayıcısına muhafaza emrini ayrı ayrı gönderebileceklerdir. Alternatif bir

yöntem de, kapsamı karmaşık olan iletişimin iletimine katıldıkları saptanan bütün hizmet sağlayıcılar için geçerli olacak tek bir talimat temin etmek olabilir.

Ayrıca, talimat emrini alan hizmet sağlayıcılarının, iletişim yayını esnasında hangi hizmet sağlayıcılarının yer aldığını tespit edecek kadar trafik verisini hızlı bir biçimde yetkili idarelere veya ilgili kişiye açıklamaları şart getirilmiştir.

4.4.5. Üretim talimatı (m.18)

Üretim talimatı, bir kişi ya da hizmet sağlayıcının mülkiyetinde olan bilgisayar verileri ve abonelik bilgileri ile ilgilidir.

Madde 18'in 1'inci paragrafında, tarafların yetkili idarelerini kendi topraklarında bulunan bir kişinin belirtilen depolanmış bilgisayar verisini sağlaması veya kendi topraklarında faaliyette bulunan bir hizmet sağlayıcının abone bilgilerini yetkili idareye vermesi için gerekli olan yasal düzenlemelerde bulunmasını öngörmektedir.

Üretim emri, söz konusu yasal düzenlemelerin uygulanmasına esneklik kazandırmakta ve özellikle İnternet hizmet sağlayıcılarının yetkililere kontrolleri altındaki verileri gönüllü olarak sunmalarında yasal bir dayanak sağlamaktadır.

Abonelik bilgileri ilke olarak, bir hizmet sağlayıcının idari bölümü tarafından hizmetlerine abone olan kişi ile ilgili olarak tutulan bilgidir. Abonelik bilgileri bilgisayar verileri biçiminde ya da kağıt üzerine tutulmuş kayıtlar gibi herhangi başka bir biçimde tutulabilir.

Soruşturmalarda abone bilgisine iki durumda ihtiyaç duyulmaktadır: l- abonenin hangi hizmetlerin kullandığının tespit edilmesi, 2- teknik adresin bilinmesi halinde kişinin tespit edilebilmesi için abonelik bilgilerinden yararlanılması.

4.4.6. Saklanan bilgisayar verilerinin aranması ve bunlara el konması (m.19)

Bu madde ile soruşturma ve takibatlarla ilgili olarak delil elde etme amacıyla saklı bilgisayar verilerinin aranması ve bu verilere el konmasına ilişkin ulusal yasaların modernleştirilmesi ve uyumlu hale getirilmesi amaçlanmaktadır.

Belgelerin ve kayıtların söz konusu olduğu klasik arama ortamında, arama kağıt üzerine mürekkep gibi maddi biçimde kaydedilmiş delillerin toplanmasından ibarettir. Soruşturmayı yürütenler bu tür kayıtlı delilleri arayıp, inceleyip ve maddi kayıtlara el koyup, fiziksel olarak alıp götürürler. Yeni teknoloji ortamında özellikle bilgisayar verileriyle ilgili olarak, delil elde etme amacıyla yapılan aramalarda da klasik aramanın birçok özelliği bulunmaktadır. Örneğin, verilerin toplanması arama esnasında ve o sırada mevcut olan veriler ile ilgili olarak gerçekleştirilmektedir. Arama yapmak için resmi bir makamdan yasal yetki alma koşulu, bilgisayar verilerinin delil elde etme amacıyla aranmasında da bulunmaktadır.

Ancak bilgisayar verileri söz konusu olduğunda, ek bazı usul hükümlere ihtiyaç duyulmaktadır. Böyle olmasının çeşitli sebepleri vardır. Bunların birincisi, verilerin maddi bir biçimde değil, elektromanyetik ortamda olması; ikincisi, verilerin bilgisayar teçhizatı yardımıyla okunabilir olmakla birlikte, onlara kağıt üzerindeki bir kayıt gibi el konulamaması, alıp götürülememesi; üçüncüsü, bilgisayar sistemlerinin birbirine bağlanabilme özelliğinden dolayı, verilerin doğrudan aramanın yapıldığı bilgisayarda değil, ama o sistemden kolayca erişilebilecek bir durumda olabilmesidir. Veriler, bilgisayarla doğrudan ya da İnternet üzerinden dolaylı olarak bağlantılı bir veri saklama cihazında bulunabilir. Bu durum aramayı verilerin gerçekte bulunduğu yeri içine alacak şekilde genişletmeye ya da geleneksel arama yetkilerini daha uyumlu ve hızlı bir biçimde kullanmaya izin verecek yasalara ihtiyaç gösterebilmektedir.

19'uncu maddenin 1'inci paragrafı uyarınca taraflar, kanunları uygulamakla yükümlü idareleri, bir bilgisayar sisteminde veya sistemin bir parçasında veya bağımsız bir saklama aracında (CD-ROM, disket) bulunan bilgisayar verisine erişimde bulunmak ve arama yapmak için yetkilendireceklerdir.

Paragraf 2'de, soruşturmayı yürütmekte olan mercilerin, gerekli verilerin başka bir bilgisayar sisteminde olduğuna dair yeterli kanıtların var olduğu durumlarda, arama ya da benzer şekilde erişimlerini bu bilgisayar sistemini ya da onun bir parçasını içine alacak şekilde genişletmelerine izin verilmektedir. Ancak diğer bilgisayar sistemi ya da sistemin parçası, taraf ülkenin ulusal sınırları içinde bulunmalıdır. Sözleşmede bir aramanın genişletilmesine nasıl izin verileceği ve

bunun nasıl gerçekleştirileceği belirtilmemektedir. Bu konu ulusal yasalara bırakılmıştır.

Bu Maddede, devletlerin olağan yasal yardımlaşma kanallarından geçmek zorunda kalmadan başka devletlerin ulusal sınırları içinde bulunan verileri aramasına ve bunlara el koymasına imkan tanıyan "sınır ötesi arama ve el koyma" konusuna değinilmemektedir. Bu konu, aşağıda, uluslararası işbirliğiyle ilgili bölümde ele alınmıştır.

Paragraf 3'de yetkili mercileri, paragraf l ya da 2 uyarınca aranmış ya da benzer şekilde erişilmiş bilgisayar verilerine el koymak ya da bunları benzer şekilde güven altına almak yönünde yetkilendirmeyle ilgili konular ele alınmıştır. Bunlar arasında bilgisayar donanımı ve bilgisayar verileri saklama ortamlarına el koyma yetkisi de bulunmaktadır.

Verilere el koyma ya da onları benzer şekilde güven altına almanın iki işlevi bulunmaktadır: l- verileri kopyalamak yoluyla delil elde etmek, ya da 2- verileri kopyalamak ve daha sonra orijinal versiyonlarını erişilmez kılmak ya da taşımak yoluyla verileri müsadere etmek. El koymak el konan verilerin nihai olarak silinmesi anlamına gelmemektedir.

Paragraf 4'de ise bilgisayar verilerinin aranmasını ve bunlara el konulmasını kolaylaştıracak cebri bir önlem getirilmektedir. Arama ve el koyma işlemlerinin bilgisayar sistemi bilgisine sahip olan kişilerce yapılması veya bu kişilere danışılarak işlemlerin gerçekleştirilmesini düzenlemektedir.

4.4.7. Bilgisayar verisinin gerçek zamanlı olarak toplanması

Sözleşmenin 20 ve 21'inci maddeleri, bir bilgisayar sisteminden iletilen belirli iletişimlerle bağlantılı trafik verilerinin gerçek zamanlı olarak toplanması ve içerik verilerine gerçek zamanlı olarak müdahale edilmesi ile ilgilidir. Maddelerde bu verilerin yetkili idare tarafından gerçek zamanlı olarak toplanması ve bunlara gerçek zamanlı olarak müdahale edilmesinin yanı sıra hizmet sağlayıcıların toplama ve müdahaleleri de ele alınmaktadır. Ayrıca gizlilik hükümlerine de yer verilmiştir.

Toplanabilen veriler iki türlüdür; trafik verileri ve içerik verileri. Trafik verileri sözleşmenin 1'inci maddesinde tanımlanmışken içerik verileri sözleşmede tanımlanmamıştır, ama iletişimin içeriği, yani iletişimin anlamı ve niyeti ya da iletişimle taşınan mesaj ya da bilgi anlamındadır.

4.4.7.1. Trafik verilerinin gerçek zamanlı olarak toplanması (m.20)

Madde 20'de soruşturmalar ve takibatlarda kullanılmak üzere trafik verisinin gerçek zamanlı olarak toplanması ve kaydedilmesi için gerekli düzenlemelerin yapılması öngörülmektedir.

Söz konusu madde uyarınca, trafik verisinin ilgili taraf ülkenin toprakları içerisindeki belirtilen iletişim ile bağlantısının bulunması gerekmektedir. İletişimin belirtilmiş olması şartı, trafik bilgisinin toplanması için büyük önem taşımaktadır.

Yine anılan maddenin 2'nci paragrafına göre, taraflar yetkili mercilerinin trafik verilerini teknik imkanlar yoluyla toplamak ve kaydedilebilmesini sağlamak zorundadır. Maddede toplamanın teknolojik olarak nasıl gerçekleştirileceği belirtilmemekte ve teknik açıdan hiçbir yükümlülük tanımlanmamaktadır.

Ayrıca, söz konusu paragraf idarenin telekomünikasyon sistemlerindeki verilere ancak bir hizmet sağlayıcının yardımı aracılığıyla müdahale edebildiği ya da hizmet sağlayıcının en azından bilgisi olmadan, gizli bir biçimde müdahale edemediği durumlarda uygulanabilmektedir.

Paragraf 3'te ise, trafik verilerinin gerçek zamanlı olarak toplanmasına ilişkin önlemlerin uygulanmasına yönelik bilgilerin İnternet servis sağlayıcıları tarafından gizli tutulmasına ilişkin yükümlülükler getirilmektedir.

4.4.7. 2. İçerikle ilgili bilgilere müdahale (m.21)

Geleneksel olarak, içerik verilerinin telekomünikasyon sisteminin (örneğin telefon konuşmaları) sağlamış olduğu imkanlardan faydanılarak elde edilmesi, uzun zamandan beri kullanıla gelen bir yoldur. Yine bilgisayar iletişimleri de suça ait delil toplanmasında önemli bir katkıya sahip olmaya başlamış ve ileride bu katkının daha da artacağı görülmektedir. Ancak, bilgisayar teknolojisi, yazılı metin, görsel imaj ve ses biçiminde çok büyük miktarlarda veriyi iletmeye imkan sağladığı için yasadışı

içeriğin (örneğin çocuk pornografisi) dağıtımı yoluyla işlenen suçlar için daha büyük bir potansiyele sahiptir.

Bu maddenin çoğu unsuru 20'nci maddenin unsurlarıyla benzerdir. Bu nedenle yukarıda belirlenen trafik verilerinin toplanması ve kaydedilmesi, işbirliği ve yardım yükümlülüğü ve gizlilik yükümlülüğü ile ilgili bütün değerlendirmeler içerik verilerine müdahale için de aynen geçerli olacaktır.

4.5. Yargı Yetkisi (m.22)

Sözleşmenin "Yargı Yetkisi" başlıklı 3'üncü kısmı, 22'nci maddesinde taraf ülkelerin suça yönelik fiillerin yargılanması ile ilgili yükümlülüklere yer verilmektedir.

Paragraf 1'de, yargı alanı belirlenmekte ve taraf olan ülkenin kendi toprakları içerisinde işlenen suçları yargılama yükümlülüğü ele alınmaktadır.

Anılan paragrafın (a) şıkkı mülkilik ilkesine dayanmaktadır. Bu ilkeye göre, tarafların her birinin bu Sözleşmede tesis edilen suçlardan kendi ulusal sınırları içinde işlenen suçları cezalandırması gerekmektedir. Örneğin, hem bir bilgisayar sistemine saldıran kişi hem de saldırının kurbanı olan sistem belli bir taraf ülkenin sınırları içindeyse, ve saldırgan olmasa da saldırıya uğrayan bilgisayar sistemi bu sınırlar içindeyse, ilgili taraf ülke mülki yargı yetkisine sahiptir.

Yine söz konusu paragrafın (b) ve (c) şıkları mülkilik ilkesinin değişik bir şekline dayanmaktadır. Bu şıklarda taraflardan her birinin kendi bandırasını taşıyan gemilerde ve kendi yasaları çerçevesinde kayıtlı bir uçakta işlenen suçlar için cezai yargı yetkisini tesis etmesi şart koşulmaktadır. Bu şekildeki gemi ve uçaklar genellikle ulusal sınırların bir uzantısı olarak kabul edildiği için, bu yükümlülük birçok ülkenin mevzuatında zaten genel bir husus olarak ele alınmaktadır. Bu tür yargı yetkisi gemi ya da uçak, suçun işlenmesi esnasında ulusal sınırlar içinde olmadığı, bunun sonucunda da Paragraf 1'in (a) şıkkının yargı yetkisi iddia etmek için temel oluşturmadığı durumlarda çok yararlıdır. Suç, bayrağın sahibi Taraf Ülkenin ulusal sınırlarının dışında işlenirse bu koşulu engelleyerek yargı yetkisini kullanacak başka bir devlet olmayabilir. Ayrıca, başka bir devletin karasularından ya da hava sahasından geçmekte olan bir gemi ya da uçakta bir suç işlenirse bu devlet

yargı yetkisini işletmekte ciddi pratik engellerle karşılaşabilir. Bu nedenle yargı yetkisinin gemi ya da uçağın kayıtlı olduğu Devlete ait olması yararlıdır.

Paragrafın (d) şıkkında ise tabiyet ilkesi ele alınmıştır. Tabiyet ilkesi, bir devletin vatandaşları kendi ülke sınırlarının dışında olsalar bile, kendi ülkelerine ait yasalara uymak zorunda olmalarını ifade etmektedir. Yani paragrafın (d) şıkkına göre, taraflar, vatandaşları kendi ülkeleri dışında bir suç işlemeleri durumunda, söz konusu suç, suçun işlendiği ülkenin yasalarına göre de suç sayılıyorsa ya da herhangi bir devletin yargı yetkisinin içerisine girmiyorsa, o vatandaşı yargılamakla yükümlüdür.

4.6. Uluslararası İşbirliği

4.6.1. Uluslararası işbirliğine ilişkin genel ilkeler

Avrupa Konseyi Siber Suç Sözleşmesinin bir diğer özelliği de uluslararası işbirliğine ilişkin genel kurallar belirlemesidir. Sözleşmede ülkelerin işbirliğini geliştirmeleri ve bilgi akışını engelleyecek uygulamalardan kaçınmaları öngörülmektedir. Söz konusu işbirliği bilgisayar sistemleri ve veri ile ilişkili her türlü suçu kapsayacak şekilde sağlanmalıdır, işbirliği hem bilgisayar sistemleri ve veri ile ilişkili suça yönelik fiillerde hem de suç hakkındaki elektronik formda delillerin toplanması konularında yapılacaktır.

4.6.2. Suçluların iadesine ilişkin ilkeler (m.24)

24'üncü maddenin 1'inci paragrafında, iade yükümlülüğünün sadece işbu Sözleşmenin 2-11'inci maddeleri çerçevesinde tanımlanan, her iki taraf ülkenin yasalarında en az bir yıllık azami süreyle özgürlükten mahrum bırakma ya da daha ağır nitelikli bir cezayla cezalandırılabilir olan cezalar için geçerli olduğu belirtilmektedir. Sözleşmeyi kaleme alanların bir eşik ceza getirmeye karar vermelerinin nedeni, Sözleşme uyarınca, taraf ülkeler bazı suçları daha kısa azami hapis süreleriyle cezalandırabilirler (örneğin madde 2 - yasadışı erişim ve madde 4 - verilere müdahale). Bu açıdan, Sözleşmeyi kaleme alanlar madde 2-11'de tanımlanan suçların her birinin başlı başına iadeye konu olabilen suçlar olarak değerlendirilmesinin şart koşulmasının uygun olacağına inanmaktadır. Bu sebeple,

bir suçun, Avrupa İade Konvansiyonu'nun (ETS No. 24) 2'inci maddesinde öngörüldüğü gibi, bu suç için verilebilecek azami cezanın en az bir yıl hapis olması durumunda iadeye konu olabilen suçlar olarak kabul edilmesi şeklinde genel bir şart getirilmesi üzerinde anlaşmışlardır. Bir suçun iadeye konu olabilen bir suç olup olmadığının belirlenmesi o an ele alınmakta olan belli bir durumda verilen gerçek cezaya değil, iade talebinde bulunulan ihlal için yasal olarak verilebilecek azami süreye bağlıdır.

Yine taraf ülkelerin her iade talebinin olumlu sonuçlanma imkanı olmamakla birlikte, iade seçeneğinin varlığının garanti altına alınması amacıyla, iadesi mümkün olan suçlar gelecekte yapılacak iade anlaşmalarına da dahil etmekle yükümlü kılınmışlardır.

Ayrıca, maddenin 5'inci paragrafına göre, talebin yapıldığı tarafın geçerli anlaşma ve yasalardaki bütün hüküm ve şartların yerine getirilmiş olduğu konusunda tatmin olmadığı durumlarda iadeyi gerçekleştirmek zorunda olmadığı belirtilmektedir.

4.6.3. Yardımlaşmaya ilişkin genel ilkeler

Yardımlaşmayı sağlama yükümlülüğü ile ilgili genel ilkeler paragraf 1'de belirlenmiştir. Buna göre taraflar arasında işbirliği, mümkün olan en geniş şekilde sağlanacaktır. Dolayısıyla yardımlaşma ilke olarak geniş olacak ve yardımlaşmayı engelleyen unsurlar sıkı bir biçimde sınırlandırılacaktır, ikinci olarak, 23'üncü maddede de belirtildiği gibi, işbirliği yükümlülüğü ilke olarak hem bilgisayar sistemleri ve verileriyle bağlantılı suçlar hem de elektronik ortamda bir cezai suçun delillerinin toplanması için geçerli olacaktır. Bu geniş suç grubuyla ilgili olarak işbirliği yükümlülüğü getirilmesinin nedeni, kolay ve elverişli uluslararası işbirliği mekanizmalarına duyulan ihtiyacın, bu kategorilerin her ikisi için de mevcut olmasıdır. Ancak, madde 34 ve 35'te tarafların bu önlemlerle ilgili olarak farklı uygulama kapsamları belirlemelerine izin verilmiştir.

Bilgisayar verileri son derece geçici niteliktedir. Birkaç tuşa basılarak ya da otomatik programların çalışması sonucunda veriler silinerek bir suçun failine kadar izlenmesi imkansız hale getirilebilir ya da kritik önemdeki suç delilleri yok edilebilir.

Paragraf 3'te amaçlanan şey, yardım alma süresini hızlandırmayı kolaylaştırarak, kritik bilgi ya da delillerin kaybolmasını önlemektir.

4.6.4. Anında iletilen bilgiler (m.26)

Sözleşmeye taraf bir ülkenin belli bir cezai soruşturma ya da takibatta başka bir taraf ülkenin işine yarayacağına inandığı bilgilere sahip olduğu ve soruşturma ya da takibatı yürüten ülkenin bunun varlığını bilmediği durumlar yaşanmaktadır. Bu gibi durumlarda, yardımlaşma talebinin yapılması söz konusu olmamaktadır. Paragraf l'de bilgiye sahip olan ülkeye, bu bilgiyi izin almaksızın diğer ülkeye iletme hakkı verilmektedir.

Paragraf 2'de ise, bazı durumlarda tarafların bilgiyi ancak hassas bilgiler gizli tutulacaksa ya da bilginin kullanımıyla ilgili başka şartlar ileri sürülebilirse anında ileteceği olgusu ele alınmaktadır. Daha özel olarak, gizlilik, bilginin açıklanması durumunda bilgiyi veren ülkenin önemli çıkarlarının tehlikeye gireceği, örneğin bilgi toplama yönteminin niteliğinin ya da bir suç grubu ile ilgili yürütülen soruşturmanın gizlenmesine ihtiyaç duyulduğu durumlarda önemli bir husus olarak görülecektir.

4.6.5. Uluslararası anlaşmaların yürürlükte bulunmadığı durumlarda gelen yardım taleplerine ilişkin usuller (m.27)

Bu madde, uygulamada karşılıklı yardım anlaşmaları, kanunlar ve düzenlemelerin bulunmadığı durumlarda geçerli olacak hükümleri içermektedir.

Karşılıklı yardım taleplerini alma ve gönderme eylemlerinden sorumlu olacak merkezi idareler kurulacak, taraflar imza veya onay esnasında Genel Sekreterliğe kurulan idarelerin isim ve adreslerini bildireceklerdir.

Yapılacak talepler, yardım talep edilen ülkenin iç hukuk kuralları ile uyumlu olmak zorundadır. Yapılan karşılıklı yardım talepleri, taleplerin siyasi bir suç ile bağlantısının olması veya talepte bulunulan ülkenin, güvenlik, birlik, kamu düzeni veya diğer hayati çıkarlarına zarar verdiği sonucuna varılır ise reddedilecektir. Yardım talebi, talepte bulunulan ülkenin yürüttüğü soruşturmalara zarar veriyor ise ertelenebilecektir. Gerekli değişiklikler yapılması kaydıyla yardım talebi yeniden gözden geçirilerek, yardım kısmen de olsa, sağlanabilecektir.

Yardım talebinde bulunan ülke talebe ilişkin sonuç hakkında bilgilendirilecektir. Talebin reddi veya ertelenmesi halinde tüm nedenler ilgili tarafa sunulacaktır.

Taraflar yardım talebine konu bilgileri gerekli ise, gizli tutmanın yanı sıra soruşturma ve takibat dışında kullanmamakla da yükümlüdürler. Bilgi gönderilecek olan taraf belirtilen koşullara uyum sağlayamayacak ise, bunu karşı tarafa bildirmekle yükümlüdür.

4.7. Özel Hükümler

4.7.1. Saklanan bilgisayar verilerinin hızlı bir biçimde korunması (m.29)

Anılan madde, 16'ncı maddede getirilen ulusal düzeydeki mekanizmanın uluslararası düzeydeki eşdeğeri bir düzenlemedir. Bu hükme göre taraflar, bir diğer taraf ülkenin topraklarında depolanan verinin hızlandırılmış muhafazasını o ülkeden talep edebileceklerdir.

Paragraf 1'e göre, verileri elde etmek için bir yardımlaşma talebinin hazırlanması, iletilmesi ve uygulanması için gerekli zaman dilimi içerisinde bu verilerin değiştirilmemesini, taşınmamasını ve silinmemesini sağlamak üzere talebin yapıldığı tarafın ulusal sınırları içinde bulunan saklı verilerin bir bilgisayar sistemi aracılığıyla hızlı bir biçimde korunması için tarafların talepte bulunmasına izin verilmektedir.

Paragraf 2'de ise, bu madde uyarınca yapılacak koruma taleplerinin içeriği belirtilmiştir. Talep, verinin muhafazası için gerekli olan asgari bilgiyi içermeli, muhafaza talebinde bulunana idare ve konu olan suçu tanımlamalıdır. Verilen bilgilerde muhafazanın gerekliliği ifade edilecek ve karşılıklı yardım talebinde bulunulacaktır.

Son paragrafta, Tarafların bu madde uyarınca korunan verilerin, ifşalarının istendiği resmi bir yardımlaşma talebinin alınması sırasında en az 60 gün tutulmasını ve talebin alınmasından sonra da tutulmaya devam edilmesini sağlamaları şart koşulmaktadır.

4.7.2. Korunan Trafik Verilerinin Hızlı Bir Biçimde İfşası (m.30)

Bu madde ile, madde 17'de ulusal düzeyde tesis edilen yetkinin uluslararası düzeydeki uygulanması ele alınmaktadır. Sözleşmenin 30'uncu maddesine göre, suçun işlendiği taraf ülkenin talebi üzerine, talebin yapıldığı taraf, iletimi kaynağına kadar izleyerek suçun failini bulmak ve kritik delillerin yerini belirlemek üzere kendi bilgisayarları aracılığıyla gerçekleştirilen bir iletimle ilgili trafik verilerini korumakla yükümlü tutulmuştur. Talebin yapıldığı taraf, talebi yapan tarafa diğer ülkedeki hizmet sağlayıcının kimliğini ve bu ülkeden yapılan iletişimin izlediği yolu belirlemeye yetecek miktarda trafik verisini hızlı bir biçimde sunmak zorundadır.

Maddenin 2'nci paragrafına göre, talebin yapıldığı taraf, trafik verilerini açıklamayı sadece açıklamanın egemenliğine, güvenliğine, kamu düzenine ya da diğer temel çıkarlarına zarar vereceğini, ya da suçun siyasi bir suç ya da siyasi bir suçla bağlantılı bir suç olduğunu düşündüğü durumlarda reddedebilir.

4.7.3. Saklanan bilgisayar verilerine erişilmesine ilişkin yardımlaşma (m.31)

Sözleşmeye göre, sözleşmeyi imzalayan ülkelerin, diğer bir tarafa fayda sağlamak amacıyla, kendi topraklarında yer alan bir bilgisayar sisteminde depolanan veriyi açıklamak, erişim sağlamak ve araştırmak yeteneğine sahip olmasını öngörmektedir. Depolanan bilgiye erişim konusunda karşılıklı yardım talebi yapıldığında, ilgili taraf talebe cevap verirken uygulamadaki antlaşmalar, düzenlemeler ve karşılıklı yardım konusunu düzenleyen iç hukuk kurallarına uygun olarak davranacaktır.

Taraflardan birinin bir başka taraf ülkede bulunan bilgisayar verisine tek taraflı olarak erişimine, karşılıklı yardım talebine gerek olmadan olanak sağlanması iki durumda söz konusu olmaktadır: 1- erişilen verinin kamu erişimine açık olması, 2- taraflardan birinin kendi toprakları dışında bulunan bir veriye kendi topraklarında bulunan bir bilgisayar sistemi vasıtasıyla erişim sağladığında veya bu bilgiyi aldığında , bu sistem ile veriyi ilgili tarafa açıklama yetkisi bulunan kişinin kanuni ve gönüllü rızası alınmış olmasıdır.

Ancak, kanunen veriyi açıklama yetkisine sahip olan kişinin kimliğine uygulamadaki kanunlar çerçevesinde açıklık kazandırılması gerekmektedir, örneğin,

bir kişinin e-postası, servis sağlayıcısı tarafından bir başka ülkede tutuluyor olabilir veya bir kişi veriyi kasıtlı olarak başka bir ülkede saklıyor olabilir. 32'nci madde uyarınca bu kimselerin, yetkililerin verilere erişim sağlamalarına izin vermeleri ya da gönüllü olarak veriyi açıklamaları gerekmektedir.

4.7.4. Trafik verilerinin gerçek zamanlı olarak toplanması konusunda yardımlaşma (m.33)

Genellikle, önem arz eden trafik verileri iletim zincirindeki bir servis sağlayıcı tarafından korunmadan önce otomatik olarak silindiğinden soruşturmayı yürütenler önceki iletimlerin izini sürerek bir iletişimi kaynağına kadar izleyebileceklerinden emin olamazlar.

Bu nedenle, bütün taraf ülkelerde soruşturmayı yürüten merciler için diğer taraf ülkelerde bilgisayar sistemleri aracılığıyla iletilen yayınlarla ilgili trafik verilerini gerçek zamanlı olarak elde etme yeterliliğine sahip olmak önemlidir. Dolayısıyla, Madde 33 uyarınca, bütün taraflar, diğer taraflar için trafik verilerini gerçek zamanlı olarak toplamakla yükümlüdür. Bu madde tarafların bu konularda işbirliğine gitmesini şart koşmakla birlikte, diğer hususlarda olduğu gibi burada da mevcut yardımlaşma biçimlerine saygı gösterilmektedir. Dolayısıyla bu işbirliğinin sağlanmasında geçerli olacak hükümler ve şartlar, genellikle cezai konularda hukuki yardımlaşmayı düzenleyen geçerli anlaşmalar, düzenlemeler ve yasalarda belirtilen hükümler ve şartlardır.

4.7.5. İçerikle ilgili verilere müdahale edilmesi konusunda yardımlaşma (m.34)

Müdahalenin özel hayatın gizliliğine de tecavüz edici niteliği sebebiyle, içerik verilerine müdahale için yardımlaşma sağlama yükümlülüğü sınırlandırılmıştır. Yardımın, tarafların geçerli anlaşma ve yasalarının izin verdiği ölçüde sağlanması düşünülmüştür. İçerik verilerine müdahale konusunda işbirliğinin sağlanması, yardımlaşma uygulamasının yeni şekillenmekte olan bir alanı olduğu için yardım sağlama yükümlülüğünün kapsamı ve sınırları konusunda mevcut yardımlaşma rejimlerine ve ulusal yasalara uyulmasına karar verilmiştir.

4.7.6. 24/7 Ağı (m. 35)

Bilgisayar sistemi kullanılarak işlenen suçlarla etkin bir biçimde mücadele etmek ve elektronik biçimdeki delillerin etkin biçimde toplanması büyük öneme sahiptir. Bu nedenle, bilgisayar çağının tehditlerine etkin bir biçimde cevap verebilmek için polis işbirliği ve yardımlaşma biçimlerine yeni kanalların eklenmesi gereklidir. 35'inci madde uyarınca bütün taraflar, günde 24 saat, haftada 7 gün ulaşılabilen bir irtibat noktası belirlemek zorundadır. Böylelikle soruşturmalarda ani yardım ihtiyacı olduğunda, bilgisayarlarla ilgili suçlara yönelik olarak hizmet verecek etkin bir ağ kurulmuş olacaktır.

4.8. Diğer Hükümler

Sözleşmenin 36 ile 48'inci Maddeleri arasındaki hükümleri, sözleşmenin imzalanması, yürürlüğe girmesi, sözleşmeye katılım ve sonuçlar, hakların saklı tutulması, anlaşmazlıkların çözülmesi, gibi konuları içermektedir.

4.9. Sonuç

23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suç Sözleşmesi uluslararası alanda siber suçlar konusunda devletler nezdinde en kapsamlı uzlaşmayı sağlayan antlaşmadır. Ayrıca bilgisayar teknolojisi ve ceza hukuku konusunda ilk uluslararası belge olma niteliğine haizdir. Sözleşmede ele alınan konular, telif hakları ihlalleri, bilgisayarlarla ilgili sahtecilik fiilleri, çocuk pornografisi, ağ güvenliği ihlalleri, siber suçla mücadelede kullanılacak olan yetki ve prosedürlerden oluşmaktadır.

Sözleşmenin amacı, ortak bir ceza politikasının ve yine ortak suç tanımlarının oluşturulması ile toplumun siber suça karşı korunması, soruşturma yöntemlerinin tanımlanması ve uluslararası işbirliğinin geliştirilmesi olarak sıralanmıştır.

Siber Suç Sözleşmesi yaklaşık dört yıl süren uzun bir çalışmanın sonucu olarak ortaya çıkmış olmasına rağmen, sivil toplum kuruluşlarından ve konuyla ilgili sektörlerden pek çok eleştiriye maruz kalmıştır.

Anlaşmanın getirmiş olduğu düzenlemelere getirilen eleştiriler genelde, anlaşmada ortaya konulan araçların uygulanmasıyla, temel insan haklarına

gelebilecek muhtemel zararları üzerinde yoğunlaşmaktadır. Ancak, anlaşma incelendiğinde, suçla ilgili araştırmanın gereksinimleri ve bireysel haklar arasında hassas bir denge kurulacak şekilde hazırlanmış olduğu anlaşılır.

Bir başka eleştiri ise sözleşmenin hazırlık aşamasında yeterli oranda sivil toplum örgütlerinin ve konuyla ilgili sektörlerin görüşlerinin alınmamasıdır.

Gerçekten sözleşmenin son halini almasına kadar geçen sürede pek çok sayıda taslak yayınlanmıştır, ilk taslak 2000 yılında yayınlandığında bu taslağa birçok eleştiri ve birçok katkı yapma isteği yöneltilmiştir. Fakat sözleşmenin son hali itibariyle bu eleştirilerden ve katkılardan pek etkilenmediği gözlemlenmiştir. Ayrıca Avrupa Konseyi'nin bu tarz belgeleri katılımcı bir süreç içerisinde oluşturma geleneği bulunmaktadır. Bu tip anlaşmalar söz konusu olduğunda Avrupa Konseyi, tarafların katkılarıyla sözleşmeleri oluşturmaktadır. Ancak Siber Suç Sözleşmesinde bu süreç işletilmediğinden dolayı bu yönde pek çok eleştiriye maruz kalmıştır.

Bununla birlikte, anlaşma, imzalayanlara belirli olaylarda ihtirazi kayıt koyma konusunda olanak sağlamaktadır. Fakat yine tarafları sözleşmenin kapsamlı bir şekilde uygulanması için teşvik etmektedir.

Sözleşmede dikkat çeken önemli konulardan birisi, sözleşmenin siber suçun bir bölümünün dışında bir çok farklı konuyu kapsamına dahil etmesidir. Yani sözleşmenin içerisine ticaret de, veri güvenliği de ve diğer pek çok konuda girmektedir. Ön plana çıkan nokta Siber Suç Sözleşmesinin usule ilişkin hükümleridir. Sözleşmenin ele aldığı konulardan, telif hakkı ihlalleri, veri ağ güvenliği, bilgisayarlarla ilgili sahtecilik suçları, içerik suçları, sözleşmenin 14'üncü maddesini yani Sözleşmenin üçte birlik kısmını oluşturmaktadır. Geri kalan üçte ikilik kısmı siber suçla mücadelede kullanılan yetki ve prosedürlerdir.

Avrupa Konseyi daimi üyeliğine rağmen, Türkiye anlaşmayı henüz imzalamamıştır. Türkiye'nin bu durumu, henüz siber suçların en ağır yönleriyle karşılaşmamış olması ve bu nedenle anlaşmayı imzalamadan önce düşünmek için yeterli zamanı olmasından kaynaklanmaktadır. Ancak Adalet Bakanlığı tarafından bir komisyon oluşturulmuş, Avrupa Konseyi Siber Suç Sözleşmesinde yer alan hükümlerede yer verilecek şekilde Bilişim Ağı Hizmetlerinin Düzenlenmesi ve

Bilişim Ağı Kullanılarak İşlenen Suçlar Hakkında Kanun Tasarısı çalışmalarına başlanmıştır. Buradan anlaşılan Türkiye gerekli alt yapıyı hazırladıktan sonra bu sözleşmeyi imzalamayı düşündüğüdür.

5. TÜRK HUKUKUNDA SİBER SUÇLAR

5.1. Siber Suçların Türk Hukuk Sistemine Girişi ve Düzenlenen Suç Tiplerinin Sınıflandırılması

5.1.1. Siber Suçların Türk Hukuk Sistemine Girişi

80'li yıllarla beraber kişisel bilgisayarların kullanımının Dünya'da hızlı bir şekilde artmaya başlaması, bununla beraber 90'lı yıllarda da bilgisayarların birbirine bağlanarak kendi aralarında veri transferini gerçekleştirebilecekleri teknolojinin geliştirilmesiyle birlikte, ülkemizde de bilgisayarın kullanılması yaygınlaşmaya başlamıştır.

Dünya'da, bilgisayar ve bilgisayar ağlarının kullanımının yaygınlaşmasıyla beraber bir takım hukuki sorunların ortaya çıkması sonucunda, gelişmiş ülkelerin bu alanda işlenen suçları cezasız bırakmama düşüncesiyle başlatmış oldukları mevzuat çalışmaları, Türk kanun koyucularının da harekete geçmesini sağlamış ve siber suçlar konusunda düzenleme yapmaya sevk etmiştir.

Türk hukukunda siber suçlara ilişkin ilk düzenleme, 6.6.1991 tarih ve 3756 sayılı Kanunun 20'nci maddesi ile 765 sayılı TCK'nın ikinci kitabına "Bilişim Alanında Suçlar" adıyla 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir bap ilave edilmesidir. Bu babtaki suçlar, 1989 tarihli Türk Ceza Kanunu Tasarısından hemen hemen hiç bir değişikliğe uğramadan alınmıştır[243].

Kanun koyucu TCK'da yapılan değişikliğin ardından, güncel gereksinimleri karşılamak ve karşılaştırmalı hukukta yapılan düzenlemelere paralel düzenlemeler yaparak ülke mevzuatını uyumlaştırmak adına 5846 sayılı Fikir ve Sanat Eserleri Kanununda 7.6.1995 tarih ve 4110 sayılı kanunla değişiklik yapmıştır. Bu değişiklikle "Herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu

[243] Tasarının bu bölümü oluşturulurken sonradan (1.3.1993 tarihinde) kanunlaşan Fransız Ceza Kanunu Tasarısından faydalanılmıştır.

doğurması koşuluyla bunların hazırlık tasarımları" da "eser" sayılarak, bilgisayar programlarına yönelik bu Kanun kapsamındaki fiillerde suç sayılmıştır[244].

15.01.2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın geçerliliği kabul edilmiş ve anılan kanunun 17'nci maddesi ile sahte elektronik sertifika yapılması ve kullanılması suç olarak kabul edilmiştir.

Son olarak 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Kanunda (YTCK) siber suçlar, "Bilişim Alanında Suçlar" adıyla ikinci kitabın Topluma Karşı Suçlar başlıklı Üçüncü Kısımının 10'uncu Bölümünde 4 madde (m.243-244-245-246) halinde düzenlenmiştir. Yine YTCK ile birtakım suçların bilişim sistemleri aracılığıyla işlenmesi suçun ağırlaştırıcı sebebi olarak kabul edilmiştir.

5237 sayılı Kanunun yürürlükte olması hasebiyle, çalışmamızda bu kanunda düzenlenen suçlar detaylı bir şekilde incelenecek, eski TCK'nun da yer alan siber suçlara ilişkin düzenlemelere ise ilgili bölümlerde değinilecektir.

5.1.2. 5237 Sayılı Yeni Türk Ceza Kanununda Düzenlenen Siber Suçların Sınıflandırılması

5237 sayılı YTCK'da siber suçlara ilişkin düzenlemeler, genel olarak 765 sayılı TCK'nunda yer alan düzenlemelere benzer şekilde fakat daha kapsamlı olarak "bilişim sistemlerine karşı suçlar" ve "özel hayatın gizli alanına karşı suçlar" bölümlerinde düzenlenmiştir. Yine bunların yanında 5237 sayılı YTCK'nın bazı bölümlerinde bilişim sistemleriyle işlenmesi mümkün olan suçlara yer verilmiştir. Buna göre 5237 sayılı YTCK'da siber suç olarak adlandırılabilecek suç çeşitlerinin yanı sıra bilişim sistemi aracılığıyla işlenebilecek ancak sadece siber suç olarak tanımlanamayacak suç tipleri de mevcuttur[245].

Bilişim alanında suçlar bölümünde, "bilişim sistemine hukuka aykırı olarak girme ve sistemde kalma suçu"[246] (m.243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m.244), " banka veya kredi kartlarının kötüye kullanılması"

[244] 3.3.2004 tarih ve 5101 sayılı Kanunla, 5846 sayılı Kanun'da siber suçları ilgilendiren değişiklikler yapılmıştır.
[245] Dülger, 2004:114.
[246] 243'üncü madde, eski TCK'nında düzenlenmeyen bir durumu şuç olarak kabul etmektedir.

(m.245) ve "tüzel kişiler hakkında güvenlik tedbiri uygulanması" hususları (m.246) düzenlenmiştir.

Özel hayatın gizli alanına karşı suçlar bölümünde ise "kişisel verilerin kaydedilmesi" (m.135); "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" (m.136) ve verilerin yok edilmesi (m.138) suçlarına yer verilmiştir.

Son olarak, 5237 sayılı TCK'nın bazı bölümlerinde siber suçları da kapsayan suç tiplerine yer verilmiştir. Bunlar, "haberleşmenin gizliliğini ihlal suçu" (m.132), "haberleşmenin engellenmesi suçu" (m.124), "hakaret suçu" (m.125), "bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçu" (m. 142 fkr.2 b. "e"), "bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık suçu" (m.158 fkr.1 b. "f") ve "müstehcenlik suçu" dur (m.226).

5.1.3. 765 Sayılı Türk Ceza Kanunu ile 5237 Sayılı Yeni Türk Ceza Kanununda Düzenlenen Siber Suçların Karşılaştırılması

765 sayılı TCK'da yer alan siber suçlar ile YTCK'da düzenlenen siber suçlar yukarıda kısaca belirtilmiştir. Buna göre söz konusu kanunların siber suçlar yönünden karşılaştırılması aşağıdaki gibidir:

- TCK m.525 a/1 YTCK m.135, m.136
- TCK m.525 b/1 YTCK m.244/1-2
- TCK m.525 b/2 YTCK m.244/4, m.245, m.158 fkr.1 b. "f", m. 142 fkr.2 b. "e"

YTCK'nın 243'üncü maddesinde düzenlenen "bilişim sistemine hukuka aykırı olarak girme ve sistemde kalma suçu" 765 sayılı TCK'da yer almayan yeni bir suçtur.

Ayrıca YTCK'da düzenlenen "kişisel verilerin kaydedilmesi" (m.135); "kişisel verileri hukuka aykırı olarak verme veya ele geçirme" (m.136); "banka veya kredi kartlarının kötüye kullanılması" (m.245); "bilişim sisteminin kullanılması yoluyla işlenen hırsızlık" (m. 142 fkr.2 b. "e") ve "bilişim sisteminin kullanılması yoluyla işlenen dolandırıcılık " (m.158 fkr.1 b. "f") suçları, 765 sayılı TCK'dan farklı bir şekilde bağımsız suç tipleri olarak düzenlenmişlerdir.

Yine 765 sayılı TCK'nın 525 a/2 maddesinde düzenlenen suç tipine yapılan eleştiriler dikkate alınarak YTCK'da yer verilmemiştir.

YTCK ile getirilen bir başka yenilik ise verilerin ele geçirilmesinin suçun unsuru olmaktan çıkartılmış olmasıdır. Yeni düzenlemeye göre bilişim sistemine hukuka aykırı olarak girilmesi, suçun oluşabilmesi için yeterli sayılmıştır.

5.2. 5237 Sayılı Türk Ceza Kanununda Düzenlenen Siber Suçlar

5.2.1. Bilişim Sistemine Girmek ve Orada Kalmaya Devam Etmek Suçu (YTCK m.243)

5.2.1.1. Genel Olarak

Türk hukukunda oldukça yeni bir düzenleme olan bu maddeyle kanun koyucu, bilişim sistemine hukuka aykırı olarak girme ve orada kalmaya devam etmeyi suç olarak kabul etmektedir. Kanun koyucunun böyle bir suçu düzenlemesinin bir nedeni de, Avrupa Konseyi Siber Suç Sözleşmesinin 2'nci maddesinde yer alan ancak 765 sayılı TCK'da tam olarak karşılığı olmayan, "yasadışı erişim" olarak da adlandırılabilecek düzenlemeyle bir paralellik sağlanması[247] olsa da, bu suçun oluşabilmesi için öngörülen "orada kalmaya devam etme" unsuru sebebiyle söz konusu sözleşmenin 2'nci maddesinde düzenlenen "yasadışı erişim" suç olmaktan çıkarılmıştır[248].

5.2.1.2. Korunan Hukuki Yarar

Bu suçla ilk olarak korunan değer, siber suçların düzenlendiği kısım başlığından da anlaşılacağı üzere toplum düzeninin korunmasıdır. Daha sonra, bilişim sistemlerinin güvenliğinin sağlanmasıdır. Bilişim sistemlerine yasadışı erişimin önlenmesiyle, sistemi kullananların farklı türdeki menfaatleri korunmaktadır. Bu menfaatlerin başlıcaları, kullanıcıların özel hayatlarının gizliliğinin korunması, özel hayatın dokunulmazlığı, kurumların ihtiyaç duyduğu

[247] Yazıcıoğlu, 2004:172-185.
[248] 243'üncü maddenin birinci fıkrasının ilk hali "giren veya kalmaya devam eden" şeklinde düzenlenmişken TBMM Genel Kurulunda yapılan değişiklikle "veya" ibaresi "ve" olarak değiştirilmiştir.

güvenlik duygusu gibi farklı hukuki yararlardır[249]. Ayrıca söz konusu bilişim sistemleri vasıtasıyla (e-posta servisleri vs.) bireylerin haberleşme faaliyetlerine hizmet edilebildiğinden, aynı zamanda bireylerin haberleşme özgürlüklerinin de koruma altına alınmaya çalışıldığı söylenebilir[250].

5.2.1.3. Fail ve Mağdur

Madde metninde cezalandırılacak kişi olarak "kimse" tabirinin kullanılması sebebiyle, bu suçun faili herkes olabilir. Günümüzde siber suç failleri için genel olarak kullanılan terim "bilgisayar korsan" dır[251].

Bu suç, mağduru bakımından da bir özellik göstermemektedir. Somut olayda hukuka aykırı olarak giriş yapılan bilişim sistemi üzerinde hak sahibi olan herkes bu suçun mağduru olabilir. Bu bakımdan bir bankanın bilişim sistemine girilmesi neticesinde, hem banka hem de o bankanın İnternet sitesini kullanan müşteriler, bu suçun mağduru konumunda olabileceklerdir.

Kanunun bu suça ilişkin düzenlemesinde, mağdurluk sıfatı bakımından gerçek kişi-tüzel kişi, özel hukuk kişisi, kamu hukuku kişisi ayrımı yapılmamıştır. Sonuçta gerçek bir kişinin evinde kullandığı kişisel bilgisayarına ait bilişim sistemi de, Emniyet Müdürlüğü'nün kullanmakta olduğu bilişim sistemi de bu suçun konusunu oluşturabilir.

5.2.1.4. Suçun Maddi Unsuru

Bu suçun meydana gelebilmesi için, hukuka aykırı olarak bir bilişim sisteminin bir kısmına veya tamamına girilmiş olması yeterli kabul edilmemekte, aynı zamanda girme eyleminin belirli bir süre devam etmesi yani failin bir süre bilişim sisteminde kalması gerekmektedir.

243'üncü maddede "orada kalmaya devam etme" eylemi suçun bir unsuru olarak düzenlenmiş olmasına rağmen, kalmaya devam etme eyleminin süresinin ne kadar olacağı konusunda madde metninde ve gerekçesinde açıklık yoktur. Yalnız, "orada kalmaya devam eden" ifadesi, "kalan" sözcüğüne nazaran zihinde daha geniş

[249] Karagülmez, 2005:166; Dülger, 2004:214
[250] Doğan, 2005:294.
[251] Bu konu ikinci bölümde detaylı olarak incelenmiştir.

bir anlam oluşturmaktadır[252]. Bu sebeple Kanunda bir devamlılıktan bahsedilmesi nedeniyle bu suç "mütemadi bir suç"[253] olarak kabul edilmeli ve suçun oluşabilmesi için sistemde kalmanın temadi (kalmaya devam etme) teşkil edebilecek bir süre devam etmesi gerekmektedir[254].

Bir görüş ise, failin sistemden hemen çıkmayıp sistemdeki bilgileri öğrenmesi durumunda "kalmaya devam etme" eyleminin gerçekleşmiş olacağı yönündedir[255]. Ancak, sistemde kalmaya devam etmeyi, failin sistemdeki bilgileri öğrenmiş olmasına bağlamak, bu suçun işlenme alanını daraltabileceği gibi, söz konusu maddede de bilgilerin öğrenilmesi suçun oluşabilmesinin bir unsuru olarak düzenlenmemiş ve madde gerekçesinde de[256] haksız ve kasten girilmiş olması suçun oluşması için yeterli görülmüştür [257].

Yukarıda kısaca belirtmiş olduğumuz gibi, ceza kanunu tasarısında bu ifade "bilişim sistemine hukuka aykırı olarak girilmesi veya orada kalınması" şeklindeydi. Yani tasarıda söz konusu suç seçimlik hareketli bir suç olarak düzenlenmekteydi. Kanun koyucunun yapmış olduğu bu değişiklikle, elde olmayan nedenlerle veya istemeden, hatalı olarak bir bilişim sistemine girme durumunu göz önüne alarak, yetkisiz erişimi suç saymamış olması ihtimal dahilinde olsa da bu düzenleme suçun uygulanabilirliğini büyük ölçüde azaltmaktadır.

5.2.1.5. Hukuka Aykırılık Unsuru

Ceza kanunlarında düzenlenen bütün suçlarda genel olarak hukuka aykırılık unsurunun bulunduğu ittifakla kabul edilen bir husus olmasına rağmen, bazı maddelerde ayrıca hukuka aykırılığın belirtilmesi durumuna öğretide "hukuka özel aykırılık" denmektedir[258]. Bu şekilde özel olarak hukuka aykırılığın vurgulandığı suçlar ile diğer suçlar arasında esas ve nitelik bakımından bir fark yoktur. Ancak yazında, hukuka özel aykırılık hallerinde hakimin hukuka aykırılığın varlığını

[252] Karagülmez, 2005:170.
[253] Failin harekete geçmesiyle son bulmayarak, icrası bir süre uzayan suç.
[254] Doğan, 2005:295.
[255] Dülger, 2004:218.
[256] 243'üncü maddenin gerekçesinden; www.tbmm.gov.tr
[257] Karagülmez, 2005:170.
[258] İçel ve ark.,2000:108-111; Artuk ve ark., 2002:470 vd.; Akbulut, 1999:110.

aramakla yetinmeyeceğini, ayrıca failin bu özel aykırılığı bilip bilmediğini ve bu şekilde hareket etmeyi isteyip istemediğini araştırması gerekeceği belirtilmektedir[259].

243'üncü maddede, bir bilişim sitemine kısmen veya tamamen hukuka aykırı olarak girilmesinin ve orada kalınmasının suç teşkil edeceği düzenlenmiştir. Madde metninden bu suçun meydana gelebilmesi için hukuka özel aykırılık durumunun gerçekleşmesi gerekeceği düşünülse de, bir bilişim sistemine girebilecek kadar teknik bilgiye sahip olan bir kişinin, yapmış olduğu eylemin hukuka aykırı olduğunu bilmediği düşünülemeyeceğinden, yukarıda belirtilen hususların bu suç için geçerli olmayacağı düşüncesindeyiz.

Kanunun hükmünü icra, bir hakkın icrası, meşru müdafaa, görevin ifası ya da mağdurun rızası şeklinde hukuka uygunluk nedenlerinin bulunması durumlarında, bilişim sistemine girilse ve orada kalmaya devam edilse yani suçun unsurları sübut etmiş olsa bile suç gerçekleşmiş kabul edilmeyecektir. Örneğin bilişim sistemi üzerinde hak sahibi olan kişilerin izniyle sistemin test edilmesi veya korunmasına yönelik erişimler bu suçu oluşturmayacaktır[260].

Bunun yanında CMK m.134'de düzenlenen "Bilgisayarlarda, Bilgisayar Programlarında ve Kütüklerinde Arama, Kopyalama ve El koyma", m.135'de düzenlenen "İletişimin Tespiti, Dinlenmesi ve Kayda Alınması" ve m.l40'da düzenlenen "Teknik Araçlarla İzleme" koruma tedbirlerinin uygulanması halinde, kanun hükmünün icrası hukuka uygunluk sebebi nedeniyle, bu suç oluşmayacaktır[261].

5.2.1.6. Suçun Manevi Unsuru

Bilişim sistemine girme ve orada kalmaya devam etme suçunun manevi unsuru kasttır. Ayrıca maddede düzenlenen bu suç için özel kast[262] aranmamaktadır. Failin genel suç işleme kastının bulunması yeterlidir. Yani fail bilerek ve isteyerek bilişim sistemine girmeli ve orada kalmaya devam etmelidir.

---

[259] İçel, 2001:8
[260] İçel, 2001:8.
[261] Doğan, 2005297.
[262] Failin belirli bir amaç için hareket etmesine "özel kast" denir. Örneğin, hırsızlık suçunun oluşabilmesi için failin başkasına ait bir malı bulunduğu yerden alma iradesi yetmez, ayrıca o maldan faydalanmak amacı ile alması gerekir.

Bu suç ve aşağıda sayılan diğer suçların sadece kasten işlenebilir şekilde düzenlenmiş olması Avrupa Konseyi Siber Suç Sözleşmesi'yle de uyumludur.

Her iki TCK'da, bir suçun taksirle işlenebiliyor olması istisnai bir durumdur ve cezalandırılabilme bakımından kanuni açıklık gerektirir[263]. Bu madde metninde taksirle bir bilişim sistemine hukuka aykırı olarak girmenin suç olarak kabul edileceğine dair bir hüküm bulunmaması nedeniyle, failin taksirle yani tedbirsizlik veya dikkatsizlik sonucu bir bilişim sistemine hukuka aykırı olarak girmesi suç olarak kabul edilemez. Ancak, anılan maddenin 3'üncü fıkrasında sözü edilen suç konusunda verilerin yok olması veya değişmesinde taksir konusu tartışmalıdır[264].

5.2.1.7. Suçun Nitelikli Halleri

5.2.1.7.1. Daha Az Ceza Verilmesini Gerektiren Hal

243'üncü maddenin ikinci fıkrasında yasadışı bilişim sistemine girme ve orada kalma suçu, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hali, daha az ceza verilmesini gerektiren bir durum olarak düzenlemiştir.

Madde metninden ve gerekçesinden bedeli karşılığı yararlanma kavramıyla tam olarak neyin kastedildiği anlaşılmamaktadır. Bir görüşe göre, bu kavramdan anlaşılabilecek dört durum bulunmaktadır: 1- İnternet üzerinden ücret karşılığı hizmet veren web siteleri, 2- İnternet kafe gibi yerlerde olduğu üzere belli bir bedel karşılığı bilişim sisteminin kiralanması, 3- bir kuruluş tarafından belli bir sistemin bedel karşılığı sunulması, 4- belli bir süre İnternet servisinin sağlanması olarak ifade edilmiştir[265].

Söz konusu kavrama, paralı hizmet veren web sitelerinin dahil olduğu konusunda bir şüphe olmamakla birlikte, diğer konular tartışmalıdır.

5.2.1.7.2. Cezanın Ağırlaştırılmasını Gerektiren Sebep

Hukuka aykırı olarak bir bilişim sistemine girme ve orada kalma fiili nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi durumunda, kanun

[263] YTCK m.22 "Taksirle işlenen fiiller, kanunun açıkca belirittiği durumlarda cezalandırılır."
[264] Karagülmez, 2005:173.; Erdağ, 2004.
[265] Dülger, 2004:226.

koyucu bu durumu anılan suç bakımından cezanın ağırlaştırılmasını gerektiren bir sebep olarak düzenlemiştir (YTCK m.243/3).

Bilişim sistemine hukuka aykırı olarak giren failin, bilişim sistemindeki verilerin bozulması ya da değişmesinden dolayı sorumlu tutulabilmesi için, en azından taksirle bu değişim veya zarara sebebiyet vermesi gerekecektir. Bunun nedeni, kanunun gerekçesinde de belirtildiği üzere failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir. Eğer failin, verileri yok etmek veya değiştirmek kastıyla hareket etmişse bu maddeden değil, YTCK m.244'de düzenlenen sistemi engelleme, bozma, verileri yok etme, veya değiştirme suçundan dolayı cezalandırılması gerekecektir.

5.2.1.8. Yaptırım

Suçun basit şekli için öngörülen yaptırım, bir yıla kadar hapis ya da para cezasıdır. Burada hakim ulaştığı sonuca göre faile ya hapis ya da para cezası[266] verecektir. Kanunun açık hükmü uyarınca hapis ve para cezası bir arada verilemeyecektir. Bu düzenleme ile hakime takdir yetkisi tanınmıştır. Ayrıca YTCK'nın 49'uncu maddesinin 1'nci fıkrasına göre, sürekli hapis cezası kanunda aksi belirtilmeyen durumlarda bir aydan az yirmi yıldan fazla olamaz. Bu sebeple, 243'üncü maddenin 1'nci fıkrasındaki hapis cezasının alt sınırı bir aydan başlamaktadır. Suçun, bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde ise yaptırım yarı oranında indirilecektir. Yasadışı erişim nedeniyle sistemin içerdiği veriler yok olur veya değişirse yaptırım, altı aydan iki yıla kadar hapis cezasıdır.

---

[266] YTCK madde 52 "Adli Para Cezası"
"(1) Adli para cezası, beş günden az ve kanunda aksine hüküm bulunmayan hallerde yediyüzotuz günden fazla olmamak üzere belirlenen tam gün sayısının, bir gün karşılığı olarak takdir edilen miktar ile çarpılması suretiyle hesaplanan meblağın hükümlü tarafından Devlet Hazinesine ödenmesinden ibarettir.
(2) En az yirmi ve en fazla yüz Türk Lirası olan bir gün karşılığı adli para cezasının miktarı, kişinin ekonomik ve diğer şahsi halleri göz önünde bulundurularak takdir edilir.
(3) Kararda, adli para cezasının belirlenmesinde esas alınan tam gün sayısı ile bir gün karşılığı olarak takdir edilen miktar ayrı ayrı gösterilir.
(4) Hakim, ekonomik ve şahsi hallerini göz önünde bulundurarak, kişiye adli para cezasını ödemesi için hükmün kesinleşme tarihinden itibaren bir yıldan fazla olmamak üzere mehil verebileceği gibi, bu cezanın belirli taksitler halinde ödenmesine de karar verebilir. Taksit süresi iki yılı geçemez ve taksit miktarı dörtten az olamaz. Kararda, taksitlerden birinin zamanında ödenmemesi halinde geri kalan kısmın tamamının tahsil edileceği ve ödenmeyen adli para cezasının hapse çevrileceği belirtilir."

5.2.2. Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçları (YTCK m.244)

5.2.2.1. Genel Olarak

YTCK'nın 244'üncü maddesinin 1'nci fıkrasında, "Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır."; 2'nci fıkrasında ise "Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır." denmektedir.

765 sayılı TCK'nın 525/b-1 ve 525/b-2 maddelerinde düzenlenen suçların, bir kısım farklılıklarla birlikte YTCK'nın 244'üncü maddesinde düzenlendiğini görmekteyiz.

Aynı zamanda, düzenlenen bu suç ile Avrupa Konseyi Siber Suç Sözleşmesi'nin 4'üncü maddesinde öngörülen "verilere müdahale" ve 5'inci maddesinde öngörülen "sisteme müdahale" düzenlemeleri ile paralellik kurulmaya çalışılmıştır.

Bu düzenleme ile kanun koyucu bilişim sisteminin işleyişinin engellenmesini, bozulmasını cezalandırmak istemiştir. Maddenin gerekçesinde de, bu maddeyle bilişim sistemine yönelik ızrar eylemlerinin ayrı bir suç haline getirildiği belirtilmektedir[267].

Ayrıca söz konusu düzenlemede, 765 sayılı TCK'da yer alan düzenlemeden farklı olarak "zarar verme" ifadesine yer verilmeyerek, bilişim sisteminin donanım kısmına zarar vermek amacıyla yapılan eylemler, bu maddenin dışında bırakılmıştır[268].

---

[267] Karagülmez, (2005:186)'e göre karşılaştırmalı hukukta, bu tip eylemler genel olarak bilişim sistemlerine işlenen nas-ı ızrar suçları olarak düzenlenmiştir. Örnek olarak, Fransa Ceza Kanunun m. 323.1, 323.2, Almanya Ceza Kanunu m.303a gösterebilir.

[268] Dülger, 2004:230; Karşı görüş için bkz: Değirmenci, 2002:154; Özel, 2001:860-865; Yazıcıoğlu, 2004:179.

5.2.2.2. Korunan Hukuki Yarar

Bu madde ile koruma altına alınan şey, madde gerekçesinde de belirtildiği gibi bilişim siteminin diğer bir ifadeyle bilgisayarın fiziki varlığı ve sistemin işlemesini sağlayan bütün diğer unsurlardır. Esasen burada hem bilişim sisteminin, hem de bu sistem içerisinde yer alan veriler veya diğer unsurların zarar görmemesi amaçlanmaktadır.

5.2.2.3. Fail ve Mağdur

Kanun maddesinde fail açısından herhangi bir özellik belirtilmediğinden bu suçun faili herkes olabilir.

Bu suçun failinin tespiti için, suç olarak kabul edilen fiil, bilişim sistemine yönelik ise sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik ise bu verilerin, hem bilişim sistemine hem de verilere yönelik ise her ikisinin mülkiyet, kullanım ve tasarruf haklarının kime ait olduğu ve zararı kimin meydana getirdiği açıkça belirlenmelidir[269].

Bu suç mağdur açısından da bir özellik taşımadığından, herkes anılan suçun mağduru olabilir. Yine bu suçun mağduru olmak için bilişim sisteminin ya da zarara uğrayan verilerin maliki ya da zilyeti olunması gerekmemektedir. Bilişim sistemine ve/veya verilerde oluşturulan yazılım, ekonomik bilgiler, bilimsel çalışmalar gibi değerlere ulaşılmasında ve kullanılmasında çıkarı ve bu veriler üzerinde tasarruf yetkisi bulunan kişi bu suçun mağduru olacaktır.

5.2.2.4. Suçun Maddi Unsuru

Kanuni sonucun birden fazla hareketle meydana geldiği suçlara seçimlik hareketli suçlar denilmektedir. Seçimlik hareketli suçlarda, kanunda belirtilen hareketlerin sadece birinin yapılması ile suç meydana gelmektedir.

YTCK'nın 244'üncü maddesinde düzenlenen suç tipi de seçimlik hareketli suçlardır. Bu sebeple aşağıda sayılan eylemlerden herhangi bir tanesinin işlenmesi suçun tamamlanması için yeterlidir.

---

[269] Dülger, 2004:232.

Söz konusu maddenin 1'inci fıkrasında "bilişim sisteminin işleyişini engelleme" veya "bozma", 2'nci fıkrasında ise "sisteme hukuka aykırı biçimde veri sokma" veya "var olanları başka bir yere gönderme", "sistemdeki verileri yok etme" veya "bozma", "değiştirme" veya "erişilmez kılma" eylemlerini suç olarak düzenlemektedir.

244'üncü maddenin ilk iki fıkrasında iki ayrı suç düzenlenmiştir. Bu suçları birbirinden ayıran nokta suçların konusudur. İlk fıkrada düzenlenen suçun konusu bilişim sisteminin bütün olarak kendisidir. İkinci fıkrada yer alan suçun konusu ise bilişim sistemini oluşturan verilerdir. Bu nedenle ilk fıkrada yer alan suçun cezası, ikinci fıkrada yer alan suça oranla daha ağırdır.

Birinci fıkra, bilişim sitemlerinin kendisine yönelik olarak işlenen bozma veya engelleme şeklindeki ızrar fiillerini özel bir suç haline getirmektedir. Bozmak, sistemin gereği gibi yani programlanmış olduğu gibi çalışmamasına neden olmak, engellemek ise sistemin uygun işleyişine mani olmak anlamına gelmektedir. Bilişim sisteminin işleyişini bozmak veya engellemek, çeşitli müdahalelerle sağlanabilir. Örneğin bilişim sisteminin çalışmasını sağlayan bilgisayara virüs göndermek hatta bir alıcıya kasten sistemin iletişim işlevlerini engellemek üzere çok büyük miktarda elektronik posta göndermek de bu suçu oluşturacaktır[270].

İkinci fıkrada ise bilişim sistemindeki verilerin bozulması, yok edilmesi, değiştirilmesi veya erişilmez kılınması ile sisteme veri sokulması, verilerin yok edilmesi, bozulması, erişilmez kılınması veya değiştirilmesi suç haline getirilmiştir.

Bu suçun seçimlik hareketleri şunlardır;

"Verilerin bozulması", verilerin işlevlerini yapamaz hale getirilmesi anlamına gelir. Bu durumda veriler, varlıklarını korumakla birlikte işe yaramaz hale getirilmektedir.

"Verilerin yok edilmesi", zaten soyut varlıklar olan verilerin silinmesi anlamına gelir.

[270] Doğan, 2005:302.

"Verilerin değiştirilmesi"yle, bir veri ya da veri grubu yerine başka verilerin konulması kastedilmektedir. Bu birkaç veriden oluşan bir bilgi notu ya da resmin değiştirilmesi şeklinde olabileceği gibi verilerden oluşan örneğin bir uygulama yazılımının değiştirilmesi şeklinde de olabilir.

"Verileri erişilmez kılmak", sistem kullanıcısının istediği zaman verilere ulaşmasının engellenmesi anlamına gelir.

"Sisteme veri yerleştirmek", fail tarafından sisteme dışarıdan ve sistemin sahibinin ya da kullanıcısının izni olmadan daha önce bulunmayan verileri sisteme girmek anlamına gelir.

"Sistemde var olan verileri başka bir yere göndermek", ise sistemin içerisinde yer alan verilerin yerini değiştirmek ya da veri taşıma aracına aktarılması, kaydedilmesi veya kopyalanması anlamına gelir.

Bu suçun meydana gelmesine sebep olan fiillerin incelenmesi sonucunda ortaya çıkan sonuç kanun koyucunun kanunda boşluk ortaya çıkmasına engel olmak için suçun maddi unsurunu geniş tuttuğudur. Kanun koyucunun bu tip bir düzenleme yapması ilk başta doğru gibi gözükse de uygulamada suçun oluşmasına sebep olan fiillerin maddede belirtilen hareketlerden hangisi ya da hangileri ile gerçekleştirildiği konusunda karışıklık yaşanabilecektir[271]. Bunun nedeni suçun meydana gelmesine sebep olarak sayılan fiillerin, bir suçun oluşması sırasında genellikle bir arada bulunabileceği ve birbirinden ayrılmasının zor olabileceğidir. Bunu bir örnekle somutlaştırmak gerekirse, verilerin yok olmasına sebep olan bir fiil, aynı zamanda verilerin bozulmasına ve değişmesine de sebep olabilecektir. Böyle bir durumda eylemin bu seçimlik hareketlerden hangisini meydana getirdiğinin tespiti, teknik bilgiye yeterince sahip olmayan uygulamacı bakımından zor olacaktır. Her ne kadar uygulamacı bilirkişi incelemesinden faydalanacak olsa dahi uygulamada yeknesaklığın sağlanması bakımından Yargıtay'a büyük yük düşmektedir[272].

244'üncü maddenin 4'üncü fıkrasında "Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir

[271] Yazıcıoğlu, 1997:263.
[272] Doğan, 2005:303.

çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezasına hükmolunur." kuralıyla, 1 ve 2'nci fıkralarda tanımlanan fiillerin işlenmesi nedeniyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır.

Maddeyi bir örnekle netleştirmek gerekirse, fail, bir bilişim sistemine bir virüs, bilgisayar solucanı, truva atı gibi bilgisayar sistemi için zararlı programları göndermek suretiyle sistemin içinde yer alan verilere zarar verirse ikinci fıkrada yer alan suçu, aynı virüs ile sistemin tamamının işleyişini engeller veya bozarsa birinci fıkrada yer alan suçu işlemiş olacaktır. Bu kişi söz konusu eylemi ile virüs koruma programları üreten bir firmanın ürün satışlarını artırmayı amaçlıyorsa ve bu amacına da ulaşırsa yani haksız çıkar sağlarsa dördüncü fıkra hükmünden cezalandırılacaktır[273].

244'üncü maddenin 4'üncü fıkrasının uygulanabilmesi için fıkra kapsamında yer alan eylemin "başka bir suç oluşturmaması" ön koşulunuda gerçekleştirmesi gerekmektedir. Yine bir örnekle[274] durumu açıklamak gerekirse, sanık (S) tarafından sahtekarlık amacıyla kurulan web sitesinden, bir bankanın web sitesinden gönderiliyormuş gibi (M)'ye banka hesabı ile kişisel bilgilerinin güncelleştirilmesinin gönderilmesi bir e-posta ile istenmektedir. Söz konusu e-posta aynı zamanda bilişim sistemine zarar verici unsurları da içinde barındırmaktadır. Sonuç olarak (M) hileli verilerle dolandırılmış ve (S) bu durumdan haksız çıkar sağlamıştır.

(S)'nin fiili kendisine haksız çıkar sağlamak amacıyla, (M)'nin bilişim sistemine haksız olarak veri yerleştirmek ve buna bağlı olarak da (M)'yi dolandırmaktadır. Söz konusu fiil eğer (M)'nin bilişim sisteminin işleyişini engellemiş veya bozmuşsa 244/1'e göre; engellememiş veya bozmamışsa 244/2'ye göre suç oluşacaktır. 2'nci fıkradaki suçun oluştuğunu kabul edersek ve (S)'nin amacının haksız çıkar sağlamak olduğuna göre, 244'üncü maddenin 4'üncü fıkrası gündeme gelmektedir. Ancak yukarıda da belirtmiş olduğumuz gibi anılan fıkranın uygulanabilmesi için fiilin 244'üncü madde dışında başka bir suç oluşturmaması

[273] Doğan, 2005:304.
[274] Karagülmez, 2005:194.

gerekir. Olayda (S)'nin fiili, aynı zamanda YTCK'nın 158'inci maddesinin 1'nci fıkrasının (f) bendindeki bilişim sistemlerinin araç olarak kullanılması suretiyle dolandırıcılığa da girmesi sebebiyle 244/4 uygulanamayacaktır. Ayrıca 244/2'de 158/1-f'le beraber uygulanmayacaktır. Bunun nedeni ise YTCK'nın "Fikri İçtima" kenar başlıklı 44'üncü maddesindeki "İşlediği bir fiil ile birden fazla farklı suçun oluşmasına sebebiyet veren kişi, bunlardan en ağır cezayı gerektiren suçtan dolayı cezalandırılır." hükmüdür. Olayımızda 158/1-f'deki suçun cezasının daha ağır olması sebebiyle, fail bu suçtan dolayı cezalandırılacaktır.

5.2.2.5. Hukuka Aykırılık Unsuru

İlk fıkrada hüküm altına alınan bilişim sisteminin işleyişini bozma, engelleme suçu bakımından hukuka uygunluk sebebi olarak düşünülebilecek ilk durum "Kanun Hükmünün İcrası"dır. Yine ilk iki fıkrada düzenlenen suçlar için mağdurun rızası da hukuka uygunluk sebebi oluşturacaktır. Ayrıca anılan maddenin 4'üncü fıkrasında ise failin hileli davranışlarla mağdurun rızasını elde etmiş olması hali dışında, mağdurun rızası hukuka uygunluk sebebi olarak kabul edilebilir. Bunun nedeni, dolandırıcılık suçunda da mağdurun rızasının olması ancak bu rıza mağdurun iradesinin sakatlanması sonucunda alındığından eylemi hukuka uygun hale getirmemesidir.

5.2.2.6. Manevi Unsur

244'üncü maddenin 1 ve 2'nci fıkralarında yer verilen suçların manevi unsuru bilerek ve isteyerek genel suç işleme kastıdır. Ancak sadece bilme, suç işleme kastının oluştuğu anlamına gelmemekte, ayrıca failin eyleminin sonuçlarını istemesi, suç işleme kastının varlığı için gerekli görülmektedir.

244'üncü maddenin 4'üncü fıkrasında düzenlenen suçun meydana gelebilmesi için kişinin "kendisinin veya başkasının yararına haksız çıkar sağlamak" amacıyla işlenmesi gerektiğinden, burada özel kast söz konusudur[275].

[275] Aksi görüş için Doğan, 2005:304.

5.2.2.7.Suçun Nitelikli Halleri

5.2.2.7.1. Daha Az Ceza Verilmesini Gerektiren Hal

Hem eski hem de yeni kanunda bu suç tipi için herhangi bir hafifletici sebep düzenlenmemiştir.

5.2.2.7.2. Cezanın Ağırlaştırılmasını Gerektiren Nitelikli Hal

Maddenin üçüncü fıkrasında sistemi bozmaya yönelik bu fiillerin banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi hali ağırlaştırıcı neden olarak düzenlenmiştir. Buna göre söz konusu ağırlaştırıcı durumun gerçekleşmesi durumunda faile verilecek ceza yarı oranında artırılacaktır

5.2.2.8. Yaptırım

Maddeye göre, bilişim sisteminin işleyişinin engellenmesinin veya bozulmasının cezası bir yıldan beş yıla kadar hapis cezasıdır. Bilişim sistemindeki verileri bozmanın, yok etmenin, değiştirmenin veya erişilmez kılmanın, sisteme veri yerleştirmenin, var olan verileri başka bir yere göndermenin cezası ise altı aydan üç yıla kadar hapis cezasıdır.

Bu fiiller neticesinde kişinin kendisi veya bir başkasına haksız kazanç sağlamasının cezası ise iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasıdır.

5.2.3. Banka ve Kredi Kartlarının Kötüye Kullanılması Suçları (m.245)

5.2.3.1. Genel Olarak

İnsanların çeşitli sebeplerden dolayı ödeme aracı olarak nakit ödeme araçları yerine banka ve kredi kartlarını kullanmaya başlamaları nedeniyle bu kartların kullanımı toplumda gittikçe artmaktadır.

Banka ve kredi kartıyla ilgili suçlar[276], İnternet kullanımının da toplumda oldukça yaygınlaşmasıyla beraber büyük bir artış göstermiştir. Avrupa'da 2002

[276] Bu suçlar e-dolandırıcılık (e-fraud) olarakda adlandırılmaktadır.

yılında kredi kartı dolandırıcılığı 4 milyar dolara ulaşmıştır. FBI, bilgisayar korsanlarının e-ticaret sitelerinden bir milyondan fazla kredi kartı numarasını çaldıklarını belirtmektedir. Bu gelişmeler sonucunda İnternet kullanıcılarının çoğunluğu, İnternet'ten yapılan alışverişi güvenli bulmamaktadır. Buna örnek olarak Avrupa'da yapılan bir araştırmanın sonucu verilebilir. Bu araştırmaya göre Avrupa'da İnternet kullanıcılarının yarısına yakını hem İnternet'teki satıcılara hem de kredi kartı bilgilerini İnternete vermeyi güvenli bulmamaktadırlar[277].

Kanun koyucular yukarıda belirtilen durumu yani İnternet kullanıcılarının güvensizliğini ortadan kaldırmak ve e-ticaret'in güvenliğini sağlamak amacıyla bu alanda düzenlemeler yapmışlardır.

Türkiye'de bu konudaki ilk düzenlemeye ETCK'nın 525/b-2[278] maddesinde yer verilmiştir. Anılan madde münhasır olarak banka ve kredi kartının kötüye kullanılmasını düzenlememekte olsa da, ülkemizde banka ve kredi kartının kötüye kullanılmasıyla[279] ilgili suçlardan dolayı mahkemelerde bir çok dava açılması ve YCGK'nın bu konuya açıklık getiren bir karar[280] vermesi sonucunda banka ve kredi

[277] Karagülmez, 2005:195:Philippsohn and Thomas'dan, 2003:7-9.

[278] Madde 525/b-2 "Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak veya başkası lehine hukuka aykırı yarar sağlayan kimseye bir yıldan beş yıla kadar hapis ve iki milyondan liradan yirmimilyon liraya kadar ağır para cezası verilir."

[279] Değirmenci, (2003:509)'e göre Emniyet Genel Müdürlüğü Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığının yaptığı araştırmaya göre, kredi ve banka kartları ile ilişkili hukuka aykırı eylemler 9 grupta toplanabilir. Bunlar;
1)Kayıp, Çalıntı Kart Kullanımı,
2)Müracaat üzerine banka veya kredi kartlı sistem kuruluşu tarafından çıkarılan kart hamilin eline geçmeden, ele geçirilmesi ve kötüye kullanılması,
3)Banka veya kredi kartlı sistem kuruluşuna sahte bir kimlikle başvurup kredi kartı alınması ve kötüye kullanılması,
4)İşyerleriyle ortaklaşa olarak yapılan faaliyet sonucunda, boş plastik üzerine kabartma olarak basılan gerçek kredi kart numaraları ile alış veriş yapılmış gibi gösterilmekte ve bu miktarın sonradan bankadan tahsil edilmesi,
5)Kredi kartları üzerinde yer alan kabartma numaralarının kesilerek değiştirilmesi veya ütülenerek yenisinin basılması,
6)Çeşitli yöntemlerle üretilen kartın arkasında bulunan manyetik şerit "encoder" denilen bir cihaz yardımı ile kodlanarak içine elektronik yollardan kart bilgilerinin yazılarak kullanıma sunulması,
7)Gerçek kartın manyetik şeridinde bulunan bilgiler silinerek, başka kartlara ait bilgilerin kodlanması,
8)Kredi kartı numarası kullanılarak posta veya telefonla mal siparişlerinde, önceden ayarlanmış bir adrese mal tesliminin sağlanması,
9)Kart hamili ATM Cihazlarında alışveriş yaparken kredi kartı ve şifre bilgilerinin ele geçirilmesi ve sonra bunların kötüye kullanılmasıdır.

[280] YCGK, K.t. 10.04.2001, E:2001/7630, K:2001/757, YKD., Haziran 2001, sf. 913-915.

kartının kötüye kullanılması ile ilgili eylemler bu madde kapsamında değerlendirilmiştir.

Banka ve kredi kartının kötüye kullanılması suçu, ETCK'nın genel düzenlemesine mukabil YTCK'da bağımsız bir suç tipi olarak 245'inci[281] maddede düzenlenmiştir.

245'inci maddenin gerekçesinde, maddenin banka ve kredi kartlarının haksız, hukuka aykırı olarak kullanılması üzerine bankaların ve kart sahiplerinin zarara sokulmasının ve bu yolla çıkar sağlamasının önlenmesi ve faillerin cezalandırılması amacıyla böyle bir maddeye yer verildiği belirtilmiştir[282].

5.2.3.2. Korunan Hukuki Yarar

245'inci maddenin gerekçesinde, bu suçun aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçları ile korunmak istenen hukuki yararın anılan madde ile korunmak istenen hukuksal değerleri oluşturduğu belirtilmektedir. Bunlardan hırsızlık ve dolandırıcılık suçları ile kişilerin mal varlığı, güveni kötüye kullanma suçu ile kişilerin birbirine karşı duyduğu güven, son olarak sahtecilik suçunda ise belgelere olan güven duygusu korunan hukuki değerdir[283]. Bunların yanı sıra, bankaların bu hizmetleri aracılığıyla yürüyen ticari hayatın ve bankacılık sisteminin güvenirliliğini de korunan hukuki yararlar arasında saymak mümkündür.

---

[281] Madde 245 "Banka veya kredi kartlarının kötüye kullanılması"
"(1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.
(2) Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adli para cezası ile cezalandırılır.
(3) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.
(4) Birinci fıkrada yer alan suçun;
a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,
b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlatlığın,
c) Aynı konutta beraber yaşayan kardeşlerden birinin,
Zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz."
[282] 245'inci maddenin gerekçesinden.
[283] Dülger, 2004:251; Kurt, 2005:178.

5.2.3.3. Fail ve Mağdur

Bu suçun faili herkes olabilir. Ancak bir kimsenin fail olarak addedilebilmesi için başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse olması gerekmektedir. Bu sebeple, kendisine ait banka veya kredi kartını kötüye kullanarak haksız çıkar elde eden kişi bu suçun faili olmaz, olsa olsa güveni kötüye kullanma veya dolandırıcılık suçunun faili olabilir. Ayrıca Banka Kartları ve Kredi Kartları Kanununda kart sahiplerinin işleyebileceği Gerçeğe Aykırı Beyan, Sözleşme ve Eki Belgelerde Sahtecilik Suçu (m.37) düzenlenmektedir. Bu kanuna göre, "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" bu kanun kapsamında cezalandırılacaklardır[284].

Burada mağdur, kredi kartı her ne şekilde olursa olsun elinden alınan veya kendisine verilmesi gereken kart kendisine verilmeyip rızası hilafına kullanılan kişidir. Ayrıca banka ve kredi kartını piyasaya sunan ve bunun karşılığında bireylere kredi veren bankalar da mağdur konumunda olabilmektedir. Zaten madde gerekçesinde de belirtildiği üzere bu maddenin düzenlenme amacı banka ve kredi sahiplerinin zararlarının önüne geçilmesidir[285].

5.2.3.4. Maddi Unsur

Bu madde ile düzenlenen banka veya kredi kartlarının kötüye kullanılması suçunun maddi unsuru, başkasına ait (veya sahte oluşturulan veya üzerinde sahtecilik yapılan) bir banka veya kredi kartını sahibinin ya da kendisine iadesi gereken kişinin rızası olmaksızın menfaat sağlamak için kullanmak, kullandırtmak veya başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satmak,

---

[284] BKKK MADDE 37- Gerçeğe aykırı beyan, sözleşme ve eki belgelerde sahtecilik
"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 hapis ve ikibin güne kadar adlî para cezası ile cezalandırılırlar.
Kredi kartı veya üye işyeri sözleşmesinde veya eki belgelerde sahtecilik yapanlar veya sözleşme imzalamak amacıyla sahte belge ibraz edenler bir yıldan üç yıla kadar hapis cezasına mahkûm edilirler."

[285] Doğan, 2005:309.

devretmek, satın almak ve kabul etmektir[286]. Yani maddede üç farklı suç tipi bir arada düzenlenmiştir.

a) Gerçek Banka veya Kredi Kartlarının Kötüye Kullanılması (YTCK m.245/1)

Anılan maddenin birinci fıkrasına göre, yasal yollardan hazırlanmış bir banka veya kredi kartının kötüye kullanılması cezalandırılacaktır.

Bu suçun meydana gelebilmesi için öncelikle failin başkasına ait bir banka veya kredi kartını ele geçirmesi veya elinde bulundurması gerekir. Fail, bu kartı çalmış veya bulmuş olabileceği gibi yanlışlıkla kendisine ulaştırılmış da olabilir. Daha sonra fail tarafından, "başkasına ait banka veya kredi kartının, sahibinin rızası olmaksızın kullanılması" veya "kullandırılması" ve "bunun neticesinde failin kendisi veya başkası lehine haksız yarar" sağlaması gerekmektedir. Sonuç olarak suçun tamamlanabilmesi için, failin kartı ele geçirmesi ve kullanması yetmemekte ayrıca haksız yarar sağlaması da gerekmektedir.

Örneğin Yargıtay'ın vermiş olduğu bir kararda "Özel hukuk tüzel kişisi olan … Bank" tarafından düzenlenen kredi kartlarının, adlarına düzenlenen kişilere teslim edilmeden, dağıtımını üstlenen şirket elemanı sanık tarafından ele geçirilip kullanılması eylemini ETCK'nın 525/b-2 maddesine uygun bulmuştur[287]. Söz konusu eylem artık YTCK'nın 245/1 maddesine göre cezalandırılacaktır.

b) Sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek (YTCK m.245/2)

YTCK m.245/2'de düzenlenen "sahte banka veya kredi kartı üretmek", "satmak", "devretmek", "satın almak" veya "kabul etmek" suçlarında, suçun oluşabilmesi için herhangi bir menfaat elde edilmiş olma şartı aranmamaktadır. Bu eylemler suçun oluşabilmesi için tek başlarına yeterlidir. YTCK yürürlüğe girmeden önce doktrinde sahte kart üretmek ve kullanmak eylemlerinin, özel evrakta sahtecilik ve dolandırıcılık, suçlarını oluşturacağı, failin fikri içtima kuralı çerçevesinde daha

[286] KURT, 2005:178.
[287] 6. CD.,26.04.1999, E:2418, K:2370.

fazla ceza öngören dolandırıcılık suçundan dolayı cezalandırılacağı kabul edilmekteydi[288].

Söz konusu maddede, suçun seçimlik hareketleri belirtilirken, bu hareketlerin "başkasına ait banka hesapları ile ilişkilendirilerek" gerçekleştirilmesinin suçun bir unsuru olduğu ifade edilmiştir. Yani failin, sahte bir banka kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmekten dolayı cezalandırılabilmesi için bu hareketleri başkasına ait banka hesapları ile ilişkilendirerek yapmış olması gereklidir. Bu nedenle başkasına ait bir banka hesabı ile ilişkilendirilemedikten sonra sahte kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek bu suçu oluşturmayacaktır[289].

c) Sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartlarının kötüye kullanılması (YTCK m.245/3)

YTCK'nın 245/3 maddesinde düzenlenen suçun konusu, bir kartın üzerinde sahtecilik yapılması veya bir kartın sahte olarak düzenlenmesidir.

Bu suçun oluşabilmesi için de birden fazla hareketin meydana gelmesi gerekmektedir. Bir başka ifadeyle, suçun tamamlanabilmesi için sahte olarak düzenlenen veya üzerinde sahtecilik yapılan bir kartı ele geçirmek ve bu kartı kullanarak haksız çıkar sağlamak gerekmektedir. Sahtecilik fiilini yapan kişi ile bu kartları kullanarak haksız çıkar sağlayan kişilerin aynı kişiler olması zorunlu değildir.

5.2.3.5. Hukuka aykırılık Unsuru

YTCK'nın 245'inci maddesinde düzenlenen banka ve kredi kartlarının kötüye kullanılması suçunda hukuka aykırılık unsuru, tarif edilen başkasına ait banka kartı veya kredi kartını ele geçiren veya elinde bulunduran kimsenin kart sahibinin rızası olmaksızın bu kartı kullanması ya da kullandırması fiilleridir. Buradan çıkan sonuca göre, mağdurun rızası bu suç bakımından bir hukuka uygunluk sebebidir.

İkinci fıkra bakımından ise bu durum geçerli değildir. Çünkü bu fıkrada suçun oluşabilmesi için ortada sahte veya üzerinde sahtecilik yapılmış bir kartın

[288] Bayraktar, 2000:201; Ekinci, 2002:101; Değirmenci, 2003:608; Doğan, 2005:311.
[289] Doğan, 2005:312.

olması gerekmektedir. Eğer kart üzerinde sahtecilik yapılmasına kart sahibi rıza göstermişse, kart sahibi de iştirak hükümlerine göre bu suçtan sorumlu olacaktır.

Burada belirtilmesi gereken diğer bir konuda 245/son maddesinde düzenlenmiş olan 245'inci maddenin 1'nci fıkrası için cezasızlık nedenidir.

Buna göre, bu suçun;

a)Haklarında ayrılık kararı verilmemiş eşlerden birinin,

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

c)Aynı konutta beraber yaşayan kardeşlerden birinin,

zararına olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmayacaktır.

5.2.3.6. Manevi Unsur

YTCK'nın 245'inci maddesinde düzenlenen her iki suç bakımından genel kast yeterlidir[290]. Her ne kadar kişinin kendisi veya başkasına haksız yarar sağlaması suçun tamamlanması bakımından gerekli ise de failin mutlaka bu suçu "kendisi veya bir başkasına haksız yarar sağlama" özel kastı ile işlemesi gerekmemektedir. Haksız yarar sağlama, bu suçun maddi unsurunun netice kısmını teşkil etmektedir[291].

5.2.3.7.Yaptırım

Birinci fıkrada düzenlenen "başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlama" fiilinin cezası üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası olarak belirlenmiş, ikinci fıkrada düzenlenen "Sahte banka veya kredi kartı üretmek, satmak, devretmek, satın almak veya kabul etmek" suçunun cezası, üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası

[290] Aksi görüşte olan Karagülmez, (2005:216)'e göre; 245/2 maddesindeki suçun failinde, başkasına ait kartla veya sahte oluşturulan veya üzerinde sahtecilik yapılan kartı kullanarak kendisine veya başkasına yarar sağlama kastı bulunmalıdır. Faildeki bu kast olarak nitelendirilmekte isede, failin yarar sağlamak maksadı dışında (örneğin, zarar vermek veya kendisini ispatlamak gibi)bir kastla suç işlemesi 245/2 maddesine girmemektedir. Bu nedenle, 245/2 maddesindeki suçta kendisine veya başkasına yarar sağlama özel kastı aranmaktadır.

[291] Doğan, 2005:312.

olarak tespit edilmiş ve son olarak üçüncü fıkrada düzenlenen, "suçun, sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle işlenmesi", dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adli para cezası olarak düzenlenmiştir.

5.2.4. Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması (YTCK m.246)

YTCK'nın 20/2 maddesiyle "Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır." şeklinde bir düzenleme getirmiştir. YTCK'nın 60'ıncı maddesinde ise tüzel kişiler hakkında uygulanacak güvenlik tedbirleri düzenlenmiştir. Bu maddeye göre;

"(1) Bir kamu kurumunun verdiği izne dayalı olarak faaliyette bulunan özel hukuk tüzel kişisinin organ veya temsilcilerinin iştirakiyle ve bu iznin verdiği yetkinin kötüye kullanılması suretiyle tüzel kişi yararına işlenen kasıtlı suçlardan mahkumiyet halinde, iznin iptaline karar verilir.

(2) Müsadere hükümleri, yararına işlenen suçlarda özel hukuk tüzel kişileri hakkında da uygulanır.

(3) Yukarıdaki fıkra hükümlerinin uygulanmasının işlenen fiile nazaran daha ağır sonuçlar ortaya çıkarabileceği durumlarda, hakim bu tedbirlere hükmetmeyebilir.

(4) Bu madde hükümleri kanunun ayrıca belirttiği hallerde uygulanır."

Bu düzenlemeye göre YTCK tüzel kişilerin cezai sorumluluğunu kabul etmemektedir. Sadece kanunda belirtilen hallerde haklarında belirli güvenlik tedbirlerinin uygulanabileceği hükme bağlanmıştır. 246'ncı[292] madde de bu maddelerden bir tanesidir. Bu madde gereği Bilişim Alanında Suçlar başlıklı bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında güvenlik tedbirlerine hükmolunacaktır.

[292] Madde 246: "Tüzel kişiler hakkında güvenlik tedbiri uygulanması"
"Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."

Karşılaştırmalı hukukta ise, üç farklı sistemin var olduğunu söylemek gerekir. Bunlardan birincisi cezai sorumluluğu kabul etmeyip idari yaptırımlar öngörenler (Almanya, İtalya, İsviçre, Portekiz), ikincisi, güvenlik tedbiri öngörenler (İspanya, Avusturya, Polonya) ve üçüncüsü, tüzel kişilerin cezai sorumluluğunu kabul eden ülkelerdir (Fransa, Belçika, Hollanda, İngiltere, Kanada)[293].

Bu düzenleme karşısında tüzel kişi vasfına haiz servis sağlama hizmeti sunan şirketlerin de güvenlik tedbiri uygulaması şeklinde sorumluluğunun önü açılmış olacaktır. Ancak bunun için yukarıda sıralanan koşulların sağlanmış olması gerekmektedir.

Yine Avrupa Konseyi Siber Suç Sözleşmenin 12'nci maddesi de Kurumsal Sorumluluğu kabul ederken bir takım koşulların gerçekleşmiş olmasını aramaktadır. Bunlardan en önemlisi anılan suçların tüzel kişiliğin menfaatine işlenmiş olmasıdır. Bu şart YTCK'da "haksız menfaat sağlanan tüzel kişiler" denmek suretiyle vurgulanmıştır. Ayrıca anılan Sözleşmede suçun yönetici konumunda bulunan kişilerce işlenmiş olması, şirketin yönetici konumunda bulunmayan çalışanlarının suçu işlemesi durumunda ise şirketin suçu işleyen çalışanı üzerinde denetim ve gözetim yükümlülüğünün ihlal edilmiş olması şartını da aramaktadır[294].

5.2.5. YTCK'da Düzenlenen Diğer Siber Suç Tipleri

Yukarıda incelenen YTCK'nın "Bilişim Alanındaki Suçlar Bölümü"nde yer alan suçlar dışında yine aynı Kanunun çeşitli maddelerinde siber suçlarla ilgili düzenlemelere yer verilmiştir. Bu düzenlemeler aşağıda "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri" ve "Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri" olarak iki ana başlık altında incelenecektir.

[293] Kangal, 2003:25; Doğan, 2005:315.
[294] Doğan, 2005:317.

5.2.5.1. Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri

5.2.5.1.1. Kişisel Verilerin Kaydedilmesi Suçu (m.135)

5.2.5.1.1.1. Genel Olarak

YTCK'nın 135'inci maddesinin[295] birinci fıkrasıyla, hukuka aykırı olarak kişisel verilerin kaydedilmesi eylemi; ikinci fıkrasıyla da kişilerin siyasi, felsefi veya dini görüşlerinin, ırki kökenlerinin, sendikal bağlantılarının, cinsel yaşamlarının ve sağlık durumlarının kişisel veri olarak kaydedilmesi eylemleri suç olarak hüküm altına alınmıştır[296].

Anılan maddedeki suçlar, ağırlıklı olarak bilgisayar aracılığıyla işlenebilir. Bu durum maddenin gerekçesinde de belirtilmiştir. Söz konusu maddenin gerekçesinde "Çağımızda kişiler ilgili kayıtların bilgisayar ortamlarına geçirilip muhafaza edilmesi uygulamasına bazı kurum ve kuruluşlar tarafından başvurulmaktadır; hastanelerde hastalara, sigorta şirketlerinde sigortalılara, bankaların ve kredili alış veriş yapılan mağazaların müşterilerine ilişkin kayıtlar böylece tutulmaktadır. Bu bilgilerin amaçları dışında kullanılmasından dolayı hakkında bilgi toplanan kişiler büyük zararlara uğrayabilmektedirler. Bu bakımdan, kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınması suç olarak tanımlanmıştır." denmektedir.

Yine anılan maddenin gerekçesinde, "Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayrım gözetilmemiştir. Bu bakımdan, Avrupa Konseyi'nin ürettiği belgelerden olan ve Türkiye'nin de tarafı[297] olduğu "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi

---

[295] Madde 135 "Kişisel verilerin kaydedilmesi"
"(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.
(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

[296] Özel, 2001:865; Değirmenci, 2002:156-157; Dülger, 2004:267.

[297] Türkiye'nin de tarafı olduğu bu sözleşmeye göre, sözleşmenin onaylanabilmesi için taraf devletlerin Sözleşmede belirtilen ilkelere uygun bir kanun (uygulama kanunu) kabul etmesi

Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanınmıştır" denilerek, bu konudaki Sözleşmeye gönderme yapılmıştır.

5.2.5.1.1.2. Korunan Hukuki Değer

135'inci madde, YTCK'nın "özel hükümler" başlıklı ikinci kitabının "kişilere karşı suçlar" başlıklı ikinci kısmının "özel hayata ve hayatın gizli alanına karşı suçlar" başlıklı dokuzuncu bölümünde yer almaktadır. Yasanın sistematiğine bakıldığında, bu suçla genel olarak kişilerin özel hayatı ve hayatın gizli alanı, özel olarak da kişisel verilerin korunması amaçlandığı görülmektedir.

1982 Anayasasının "Özel hayatın gizliliği ve korunması" başlıklı 20'nci maddesindeki, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz…" ifadeyle hüküm altına alınmıştır.

1982 Anayasasının 20'nci maddesiyle, bireylerin özel hayatı korunmak istemiştir. Bu ise her şeyden önce özel hayatın gizliliğinin korunması yoluyla sağlanabilir. YTCK'nın 135'inci maddesindeki düzenlemeyle de gerçek kişilerin özel hayatı korunmaktadır.

5.2.5.1.1.3. Fail ve Mağdur

Bu suç fail açısından herhangi bir özellik taşımadığından, bu suçun faili herkes olabilir. Ancak failin kamu görevlisi olması durumunda bu suç için verilecek ceza ağırlaşacaktır. Aşağıda bu konu daha detaylı bir şekilde anlatılacaktır.

Bu suç mağdur açısından da bir özellik göstermemektedir. Bu sebeple bu suç açısından mağdur herkes olabilir. Burada belirtilmesi gereken husus yasada bir ayrım yapılmaması sebebiyle tüzel kişilerin de mağdur olabileceğidir.

5.2.5.1.1.4. Maddi Unsur

135'inci maddede suçun işlenme şekli ve alanı sınırlandırılmamıştır. Bu suçla her türlü kişisel verinin hukuka aykırı olarak kaydedilmesi fiili cezalandırılmıştır.

---

gerekmektedir. Bu sebeple hazırlanan "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" bir türlü yasallaşamamıştır.

Ayrıca bu suçun en çok işlenebileceği yer bilişim sistemleri olsa da sadece burada işlenebileceğini söylemek doğru değildir. Yani verilerin kaydedilmesi bir bilişim sistemine ya da veri taşıma aracına sayısal kod halindeki dar anlamda verilerin girilmesi şeklinde olabileceği gibi kişisel bilgilerin bir dosya kağıdına el yazısı ya da daktilo ile geçirilmesi şeklinde de olabilir[298].

Söz konusu suç serbest hareketli bir suçtur. Yani verilerin kaydedilmesi işleminin nasıl yapıldığı hususunun bu suçun gerçekleşmesi için her hangi bir özelliği yoktur. Ayrıca, bu suçta neticeye de önem verilmemiştir. Bir başka ifadeyle verilerin kaydedilmesi fiili bu şuçun oluşabilmesi için yeterlidir. Yine kayıt etme fiilinin aleniyete dökülüp dökülmemesinin, bu fiille bir zararın ortaya çıkıp çıkmamasının suçun oluşumunda bir önemi yoktur.

5.2.5.1.1.5. Hukuka Aykırılık Unsuru

Yasada, bu suçun oluşabilmesi için fiilin hukuka aykırı olarak işlenmesi gerektiği açıkça belirtildiğinden, hukuka aykırılık unsurunun özel olarak araştırılması ve failin gerçekleştirdiği fiilin hukuka aykırı olduğunu bilmesi aranmıştır.

Kişisel verilerin kaydedilmesi suçunda, kişinin rızası en temel hukuka uygunluk nedenidir. Rızanın varlığı durumunda bu suç oluşmayacaktır. Verileri kaydeden kişinin, veri sahibi veya ilgilisince verilen bir izne dayanarak verileri kaydetmesi veya kanunun kendisine verdiği bir yetkiye dayanarak böyle bir işlem yapması durumunda söz konusu suç oluşmayacaktır.

Mağdurun rızasına dayanan hukuka uygunluk sebebinde, mağdurun rızasının fiilin gerçekleştiği anda var olması gerekir. Bu rızanın zımni veya açık olması bir önem teşkil etmemektedir.

5.2.5.1.1.6. Suçun Manevi Unsuru

Bu suçun manevi unsuru bilerek ve isteyerek genel suç işleme kastıdır. Madde metninde fiilin hukuka aykırı olarak işlenmesinin vurgulanması nedeniyle failin kastının, fiilin hukuka aykırı olduğunu da kapsaması gerekir[299].

---

[298] Dülger, 2004:271.
[299] Karagülmez, 2005:230.

Kanunda bu suç için failin bilerek ve isteyerek hareket etmesi arandığı için taksirle işlenemez.

5.2.5.1.1.7. Suçun Nitelikli Halleri

5.2.5.1.1.7.1. Daha Az Ceza Verilmesini Gerektiren Hal

Bu suç tipi için yasada herhangi bir hafifletici sebep düzenlenmemiştir.

5.2.5.1.1.7.2. Cezanın Ağırlaştırılmasını Gerektiren Nitelikli Hal

YTCK'nın 137'nci[300] maddesinde özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenen suçlar için failin sıfatından dolayı ağırlaştırıcı nedenler öngörülmüştür.

Buna göre, anılan maddenin "a" bendinde kişisel verilerin kaydedilmesi suçunun bir kamu görevlisi tarafından ve görevinin verdiği yetkinin kötüye kullanılması durumunda failin cezası arttırılarak verilecektir.

Söz konusu maddenin "b" bendinde ise belirli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle bu suç gerçekleştirilirse failin cezası yine arttırılarak verilecektir.

5.2.5.1.1.8.Yaptırım

Kanunda kişisel verilerin kaydedilmesi suçunu işleyen failler için öngörülen ceza altı aydan üç yıla kadar hapis cezasıdır.

[300] Madde 137 "Nitelikli haller"
"Yukarıdaki maddelerde tanımlanan suçların;
a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,
b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,
İşlenmesi halinde, verilecek ceza yarı oranında artırılır."

5.2.5.1.2. Kişisel Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme Suçu (m.136)

5.2.5.1.2.1.Genel Olarak

YTCK'nın 136'ncı maddesinde "Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır." hükmüne yer verilmiştir.

Bu suç, en yaygın bir şekilde İnternet'te işlenmektedir. Kimlik hırsızlığı olarak da adlandırılan İnternet'teki kişisel verilerin ele geçirilmesi fiillerinde, genellikle müşterilerin ismi, doğum tarihi, sosyal güvenlik numaraları, kredi kartı bilgileri kendi bilgisi dışında ele geçirilmektedir. Daha sonra bu verilerle, haksız kazanç elde etmek üzere, İnternet dolandırıcılığı da olmak üzere pek çok suç işlenmektedir. Ele geçirilen kredi kartı bilgileri ise, çoğunlukla müşteri hesaplarından nakit para transferinde veya kartın sahte bir kopyasının çıkartılmasında kullanılmaktadır[301].

5.2.5.1.2.2. Korunan Hukuki Yarar

Bu suçla korunan hukuki yarar 135'inci maddede düzenlenen hukuki yararla aynıdır.

5.2.5.1.2.3. Fail ve Mağdur

Kişisel verilerin ele geçirilmesi suçunda da fail açısından bir özellik aranmadığından, bu suçun faili herkes olabilir.

Bu suçun mağduru da herkes olabilir. Ayrıca mağdur olmak için bilişim sistemine kaydedilen verilerin sahibi veya zilyedi olmasına da gerek yoktur. Ele geçirilen verilerin bireyle ilgili olması yeterlidir.

[301] Karagülmez, 2005:233:Fedorek'ten, 2004:5.

5.2.5.1.2.4. Suçun Maddi Unsuru

Bu suçla hukuka uygun olarak kaydedilen veya kaydedilmeyen kişisel verileri hukuka aykırı olarak başkasına verme, yayma, veya ele geçirme bağımsız bir suç olarak düzenlenmiştir[302].

Kişisel verilerin başkasına verilmesi fiilinde herhangi bir yöntem belirlenmemiş olması sebebiyle, bu suç çok değişik şekillerde işlenebilecektir. Bu duruma örnek olarak, yazılı verilerin elden ya da posta (e-posta) yoluyla verilmesi gösterilebilir.

Kişisel verilerin yayılması fiili de bir çok şekilde gerçekleştirilebilir. Örneğin mektupla bir çok kişiye gönderilerek gerçekleştirilebileceği gibi, bir web sitesinde yayınlanarak bu bilgileri erişebilir kılarak ya da forum odasında açıklama yaparak gerçekleştirilebilir[303].

Kişisel verilerin ele geçirilmesi fiili siber alanda en sık karşılaşılan suç tiplerindendir. Genellikle bilişim ortamında kişisel verilerin yetkisiz erişimle ele geçirilmesi en yaygın şekilde görülen fiillerdir.

Maddenin gerekçesinde de ifade edildiği gibi başkasına verilen, yayılan ya da ele geçirilen verilerin hukuka uygun olarak kaydedilmiş olup olmaması suçun meydana gelebilmesinin koşulu değildir. Veriler nasıl kaydedilmiş olursa olsun yukarıda belirtilen fiillerin gerçekleşmesiyle suç meydana gelmiş olacaktır.

5.2.5.1.2.5. Hukuka Aykırılık Unsuru

Bu suçun cezalandırılabilmesi içinde hukuka özel aykırılığın gerçekleşmesi gerekmektedir. Yani failin hukuka aykırı olarak hareket ettiğinin ispatlanması lazımdır.

Bu suç için de mağdurun rızası veya kanunla verilen bir yetkinin kullanılması, hukuka uygunluk sebebi olarak kabul edilecek, bu sebeple suç oluşmayacaktır.

---

[302] Madde gerekçesinden.
[303] Dülger, 2004:271.

5.2.5.1.2.6. Suçun Manevi Unsuru

Bu suç da kasten işlenebilen bir suçtur. Anılan maddede fiilin hukuka aykırı olarak işlenmesi gerektiği ifade edildiğinden, failinin kastının, fiilin hukuka aykırı olduğunu da kapsaması gerekir[304].

Kanunda bu suç için failin bilerek ve isteyerek hareket etmesi arandığı için taksirle işlenemez.

5.2.5.1.2.7. Suçun Nitelikli Halleri

5.2.5.1.2.7.1. Daha Az Ceza Verilmesini Gerektiren Hal

Bu suç tipi için yasada herhangi bir hafifletici sebep düzenlenmemiştir.

5.2.5.1.2.7.2.Cezanın Ağırlaştırılmasını Gerektiren Nitelikli Hal

YTCK'nın 137'nci maddesinde özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenen suçlar için failin sıfatından dolayı ağırlaştırıcı nedenler öngörülmüştür. Bu maddede düzenlenen durumların gerçekleşmesi durumunda, belirlenen ceza yarısı oranında arttırılarak verilecektir.

5.2.5.1.3.Verilerin Yok Edilmemesi Suçu (m. 138)

5.2.5.1.3.1. Genel Olarak

Bu maddeyle[305], hukuka uygun olarak kaydedilmiş kişisel verilerin kanunların belirlediği sürelerin geçmiş olmasına rağmen yok edilmemesi, bağımsız bir suç olarak tanımlanmıştır.

5.2.5.1.3.2. Korunan Hukuki Yarar

Bu maddeyle korunan hukuki yarar gerçek kişinin özel hayatı ve buna bağlı olarak kişisel verilerin korunmasıdır.

---

[304] İçel ve ark., 2000:8.

[305] Madde 138 "Verileri yok etmeme"
"Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir."

138'inci madde, sadece kamu tarafından tutulan kişisel verileri değil, hukuka uygun olarak elinde kişisel veri bulunduran özel kuruluşları da kapsamaktadır. Bu sebeple kamu ve özel kuruluşları kendilerinde mevcut olan kişisel verileri kanunların belirlediği sürelere uygun olarak yok edeceklerdir.

Bu suçla korunan diğer bir hukuki yarar ise kamu görevinin yerine getirilmesi sırasında disiplin oluşturmak ve kamu yararının elde edilmesini sağlamaktır[306].

5.2.5.1.3.3. Fail ve Mağdur

Bu suçun faili, verileri yok etmekle görevlendirilen kişidir. Söz konusu görev kanunlarla verilecektir. Her somut olayda kimlere nasıl bir veri yok etme görevi verildiği araştırılacaktır.

Bu suçla korunan hukuki değer kamu idaresine duyulan güven duygusuysa, suçun asıl mağduru da kamudur.

Fakat kişisel verileri yok edilmeyen ve bundan zarar gören şahıslar da davaya müdahil olarak katılabilirler.

5.2.5.1.3.4. Suçun Maddi Unsuru

Bu suç, verileri yok etmekle sorumlu olan kişinin görevini yerine getirmemesiyle oluşur. Verileri yok etmeme suçu ihmali hareketle gerçekleşmektedir. Yok etme verinin tamamen bir daha geriye döndürülemeyecek şekilde ortadan kaldırılmasıdır. Kısmen yok etmede, verinin kalan kısmı veri niteliği taşıyorsa anılan maddedeki suç gerçekleşir ve buna göre ceza verilir.

5.2.5.1.3.5. Hukuka Aykırılık Unsuru

Bu suçun mağdurunun kamu düzeni olması hasebiyle, anılan suçtan zarar gören kişinin rızası suçun hukuka uygunluk nedeni olarak kabul edilemeyecektir. Kanunda bu suç için herhangi bir hukuka uygunluk nedeni kabul edilmemiştir.

[306] Dülger, 2004:283.

5.2.5.1.3.6. Suçun Manevi Unsuru

Bu suçun manevi unsuru genel kast ile işlenmesidir. Yani fail, suçun kanuni tanımındaki unsurları bilerek ve isteyerek gerçekleştirmiş olmalıdır. Bu sebeple anılan suç taksirle işlenemez.

5.2.5.1.3.7. Yaptırım

Kanunda bu suçun cezası altı aydan bir yıla kadar hapis cezası olarak belirlenmiştir.

5.2.5.2. Bilişim Sistemleri Aracılığıyla İşlenebilecek Diğer Suç Tipleri

5.2.5.2.1. Haberleşmenin Gizliliğini İhlal Suçu (m.132)

YTCK'nın "haberleşmenin gizliliğini ihlal" kenar başlıklı 132'nci maddesinde, "(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır."hükmüne yer verilmiştir.

Bu suç YTCK'da düzenlenirken kanun koyucu ETCK'nın 195'inci maddesinden farklı olarak (bu maddede posta ve telefon haberleşmesinin gizliliği koruma kapsamına alınmıştır.) yalnızca "haberleşme" kavramına yer vermiş ancak bunun hangi yollarla gerçekleşeceğinden bahsetmemesi nedeniyle her türlü haberleşmenin bu maddenin koruma kapsamında olduğunu söylemek yanlış olmaz.

Bugün teknolojinin hızlı gelişimiyle beraber bilişim sistemlerinden yararlanarak özellikle de İnternet vasıtasıyla e-posta, elektronik sohbet (chat),

internet üzerinden telefon görüşmesi gibi çeşitli yöntemlerle haberleşme sağlanmaktadır. İşte bilgisayar ağları aracılığıyla yapılan bu yeni haberleşme yöntemleri YTCK'nın anılan maddesiyle koruma altına alınmakta ve bu tür haberleşmeyi ihlal edenler de cezalandırılmak istenmektedir. Ayrıca bu düzenleme ile yukarıda sayılan yöntemlerle yapılan haberleşmenin ihlal edilmesi durumunda ETCK'nın 195'inci maddesine göre cezalandırılıp cezalandırılamayacağına ilişkin tartışmalarda sona erdirilmiştir[307].

5.2.5.2.2. Haberleşmenin Engellenmesi (m.124)

YTCK'nın "haberleşmenin engellenmesi" kenar başlıklı 124'üncü maddesinde;

"(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adli para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezalandırılır." hükümlerine yer verilmiştir.

Yukarıda haberleşmenin gizliliğini ihlal suçuna ilişkin açıklamalar yapılırken de belirtildiği gibi günümüzde haberleşme büyük bir çoğunlukla e-posta ve İnternet'te sohbet aracılığıyla yapılmaktadır. Bu yöntemlerle haberleşmenin yaygınlaşmasının nedeni ucuz ve hızlı olmasıdır.

YTCK'nın 124'üncü maddesinde de yalnızca haberleşme denmesi ve haberleşme araçlarının belirtilmemesi nedeniyle haberleşme hangi araçla gerçekleştirilirse gerçekleştirilsin bunun engellenmesi suç olarak kabul edilmiştir.

[307] Dülger, 2004:287.

5.2.5.2.3. Hakaret Suçu (m.125)

YTCK'nın 125'inci maddesinde[308] düzenlenen hakaret suçu, bilgisayar ağları vasıtasıyla da işlenebilecek bir suçtur ve bu durum maddenin ikinci fıkrasında eylemin mağdura yönelik sesli, yazılı veya görüntülü bir iletiyle işlenirse hakaret suçunun gerçekleşeceği kabul edilmektedir.

Yine maddenin diğer fıkralarında belirtilen ağırlatıcı nedenlerden özellikle hakaret suçunun alenen veya sanal basın ve yayın yoluyla işlenmesinin bilgisayar ağları vasıtasıyla gerçekleştirilmesi çok sık rastlanılan bir durumdur. Bu düzenlemeyle bilgisayar ağları vasıtasıyla işlenen veya alenen olan ya da sanal basınla işlenen hakaret suçları ağırlaştırıcı neden olarak kabul edilmektedir.

5.2.5.2.4. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Hırsızlık Suçu (m. 142 fkr.2 b. "e")

YTCK'nın malvarlığına karşı suçlar başlıklı onuncu bölümünün 142'nci maddesinin ikinci fıkrasının "e" bendinde bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçuna yer verilmektedir. Teknolojinin her gün ileriye doğru gitmesi yeni siber suç işlenme şekillerinin ortaya çıkarması sebebiyle böyle bir düzenleme yapılması gerekliliği ortaya çıkmıştır.

Ancak bilişim sistemiyle gerçekleştirilen hangi tür hırsızlık eylemlerinin bu suçu oluşturacağı da bu düzenlemeden çıkarılamamaktadır. Bilişim sisteminin

---

[308] Madde 125 "Hakaret"
"(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adli para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir.
(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.
(3) Hakaret suçunun;
a) Kamu görevlisine karşı görevinden dolayı,
b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,
c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,
İşlenmesi halinde, cezanın alt sınırı bir yıldan az olamaz.
(4) (Değişik fıkra: 29/06/2005 - 5377 S.K./15. md.)(**) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır.
(5) (Değişik fıkra: 29/06/2005 - 5377 S.K./15. md.)(**) Kurul halinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi halinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır.

kullanılmasıyla somut nesnelerin çalınması mı yoksa verilerin çalınması mı bu suçla hüküm altına alınmak istenmiştir? Burada kişinin rızası dışında, failin kendisine veya başkasına yarar sağlamak amacıyla hareket edip kişinin eşya üzerindeki hakimiyetini bilişim sistemi aracılığıyla sona erdirilmesi fiiliyle bu suç gerçekleşecektir.

Yine burada belirtmek gerekir ki, bu suçun bağımsız bir suç olarak düzenlenmesi ve suçun konusunun neler olduğu ile hangi eylemlerin cezalandırılmak istendiğinin açıkça ifade edilmesi doğabilecek uygulama ve yorum hataları ile karışıklıkları önleyecektir[309]. Bu tip bir düzenleme yapılmadığından uygulamada çıkacak aksaklıkları düzeltmekte Yargıtay'a düşmektedir.

5.2.5.2.5. Bilişim Sisteminin Kullanılması Yoluyla İşlenen Dolandırıcılık Suçu (m.158 fkr.1 b. "f")

Bu suçla yukarıda incelenen bilişim sisteminin kullanılması yoluyla işlenen hırsızlık suçunun düzenlenme nedenleri ve yöntemleri aynı olduğundan, yukarıda yapılan açıklamalar bu suç için de geçerlidir.

Bu madde ile uygulamada siber suçların en sık karşılaşılan türlerinden biri düzenlenmekte ve bilgisayar ağlarıyla gerçekleştirilen hileli işlemler cezalandırılmaktadır.

5.2.5.2.6. Müstehcenlik Suçu (m.226)

YTCK'nın 226'ncı maddesinde[310] müstehcenlik suçu düzenlenmiştir. Bu maddede müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına

---

[309] Dülger, 2004:290

[310] Madde 226 "Müstehcenlik"
(1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,
b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,
c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,
d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,
e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,
f) Bu ürünlerin reklamını yapan,
Kişi, altı aydan iki yıla kadar hapis ve adli para cezası ile cezalandırılır.
(2) Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.

yönelik düzenlemelere yer verilmiştir. Maddede belirtilen yayınların bilgisayar ağlarıyla yayılması ve paylaşılması mümkün olduğundan bu suç bilgisayar ağları ile işlenebilmektedir.

Söz konusu düzenlemede, bu suçun bilgisayar ağlarıyla da işlenebileceğinin belirtilmemesi uygulamada karışıklıklara neden olabilecektir.

Ayrıca, çocuk pornografisinin Avrupa Konseyi Siber Suç Sözleşmesi dikkate alınmadan ayrı bir suç olarak düzenlenmemesi YTCK açısından önemli bir eksiklik oluşturmaktadır.

Her ne kadar maddede düzenlenen bu suç tipi yetersiz olsa da bilgisayar ağlarıyla işlenen müstehcen yayın fiillerine uygulanabilecektir.

Yukarıda açıklanan nedenlerden ötürü özellikle çocuk pornografisi ve her türlü pornografinin bilgisayar ağları yolu ile yayılması, satılması, depolanması fiillerinin ayrı bir suç olarak düzenlenmesi gerekmektedir.

5.3. YTCK İle İlgili Olarak Yapılan Eleştiriler

Öncelikle belirtmek gerekir ki YTCK'nın "Bilişim Alanında Suçlar" düzenlemesi ve diğer maddelerdeki düzenlemeleri genel olarak Avrupa Konseyi Siber Suç Sözleşmesinde yer alan suç tiplerini kapsar nitelikte olsa dahi bir takım eksiklikleri bünyesinde barındırmaktadır. Bunlardan en önemlisi yukarıda da

---

(3) Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.
(4) Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.
(5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır.
(6) Bu suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.
(7) Bu madde hükümleri, bilimsel eserlerle; üçüncü fıkra hariç olmak ve çocuklara ulaşması engellenmek koşuluyla, sanatsal ve edebi değeri olan eserler hakkında uygulanmaz.

belirtilmiş olduğu gibi çocuk pornografisinin Avrupa Konseyi Siber Suç Sözleşmesi dikkate alınmadan ayrı bir suç olarak düzenlenmemesidir.

YTCK'da "sistemlere girebilmek için parola ve şifrelerin hukuka aykırı olarak temini, dağıtımını ve satılmasını veya sistemlere girebilmek bakımından gerekli ekipman satımını, dağıtımını veya tedarikini" yaptırıma bağlayan bir düzenlemeye tasarıda dahi yer verilmemesi YTCK için bir eksiklik teşkil etmektedir.

765 sayılı TCK'da düzenlenmeyen "yasadışı erişim" olarak da adlandırabileceğimiz bilişim sistemine yetkisiz girilerek bilgilerin ele geçirilmeden öğrenilmesi fiili YTCK'nın 243'üncü maddesi ile suç olarak düzenlenmesi olumlu bir eleştiri olarak söylense de, bu suçun oluşabilmesi için aranan "orada kalmaya devam etme" unsuru sebebiyle bu suçun cezalandırılabilmesi güçleşmiştir. Ceza kanunu tasarısında bu ifade "bilişim sistemine hukuka aykırı olarak girilmesi veya orada kalınması" şeklindeydi. Yani tasarıda söz konusu suç seçimlik hareketli bir suç olarak düzenlenmekteydi. Kanun koyucu yapmış olduğu değişiklikle, elde olmayan nedenlerle veya istemeden, hatalı olarak bir bilişim sistemine girme durumunu göz önüne alarak, yetkisiz erişimi suç saymamış olması ihtimal dahilinde olsa da bu düzenleme suçun uygulanabilirliğini büyük ölçüde azaltmaktadır. Bu sebeple YTCK'da bir değişiklik yapılarak bu suçun tasarıdaki gibi düzenlenmesi gerekmektedir.

Bilgisayar ağlarının organize suçlarda ve sanal terörizmde bir araç olarak kullanılması durumlarının düzenlenmesi ve ilgili yasalarda düzenlenme yapılması gerekmektedir. Ayrıca yine şiddete çağrı, halkı kin ve düşmanlığa tahrik, suça teşvik ve terör örgütlerinin propagandalarını bilgisayar ağları aracılığıyla siber uzayda yapmaları hakkında da düzenleme yapılması gerekmektedir[311].

Terör eylemlerinin siber uzayda gerçekleştirilmesi hem bu eylemleri işleyenler için daha az riskli hem de suçun işlenişinin daha kolay olması sebebiyle bilgisayar ağları kullanılarak terör eylemlerinin gerçekleştirilmesi ağırlatıcı neden olarak kabul edilmelidir.

[311] Ünver, 2001:106-107.; Dülger, 2004:33.

Organize suç örgütlerinin bilgisayar ağlarını kullanarak işledikleri suçlar da ağırlaştırıcı neden olarak kabul edilmelidir. Bu konuda YTCK'da herhangi bir düzenleme olmaması önemli bir eksikliktir.

Yine bilgisayar ağları vasıtasıyla kumar oynatma ve oynama fiillerinin ayrı bir suç tipi olarak düzenlenmesi gerekmektedir. Bu konuda Türk Mevzuatında boşluk bulunmaktadır. YTCK'da bu fiiller için özel bir düzenleme mevcut değildir. Ülkemizde kumarhaneler yasaklanmışken, dileyen herkes bugün siber uzayda kumar oynayabilmektedir. Her ne kadar YTCK'nın 228'inci[312] maddesinde "kumar oynanması için yer ve imkan sağlanması" denilerek geniş bir ifade kullanılmış olsa da yorum sorunlarının yaşanmaması ve uygulamada karışıklıklara sebebiyet vermemek için "sanal alanda bilişim sistemleriyle kumar oynatılmasının" da madde metninde belirtilmesi gerekmektedir[313].

Türk mevzuatında SPAM'ı yasaklayan veya cezalandıran bir düzenleme bulunmamakla birlikte, SPAM ileti gönderilmesini engelleyebilecek hükümler bulunmaktadır. Bunlardan biri olan Tüketicinin Korunması Hakkında Kanun, sadece içeriği reklam olan e-postalara karşı bir yaptırıma sahipken, Medeni Kanunun 24 üncü maddesi ve devamı hükümleri, kitlelere gönderilen gayri ticari iletilere karşı korumayı sağlayan hükümlerdir. Ancak SPAM'la ilgili olarak etkin bir mücadele yapılabilmesi için ceza kanunda da bir düzenleme yapılması faydalı olacaktır.

Sanal alanda yer alan kişilerin cezai sorumluluklarına ilişkin olarak bugün için ülkemizde bir düzenlemenin mevcut olmaması sebebiyle suç ve failler tespit edilse dahi yasal boşluk sebebiyle bu kişilere ceza verilememektedir. Bu boşluk, ya yukarıda incelemiş olduğumuz Alman Teleservisler Yasası'nda düzenlendiği gibi ayrı bir yasal düzenleme yapılarak ya da konuyla ilgili yasalarda düzenleme yapılarak doldurulabilir.

---

[312] Madde 228 "Kumar oynanması için yer ve imkan sağlama"
"(1) Kumar oynanması için yer ve imkan sağlayan kişi, bir yıla kadar hapis ve adli para cezası ile cezalandırılır.
(2) Çocukların kumar oynaması için yer ve imkan sağlanması halinde, verilecek ceza bir katı oranında artırılır.
(3) Bu suçtan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.
(4) Ceza Kanununun uygulanmasında kumar, kazanç amacıyla icra edilen ve kar ve zararın talihe bağlı olduğu oyunlardır."

[313] Dülger, 2004:333

Yine İnternet kişileri olan İnternet servis sağlayıcıları, erişim sağlayıcıları ve içerik sağlayıcıların ceza hukuku açısından sorumlulukları ayrı ayrı düzenlenmelidir.

Siber suçlarla etkin bir şekilde mücadele edilebilmesi için ceza hukukunun ve ceza muhakemesi hukukunun birlikte ele alınması gerekmektedir. Siber suçların uluslararası niteliği, suçun işlendiği yer açısından bazı problemler çıkmasına sebep olmakta, bu da suçun kovuşturmasının nerede yapılması gerektiği konusunda sorun yaratmaktadır. Tezimizde belirtmiş olduğumuz gibi bu sorunların aşılabilmesi için uluslararası işbirliğine gidilmesi gerekmektedir. Şu an için 42 ülke tarafından imzalanmış olan Avrupa Birliği Siber Suç Sözleşmesi'nde bu konuyla ilgili olarak ayrıntılı düzenlemeler yapılmıştır. Bu Sözleşme henüz ülkemiz tarafından imzalanmamıştır. Sözleşme imzalanıp, suçun işlendiği yer konusu hakkındaki düzenlemelere YTCK'da yer verilirse bu problem büyük ölçüde giderilmiş olacaktır.

Son olarak, bilgisayar ağları üzerinden özellikle de İnternet'ten kişilik haklarına saldırılması söz konusu olursa, bu fiiller çok kısa zamanda çok fazla kişinin bilgisine ulaşmaktadır. Yine haber siteleri veya forum alanlarında bu fiillerin gerçekleştirilmesi durumunda Basın Kanunu'nda basılı eserlerde olduğu gibi İnternet açısından bir hüküm bulunmamaktadır. Bu sebeplerden ötürü hem bu alana ilişkin düzenlemelerin yapılması hem de İnternet'te hakaret, sövme, tehdit ve haberleşme özgürlüğünün ihlali gibi suçların işlenmesi ağırlaştırıcı neden olarak kabul edilerek, buna uygun düzenleme yapılması gerekmektedir[314].

[314] Karacaoğlu, Ömer; *İnternet Ortamında Gerçekleştirilebilecek Bir İhlal Türü Olarak Asılsız İsnat.* Bilişim Hukuku Net. http://www.bilisimhukuku.net/index.php?option=content&task=view&id=337&Itemid=40, (02.05.2005)

SONUÇ

Siber uzay ortamında mevcut olan ve bu ortamın baş aktörü olan İnternet'in bu kadar yaygınlaşmasını sağlayan en önemli özellik olarak kabul edilen özgürlüğün İnternet alanında yapılacak düzenlemeler ile sakatlanacağı ileri sürülmektedir. Fakat, bu alanda yapılan hukuksal düzenlemeler ölçülülük ilkesi göz ardı edilerek gereksiz biçim ve boyutta yapılmamışsa sansür veya özgürlükleri sınırlayıcı düzenlemeler olarak kabul edilmemelidir. Bu düzenlemeler ile hukuka aykırı fiillere hukuki yaptırımlar uygulanırken gerçekte İnternet alanında özgürlükler ve kullanımlar güvence altına alınmaktadır. Gelişmiş bir teknoloji ürünü olan İnternet, insan oğlunun faydasına kullanıldığında hukuka uygun ve yararlı olur, yoksa kişilerin bir bilgisayar sahibi olması ya da İnternet'in gelişmiş teknolojik niteliği suç işleme imtiyazını ve hukuksuzluğu ortaya çıkarmaz. Kısaca bu alanda düzenleme yapılması baskıcı ve özgürlükleri sınırlayan bir anlayış olmayıp, başkalarının özgürlüklerini korumak olarak anlaşılması gerekir.

Bilgisayar ağlarının özellikle de bu ağlardan İnternet'in kullanımının tüm dünyada yaygınlaşması ve insanlar için hayatın vazgeçilmez bir parçası durumuna gelmesi, bu ağların ceza ve ceza muhakemesi hukukunun en problemli alanını oluşturmasına sebep olmuştur. Günümüzde bilgisayar ve bilgisayar ağları aracılığıyla kolay ve kapsamlı suçlar işlenmeye başlanmıştır. Aynı zamanda siber uzay ortamında her geçen gün yeni bir suç tipinin ortaya çıkması nedeniyle ceza ve ceza muhakemesi kanunları yetersiz kalmaktadır. Bu sebeple bu alanı düzenlemek amacıyla getirilecek hukuki düzenlemelerde bilişim teknolojilerinin her an gelişmekte olduğu da göz önüne alınarak kısa bir süre içerisinde uygulanamayacak hale gelecek olan kanunların yapılmamasına dikkat edilmelidir. Bu konuda acele edilmeyerek bazı sorunların genel hükümler çerçevesinde çözülmesine gayret edilmelidir.

Ayrıca şunu belirtmek gerekir ki, İnternet üzerinden işlenen suçlarla ilgili cezai yaptırıma bağlayan temel bir yasa, İnternet'in bilgi ve iletişim aracı olması, çok hızlı gelişim göstermesi, teknolojik yönünün ağır basması ve tüm ülkeler arası bağlantıya sahip olması nedeniyle gerek hukukumuzda gerekse mukayeseli hukukta

henüz bulunmamakta olup, yukarıda belirtilen nedenlerden ötürü de böyle bir düzenlemenin siber suçlarla mücadelede faydalı olacağı düşünülmemektedir.

Siber uzay ortamını düzenlemek için özel bir kanun değil, ancak bu alanla ilgili özel düzenlemeler yapılmalıdır. Hem ceza hukuku hem de diğer hukuk dallarında bilgisayar ağlarıyla ilgili olarak yapılması gereken pozitif düzenlemeler için ya madde değişikliğine gidilmeli ya da yeni hükümler ilgili kanunlara eklenmelidir. Yani Ülkemizde, Kıta Avrupası siteminden ayrılınmayarak ABD ve İngiltere gibi Anglo-Sakson hukuk sistemini benimseyen ülkelerin aksine, tüm mevzuatımız gözden geçirilerek ilgili ve gerek görülen yerlerinde değişikliğe gidilmeli ya da ek düzenlemeler yapılmalıdır.

Siber suçlarla mücadele etmek amacıyla hazırlanan yasalarda dikkat edilmesi gereken husus, bireyin herhangi bir müdahaleyle karşılaşmaksızın düşünme, düşündüklerini ifade etme, her türlü bilgiyi ve düşünceyi sınırsız şekilde arama, alma ve iletme ve özel hayatın gizliliği haklarına saygı konusunda sağlıklı bir dengenin kurulmasıdır. Bu denge, ceza hukuku alanında yapılacak düzenlemelerde, ceza hukukunun "son araç" olma özelliğinin dikkate alınması, ceza muhakemesi alanında yapılan düzenlemeler de ise, elektronik ortamda delillerin toplanması için alınacak tedbirlerle bireyin hak ve özgürlükleri arasında uygun bir orantının kurulmasını gerektirmektedir.

Siber suçlar, günümüzde tüm dünya ülkelerinin en problemli konularından biri haline gelmiştir. Bununla birlikte bu suçların ciddiyeti konusunda gerek bireysel gerekse toplumsal düzeyde yeterli duyarlılık gösterilmemektedir. Bireylerin eğitimi ve bu suçlara karşı bilgilendirilmesinin gerekliliği önemli bir gerçektir. Özellikle çocukların küçük yaşlardan itibaren bilişim teknolojilerini kullanırlarken bir takım temel ahlak prensiplerine sahip olmalarını sağlamak hem ailelerin hem de devletin başlıca görevleri arasındadır. Burada devlet tarafından yapılması gereken müfredata konulacak bilgisayar derslerinde öğrencilere bu suçların ciddiyetinin anlatılması ve sanal alemde işlenen suçların gerçek hayatta işlenen suçlarla aynı olduğunun anlatılmasıdır. Bu şekilde genç neslin bilinçlendirilmesi durumunda ileride onların bu suçları işlemelerinin önüne geçilebilir. Ancak siber suçlular konusunda gazetelerde çıkan haberlere baktığımızda, siber suçlular zeki, yapmış oldukları fiiller

ise masum olarak gösterilmektedir. Hal böyle olunca bilgisayar teknolojilerine merakı olan gençlerin çoğunda bilgisayar korsanı olma isteği uyanmaktadır.

Siber suçlarla mücadelede mağdurlardan elde edilecek verilerin büyük bir önem taşıması nedeniyle mağdurların bu konudaki çekingenliği giderilmeye çalışılmalıdır. Burada belirtilmesi gereken bir husus da özellikle İnternet üzerinden ticari faaliyette bulunan şirketlerin, siber suçlar sebebiyle mağdur olduklarında, şirketin güvenliğini zarar gelecek ve bu durumun müşteri kaybına sebep olacağı endişesiyle bu suçları adli makamlara bildirmemeleridir. Bu durum siber suçlarla etkin bir şekilde mücadele edilebilmesini engellemektedir. Burada devlet, bu tip şirketlere belli güvenceler vererek, karşılaşmış oldukları siber suçları adli makamlara bildirmeleri konusunda teşvik etmelidir. Verilecek olan güvencelere örnek olarak ticari faaliyette bulunan şirketlerin bir siber suça maruz kalmaları durumunda, adli mercilerin soruşturmayı gizli yapmaları ve basına sızdırmamaları konusunda belli düzenlemeler yapılabilir. Yine soruşturma bilgilerinin basına sızdırılması durumunda, adli soruşturmayı yapan memurların cezalandırılmasına ilişkin düzenleme yapılabilir.

Günümüzde her ne kadar siber uzay ortamında işlenen suçlar Emniyet Teşkilatı için bir sorun olarak görünmüyorsa da İnternet ve elektronik ticaretin ülkemizdeki hızla gelişimi dikkate alındığında ileride bu alanda da suç patlaması olacağı tahmin edilmektedir. Bu sebeple bu suçlarla mücadele için gereken önlemlerin şimdiden alınması gerekmektedir.

Siber suçların takibi, tespiti ve yakalanması ancak bu konuda uzmanlaşmış personel ve sürekli bir çalışma ile mümkün olacaktır. Her gün değişen ve gelişen bilgisayar teknolojisinin gerisinde kalmamak için bilinen klasik polisliğin ötesinde teknik donanıma sahip gerek kolluk kuvvetlerinde gerekse Adalet Bakanlığı içinde konu hakkında uzman personelin istihdamı bugün için olmasa da yarının Türkiye'sinde bir mecburiyet teşkil edecektir. Bu sebeple en kısa zamanda bu alandaki eğitim ve yapılanma çalışmaları başlatılmalıdır.

Siber suçlarla ilgili olarak (elektronik) delil toplama konusunda başarılı olabilmek için de konunun; kurallar, teknik donanım ve uzman personel bağlamındaki dayanakları bir bütün olarak ele alınmalıdır. Yani yukarıda belirtilen unsurlara aynı anda sahip olunduğu zaman bu konuda başarılı olunabilecektir. Teknik donanıma sahip olunsa ama uzman personel olmasa siber suçlarla ilgili delil toplamada bir başarı sağlanamayacaktır.

Şu an için olmasa da ileride siber suçlarla daha etkin mücadele edebilmek için özel ihtisas mahkemeleri kurulması, bu suçlarla daha hızlı ve etkin mücadeleyi sağlayacak bir tedbir olabilir. Bu sebeple şimdiden teknik uzman personel yetiştirilerek geleceğe hazırlık yapılmalıdır.

Bu suçların ileride daha fazla işlenmesi nedeniyle insanlar arasında bu suçla ilgili olarak bilgi edinme isteği artacaktır. Bu isteklerini karşılayacak olanlar doğal olarak hukuk fakültesi mezunlarıdır. Bu sebeple hukuk fakültelerinin gerekli hazırlıkları yaparak, bilgisayar ağları ile ilgili suçlar başlıklı bir dersi ilk başta seçimlik ders olarak programlarında yer vermesi gerekmektedir.

Halihazırdaki mevzuatımızda siber suçların özellikle İnternet aracılığıyla işlenmesi durumunda, İnternet öznelerinin cezai sorumluluklarını belirleyen bir düzenleme mevcut değildir. İnternet'te yer alan kişiler olan içerik, servis ve erişim sağlayıcıları arasında bir ayrım yapılarak, her birinin ceza hukuku açısından sorumlulukları belirlenmelidir.

Gelecek yüzyılda tamamıyla olmasa da klasik terörün yerini siber terörün alacağı, çok büyük zararlara yol açacağı, bireylerin güvenliğinin, siber terörizmle daha fazla tehdit altında kalacağı düşünülmektedir. Bu sebeple ceza kanununda terör maksadıyla yapılacak siber eylemlerin ağırlatıcı hal olarak düzenlenmesi gerekmektedir.

Yine suç örgütleri, mafya ve mafya benzeri organize suçlulukta İnternet'in araç olarak kullanılması da ağırlatıcı neden olarak kabul edilmelidir.

İstenmeyen iletilerin (SPAM) muhatabın olumsuz rızasına karşın gönderilmesi, bu tip iletilerle etkin bir mücadele yapılabilmesi için ceza kanunda da

bir düzenleme yapılarak anılan iletileri gönderenlerin cezalandırılması gerekmektedir.

Siber suçlar genellikle uluslararası boyutta olduğu için, suçlular hukuk sistemlerindeki boşluklardan yararlanarak tutuklanma ve/veya kovuşturmadan kaçabilmektedirler. Bu nedenle, siber suçlarla mücadele edebilmek için her ülke kendi hukuk sistemi içerisinde ceza ve usul hukuklarında gerekli düzenlemeleri yaparak bu suçları işleyenleri cezasız bırakmamaları gerekmektedir. Ancak şu da bir gerçektir ki sadece milli kanunlarda yapılan düzenlemeler bu suçlarla mücadelede tek başlarına yeterli olamamaktadırlar. Bu sebeple, siber suçlarla etkin bir mücadele yapabilmek için devletlerin ortak bir bilinçle hareket etmeleri gerekmektedir.

Yukarıda belirtilen gereksinimden hareketle, Türkiye'nin üyesi olduğu Avrupa Konseyi tarafından hazırlanan Avrupa Siber Suç Sözleşmesi'nin bir an önce kabul edilerek, bu Sözleşmede yer alan hükümler doğrultusunda milli mevzuatımız uyumlaştırılmalıdır. Her ne kadar YTCK'da siber suçlara ilişkin düzenlemeler yapılırken bu Sözleşmeyle getirilen hükümlere uygun düzenlemeler yapılmaya çalışılsa da, bir çok eksiklik mevcuttur. Bu Sözleşmenin imzalanmasıyla birlikte siber suçlarla etkin bir şekilde mücadele edilmesi mümkün olacak ve kovuşturma açısından yetki sorununun aşılması sağlandığından siber suçların faillerinin belirlenmesi ve yakalanması kolaylaşacaktır.

KAYNAKLAR

ADALI, Eşref: "İnternet Suçları", Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Paneli, Bursa, 24 Mart 2001.

AKBULUT, Berrin, "Türk Ceza Hukukunda Bilişim Suçları", (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Doktora Tezi), Konya, 1999.

AKÇAM, Bahadır, *Suçla Mücadele Edenler İçin İnternet*, Türkiye Bilişim Derneği Yayınları, Ankara, 1999.

AKDENİZ, Yaman, *Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach*, Cyber-rights & Cyber – Liberties. 2000, (çevrimiçi)

http://www.cyber-rights.org/reports/governan.htm, 10 Aralık 2004.

AKDENİZ, Yaman, *Section 3 of the Computer Missuse Act 1990: an Antidote for Computer Viruses!. Web Journal of Current Legal Issues,* 1996, (çevrimiçi)

http://webjcli.ncl.ac.uk/1996/issue3/akdeniz3.html, 24 Aralık 2005.

AKDENİZ, Yaman. *The Regulation of Pomography and Child Pomography on the Internet*, Cyber-rights & Cyber – Liberties, 2001, (çevrimiçi) http://www.cyber-rights.org/documents/us_article.pdf, 19 Eylül 2004.

AKGÜL, Mustafa,. *Türkiye İnterneti'nin ve İnternet Kurulunun Kısa Tarihi*, Türkiye Bilişim Derneği, 2001, (çevrimiçi)

http://dergi.tbd.org.tr/yazarlar/20082001/mustafa_akgul.htm, 22 Ağustos 2004.

AKGÜN, K.; H. IŞIKLI, M. İNCE, H. PEKŞİRİN, *İnternet Yayıncılığı ve Internet Servis Sağlayıcılarının Sorumlulukları, Genel Politikalar ve Düzenleme Önerileri*, (çevrimiçi)

http://www.teknoturk.org/docking/yazilar/tt000086-yazi.htm, 22 Temmuz 2005.

AKINCI, Hatice, A. E. KILIÇ, C. ER, "Türk Ceza Kanunu ve Bilişim Suçları", *İnternet ve Hukuk*, der. Yeşim ATAMER, ss.156-275, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

AKINCI, S. Füsun, "Avrupa Konseyi Siber Suç Sözleşmesinde Yer Alan Maddi Ceza Hukukuna İlişkin Düzenlemeler ve Özellikle İnternette Çocuk Pornografisi", İÜHFM, Cilt LIX, Sayı 1-2, 2001, ss.11-38.

Ankara Ticaret Odası Yayınları, *Elektronik Ticaret ve İnternet*, Ankara, 1999, (çevrimiçi)

http://195.155.145.1/turkce/index10.html, 28 Mart 2005.

ARTUK, Mehmet Emin, A. GÖKÇEN, C. YENİDÜNYA, C*eza Hukuku Genel Hükümler-I*, Ankara, Seçkin Yayın Evi, 2002.

AYDIN, Emin, *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınları, Ankara, 1992.

BAŞARAN, Funda, Ö. ÖZDEMİR, "Türkiye'de İnternet'in Dünü, Bugünü". 01 Aralık 2003, (çevrimiçi)

http://www.hacettepekamu.org/forum_posts.asp, 12 Nisan 2005.

BAYRAKTAR, Köksal, " Banka Kredi Kartları İle Ortaya Çıkan Ceza Hukuku Sorunları", Prof. Dr. M. Kemal Oğuzman'ın Anısına Armağan, Beta Yayınevi, İstanbul, 2000, ss.195-203.

BECENİ, Yasin, "Siber Suçlar", 2003, (çevrimiçi)

www.hukukcu.com/bilimsel/kitaplar/yasinbeceni/indeks.htm, 29 Nisan 2004.

BECENİ, Yasin, "Siber Uzayda Mahremiyet", 2004, (çevrimiçi)

www.bilisimsurasi.org.tr/hukuk/docs/siber_uzayda_mahremiyet.pdf, 29 Mayıs 2004.

BEYHAN, Cem, "Bilişim Sucları İle Etkin Mücadele Yöntemleri", (çevrimiçi)

http://birimweb.icisleri.gov.tr/strateji/rapor/Bilisim_suc_m%FCcadele.html, 13 Ekim 2005.

BİLA, Cenk, "Bireysel ve Kitle İletişim Aracı Olarak İnternet ve Toplumsal Etkileri", (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), Ankara, 2001.

BOĞAÇ, Erkan, M. SONGÜR, *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü*, Hacettepe-TAŞ Yayınevi, Ankara,1999.

BRENNER, Susan, "Can There be Truly Virtual Crime- Part I: Virtual Crimes - The Issues", (çevrimiçi)

www.cybercrimes.net/virtual/brenner/Part l.html, 17 Eylül 2004.

BRENNER, W. Susan. *Is There Such a Thing as "Virtual Crime"?*, Computer Crime Research Center. 1999, (çevrimiçi)

^http://www.crime-research.org/library/Susan.htm, 13 Eylül 2004.

BUGMAN, *Telnet Nedir?*, PCnet - Bilgisayar ve İnternet Dergisi, 2002, (çevrimiçi)

http://www.pcnet.com.tr/modules.php?name=Forums&file=viewtopic&p=116314, 01 Nisan 2005.

CADEN, Marc L., LUCAS Stephanie E., *Accidents On The İnformation Super Highway, The Richmond Journal of Law and Technology*, 1996, (çevrimiçi)

www.law.richmond.edu/jolt/v2i1/caden_lucas.html, 27 Nisan 2005.

CERRAH, İbrahim: "Bilişim Teknolojileri ve Etik", Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Paneli, Bursa, 24 Mart 2001.

CHEBİUM, Raju, *Experts Say More Laws Won't Stop Computer Hackers*, 2000, (çevrimiçi)

www.cnn.com/2000/LAW/05/05/love.bug/index.html, 17 Aralık 2004.

COLLİNS, Matthew, "*The Law of Defamation and The Internet"*, Oxford University Press, London, 2001.

Council of Europe, *Convention on Cybercrime Explanatory Report*, ETS. No. 185, (çevrimiçi)

http://conventions.coe.int/Treaty/en/Reports/Html/185.htm, 16 Ekim 2004.

Council of Europe, *Convention on Cybercrime*, 2001, (çevrimiçi)

http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm, 16 Ekim 2004.

ÇAĞILTAY, Kürşat, *Herkes İçin İnternet*, Ankara, 2001.

ÇEKEN, Hüseyin, "Amerika Birleşik Devletlerinde Siber Suçlar", 2002, (çevrimiçi)

www.jura.uni-sb.de/turkish/HCeken.html, 17 Nisan 2005

ÇEKEN, Hüseyin, "Council Of Europe's Convention 2001 On Cybercrimes and Turkey", (Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), İstanbul, 2003.

ÇEKEN, Hüseyin; "ABD'de Internet Yoluyla İşlenen Suçlardan Doğan Ceza Sorumluluğunun Hukuki Esası", (çevrimiçi)

http://www.jura.uni-sb.de/turkish/HCeken1.html, (18.05.2005)

DAMON, W.D. Wright, *Cybercrimes*, Venable LLP, 2003, (çevrimiçi)

http://www.venable.com/docs/resources/ebookcybercrimes.cfm, 18 Mayıs 2005.

DEĞİRMENCİ, Olgun : "Bilişim Suçları", (Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi), İstanbul, 2002.

DEĞİRMENCİ, Olgun, "Ceza Hukuku Açısından Kredi ve Banka Kartları", *Legal Hukuk Dergisi*, S.3, Mart 2003, ss.592-609);

DEMİR, Önder, "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu", *Dokuz Eylül Üniversitesi Ulıslararası İnternet Sempozyumu*, ss.471-484, İzmir, 2002.

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

DIBEL, Julian, *A Rape in Cyberspace (or tinysociety, and how to make one)*, 1998, (çevrimiçi)

http://www.juliandibbell.com/texts/bungle.html, 14 Mayıs 2004.

DIBEL, *Julian, My Dinner With Catharine MacKinnon And Other Hazards of Theorizing Virtual Rape*, 1996, (çevrimiçi)

www.juliandibbell.com/texts/mydinner.html, 14 Mayıs 2004.

DOĞAN, Koray, "Bilişim Suçları ve Yeni Türk Ceza Kanunu", *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, Y:2, S:6-7, Ekim 2005, ss. 290-319.

DOKURER, Semih, *Ülkemizde Bilişim Suçları ve Mücadele Yöntemleri*, Emniyet Genel Müdürlüğü, 2003, (çevrimiçi)

www.egm.gov.tr/docs/inet-tr2001Metni.pdf, 24 Mart 2004.

DÜLGER, M. Volkan, *Bilişim Suçları*, Seçkin Yayıncılık, Ankara, 2004.

EKİNCİ, Mustafa, *Banka Kartları ve Kredi Kartları*, Adalet Yayınları, Ankara, 2002.

EREM, Faruk, "Bilgisayar Suçları ve Türk Ceza Kanunu" *İstanbul Barosu Dergisi*, C.69,S.10-11-12, Ekim-Aralık 1993, ss.727-732.

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

FEDOREK, Thomas, "Computers + Connectivity = New Opportunities for Criminals And Dilemmas for Investigators", *The New York State Bar Association Journal*, Vol.76, No.2, February 2004.

GIBSON, W., *Neuromancer*, Grafton Books - Collins Publishing Group, London, 1984.

GÖKÇOL, Orhan, *Usunet Nedir?*, 1997, (çevrimiçi)

http://www.po.metu.edu.tr/links/inf/css25/bolum4.html, 31 Mart 2005.

GÖKÇOL, Orhan. *TCP/IP Nedir?*, 1997, (çevrimiçi)

http://www.po.metu.edu.tr/links/inf/css25/bolum1.html, 25 Mart 2005.

GRABOSKY, Peter: "Cyber Crime And Information Warfare", Australian Institute of Criminology, *Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service*, Canberra, 9-10 Mart 2000, (çevrimiçi)

www.aic.gov.au/conferences/transnational/grabosky.pdf, 12 Ekim 2005.

GRINGRAS, Clive; "*The Laws of the Internet"*, Second edition, Butterworths LexisNexis, London, 1999.

GRİFFİTHS, T. Richard, "TheCreationof ARPANET", 2002, (çevrimiçi)

http://www.let.leidenuniv.nl/history/ivh/chap2.htm, 06 Eylül 2004.

GÜNAYDIN, Barış, *Türkiye'de İnternet Hukuku ve İnternet Davaları*, (çevrimiçi)

http://www.hukuki.net/hukuk/index.php?article=259, 13 Nisan 2005.

GÜNGÖR, Müberra, G. EVREN: *İnternet Sektörü ve Türkiye İncelemeleri*, 2002, (çevrimiçi)

.http://www.tk.gov.tr/yayin/Raporlar/pdf/internetraporu.pdf, 11 Mayıs 2002.

GÜRAN, Sait, T. AKÜNAL, K. BAYRAKTAR, E. YURTCAN, A. KENDİGELEN, Ö. BELLER, B. SÖZER: "İnternet ve Hukuk", *Superonline Workshop Metni*, İstanbul, 2000.

HELVACIOĞLU, A. Deniz, "Avrupa Konseyi Siber Suç Sözleşmesi Temel Hükümlerinin İncelenmesi", *İnternet ve Hukuk*, der. Yeşim ATAMER, ss.277-299, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

ICOVE David, Karl Seger, William Vonstorch, *Computer Crime*, O'Reilly & Associates, 1995.

İÇEL, Kayıhan, "Avrupa Konseyi Siber Suç Sözleşmesi Bağlamında Avrupa Siber Suç Politikasının Ana İlkeleri", İÜHFM., Cilt.LIX, S.1-2, İstanbul, 2001, ss.3-10.

İÇEL, Kayıhan, "*Kitle Haberleşme Hukuku (Basın,Radyo-Televizyon, Sinema, İnternet)*", 5. Baskı, Beta Yayıncılık, İstanbul, 2000.

İÇEL, Kayıhan, F. S. AKINCI, İ. ÖZGENÇ, A. SÖZÜER, F. MAHMUTOĞLU, Y. ÜNVER, *Suç Teorisi*, 2. Kitap, Yeniden Gözden Geçirilmiş İkinci Baskı, İstanbul, Bata Yayıncılık, 2000.

İNCEKAŞ, Serkan: "Bilgisayara (Kullanıcıya) Dışarıdan (Haksız) Müdahale", *10 - 12 Mayıs 2002 tarihinde Ankara'da yapılan Türkiye Bilişim Şur'asına İzmir Barosu adına sunulmuş tebliğdir.*

KANGAL, Zeynel T., Fransa'da İnternet Yoluyla İşlenen İşlenen Suçlardan Doğan Ceza Sorumluluğu, İÜHFM, C.LIX, S.1-2, İstanbul, 2001, ss.227-240.

KANGAL, Zeynel T., *Tüzel Kişilerin Ceza Sorumluluğu*, Seçkin Yayıncılık, Ankara,

KARACAOĞLU, Ömer, *İnternet Ortamında Gerçekleştirilebilecek Bir İhlal Türü Olarak Asılsız İsnat*, Bilişim Hukuku Net, (çevrimiçi)

http://www.bilisimhukuku.net/index.php?option=content&task=view&id=337&Itemid=40, 02 Mayıs 2005.

KARAGÜLMEZ, Ali, *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Seçkin Yayıncılık, Ankara, 2005.

KESMEZ, Necdet : "Avrupa Konseyi ve Siber - Uzay Suçları", Bilişim Kültürü Dergisi, 2001, (çevrimiçi),

http://tbd.org.tr/sayi79_html/hukuk_kesmez.html, 11 Eylül 2004

KOCA, Mahmut, "Avrupa Konseyi Siber Suç Sözleşmesi'nin Maddi Ceza Hukuku Alanında Öngördüğü Düzenlemeler ve Türk Hukuku", *Ünal Tekinalp'e Armağan Cilt. III.*, ss. 785-816, İstanbul, 2003.

KURT, Levent, *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yayıncılık, Ankara, 2005.

LEINER, M.Berry at al., *A Brief History of the Internet, Internet Society*, 2003, (çevrimiçi)

http://www.isoc.org/internet-history/brief.html, 26 Aralik 2005.

LlOYD, Ian J, *Information Technology Law*, Butterworths, Londan, Edinburh, Dublin, 2000.

MAGNİN, J. Cedric, *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?*, 2001, (çevrimiçi)

http://www.magnin.org/Publications/2001.06.SCU.LLMDissertation.PrHammond.COEConvention.Cyber-crime.pdf, 09 Aralık 2004.

MEMİŞ, Tekin, *Hukuki Açıdan Kitlelere E-posta Gönderilmesi*, Saarbrücken Hukuki İnternet Projesi, (çevrimiçi)

www.jura.uni-sb.de/turkish/TMemis1.html, 18 Ağustos 2005.

NAGPAL, Rohas, *What is a Trojan?*, Asian Schol of Cyber Laws, 2004, (çevrimiçi)

www.asianlaws.org/cyberlaw/library/cc/what_trojan.htm, 11 Kasım 2005.

New York Eyalet Mahkemesi, *Prody Vakası*, 1995, (çevrimiçi)

www.phillipsnizer.com/library/cases/lib_case80.cfm, 07 Mayıs 2004.

ÖNDER, Ayhan, *Şahıslara ve Mallara Karşı Cürümler ve Bilişim Alanında Suçlar*, Filiz Kitapevi, İstanbul, 1994.

ÖZCAN, Mehmet, "Yeni Milenyumda Yeni Tehdit: Siber Terör", 2004, (çevrimiçi)

http://www.turkishweekly.net/turkce/makale.php?id=12, 18 Temmuz 2005.

ÖZDİLEK, Ali Osman, "Bilgisayar Suçları Ne Kadar Ciddi?", 2002a, (çevrimiçi),

http://www.hukukcu.com/bilimsel/kitaplar/bilgisayar_suclari.htm 11 Mayıs 2004.

ÖZDİLEK, Ali Osman, *İnternet ve Hukuk*, Papatya Yayıncılık, İstanbul, 2002b.

ÖZEL, Cevat, "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", İstanbul Barosu Dergisi, C.LVI, S.7-8-9, Eylül 2001, ss.858-872.

ÖZEL, Cevat, *Bilişim-İnternet Suçları*, Bahçeşehir Üniversitesi Sürekli Eğitim Merkezi, 2002, (çevrimiçi)

http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm, 13 Mayıs 2004.

ÖZEL, Cevat: "Bilişim Suçları ile iletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", *İnternet ve Hukuk*, der. Yeşim ATAMER, ss.341-361, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

PHİLİPPSOHN, Steven, Samanta Thomas, "E-fraud - What Companies Face", *Computer Fraud & Security*, Volume.2003, Issue.1, January 2003.

QUARANTİELLO, E. Laura, *Cyber Crime*, LimeLigts Book, 1997.

SARIHAN, Tan Deniz, *Herkes İçin İnternet*, Sistem Yayıncılık, İstanbul, 1995.

SEVİ, Evrim Nüket; "İnternet Servis Sağlayıcılarının Hukuki Sorumluluğu", *Banka ve Ticaret Hukuku Dergisi*, Sayı. 3., Cilt. XXII., Haziran 2004, ss.189-231.

SINAR, Hasan, *İnternet ve Ceza Hukuku*, Beta, İstanbul 2001.

SINAR, Hasan, İstanbul Bilgi Üniversitesi ve İstanbul Barosu tarafından 16 Mart 2002 tarihinde düzenlenen İnternet ve Ceza Hukuku konulu paneled yapılan konuşması. İnternet ve Hukuk, der. Yeşim ATAMER, ss.277-299, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004, ss. 659-669.

SIRABAŞI, Volkan, "Radyo Televizyon ve İnternet Aracılığıyla Kişilik Haklarına Tecavüz", (Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi) Ankara, 2002.

SIRIMCIYAN, Ali, Domain Hırsızları, CHIP, Mart 2000 sayısı, s.258.

SİEBER, Ulrich "Internet Law Part I", Computer Law and Security, Report Vol:13, No:3, Köln, 1997.

SİEBER, Ulrich, "Legal Aspects of Computer-Related Crime in Information Society - A Comcrime Study", 1998, (çevrimiçi)

http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html, 17 Ağustos 2004.

STONEBANK, Michael, *What is Usenet News?*, 1994, (çevrimiçi)

http://www.eps.surrey.ac.uk/FAQ/usenet.html, 30 Mart 2005.

ŞEHİTOĞLU, Onur, Bilgisayar ve Ağ Üzerinden İşlenen Siber Siber Suçlarla Mücadelenin Hukuksal ve Güvenlik Boyutu (Kara Harp Okulu Savunma Bilimleri Enstitüsü, Yüksek Lisans Tezi), Ankara, 2005.

T.C. Başbakanlık, *Bilgi Toplumuna Doğru*, Türkiye Bilişim Şurası Taslak Raporu,

T.C. Ulaştırma Bakanlığı İnternet Üst Kurulu, *İnternet Üst Kurulu SPAM Bildirgesi*, 2000, (çevrimiçi)

http://kurul.ubak.gov.tr/m08.php, 18 Ağustos 2005.

TechTarget, *TCP/IP*, 2005, (çevrimiçi)

http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci214173,00.html, 03 Ağustos 2005.

The Information Security Glossary, *Logic Bomb*, 2002, (çevrimiçi)

http://www.yourwindow.to/information-security/gl_logicbomb.htm, 17 Temmuz 2005.

TUNCEL, Mustafa, *Bilgisayar Ağları*, Kişisel web sayfas, 2004, (çevrimiçi)

http://www.mtuncel.com/bilgisayaraglari.htm, 14 Ocak 2005.

UÇKAN, Özgür, Y. BECENİ : "Bilişim-İletişim Teknolojileri ve Ceza Kanunu", *İnternet ve Hukuk*, der. Yeşim ATAMER, ss.363-430, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2004.

Unıted Natıons Crıme And Justıce Informatıon Network, *International Review of Criminal Policy – United Nations Manual on The Prevention And Control Of The Computer- Related Crime*, (çevrimiçi)

http://www.uncjin.org/Documents/irpc4344.pdf, 14 Temmuz 2005.

ÜLŞEN, Recep; ANALAY, Cengiz, *Bilişim Suçları İçinde Çocuk Pornografisi Ve Mücadele Yöntemleri*, (çevrimiçi)

http://www.hukuki.net/, 14 Temmuz 2005.

ÜNVER, Yener, "TCK VE CK Tasarısının İnternet Açısından Değerlendirilmesi", İÜHFM., Cilt.LIX, S.1-2, İstanbul, 2001, ss.51-153.

WHITTAKER, Jason, *The Internet: The Basic*, Taylor & Francis Group, NewYork 2002.

WROBLESKI, M. Henry- M.K. HENS , "*Introduction to Law Enforcement and Criminal Justice*", third edition, West Publiching Company, 1990.

YAZICIOĞLU, Yılmaz, "Bilgisayar Ağları ile İlgili Suçlar Konusunda Türk Ceza Kanunu 2000 Tasarısı", *Dokuz Eylül Üniversitesi Ulıslararası İnternet Sempozyumu*, ss. 451-470, İzmir, 2002.

YAZICIOĞLU, Yılmaz, "*Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuki Boyutları İle*", Alfa Yayıncılık, İstanbul, 1997.

YAZICIOĞLU, Yılmaz, "Bilişim Suçları Konusunda 2001 Türk Ceza Kanunu Tasarısının Değerlendirilmesi", *Hukuk ve Adalet: Eleştirel Hukuk Dergisi*, İstanbul, Y:1, S:1, Ocak-Mart 2004, ss. 172-185.

YENİDÜNYA, A.Caner; O. Değirmenci, *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayıncılık, 2003.

YENİSEY, Feridun, "İnternet Suçlarının Yeni İşleniş Biçimleri", *Dokuz Eylül Üniversitesi Ulıslararası İnternet Sempozyumu*, ss. 447-450, İzmir, 2002.

ZETTER, Kim, "Yeni Nesil Virüsler", PC Life, Aralık 2000.