T.C.
DİCLE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

(YÜKSEK LİSANS TEZİ)

BİLİŞİM SUÇLARI VE TÜRK HUKUK SİSTEMİNDEKİ YERİ

HALİL İBRAHİM DİLEK

DANIŞMAN
PROF.DR.AHMET GÜRBÜZ

KAMU HUKUKU ANABİLİM DALI

DİYARBAKIR-2007

ÖZET

Bilişim Suçları; her türlü teknolojinin kullandığı araçlarla işlenen suçlardır. Bunların içerisine; bilgisayar, Internet, Pos makineleri, cep telefonları gibi teknolojik cihazları sayabiliriz. Bilişim Suçlarının kısa tanımı bu şekildedir. Ülkelere göre bu tanım ve adlandırmalar değişebilmektedir. Bu suçlarla mücadelede hukuki yapılanmalarda ortaya çıkmaktadır. Ülkemizde de bu suçlarla mücadele için 5237 sayılı Yeni Türk Ceza Kanunu'nda gerekli maddeler ortaya konulmuştur.

Bilişim suçunun tanımını ve yöntemlerini bilmeden onunla mücadele etmenin zor olacağı hatta imkânsız olacağı aşikârdır. Bunun için bu suçlardan kastedilenin ne olduğunu, nasıl işlendiğini, hangi yöntemlerin kullanıldığının açıklanması gerekmektedir. Bu yüzden birinci bölümde bu suçların tanımıyla birlikte sınıflandırılması, suçun yöntemleri, teknikleri ve türleri incelenmiştir. Bu suçları anlamak gerçekten teknik bir çalışmayı ve bilgiyi gerektirmektedir.

Bilişim suçlarının daha iyi anlaşılması için bu bilgiler gerçekten önemlidir. Ülkemizde bu konuyla ilgili bilgiler çok dağınık bir şekildedir. Henüz bununla ilgi kapsamlı bir eser ortaya konulmamıştır. Bu çalışmadaki amacım bu dağınık bilgileri toplamak ve gerekli eklemeleri yaparak bir bütünsel çalışma ortaya koymaktır.

Özellikle bu suçlarla mücadele ederken gerekli hukuki düzenlemelerin ne seviyede olduğunu görmekte fayda olacağına inanıyorum. Yapılan düzenlemelerin şuan için yeterli olduğu düşünülüyorsa da kanımca ileriki dönemlerde yetersiz kalacaktır. Ayrıca hukuki olarak da dağınıklık göze çarpmaktadır. Bu suçlarda, 5237 sayılı Türk Ceza Kanunu'nun içerisinde Onuncu Bölüm başlığı altında ve ayrıca Nitelikli Dolandırıcılık başlıklı 158. maddenin "f" bendinde de "Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle" işlenmesi şeklinde düzenlenmiştir. Bu çalışmada görüleceği üzere sadece bu kanunun düzenlemesinin yeterli olmadığı, bunun yanında 5846 sayılı Fikir ve Sanat Eserlerini Koruma Kanunu kapsamındaki birçok suçunda teknolojik cihazlarla işlendiği ve bilişim suçları kapsamında olduğu görülmektedir. Belki de ileriki yıllarda 5070 sayılı Elektronik İmza Kanunu gibi Bilişim Suçlarıyla ilgili ayrı bir hukuki düzenlemenin yapılması kaçınılmaz olacaktır.

Internet gibi bilgi deryası bu çalışmayı yaparken tabi ki en büyük kaynağım oldu. Burada bulunan makalelerden ve fikir yazılarından yararlandım. Bunları belirli bir düzen içerisinde sunmak anlaşılabilir kılmak benim temel amacım oldu.

Sonuç olarak; Bilişim Suçlarıyla hukuki ve teknik olarak mücadele etmek için teknolojik gelişmelerin takip edilmesi, personelin bu yönde eğitilmesi ve buna paralel olarak hukuki düzenlemelerin yerel ve küresel olarak düzenlenmesi gerekmektedir.

ABSTRACT

Technoligical Crimes; these are the crimes commites by the all means that the technology uses. We can exemplify these means as Internet, bank machines, cellular phones and etc. This is how we briefly define the crimes. The definitions and the name can vary according to the countries at hand. The struggle against these crimes create legal restructural formations into the 5237 Turkish Penal Code. Necessary articles have been put to struggle against these crimes in our country.

It is obvious that the struggle against technological crimes will be difficult or even impossible without knowing the definitions and the methods to handle. That is why it is a must what is meant by these crimes, how these crimes are committed, what sort of methods are used that needs to be explaines. So, in the first chapter, the definition of these crimes, classification, methods,techniques and varieties had been processed. To understand these crimes actually, technical study and information.

These informations really important for the technological crimes to be understood. In our country the information about the issue has not been compact but spread. No conclusive written work had been printed about these crimes up till now. My purpose in this work is to bring together the spread information and add necessary attachments to produce a beter built and a complete work.

I believe that it will be helpful to see what the level of these penal codes are especially while use struggle with these crimes. Even though the arrangements in my understanding are seeming enough for how will not be for the future. Besides, from the legal side point of view, story is the same. These crimes have been seen as well qualified fraud even though they have been in Chapter 10 of the 5237 Turkish Penal Code. In this work as will be seen, it is not only enough fort his code to be arranged, besides, 5846 code,the protection of opinion and work of art crimes have been committed by technological means and included in the technological it will be inescapable to have distinct rearrangements fort he technological crimes. Maybe in the following years to have distinct rearrangements for the technological crimes 5070 Electronic Signature Code.

While I was doing this work I used the Internet which is the ocean of information. The articles and the opinions were the sources I have used. And the first priority of wine was to present the information in arrangement that is much easier to understand.

As a result; To struggle against these technological crimes with legality and technicality, it is a necessity to follow all the developments, educate all the personel in this tilt and set up penal arragements both locally and globally.

TUTANAK

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu çalışma jürimiz tarafından KAMU HUKUKU Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan :

Üye :

Üye :

Üye :

Üye :

ONAY

Yukarıda imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım. …./…/2007.

……..

ÖNSÖZ

21.yüzyıl bilişim ve teknoloji çağı olarak tanımlanmaktadır. Bu yüzyıldaki gelişimler o kadar hızlı olmaktadır ki takip etmek, yetişmek ve adapte olmak zorlaşmaktadır. Tabi ki bu gelişimin en büyük aracıda bilgisayar olmaktadır. İnsanoğlunun aya çıkma hedefini gerçekleştirmede, uzay teknolojisinde kullanılmak için tasarlanan ve geliştirilen bilgisayarlar artık hayatımızın her alanına girmiş bulunmaktadır. Bu gün nerdeyse ülkemizde bilgisayarsız okul bulunmamakta ve özellikle genç nesiller bu aleti bir şekilde kullanarak öğrenmekte ve faydalanmaktadırlar.

Gelişimi ve kullanım alanıyla bilgisayarlar sosyal hayatımızın bir parçası olmuştur. Elbette ki bu alan içerisinde bunu kendi menfaatleri için kullanan insanlar olacaktır. Ancak bu hızlı teknolojik gelişime paralel olarak hukuki düzenlemeler yetersiz, eksik ve yavaş kalmaktadır. Tabi ki nerdeyse her gün gelişen ve değişen teknolojiye ayak uydurmak hukuki manada imkânsızdır. Ancak bunun içinde geç kalmamak gerekir. Çünkü bu süre içerisinde birçok insan mağdur olmakta, suçlular cezalarını çekmemektedir. Buda yeni suç ve suçluları meydana getirmektedir.

Ülkemiz teknolojik ve bilişim alanındaki gelişmeleri takip etmekte, buna da toplumumuz özellikle gençlerimiz çabucak uyum sağlamaktadır. Ancak bilişim suçları ile ilgili hukuki düzenlemelerimiz maalesef istenilen düzeye gelememiştir. Amerika Birleşik Devletleri'nde bilişim suçlarıyla ilgili düzenlemeler yaklaşık 25–30 yıl öncesine dayanmakla birlikte hala yeni düzenlemelere ihtiyaç olduğu belirtilmektedir. Ayrıca üye olmak için çabaladığımız Avrupa Birliği de kurduğu komisyonlar ve üye ülkelerin iç hukuk düzenlemeleriyle birlikte bilişim suçlarıyla ilgili hukuki düzenlemelere gitmiştir.

Bu tez çalışmamda görüleceği gibi ülkemizde bilişim suçlarıyla ilgili kanun ve mevzuatların yeterli olmadığı, gelişen teknolojiyle birlikte yeni düzenlemelere ihtiyaç duyulduğu meydana çıkmaktadır. Ayrıca toplumumuzun bu suçlarla ilgili bilgisinin de yetersizliği bilişim suçlarının ülkemizde günden güne çoğaldığını gözlemliye bilmekteyiz. Bu çalışmam da bilişim suçlarıyla mücadelenin ilk önce bu suçun teknik

yöntemlerini bilmek olduğunu, suçun kavramsal olarak bilinmesi gerektiğini vurgulamak için; suç teknikleri ve bilişimle ilgili kavramları açıkladım. Daha sonra hukuki olarak konuyu ele aldım. Çünkü virüs, Truva Atı, Hacker gibi kavramları anlamadan bunlarla ilgili kanuni metinleri anlamak oldukça zor olmaktadır. Ayrıca bilişim suçlarının kapsamının sadece bilgisayar değil; kredi kartı, ATM para çekme makineleri gibi konuları içerdiğini de bilmekte fayda olacağını düşünerek bu konularla ilgili gerekli bilgileri de işledim. Burada bilişim suçlarının sadece ceza hukuku yönünü ele aldım, özel hukukla ilgili ayrıca bir çalışmanın yapılması gerekmektedir. Çünkü bu konu oldukça geniş bir alanı kapsamaktadır.

Bu çalışmayı bitirdiğim dönem içerisinde "Bilişim Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun" tasarısı Türkiye Büyük Millet Meclisi alt komisyonunda görüşülmeye başlanmıştı. Bu da tezimizde belirttiğimiz gibi mevcut yasaların yetersiz olduğunu, gerekli hukuki düzenlemelerin teknolojik gelişimler karşısında zorlandığını göstermektedir. Yeni tasarıda mevcut Türk Ceza Kanunu'nda ki maddeleri geçersiz kılmakla birlikte ceza limitlerinin arttırıldığı görülmektedir. Tabi ki yeni düzenlemeler ileriki dönemlerde de devam edecektir. Şimdiden gerekli tedbirlerin alınması olumlu gelişme olarak değerlendirilmekle birlikte geç kaldığı konusunda da sanırsam hem fikiriz. Internet ve bilgisayarın kullanımı henüz ülkemizde gelişim sürecinde olmasına rağmen bu alandaki suç oranının kamuoyunda çokça gündeme getirilmesi belkide yeni hukuki düzenlemelerin artmasına neden olacaktır. Ancak kanunlarla birlikte toplumunda bilişim konusunda bilinçlenmesi, eğitilmesi gerekmektedir. Şuan ülkemizde Internet veyahut Internet Café denildiği zaman gayri ahlaki işlerin ön planda olduğu ancak bilişim alanında işlenen suçların çoğunu toplumun henüz tanımadığı anlaşılmaktadır.

Bilişim suçlarıyla mücadele sadece bir ülkenin iç hukuki düzenlemesiyle yeterli olmamaktadır. Global dünyada daha doğrusu küçülen dünyada bu suçlarla başa çıkmanın yolu işbirliği ile mümkün olacaktır kanaatindeyim. Çok geniş bir alanı kapsayan bu konuyla ilgili yapmış olduğum çalışmanın bu alanda katkı sağlayacağını umut ederim.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

SEMBOLLER / KISALTMALAR LİSTESİ

a.g.e: Adı geçen eser

a.g.w.s: Adı geçen web sitesi

AET: Avrupa Ekonomik Topluluğu

ATM: Automated Teller Machine-Otomatik Para Çekme Makinesi

BSA: Business Software Alliance-Ticari Yazılımlar Anlaşması

BBS: Bulletin Board Services-Duyuru Tahtası Hizmetleri

CVV2: Card Verification Value-Kart Doğrulama Değeri

EGM: Emniyet Genel Müdürlüğü

FTP: File Transfer Protocol-Dosya Aktarma İletişim Kuralları

FBI: Federal Bureau of Investigation-Federal Araştırma Bürosu

FSEK: Fikir ve Sanat Eserleri Kanunu

HTTP: Hypertext Transfer Protocol-Yardımlı Metin Aktarma İletişim Kuralları

PIN: Personal Identification Number-Kişisel Kimlik Numarası

SSL: Secure Sockets Layer-Güvenlik Protokolü

vb: ve benzeri

www: world wide web-Dünya Çapında Ağ

GİRİŞ

Bilişim suçları özellikle bilgisayar ve Internet kullanımının yaygınlaşmaya başlamasına paralel olarak ortaya çıkmış; tanımı ve yapısı üzerinde henüz tam olarak bir konsensüs sağlanamamıştır. Özellikle elektronik ortam içerisinde işlenmesi ve bu ortam içerisinde genel olarak hukuka aykırılık unsurunu içerisinde barındırması bu suçların en kabul gören unsurları olmuştur. Bilişim doğası sağladığı özgür iletişim platformunun yanında , bireylerin şeref ve haysiyetine yönelecek ihlaller açısından gerçekleştirilmesi çok kolay, kontrol edilmesi çok güç olan bir ortamın ortaya çıkmasını da sağlamıştır. Özellikle Internet üzerinden yapılan yayınlarla ve hukuk dışı girişimlerle bireylerin gerek malvarlıklarını hedef alan, gerekse şahsiyet haklarını ihlal eden bir boyuta ulaşması güncel bir sorun olarak karşımıza çıkmaktadır. Internet'in özgür bir iletişim platformu olması ve teknik imkansızlıklar bu suçlarla mücadelede karşılaşılan en büyük güçlükler olarak göze çarpmaktadır.

Ülkemizde yeni düzenlenen Türk Ceza Kanunu'nda bilişim suçu; bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle işlenen suçlar olarak 158. maddenin "f" fıkrasında yer almıştır. Tabi ki bu da Nitelikli Dolandırıcılık başlığı altındadır. Ancak bilindiği gibi bu tanımlama bilişim suçları açısından yetersiz kalmaktadır. Çünkü bu suçların içeriğine ve sınıflandırılmasına baktığımız zaman farklılıkları ve en azından genişliğini görebiliriz.

Bilişim suçları tabi ki sadece bilgisayar ve Internet üzerinden işlenen suçlar olarak tanımlanamaz. Örneğin ATM (Automated Teller Machine)'lerde işlenen suçlar, kredi kartların ENCODER (Kodlayıcı) denilen aletlerle kopyalanması gibi suçlarda bilişim suçları olarak değerlendirilmektedir. Bu suçlar bir bilgisayar, Internet, bir ENCODER cihazı, kısaca elektronik cihazlarda diye biliriz ve hatta cep telefonlarıyla da işlenebilmektedir.

Bu suçlara dünya genelinde verilen isimlendirmelere bakacak olursak; Computer Crimes (Bilgisayar Suçları), Cyber Crimes (Siber Suçlar), IT Crimes (Information Technologies-Bilgi Teknolojileri Suçları), Crime of Networks (Ağ Suçları) vb. olarak adlandırılmaktadır. Ancak ülkemizde biz buna kısaca **"Bilişim Suçları"** demekteyiz.

Bilişim suçlarının daha iyi anlaşılabilmesi için sınıflandırılmalar yapılmıştır. Bu şekilde suçun kapsam alanları daha iyi incelenebilmektedir. Bu sınıflandırma beş ana başlık altında toplanmıştır;

1.Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme,

2.Bilgisayar Sabotajı,

3.Bilgisayar Yoluyla Dolandırıcılık,

4. Bilgisayar Yoluyla Sahtecilik,

5.Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı.

Yukarıda beliritilen sınıflandırmalar bu çalışma içerisinde açılımları yapılarak açıklanmıştır.

Bilişim suçlarının nasıl işlendiğini anlamadan bu suçlarla mücadele etmek çok zordur. Bundan dolayı bu suçların nasıl işlendiğ, teknik olarak nasıl yapıldığı, hangi yöntemlerin kullanıldığı bilinmesi gereken konulardır. Bu konular da başlıkları altında incelenmiştir. Bu konular özellikle bu suçlarla mücadele eden güvenlik görevlileri tarafından bilinmesi gerekir. Suçun delillerini ortaya koymak adli soruşturmaya esas teşkil etmesi açısından çok büyük önem arzetmektedir.

Bilişim suçları, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Kanunu'nda; Onuncu Bölüm'de, Bilişim Alanında Suçlar başlığı adı altında **243, 244, 245** ve **246**. maddeleri arasında yeniden düzenlenmiştir.

Ayrıca, **"**Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılmasını ve kullanılmasını düzenleyen 5846 sayılı Fikir ve Sanat Eseleri Kanunu'nda (FSEK) bilişim suçları ile ilişkilidir. Çünkü bu kanunda belirtilen konuların işlenmesi bilgisayar, Internet gibi teknolojik cihazlarla gerçekleştirilmektedir.

Bilişim suçlarıyla ilgili kanuni olarak yapılan düzenlemelerle birlikte bu suçların yer yönünden yetkili mahkemeler ve alınan yargıtay kararları da bu çalışma içerisinde yer almıştır. Ancak bu konu incelenirken görülecektir ki bilişim suçlarının sıkı bir uluslararası ilişkiye ve yardımlaşmaya muhtaç olduğudur. Özellikle Internet yoluyla işlenen suçlarda uluslararası yardımlaşma ve dayanışma ön plana çıkmaktadır.

Günümüzde medyadan da takip edildiği üzere özellikle yabancı ülkelerin çocuk pornografisi konusunda ülkemizde tespit edilen kullanıcılar belirlenmekte ve haklarında gerekli yasal işlemin yapılması için isim ve adresleri tespit edilerek yakalanmaktadırlar.

Bu çalışmanın son kısmında bilişim suçlarının diğer ülkelerdeki yasal konumları ve alınan tedbirler de ortaya konmuştur.

Bilişim suçlarını incelerken tabi ki en büyük kaynağım Internet olmuştur. Bunun yanında Emniyet Genel Müdürlüğü'nün bu konuyla ilgili yapmış olduğu çalışmalar da kaynak olarak değerlendirilmiştir. Ancak kaynağımın Internet olmasının bir sebebi de bu konuyla ilgili geniş bir çalışmanın bütünsel olarak kitaplaştırılmamış olmasıdır. Umarım ki ileri ki dönemlerde bu konuyla ilgili kapsamlı çalışmalar yaygınlaşır. Çünkü teknoloji her gün ve hatta her saat gelişmekte buna paralel olarak da suç ve çeşitleriyle birlikte suçlu profilleride değişmektedir. Ülkemizde bu suçlarla ilgili 5237 sayılı Türk Ceza Kanunu'nda gerekli düzenlemeler yapılmıştır. Ancak teknoloji o kadar hızlı gelişmektedir ki karşımıza yeni suç tipleride çıkabilmekte bunları anlayana kadar da belirli bir süre geçmektedir. Bu arada da insanlar mağdur olmaktadırlar.

Bilişim suçlarını iyi anlamak ve tahlil etmek için ilk önce tanımını bilmekte fayda olduğunu düşünerek ilk bölümde tanımını daha sonra da bu suçların sınıflandırılmasını ve suçların işlenme teknik ve yöntemlerinin incelenmesini ele aldım. Daha sonra bu suçların hukuk sistemimizin içerisindeki yerini gösterdim. En son olarak da bilişim suçlarının yabancı ülkelerdeki yasal ve idari yapılanmasını belirttim. Çünkü bu suçlarla mücadele de uluslar arası yardımlaşmanın, desteğin ve etkinliğin çok önemli olduğu bilinmekte, hatta zorunlu hale geldiği görülmektedir.

BİRİNCİ BÖLÜM

Bir suçu tanımadan onunla mücadele edilemez. Bunun için bilişim suçlarının tanımını açıklamak, kavram olarak neleri ifade ettiğini görmek için ilk bölümde tanımlara yer verilmiştir. Burada görüleceği üzere tanım konusunda ne ülkemizde ne de diğer ülkelerin üzerinde uzlaşıya vardığı bir tanım bulunmamaktadır. Her ülke kendi sosyal şartlarına, hukuki anlayışlarına göre tanımlarda bulunmuştur. Bu bölümde yapılan tanımların hepsine yer verilmeye çalışılmıştır.

Ayrıca bu bölümün içerisinde bilişim suçlarının sınıflandırılmasına, işlenme yöntemlerine, virüsler gibi kötü yazılımların neler olduğuna, nasıl çalıştığına ve ATM para çekme makineleri ile kredi kartlarına yönelik işlenen bilişim suçlarının yöntemlerine de yer verilmiştir.

BİLİŞİM VE BİLİŞİM SUÇUNUN TANIMI

Bilişim; insanların teknik, ekonomik ve toplumsal alanlarda ki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi, informatik demektir.[1]

Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenilen suçlardır.[2] Bu suçun tanımı hem eski hem de yeni Türk Ceza Kanunu'nda yer almamıştır. Ancak yeni Türk Ceza Kanunu'nun Nitelikli Dolandırıcılık başlıklı 158. maddesinin "f" fıkrasında ki tanım şu şekildedir; Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle, işlenen suçlar olarak yer almaktadır.

1-Türk Dil Kurumu, **Türkçe Sözlük**, Ankara 1983, Cilt 1,s.156

2- http://www.iem.gov.tr/iem/?m=3&s=51#1, 10.08.2006

Günümüzde bilişim suçlarına halk arasında genellikle "bilgisayar suçları" da denilmektedir. Bilişim kelimesi, bilgisayardan faydalanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini, bilgisayar ise bu faaliyetin gerçekleştirilmesinde en önemli etken olan cihazı ifade etmektedir.

Bilgisayar suçları yada bilişim suçları konusunda herkesin ittifak ettiği bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır."

Avrupa Ekonomik Topluluğu bir tavsiye kararında bu suçları beşe ayırmıştır. Bunlar sırası ile;

1-Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,

2-Bir sahtekarlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

3-Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,

4-Ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,

5-Bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme kasten girerek müdahalede bulunmaktır.[3]

Bilişim suçlarıyla ilgili olarak karşımıza bir çok tanım çıkmaktadır; Bilgisayar suçları, dijital suçlar, Internet suçları, siber suçlar, ileri teknoloji suçları v.b. Diğer

---

3- ÖZEL, Cevat, http://www.hukukcu.com/bilimsel/kitaplar/**bilisimsuclari_TCKtasarisi**.htm, 03.05.2006

ülkelerde ise; Computer Crimes (Bilgisayar Suçları), IT Crimes (Bilgi Teknolojileri Suçları), Cyber Crimes (Siber Suçlar), Crimes of Network (Ağ Suçları) v.b. Aslında her bir tanım bize bir açıklık getirmektedir. Çünkü bu suç türleri bir bilgisayar vasıtasıyla yapılabileceği gibi bir Network veya Internet üzerinde de olabilmekte yada bir ufak elektrik devresi veya kredi kartı da kullanılabilinmektedir. Bilişim kelimesi ise; Bilgisayar ve bilgisayar teknolojileri ile iletişim teknolojilerini kapsadığından "bilişim suçları" adı altında toplanmıştır. Dolayısıyla bilişim suçları terimi kullanıldığında bahsedilen bu teknolojileri kullanarak işlenen bir suç unsuru olduğu unutulmamalıdır.[4]

Tanımlamalar da bu yüzden hep değişik olmuştur. En basit tabiriyle bilgisayar suçları olarak tanımlayabildiğimiz gibi; Siber Suçlar, Dijital Suçlar, Bilişim Suçları, İleri Teknoloji Suçları vs. tanımlamaları ile de karşılaşmaktayız. Diğer ülkelerde yapılan tanımlamalarda ise; Computer Crimes, Cyber Crimes, IT Crimes (Information Technologies-Bilgi Teknolojileri), Crime of Networks vb. Aslında tüm bunlar ile bu suçların bir kısmı tanımlanmış olmaktadır. Ancak Türkçe'ye "bilişim teknolojileri suçları" olarak geçen IT Crimes (Information Technologies) bu suçların alanı açısından tanım olarak daha iyi uymaktadır. Bu yüzden daha kısa ve yalın bir ifade ile "bilişim suçları" olarak kullanılması daha uygun olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken suçun işlenmesindeki amaç olmalıdır.[5]

21. yüzyılın en önemli güç kaynağı hiç şüphesiz bilgidir. Bilgiyi elinde tutan gücü de elinde tutmuş olmaktadır. Bilginin gücüyle teknolojik alandaki gelişmeler tüm yaşamımızı olumlu yönde etkiliyor. Internet, bilgisayar, uydular, cep telefonları gibi. Bunlar sadece günlük yaşamımıza giren teknolojinin ürünlerinden bazıları. Yine bilginin gücünü kullanarak aynı araçlar birer silaha dönüşebilmekte ve karşımıza siber savaş ve siber terör kavramları çıkmaktadır. Siber terör, yeni yüzyılda terörizmin yeni yüzü olarak yansıyacaktır ki teröristlerin elektronik bir saldırı yaparak bir barajın kapaklarını açabilecekleri, ordunun haberleşmesine girip yanıltıcı bilgiler bırakabilecekleri, kentin bütün trafik ışıklarını durdurabilecekleri, telefonları felç edebilecekleri, elektrik ve doğalgazı kapatabilecekleri, bilgisayar sistemlerini karmakarışık hale getirebilecekleri, ulaşım ve su sistemlerini allak bullak edebilecekleri,

---

4-http://www.iad.org.tr/ayinkonusu04.html, 18.09.2006

5- DOKURER, Semih, EGM Bilgi İşlem Daire Başkanlığı, Yayınlanmamış Eser

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.[6]

Terörizmin tanımı; belirli bir siyasal hedefe ulaşmak veya siyasal bir davayı yüceltmek amacıyla ve genelde kurulu düzeni değiştirmeye veya söz konusu siyasal davaya boyun eğmeye mecbur etmek için başvurulan zorlayıcı ve şiddet içeren davranışlardır.

Siber terörizm ise; belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır.

Siber terörizmi klasik anlamda terör eylemlerinin bilgisayar ve bilgisayar sistemleri kullanılarak icra edilmesi olarak tanımlamak da mümkündür.

Siber terörizmi tanımlarken temelde terörizm olgusunun nitelikleri değil ancak terör olgusunun nasıl yaşama geçirildiği önem arz etmektedir. Temel amacı bir kısım siyasal sonuçlara ulaşmak olan insanların, ellerine geçirdikleri yeni teknolojik donanımlar ile terör eylemini gerçekleştirmek için yola koyulmuş olmalarıdır. Dolayısıyla terörizmde felsefi olarak köklü bir değişimden bahsetmek güçtür ancak yöntemler ve araçlarda önemli değişimler olmuştur denebilir. Bu bağlamda Siber terörizm araçları bakımından ileri teknoloji ve bilgiyi kullanarak klasik terörizm tanımlamasının yeni şekliyle devamıdır denebilir.[7]

Siber terörizmin halihazırda resmi bir tanımı yok ve kavram, sıklıkla "Hacker'lıkla" karıştırılıyor. Genellikle kişisel tatminler yada çıkarlar doğrultusunda kişilerin ve kurumların bilgisayar sistemlerine zarar veren, kayıtlı bilgileri yok etmek yada çalmak üzere düzenlenen saldırılar " hacker saldırıları " olarak ele alınıyor ve siber terörizm kapsamının dışında kalıyor.

Türkasya Stratejik Araştırmalar Merkezi'nin (TASAM) hazırladığı "Siber

---

6- ÖZCAN, Mehmet, **Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu**, http://www.usakgundem.com/makale.php?id=114, 17.02.2006

7- ÖZCAN, a.g.w.s, 17.02.2006

Terörizm Raporu'nda" Amerikalı bilgisayar bilimi profesörü Dorothy Denning'in tanımına yer veriliyor. Denning'in bilgisayarla yapılan her türlü suçu siber terörizmin kapsamına sokmayan soğukkanlı tanımı bir yandan da potansiyel tehditlere ilişkin ipuçları veriyor.

Siber boşluk ile terörizmin bir bileşimi olarak siber terörizm, siyasi ve sosyal mercilere ve kişilere gözdağı vermek, baskı oluşturmak maksadıyla resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Ancak bir saldırının siber terörizm olarak tanımlanabilmesi için bir bireye ve mala karşı şiddet içermesi gerekmektedir.[8]

Bu tanımın problemli yönü, "Hacker'ların" ataklarının şiddet içermediği savı üzerine kurulmuş olmasından kaynaklanıyor. Çünkü, sıradan bir bireyin malına yada kişisel bilgilerine zarar verme veya erişme eyleminin de şiddet kapsamında ele alınması gerektiğini ifade eden uzmanların sayısı hayli fazla. Dolayısıyla, hem "Hacker'lığın" hem de siber terörizmin şiddet içerdiği konusunda uzlaşılması durumunda geriye, siber terörizmi tanımlayan tek bir ayırt edici özellik kalıyor o da Politik Motiv. Herhangi bir politik motiveden hareketle planlanmış olan ve dijital ortamda gerekleştirilen bilgi toplama ya da zarar verme amaçlı saldırı eylemini siber terörizm olarak tanımlamak şu an için doğru gibi görünüyor.

Mobil ve uydu telefonlarından Internet'e uzanan yeni iletişim teknolojileri kötü niyetliler için gerekli kaynakların bir araya getirilmesine ve yeryüzünün herhangi bir noktasındaki eylemlerine organize etmelerine olanak tanıyor.

Terörist örgütler, silah bilgilerini paylaşma ve geliştirme, taktik kabiliyet, finansmanın güvenli transferleri, güvenli haberleşme vb. konularda Internet'i kullanıyorlar. Mesajları gizleme ve şifreleme sağlayan bilgi işlem teknolojileri de teröristler için biçilmiş kaftan. Modern bir diz üstü bilgisayarın gücü, ABD Savunma Bakanlığı'nın 1960'lardaki toplam bilgisayar gücünden fazla. Mesajları dijital fotoğraflların ya da müzik kliplerinin içine saklayan "steganografi-gizli yazışma" tekniklerini isteyen herkes kullanabiliyor. (Bu tekniğin 2001 yılında ABD Paris

---

8- ÖZCAN, Mehmet, **Siber Terör Küresel Tehlike**, http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=36&Itemid=29, aksam.com.tr, Pazar, 29.01.2006

Büyükelçiliği'ni havaya uçurmayı planlayan teröristler tarafından kullanıldığı biliniyor.) Internet'te kolay kullanılabilir yaklaşık 160 steganografi tekniği mevcuttur.[9]

Bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve rasyonel biçimde işlenmesi bilimidir. Bilgi olgusunu, bilgi saklama, erişim dizgileri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalıdır. Disiplinler arası özellikler taşıyan bir öğretim ve hizmet kesimi olan bilişim, bilgisayarı da kapsayarak bilişim ve bilgi erişim dizgelerinde kullanılan her türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar.[10]

Bilişim suçu kavramı farklı kaynaklarda farklı şekillerde tanımlanmış ve "Bilişim Suçları", "Bilgisayar Suçları", "Internet Suçları", "Siber Suç", "İleri Teknoloji Suçu", "Dijital Suçlar", "Sanal Suç", "Siber Terörizm" gibi kavramlar iç içe girmiş durumdadır. Bilişim suçları ile ilgili yapılmış tanımlara bakacak olursak; "Bilişim alanındaki gelişmelere paralel artış gösteren ve teknolojin yardımı ile genellikle sanal bir ortamda kişi veya kurumlara maddi veya manevi zarar verecek davranışlarda bulunmaktır."

"Verilerin bilişim temelli olarak ve otomatik şekilde işlenmesi, saklanması, tasnif edilmesi, terkibi ve iletilmesi ile ilgili ve bilişim alnında işlenen, bir bilgisayar yada ağına yönelik olarak yada onları kullanarak icra edilen her türlü yasadışı haksız eylem olarak tarif etmek mümkündür." Bilgisayar, çevre birimleri, pos makinesi, cep telefonu gibi her türlü teknolojinin kullanılması ile işlenilen suçlardır. Bilişim teknolojileri kullanılarak işlenen tüm suçlar bilişim suçlarını oluşturur. "Bilgisayar Suçu (Computer Crime): Bir bilgisayar yada bilgisayar ağına yönelik yada onları kullanarak (bilgisayar teknolojisi bilgilerinden yararlanılarak) gerçekleştirilen yasa dışı eylem."

Siber Suçlar (Cyber Crimes): Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkanı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak

---

9- ERSANEL, Nedret, **Siber İstihbarat**, Hayykitap, İstanbul, Ekim 2005, s.203

10- AKARSLAN, Hüseyin, **Bilişim Suçu Kavramı**, http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=142&Itemid=28, 05.08.2006

hukuka aykırı veya suç olarak tanımlanabiliyorsa bu suçları siber suçlar olarak tanımlayabiliriz. Siber suç, bilgisayar ve ağ sistemleri yoluyla bilgisayar veya ağ sistemleri içerisinde yada bilgisayar tarafından suç olarak yaratılmış fiillerin siber ortamda işlenmesi ve daha önce suç olarak yaratılmamış bu ortamın karakteristiğe has bir takım ihmallerin bir bütünüdür. [11]

Bilişim; (Informatics, Information System) kelime anlamıyla; insanların teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı bir şekilde işlenmesine denir. Halk arasında bilişim kavramı ile bilgisayar birlikte anılmaktadır. Buna rağmen bilişim bir bilim olmasına rağmen, bilgisayar ise bilişimin bir ürünüdür. Bununla birlikte bilgisayarın sözlükteki manasını dikkate aldığımızda da bu ayrımı görebiliriz. Tanıma göre bilgisayar; çok sayıda aritmetiksel veya mantıksal işlemlerden oluşan bir işi, önceden verilmiş bir programa göre yapıp sonuçlandıran elektronik araç veya elektronik beyin olarak ifade edilir. Bilişim ve bilgisayar terimleri arasındaki bariz fark; bilişim bilginin kendisi olarak tabir edilirken, bilgisayar ise bu bilgiyi işleyen araçtır. "Bilişim Suçları" halk deyimiyle "Bilgisayar Suçları" olarak da tanımlayabildiğimiz gibi "İletişim Suçları" , "Internet Suçları" , "Dijital Suçlar" , "Teknolojik Suçlar" gibi tanımlamalar da yapabiliriz. (Computer Crimes, Cyber Crimes, Internet Technology Crimes, Digital Crimes). [12]

Genel manada bilişim suçları, her türlü teknoloji kullanılarak, kanuni olmayan yollarla kişisel yada kurumsal bilgisayarlarda, sistemler üzerinde zarar verici etki bırakmaktır. Bilişim teknolojilerinde suç meydana gelebilmesi için mutlaka teknoloji kullanılmalıdır. Bu teknoloji bilgisayar, kredi kartı, telefon, pos makinesi, elektronik bir cihaz olarak düşünülebilir. Bilişim suçları hakkında AET Uzmanlar Komisyonu'nun Mayıs 1983 yılında Paris Toplantısı'nda yaptığı tanımlamaya göre; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlakî ve yetki dışı gerçekleştirilen her türlü davranıştır." denmektedir.

11- AKARSLAN, a.g.w.s, 05.08.2006

12- EKER, Mehmet Akif, **Bilişim Suçları, Bilişim Suçlarıyla Mücadele,Türkiye'de Bilişim Suçları**, http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=123&Itemid=28, 13.06.2006

Tanımlarda da görüldüğü gibi bilişim suçlarının net olarak çizgileri çizilmemiştir. Çünkü gelişen teknolojiyle birlikte bilişim suçları da değişmektedir. Bu nedenle **bilişim suçları, bilgisayar suçları, Internet suçları, siber suç, ileri teknoloji suçu, dijital suçlar, sanal suç** gibi kavramların tek bir tanımının yapılmaması bir eksiklik olarak değerlendirilmemelidir. Ancak biz bu kavramların hepsini genel olarak **"Bilişim Suçu"** olarak adlandırabiliriz.[13]

Bilişim suçları özellikle bilgisayar ve Internet kullanımının yaygınlaşmaya başlamasına paralel olarak ortaya çıkmış; tanımı ve yapısı üzerinde henüz tam olarak bir konsensüs sağlanamamıştır. Özellikle elektronik ortam içerisinde işlenmesi ve bu ortam içerisinde genel olarak hukuka aykırılık unsurunu içerisinde barındırması bu suçların en kabul gören unsurları olmuştur. Bilişim doğası sağladığı özgür iletişim platformunun yanında , bireylerin şeref ve haysiyetine yönelecek ihlaller açısından gerçekleştirilmesi çok kolay, kontrol edilmesi çok güç olan bir ortamın ortaya çıkmasını da sağlamıştır.

Özellikle Internet üzerinden yapılan yayınlarla ve hukuk dışı girişimlerle bireylerin gerek malvarlıklarını hedef alan, gerekse şahsiyet haklarını ihlal eden bir boyuta ulaşması güncel bir sorun olarak karşımıza çıkmaktadır. Internet'in özgür bir iletişim platformu olması ve teknik imkansızlıklar bu suçlarla mücadelede karşılaşılan en büyük güçlükler olarak göze çarpmaktadır.

Avrupa Ekonomik Topluluğu'nun bir tavsiye kararında belirtildiği gibi bilişim suçlarının farklı şekillerde işlenebildiği görülmüş, suçun farklı görünüş biçimlerinin değişik özellikler arz ettiği ortaya konulmuştur. Şöyle ki; Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek bilişim suçu olarak değerlendirilirken burada suçun sujesi olarak bir bilgisayar kaynağına gayrı meşru şekilde ulaşılması hususu vurgulanmıştır. Bir diğer şekliyle bilişim suçları, sahtekarlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek, olarak tanımlanmış ve suçun unsurlarında sahtekarlık yapma amacını veya sanığın bir menfaat temin etmesini aramıştır. Yine diğer bir

---

13- AKARSLAN, a.g.w.s, 05.08.2006

şeklinde suçun manevi unsurunda taksire yer vermeyerek bu suçların bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek, olduğunu tanım olarak getirmiştir. Ayrıca ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmayı ve bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme kasten girerek müdahalede bulunma yada bilişim suçlarının yapısı içerisinde yer vermiştir. Bu bağlamda bilişim suçlarının yapısını ortaya koymak için yukarıda değindiğimiz bilişim suçlarını hazırlayanlar ve işleyenler ile ilgili makaleler yazılmakta, bu makalelerin bir çoğunda bazı sosyal varsayımlara dayanarak her şey bilişim suçu olarak adlandırılamaktadır.

Bilişim suçlarının alanına hangi faaliyetlerin girdiği yargılamanın başlıca sorunudur. Bu sorunun çözümünde bilişim suçlarının yapısının tam olarak ortaya konulamaması en temel sorun olarak önümüze çıkmaktadır. Bu sorun genel hatları ile değerlendirildiğinde şöyle bir sonuç çıkmaktadır. Faaliyet bilgisayar sistemi ile mi temellen dirilmektedir, yoksa bilgisayar o faaliyetin gerçekleşmesinde yardımcı bir unsur olarak mı kullanılmaktadır? Örneğin bankaların ATM uygulaması bilgisayar temelli olduğu için bilişim faaliyetidir. Çünkü bu sistem çöktüğünde bu faaliyet asla icra edilemez. Ancak radyo ve televizyon yayıncılığı bilgisayar sistemlerini faaliyetlerinin çeşitli aşamalarında kullanılmakta ise de bunların faaliyeti bilişim temelli değil iletişim temellidir. Yararlanma, bu suçları bilgisayar temelli haline getirmez. Bilişim suçları geleneksel anlamı ile gerçek yaşam alanı olarak adlandırılan ve fiziksel gerçeklerin paylaşıldığı alan içinde kalmaktadır. Bu nedenle bilişim suçları özel hayata müdahale, kamu haklarını ihlal gibi alanlarda değerlendirilmektedir. Yine bilişim suçlarında, suçun bilgisayar yardımı ile mi işlendiği yoksa suçun amacı mı olduğu konusu tartışılmaktadır. Bilgisayar ile işlenen bilişim suçlarının en temel özelliği, bir suç işlenirken kullanılan bir alet edevat gibi bilgisayarın bir araç olarak kullanıldığı suçlardır. Bu dolandırıcılık ile bilgileri kayıt etme, hatalı kimlik tanımlama, telif haklarını ihlal ederek kopya yapmak, dağıtmak ve diğer suçları işlemeyi ifade eder.

Bilişim suçlarına ilişkin bir diğer durumda kişisel verilerin korunması ve bunlara yönelik gerçekleşen ihlallerdir. Gerçekten günümüzde kişilerin hususiyetlerini belirten bir takım bilgiler bilgisayar ortamında saklanmaktadır. Bu bilgilerin sahiplerinin rızası hilafına hukuka aykırı olarak el değiştirmesi, yok edilmesi, ifşa edilmesi, değişikliğe

uğratılması bir çok Avrupa ülkesinde ve Amerika'da yaptırım altına alınmıştır. Aynı zamanda bu bilgileri muhafaza eden, koruyan, işleyen kurum veya kişilerin koruma, muhafaza ve işleme görevlerinde ihmal göstermeleri ve bu durum sonucu kişilerin zarar görmeleri ek ceza sorumluluklarının kabul edilmesini gündeme getirmiştir. Bu şekilde kişilerin hususiyetlerini yansıtan bilgilerin gizlilik , bireysel hakların korunması ve özel hayata saygı ilkeleri çerçevesinde hukuki himaye altına alınması sağlanmıştır. Yine bilişim suçlarının temel özelliği suçların işlenmesinin oldukça kolay, buna mukabil belirlenmesinin oldukça güç olduğu gerçeğidir. Çoğu bilgisayar suçunun "köstebek" diye bilinen kurum içi çalışanlar vasıtasıyla ve "insider information (içeriden bilgi)" şeklindeki yöntemlerle işlenmesi sebebiyle belirlenmesi zor ve takibi oldukça güçtür. Buna mukabil suçun kolay işlenebildiği ancak, faillerinin tespit edilememesi ile ilgili pek çok örnek de verilmektedir.

Örneğin ABD'nin Seattle kentinde gelişmiş ülkelerin liderlerinin katıldığı küreselleşme toplantıları sırasında küreselleşme karşıtlarının Internet üzerinde çok iyi organize olarak eş zamanlı olarak yoğun protesto gösterileri düzenlenmiş, yani ortalığı cehenneme çevirmiş oldukları bilinmektedir. Bilişim suçlarının bir diğer özelliği de beyaz yakalı yani sanığın mesleği veya iş dünyası ile ilgili olmalıdır. Beyaz yakalı suçlar sokak suçlarından daha az göze gözükmesine rağmen sokak suçlarından daha fazla bir zarara sahiptir. Bilişim suçları kriminal eylemler ile ilgili geleneksel anlayıştan farklı olarak zamana, mekana bağlı olmaksızın gerçekleşir ve anlıktır.

Bilişim suçlarında suç failinin amacıda klasik suçlu amacından farklıdır. Mesela "Computer Hacking (Bilgisayarda Yetkisiz Erişim)" fiillerinde fail bir yarar sağlamak veya zarar vermek için değil, marifet göstermek amacındadır. Hatta fail fiillerinin işlendiğinin anlaşıldığını belli edecek bir iz veya bir mesaj bırakmaktadır. Yardım amacıyla suçu işleyenler bulunmaktadır. Bu durumdaki suçlu eylemi meşru kabul etmektedir. Bilişim suçlarını klasik suçlardan ayırt eden özelliklerden belki de en önemlisi bu suçların, suçun işlenmesinden sonra arkada herhangi bir iz bırakılmaması sebebiyle maddi hareketin tespitinin zorluğudur. Ayrıca bilişim suçlarının meydana getirdiği sonuçlar diğer suçlara oranla çok büyük ve tahrip edicidir.[14]

14- YÜZER, Muharrem , **Bilişim Suçlarının Yapısı Ve Özelliklerine Bir Bakış**, http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=253, 22.03.2006

1.1 Bilişim Suçlarının Sınıflandırılması:

Suçun işlenmesindeki esas konuyu suçlar arasındaki farklar oluşturur. Bir hedefe ulaşabilmek için türlü yollar kullanılabilir, bunun ötesinde asıl amaç hedeftir. Suç çeşitleri ayrımında 11.06.1999 tarihinde Birleşmiş Milletler ve Avrupa Birliği tarafından hazırlanan "Bilişim Suçları" raporuna göre; suç çeşitleri altıya ayrılmaktadır. Bunlardan birincisi; "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme" olarak tanımlanır. İkinci olarak tanımlanan bilişim suçu; "Bilgisayar Sabotajı dır." Bir diğer suç kavramı; "Bilgisayar Yoluyla Dolandırıcılık" olarak kabul görür. Başka bir siber suç ise; "Bilgisayar Yoluyla Sahtecilik" kavramıdır. Beşinci suç türü ise; "Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" şeklindedir. Son olarak tanımlanan bilişim suçu ise; "Diğer Suçlar" başlığı altında Yasadışı Yayınlar, Pornografik Yayınlar (Büyük ve Çocuk Pornografisi), Hakaret ve Sövme olarak değerlendirilir. "Computer Sabotage", "Unauthorized Access", "Computer Fraud" , "Child-Adult Porn", buna benzer yine Internet ortamında işlenen suçlarla mücadele etmek maksadıyla, 23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan, Avrupa Ülkeleri ile Kanada, Japonya, Güney Afrika ve ABD dahil 33 devlet tarafından imzalandığı halde henüz Avrupa Birliği ile flört eden Türkiye'nin imzalamamış olduğu; Avrupa Konseyi Siber Suç Sözleşmesine göre; bilgisayar veri ve sistemlerinin gizliliğine, bütünlüğüne ve kullanımına açık bulunmasına yönelik suçlar kapsamında hukuka ayıkırı erişim, yasa dışı müdahale, verilere müdahale, sistemlere müdahale, cihazın kötüye kullanımı fiilleri; bilgisayarla ilişkili suçlar çerçevesinde ise sahtecilik, dolandırıcılık, telif haklarının ve benzeri hakların ihlaline ilişkin fiiller ve içerikle ilişkili olarak çocuk pornografisine yönelik fiiller, cezalandırma konuları arasında sayılmış; bu hususlarda ulusal ve uluslar arası alanda gerekli etkin yaptırım ve işbirliğine ilişkin düzenlemeler belirtilmiştir. Avrupa devletlerinin bir çoğu (Almanya, İtalya, Finlandiya, Avusturya, Yunanistan, İsveç, Danimarka, Norveç ve Hollanda gibi) mevcut yasal hükümlere eklemeler yapmış; ABD, İngiltere ve İrlanda gibi Anglosakson sistemine dahil bazı devletler ise bu konularda özel düzenlemelere gitmişlerdir. [15]

15-EKER, a.g.w.s, 13.06.2006

Bilişim suçları kapsamına giren suçların tanımlanması ve sınıflandırılmasının yapılması daha sonra yapılacak çalışmalara hazırlık teşkil edecek ve her bir suç tipi daha rahat anlaşılmış olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken suçun işlenmesindeki amaç olmalıdır. Bu tür suçlar hangi yöntemle işleniyor olsa da, hangi amaca hizmet ettiğine bakmak lazımdır. Örneğin; bir bilgisayar sistemine girmek için bir çok yöntem bulunabilir; bir virüs veya Trojan kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Ancak burada amacın sisteme girme eylemi olduğuna dikkat etmek lazımdır. Burada kullanılan yöntemler ancak suçun ağırlaştırıcı sebeplerini oluşturabilir. Mesela bir sisteme girerken başka sistemlere de sızmış olması gibi. Aşağıda tanımlaması yapılan suç tipleri gerek Avrupa Birliği, gerek Avrupa Konseyi ve gerekse diğer Avrupa ülkeleri tarafından yapılan tanımlamaların ülkemize uyarlanmış halidir. Benzer tanımlamalarda İngilizce tabirleri ile karşılaşmak mümkündür. "Unauthorized Access (Yetkisiz Giriş), Computer Sabotage (Bilgisayar Sabotajı), Computer Fraud (Bilgisayar Dolandırıcılığı)" gibi.

Bu suç tiplerine bakacak olursak;

1.Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme:

Anayasa'mızda belirtilen "Özel Hayatın Gizliliği" maddesine aykırı olarak teknolojik dinlemelerin yapıldığına güncel olarak karşılaşmaktayız. Günümüzde daha modern bir yapıya ulaşan iletişim kavramı artık bilgisayarlar üzerinden yapılmakta ve hatta kişilere ait önemli bilgiler bu ortamda iletilebilmektedir. Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerinin tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır. Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır. İşte bu noktada gizlilik gerektiren bilgilere yetkilisi haricinde yapılan erişimler bu suç tipine girmektedir. Erişim haricinde haberleşme amacıyla kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de aynı şekilde değerlendirilmektedir. İletişimin dinlenmesi; sadece bilgisayar başındaki iki kişinin birbiri ile görüşmesi olarak düşünülmemelidir. Birbirine bilgi gönderen ve uyum içinde çalışan bilgisayarların Network (Ağ) içinde göndermiş oldukları bilgilerin dinlenmesi de dinleme olarak değerlendirilmelidir.

Erişim sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere, programlara; yine programlar, casus yazılımlar, virüsler, Trojan horses (Truva atları),

worms (solucanlar) vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler, erişimler, izinsiz kişi yada kurum bilgisayarlarına, sistemlerine girmek suç olarak kabul edilmiştir.

Günlük yaşantımızda gelişen teknoloji ile birlikte daha rahat ve modern bir ortam sağlayan iletişim kavramı ile birlikte gelişen bilgisayar teknolojisi sayesinde işlemler kolaylaşmakta ve kişiler, bankalar, resmi kuruluşlar, ticari kuruluşlar, hastaneler, bilgi depolayan sistemler, istihbarat birimleri, hızlı iletişim gerektiren işlemler çoğu zaman bilgisayar teknolojileri kullanılarak yapılmaktadır. Türkiye'de işlemekte olan kamu kurumları, şirketler, özel ve tüzel eğitim kurumları, bankalar, ticari kurumlar ve birçok organizasyon; teknolojinin getirmiş olduğu gelişmelerden faydalanmakta ve bu sayede daha rahat ve kolay işlemlerini tamamlamakta, bir yandan kahvaltısını yaparken diğer yandan Internet üzerinden alışveriş yapabilmekte, büyük miktarda paraları rahatça bir yerden başka bir yere aktarabilmekte, kamu hizmeti olarak online pasaport, hastane muayene fişi, iş başvurusu gerçekleştirebilmekte, bir çok işlemi zahmetsiz bir şekilde yürütebilmektedir. Fakat bu işlemler sırasında belirli bir politikanın yapılmaması, gerekli düzenlemelerin uygulamaya konulamaması sonucunda kişi yada kurumlar küçümsenmeyecek şekilde tehlikelere maruz kalmakta ve sonuç olarak bilişim suçu ortaya çıkmaktadır.

Bilgilerin toplandığı bu tür sistemlere, bilgisayarlara girmek, bilgilere erişmek suç olarak kabul edilmektedir. Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz bilgilerin alınması da kişinin özel mülkü yada kişilerin şahsiyetlerine taciz olarak kabul edilmektedir ve suç oluşturmaktadır.[16]

2.Bilgisayar Sabotajı:

Bilgisayar sabotajı; yetkisiz erişimin ikinci safhası olarak değerlendirilebilir. Çünkü; Yetkisiz erişimde bulunan birisi sadece pasif bir davranışta bulunup özel hayatın gizliliğini bozmuş olur. Ancak bilgisayar sabotajı erişimden sonra elde ettiği

16- EKER, a.g.w.s, 13.06.2006

bilgilerin silinmesini ve değiştirilmesini içerir. Bu suç tipi iki şekilde karşımıza çıkmaktadır. Birincisi; yine bilgisayar teknolojileri kullanılarak erişilen bilgilerin silinmesi, yok edilmesi ve değiştirilmesidir. İkincisi ise bilgisayar teknolojileri kullanılmadan direkt olarak bilgilerin tutulduğu bilgisayarı ve/veya bilgisayarları fiziksel olarak zarara uğratmaktır. Burada önemli olan mala karşı değil de, bilgisayarın içindeki bilgilere karşı yapılmış bir hareket olarak algılamak lazımdır. Çünkü bu bilgiler bilgisayarın kendisinden daha değerli olabilir.

Yetkisiz erişimin aktif sahası olarak da nitelendirilen bilgisayar sabotajı, yalnız sisteme erişimle kalmamakla birlikte, eriştiği sistemin (bilgisayarın) içerdiği bilgileri silme veya değiştirme olarak ifade edilir. Fiziksel olarak bilgilerin yok edilmesi veya silinmesi yani bilgilere sanal ortam haricinde yapılan dış etkiler de bilgisayar sabotajına girmektedir.

Bir bilgisayara veyahut sisteme yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle, kopyalamakla kalmıyor, kendi menfaatleri doğrultusunda bu bilgileri değiştirebiliyor, silebiliyor yada bu bilgileri kanun dışı kullanmak isteyenlere satabiliyorlar.[17]

3.Bilgisayar Yoluyla Dolandırıcılık:

Klasik olarak bildiğimiz ve karşılaştığımız dolandırıcılık suçunun bilgisayar ve iletişim ortamları üzerinden yapılıyor olmasıdır. Bilgisayar yoluyla dolandırıcılık en çok kredi kartlarının kullanımıyla yapılmaktadır. Bunun için üretilmiş birçok "Card (Kart Üreteçi)" programı bulunmaktadır. Bunlar sayesinde Internet üzerinden alışveriş yapılırken, istenilen kredi kartı şirketi için mantıksal olarak olası kredi kartı bilgileri üretilmekte ve bu olaydan kredi kartı sahibinin haberi bile olmamaktadır. Bununla beraber yine finans bilgilerinin tutulduğu programlarda yapılan değişiklikler ile istenilen kişinin hesabına istenildiği kadar para aktarılması yapılabilmektedir.

Dolandırıcılık genel bağlamda "hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaya" denmektedir. Bilişim kavramı olarak "dolandırıcılık" bilgisayar veya iletişim araçlarıyla

17- EKER, a.g.w.s, 13.06.2006

kişileri şaşırtma, aldatma, kandırma olarak tarif edilebilir.

Bilgisayar yoluyla dolandırıcılık; kredi kartlarının bir benzerinin yardımcı programlarla oluşturulması ile yetkisiz ve izinsiz erişilen bilgilerin kopyasını almak şeklinde, finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle ve kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak; kişileri kandırarak dolandırıcılık suçu işlemektedir.

4. Bilgisayar Yoluyla Sahtecilik:

Yine klasik olarak bilinen sahtecilik suçunun, yüksek teknoloji ürünü cihazlar kullanılarak yapılmasıdır. Bilgisayar suçlarının tanımı içerisinde bu suçlara bakıldığında diğer sahtecilik suçlarından ayırt edebilmek için bilgisayar yoluyla sahteciliği ayrı olarak ele almak gerekmektedir. Çünkü; bilgisayar kullanımı ile üretilmiş sahte para suçunda, olay yerinde delil niteliği teşkil edecek bilgilerin bulunması çok zordur ve bu delillerin toplanması ve soruşturulması teknik bir olay olarak karşımıza çıkmaktadır.

Bazen ileri teknoloji ürünü cihazlar kullanılarak, bazen de çok basit Web (Ağ) programcılığı (Fake mail-sahte mail, Phishing-oltalama, avlama) yöntemiyle sahtecilik yapılmaktadır. Günümüzde başkalarının adına e-mail göndererek, ticari ve özel ilişkilerin zedelenmesini sağlamak, başkalarının adına web sitesi hazırlamak ve bu Web sitesinin tanıtım amacıyla başkalarına e-mail ve mesaj göndererek (iletişim kurarak) ve bu mesajlarda da mağdur olan şahsın telefonlarını vererek, sahte para, sahte evrak, sahte bilet vb. basma yönetimiyle bu suç işlenmektedir. [18]

5.Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı:

5846 Sayılı Fikir ve Sanat Eserleri Kanunu'nda, eser olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılmasıdır. Kanunla korunmuş bir yazılımın izinsiz kullanımı, yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılmasını ve kullanılmasını ifade eder. Bilgisayar yazılımları satın alınırken üzerinde gelen lisans sözleşmesine göre bir yazılımın bir adet kopyası ancak satın alan şahıs tarafından yapılacağı ve bu yazılımın

18- EKER, a.g.w.s, 13.06.2006

başka bir kişi tarafından kopyalanmayacağı ve kiralanmayacağı belirtilmektedir. Bir çok yazılım şirketinin yazılım korsanlığına karşı hukuki işlemlerini yürüten BSA (Business Software Alliance)'nın verdiği rakamlara göre ülkemizde lisanssız yazılım kullanımının %80'lerin üzerinde olduğu belirtilmektedir.

Günümüzde korsan CD basımı ve dağıtılması korkunç büyüklükte boyutlara ulaşmakta, yapılan operasyonlar sonucu ele geçirilen lisanssız ürünlerin mali değerinin yüksekliği bu gerçeği ortaya koymaktadır. Tüketici (yazılımı satın alan) da lisanssız çoğaltılan ürünleri ucuz olmasından dolayı tercih etmektedir. Unutmamak gerekir ki korsan yazılımları alan ve satan kişiler kanun önünde suçlu sayılmaktadır. Bu korsan yazılımlar; güvenlikli olmamakla birlikte; kullanımından doğan sorunlar karşısında herhangi bir müracaatta bulunulamamaktadır. Zira bu tür korsan yazılımlar genellikle bilgisayar ve kullanıldığı teknolojik araca zarar vermekte, tamir edilmesi imkansız sorunlara yol açmakta, bazı durumlarda boş çıkmakta, bazen de virüs barındırmaktadır.

6.Yasadışı Yayınlar:

Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, Internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir. Kanunun yasaklamış olduğu bu materyaller; Web siteleri (sayfaları), BBS (Bulletin Board Services-Duyuru Tahtası Hizmetleri)'ler, elektronik postalar, haber grupları, forumlar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir.

Yasadışı yayınları üç gruba ayırmak mümkündür:

Bunlardan birincisi; ülkenin bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli Internet sayfalarıdır. Özellikle terör örgütleri tarafından hazırlanan bu sayfalarda Türkiye içerisinde yayınlayamadıkları bölücü fikirlerini Internet ortamında çok rahat teşhir edebilmektedirler. Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş (yapmak istedikleri yayınları kabul edilmediğinden- Anayasa'nın 3. maddesine, bölünmez bütünlüğe aykırılık) anonim olan Internet'i kullanarak kendilerine taraf toplamayı hedeflerler ve bilinen klasik yollardan ulaştıramadıkları ideolojilerini, vatanın bütünlüğünü bozacak düşüncelerini bu sayede ifade etmektedirler.

İkinci olarak; halkın ar ve haya duygularını incitecek şekilde genel ahlaka aykırı pornografik görüntüler içeren Internet sayfaları da yayınlana bilmektedir.

Yurtdışındaki diğer ülkelerde genel itibariyle çocuk pornografisi üzerine yoğunlaşmış ve ona göre çalışmalar yapılmıştır. Ülkemizde ise; çocuk veya büyük pornografisi şeklinde bir ayrım yapılmadığından bütün pornografik yayınlar yasaklanmış durumdadır.

Üçüncü olarak da; bir kişiye karşı yapılan hakaret ve sövme suçudur. Bu suç türü Internet üzerinden başkalarının adına uygun olmayan e-mailler göndererek kişi yada kurumların itibarını zedelemek suretiyle olabilmektedir. Bir başka yol ise yine kişi yada kurumların sahip oldukları adın, lakabın Web üzerinden satın alınarak, kişi aleyhine yayında bulunmak suretiyle meydana gelebilmektedir. Ülkemizde bu ve benzeri olaylar sıkça yaşanmaktadır. Gazetelere yansıyan olaylarda; birbirini tanımayan insanların chatte-sohbet odalarında küfürleşmeleri ve daha sonra buluşup birbirlerini yaralamaları yada bir zaman milletvekilliği yapmış bir kişinin adı ve soyadını oluşturduğu domain-alan adını alarak pornografik site oluşturmaları gibi.

Her geçen gün gelişen iletişim araçları (Internet vb.) üzerinden meydana gelen hakaret, sövme konusunda maalesef etkili bir önlem alınamamaktadır. Bu tür durumlarda kişilerin kendi çabalarıyla halletmeye çalıştıkları, bu konuda savcılığa başvurunun az olduğu görülmüştür. Halbuki bu suç Internet'te işlenmesi yüksek olan bir suç türüdür. Alınabilecek önlemler, kullanıcıların daha duyarlı ve dikkatli olması, gelen e-mailleri dikkatli okuması, spam mesajları derhal silmeleri, gerekirse önemli gördükleri kişi yada kurumlarla iletişim kurarken özel bir işaret kullanarak irtibatı sağlamaları şeklinde olmalıdır.

Bilişim suçları kapsamına giren suçların tanımlanması ve sınıflandırılmasının yapılması daha sonra yapılacak çalışmalara hazırlık teşkil edecek ve her bir suç tipi daha rahat anlaşılmış olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken "suçun işlenmesindeki amaç" olmalıdır. Bu tür suçlar hangi yöntemle işleniyor olsa da, hangi amaca hizmet ettiğine bakmak lazımdır. Örneğin; bir bilgisayar sistemine girmek için bir çok yöntem bulunabilir; bir virüs veya trojan kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Ancak burada amacın "sisteme girme" eylemi olduğuna dikkat etmek lazımdır. Burada kullanılan yöntemler ancak suçun ağırlaştırıcı sebeplerini oluşturabilir. Mesela bir sisteme girerken başka sistemlere de sızmış olması gibi. Bu suç tiplerine bakacak olursak;

- Bilgisayar sistemlerine ve servislerine yetkisiz olarak girme ve engelleme,
- Bilgisayarlara fiziksel veya mantıksal yollar ile zarar verme,
- Bilgisayar yoluyla dolandırıcılık,
- Bilgisayar yoluyla sahtecilik,
- Lisans haklarına aykırı olarak bir bilgisayar yazılımının izinsiz kullanımı,
- Internet üzerinden yasadışı yayın yapma.[19]

Yukarıda belirtilen, bilişim suçlarının çeşitlerine ek olarak bilgisayarla işlenen suçları aşağıdaki şekilde de tasnif edebiliriz:

A-Sahtekarlık:

1. Kredi almak veya ödemelerden faydalanmak için şirketler kurmak,

2. Var olmayan eşyalar veya servisler için faturalar hazırlamak,

3. Şirketin finansal menkul veya gayri menkulleri veya sahte şahıslar oluşturarak bilgilerin değiştirilmesi ve düzenbazlığı,

4. Sahte bilgisayar kayıtları, ödemeler, dokümanlar, bilgi kartları, işlem hesaplarını içeren sahtekarlığın diğer çeşitleri. Örnek olarak aşağıdaki olaylar incelenebilir;

20 Nisan 1983'te Uluslararası Birleşik Basın'ın bildirdiğine göre 27 yaşındaki bir teknisyen Los Angeles Dodgers şirketine ait bilgisayarlı bilet sistemine girerek hileli bir şekilde 7000 bilet çalmaktan tutuklanmıştır.

28 Martta Dodgers şirketi biletlerde önemli miktarda azalma olduğunu fark ettiğinde 21 Şubat tarihinde hesap uzmanları bilgisayarın ve hesabın yapıldığını gördüler. Ama bu tarihte bilgisayarın açılmayacağı herkesçe biliniyordu.

Polis 11 Nisan'da oynanan bir oyun sırasında sahte biletleri tespit ederek bileti nereden aldıklarını sordu. Tahkikatın hızlı ve etkili bir şekilde yürütülmesinin ardından kendini bilgisayar dahisi olarak tanıtan birisi, bu sisteme girmede asıl suçlu olan

---

19- **Bilişim Suçları ve Siber Terörizm**, inet-tr.org. tr, http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=37&Itemid=29, 02.04.2006

teknisyene yardımcı olduğunu ve bu sayede her türlü bilgisayara girerek kolaylıkla işlem yapabildiklerini söylemişti.

B-Zimmetine Geçirme:

1. Şirketin parasını vb. kendi üzerine geçirme işlemidir.

Örnekler:

a) Banka sekreterlerinin vadeli, vadesiz hesaplarda bulunan paraları şahsi hesabına transfer etmesi veya ciro edilebilir eşyaların alışverişini yapması,

b) Yüksek ücret veya haksız fazla mesai ücreti elde etmek için bilgisayara sahte ücret bordro bilgileri girilmesi,

c) Gerçekte kendisi olan ama bilgisayarda firma olarak görünen yerlere ödeme talimatı çıkarmak.

Bilgisayar bağlantılı suçlar düzenlemek için iyi bir uzman olmanız gerekmez. Bilgisayar operatörleri bir haftadan daha az bir zaman içinde çalışarak bu konuyla ilgili bilgi alabilir. Bu çalışma onlara sistemin şifresine girme veya diğer güvenlik sistemleriyle ilgili çok önemli bilgileri elde etmek imkanını sağlayacaktır. Banka mevduat hesapları ve diğer hesaplar, banka envanterleri ve alındı makbuzları gibi bilgisayara girişi yapılan belgelerde değişiklik yaparak işlenen bilgisayar hilekarlıkları genelde bu şekildedir.

C-Bilgisayarı Hizmet Dışında Kullanmak:

1. Bilgisayar imkanlarının özel eğlence veya özel kar amacıyla yetkisizce kullanılması.

Örnekler:

a) Bazı gizli bilgilerin dökümünü bilgisayardan alarak rakip bir firmaya satmak,

b) Şirketin, kurumun, kuruluşun sahip olduğu bilgi ve imkanları içeren sistemi özel bilgisayarını kullanarak kendi özel işlerine tahsis etmek,

c) Bir yabancı şirketin, kurumun, kuruluşun bilgisayarına bağlantı yaparak;

- Hesaplarla oynanabilir,

- Şahsi araştırmalar için ihtiyaç duyulan bilgiler sağlanabilir,
- Şirket kayıtları eğlence için gözden geçirilebilir,
- Bilgisayarın iç güvenlik korumasını deşifre ederek her türlü gizli bilgi kontrol edilebilir,
- Yüksek teknolojiyi yıkıcı hareketler düzenlemek için programları değiştirilebilir.

D-Program Hırsızlığı:

1. Telekomünikasyon araçlarını veya bilgisayarları yetkisizce kullananlar, hazırlanması yüksek meblağlar tutan gelişmiş programlar şahsi işlerinde kullanmak veya diğerlerine satmak üzere çalarlar.

Örnekler:

- Hesaplama programları,
- Mühendislik programları; deneysel modellerin yapılmasında kullanılan programlar, uçaklar için rüzgar dirençleri, inşaat yapımında kullanılan baskı maddeleri vb.

E-Bilgi Hırsızlığı:

1. Müşteri listesi veya posta adresleri gibi bilgi ve programlar çoğaltılır ve rakiplere veya bu bilgilere değer veren şahıslara satılır. Çünkü orijinal bilgi genellikle bilgisayarda kalır. Bu suç, bilgisayardaki bilgilerin print (yazmak, yazdırmak) edilmesiyle meydana gelen küçük bir hırsızlık türüdür.

2. Çok kıymetli ve gizli bilgilerin illegal olarak elde edilmesi. Örneğin;

- Pazarlama planları,
- Gizli işlemler,
- Üretim düzeni,
- Telif hakkı olan materyaller,
- İç haberleşmenin elektronik olarak dağıtılması,
- Teknik bilgiler.

F-Sabotaj:

1. İşverene karşı yıkıcı hareketler,

2. Şirket çalışanlarına engel olmak için bilgisayarı kullanmak,

3. Siyasi protestolar.

Teknolojinin ilerlemesi ile birlikte birçok yeni suç tipinin çıkması muhtemeldir. Bahsedilen suç tiplerine dikkat edildiğinde iki şekilde kategorize edebiliriz. Bunlardan birincisi; geleneksel suçların bilgisayar yolu ile işlenmesi diğeri ise yeni teknolojiler ile birlikte ortaya çıkan suç tipleridir.[20]

1.1.1 Interpol'e Göre Bilişim Suçlarının Sınıflandırılması:

Bilişim alanındaki suç tiplerini incelerken Interpol'ün hazırlamış olduğu "Interpol Computer Crime Manual (Interpol Bilgisayar Suçu El Kitabı)" esas olmak üzere, Birleşmiş Milletlerin hazırlamış olduğu "United Nations Manual on The Prevention and Control of Computer-Related Crime (Birleşmiş Milletler Bilgisayar Suçunu Önleme El Kitabı)" kitapçığı ve Avustralya polis teşkilatının hazırlamış olduğu "Minimum Provisions for The Investigation of Computer Based Offences (Temel Bilgisayar Suçunun Araştırılmasının Minimum Şartları)" kitapçıklarından istifade edilerek aşağıdaki suç tipleri belirlenmiştir.

1-Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim:

A-Yetkisiz Erişim:

Tanım: Bir bilgisayar sistemine yada bilgisayar ağına yetkisi olmaksızın erişmektir.

Açıklama: Suçun hedefi bir bilgisayar sistemi yada ağıdır. "Erişim" sistemin bir kısmına yada bütününe ve programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Bu bir kişi tarafından bir bilgisayara direkt olarak

---

20- ÖZCAN, a.g.w.s, 29.01.2006

yakın bir yerden erişebileceği gibi, dolaylı olarak uzak bir mesafeden örneğin bir modem hattı yada başka bir bilgisayar sisteminden de olabilir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 2)

B-Yetkisiz Dinleme:

Tanım: Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir.

(Interpol Computer Crime Manual, 2.Offences, Sayf a 3)

Açıklama: Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferini içerir.

C-İletişim:

- Tek bir bilgisayar sistemi içerisinde,
- Aynı kişiye ait iki bilgisayar sistemi,
- Bir biriyle iletişim kuran iki bilgisayar arasında,
- Bir bilgisayar ve bir kişi arasında yer alabilir.

Teknik anlamda dinleme, iletişimin içeriğinin izlenmesi, verilerin kapsamının ya direk olarak (bilgisayar sistemini kullanma yada erişme yoluyla) yada dolaylı olarak elektronik dinleme cihazlarının kullanımı yoluyla) elde edilmesi ile ilgilidir.

Suçun oluşması için hareket yetkisiz ve niyet edilmiş olarak işlenmesi gerekir. Uygun yasal şartlar çerçevesinde soruşturma yetkililerinin yaptıkları bu kategoriye girmez.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 3)

D-Hesap İhlali:

Tanım: Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının dijital hesabını kötüye kulanma.

Açıklama: Bu tip suçlar normalde geleneksel suçlardaki hırsızlık, dolandırıcılık gibidir. Pek çok bilgisayar servis şirketleri ve ağları kullanıcılar için yaptıkları ödemeleri ve hesaplarını kontrol etmek amacıyla otomatik faturalandırma araçları temin

etmişlerdir. Hesap ihlali, yetkisiz erişim yapılarak başkasının hesabını kullanarak sistemlerden istifade etmek şeklinde olabilir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 3)

2-Bilgisayar Sabotaj:

A-Mantıksal (Bilgisayar verilerine zarar verme yada değiştirme):

Tanım: Bir bilgisayar yada iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir.

Açıklama: Bir bilgisayar yada iletişim sisteminin fonksiyonlarının çalışmasını engellemek amacıyla verilerin yada programların Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horses), Virüsler, Solucanlar (Worms) gibi yazılımlar kullanarak değiştirilmesi, silinmesi, ele geçirilmesi yada çalışmaz hale getirilmesidir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 4)

B-Fiziksel:

Tanım: Bir bilgisayar yada iletişim sistemine fonksiyonlarını engelleme amacıyla fiziksel yollarla zarar vermedir.

Açıklama: Bir bilgisayar yada iletişim sistemini oluşturan parçalara sistemin fonksiyonlarını yerine getirememesi amacıyla fiziksel yollarla zarar verilmesidir.

3-Bilgisayar Yoluyla Dolandırıcılık:

Tanım: Bilgisayar ve iletişim teknolojileri kullanarak verilerin alınması, girilmesi, değiştirilmesi, silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek veya mağdura zarar vermektir.

Açıklama: Bilgisayar bağlantılı dolandırıcılık suçları genellikle dolandırıcılığın geleneksel ceza kanunları içerisindeki tanımlarındaki gibi değerlendirilir ve kovuşturması bu kapsamda yapılır. Suçlunun hedefi kendisine veya bir başkasına mali kazanç sağlamak yada mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları suçluların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık gösterir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 6)

A-Banka Kartları:

Tanım: Bankamatik sistemlerinden yapılan dolandırıcılık ve hırsızlık suçlarıdır.

Açıklama: Bankamatik sistemleri (ATM -Automated Teller Machine- olarak da bilinir) genelde bankalar yada benzer finans kuruluşları tarafından kullanılır ve şifreli ağ sistemlerini kullanırlar. Erişim genellikle bir kişisel tanımlama numarası (PIN - Personel Identification Number) girişi gerektiren bir kart yada benzeri bir sistem iledir. Dolandırıcılık bu kartların çoğaltılması, kopyalanması yada iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur.

Uluslararası olaylarda, diğer ülkelerdeki yetkililerle görüşülmesi durumunda sistemin özelliklerinin bildirilmesi çok önemlidir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 7)

B-Girdi/Çıktı/Program Hileleri:

Tanım: Bir bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden çıktı almak yada sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır.

Açıklama: 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.

Yanlış çıktı daha az yaygındır ve genellikle sahte dokümanların veya çıktıların üretiminde kullanılır. Bu tür suçları araştırırken kullanılan sistem incelenmelidir ve saklı veya silinmiş dosyaları kurtarmak için her türlü çaba gösterilmelidir.

Program hilelerinin tanımlanması teknik açıdan daha zordur. Yaklaşık üç çeşit geniş bilgisayar programı kategorisi vardır:

I- Ticari piyasa için yazılmış yazılımlar ki satışa açıktır,

II- Yukarıda belirtilen şekilde alınmış fakat sonradan belli bir amaç için değiştirilmiş yazılımlar,

III- Belirli bir amaç için özel olarak yazılmış ve satışa yada dağıtıma açık olmayan yazılımlar.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 9)

C-İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma:

Tanım: Kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerine veya diğer bilgisayar sistemlerine hakkı olmadan girmek.

Açıklama: İletişim servislerinin değişik şekillerde kötü kullanımı olarak tanımlanabilir. Fiil bazen yüksek telefon faturalarının önüne geçmek için işlenebilir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 10)

4-Bilgisayar Yoluyla Sahtecilik:

Tanım: Kendisine veya başkasına yasa dışı ekonomik menfaat temin etmek veya mağdura zarar vermek maksadıyla; bilgisayar sistemlerinin kullanılarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

Açıklama: Dijital ortamda tutulan dokümanlar üzerinde değişiklik yapmak sahteciliktir. Bilgisayarlarda tutulan dokümanlarda (İş akış programları, raporlar, personel bilgileri gibi) sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilmektedir. Bu ve bundan önceki örneklerde bilgisayar sistemleri suçlu aktivitelerin hedefi durumundadır. Fakat bilgisayarlar sahtecilik yapmak amacıyla bir araç olarak da kullanılabilir. Modern yazılımların güçlendirilmiş grafik kapasitesi, ticari alandaki pek çok belgenin sahtesini yapmak için olanak sağlamıştır. Modern teknoloji, özellikle renkli lazer yazıcıların ve fotokopi cihazlarının gelişimi ile daha önceden üretilmesi çok zor olan belgelerin kopyalanmasını mümkün kılmıştır.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 7)

5-Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı:

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

(Interpol Computer Crime Manual, 2.Offences, Sayfa 11)

A-Lisansız Sözleşme İhlali.

B- Lisans Sözleşmesine Aykırı Kullanma:

Tek bir bilgisayar için bir yazılımın birden fazla bilgisayarca paylaşılarak kullanılmasıdır. Yazılım lisansları genellikle tek bir bilgisayarla kullanılmak için tanzim edildiğinden, ayrıca ek lisans alınmaması halinde diğer bilgisayarlarca da kullanılması durumunda lisans sözleşmesi ihlal edilmiş olur. Tüm bilgisayarlar için ayrı ayrı lisans alınması şarttır.

C- Lisans Haklarına Aykırı Çoğaltma:

Lisans Sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kopyalanmasıdır. Genel itibariyle; ödemeden kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılım, başka bir medya ortamına taşınır. Burada sözkonusu yazılımı kopyalayanda kopyalatanda sözleşme ihlali etmiş olur.

D- Lisans Haklarına Aykırı Kiralama:

Değişik medyalar üzerine kayıtlı oyun, film ve yazılım programlarının lisans haklarına aykırı olarak kiralanmasıdır.

E- Taklitçilik:

Yazılım taklitçiliği, fikri haklara tabi olan yazılımların, çoğunlukla yasalmış gibi bir görünüme sahip olacak şekilde yasadışı çoğaltılması ve satılmasıdır. Son kullanıcıların aksine, yazılım taklitçileri salt kar amacıyla hareket eder ve para alış verişi söz konusudur.

Fatura yada benzeri belgeler yazılım taklitçiliğinin saptanması ve izlenmesine olanak vermektedir.

F- İzinsiz İthalat

Yazılım hakkı sahibinden ve yetkili makamlardan gerekli izni almaksızın, herhangi bir bilgisayar yazılımının ithal edilmesidir.

6-Yasadışı Yayınlar:

Tanım: Yasadışı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılmasıdır.

Açıklama: Kanun tarafından yasaklanmış her türlü materyalin Web sayfaları, BBS (Bulletin Board Service-Duyuru Tahtası Hizmetleri)'ler, elektronik postalar, haber

grupları ve her türlü veri saklanabilecek optik medyalar gibi dijital kayıt yapan sistemler vasıtasıyla saklanması, dağıtılması ve yayınlanmasıdır.

7-Diğer:

A-Ticari Sırların Çalınması:

Tanım: Ekonomik kayıp vermek yada yasal olmayan bir ekonomik avantaj sağlamak niyetiyle yetkisi yada herhangi bir yasal sebebi olmaksızın uygun olmayan yollarla bir ticari sırrın kullanımı, transferi, ifşası yada elde edilmesidir.

Notlar: Bilişim suçları, ticari sırların hırsızlığını da özellikle suç bir bilgisayardaki saklanmış verileri ilgilendiriyorsa kapsayabilir. Endüstriyel espiyonaj olarak da bilinir.

(Interpol Computer Crime Manual, 2.Offences, Sayfa 15)

B-Verilerin Suistimali:

Tanım: Ticari yada mesleki sırların, kişisel bilgilerin yada değerli diğer verilerin kendisine veya başkasına menfaat sağlamak yada zarar vermek amacıyla bu bilgilerin kullanımı, satılması ve dağıtımıdır.

Açıklama: Müşteri bilgileri, hasta bilgileri gibi banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kendisine yada başkasına menfaat sağlamak veya zarar vermek amacıyla kişilerin rızası dışında kullanılmasıdır.

(Minimum Provisions for The Investigation of Computer Based Offences, Sayfa 21)

C-Sahte Kişilik Oluşturma ve Kişilik Taklidi:

Tanım: Hile yolu ile kendisine veya bir başkasına menfaat sağlamak yada zarar vermek maksadıyla hayali bir kişilik oluşturmak veya bir başkasının bilgilerini kullanarak onun kişiliğini taklit etmektir.

Açıklama: Bilgisayar sistemlerine yetkisiz erişim sağlamak yada kullanma hakkı kazanmak amacıyla gerçek kişilerin taklidi yada hayali kişiler oluşturmak etkili metotlardan biri olarak bilinir. 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.

(Minimum Provision for The Investigation of Computer Based Offences, Sayfa 21)[21]

1.2 Bilgisayar Suç Teknikleri:

A-Salami Tekniği:

1. Banka hesabında bulunan bononun küçük bir kısmını çıkışlı bir bilgisayarla alarak, bu hesabı olayı düzenleyen tarafından oluşturulmuş bir başka banka hesabına transfer etmek.

2. İpotek ödemeleri, ücret bordro çekleri ve diğer ödeme şekilleri genellikle brüt rakamları içerir ki bunlar belli hafta ve aylara bölünmüştür. Eğer hırsız, binlerce ödemeyi içeren bilgisayar programına girmeyi başarırsa kısa bir zaman aralığında hırsız kendi hesabına büyük miktarda para transfer etmiş olur.

B-Mantık Bombası:

1. Amaç zorla alma veya intikam alma,

2. Şahıs eğer kesin kriterler bulunduysa, mevcut programların bazıları veya tamamını yok etmek veya tahrip etmek için bilgisayarı programlar.

Örnekler:

a) Eğer operatör şahıs bilgisayarın şifresini çözebildiyse bilgisayardaki tüm kayıtları ve programları silebilir.

b) Bir operatör, şirketin bilgisayarına, içindeki tüm bilgileri yok edecek veya kullanılmaz hale getirecek "mantık bombası" atar. Ve sonra fidye ister, fidye verilmediği taktirde tüm giriş sistemini tahrip eder.

c) Elektronik ekipman kullanarak gizlice dinleme,

21- COŞKUN, Özkan, **Bilişim Suçlarının İşlenme Şekilleri**, http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=251, 13.01.2007

1. Terminaller, daktilolar, printer (yazıcı) ve tele teypler gibi bilgisayarlar ve cihazlar elektronik gözetime tabi tutularak, yaydıkları sinyaller engellenebilir.

2. Suçlu türleri;

- Endüstriyel veya düşman casusları,
- Radikal gruplar,
- Gaspçılar,
- Şantajcılar.

1.3 Bilgisayara Giriş Metotları:

A-Göz Gezdirmek ve Temizlemek:

1. Yetkisiz şahıs, aşinalığıyla beraber bilgisayar uzmanlarıyla birlikte doğru kodları geliştirir.

2. Yetkisiz şahıs, bilgisayar kullanıcısı veya yetkili programcının omuzları arkasından bakarak giriş kodunu okur.

3. Yetkisiz şahıs, çöp kutusuna bakarak giriş koduyla ilgili bir döküm, kayıt veya disk bulmaya çalışır.

Örnek: Birkaç yıl önce Kaliforniya'da amatör bilgisayar heveslisi Pasifik Telefon ve Telgraf Şirketi çöplüğündeki çöpleri karıştırarak, bilgisayar dökümü atıklarından kendine bir kütüphane kurdu. Bu kütüphane, dökümlerdeki yöntemleri izleyerek şirketin bilgisayarını kullanabileceği bir sistem kurmasını sağladı. Daha sonra bilgisayara talimat verecek bir metot geliştirdi ve bilgisayar sistemiyle donatılmış küçük odasından ekipman dağıtımını yönetti.

Bu hevesli, ekipman dağıtımı ve pazarlama işini öğrendikten sonra bir şirket kurdu, şirketin sattığı ekipmanlar PT ve T'nin fiyatları altında ve cazip olduğu için, şirket kısa sürede gelişti ve büyüdü. 40 günde tam kapasiteyle çalışan bir fabrika haline geldi, fakat aldığı maaşın azlığından şikayet eden ve işinden atılan bir işçinin polise başvurması sonucunda her şey ortaya çıktı ve hevesli tutuklanarak 2 ay hapis cezasına çarptırıldı. Heveslinin ucuz hizmeti 40 gün sürmüştü.

B-Sahne Kapısı:

1. Bilgisayar yazılım programındaki normal güvenlik kontrollerini bertaraf eden bir elektronik yöntemdir.

2. Şu şekilde meydana gelebilir;

a) Programcı bunu programın dizaynını basitleştirmek için yapar fakat kasıtsız olarak programın kullanıma hazır olduktan sonra silme de başarısız olur.

b) Bir suçlu saldırıda bulunulacak programın şifresini öğrenir.

Örnek: Bir suçlu; kalem regülatörü denilen şifre çevrilirken çıkan sesleri analiz eden ve kaydeden bir aygıt kullanabilir. Bu alet, kombinasyonları da değerlendirerek bilgisayarın giriş numarasını bulmuş olur.

C-Canlandırma:

1. Bir suçlu bilgisayar sistemine girebilmek için meşru kullanıcının imkanlarından faydalanır ve vasıtalarını kullanır.

2. İkinci bir kullanıcının kimlik tespiti şifresini kullanarak, suçlu ikinci kullanıcının bilgisayar kayıtlarına girer.

D-Maskeleme:

1. Suçlu bilgisayar sistemine girebilmek için komünikasyon hatlarına girer.

2. Kendi mini bilgisayarını veya diğer ekipmanları kullanarak bilgisayar kullanıcıları ile merkezi sistemi arasında yapılan mesajları keser.

3. Suçlu "Piggy-arka kapı girişi" denilen basit bir sistem kullanarak bilgisayarla diğer şirketler arasına girerek kendi mesajlarını gönderebilir. Örneğin banka hesabına girerek hesabın miktarını artırma, azaltma gibi veya şirketin kredi başvurusuyla ilgili bazı sahtekarlıklar vb.

1.3.1 Bilgisayar Dolandırıcılığında Phishing Yöntemi:

İnsanoğlunun her daim hızlı bir değişim içinde bulunduğu, çağlar boyunca görülmüş ve kendi doğası içinde hep yeni şeyler arayışını doğurmuştur. İnsanoğlunun

eski alışkanlıklarını bıraktığı ve hızla çağa ayak uydurduğu şu günlerde, bunu en güzel yansıtan şey ise şüphesiz ki **Internet'tir.**

Eskiden bir banka işlemi için saatlerce kuyrukta beklenirken artık bu gibi işlemler saniyelerle ifade edilebilen bir hıza ulaşmış durumda veya saatlerce dolaşılıp alınan bir hediye Web sayfalarından anında alınabiliyor. Bu ve benzeri güzelliklerini gördüğümüz Internet'in ne yazık ki kullanıcı tabanlı olarak kötü yanları da bulunmakta.

Günümüzde Internet kullanıcılarının %80 gibi bir kısmının artık olmazsa olmazlarından olan e-posta, Internet bankacılığı, e-alışveriş gibi birçok kullanım alanları kötü niyetli Internet kullanıcıları tarafından istismar edilmekte.

İşte özellikle ülkemizde şu günlerde bu şekil istismarların başında gelen olay ise: **PHISHING** yani kısaca bankanızın, e-postanızın veya bunun gibi bilgi girmenizi gerektiren bir kuruluşun Web sayfasının bir kopyasını yapıp kullanıcının hesap bilgilerini çalmayı amaçlayan bir Internet dolandırıcılığı. İngilizce "balık tutma" anlamına gelen "Fishing" sözcüğünün "f" harfinin yerine "ph" harflerinin konulmasıyla gelen terim, oltayı attığınız zaman en azından bir balık yakalayabileceğiniz düşüncesinden esinlenerek oluşturulmuş ve uygulanıyor.[22]

Phishing yöntemiyle kredi kartı, ATM kart numaraları (şifreleri, güvenlik kodları), genel bağlamda şifreler veya parolalar, hesap numaraları, Internet bankacılığında kullanılan kullanıcı adı ve şifreleri vs. ele geçirilebilmektedir. Phishing yöntemi sahte posta (fake-mail) ile hedef kullanıcıya ulaşarak yapılmaktadır.

Bu yöntem; hedef kullanıcının bağlantı halinde olduğu kullanıcı adı, şifre yazarak girdiği her türlü Web site adına (Internet bankacılığı, e-ticaret); kullanıcıya e-posta göndermek suretiyle dolandırmayı (aldatmayı) amaçlarlar. Bu dolandırma yada aldatma türü bazen kişilerin e-maillerine sanki ilişkisi olduğu Web sitelerinin adına gönderiliyormuş hissi verilerek yapılır. Gelen mailde kişiye kullanıcı adı ve şifresinin süre aşımına uğradığı yada güncelleştirmesi gerektiği vb. türlü yazılar, formlar gönderilir. Kişi de bu formları farkında olmadan doldurur ve halen geçerli olan kullanıcı

22 - http://www.iem.gov.tr/iem/?m=3&s=51#1, 10.08.2006

adı ve şifre dolandırıcıların eline geçmiş olur. Bazen de yarışma olduğunu yada e-kart geldiğini söyleyerek gerekli formların doldurulması sağlanmak suretiyle "Phishing" yapılmış olur.[23]

Örneğin; kullandığınız elektronik posta servisinin giriş ekranının bir kopyası elektronik posta olarak geliyor ve bir şekilde kullanıcı adınızı ve şifrenizi girmenizi istiyor. Dikkatsiz bir şekilde bilgileri verdiğinizde, sayfanın içine gizlenmiş bir kod parçası kullanıcı adınızı ve şifrenizi dolandırıcılara gönderiyor.

1.3.2 Neler Çalınıyor ?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen işlemleri çalıyorlar:

1. Kredi, Debit/ATM Kart Numaraları/CVV2,

2. Şifreler ve parolalar,

3. Hesap numaraları,

4. Internet bankacılığına girişte kullanılan kullanıcı kodu ve şifreleri.

1.3.3 Phishing Saldırılarından Nasıl Korunmalıyız?

Unutulmaması gereken nokta her türlü online dolandırıcılık, sahtekarlık ve virüslere karşı en büyük korunma aracı, bu konuda bilinçli ve bilgili olmaktır. Bunu aklımızın bir kenarında devamlı bulundurmalıyız. Tabii ki Internet'te güvenli alışveriş yapmayı istiyorsak.

1. e-postanıza gelen mesajların doğruluğunu ispatlayın. Tanımadığınız kimselerden gelen mesajları silin, asla cevap vermeyin. "Aşağıdaki bağlantıya tıklayın" gibi e-posta isteklerine asla yanıt vermeyin.

23- EKER, a.g.w.s, 13.06.2006

2. İşlemlerinizi online yaparken, işlem yaptığınız Web sayfasının güvenli olup olmadığını mutlaka kontrol edin.

Internet tarayıcınızın üst kısmında bulunan adres bölümünde bulunan adresin "https://" olup olmadığını kontrol edin. “https://” in sonunda bulunan “s” harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırdığını belirtir.

Ek olarak, Internet tarayıcınızın sağ alt kısmında yer alan kapalı kilit işareti, yine güvenli ve şifrelenmiş bir sayfada işlem yaptığınızı gösterir.

Şekil 1

Yukarıdaki şekilde gösterilen işaret sayfanın SSL (Secure Sockets Layer) ile şifrelendiğini ve sitenin gerçekten çalıştığınız kuruluşa ait olup olmadığını göstermektedir, üzerine iki kez tıklandığında ise; aşağıdaki örnekte görüldüğü gibi bir mesaj çıkacaktır.

-Örnek olarak; "Issued to:www.abidayibank.com.tr ve "Issued by: www.verisign.com/CPS Incorp.by Ref.LIABILITY LTD.(c)97 VeriSign" bilgileri kontrol edilmelidir.

Unutulmaması gereken noktaların başında ise yukarıda anlatılan bu iki güvenlik önlemi de dolandırıcılar tarafından tekrar oluşturulabiliyor. Bu sebeple; eğer Internet bankacılığını veya e-alışveriş yapmak istiyor iseniz yapmanız gereken şey, işlem yapmak istediğiniz sayfayı kendinizin girmesi en güvenilir yoldur.

3. Internet adresi olarak sayısal rakamlar içeren adresler ile karşılaşırsanız kullanmadan önce **mutlaka** kontrol edin.

Ziyaret ettiğiniz Web sitelerinde; adresler çoğunlukla adres kısmı, ardından firmanın ve şirketin ismine ek olarak, “com, org, net” gibi uzantılar ile biter. Örneğin;

“https://www.abidayibank.com.tr” Sahte sitelerde, çoğu zaman sayısal adresler kullanılmaktadır. Eğer bu tür bir durum ile karşılaşırsanız, direkt olarak çalıştığınız kuruluş ile irtibata geçin.

-Örnek olarak; Sahte siteler aşağıdaki gibi sayısal bir link verirler:

Şekil 2

4. Size ulaşan e-posta’nın kimden geldiğinden ve doğruluğundan mutlaka emin olmalısınız.

Öncelikle gelen e-postanın kimden geldiğine muhakkak emin olmalısınız, eğer ki e-posta’nın kimden geldiğinden emin olamıyor veya gönderilen içerik ile ilgili bazı şüpheleriniz oluyor ise mutlaka direkt olarak sizden bilgi talep ettiğini öne süren gerçek kuruluş ile irtibata geçiniz. Çünkü çalıştığınız kurum size asla kişisel bilgileriniz veya şifrenizi soran e-posta göndermez.

5. Güvenmediğiniz Networks (Ağlarda) kesinlikle elektronik işlem yapmayınız. Kullandığınız bilgisayar güvenilir olsa bile eğer Networks (Ağlarda) güvenmiyorsanız elektronik işlem yapmayınız.

6. Bankanızdan gelen kart ekstralarını, hesabınızı düzenli olarak kontrol etmeyi unutmayın. Olası aksiliklerde bankanızla ile kesinlikle irtibata geçin.

7. Sisteminizi düzenli olarak kontrol edin. İşletim sisteminizin güvenlik yamalarını yükleyin, anti virüs yazılımınızı devamlı olarak güncelleyin. Internet tarafından güncel kalmasını sağlayın.

8. Çeşitli kurumlardaki hesaplarınızı veya eğer ki birden fazla e-posta adresiniz var ise kesinlikle kendinizi her biri için farklı şifreler belirleyin.

9. Belirlediğiniz şifreleri belli aralıklar ile muhakkak değiştirin. Bunu kendinize alışkanlık haline getirin.

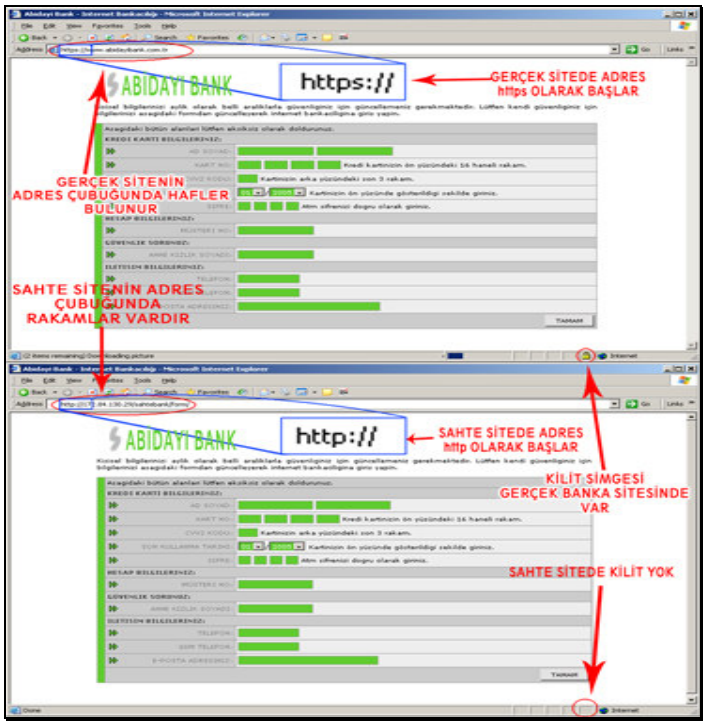
10. Phishing saldırılarına aracı olmayın; dolandırıcılığı gerçekleştirecek kişi veya kişiler Phishing yöntemi ile ele geçirdikleri kurumsal veya finansal bilgileri kullanarak hesaplar üzerinden paraları ele geçirme imkânına sahip olurlar. Paranın hesaptan çekilmesi aşamasında kendilerinin tespitini zorlaştırmak yada hiçbir şekilde tespit edilmemelerini sağlamak için ise şüphelenilmeyecek kişilere Internet üzerinde iş ilanları sunmaktalar. Bu ilanlarda çaba harcamadan kolay para kazanılacağı bunun çok kolay bir iş olduğu şeklinde bilgi verilmektedir.

Internet'te verilen bu ilan ile bulunan kişilerin banka hesapları kullanılarak Phishing yöntemi ile çalınan hesaplardan para transferi yapılmaktadır. Yine ilan ile bulunan kişiler hesaplarından bu paraları çekmek ve belirli bir komisyon karşılığı dolandırıcılığı gerçekleştiren kişilere parayı uluslararası para transferi yapan şirketler aracılığı ile transfer etmek için kullanılmaktadırlar. Böylece dolandırıcılığı gerçekleştiren kişi yada kişiler kimliklerini gizlemiş olup, ilan aracılığı ile bu işe başvuran kişilere suçu atmış olmaktadırlar.

Bu tip belirli bir parayı alıp, komisyon karşılığında başka bir yere transfer etmek şeklindeki iş ilanları konusunda çok dikkatli olunması gerekmektedir. Bu şekilde yapılan işlem kara para aklama işlemi olup, sonucu kanuni takibata varacak şekilde bitmektedir.

11. Eğer böyle bir eyleme maruz kalırsanız size gelen e-postayı kesinlikle silmeyin ve yönlendirdiği Web sitesiyle ilgili bilgileri toplamayı deneyin. Örneğin; "ripe.net" Internet adresinden "Who is? (Kim)" sorgulaması yapıp ilk bilgileri toplamaya çalışın. Derhal üstlerinize ve bilgi işlem departmanına haber verin. Eğer bireysel kullanıcıysanız bir dilekçe ile hemen savcılığa başvurup ilgili polis birimlerine elden havale alın ve yazıyı polise götürün.

Genel olarak sahte site ile gerçeğini ayırt etmek için aşağıdaki şekli inceleyebiliriz:



Şekil 3

1.3.4 E-Posta Yöntemi Nedir?

e-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları üç şekilde aldatma yoluna gidiyorlar. Şöyle ki:

a) e-postanıza devamlı temas halinde olduğunuz kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir posta gönderiliyor. Bu e-postalarda kullanıcıya kurumun Web sitesine giderek şifresinin süresinin dolduğu söyleniyor ve altta o sayfaya yönlendirileceği bir link (bağlantı yolu) veriyor. Korsan daha önceden hazırladığı ve kuruluşun sitenin aynısı olan bu siteye kurbanına getirdikten sonra, ondan şifreyi girmesini istiyor, sonra da kullanıcı kendi şifresini yeni şifresiyle değiştiriyor (normal de tabii ki değiştirmiyor. Esasen eski şifre hala geçerli olduğu için korsan bu şifre ile Internet aracılığı ile para transferi, e-ticaret vb. işler yapabiliyor)

b) Bazı e-postalarda ise; bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak BMW marka bir araç kazandıkları ancak gerekli

kişisel bilgileri vermeleri gerektiği söyleniyor. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının yani korsanın eline geçiyor.

c) Bir başka kullanılan teknikte ise; gelen e-posta da müşteriye kişisel bilgilerini güncellemesi gerektiği tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söyleniyor.

d) Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği belirtilmektedir.

Aşağıda örnek olarak e-posta iletisi verilmiştir:

Örnek:

Sayin Abidayı Bank Musterisi

Hesabiniza 24/subat/2005 tarihinde Huseyin ABİDAYI tarafindan 270 YTL. havale edilmistir. Yapilan havale ile

ilgili ayrintilar asagidadir.

Gonderen: Huseyin ABİDAYI

Miktar: 270,00 YTL. (iki yuz yetmis yeni turk lirasi)

Sube: Mardin / Merkez

Aciklama: -

Havale onay ve/veya red islemi icin asagidaki linkden internet bankaciligini kullanabilirsiniz ve/veya hesabinizda gerekli incelemeleri yapabilirsiniz. Size havale gonderen kisinin bilgileri icinde asagidaki linki kullanabilirsiniz...

www.abidayibank.com.tr

Eger yukaridaki link calismiyorsa lutfen asagidaki linki kullaniniz.

http://172.84.130.29/abidayibank/form/

Şekil 4

1.3.5 Bilgisayar Dolandırıcılığında Keylogger ve Screenlogger Yöntemi:

Dolandırıcılar Phishing yöntemiyle kullanıcının gizli bilgilerini elde etmenin yanı sıra bu bilgilere birde başka bir yöntem olan Keylogger adı verilen klavye ve ekran görüntülerini kopyalayabilen programlar vasıtası ile ulaşabilmekteler.

Internet kullanan banka müşterilerinin veya Internet üzerinden ticaret yapan kullanıcıların online işlem şifrelerinin çalınmasının bir diğer yöntemi ise Keylogger yani klavye tuş girdilerini kayıt eden yazılımlar vasıtasıyla gerçekleşmesidir. Kullanıcıların bilgisayarlarına yerleştirilen Keylogger adlı yazılım, bilgisayarda yapılan her türlü işlemlerin bir kaydını tutar ve bu kayıtlar klavyeden girilen bilgilerin yanı sıra ekran görüntüleri de olabilir. Bu kayıtlar ya sistemde bir "txt (metin)" dosyası olarak tutulur ya da klavye girdileri e-posta ile saldırgana gönderilir.

Keylogger, temel olarak, gerçek sahibinin bilgisi dışında düzenli olarak Internet üzerinden bir başkasına veri transferi yapan küçük boyutlu bir program olarak tanımlanabilir. Kötü niyetli kişiler, bilinen Keylogger programlarından birini kullanarak ya da kendileri küçük bir Keylogger oluşturarak bu programcıkları çeşitli şekillerde uzak bilgisayarlara gönderirler. Keylogger, uzak bilgisayara kendi kurulumunu gerçekleştirdikten sonra genellikle kendini hiç belli etmeden çalışmaya başlar ve kaydettiği verileri programlandığı zaman aralıklarında Hacker'a iletir. Genellikle tüm klavye hareketlerini ara hafızasına alır ve transfer eder.[24]

1.3.6 Keylogger Türü Yazılımlar Sisteme Nasıl Giriyor?

1) Kötü niyetli kişiler tarafından yazılan ve işletim sistemlerinin açıklarından yararlanılarak hedef bilgisayarın kısmen veya tamamen yönetici haklarını saldırgana teslim eden "Truva Atı (Trojan Horses)" adlı yazılımlar aracılığıyla Keylogger yazılımları sisteme yüklenirler.

2) Keylogger yazılımı bilgisayara kullanıcı tarafından yüklenebilir. Örneğin; güvenilmeyen bir bilgisayarda bilgisayar sahibi tarafından sisteme başkaları tarafından giriş yapılması halinde (login-oturum açılması) ne gibi işlemler yapıldığı bilgisayar sahibi tarafından bilinmek istenebilir. Bu durumda sisteme yüklenecek bir Keylogger yazılımı ile bilgisayarda başka kullanıcıların yaptıkları bütün işlemler kaydedilmiş olur. Eğer bilgisayar pek çok kişiye açık bir ağda ise bilgisayarda yapılan bütün işlemler

24- http://www.isbank.com.tr/interaktif/i-interaktif-guvenyontem.html, 25.10.2006

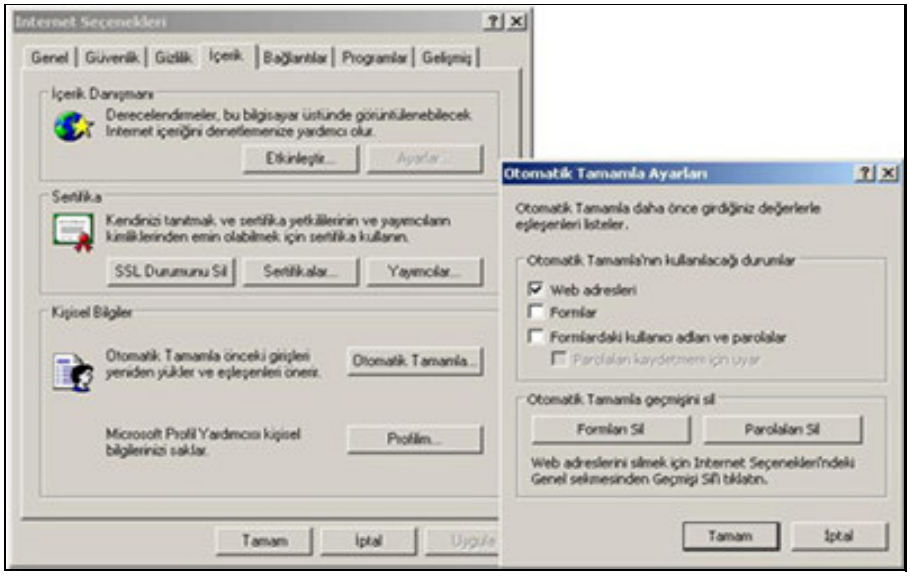
Keylogger yükleyen kişi tarafından öğrenilebilir.

Ayrıca işletim sistemlerinde tespit edilen açıklarla sisteme rahatlıkla uzaktan müdahale edilebilmekte ve bu müdahalelerin başında sisteme dosya aktarma, aktarılan dosyayı çalıştırma gibi işlemlerle sonrasında kullanıcılar takip edilebilmektedir. Bu tür açıklar, yamalarla kapanmış olmakla birlikte sistemlerini güncellemeyen kullanıcılar halen büyük bir tehlike altındadır.

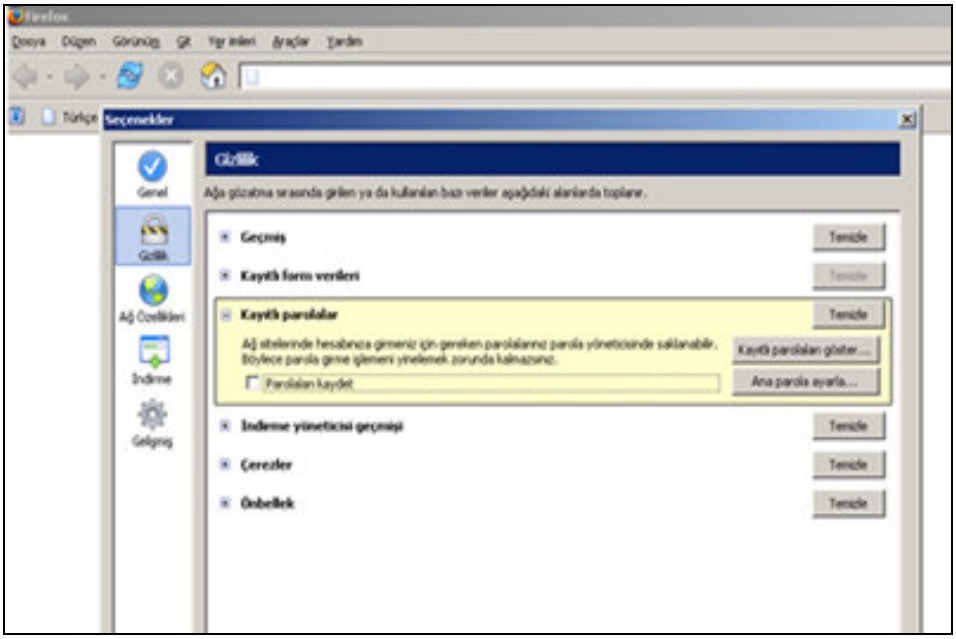
Keylogger ve benzeri programlardan etkilenmemek için:

- Mutlaka işletim sisteminin güncelleştirmelerinin yapılması,
- Bir güncel ve aktif anti virüs programının bilgisayarda bulundurulması,
- Bankacılık ve önemli işlemlerin güvenli olmayan bilgisayarlardan yapılmaması,
- Kullanılan bilgisayarın "web browser-Internet tarayıcısı)" nın otomatik tanımlama özelliğindeki "Formlarda kullanıcı adları ve parolalar" ile ilgili kısmının işaretsiz olmasına dikkat edilmesi gerekmektedir.

Yukarıda bahsettiğimiz " Formlarda kullanıcı adları ve parolalar " bölümüne şu şekilde giriş yapılmalıdır:



Şekil 5



Şekil 6

Screen Logger da; Keylogger ile aynı temel mantığa dayanır. Ancak Screenlogger programlar ile taşınabilen data yalnız klavyenizde yaptığınız tüm vuruşlarla sınırlı olmayıp ekran görüntülerinizi de içerir. Fare ile ekranda bir noktaya tıklamanız ile beraber aynı anda Screenlogger, adeta ekranın tamamının ya da küçük bir bölümünün (genellikle fare merkezli olarak küçük bir dörtgenin) o anki resmini çekerek bunları Internet ortamında sabit bir adrese iletir.[25]

1.5 Casus Yazılımlar ve Etkileri:

Casus yazılımlar bir bilgisayara kurulduktan ve bilgisayarınıza girdikten sonra bilgisayarınızda farklı etkiler bırakarak yada bilgisayarınız içerisinde deyim yerindeyse casusluk yaparak rahatsız eden yazılımlar olarak ifade edilir.

25- http://www.isbank.com.tr/interaktif/i-interaktif-guvenyontem.html, 25.10.2006

Casus yazılımların belli başlı amaçları; eriştiği yada kurulduğu bilgisayarlardaki verileri, gezilen siteleri, bilgisayar içeriğindeki bilgilerin işe yarayan kısımlarını belli bir hedefe (doğrudan merkeze) göndermesine yada bilgisayardan istenmeyen reklamların çıkmasına, Internet'ten reklam indirmesine yol açmaktadır.

Casus yazılımların bu şekilde çalışmasının başlıca sebepleri arasında; bu tür yazılımların milyonlarca bilgisayarda olması ve herhangi bir reklamın yukarıda bahsettiğimiz şekilde yayınlanması demek, milyon dolarlarla hesap edilebilecek bir getiri demektir. Yani bu sayede büyük kitlelere ulaşılmakta ve casus yazılımlar esas amaçlarına ulaşmaktadır.

Bu yazılımlar siz farkınızda olmadan çok kolay şekilde bulaşmaktadır. Yüklediğiniz oyunlarda, download (yükleme) programlarında, yardımcı araçlarda ve daha birçok sizin bilgisayarınıza aktarılabilecek yollarla bulaşabilmektedir. Yapmakta olduğunuz işlemler sırasında bir programın vb. casus yazılımı olup olmadığını "Casus Yazılımlar Listesi " (Genel olarak Gator, Kazaa, Imesh, DC++, Alexa, Google Toolbar, Tüm Toolbarlar [All Tollbars], Cute FTP, Getright, Flashget) oluşturulmuş kaynaklardan bakarak anlayabilirsiniz.

Casus yazılımların kişiye ve bilgisayarına yönelik zararların başında; kişisel bilgilerinizi çalmak diyebiliriz. Bu tür programlar Internet'i yavaşlatırken, dışarı veri gönderip bilgisayarınıza reklam yükler. Bilgisayarınızda açıklar oluşturur ve bilgisayarı yavaşlatır. Bazıları "Dialer-Arayan" dediğimiz programlar ile yurtdışı Internet bağlantısı yaparak yüksek miktarda telefon faturası ödemenize sebep olur. Dialer dediğimiz programlar genellikle pornografik sitelerden bilgisayara bulaşır. Bu tür site ve programlardan uzak durulması hem sizin hem de bilgisayarınız açısından en iyisi olacaktır.

Casus yazılımlar virüs değildir, dolayısıyla anti-virüs programları işe yaramaz. Bu tür programları bilgisayarınızdan silmek için "Casus Yazılım Temizleme Programları" kullanılmalıdır. Gerekli görülmediği sürece Internet onayı gerektiren sitelerde "Evet" e tıklanmaması, bilinmeyen programların yüklenmemesi, Firewall (Koruma Duvarı) kullanılması, anti-casus programlarının kullanılması ve devamlı güncelleştirilmesi gerekir.

e-mail güvenliğini zora sokan birden çok yol vardır. Bu yolla dolaşan ve bulaşan virüsler, Spam ve Spammer'lar (gereksiz bilgi gönderen ve zaman kaybına neden olan mailler), arşivlenemeyen e-maillerin kaybolması ve ekli dosyalar (sistem yavaşlamasına ve birikmeye neden olur), e-mail kullanarak bilgilerin çalınması Sniffer'ler (e-mailleri üçüncü şahsa gönderen ya da bildiren yasadışı yazılımlar) gibi.

"Spam" ilk olarak bir mesajı bir sohbet odasında arka arkaya göndermek olarak tanımlanmıştır. Elektronik posta adreslerini toplayarak bunlardan bir veri tabanı oluşturan ve bu veri tabanlarını satan kişilere **"Spammer"** adı verilmektedir.[26]

Bilgisayarla iletişim yollarını kullananların neredeyse tamamı haftada en az bir kere Spam almaktadır. Spammmer'ların yarattığı dosyalama, yersizlik, zaman kaybı dışındaki en ciddi sakıncası güvenliktir. Bunlar sizin serverınızı e-mail göndermek için kullandıkları gibi, bilgilerin dışarı taşınmasına da neden olabilirler .Amatörcedir ama işlevseldir. Kurumların güvenliğini tam olarak sağlayamadığı e-mailler, istihbarat niyetli yazılımların basit avları olacaktır. Bu yazılımlar genelde otomatik olarak ilginç bilgiler taşıyan postaları izlemektedir. Ama yazılım zaten belli bir adresi izlemeye programlandıysa, hedef için durum bir anda sürek avına dönüşecektir. e-mail gönderen alan kişinin hiçbir şeyden haberi yoktur ve Sniffer'lar bilgisayarlara gelen giden tüm yolların üzerinde konumlandırılmıştır.[27]

Kanunen bu tür yazılımlar suç sayılmıyor, fakat bu da tartışmaya açık bir konu olarak süregelmektedir. Bu tür yazılımların lisans anlaşmasında, yazılımların kullanılmasını siz kabul etmiş sayıp yüklüyorsunuz, bu da bu tür yazılımları kanuni olarak gösteriyor.

1.6 Virüsler, Worms (Solucanlar), Trojan Horses (Truva Atları), Droppers (Damlalıklar) ve Zombiler:

Virüs; Kendi kodlarını başka programlara veya program niteliği olan dosyalara bulaştırarak kendilerini kopyalayabilen, bulaştıkları bilgisayarda genelde hızlı bir

---

26- ÖZDİLEK, Ali Osman, **İnternet ve Hukuk**, Papatya Yayıncılık, İstanbul, Eylül 2002, s.153

27- ERSANEL, Nedret, **Siber İstihbarat**, Hayykitap, İstanbul, Ekim 2005, s.47

şekilde yayılan, belli bir amaca yönelik olarak yazılmış (zarar vermek veya eğlence) olan bilgisayar programlarıdır. Virüs; programa kendini iliştirerek hatta onunla yer değiştirerek özgün programla birleşir ve bazen bu kopyalama virüs programının değiştirilmiş bir sürümü şeklinde olur. Bir makrodan (ön ek), bir disketin boot (ön yükleme) kısmından veya yüklenen bir programdan sisteme bulaşabilir.

Bilgisayarlara ve bilgilere zarar veren programların hepsi virüs değildir. Bunlar programın karakteristik özelliğine göre farklılıklara ayrılırlar. Virüslerin ortak yani ise; bilgisayar bilgilerine zarar vermesi ve etkilemeleridir. Bunlar Worms (Solucanlar), Trojan Horses (Truva Atları) ve Droppers (Damlalıklar) olarak tasnif edilebilir.[28]

Virüsler ve Worms (Solucanlar) kötü amaçlı olarak yazılmış kodlardır. Virüsler, bilgisayarda çalıştırıldığında herhangi bir şekilde zarar veren küçük programcıklardır ve bu programcıklar sanılanın aksine bilgisayarda çok yer kaplamazlar.

Worms (Solucanlar) ise; virüsler gibi kodlardan üretilmiştir, fakat virüslerden farkı virüs ile etkileşim halinde olunca aktif olur. Ancak Worms (Solucanlar) bilgisayara girdiği andan itibaren çalışmaya başlar ve kendisini farklı bilgisayarlar aramaya devam ederler. Bir diğer farkı da bilgisayar Worms (Solucanlar), bilgisayarınızın hafızasında boş yer kalmayana kadar kendini kopyalıyan programlardır. Bilgisayar kurtları bilgisayarın hafızasını kaplar ve böylece bilgisayarın yavaşlamasını ve hatta çökmesini amaçlar. Virüsler; disket, CD, Internet, e-posta gibi yolları kullanarak bilgisayara bulaşırlar. Bilgisayar Worms (Solucanlar) ilk önce RAM (Random Access Memory-Rasgele Erişimli Bellek) kendine bir yer bulur ve kendini oraya kopyalar daha sonra ise yeni kopyayı çalıştırır. Bu programın çalıştırılmasıyla bir döngü oluşur ve devamlı olarak ilk başlatılan programın kopyası üretilmekte sonra da bu kopyalar çalıştırılmaktadır. Bu kopyalama hafızada yer kalmayıncaya kadar devam eder ve hafıza dolduktan sonra bilgisayar yavaş çalışmaya başlayacak veya çökecektir.

Virüsleri benzeri kavramlardan ayırt etmek gerekir. Virüslere yakın sayılabilecek Worms (Solucanlar), Truva atları ile mantık bombaları ve saatli bombalar birbirleri ile karıştırılmaktadır. Virüsleri bunlardan ayıran en büyük özellik virüslerin

---

28- http://www.egm.gov.tr, **Bilişim Suçları Genel Bilgiler**, 30.05.2007

kendi kendilerine çoğalıp diğer programlara bulaşabilmeleridir. Halbuki Truva atları, bombalar veya solucanlar diğer programlara bulaşmazlar.

Truva Atları (Trojan Horses); Truva Atları, görünüşte zararsız bir programın içine gizlenmiş bir program (backdoor) veya kendi başına uzaktan kontrole veya programın özelliklerinin çalışmasına imkan tanıyacak özel bir sunucu kodu olan programlardır.

Bugün Internet literatüründe Trojan programı denildiğinde hemen "netbus , boo, subseven" ve benzeri belli başlı programlar akla gelir.[29]

Trojan olarak bilinen ve dilimize "Truva Atı" olarak giren virüsler, bilgisayarınızı uzaktan kumanda etme amacına hizmet ederler. Genel olarak iki ayrı modülden oluştukları söylenebilir. İlk modül, kötü niyetli kullanıcıların bilgisayarınıza uzaktan erişimine ve kontrol sağlamasına izin verirken ikinci modül, Hacker ile sizin bilgisayarınız arasında bağlantı sağlayacak bir "açık kapı" yaratır.

Trojan tarzı programlar, siz izin vermedikçe bilgisayarınıza yüklenmez. Internet ortamında gelen ".ini" ya da ".exe" uzantılı dosyalar, bu küçük Trojan yazılımlarını barındırıyor olabilir. Bilgisayarınıza özellikle ücretsiz yazılımları kurmadan önce güncel bir tarayıcı programla kontrol etmeyi ihmal etmemelisiniz. Anti virüs yazılımınızı sürekli olarak resmi sitesinden güncellemeli ve bir Firewall (Koruma Duvarı) programı ile bilgisayarınızı koruma altına almalısınız.[30]

Damlalıklar (Droppers); antivirüs saptamasını önlemek üzere tasarımlanmış programlardır. Damlalıkların tipik işlevleri virüsleri taşımak ve kurmaktır. Sistemde gerçekleşen ve kendi kendilerini başlatabilecekleri özel bir olay bekler ve taşıdıkları virüsü sisteme bulaştırırlar.

Zombiler (Ddos saldırıları)'nın; hedefi sistemi işlemez hale getirmektir. Bazı "Ddos atakları" hedef sistemi iflas ettirmek için tasarlanmışken diğer bazıları da hedef sistemi meşgul edip normal işleyişini yavaşlatmak için tasarlanmıştır. "Ddos atağı" düzenleyen kişi kimliğini ele vermemek için atakları "zombi" adı verilen bilgisayarlar

---

29- http://www.egm.gov.tr, 30.05.2007

30- http://www.isbank.com.tr/interaktif/i-interaktif-guvenyontem.html, 25.09.2006

üzerinden yapar. Bu kişiler IP Spoofing (IP-Internet Protocol-gizleme) yaparak kimliklerini saklayabilmektedir. "Ip Spoofing" aslında bir güvenlik önlemi olarak yaratılmıştır. Fakat bunu suç aleti olarak ele alınması amaca göre kullanılması şeklinde olmaktadır.[31]

1.7 Hacker, Cracker, Phreaker Nedir? Nasıl Çalışırlar?

"Hack"; işletim sistemlerinin, daha genel bir ifadeyle sistemlerin doğasındaki açık kapıların kullanılarak, bu açık kapılardan sisteme sızılmasıdır. Yani normalde erişim izni olmayan sistemlere, o sistemlerin güvenlik duvarının aşılarak girilmesidir. Bu eylemleri yapan kişilere de **"Hacker"** denir.[32]

Hacker'lar; her türlü işletim sisteminin yapısı ve derinlikleriyle ilgilenen kişilerdir. Hacker'lar genellikle çok iyi programcılardır; işletim sistemleriyle ve programlama dilleriyle ilgili olarak çok üst düzeyde bilgiye sahiptirler. Sistemlerde bulunan açıkları ve sebeplerini iyi bilirler ve hepsinden önemlisi Hacker'lar her zaman için daha fazla şey öğrenmek için uğraşırlar, öğrendiklerini diğerleriyle paylaşırlar. Hiçbir zaman kasıtlı olarak zarar verme eğiliminde değildirler.

Hacker'lar; işletim sistemi ve programlama dillerini iyi bilerek başka programlardaki hataları test etmek için program yazarlar, mesela uzak bilgisayarlardaki açıkları otomatik test edebilen programlar gibi.

"Crack"; kendisine yahut bir başkasına çıkar sağlamak için, Web sayfalarının veya sistemlerin güvenlik duvarlarının, şifrelerinin kırılarak Web sayfasına veya sistemlere zarar verilmesine **"Crack"** denir. Bu eylemleri gerçekleştirenlere ise **"Cracker"** denir.[33]

Kötü niyetli kişilerdir ve sistemlere girerek bilgi çalarlar, sisteme zarar verebilirler. Hedeflerine sızmayı başaran Cracker'lar önemli bilgileri silebilir, sistemin işleyişini durdurabilirler. Cracker'lar program yazmazlar. Bir kişi hem Hacker hem de

---

31- EKER, a.g.w.s, 13.06.2006
32- ÖZDİLEK, a.g.e, s.166
33- a.g.e,

Cracker olabilir. Hacker ve Cracker kavramları zamanla içice geçmiştir. Aralarındaki temel fark şudur; Hacker'lar bir sistemin güvenlik duvarını aşarak sisteme sızmak suretiyle her türlü bilgiye ulaşırlar. Fakat Cracker'lar güvenlik duvarlarını kırarak sistemlere girerler ve verileri yok etme, değiştirme, şifreleri kırma ve bunları dağıtma gibi eylemlerle zarar verirler. Yani temel fark Cracker'ların zarar vermeleridir. Hukuki ve cezai sorumluluğun belirlenmesinde eylemin hangisine girdiğinin belirlenmesi önem taşır. [34]

Hacker, kelimesinin ortaya çıkışı 1960'larda çok kaliteli programcıların FORTRAN ve diğer eski dillerde program yazdığı MIT'te başladı. Çok zeki ve entelektüel kişiler olan bu programcılar günümüzde gerçek Hacker olarak nitelendirdiğimiz Hacker'ların ataları, öncüleri olarak bilinirler. Gerçek Hacker'lar devamlı yeni şeyler öğrenme yolunda önüne geçilmez bir isteğe sahiptirler ve korkunç bir şekilde ayrıntıya önem verirler.

Günümüzde Hacker ve Cracker'lar ağ ortamında savaşlarını sürdürmektedirler. Cracker'lar daha çok tanınmak için ve bazen gelir elde etmek için çalışmaya devam etmektedirler. Günümüzde artık neredeyse her gün onlarca site Crack edilmektedir. Hacker'lar ise Crack'lare karşı güvenlik için yeni teknikler aramaktadırlar. Firmaların güvenlik sektörüne çok miktarda yatırım yapması güvenlik araçlarının çok fazla gelişmesine ve kalitesinin artmasına neden olmaktadır. Bu da Cracker'ların işini zorlaştırmaktadır. Güvenlik araçlarının karmaşıklaşması ve daha kaliteli olması aslında Cracker'larin yok olmasına değil onlarında artık daha karmaşık teknikler kullanmasına neden olmaktadır. Çünkü bir sistem ne kadar çok karmaşık hale gelirse içerisinde o kadar çok hata ve açık olacak demektir. İşte Cracker'lar bu açıkları bulmak için uğraşıyor olacaklardır.

1970'lerde "Captain Crunch" bedava uzak telefon görüşmesi yapabilmek için bir yol bulunca daha sonra **"Phreakers"** olarak anılacak olan Hacker'lar çıktı. Preaking olarak adlandırılan bu işlem telefon şirketlerinin güvenlik sistemlerini kırmak olarak bilinir. Ancak gerçekte Preaking daha çok telefon sisteminin çalışmasının öğrenilmesi ve işletilmesi anlamına gelmektedir. Preaking için değişik yöntemler kullanılmaktadır.

34- ÖZDİLEK, a.g.e, s.166

İlk olarak telefon kulübelerinde jeton kullanmadan telefon görüşmesi yapmayı sağlayan cihazlar kullanıldı. Bu cihazlarla ilgili ayrıntılı bilgileri Internet'te yüzlerce sayfada bulabilirsiniz. Ancak telefon teknolojilerindeki gelişmeler eskiden kullanılan Preaking tekniklerinin günümüzde işlemez hale gelmesine neden oldu. Bilgisayarların gelişmesiyle Preaking ve bilgisayar birleşti ve daha güçlü araçlar ortaya çıkmaya başladı. Bunların içlerinde en önemli olan BlueBeep Preaking/Hacking aracı olarak karşımıza çıktı. Özellikle eski tip telefon hatlarında bu araç çok fazla yeteneklere sahipti. "Pascal ve Assemble" dilinde yazılan bu program telefon santrallerinin "Scan-Tarama" edilmesi, "Dial Tone" üretilmesi gibi bir sürü işleve sahipti. Preaking'lerin ilk defa Interne'te ne zaman ve nasıl girdikleri tam olarak bilinmiyor ancak Preaking'ten sonra 1980'lerde Cracking işine merak salan programcılarla, Cracker'lar tahmin edebileceğiniz her türlü sisteme girmeye başladılar ve hala giriyorlar.

Dünya üzerindeki en tanınmış Cracker olarak Kevin MITNICK diye biliriz. Kevin MITNICK'te bu alana Preaking olarak başladı. MITNICK o zamanlar çok güvenli sayılabilecek hemen hemen her türlü sisteme girmeyi başarmıştır. Bunlar arasında finans firmaları, yazılım şirketleri, askeri siteler ve teknoloji siteleri yer almaktadır. MITNICK daha genç yaşlarda "North American Aerospace Defense Command" sistemini Cracklemiştir. 1990'larda Tsutomu SHIMOMURA tarafından takip edilen Kevin MITNICK tutuklandı ve her türlü elektronik cihazı, Internet'i, hatta bu konuda konuşması bile yasaklandı. Daha sonra tahliye edilen Kevin MITNICK bir firma için güvenlik konusunda makale yazmak için mahkemeye başvurdu ve şuan köşe yazarlığı yapmaktadır.[35]

1.8.Bilişim Yoluyla İşlenen Kartlı Ödeme Sistemleri Sahteciliği ve Dolandırıcılığı:

Suçlular bankaların kartlı ödeme sistemlerine yönelik suçları işlerken bir çok yöntem kullanmakta ve bu suçun icrası sırasında da bilgisayar ile Internet

35- http://forum.flash.gen.tr/archive/index.php?t-559.html, **Bilgisayar Suçları,** 18.03.2006

teknolojilerinden yararlanmaktadırlar. Öncelikle suçluların bu suçu işleyebilmesi için bir şekilde bankalara ait kart bilgilerini temin etmeleri daha sonra bunları kullanabilmek için elverişli cihazlarının ve imkanlarının olması gerekmektedir. Bankalara ait kart bilgilerinin temini bir çok farklı şekilde olabileceği gibi asıl olarak iki ana gruba ayrılmaktadır. Bunlar alt başlıklarıyla birlikte aşağıdaki şekilde incelenebilir:

1- Kart Bilgilerinin Kopyalanması;

a- Kopya kartlar ile alış veriş,

b- Nakit para çekimi,

c- Havale yada EFT.

2- Online Alış Veriş

a- Mal alımı,

b- Hizmet alımı.

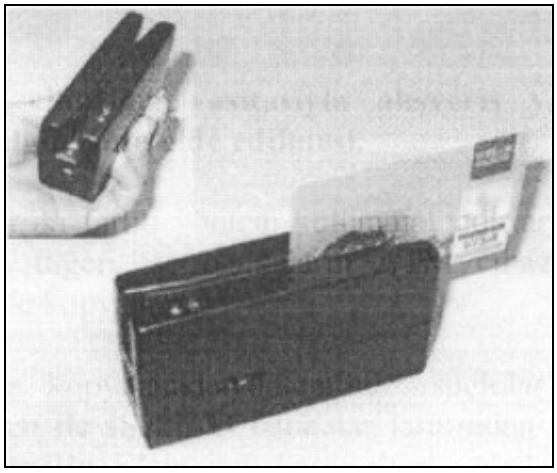
Bu suçları işlemekte kullanılan yöntemleri aşağıdaki şekillerde görmekteyiz:

1- Kart bilgilerinin temin edilme yöntemleri;

a- Manyetik kopyalama cihazları vasıtasıyla alış veriş yada ATM makinelerinin kullanımı sırasında kart bilgilerinin elde edilmesi:

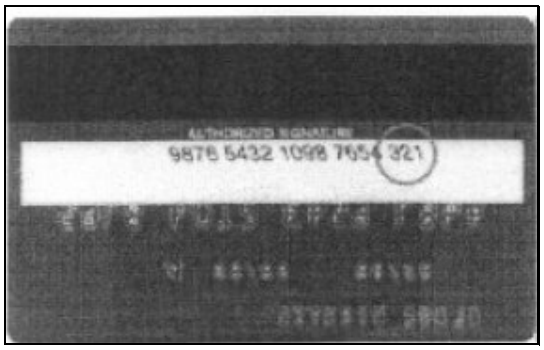
Suçlular bu durumda iki farklı yöntem kullanmaktadırlar. Birincisi direkt olarak alış veriş esnasında kopyalama diğeri ise bankaların ATM cihazlarının kart giriş yerlerine yerleştirilen minik cihazlar ile kopyalama.

Alış veriş esnasında kopyalama yönteminde; suçlular ellerindeki manyetik kart kopyalama cihazları vasıtası ile **(Şekil 7)** bankalar tarafından kullanıcısına verilmiş olan kredi kartlarını kopyalamaktadırlar. Bu işlem için kart sahiplerinin alış veriş yaptıkları yerlerde kredi kartları pos cihazlarından geçirilmeden önce veya sonra kopyalama cihazlarından geçirilmekte ve kartın manyetik şeridinde bulunan (TRACK 1, 2, 3) bilgileri bu cihazlar vasıtası ile kaydedilmektedir.



Şekil 7

Banka ve kredi kartlarının arka yüzünde bulunan manyetik şeritler, TRACK adı verilen alanlarda ISO 7811/1~6 standartlarında TEXT ve SAYISAL bilgi içermektedir. Genelde bu bilgiler TRACK 1, 2, 3 şeklinde üç ayrı alana bölünmüştür.



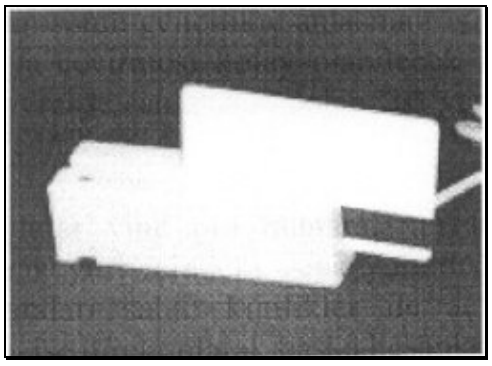
Şekil 8

Banka ve kredi kartlarının manyetik şeritlerinde bulunan TRACK bilgileri bankaların belirlemiş oldukları kendi standartlarına göre farklı şekillerde bilgi ihtiva edebilir. Örneğin bir banka kartın son kullanma tarihini TRACK denilen alanlarda saklayabileceği gibi bir başka banka bu alanı kart numarasını okuduktan sonra Online olarak veri tabanlarından öğrenebilir. Manyetik şeritlerde bulunan ve TRACK adı verilen bilgiler genellikle aşağıda bulunan şekildeki gibidir.

Şekil 9

Suçlular alış veriş esnasında kopyalama yönteminde; bazı durumlarda ise pos cihazlarında arıza var şeklinde müşteriler kandırılıp kartlarının PIN kodlarını elle girmeleri istenmekte bu sayede de kartların PIN kodlarını elde etmektedirler.

Suçlular tarafından kopyalanması yapılıp PIN (Personel Identification Number) kodu elde edilemeyen bazı kartlar boş PVC manyetik kartlara ENCODER (Kodlayıcı) adı verilen cihazlar **(Şekil 10)** ile kopyalanıp kartın ikizi çıkarıldıktan sonra genellikle anlaşmalı iş yerlerinden cep telefonu, altın ve ziynet eşyası gibi nakit paraya çevirmesi kolay olabilecek parçalar satın alınmakta, bunlar daha sonra gerek satılarak gerekse anlaşmalı olan iş yerlerinden alınmış gibi gösterilerek nakit paraya çevrilmektedir.



Şekil 10

Suçlular yine PIN numaralarını tespit ettikleri kart bilgilerini boş PVC kartlara kopyalarak yurt içindeki veya yurt dışındaki ATM cihazlarından nakit para çekmekte ve

çekilen paraları sahte kimlikler ile açtıkları banka hesaplarına yatırmaktadırlar. Bazı durumlarda ise direkt olarak başka hesaplara havale yapmaktadırlar.

ATM makinelerinin kart giriş yerlerine yerleştirilen kopyalama cihazlarında ise suçlular genellikle uzak bir yerlerde gözetlemede bulunmakta, daha sonra kopyaladıkları kartları manyetik kart yazma cihazıyla boş kartlara yazıp kartın ikizini çıkartabilmektedirler. Bazı durumlarda ise kopyalanan kartın şifresini öğrenebilmak için ATM cihazlarının üst köşelerine micro kameralar yerleştirmek suretiyle ATM cihazının tuş takımını izleyerek şifreleride alabilmektedirler.

ATM makinelerine yönelik yapılan diğer bir yöntemde şu şekildedir; suçlular ATM makinelerinin kart girişlerine bir aparat yerleştirerek kartların makinede kalmasını sağlamaktadırlar. Kartını makineye kaptıran şahsın yanına gelen suçlular yardım etmek bahanesiyle şahısa yaklaşmakta ve bankaya telefon etmesi gerektiği söylenerek şahsı yönlendirmekteler. Daha önce ATM makinelerinin yanına bir telefon kutusu yerleştiren suçlular ahizenin iç kısmına da kendilerine ait cep telefonunu koymaktadırlar. Zor durumda olan şahısa hemen telefonu uzatarak karşıdaki banka görevlisiyle irtibat kurmasını telkin ederler. Ancak telefonun karşısında zanlıların arkadaşı vardır. Kartı ATM makinesinde sıkışan şahıs karşı tarafın sorularına cevap verirken şifre ve kişisel bilgilerini aktırdığının farkında değildir. ATM'den uzaklaştıktan sonra makinede sıkışan kart suçlular tarafından alınarak kullanılmaktadır.

b-Alış veriş sırasında kart bilgilerinin izlenmesi:

Genellikle profesyonel olmayan suçlular tarafından uygulanan bu yöntemde suçlular kullanıcısına farkettirmeden alış veriş esnasında veya başka zamanlarda başkasına ait kredi kartının ön ve arka yüzlerindeki yazılı numaraları (kart numarası, son kullanma tarihi, CVV2-Card Verification Value-Kart Doğrulama Değeri) not ederek yada akılda tutarak almaktadır. Bu yöntemle genellikle Internet üzerinden Online alış veriş gerçekleştirilmektedir.

c-Internet üzerinde bulunan Online alış veriş sitelerinin kayıtları elde edilerek buradaki kart sahiplerinin SPAM mail yoluyla kandırılması suretiyle:

Internet üzerinde bulunan bir çok Online alış veriş sitesi kredi kartı ile Online para transferi yapmak suretiyle müşterilerine hizmet vermektedir. Bu hizmetleri sırasında ister istemez müşterilerine ait bazı bilgileride veri tabanlarında tutmakta,

bunları Online olarak kaydetmektedirler. Bu bilgiler arasında müşterinin satın aldığı ürün, teslimat adresi, müşterinin telefonu, e-posta adresi, ürünü aldığı tarih ve bazı sitelerin veri tabanlarında ise müşterinin kredi kartı numarası ile kartın son kullanma tarihi tutulmaktadır.

Aşağıda örnek olarak Internet üzerindeki bir Online alış veriş sitesinin veri tabanından bir kısmı yer almaktadır.


Bill-Address1 = 521 Blackhawk Club Drive
Bill-City = Danville
Bill-Country = US United States
Bill-Email = a94506@yahoo.com
Bill-Firstname = Michael
Bill-Lastname = Deffina
Bill-Phone = 925-736-8433
Bill-State = CA
Bill-Zip = 94506
Card-Expiry = 3/2006
Card-Number = 4337369000000914
CardAuth-Amount = 9.94
Date = Mon Dec 29 04:55:46 2003 GMT
Item-Code-1 = HF-ADNOK7210
Item-Count = 1
Item-Description-1 = Hands-free Audio Adaptor 7250i
Item-Id-1 = adaptor7210
Item-Quantity-1 = 1
Item-Taxable-1 = YES

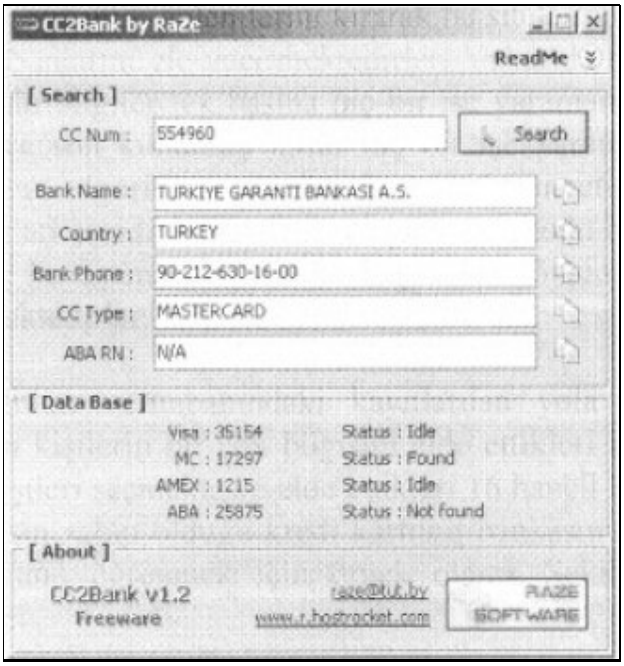
Şekil 11

Buna bilişim dilinde Order Log (alış veriş kaydı) denmektedir.

Burada da görüldüğü gibi alış veriş yapan kişiye ait bir çok Online alış veriş sitesinin veri tabanında yer almaktadır. İşte bu aşamada uzman bilgisayar korsanları devreye girmekte ve suçun işlenmesi için kredi kartı bilgilerini temin etmek üzere Online alış veriş sitelerinin güvenlik önlemlerini kırarak bu sitelerin Order Log'larının (alış veriş kayıtları) tutulduğu veri tabanlarını ele geçirmektedirler. Yukarıda da belirtildiği gibi aslında bu veri tabanlarında tutulan bilgiler tek başına hiçbir işe yaramamaktadır. Özellikle sadece kredi kartının numarası ve son kullanma tarihi hiçbir işe yaramamaktadır. Gerek Online alış veriş gerekse bankaların algoritmasına göre boş PVC manyetik kartlarına yazmak için gerekli olan kredi kartının arkasında bulunan

CVV2 güvenlik kodu bu veri tabanı kayıtlarında bulunmadığı için suçlular bu aşamadan itibaren başka bir yöntem ile gerekli bilgileri kart sahibinden almaya çalışmaktadırlar.

Bu aşamada suçlular, veri tabanındaki kayıtlardan yola çıkarak Online alış veriş sitesinden alış veriş yapan kişilerin bir çok bilgisini elde ettikleri için (özellikle şahsın e-mail adresi), hedef olarak bu kişileri seçmekte ve elde ettikleri 16 haneli kredi kartı numarasının ilk 6 hanesinden (BIN ID) şahsın sahip olduğu kredi kartının bankasını öğrenmektedirler. Kartın hangi bankaya ait olduğunu öğrenmek için örnek olarak **(Şekil 12)**' deki gibi programlar kullanmaktadırlar.



Şekil 12

Suçlular böyle programlar vasıtasıyla ile hedef şahısların kartlarının ait olduğu bankayı öğrendikten sonra elde ettikleri veri tabanı kayıtlarına göre kart sahibinin mail adresine sanki bankaymış gibi e-posta (Spam mail) atmakta ve yapılan alış verişin teyyidi için güvenlik amacıyla gönderilmiş bir teyyid maili hissi uyandırmaktadırlar. Bu mail ile şahıslardan mail ekindeki forma veya verilen Internet adresindeki siteye girip buradaki forma kart bilgilerini tekrar girmesi ve alış verişi onaylaması istenmektedir. Maili alan kurban kişiler mailde kart bilgilerinin ve yaptıkları alış verişin detayını

gördükleri için şüphelenmemekte ve formu doldurma işlemini gerçekleştirmektedirler. Ancak bu tarz mailler vasıtası ile fazladan şahsın kredi kartının CVV2 güvenlik kodu ve ATM cihazlarında kullanabilecek PIN kodu da istenmektedir. Kurban kişiler formu doldurduktan sonra suçlular için tamamlanmış bilgiler artık hazır demektir. Bu aşamadan sonra suçlular ellerindeki bilgileri bankaların algoritmalarına göre boş PVC kartlara yazarak kullanabilmektedirler. Bu bilgiler ile boş PVC kartlara yazma işlemi gerçekleştirerek para çekilebilmekte, sonradan nakite çevirebilecek alış verişler gerçekleştirebilmekte ve de Online alış veriş yapılabilmektedir.

d-Internet üzerindeki sohbet kanallarından:

Internet'de IRC (Internet Relay Chat) adı verdiğimiz sohbet alanlarında suçlular buluşarak bir önceki başlıkta anlatılan Internet üzerinde bulunan Online alış veriş sitelerinin kayıtları elde edilerek buradaki kart sahiplerinin SPAM mail yoluyla kandırılması suretiyle elde ettikleri kart bilgilerini karşılıklı olarak paylaşmaktadırlar. Burada suçlular genellikle uluslar arası çalışmakta ve örneğin bir ülkede elde edilmiş kart bilgileri diğer ülkede bulunan ortaklarına gönderilerek yarı yarıya usulü karşıklı çıkar sağlamaktadırlar. Burada elde edilen haksız gelir genellikle Western Union şirketi gibi para transfer vasıtası ile karşılıklı gönderilmektedir.

Dikkat edilmesi gereken konu; her bankanın her dünya ülkesinde ödeme yapmamasıdır. Dolayısıyla suçlular ödeme yapılabilecek ülkedeki arkadaşlarına kart bilgilerini göndererek hem gizlemeyi hedeflemekte hem de suçun işlenmesini kolaylaştırmaktadırlar. Dolayısıyla ülkemizden çalınan bir kart bilgisi yurt dışında kullanılabilmektedir.

Kart kopyalamada kullanılan cihazların temini; bu tip manyetik kopyalama cihazları Internet üzerinden Online alış veriş sitelerinden satın alınabilmekte yada suçlular yurt dışında bulunan elemanları vasıtası ile temin etmekte, yanlarında yada kargo ile yurt içine sokulmaktadır. Yurt içinde ve yurt dışında bir çok Online alış veriş sitesi bu cihazları ve boş manyetik kartların satışını yapmaktadır.

Manyetik kartların kullanım alanı sadece kartlı banka sisteminden ibaret olmayıp, kapı güvenlik sistemlerinde, kimlik tanıma sistemlerinde ve daha bir çok alanda kullanılabileceği için ülkemize bu kart okuma cihazların girmesi veya pazarlanması suç teşkil etmemektedir.

2-Online Alış Veriş:

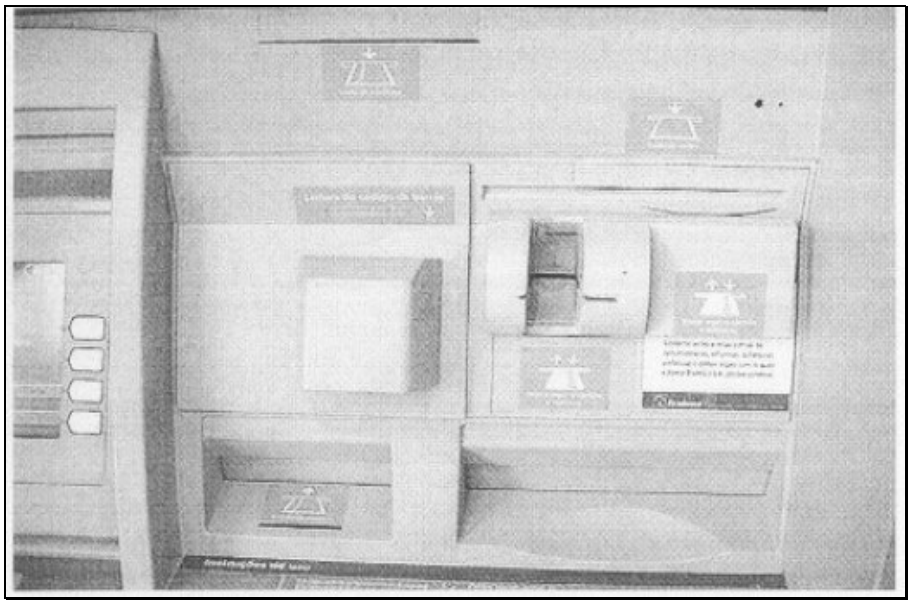
Çeşitli yollarla elde edilen kredi kartı bilgileri ile haksız kazanç sağlayacak Online alış verişlerde mümkün olabilmektedir. Online alış verişlerdeki satışı genellikle ikiye ayırabiliriz:

a-Ürün satışı; ürün satışında Online alış veriş yapan kişiler kredi kart bilgilerini alış veriş sitesinde kullanarak ödeme yaptıktan sonra posta veya kargo aracılığı ile alış veriş sırasında verdikleri adrese satın aldıkları ürünleri sipariş vermekte, genelde ise kargo şubelerinden malları sahte kimlikle teslim almaktadırlar. Burada genellikle ürün teslimi yapıldıktan sonra şahısların hesaplarından tahsilat yapılmaktadır.

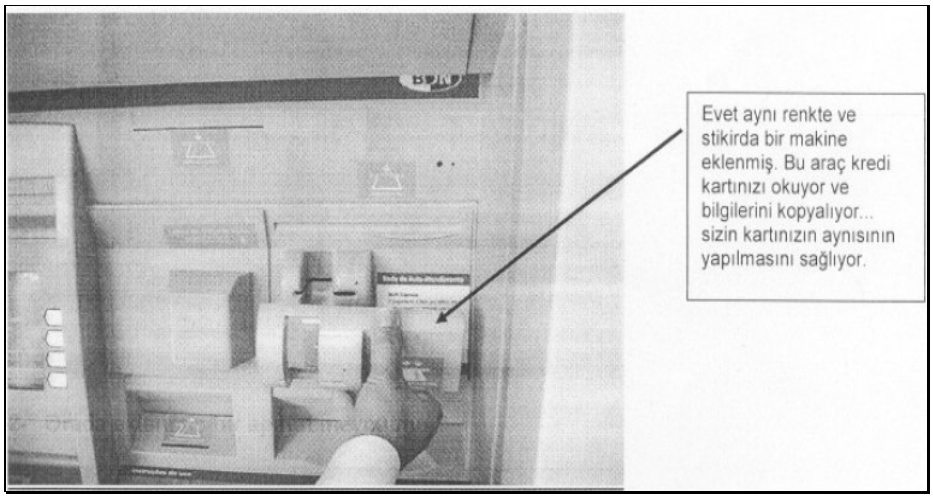
b-Hizmet satışı; Burada elle tutulur bir ürün ortada yoktur. Internet'in verdiği hizmetler arasında ücretli üyeliği bulunan sitelerde bulunmaktadır. Örneğin kredi kartı ile ödeme yaparak bir bilgi topluluğuna, arkadaşlık sitesine üye olunabilir yada program veya elektronik doküman satın alınabilir.

İşte bu aşamada suçlular genellikle takibi zor olan elle tutulur bir ürün olmadığı hizmet satışlarından faydalanmaktadırlar. Bir Internet adresinin tescil edilmesi, site bulundurma hizmetinin alınması gibi hizmetler suçluların en çok tercih ettikleri alış verişlerdir. Bir ürünün teslimatının olduğu alış verişlerde ise suçlular genellikle teslimat sırasında sahte kimlikler kullanmakta ve teslimatın kargo bürosunda gerçekleşebilmesi içinde yanlış adres bilgisini alış veriş sitesine vermektedirler.

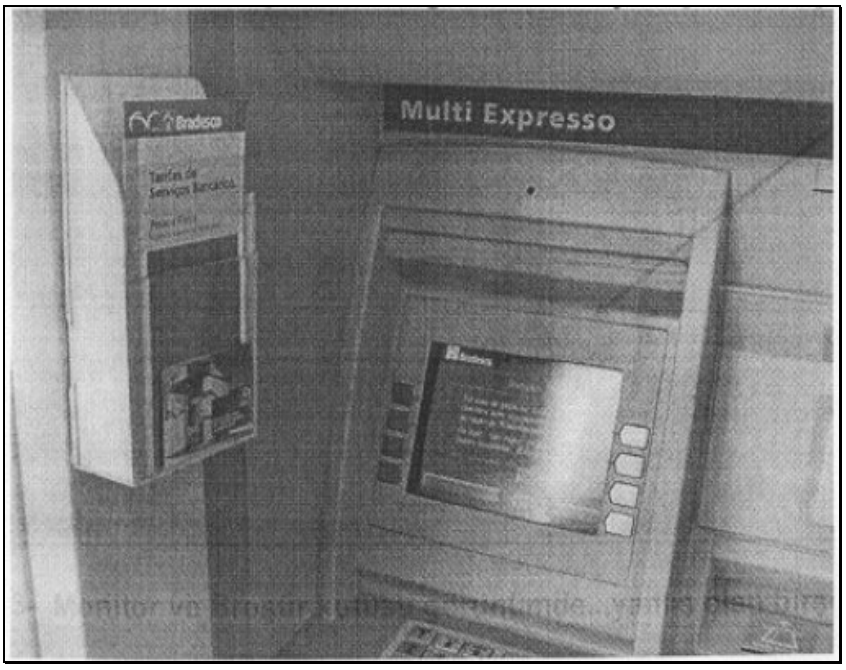
Aşağıda verilen fotoğraflarda bu suçların işlenme yöntemleriyle ilgili örnekler verilmektedir: [36]



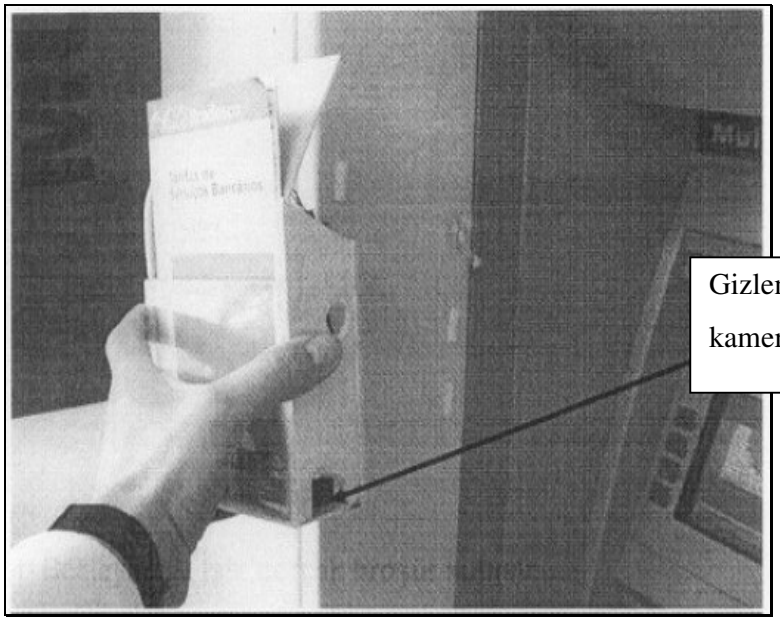
Şekil 13



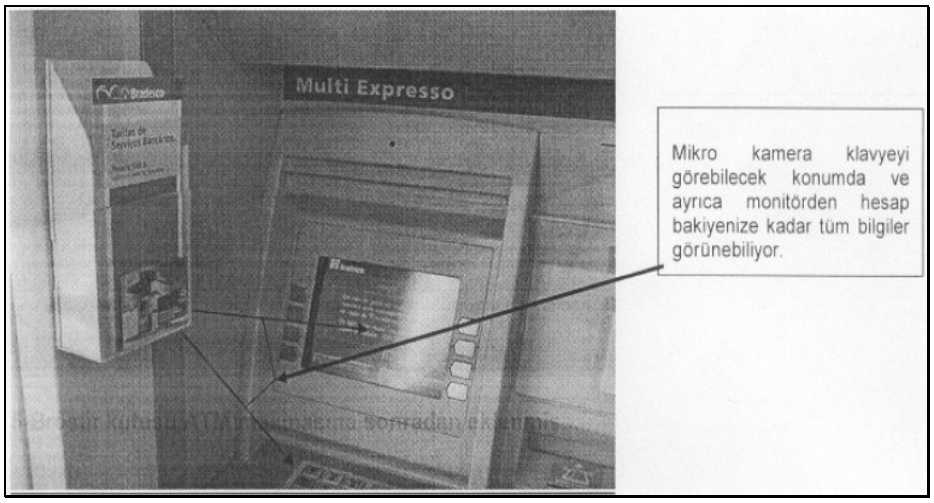
Şekil 14



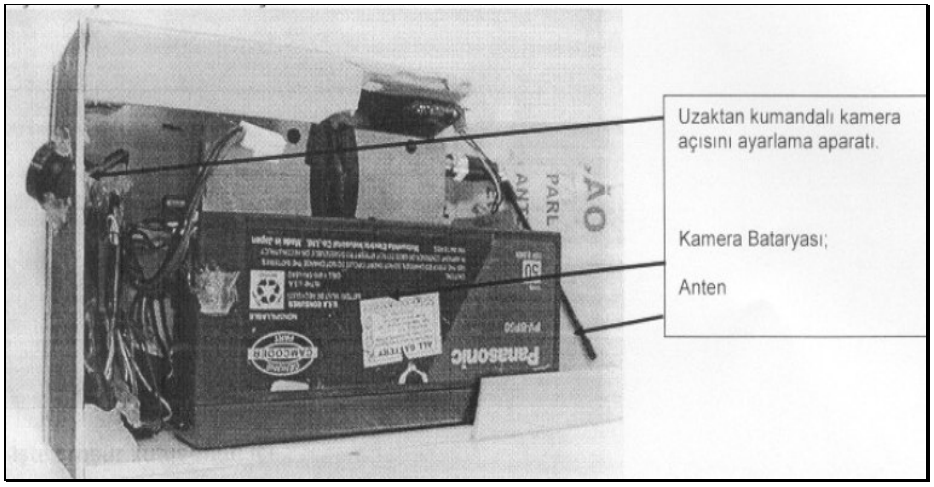
Şekil 15



Şekil 16



Şekil 17



Şekil 18

36- DOKURER, a.g.e

İKİNCİ BÖLÜM

Birinci bölümde bilişim suçlarının tanımına, sınıflandırılmasına, işlenme yöntemlerine, virüs gibi kötü yazılımlara yer verilmiştir. Hukuki açıdan konunun daha iyi anlaşılabilmesi ve mücadele içerisinde ki hareket tarzının belirlenmesi yönünden bu suçların mutlak suretle her yönüyle bilinmesi gerekmektedir. Bu bölümde ise; bilişim suçlarının hukuk sistemimiz içerisindeki yeri, bu suçlara verilecek cezai yaptırımların neler olduğu incelenecektir. Ayrıca bölüm içerisinde çocuk pornografisine, Fikir ve Sanat Eserleri Kanunu ile ilgili konulara, yer yönünden yetkili mahkemelere, delillerin elde edilmesine, yargıtay kararlarına da yer verilmiştir.

BİLİŞİM SUÇLARININ TÜRK HUKUK SİSTEMİNDEKİ YERİ

Bilişim suçları olarak adlandırılan suç tipi hukukumuza ilk defa 765 sayılı Türk Ceza Kanununa "Bilişim Alanında Suçlar" adlı Onbirinci Bap'ın eklenmesiyle 06.06.1991 tarihinde girmiştir. 01 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Türk Ceza Kanunu da eski kanuna oranla daha kapsamlı hükümler getirerek "Bilişim Suçları" hakkında düzenlemeler getirmiştir.

Bilişim suçları, 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Kanunu'nda; Onuncu Bölüm, "Bilişim Alanında Suçlar" başlığı adı altında **243, 244, 245 ve 246.** maddeleri arasında yeniden düzenlenmiştir. Bu maddeleri sırasıyla inceleyecek olursak:

5237 sayılı Yeni Türk Ceza Kanunun **243.** maddesinin başlığı **"Bilişim Sistemine Girme"** başlığını taşımaktadır:

MADDE 243 - Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

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

Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur denilmektedir. ***(Sulh Ceza)***

Bu maddenin gerekçesi de şu şekilde düzenlemiştir:

Bilişim sistemlerine karşı suçların düzenlendiği bölümde yer alan bu maddede bilişim sistemine girme fiili suç olarak tanımlanmıştır.

Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tâbi tutma olanağını veren manyetik sistemlerdir.

Maddenin birinci fıkrasında bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmaya devam etmek fiili suç hâline getirilmiştir. Sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.

İkinci fıkraya göre, birinci fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi, bu suç açısından daha az ceza ile cezalandırılmayı gerektirmektedir.

Üçüncü fıkrada, bu suçun neticesi sebebiyle ağırlaşmış hâli düzenlenmiştir. Birinci fıkrada tanımlanan suçun işlenmesi nedeniyle sistemin içerdiği verilerin yok olması veya değişmesi hâlinde failin, suçun temel şekline nazaran daha ağır ceza ile cezalandırılması öngörülmüştür. Dikkat edilmelidir ki, bu hükmün uygulanabilmesi için, failin verileri yok etmek veya değiştirmek kastıyla hareket etmemesi gerekir.

Birinci fıkrada, ne maksatla olursa olsun hukuka aykırı olarak sisteme girilmesi suç olarak kabul ettiğinden sisteme haksız olarak genel kasıtla girilmesi suçun oluşması için kafidir, belirli ve özel bir saikla hareket etmesi aranmamaktadır.

Maddenin ikinci fıkrası; yeni bir suç türü ihdas etmemekle birlikte ilk fıkraya bağlı bir ağırlaştırıcı sebebi düzenlemektedir. Failin hangi nedenle olursa olsun sisteme haksız ve kasıtlı bir şekilde girmesi sonucu sistemde bulunan veriler imha edilir veya değiştirilirse sadece bu neticeden dolayı fail daha ağır bir ceza ile cezalandırılmaktadır.

Burada failin sisteme girmesi ve bu girme sonucunda verilerin imha edilmesi yada değiştirilmesi kafi olup failin ayrıca bu neticeyi isteyip istememesi önemli değildir.

Üçüncü fıkraya göre, sisteme haksız olarak girmeye teşebbüs edilmesi halinde de faile suç tamamlanmış gibi ceza verilmesi söz konusudur. Diğer bir deyişle fail suça teşebbüs halindeki genel indirim maddelerindeki indirimlerden yararlanamaz. [37]

Sistem içindeki bütün soyut unsurlar, fıkrada geçen " veri " teriminin kapsamındadır. Bilgilerin toplandığı bu tür sistemlere, bilgisayarlara girmek, bilgilere erişmek suç olarak kabul edilmektedir.

Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz bilgilerin alınması da kişi özel mülkü yada kişilerin şahsiyetlerine taciz olarak kabul edilmektedir ve suç oluşturmaktadır.

Bu maddeyle hangi amaçla olursa olsun bilişim sistemine girme fiili suç olarak tanımlanmıştır. Bilişim sisteminden maksat, verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabii tutma olanağını veren manyetik sistemlerdir. Sisteme, doğal olarak, haksız ve kasten girilmiş olması bu suçun oluşması için yeterlidir. Ayrıca bir menfaat temini veya zarar meydana gelmesine gerek yoktur. Maddenin ikinci ve üçüncü fıkralarında ise hafifletici ve ağırlaştırıcı sebeplerini düzenlemektedir. Resen takibi yapılacak olan suçlardan olup, takibi şikayete bağlı değildir. Sulh Ceza Mahkemelerinin görev alanındaki suçlardandır.[38]

5237 sayılı Yeni Türk Ceza Kanunu'nun **244.** maddesinin başlığı **"Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme"** dir.

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

Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan

---

37- ÖZEL, a.g.w.s, 03.05.2006

38- GENÇ, Gökhan, **Bilişim Suçlarına İlişkin Yeni Türk Ceza Kanunu'ndaki Düzenlemeler**, http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=252, 02.04.2006

üç yıla kadar hapis cezası ile cezalandırılır. Bu fiillerin bir banka veya kredi kurumuna yada bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur. ***(Asliye Ceza)***

Gerekçesi ise:

Maddenin birinci fıkrasında bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, var olan verileri başka bir yere gönderme, erişilmez kılma, değiştirme ve yok etme fiilleri, suç olarak tanımlanmaktadır. Böylece sistemlere yöneltilen ızrar fiilleri özel bir suç hâline getirilmiştir. Aracın fizik varlığı ve işlemesini sağlayan bütün diğer unsurları, söz konusu suçun konusunu oluşturmaktadır. Fıkrada seçimlik hareketli bir suç meydana getirilmiştir.

İkinci fıkrada, bu fiillerin bir banka veya kredi kurumuna yada bir kamu kurum veya kuruluşuna ait bilişim sistemi hakkında işlenmesi hâlinde, verilecek cezanın artırılması öngörülmüştür.

Üçüncü fıkrada ise, bir ve ikinci fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması, ceza yaptırımı altına alınmıştır. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir. Bu bakımdan, fiilin örneğin dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyecektir.

Maddenin birinci fıkrası, bilişim sistemlerine yönelik olarak işlenen bozma, engelleme gibi ızrar fiillerini özel bir suç haline getirmektedir. Burada koruma altına alınan şey, bilişim sisteminin diğer bir deyişle bilgisayarın fiziki varlığı ve sistemin işlemesini sağlayan bütün diğer unsurlardır.

İkinci fıkrada ise bilişim sistemine veri sokulması, verilerin yok edilmesi, değiştirilmesi suç haline getirilmiş olup bu fıkranın uygulanabilmesi için failin bu neticelerin gerçekleşmesine yönelik özel bir kasıtla hareket etmesi gerekmektedir. 243.

maddenin ikinci fıkrasında fail, özel bir kasıtla istemediği ancak sisteme haksız olarak girmesi sebebi ile gerçekleşmesine neden olduğu neticeden dolayı cezalandırılırken burada gerçekleşmesi için özel bir kasıtla hareket ettiği ve gerçekleştirdiği yukarıda sayılan fiillerden dolayı cezalandırılmaktadır.

Üçüncü fıkrada ise failin, yukarıdaki iki fıkrada sayılan eylemleri ile başkasının zararına, kendisinin veya başkasının yararına haksız maddi yarar elde etmek için bilişim sistemine girmesi cezalandırılmaktadır.

Suçlara teşebbüs halinde de faile suç tamamlanmış gibi ceza verilecektir. [39]

Kötü amaçlı yazılmış kodlar, başkalarına zarar vermediği sürece suç sayılmamaktadır. Fakat bu tür kodlar; kişi yada kurumlara intikal eder ve zarar verirse suç teşkil etmeye başlar. Bir tehlike açısından suçtan bahsedebilmek için objektif olarak bir hareketin yapılması ve bu hareketin sonucunda ceza hukuku açısından bir netice meydana gelme ihtimalinin kuvvetli olması gerekir. Yoksa sırf kod yazımı saikten öte bir anlam ifade etmemelidir.

Günümüzde tüm dünya ülkelerinin baş belası olarak kabul edilen ve son zamanlarda etkili olan "Bilgisayar Sabotajı" suçu ile ilgili olarak birçok örnek vermek mümkündür. Çünkü bu tür olaylarda mali zarar yüklü miktarda olmakta ve derhal önlem alınması gerekmektedir. Örnek vermek gerekirse: Bilgisayarın içerdiği bilgileri kısmen yada tamamen alıp tehdit yoluyla para sızdırması olmakta, girdiği bilgisayara zarar vererek verilerin kaybolmasına yada kendi menfaatleri doğrultusunda kullanmak şeklinde olmaktadır.

Genellikle Rusya, Doğu Avrupa ve Uzakdoğu'da odaklanan Hacker, Cracker grupları belirli bir örgütsel hiyerarşi ve çalışma sistemi çerçevesinde para karşılığı dijital bilgi çalma, bozma gibi faaliyetler yürütmektedirler.

Ülkemizde ise bu tür faaliyetler organizasyon şeklinde (e-mafya) şeklinde olmasa bile (nadir faaliyet gösterebilmektedir), fazla olmamakla birlikte gruplar, çeteler oluşturmak suretiyle kişisel yada kurumsal bilgisayarlara saldırı düzenlemek suretiyle gerçekleşmektedir.

39- ÖZEL, a.g.w.s, 03.05.2006

Bu maddeyle de bir bilişim sisteminin işleyişini engelleme, bozma, sisteme hukuka aykırı olarak veri yerleştirme, sistemde var olan verileri başka bir yere gönderme, sistemde varolan verileri erişilmez kılma, verileri değiştirme ve yok etme fiilleri suç olarak tanımlanmaktadır.

Özellikle teknolojik gelişmeler ve Internet alanındaki hızlı ilerlemelerden sonra hukukumuzdaki çok büyük eksikliği bu madde doldurmuştur. Üçüncü ve Dördüncü fıkralarda suçun ağırlaştırıcı ve hafifletici sebepleri bulunmaktadır. Resen takibi yapılacak olan suçlardan olup, takibi şikayete bağlı değildir. Asliye ceza mahkemelerinin görev alanındaki suçlardandır.[40]

5237 sayılı Yeni Türk Ceza Kanunu'nun **245.** maddesinin başlığı **"Banka veya Kredi Kartlarının Kötüye Kullanılması"** şeklindedir.

MADDE 245- (8.7.2005 T. 5377 sk değ.) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

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

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

Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

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

---

40- GENÇ, a.g.w.s, 02.04.2006

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

Gerekçesi ise:

Madde, banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmak amacıyla kaleme alınmıştır.

Banka kartı, bankanın kurduğu sisteme hukuka uygun olarak girmeyi sağlamaktadır. Bu kart, saptanan ve kart sahibince bilinen bir numara marifetiyle, banka görevlisinin yardımı olmadan, kart sahibinin kendi hesabından para çekmesini sağlamaktadır.

Kredi kartları ise, banka ile kendisine kart verilen kişi arasında yapılmış bir sözleşme gereğince, kişinin bankanın belirli koşullarla sağladığı kredi olanağını kullanmasını sağlayan araçtır.

İşte bu kartların kötüye kullanılmaları, söz konusu maddede suç olarak tanımlanmıştır.

Maddeye göre, aşağıdaki şekillerde gerçekleştirilen hareketler bu suçu oluşturmaktadır:

1. Başkasına ait bir banka veya kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası bulunmaksızın kullanılması veya kullandırtması ve bu suretle failin kendisine veya başkasına haksız yarar sağlaması.

2. Aynı fiilin, aynı koşullarla sahibine verilmesi gereken bir banka veya kredi kartının bunu elinde bulunduran kimse tarafından kullanılması veya kullandırtması; sözgelimi kartı sahibine vermekle görevli banka memurunun kartı kendi veya başkası yararına kullanması.

Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının "ratio legis-kanunun koyuluş amaçlarının" tümünü de içeren bu fiillerin, duraksamaları ve içtihat farklılıklarını önlemek amacıyla, bağımsız suç hâline getirilmeleri uygun görülmüştür.

Maddenin ikinci fıkrasına göre; birinci fıkrada belirtilen fiillerin, oluşturulmuş sahte bir banka veya kredi kartını kullanmak suretiyle işlenmesi, daha ağır ceza ile cezalandırılmayı gerektirmektedir. Ancak, bu fıkra hükmüne istinaden cezaya hükmedilebilmesi için, fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması gerekir.

"Banka veya Kredi Kartlarının Kötüye Kullanılması" başlıklı **245.** maddenin kaleme alınmasının amacı, bu maddenin gerekçesinde de ifade edildiği üzere; bu kartların haksız, hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemektir.

Bilindiği gibi banka kartı, bankanın kurduğu bilişim sistemine hukuka uygun olarak girmeyi, kart sahibince bilinen bir numara marifetiyle banka görevlisinin katkısı olmadan kart sahibinin kendi hesabından para çekmesini sağlamaktadır.

Kredi kartı ise, banka ile müşterisi arasında yapılmış bir akit gereğince kişinin bankadan önceden koşulları saptanan kredi olanağını kullanmasını sağlayan bir araçtır.

Madde gerekçesine göre aşağıda zikredilen iki hal gerçekleştiğinde birinci fıkradaki suç oluşur:

a) Başkasına ait banka yada kredi kartının, her ne suretle olursa olsun ele geçirilmesinden sonra, sahibinin rızası hilafına kullanılması, başkasına kullandırılması, bu suretle failin kendisine yada bir başkasına haksız yarar sağlaması,

b) Sahibine verilmesi gereken bir banka yada kredi kartının bunu elinde bulunduran kimse tarafından kullanılması yada bir başkasına kullandırılması.

İkinci fıkra ise, ilk fıkrada sayılan eylemlerin esasen mevcut olan banka yada kredi kartlarının tahrif edilerek kullanılması veya bu kartların sahtecilik sureti ile yapılarak kullanılması hallerini cezalandırmaktadır.

Ceza kanununun amaçlarından birinin her konuda meydana gelebilecek hukuka aykırılıkları yaptırımsız bırakmamak olarak düşünürsek bu madde günümüz ekonomik hayatının en çok kullanılan ensturumanlarından kredi kartlarına ilişkin suiistimalleri düzenlediği için çok önemlidir. Yalnız burada dikkat edilmesi gereken nokta maddenin kredi kartlarına ilişkin her türlü kötüye kullanmayı değil, kredi kartlarına bilişim yoluyla müdahale edilmesini düzenlemesidir.

İkinci fıkrada suçun ağırlaştırıcı sebebi düzenlenmektedir. Resen takibi yapılacak olan suçlardan olup, takibi şikayete bağlı değildir. Asliye Ceza Mahkemelerinin görev alanındaki suçlardandır.[41]

Klasik olarak tabir ettiğimizde; bir şeyin aslına benzetilerek yapılan, düzme, düzmece olarak tarif edilmektedir. Bazen ileri teknoloji ürünü cihazlar kullanılarak, bazen de çok basit Web programcılığı (Fakemail, Phishing) yöntemiyle sahtecilik yapılmaktadır. Günümüzde başkalarının adına e-mail göndererek, ticari ve özel ilişkileri zedelenmesini sağlamak, başkalarının adına Web sitesi hazırlamak ve bu Web sitesinin tanıtım amacıyla başkalarına e-mail ve mesaj göndererek (iletişim kurarak) ve bu mesajlarda da mağdur olan şahsın telefonlarını vererek, sahte para, sahte evrak, sahte bilet vb. basma yöntimiyle bu suç işlenmektedir.[42]

Bu maddedeki düzenleme ile Yargıtay Ceza Genel Kurulu'nun 11.4.2000 tarih, 2000/6-62 esas, 2000/72 sayılı kararındaki anlayış madde metni haline getirilmiş bulunmaktadır. Bu kararın konusunu teşkil eden olay kısaca şöyledir:

Bu olayda sanık müştekiye ait banka kredi kartını haksız olarak eline geçirmiş, şifresini de öğrenerek bir bankanın üç ayrı şubesine ait ATM'lerden muhtelif tarihlerde para çekmiştir, İstanbul 1. Ağır Ceza Mahkemesi banka kartını TCK'nun 493/2. maddesinde zikredilen " sair alet" kapsamında mütalaa ederek bu madde uyarınca sanığı cezalandırmış, Yargıtay 6. C.D. mahkeme kararını onamıştır. Bu onama kararına karşı itiraz yoluna başvuran Yargıtay Cumhuriyet Başsavcılığı; banka kartının "sair alet" olarak kabul edilemeyeceğini, olayın TCK'nun 525 inci maddesine uyduğunu ileriye sürerek konunun Yargıtay Ceza Genel Kurulu önüne gelmesini sağlamıştır. Genel Kurul ise yukarıda tarih ve sayısı verilen kararında; ATM olarak adlandırılan sistemin işlemesi için iki unsura gereksinim bulunduğunu, bunlardan birincisinin kart, diğerinin ise şifre olduğunu, ATM makinelerinin bir bilgi işlem sisteminin ünitesi olarak kabul edilmesi gerektiğini, sistemi harekete geçirmede kullanılan kartların geleneksel hırsızlık suçları bakımından söz konusu olan "sair alet" sayılamayacağını, olayın TCK'nun 525/b-2

41- GENÇ, a.g.w.s, 02.04.2006
42- EKER, a.g.w.s, 13.06.2006

madde ve fıkrasına uyduğunu gerekçeleri ile ileriye sürerek Başsavcılığın itirazını kabul etmiş ve böylece aynı görüşteki Yargıtay 11. C.D.'nin bir başka olayla ilgili olarak verdiği içtihattaki anlayışı kabul etmiştir. Bu genel kurul kararı oy çokluğu ile verilmiş bir karar olup 245. maddedeki düzenleme bu konudaki tartışmaları tamamen ortadan kaldırıcı mahiyette olmakla isabetli bir tasarruf olarak gözükmektedir.[43]

5237 sayılı Yeni Türk Ceza Kanunu'nun **246.** maddesinin başlığı **"Tüzel Kişiler Hakkında Güvenlik Tedbiri Uygulanması"** adı altındadır.

MADDE 246 - Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Gerekçesi ise:

Madde metninde, bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında da bunlara özgü güvenlik tedbirlerine hükmolunacağı düzenlenmiştir.

Ayrıca, 5237 sayılı Türk Ceza Kanunu'nun **"Nitelikli Dolandırıcılık"** başlıklı **158.** maddesinin **"f"** bendinde **"Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"** yapılan sahtekarlık ve dolandırıcılığa ceza verilmiştir.

Kanunun gerekçesinde; birinci fıkranın "f" bendinde bu suçun bir nitelikli unsuru olarak kabul edilmiştir. Bilişim sistemlerinin yada birer güven kurumu olan banka veya kredi kurumlarının araç olarak kullanılması, dolandırıcılık suçunun işlenmesi açısından önemli bir kolaylık sağlamaktadır. Banka ve kredi kurumları açısından dikkat edilmesi gereken husus, bu kurumları temsilen, bu kurumlar adına hareket eden kişilerin başkalarını kolaylıkla aldatabilmeleridir, denilmek suretiyle bilgisayar veya iletişim araçlarıyla yapılan bu türlü suçların cezalandırılması gerektiği öngörülmüştür.

Bu Kanunun **157**. maddesinde dolandırıcılığın tanımı şu şekilde yapılmıştır: Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine

---

43- ÖZEL, a.g.w.s, 03.05.2006

veya başkasına bir yarar sağlayan kişinin işlemiş olduğu suçtur. Bilişim kavramı olarak ise dolandırıcılık; hileli davranışların bilgisayar veya iletişim araçlarıyla kişileri şaşırtma, aldatma, kandırmaya yönelik olarak kullanılarak yapılan suçlardır diyebiliriz.

Bilgisayar yoluyla dolandırıcılık; kredi kartlarının bir benzerinin yardımcı programlarla (Card Generator vb.-Kart Üreteçi) oluşturulması ile yetkisiz ve izinsiz erişilen bilgilerin kopyasını almak şeklinde, finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle ve kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak, kişileri kandırarak suçu işlemektedir.

2.1 Kanuni Yazılımların İzinsiz Kullanımı:

"Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılmasını ve kullanılmasını ifade eder.

Ülkemizde **5846 sayılı Fikir ve Sanat Eseleri Kanunu (FSEK)** lisanslı yazılımları satın alan kişiye bir adet kopyalama hakkı vermekte, daha fazla kopyanın yapılmasını, satılmasını, yazılımın kiralanmasını yasaklamaktadır.

Günümüzde korsan CD basımı ve dağıtılması korkunç büyüklükte boyutlara ulaşmakta, yapılan operasyonlar sonucu ele geçirilen lisanssız ürünlerin mali değerinin yüksekliği bu gerçeği ortaya koymaktadır. Tüketici (Yazılımı Satın Alan) da lisanssız çoğaltılan ürünleri ucuz olmasından dolayı tercih etmektedir. Unutmamak gerekir ki korsan yazılımları alan ve satan kişiler kanun önünde suçlu sayılmaktadır. Bu korsan yazılımlar; güvenlikli olmamakla birlikte, kullanımından doğan sorunlar karşısında herhangi bir müracaatta bulunulamamaktadır. Zira bu tür korsan yazılımlar genellikle bilgisayar ve kullanıldığı teknolojik araca zarar vermekte, tamir edilmesi imkansız sorunlara yol açmakta, bazı durumlarda boş çıkmakta, bazen de virüs barındırmaktadır. Çoğu yazılım şirketinin yazılım korsanlığına karşı hukuki işlemlerini yürüten B.S.A.'nın (Business Software Ailliance) verdiği rakamlara göre ülkemizde lisanssız kullanımın %80'lerin üzerinde olduğu belirtilmektedir.

2.2. Yasadışı Yayınlar:

Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, Internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir. Kanunun yasaklamış olduğu bu materyaller; Web siteleri (sayfaları), BBS'ler (Bulletin Board Services- Duyuru Tahtası Hizmetleri), elektronik postalar, haber grupları, forumlar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir.

Yasadışı yayınları üç gruba ayırmak mümkündür. Bunlardan birincisi, ülkenin bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli Internet siteleridir. Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş (Anayasa'nın 3. maddesine aykırılık, yapmak istedikleri yayınları kabul edilmediğinden) anonim olan Internet'i kullanarak kendilerine taraf toplamayı hedeflerler ve bilinen klasik yollardan ulaştıramadıkları ideolojilerini, vatanın bütünlüğünü bozacak düşüncelerini bu sayede ifade ederek propagandalarını yapmaktadırlar.

Yasadışı yayınların bir diğeri ise toplumun genel ahlakına, ar ve haya duygularına aykırı düşen yayınlardır. Bunlar pornografik görüntü veya yazılar şeklinde olmaktadır. Belki de her gün binlerce pornografik yayın Internet üzerinden faaliyete geçmekte, bunların çoğu da çocuk pornografisi üzerine olmaktadır.

Internet aracılığıyla fiilen işlenen suçlardan üçüncüsü ise; bir kişiye, kuruma vb. karşı yapılan hakaret ve sövme suçudur. Bu suç türü Internet üzerinden başkalarının adına uygun olmayan e-mailler göndererek kişi yada kurumların itibarını zedelemek suretiyle olabilmektedir. Bir başka yol ise yine kişi yada kurumların sahip oldukları adın, lakabın web üzerinden satın alınarak, kişi aleyhine yayında bulunmak suretiyle medyana gelebilmektedir.

Ülkemizde bu ve benzeri olaylar sıkça yaşanmaktadır. Gazetelere yansıyan olaylarda; birbirini tanımayan insanların chatte (sohbet odaları) küfürleşmeleri ve daha sonra buluşup birbirlerini yaralamaları, yada bir zaman milletvekilliği yapmış bir kişinin adı ve soyadını oluşturduğu domain adını alarak pornografik site oluşturmaları gibi.

Her geçen gün gelişen iletişim araçları (Internet vb.) üzerinden meydana gelen hakaret, sövme konusunda maalesef etkili bir önlem alınamamaktadır. Bu tür durumlarda kişilerin kendi çabalarıyla halletmeye çalıştıkları, bu konuda savcılığa

başvurunun az olduğu görülmüştür. Halbuki bu suç Internet'te işlenmesi yüksek olan bir türdür. Alınabilecek önlemler, kullanıcıların daha duyarlı ve dikkatli olması, gelen e-mailleri dikkatli okuması, Spam mesajları derhal silmeleri, gerekirse önemli gördükleri kişi yada kurumlarla iletişim kurarken özel bir işaret kullanarak irtibatı sağlamaları şeklinde olmalıdır.[44]

2.3 Çoçuk Pornografisi:

Bilgisayar (Internet destekli) resim ve videolar şeklinde müstehcenlik, toplum ahlakına aykırı biçimlerin oluşturulma ile sübyancı olarak ifade edilen sapkın ve çirkin fikirlerin faaliyete geçmesi sonucu "pornografi" ve özelde "çocuk pornografisi" kavramı belirginleşmiştir.

WWW (world wide web)'in sağladığı anonimlik hakkı kullanılarak, çocuk pornografisi ile ilgili yayınlar tedbirsizce dağıtılmakta, bu dağıtım katılımcı, hızla artan "peer to peer" (Eşler Arası Network)'ler, download linkleri (FTP, HTTP), Web siteleri ile olmakta ve çocuklara yönelik cinsel maruzlar teşhir edilmektedir.

1988 yılında 14 ülke arasında yapılan, 100 kişinin gözaltına alınmasıyla sonuçlanan "Wonderland" adlı klubün piyasaya sürdüğü çocuk pornografisi türü yayınların iki yaşında bir çocuğa ait pornografik malzemesi bulundurması ne kadar "sapkın" eğilimin olduğu ve çocuk pornografisinin ulaştığı boyutları yeterince açıklamaktadır. Bu konuda Amerikan Adalet Bakanlığı Ceza Departmanı'nda görevli Adalet Bakan Yardımcısı ve vekili John G.Malcomn'un Senato Adli Komitesine yaptığı açıklama çok çarpıcıdır: "Bu tür materyallerin çoğalması ve pornografiyle uğraşanların kendileri bu sıkı yarışmacı ortamda ayırt ettirme istekleri bu kişilerin daha da saldırgan nitelikli materyaller üretmelerine yol açacaktır." Yine Malcomn : "Eskiden itibarsız dükkanların tezgahlarının arkasındaki evrak çantalarında saklanan materyaller, şimdi bunun çok daha ötesine geçmiş ve bu tür materyaller bulmayı aklından bile geçirmeyen ve görmek de istemeyen çocukların ve yetişkinlerin erişimindeki bir bilgisayar faresine birkaç tıklamayla bir iki dakika içerisinde Internet bağlantısı üzerinden kolayca elde

---

44- EKER, a.g.w.s, 13.06.2006

edebiliyor." demiştir. Malcomn'un da bahsettiği gibi çocuk pornografisine erişmek artık deyim yerindeyse "çocuk oyuncağı" şeklinde olmaktadır. Günümüzde hızla yayılan bu tür yayınların etkisi o kadar büyüktür ki; yetişkin olmayan her beş bireyden biri bu tür cinsel tahrik, teşhir veya etkilerine maruz kalmaktadır.

Gelişmiş dünya ülkelerinde bu tür yasadışı yayınlar üzerine bir çok operasyon yapılmış, pornografik yayınların yaygınlığı bir kez daha ortaya çıkmıştır. Örnek verecek olursak: Bu tür yayınlar tüm dünya üzerinde 1996-2004 yılları arasında 42 bin civarında ve bu yayınların görüntülenmesi 27 milyonun üzerindedir. İtalya'da 1998 yılında çocuk pornografisi kanunda yasaklandıktan sonra 100 binin üzerinde pornografik yayın ele geçirilmiştir. Bu tür yayınların çoğu Amerika'da bulunmaktadır. Fakat en hızlı artış ise Rusya'da olmaktadır. 2002 yılından itibaren çocuk pornografisine yönelik yapılan Web sitelerin hızla artışı %64'ün üzerinde bulunması ne kadar ilgi çektiğinin bir göstergesidir. Gerçekten yukarıdaki örneklere benzer birçok örnek gelişmiş ve gelişmekte olan ülkelerde meydana gelmektedir ve sayısal verilerin büyüklüğü ürkütücü olmaktadır.

Cinsel istismarın bir türü olan çocuk pornografisinin cezalandırma konusu olması, her şeyden önce, çocuğun ruhsal ve fiziksel gelişimini henüz tamamlamamış olması ve onun kendi cinsel davranışı üzerinde özerk bir karar verme yeteneğinin henüz gelişmemiş olmasından kaynaklanmaktadır. Avrupa Konseyi Siber Suç Sözleşmesine göre (madde 9) çocuk pornografisi kavramı;

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 gerçeğe benzer görüntüleri, ifade etmektedir. Bu konuda, bu sözleşmeyi imzalayan devletler 18 yaşından küçük olanları, reşit olmayan kişileri, çocukları kast etmektedir.

BM Genel Kurulu tarafından 20 Kasım 1989 yılında kabul edilen "Çocuk Haklarına Dair Sözleşme" ve bu sözleşmeye ek 25 Mayıs 2000 tarihli "Çocuk Satışı, Çocuk Fahişeliği ve Çocuk Pornografisi İle İlgili Seçmeli Protokol" Ülkemiz tarafından da onaylanmıştır.

Bu protokolun 2. maddesinin (c) fıkrasında çocuk pornografisinin tarifi yapılmıştır:

"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 gösterilmesi anlamına gelmektedir."

Yine Çocuk Haklarına Dair Birleşmiş Milletler Sözleşmesinin 32. maddesi ve 34. maddesine göre;

a) Çocuğun yasadışı bir cinsel faaliyete girişmek üzere kandırılması veya zorlanmasını,

b) Çocukların fuhuş yada diğer yasadışı cinsel faaliyette bulundurularak sömürülmesini,

c) Çocukların pornografik nitelikteki gösterilerde ve malzemede kullanılmasını önlemek amacıyla ulusal ve uluslararası düzeyde gerekli her türlü önlemi alırlar.

23 Kasım 2001 tarihinde Budapeşte'de imzaya açılan Avrupa Konseyi Siber Suç Sözleşmesi'ne göre de (madde 9), taraf devletler;

a) Bir bilgisayar sistemi üzerinden dağıtmak amacıyla çocuk pornografisi üretmek,

b) Bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak yada çocuk pornografisine erişim sağlamak,

c) Bir bilgisayar sistemi üzerinden çocuk pornografisi dağıtmak yada yaymak,

d) Kişinin, bir bilgisayar sistemi üzerinden kendisi yada başkası için çocuk pornografisi temin etmesi,

e) Bir bilgisayar sisteminde yada bilgisayar verilerinin saklandığı başka cihazlarda çocuk pornografisi bulundurmak konularında kasten işlenmesi halinde, kendi mevzuatlarında suç ihdası için gerekli yasama ve diğer işlemleri yapacaktır.

Ülkemizde, 5237 sayılı Türk Ceza Kanunu'nda; **"Cinsel Saldırı" 102**. madde de; cinsel davranışlarla bir kimsenin vücut dokunulmazlığını ihlal, fiilin vücuda organ veya sair bir cisim sokulması suretiyle işlenmesi;

"Çocukların Cinsel İstismarı" başlıklı **103.** maddesine göre de;

Çocuğu cinsel yönden istismar eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır. Cinsel istismar deyiminden;

a) On beş yaşını tamamlamamış veya tamamlamış olmakla birlikte fiilin hukukî anlam ve sonuçlarını algılama yeteneği gelişmemiş olan çocuklara karşı gerçekleştirilen her türlü cinsel davranış,

b) Diğer çocuklara karşı sadece cebir, tehdit, hile veya iradeyi etkileyen başka bir nedene dayalı olarak gerçekleştirilen cinsel davranışlar, anlaşılır. ***(Asliye Ceza)***

Cinsel istismarın vücuda organ veya sair bir cisim sokulması suretiyle gerçekleştirilmesi durumunda, sekiz yıldan on beş yıla kadar hapis cezasına hükmolunur.***(Ağır Ceza)***

(8.7.2005 T. 5377 sk değ.) Cinsel istismarın üstsoy, ikinci veya üçüncü derecede kan hısımı, üvey baba, evlat edinen, vasi, eğitici, öğretici, bakıcı, sağlık hizmeti veren veya koruma ve gözetim yükümlülüğü bulunan diğer kişiler tarafından yada hizmet ilişkisinin sağladığı nüfuzu kötüye kullanılmak suretiyle veya birden fazla kişi tarafından birlikte gerçekleştirilmesi hâlinde, yukarıdaki fıkralara göre verilecek ceza yarı oranında artırılır.

Cinsel istismarın, birinci fıkranın **(a)** bendindeki çocuklara karşı cebir veya tehdit kullanmak suretiyle gerçekleştirilmesi hâlinde, yukarıdaki fıkralara göre verilecek ceza yarı oranında artırılır.

Cinsel istismar için başvurulan cebir ve şiddetin kasten yaralama suçunun ağır neticelerine neden olması hâlinde, ayrıca kasten yaralama suçuna ilişkin hükümler uygulanır.

Suçun sonucunda mağdurun beden veya ruh sağlığının bozulması hâlinde, onbeş yıldan az olmamak üzere hapis cezasına hükmolunur.

Suçun mağdurun bitkisel hayata girmesine veya ölümüne neden olması durumunda, ağırlaştırılmış müebbet hapis cezasına hükmolunur.***(Ağır Ceza)***

5237 sayılı Türk Ceza Kanunu **"Fuhuş" 227.** maddesinde; çocuğu fuhşa teşvik eden, bunun yolunu kolaylaştıran, bu maksatla tedarik eden veya barındıran ya da çocuğun fuhşuna aracılık etmenin suç olduğunu belirmektedir.

Yine 5237 sayılı Türk Ceza Kanununun **226.** maddesine göre:

a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren yada bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde yada 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 adlî para cezası ile cezalandırılır.

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 adlî para cezası ile cezalandırılır.

Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları kullanan kişi, beş yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır. Bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran yada başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

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 adlî para cezası ile cezalandırılır.

Üç ve Dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden yada çocukların görmesini, dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

Bu suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Bu madde hükümleri, bilimsel eserlerle; üçüncü fıkra hariç olmak ve çocuklara ulaşması engellenmek koşuluyla, sanatsal ve edebi değeri olan eserler hakkında uygulanmaz, demektedir.[45]

Kanunun gerekçesi de şu şekilde belirtilmiştir:

Madde metninde, müstehcenlik ve çocukların bu tür zararlı yayınlara karşı korunmasına ilişkin hükümler düzenlenmiştir. Normatif (değerlendirilebilir) bir unsur niteliğini taşıyan müstehcenlik kavramının içeriğinin belirlenmesinde, toplumda egemen olan değer ölçüleri ve yukarıdaki madde gerekçesinde hayasızca hareketler kavramına yönelik olarak yapılan açıklamalar, göz önünde bulundurulmalıdır.

Maddenin birinci fıkrasında müstehcenlikle ilgili çeşitli davranışlar, suç olarak tanımlanmıştır. Fıkranın (a) bendinde, bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünlerin verilmesi yada bunların içeriğinin gösterilmesi, okunması, okutulması veya dinletilmesi; (b) bendinde ise, bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde yada alenen gösterilmesi, görülebilecek şekilde sergilenmesi, okunması, okutulması, söylenmesi veya söyletilmesi, suç olarak tanımlanmıştır.

Fıkranın (c) bendine göre, müstehcen görüntü, yazı veya sözleri içeren ürünlerin, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz edilmesi, suç oluşturmaktadır. (d) bendine göre, bu ürünler ancak, bunların satışına özgü alışveriş yerlerinde, erişkin kişilere satılabilir veya kiraya verilebilir. Bu itibarla, müstehcen görüntü, yazı veya sözleri içeren ürünlerin satışına mahsus alışveriş yerleri dışında, satışa veya kiraya arz edilmesi, satılması veya kiraya verilmesi, suç olarak tanımlanmıştır.

45- EKER, a.g.w.s, 13.06.2006

Fıkranın **(e)** ve **(f)** bentlerine göre; müstehcen görüntü, yazı veya sözleri içeren ürünlerin, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak başkalarına verilmesi veya dağıtılması yada reklamının yapılması, suç oluşturacaktır.

Seçimlik hareketler olan bu fiillerin işlenmesi suretiyle bir kazanç elde edilebileceği için, bu suçun karşılığında hapis cezasının yanı sıra adlî para cezası da öngörülmüştür.

Maddenin ikinci fıkrasında, müstehcen görüntü, yazı veya sözlerin basın ve yayın yolu ile yayınlanması veya yayınlanmasına aracılık edilmesi, ayrı bir suç olarak tanımlanmıştır.

Üçüncü fıkrada, müstehcenliğe karşı çocukları korumaya yönelik iki ayrı suç tanımına yer verilmiştir. Bunlardan birincisi; müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukların kullanılması suretiyle oluşmaktadır. İkinci suç ise, bu ürünlerin ülkeye sokulması, çoğaltılması, satışa arzı, satışı, nakli, depolanması, ihracı, bulundurulması yada başkalarının kullanımına sunulması fiillerinden birinin işlenmesiyle oluşmaktadır.

Dördüncü fıkraya göre; şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünlerin üretilmesi, ülkeye sokulması, satışa arzı, satışı, nakli, depolanması, başkalarının kullanımına sunulması veya bulundurulması fiilleri suç oluşturmaktadır. Bu hükümle, belirtilen içerikte olan ürünler açısından mutlak bir yasak getirilmiştir.

Maddenin beşinci fıkrasına göre; üç ve dördüncü fıkralardaki suçların konusunu oluşturan ve müstehcenlik bakımından mutlak yasak kapsamına giren ürünlerin içeriğinin basın ve yayın yolu ile yayınlanması, yayınlanmasına aracılık edilmesi yada çocukların görmesinin, dinlemesinin veya okumasının sağlanması, ayrı bir suç oluşturmaktadır.

Son fıkrada ise, bu madde kapsamında tanımlanan suçlardan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunacağı kabul edilmiştir.

2.4 Fikir ve Sanat Eserleri Kanunu'ndaki Düzenleme:

5846 Sayılı Fikir ve Sanat Eserleri Kanunu nedir neyi düzenlemektedir noktasından bakacak olursak; Fikir ve Sanat Eserlerini meydana getiren eser sahipleri ile bu eserleri icra eden veya yayımlayan icracı sanatçılarının, fragman yapım ile filmlerin ilk tespitlerini yapan gerçek yapımcıların ve radyo televizyon kuruluşlarının ürünleri üzerlerindeki manevi ve mali hakları belirlemek korumak ve bu ürünlerden yararlanma şartlarını düzenlemek öngörülen esas ve usullere aykırı yararlanma halinde eserleri izinsiz olarak kullanan, çoğaltan, işleyen, bilgisayar programlarını koruyan aygıtları geçersiz kılan teknik araçları bulunduran, dağıtan ve bu tip eser ve programları çıkar sağlamak için yayınlayanlar hakkında yayın durdurma, maddi ve manevi tazminatların yanı sıra cezai sorumluluklarda getirmekte ve eser sahiplerinin bu konuda manevi yani, eserinin sahipliğini üstlenme ve eserinin özelliğine ve bütünlüğüne saygı gösterilmesini talep etme hakları ve maddi yani eser sahibinin para kazanmasına yarayan işlemler olan, çoğaltma, yayma ve temsil etme haklarına müdahalenin tazminine ve bu suçları işleyenlerin cezalandırılmasına yönelik bir kanundur.

Oysaki, 5237 sayılı 2005 Haziran ayında yürürlüğe giren yeni Türk Ceza Kanunu'nun **243-246** maddeleri arasında düzenlenen "Bilişim Suçları" bilgileri otomatik işleme tabi tutulmuş bir sisteme müdahaleyi cezalandırmaktadır.

Ülkemizde bilişim hukuku açısından Fikir ve Sanat Eserleri Kanunu'nda düzenlenmiş olan en etkili mücadele 12.03.2004 tarihinde yürürlüğe giren ve başta FSEK olmak üzere, bazı yasalarda değişiklik yapan **5101** sayılı Kanun'un kabul edilmesi olmuştur. Bu yasa yayıncı, dağıtımcı, müzik, sinema, radyo-TV kuruluşları, otel ve eğlence gibi umuma açık yerleri ilgilendiren hükümler taşımaktadır. Bu bağlamda Fikir Sanat Eserleri Kanunu'ndaki ilgili maddelere bakacak olursak;

Madde 70- (Değişik birinci fıkra : 7/6/1995 - 4110/22 md.) Manevi hakları haleldar edilen kişi, uğradığı manevi zarara karşılık manevi tazminat ödenmesi için dava açabilir. Mahkeme, bu para yerine veya bunlara ek olarak başka bir manevi tazminat şekline de hükmedebilir.

Mali hakları haleldar edilen kimse, tecavüz edenin kusuru varsa haksız fiillere müteallik hükümler dairesinde tazminat talep edebilir.

Birinci ve ikinci fıkralardaki hallerde, tecavüze uğrayan kimse tazminattan başka temin edilen kârın kendisine verilmesini de isteyebilir. Bu halde **68 inci** madde uyarınca talep edilen bedel indirilir.

Maddenin kapsamından da anlaşılacağı üzere bir eser sahibinin haklarının ihlal edilmesi durumunda hak sahibi manevi tazminat ve maddi tazminat isteme hakkına sahip olacaktır.

Ceza davaları:

I- Suçlar;

1. Mânevi haklara tecavüz;

Madde 71- (Değişik: 1/11/1983 - 2936/11 md.)

Bu Kanun'un hükümlerine aykırı olarak kasten:

1. Alenileşmiş olsun veya olmasın, eser sahibi veya halefinin yazılı izni olmadan bir eseri umuma arz eden veya yayımlayan,

2. Sahip veya halefinin yazılı izni olmadan, bir esere veya çoğaltılmış nüshalarına ad koyan,

3. Başkasının eserini kendi eseri veya kendisinin eserini başkasının eseri olarak gösteren veya 15 inci maddenin ikinci fıkrası hükmüne aykırı hareket eden,

4. 32, 33, 34, 35, 36, 37, 39 ve 40 ıncı maddelerdeki hallerde kaynak göstermeyen veya yanlış yahut kifayetsiz veya aldatıcı kaynak gösteren.

(Değişik : 7/6/1995 - 4110/23 md.) Kişiler hakkında üç aydan bir yıla kadar hapis ve 300 milyon liradan 600 milyon liraya kadar ağır para cezasına hükmolunur.

2. Mali haklara tecavüz:

Madde 72 - (Değişik: 1/11/1983 - 2936/12 md.)

Hak sahibinin yazılı izni olmaksızın, bu Kanun'a aykırı olarak kasten:

1. Bir eseri herhangi bir şekilde işleyen,

2. Bir eseri herhangi bir şekilde çoğaltan,

3. Bir eser veya işlenmelerinin kendi tarafından çoğaltılmış nüshalarını satan veya satışa veyahut tedavüle arz eden,

4. Bir eseri veya işlenmelerini temsil veya teşhir eden yahut umumi yerlerde gösteren veya radyo yahut buna benzer vasıtalar ile yayan,

5. (Ek: 7/6/1995 - 4110/24 md.) Bir eseri veya işlenmelerini kiralayan,

6. (Ek: 7/6/1995 - 4110/24 md.) Eser sahibinin izni olmadan yapılan nüshaları ithal eden,

(Değişik: 7/6/1995 - 4110/24 md.) Kişiler hakkında üç aydan bir yıla kadar hapis ve 300 milyon liradan 600 milyon liraya kadar ağır para cezasına hükmolunur.

Bu maddenin tanımından anlaşılacağı üzere; Lisanslı (orijinal) yazılımlardan izinsiz olarak yazılımın şifrelerini kırarak çoğaltan (lisanssız) yazılımları elinde bulunduran , kullanan, kiralayan, satan ve dağıtan, yazılımın şifre veya kilitlerini açan yöntem ve araçları ticari amaçla elinde bulunduran veya dağıtan, bilgisayar sistemindeki programları, verileri veya diğer unsurları hukuka aykırı olarak ele geçiren, her kişi Fikir ve Sanat Eserleri Kanunu (FSEK) gereğince cezalandırılacaktır.

3. Diğer suçlar:

Madde 73- (Değişik: 1/11/1983 - 2936/13 md.)

Kasten:

1. Bu Kanunun hükümlerine aykırı olarak çoğaltıldığını bildiği veya bilmesi icap ettiği bir eserin nüshalarını satışa çıkaran veya bunlardan umumî yerlerde temsil veya radyo ile yayım maksadı ile yahut kâr temini için diğer herhangi bir suretle faydalanan,

2. Bu Kanun hükümlerine aykırı olarak satışa çıkarıldığını bildiğini veya bilmesi icap ettiği bir eserin nüshalarını başkalarına satan veya bunlardan umumî yerlerde temsil veya radyo ile yayım maksadıyla veya kâr temini için herhangi bir surette faydalanan,

3. Mevcut olmadığını veya üzerinde tasarruf salâhiyeti bulunmadığını, bildiği veya bilmesi icap ettiği mali hakkı veya ruhsatı başkasına devreden veya veren yahut rehin eden veyahut herhangi bir tasarrufun konusunu yapan,

4. Kendisine sözleşme veya kanunla müsaade edilen miktardan fazla nüsha çoğaltan veya çoğalttıran,

5. (Ek: 7/6/1995 - 4110/25 md.) Bu Kanun hükümlerine aykırı olarak çoğaltıldığını bildiği veya bilmesi icap ettiği bir eserin nüshalarını ticarî amaçla elinde bulunduran,

6. (Ek: 7/6/1995 - 4110/25 md.) Yegane amacı bir bilgisayar programını korumak için uygulanan bir teknik aygıtın geçersiz kılınmasına veya izinsiz ortadan kaldırılmasına yarayan herhangi bir teknik aracı ticarî amaç için elinde bulunduran veya dağıtan,

Bu 6. fıkra kapsamında bu araçları üreten kişi de değerlendirilebilmelidir. (Değişik : 7/6/1995 - 4110/25 md.) Kişiler hakkında üç aydan üç yıla kadar hapis ve 300 milyon liradan 600 milyon liraya kadar ağır para cezasına hükmolunur.

Fail:

Madde 74 - 71, 72 ve 73 üncü maddelerde sayılan suçlar, hizmetlerini ifa ettikleri sırada bir işletmenin temsilcisi veya müstahdemleri tarafından işlenmiş ise, suçun işlenmesine mâni olmayan işletme sahibi veya müdürü yahut herhangi bir nam ve sıfatla olursa olsun işletmeyi fiilen idare eden kimse de fail gibi cezalandırılır. Cezai mucip fiil işletme sahibi veya müdürü yahut işletmeyi fiilen idare eden kimse tarafından emredilmiş ise bunlar fail gibi; temsilci veya müstahdem ise, yardımcı gibi cezalandırılır.

Temsil edilmesinin kanuna aykırılığını bildiği bir eserin umuma gösterilmesi için karışlıklı veya karışlıksız olarak bir mahalli tahsis eden veya böyle bir eserin temsilinde vazife veya rol olan kimse, yardımcı olarak cezalandırılır.

Bir tüzel kişinin işleri çevrilirken 71, 72 ve 73 üncü maddelerde sayılan suçlardan biri işlenirse, masraf ve para cezasından tüzelkişi diğer suçlularla birlikte müteselsilsen mesuldür.

Ceza Kanunu'nun 64, 65, 66 ve 67 nci maddelerinin hükümleri mahfuzdur.Bu Kanunu'n önemli bir noktasında sorumluluğun özel olarak düzenlenmesinden kaynaklanmaktadır.

Buna göre suçun işlenmesine mani olamayan işletme sahibi veya müdürü ve her ne surette olursa olsun işletmeyi fiilen idare eden kimse de cezalandırılır. Bu hukuka aykırı fiillerden dolayı masraf ve para cezasından tüzel kişi de sorumludur.[46]

Internet ve hukuk çalışmalarında en önemli yerlerden birini de fikri haklar meseleleri oluşturmaktadır. Müzik, sinema, resim gibi ve Internet'e özgü eserlere yapılan tecavüzler sonucu hak sahipleri büyük zararlara uğramakta ve fakat buna karşın yeterli korumaya sahip olmamaktadırlar. Bu korumanın zayıf olmasındaki en büyük etken Internet'in sınır tanımayan karakterde oluşudur. Dolayısıyla ihlallerin tespiti, kovuşturulması, sorumluların belirlenmesi çok zor olmaktadır. Bu konudaki çözüm ise Internet'e ilişkin uluslar arası ve etkin yaptırımlara sahip düzenlemelere gidilmesidir. Devletler ise iç hukuklarında fikri haklara ilişkin kanunlarında teknik gelişmeleri takip edebilecek esnek hükümler getirmelidirler. Aksi halde her seferinde kanun teknik gelişmeler karşısında zorlanacak ve yapay, geçici çözümler üretilmeye çalışılacaktır.[47]

2.5 Bilişim Suçlarında Soruşturma ve Görevli Mahkeme:

Türk Ceza Kanunu'nun **243, 244, 245 ve 246.** maddelerinde düzenlenen "Bilişim Suçları" ile ilgili fiilleri işleyen kişi, kişiler, kurum ve kuruluşlar hakkında soruşturma Cumhuriyet Savcılıkları kanalı ile resen takibi yapılacak suçlardandır. Bu suçlar şahsi dava yada takibi şikayete bağlı olarak tanzim edilen suçlardan değildir. Keza Yeni Ceza Usul Kanunu şahsi dava ayrımını kabul etmemiştir.

Dolayısı ile Cumhuriyet Savcısı bilişim suçlarından her hangi birisinin, Ceza Usul Kanunu'nun **160.** maddesi delaleti ile ihbar veya bir başka surette fiilin işlendiği izlenimini veren bir hali öğrenir öğrenmez gerekli araştırma, soruşturma ve delillendirme işleminin ardından yine aynı yasanın **170.** maddesi gereğince kamu davasını açacaktır. 1 Haziran 2005 tarihinde yürürlüğe giren 5237 sayılı Yeni Türk Ceza Kanunu'nun **243 -246.** maddeleri arasında düzenlenen "Bilişim Suçlarına" bakmakla görevli mahkeme kanunun metninde tayin edilmemiştir. Dolayısı ile bu konuda Ceza

---

46- KODAN, Mahmut, **Bilişim Suçlarının 5846 Sayılı Fikir Ve Sanat Eserleri Kanunu Açısından Değerlendirmesi, Bilişim Suçları**,
http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=254, 30.07.2006
47- ÖZDİLEK, a.g.e, s.92

Hukukunun yargılamaya ilişkin genel görevle ilgili kuralları uygulama alanı bulacaktır. Buna göre;

Sulh Ceza ve Ağır Ceza Mahkemelerinin görevleri dışında kalan, özel yasasında Asliye Ceza Mahkemesince görülüp karara bağlanacağı açıklanan veya özel yasasında hangi mahkemede görülüp karara bağlanacağı açıklanmamış olmakla birlikte Sulh ve Ağır Ceza Mahkemesinin görevi içinde bulunmayan bütün ceza davalarına bakmakla görevli olan Asliye Ceza Mahkemeleri, bilişim suçlarına bakmakla da görevli mahkemeler olacaktır.

Yeni Türk Ceza Kanunu'nun "Bilişim Suçları" ile ilgili düzenlemeleri incelendiği vakit görev alanları kanunla belirtilmiş olan Sulh Ceza Mahkemeleri ile yine görev alanları yasa ile belirlenmiş olan Ağır Ceza Mahkemelerinin görev tanımı ile ilgili bir ilişkilendirme yapılmadığı, suçun hangi mahkeme tarafından bakılacağının belirtilmediği görülecektir. Dolayısı ile yukarıda da arz edildiği üzere görev alanları belirtilmemiş bu suçlara ait yargılamaya genel görevli mahkeme olan asliye ceza mahkemeleri tarafından bakılacaktır. Nitekim uygulamada bu şekilde davalar görülmekle birlikte yargılamaya ilişkin görev yönünden uyuşmazlık çıkmamaktadır.[48]

2.6 Bilişim Suçlarında Yer Yönünden Yetkili Mahkeme:

Bilişim suçlarında yer yönünden yetkili mahkemenin tayininde Ceza Usul Kanunu'nun **12.** maddesinin **1.** ve **2.** fıkraları uygulama alanı bulacaktır.

CMUK MADDE 12:

1- Davaya bakmak yetkisi suçun işlendiği yer mahkemesine aittir.

2- Teşebbüste son icra hareketinin yapıldığı, kesintisiz suçlarda kesintinin yapıldığı yer mahkemesi yetkilidir. Seçimlik hareketli fiiller ile işlenebilen "Bilişim Suçları" teşebbüse de müsait suçlardır. Dolayısı ile yer yönünden yetkili mahkemenin tayininde **CMK 12**. maddenin **1-2**. fıkralarının işlerliği farklı olabilecektir.

48- ASLAN, Fırat, **Bilişim Suçlarında Kovuşturma,**
http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=250, 28.09.2007

A- 243/1-Bilişim Sisteminin Bütününe veya bir kısmına hukuka aykırı olarak girme veya orada kalma; yeni Türk Ceza Kanunu'nun **243.** maddesine yönelik suçun işlenmiş olduğu her durumda yer yönünden yetkili mahkeme genel kural gereği suçun işlendiği yer mahkemesi yani "Bilgileri otomatik işleme tabi tutulmuş sistemin tamamına yada bir kısmına hukuka aykırı olarak girme'' şeklinde gerçekleşen fiilin işlendiği yer mahkemesi olan Asliye Ceza Mahkemesi olacaktır.

243/1. fıkrada belirtilen seçimlik hareketli suçun diğer bir işlenme şekli olan bilişim sistemine girmenin yanında orada kalma şeklinde de işlenebilmesi halidir. Yani sisteme yasa dışı girmek suçu oluştururken sistemde yasa dışı kalmakta suçun oluşumunu sağlayacaktır. Kalmak fiili ise Ceza hukukunda eylem olarak, devam eden, süreklilik (kesintisiz) arz eden hareket gruplarındandır. Dolayısı ile **CMK 12-2.** maddesi gereği "kesintisiz suçlarda kesintinin başladığı yer mahkemesi'' görevli olacaktır.

Teşebbüs halinde ise son icra hareketin yapıldığı yer mahkemesi yer yönünden yargılamayı yapacak olan mahkeme olacaktır.

B- 244/1. madde; Sistemi engelleme, bozma, veri yerleştirme, verileri yok etme, verileri değiştirme; şeklinde birden fazla seçimlik hareketle suçun işlenebileceğini netice itibari ile engelleme, bozma, yerleştirme yok etme, değiştirme fiillerinin işlendiği yer mahkemesi davayı görecektir. Teşebbüse müsait olup **CMK 12.** maddesinin **1.** ve **2**. fıkraları uygulama bulacaktır.

C- 245/1. maddesi; 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; şeklinde tanzim edilen bu suçta cezalandırılan hareket kullanma, kullandırtma sonucu kendisi veya başkasına menfaat temini şeklinde düzenlenmiş olup bu hali ile kullanma kullandırma fiilinin işlendiği yer mahkemesi yargılamada yer yönünden yetkili mahkeme olacaktır.

TCK 245/1. maddaesi, teşebbüsse müsait bir suç tipi olup suçun teşebbüs aşamasında kalması halinde ise genel kural gereği son icra hareketinin yapıldığı yer mahkemesi yer yönünden yetkili mahkeme olacak ve yargılamayı yürütecektir.

D- 245/2. maddesi; Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi; şeklinde düzenlenen bu fıkra **245/1** in ağırlaştırılmış halini tanzim etmiş olup yasa menfaat teminini cezalandırmaktadır. Suç, sahte oluşturulan veya üzerinde sahtecilik yapılan banka yada kredi kartını kullanmak sureti ile kendi yada başkasına menfaat teminin sağlandığı anda oluşacaktır. Suça teşebbüs hali mümkündür. Bu fiilden dolayı yer yönünden yetkili mahkeme sahte veya sahtecik yapılan banka yada kredi kartının kullanıldığı yer fiilin işlendiği yer olarak kabul edilecek dolayısı ile bu yer mahkemesi **CMK 12/1**. maddesi gereği yer yönünden yetkili mahkeme olacaktır.[49]

2.7 Bilişim Suçlarında Delillerin Elde Edilmesi ve Hukuki Durumu:

Bilgisayar delillendirme süreci ilginç ve dikkat gerektiren bir süreçtir. Beş farklı seviyede hard disk sürücüleri, zip diskleri, disketler, CD'ler, DVD'ler ile bilgisayar yedeklemesi yapılabilir. İlk iki yedekleme bilgisayar kullanıcılarına anlamlı gelmeyebilir. Bu iki delillendirme çalışması hassas çalışmayı gerektirir, bilgisayarda yapılan normal çalışmalarda çalışma aygıtında kolaylık ile bozulmalara neden olabilirler. Elektro mıknatıs etki, zarar verici Trojan Horses (Truva Atı) ve virüs, programları ve diğer belirsiz nedenler ile birkaç saniyede bilgisayar delilleri yok olabilir. Bu konu ile ilgili başka benzer delillendirme süreçlerinde bu kadar araştırmacıya potansiyel problem ve zorluk çıkaran başka bir alan bilinmemektedir. Önceleri Amerikan Adli Sisteminde avukatlar ve savcılar delillendirme süreci ile ilgili çok şey bilmiyorlardı.

Bu nedenle savunma konuları çok karmaşık bir durumda idi. Zamanla durumlar değişti ve kanun adamları hukuk alanında elektronik dokümanları keşif etmişlerdir ve zaman değişti, bir şeyleri kitaba göre yapmadan daha önemli hale geldi. Bilgisayar araştırmacıları sadece bilgisayarın sahibi tarafından oluşturulan yıkıcı süreçler ve aygıtlardan endişelenmek ile kalmaz ayrıca, bilgisayar çalışma sistemi ve aygıtlardan endişelenmelidir. Deliller tipik bellek içinde, tablolama programlarında, veri tabanı ve

---

49- ASLAN, a.g.w.s, 28.09.2007

kelime işlem dosyalarında bulunabilir. Ayrıca potansiyel deliller herhangi bir yerde, silinmiş dosyalarda ve Windows'un geçici dosyalarında bulunabilir. Bu gibi deliller Windows'un bilgi parçalarında ve kolaylıkla üzerilerine bilgisayarın yeniden başlatılması ile ve/veya Microsoft Windows'un çalışması ile yazılabilecek durumda bulunur. Windows başladığı zaman potansiyel olarak yeni dosyalar oluşturur ve normal bir süreç olarak var olan dosyayı açar. Bu durum silinmiş dosyaların üzerine yeniden yazılmayı ve Windows'un geçici dosyalarının değişmesine yada bozulmasına sebep olur. Ayrıca Windows normal işletim sürecinde dizin girişlerini günceller, bu noktada tabi ki dosya zaman ve tarihleri delillendirme sürecinde çok önemlidir.

Bilgisayar araştırmacıları için bir diğer sıkıntı, konu olan bilgisayardaki bir diğer programın çalışmış olmasıdır. Suçlular işletim sisteminde standart sistem komutları ile delilleri yok edebileceklerdir. Nitekim bu konuda uygulamalı yapılan eğitimlerde delil olarak düzenlenmiş düzeneğin **"DIR"** komutu ile yok edildiği gösterilmiştir. Yüksek teknolojik bilgilere sahip olan suçlularca (bugün artık bilgisayar okur yazarlığına sahip suçlularca) standart program isimleri ve Windows program ikonlarının fonksiyonları değiştirilip yıkıcı ve ortadan kaldırıcı etkilere sahip olarak oluşturulabiliyor. Bilişim polislerinin kelime işlemcilerden Microsoft Word ve Word Perfect gibi programlara dahi güvenmesi kendi adlarına bir tehlike yaratabilir. Bu programların çalışma anlayışı; kelime işlemci dosyalar açıldığı ve göründüğü zaman, geçici dosyalar kelime işlemci tarafından oluşturulmaktadır. Bu dosyalar geçici dosyalar üzerine daha önceden potansiyel delil olarak kullanılabilecek bölümlerin üzerine yazar.

Bilgisayar delillendirme süreci potansiyel riskler taşıyan bir iştir. Bilgisayar araştırmacılarının omuzlarında bazı kritik materyallerin kayıp olması yada önem arz eden işin devri gibi bir yük yükler. Birçok içsel problem bilgisayar delillerinin üzerinde çalışma sürecinde kayıp olması gibi bir sonuç vermektedir. Bilgisayar delillendirme de bilgisayarı güvene aldıktan sonra ilk yapılacak şey, bilgisayarın bütün bilgilerinin bitlerini içeren yedeklemesinin (bit stream back up) üzerinde çalışmadan ve tekrar gözden geçirmeden yapılmasıdır. Bilgisayar çalıştırılmadan önce bu işlem normal olarak yapılmalıdır. Bütün suç ile ilgili işlemlerde delillerin sunulması öncelikli iştir, bundan bilgisayar delillendirme işlemini soyutlayamayız. Delillendirmenin bu temel kuralı değişmez. Bütün acemilerde bilir ki bedeli ne olursa olsun deliller adalete sunulmalıdır. Yukarıda da belirtildiği gibi deliller çok yönlü düzeylerde ve farklı bellek

konumları içinde bulunabilir. Bu düzeyler tahsis edilmiş dosyalar, silinebilir yada silinmeye uygun dosyaları ifade eder. Hard diskin standart kopyalanmasında bu yeterli olmayabilir. Eğer böyle standart bir yedekleme yapılır ise bilgilerin dosya alanından silinmesi yada bozulması mümkün olabilecektir. Bir alanda delillerin yedeklenmeden üzerinde çalışmak bunları bozabilecek veya üzerinde değişikliklere neden olabilecektir. Standart yedeklemedense bitlerini içeren yedekleme çok daha fazla özenli yedeklemedir. Bit stream yedeklemesi bilgi saklama aracı üzerindeki her bir biti birebir yedekler ve genelde bu işle uğraşanlar orijinal hard diskin iki kopyasını yapmaktadırlar. Hangi süreç denenmek isteniyor ise yedeklenen kopya üzerinde bu işlem yapılabilir. Daha önceden sıkıntı oluşturabilecek delillendirme süreci artık " kolay bir süreç " haline gelir. Unutulmamalıdır ki; bilgisayar delillendirme sürecinde kullanılabilecek sadece bir tek hak vardır, bunu iyi kullanabilmek ancak kullanılan araçlar üzerinde tam hakimiyet ile olabilir.[50]

Suçluların bulunmasında en etkili yöntem delilerin toplanmasıdır. Toplanan her delil sorusturma süresince polise ışık tutacak ve mahkeme aşamasında önemli sonuçlar ortaya koyacaktır. Bilgisayar suçlarında delil niteliği teşkil eden bilgiler ise; yine bilgisayar ortamında tutulmus olan kayıtların olacağı da aşıkardır. Bu kayıtların delil niteliği teşkil edebilmesi için sağlam ve değiştirilemez bir yapıya sahip olması gerekmektedir. Ancak bilgisayarın kullanıcısı tarafından belirlenen yöntemlerle kaydedilen bilgiler yine bilgisayarın kullanıcısı tarafından değiştirilebilme ihtimali taşımaktadır. Böyle olunca sağlam bir delil olmaktan çıkmaktadır. Kanunlarımızda faks çıktıları dahi delil olarak nitelendirilmediği göz önünde bulundurulacak olursa, bilgisayar kayıtlarının ne kadar delil teşkil edip etmeyeceği gözükecektir. Bilişim suçlarında delil niteliği olan sadece bu kayıtlı bilgiler olduğundan dijital delilerin hukuki durumu tartışılması en önemli konulardan biri olmalıdır.

Delilerin elde edilmesi; Ülkemizde dijital kayıtların delil niteliğinin düzenlenmiş olduğunu varsayacak olursak, bu sefer delilerin elde edilmesi problemi karşımıza çıkmaktadır. Internet'e bağlanmak için ya bulunduğunuz kurumun bilgisayar ağına bağlı olmanız, ya bir Internet Servis Sağlayıcıdan hizmet almanız veya bir Internet

---

50- ŞEKER, Güven, **Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması Ve Ülkemizdeki Durum**, http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=295, 07.03.2006

kafeye gitmeniz gerekmektedir.

Tabi bilgisayar üzerinden bir suç işlemeniz içinde bu yerlerden servis alarak Internet'e bağlanmanız gerekir. Böyle olunca suçu işleyen kişiye ait bilgiler sadece buralardan bulunabilir. Ancak ülkemizdeki Internet Servis Sağlayıcıları ve özelikle de Internet kafeler düzenli kayıt tutma işleminin masraflı olmasindan dolayi bu sistemleri kurmamaktadırlar. Bu yüzden emniyet tarafından takip edilen bir soruşturma da kayıtların elde edilmesi aşamasında problem yaşamaktadır. Bu da; suçların yaygınlaşmasında önemli bir rol oynamaktadır. Bu yüzden bu türden Internet servisi veren yerlere en kısa zamanda devlet tarafından belli standartların getirilmesi ve bu konuda sorumluluklar verilmesi gerekmektedir.

2.8 Bilişim Suçları ile İlgili Yargıtay Kararları:

1- Birden ziyade karşı mağdura karşı işlenen bilişim suçlarında TCK'nun **71.** maddesi hükmü gözetilerek mağdurlardan her birine yönelik eylemlerin ayrı ayrı değerlendirilmesi gerekir.

Y.6.C.D.2.2.1999 1999/172-102

a) Sanığın pompacı olarak çalıştığı petrol istasyonundan kredi kartı ile petrol alan müştekinin unuttuğu kartla, müşteki adına değişik tarihlerde petrol almış gibi fişler düzenleyip imzalayarak borçlandırmak suretiyle bankadan tahsil ettiğinin iddia edilmesi karşısında, eylemin sübutu halinde TCK'nun 3679 sayılı Yasa ile değişik **504/3.** maddesinde öngörülen suçu oluşturup oluşturmadığı ve delilleri takdir ve tartışmasının üst dereceli ağır ceza mahkemesinin görevine girdiği gözetilmeden duruşmaya devamla yazılı şekilde karar verilmesi,

b) Kabule göre de; TCK'nun **525/b-2.** maddesine uyan suçların asliye ceza mahkemesinin görevine girdiği gözetilmeden yargılamaya devam edilerek yazılı şekilde karar verilmesi bozmayı gerektirmiştir.

Y.6.C.D. 3.11.1998 1998/9563-9816

(Bu içtihat Karacabey Sulh Ceza Mahkemesinin bilişim suçundan verdiği bir mahkumiyet kararı ile ilgilidir.)

2- Her ne kadar TCK'nun **119.** maddesi uyarınca ön ödeme nedeniyle verilen ortadan kaldırma kararları temyiz incelemesine tabi değilse de müdahil vekillerinin itirazları suç vasfına yönelik bulunması nedeniyle yapılan incelemede:

İddianamede sanığın CINE-5 yayınlarını bir cihazla izinsiz çözerek şifresiz olarak kamuya açık ve aleni biçimde toplu şekilde gösterip izlettirmekte olduğundan **TCK'nun 525/b** son maddesi uyarınca cezalandırılması istemi ile kamu davası açılmış, sanık dekoder sahibi olmadığını, iş yerinde CINE-5 yayınlarını şifresiz olarak başkalarına izlettirmediğini savunmuş, Samsun 3. Noterliğinin 22.10.1995 gün ve 35237 sayılı düzenleme şeklindeki tespit tutanağında ise, 22.10.1995 gününde Samsun Pazar Mahallesi Çiftehamam Caddesi Lezzet Pazarlama Kantariye ve Gıda Maddeleri Lezzet Bisküvileri Karadeniz Bölge Bayisi işyerinde şifresiz olarak televizyonda kalabalık bir müşteri grubuna Fenerbahçe-Galatasaray lig maçının izletildiği saptanmıştır.

Öncelikle yukarıda adı geçen işyeri sahibi ve izlettiren kişinin sanık olup olmadığı araştırılarak, sahibi ve izlettiren kişinin sanık olduğunun belirlenmesi halinde, noter tespitinde belirtilen şifresiz olarak maç izlettirmenin ne anlama geldiği, dekoderin takılı bulunup bulunmadığı, takılı ise dekoderin sanığa veya başkasına ait olup olmadığı, takılı değilse CINE-5 yayınındaki şifrenin ne şekilde çözüldüğü, başka bir araçla kullanılıp kullanılmadığı, çanak antenle izleme hususunun bulunup bulunmadığı araştırılarak sanığın hukuki durumunun tayin ve takdiri gerekirken noksan inceleme ve soruşturma ile yazılı şekilde hüküm kurulması yasaya aykırıdır.

Y.6.C.D. 11.11.1997 1997/10376-10580

3- A) Teknisyen olan sanığın çalıştığı "X-Bar" tipi telefon santralında bazı telefonların "sliv" tellerini kopartarak kontür yazılmasını engelleme ve zaman zaman bu kontürleri elle küçük miktarlarda ilerletip durumu gizlemek ve başkalarına çıkar sağlamaktan ibaret eylemlerinde, "sliv teli-kontür" düzeneğinin bilişim suçlarının konusu olan "bilgileri otomatik işleme tabi tutmuş sistem" olup olmadığının bilirkişiye başvurularak araştırılması ve sonucuna göre:

1) Böyle bir sistem olduğunun saptanması durumunda **TCK'nun 525/b**, 80;

2) Başlı başına bir sistem olmamakla birlikte sisteme veri yerleştirme "input" görevi yaptığının saptanması halinde ise Yasada sözü edilen sistemin dar manada bir

bilgisayar mı, yoksa fizik ve soyut ögelerle birbirini tamamlayan geniş anlamda bir bilişim sistemi mi olduğunun tartışılması ve:

a- Sistemin dar manada ve fiziki olarak bilgisayar anlamına geldiğinin kabulü durumunda sistemin dışında kalan veri yerleştirme düzeneklerindeki eylemlerin bilişim suçu sayılmadığından sanığın eyleminin **TCK'nun 240, 80**;

b- Yasada sözü edilen sistemin geniş anlamda bilişim sistemi olduğunun kabulü durumunda ise sisteme veri "input" sağlayan düzeneklerin de sistemde yer alacağı, dolayısıyla sanığın eyleminin **TCK'nun 525/b, 80;**

3) "Sliv teli-kontür" düzeneğinin ne Yasanın öngördüğü anlamda başlı başına bir sistem ne de böyle bir sisteme veri "input" sağlayan bir öge olduğunun saptanamaması durumunda ise eylemin yine Yasanın **240, 80.**maddelerine gireceği gözetilmeden eksik soruşturma ve yetersiz gerekçeyle yazılı biçimde **(TCK.525/b,80)** hüküm kurulması,

B) Kabule göre de **TCK'nun 525/d.** madde ve fıkrası gereğince meslek ya da sanattan yasaklama cezası verilmemiş olması.

C) Katılan idare vekiline maktu vekalet ücretine hükmedilmemesi yasaya aykırıdır.

Y.4.C.D.24.3.1998 1998/1101-2021

4- Hükümlünün haksız olarak ele geçirdiği müştekiye ait kart ile şifreyi kullanarak para çekme makinesindeki kredi hesabından para çekmesi suretiyle oluşan suç için; süreklilik gösteren Dairemiz içtihatları ve YCGK'nun 11.4.2000 gün ve 2000/6-62-72 sayılı kararında belirtildiği gibi **TCK'nun 525/b-2**. madde ve fıkrası yerine aynı Yasanın 491/3. maddesi ile ceza tayini yasaya aykırıdır.

Y.11.C.D.6.2.2001 2000/5573 2001/991

5- Sanığın, komşuları bulunan Aysun Mercan ve Uğur Belge'ye bankalardan gelen hesap bildirim cetvellerini ele geçirerek bu belgelerdeki bilgilerden yararlanıp, evinde bulunan enkoder cihazı ile kendisine ait kredi kartının manyetik şeridini yeniden kotlamak suretiyle ve Internet yoluyla yurt dışındaki şirketlerden mal siparişinde bulunduğu ileri sürüldüğüne göre:

Öncelikle, İletişim Fakültesi öğretim üyesi, elektronik yüksek mühendisi ve Banka ve Kredi Kartları Merkezinde bu işlerde bilgi ve uzmanlığı bulunan üç kişilik bir bilirkişi kurulu oluşturularak sanığın eyleminde **TCK'nun 525/a** ve **(b)** bentlerinde gösterilen;

a- Bilgileri otomatik olarak işleme tabi tutmuş bir sistemden programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirmek,

b- Bilgileri otomatik işleme tabi tutmuş bir sistemde yer alan bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanmak,

c- Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip etmek veya değiştirmek veya silmek veya sistemin işlemesine engel olmak veya yanlış biçimde işlemesini sağlamak,

d- Bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak,

Durumlarından herhangi birinin veya birkaçının bulunup bulunmadığı kesinlikle tespit edildikten sonra sanığın hukuki durumunun takdiri gerekli iken, uzman olmayan bilirkişinin beyanına dayanılarak eylemin dolandırıcılığa kalkışma olarak kabulü ile **TCK'nun 504/3, 61, 522**. maddeleri ile uygulama yapılması,

Kabule göre de; değerin suç tarihindeki ekonomik koşullara ve paranın satın alma gücüne göre pek fahiş olduğunun gözetilmemesi yasaya aykırıdır.

Y.6.C.D.29.11.2000 2000/4851-8874

6- Sanığın işletmecisi olduğu otelde kime ait olduğu belirlenemeyen dekoderle CINE-5 Filmcilik ve Yapımcılık A.Ş. ile abonelik sözleşmesi olmayan şifresiz yayın izletmek şeklinde oluşan eyleminin hukuki mahiyet arz ettiği gözetilmeden beraatı yerine yazılı şekilde mahkumiyetine karar verilmesi yasaya aykırıdır.

Y.6.C.D.9.11.1998 1998/10188-10082

7- a) Hizmetli olarak çalıştığı bankanın bilgisayar sistemine girerek usulüne uygun açılmış bir maaş kredi limitli bankomat hesabının kredi limitini yükseltmek ve ayrıca kendi adına usulsüz olarak bankomat 7/24 hesabı açmak suretiyle haksız yarar

sağladığı oluşa uygun olarak kabul edilen sanığın eyleminin **TCK'nun 525.** maddesinin **1.** fıkrasındaki suça uygun bulunduğu gözetilmeden, aynı maddenin **2.** fıkrasıyla hüküm kurulması,

b) Sanığın bir suç işlemek kararı ile kanunun aynı hükmünü birinci bentte açıklanan iki ayrı eylemiyle ihlal ettiği anlaşıldığı halde teselsül hükmünün uygulanmaması yasaya aykırıdır.

Y.11.C.D.2.12.1997 1997/5052-6536

8- a) Sanığın, sözleşme ile evinde kullanmak üzere aldığı dekoderi bu sözleşme hükümlerine aykırı olarak başka yerde istifadeye sunmaktan ibaret eyleminin hukuki nitelikte bulunduğu düşünülmeden yazılı biçimde hüküm kurulması,

b) Kabule göre; **TCK'nun 525/b-2**. maddesinde öngörülen cezanın süresine göre, aynı Yasanın **119.** maddesinin olayda uygulama yerinin bulunmadığının gözetilmemesi yasaya aykırıdır.

Y.6.C.D.25.9.1997 1997/8217-8223

9- Sanıkların Yapı Kredi Bankasına ait bankamatiğin paranın çıkmakta olan bölümüne yapışkan bant yapıştırmak suretiyle paranın çıkmasını engellemek ve sonradan buradan almak üzere yakında beklemekten ibaret eylemlerinin bilgileri otomatik işleme tabi tutmuş sisteme teknik anlamda bir müdahale sayılmayacağı gözetilmeden ve bankamatiğin bulunduğu yerin bina vasfında bulunup bulunmadığı da araştırılıp sonucuna göre; **TCK'nun 492/1, 491** ilk maddelerinin tatbiki olanağı da karar yerinde tartışılmadan aynı Yasanın **525/b**. maddesi ile uygulama yapılması yasaya aykırıdır.

Y.6.C.D.11.3.1997 1997/2358-2515

10- Sanığın yarar sağlamak amacı ile çalıştığı bankada bilgileri otomatik işleme tabi sistemde prestige card limitini yükseltip temin ettiği kart ve şifresi ile ATM'lerden birden çok para çektiği, kredi limitini yükseltmek suretiyle sistemi değiştirip yanlış işlemesini sağladığı dosya kapsamından anlaşılmasına göre kül halindeki eylemlerin **TCK'nun 525/b-1, 525/d, 80.** maddelerine uyduğu gözetilmelidir.

Y.6.C.D.23.5.1995 1995/4699-5273

11- Sanığın haksız olarak ele geçirdiği başkasına ait bankamatik kartı ile ATM'den para çekmek istediği, ancak şifreyi bilmemesi karşısında eyleminin **TCK'nun 493/2, 61**. maddelerine uyan suçu oluşturduğu düşünülmeden yazılı şekilde hüküm kurulması yasaya aykırıdır.

Y.6.C.D.5.5.1997 1997/4642-4661

12- TCK'nun 525. maddesinde yazılı suçlara ilişkin kamu davasına bakma görevinin asliye ceza mahkemesine ait olduğu gözetilmeden duruşmaya devamla yazılı şekilde hüküm kurulması yasaya aykırıdır.

Y.6.C.D.9.11.1998 1998/10205-10071

13- Özel Daire ile yerel mahkeme arasındaki uyuşmazlık, sanığın sabit görülen eyleminin TCK'nun 491 ilk maddesindeki hırsızlık suçunu mu, yoksa **TCK'nun 525/b-2.** maddesinde düzenlenen bilişim suçunu mu oluşturduğu hususundadır. 06.04.1990 tarih ve 2/3 sayılı Yargıtay İçtihadı Birleştirme Büyük Genel Kurulu Kararı'nın gerekçesi ve tüm yargı mercilerini bağlayıcı nitelikteki kabulü karşısında; somut olayda sanığın, telsiz telefonuyla müdahilin frekansına girmek suretiyle konuşma yapmak eylemenin "Bilişim Alanında Suçlar" başlığı altında 3756 sayılı Yasayla yeniden düzenlenen **TCK'nun 525.** maddesine göre değil, 491'in ilk maddesine göre cezalandırılması gerekmektedir. Esasen, TCK'nun sonradan değişik biçimde düzenlenmiş **525**. maddesinde, telsiz telefon vasıtasıyla yapılan kaçak konuşmaların bu madde metnine dahil edilip yaptırıma tabi tutulduğuna ilişkin bir ibare de mevcut değildir.

Y.C.G.K 25.6.1996 1996/6-151-152

14- Dava konusu olayda, sanığın çalıntı kredi kartı ile ve kart sahibinin imzasını taklit ederek değişik mağazalardan alışveriş yapmak suretiyle kendisine ve suç ortağına hukuka aykırı yarar sağladığında kuşku bulunmamakla beraber, kredi kartı gösterilmek ve bu kartın geçerliliği belirlendikten sonra sahte imza atılarak yapılan alışverişte **TCK'nun 525/b**. maddesindeki suçun teşekkülü için aranan sistemi kullanma şartının yerine getirildiğini söylemek mümkün değildir. Eylemin bilişim suçu kabul edilebilmesi için aranan husus sistemin kullanılması olup, olayımızda kredi kartının verdiği güvenden istifade ile mağazanın dolandırıldığı, kredi kartının bir kimlik kartı gibi kullanıldığı, yoksa kanun yazıcının amaçladığı anlamda bir sistem kullanılmasının söz

konusu olmadığı görülmekle itirazın kabulü ve itiraza atfen ikinci eylem için suç vasfının dolandırıcılık olacağı kanaatine varılmıştır.

Askeri Yargıtay Daireler Kurulu Kararı 13.10.1994 97/106

15- Sistem-12 santralına bağlı 762 47 42 ve 762 52 32 numaralı telefonların, bilgisayarda bilgilerini değiştirip verilen yeni komut sonucunda kontürlerini durdurarak santral disk ve belleğinde de herhangi bir kayıt tutulmamasını sağlayan sanığın eyleminin **TCK'nun 525/b-1, 251**. maddelerine uyan özel suç niteliğinde olduğu gözetilmeden genel hüküm niteliğinde olan aynı Yasanın **240/1.** maddesi ile karar verilmesi yasaya aykırıdır.

Y.4.C.D.25.2.1998 1998/11798-674

16- Şifrenin müdahil şirkete ait dekoder dışında özel bir alet yardımıyla çözüldüğü saptanmadığına göre, abonelik sözleşmesi ile alınan dekoderi sözleşme hükümlerine aykırı olarak başka yerde istifadeye sunmaktan ibaret eylemin hukuki nitelikte bulunduğu gözetilmeden sanığın hükümlülüğüne karar verilmesi,

Kabule göre de;

a) Uygulanan maddede öngörülen cezanın süresine göre sanığa TCK'nun 119. maddesi uyarınca ön ödeme önerisinde bulunulmaması,

b) Yasa maddesindeki seçimlik cezalardan biri yerine her ikisinin uygulanması yasaya aykırıdır.

Y.6.C.D.29.12.1997 1997/13195-13244

17- CİNE-5 Filmcilik ve Yapımcılık A.Ş. ile abonelik sözleşmesi bulunmayan U.T isimli otelde CINE-5 yayınının izlettirildiği noter aracılığı ile tespit ettirilmiş ise de, bu suretle kullanmanın şifre çözülmek suretiyle olup olmadığı saptanamadığına göre, abonelik sözleşmesi ile alınan dekoderin, sözleşme hükümlerine aykırı olarak başka yerde istifadeye sunulmasından ibaret eylemin hukuki nitelikte bulunduğu düşünülmeden yazılı biçimde hüküm kurulması yasaya aykırıdır.

Y.6.C.D 2.12.1997 1997/11750-11698

18- Sanık, olay günü oynanan Fenerbahçe-Samsunspor maçının naklen yapılan canlı yayınını çanak anten vasıtasıyla uydudan alarak Giresun'daki vericilere

yansıttığını savunmuş bulunması karşısında; mahallinde konusunda uzman bilirkişiler aracılığıyla inceleme yaptırılarak, dekoder kullanılmaksızın CINE-5 yayınının bu suretle elde edilmesinin imkan dahilinde olup olmadığı ve ayrıca dekoder abonesi bulunup bulunmadığı saptanıp, sonucuna göre hukuki durumun tayini gerekirken noksan soruşturma ile yazılı şekilde hüküm kurulması yasaya aykırıdır.

Y.6.C.D.22.6.1997 1997/6043-7210

19- Santral işletme mühendisi A.G.Ö. da dinlenmesi ve sanıkların kabulleri gibi bilgisayara verilmemesi gereken komutlarla dairelere yazım yapmadan, telefonları kentler arası ve 900'lü konuşmalara açıp açmadıklarının saptanması ve sonucuna göre eylemlerinin **TCK'nun 525/b.** maddesine girip girmediğinin tartışılması gerekirken eksik inceleme ve yetersiz gerekçeyle hüküm kurulması yasaya aykırıdır.

Y.4.C.D.20.11.1996 1996/7598-8663

20- Sanığın kamu kurumundan sayılan Ziraat Bankası ile özel banka niteliğindeki Vakıflar Bankasının muhtelif şubelerindeki banka görevlilerini hile ve desiseler yaparak hataya düşürüp daha önce hayali isimlerle açtırdığı hesaplara havale yoluyla para aktarılmasını sağlayarak karşılığını vezneye yatırmadan sahibi olduğu bankamatik kartı ile çekmek suretiyle gerçekleştirdiği dolandırıcılık eylemlerinin **TCK'nun 504/7, 80. ve 503/1, 80**. maddelerine uyan suçları oluşturduğu gözetilmeden aynı Yasanın **525/b.** maddesi ile yazılı şekilde uygulama yapılması yasaya aykırıdır. [51]

Y.6.C.D 11.11.1996 1996/11031-10933

51- ÖZEL, Cevat, **Bilişim-İnternet Suçları**, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm, 08.10.2006

ÜÇÜNÇÜ BÖLÜM

Son bölümde bilişim suçlarının yabancı ülkelerdeki hukuki durumları, mücadele için oluşturulan kuruluşlar yer almaktadır. Bilişim suçlarla mücadele; ülkelerin birlikte çalışma sorumluluğunu da gerektirmektedir. Çünkü servis sağlayacılar ve erişim sağlayıcılar değişik ülkelerde bulunmakla birlikte işlenen suçlar farklı ülkelerde olabilmektedir. Bu durumda suç ve suçlunun tespiti, yakalanması sürecinde mutlak suretle işbirliği lazımdır.

DİĞER ÜLKELERDE BİLİŞİM SUÇLARI ALANINDAKİ HUKUKİ VE İDARİ YAPILANMA

Yeni teknolojilerin geleneksel suçları işlemede kullanılması yeni olan bir kavram değildir. Teknolojik gelişmeler, suç işleyen kişilere yasadışı işler yapmada yeni yollar tanımaktadır. Bilişim suçları da yeni teknolojilerin suç işlemede kullanılmasıdır. Bilgisayar ve iletişim teknolojilerindeki gelişmeler geleneksel suçların işlenmesinde yeni bir araç olmasının yanında yeni suç tiplerinin de çıkmasına sebep olmuştur. Her şeye rağmen şu da göz ardı edilmemelidir ki polis teşkilatları da yeni teknolojileri takip ettikçe ve kullanmaya başladıkça, suçla mücadelede ve vatandaş memnuniyeti yönünde ciddi mesafeler kat etmiştir.

Bugün en karmaşık suç tipleri bilgisayar teknolojileri kullanılarak işlenen suçlardır. Özelikle Internet'in uluslararası bir bilgisayar ağı olması nedeni ile suç ve suçlu ile mücadele de bir çok zorluklar ortaya çıkmaktadır. Teknolojiyi kullanan suçlular veya ileri teknolojiye hakim olup suç işlemeye meyilli insanlar için Internet bulunmaz bir ortam oluşturmaktadır. Internet ve ileri teknoloji ürünü aletler kullanılarak işlenen suçlarda en büyük problem bu insanların kimliklerini tespit etmektir. Internet'in büyüyerek herkesin ilgisini çektiği günümüzde Internet üzerinde işlenen ve işlenecek suçlarla mücadele bütün polis teşkilatlarının öncelikli gündemi haline gelmektedir. Teknolojik gelişmelerin ülke sınırları ile sınırlandırılamadığı günümüzde bu tür suçlarla mücadele içinde uluslararası boyuta işbirliği ve çalışmalar kaçınılmaz hale gelmiştir.

Suçluların teknolojik gelişmeleri kullanarak kazandıkları hızı, polis teşkilatları da yapacakları işbirliği ve geliştirecekleri yeni çalışma sistemleri ile bir an önce kazanmalıdırlar. Bu tip suçlarla mücadelede ulusal düzenlemeler ve yapılanma çok önemlidir ama uluslararası koordinasyon ve işbirliği her zamankinden daha fazla ihtiyaç duyulan hayati bir konu haline gelmiştir.

2000 yılı Şubat ayında Amerika Birleşik Devletleri'nin önemli Internet sitelerine yapılan saldırılar ile hizmet dışı kalmış, bu saldırılar neticesinde (Denial of Service) Yahoo, CNN, E-Bay ve bunun gibi pek çok site hizmet veremez hale gelmiştir. Yine bir kaç ay sonra "I Love You" ve "New Love" virüs saldırıları ile dünya üzerindeki pek çok şirketin bilgisayar sistemlerinde ciddi zararlar meydana gelmiştir. Devlet ve özel kuruluşların vatandaşlara ve müşterilerine daha iyi ve hızlı hizmet verebilmek için her geçen gün daha fazla kullanmaya başladıkları bilgisayar sistemlerini düşünürsek karşılaşılan tehlikenin ne kadar önemli olduğunu anlamakta zorlanılmayacaktır.

"The Computer Security Institut " ve FBI tarafından yapılan bir araştırmada "Bilgisayar Suçları ve Güvenliği" anketine katılan sadece 273 organizasyonun toplam 265.589.940 $ mali kayıpları olduğu tespit edilmiştir. Bunu bilgisayar kullanan şirketlerin dünya çapında ne kadar olduğunu düşünürsek ve yaklaşık üç yüz milyon Internet'e bağlı bilgisayar olduğunu da değerlendirirsek her sene bilgisayar sistemlerine verilen zararlar sonucu milyarlarca dolar zarar edildiği görülecektir. Bilgi çağına girdiğimiz şu dönemde, bilgi teknolojileri günlük iş ve sosyal hayatımızın her alanına girmiş durumdadır. Bu durum kanun uygulayıcı kuvvetler açısından yeni problemler doğurmaktadır. Yukarıda da bahsedildiği gibi geleneksel suçların ileri teknolojinin yardımı ile daha farklı yollardan işlenmesi kanun uygulayıcı kuvvetlerin işini zorlaştırmakta ancak, yine ileri teknolojiler sayesinde kanun uygulayıcı kuvvetler siber suçluların takibini ve yakalamasını gerçekleştirmektedir. Tabi geleneksel suçların yeni yollarla işlenmesi beraberinde yeni suç tiplerinin belirlenmesi ihtiyacını doğurmuş ve ülkelerin bu alanda kanuni düzenlemeler yapmasını gerekli kılmıştır. Aşağıda Interpol vasıtası ile ulusal mevzuatlarına ulaştığımız ülkelerin hukuki durumları ile "Bilişim Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun" tasarısının genel gerekçeleri içerisinde görülmektedir.

Avrupa Birlriği:

Uluslar arası alanda bilişim suçlarıyla ilgili en önemli düzenleme, 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suç Sözleşmesi'dir. Sözleşmeyle, Avrupa Konseyi'ne üye ülkeler arasında ortak ceza politikasının oluşturularak toplumun bilişim suçlarına karşı korunması, bu amaçla ulusal mevzuatlarda gerekli düzenlemelerin yapılarak uluslar arası alanda da işbirliğinin geliştirilmesi amaçlanmıştır.Sözleşmeyle, bilişim alanına ilişkin olarak bir takım terimlerin tanımı yapılmakta, bilişim ortamında veya bilişim ağı sistemleri vasıta kılınarak işlenebilecek suçlar düzenlenerek bu suçların soruşturulması usulüne ilişkin bir takım hükümlere yer verilmektedir. Ayrıca sözleşmeyle uluslar arası işbirliği düzenlenmekte ve bilişim ağında hizmet verenlerin yükümlülüklerine yer verilmektedir.

Avrupa Birliği'nin 8 Haziran 2000 tarihli ve 2000/31/EG "Bilgi Toplumu Hizmetlerinin, Özellikle Elektronik Ticaretin Ortak Pazardaki Bazı Yönleri Hakkında Direktifi" ile 1997/66 ile 2002/58 sayılı "Elektronik İletişimde Kişisel Verilerin İzlenmesi ve Gizliliğinin Korunması Yönergesi" ile üye ülkeler için konu ile ilgili bir takım yükümlülükler öngörmektedir. Avrupa Birliği'nin 2000/31 sayılı "e-ticaret Direktifi" ile bilgi toplumu alanında hizmet verenlerin tabi olacakları hükümler, genel bilgilendirme yükümlülükleri, ticari iletişim için gerekli şartlar, istenmeyen elektronik iletiler, elektronik vasıtalarla yapılacak sözleşmelere uygulanacak kurallar ve sözleşme öncesi verilmesi gerekli bilgiler (özel bilgilendirme yükümlülüğü), ara hizmet sunucularının sorumlulukları ve mesleki davranış kurallarına ilişkin olarak üye ülkelere bir takım sorumluluklar yüklenmektedir.

Avrupa Birliği'nin 2002/58 sayılı "Elektronik İletişimde Kişisel Verilerin İzlenmesi ve Gizliliğinin Korunması Yönergesi" ise; Topluluk içinde elektronik iletişim ekipmanları ile elektronik iletişim vasıtasıyla işlenen kişisel verilerin, temel haklar ve özgürlüklerin korunması ilkesi de dikkate alınarak eşit seviyede korunmaları ve bu şekilde serbest dolaşımlarının sağlanması amaçlanmakta, bu çerçevede elektronik iletişime ilişkin bir kısım tanımlar yapılarak iletişimin gizliliğinin korunması, gerekli

güvenlik tedbirleri, trafik bilgilerinin saklanması gibi konularda hükümler ihdas edilmektedir.

Amerika Birleşik Devletleri:

Uluslar arası alanda bilişim suçlarıyla ilgili olarak ilk kanun tasarısı Amerika Birleşik Devletleri Kongresine 1977 yılında verilmiştir.Amerika Birleşik Devletleri, bilgisayarın anavatanı olması nedeniyle bilişim suçlarıyla ilk defa karşılaşan ülke olmuştur. Bunun doğal sonucu olarak hem öğreti hem yasal düzenlemeler hem de uygulamada ABD merkez ülke konumundadır.

Amerika Birleşik Devletleri'nde ilk defa 1984 yılında "Counterfeit Access Device and Computer Fraud and Abuse Act-Erişim Aygıtlarını Taklit Etme, Bilgisayar Dolandırıcılığı ve Bilgisayarı Kötüye Kullanma Kanunu" ile "Credit Card Fraud Act-Kredi Kartı Sahteciliği Kanunu" yürülüğe girmiş, bu kanunda 1986 yılında "Computer Fraud and Abuse Act-Bilgisayar Dolandırıcılığı ve Köyüye Kullanımı Kanunu" ile değişiklik yapılmıştır.

Amerika Birleşik Devletleri'nde teknolojik suçlar ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır. Bunlardan bazıları şunlardır; FBI National Infrastructure Protection Center-Ulusal Altyapı Koruma Merkezi, Information Technology Association of America-Amerikan Bilgi Teknolojisi Kurumu, Trap and Trace Center Authority-Yakalama ve İzleme Yetki Merkezi, Carnegie Melon's Emergency Response Team ile bazı üniversiteler bünyesinde kurulan birimler bunların en önemlileridir. ABD yönetimi, bu suçlarla mücadelenin gerekliliğini anlayarak Temmuz 1996 yılında "Commission of Critical Infrastructure Protection-Kritik Altyapı Koruma Komisyonu" adlı, ABD başkanına bağlı bir komisyon oluşturmuştur. Bu komisyon, elektronik haberleşme ve bilgisayar ağlarının ABD açısından hayati önem taşıdığını, söz konusu ağların dış saldırılara karşı açık olduğunu, öte yandan, kamu ve özel sektörün mevcut tehditleri ciddiye almadığını belirtmiş ve bu ağların korunması için önlemler alınmasının gerekliliğini savunmuştur. Söz konusu komisyon, suçun takip edilmesi ve araştırılması ile önceden alınacak önlemler konusunda yöntemler tespit etmiştir. Bu komisyon bu alanda çalışma yapan ilk ulusal grup olmuştur.

Bununla birlikte, bir çok kamu kurumu ve kuruluşu bu suçlarla mücadele etmede bazı birimler oluşturmuşlardır. Örneğin; CIA, "Information Warfare Center-Bilişim Mücadele Merkezi" adında ve 1000 kişilik bir personele 24 saat hizmet veren bir birim oluşturmuştur. FBI ise bilgisayar sistemlerine girme ve benzeri suçları takip etmek amacıyla "National Infrastructure Protection Center-Ulusal Altyapı Koruma Merkezi" ve "Computer Crime Squad-Bilgisayar Suçu Ekibi" oluşturmuştur.

Yine Adalet Bakanlığı bünyesinde oluşturulan "Computer Crime and Intellectual Property Section-Bilgisayar Suçu ve Zihinsel Özellik Bölümü" bu alanda çalışmalar yapmakta, gerekli eğitim faaliyetlerinde bulunmakta ve diğer birimlere destek vermektedir.

ABD'de bu suçlarla mücadelede kullanılan kanunların bazıları şunlardır:

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices (Erişim Aygıtlarıyla İlgili Sahtecilik ve Bağlı Eylemler),
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers (Bilgisayarlarla İlgili Sahtecilik ve Bağlı Eylemler),
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems (Sistemlerle, İstasyonlarla veya Hatlarla İletişim),
- 18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral or Electronic

Communications Prohibited (Telli, Telsiz ve Elektronik İletişime Müdahale ve İletişimin Açıklanmasının Yasaklanması),

- 18 U.S.C. § 2701. Unlawful Access to Stored Communications (Depolanmış İletişime Kanunsuz Erişim),
- 18 U.S.C. § 2702. Disclosure of Contents (İçeriğin Açıklanması),
- 18 U.S.C. § 2703. Requirements for Governmental Access (Yasal Erişim İçin Gerekli Şartlar).

Ayrıca bilişim hukuku alanında mevcut düzenlemeler arasında 1986 tarihli "Elektronik Haberleşme Gizlilik Kanunu", 1992 tarihli "Bilgi ve Teknoloji Kanunu, Ulusal Bilgi Altyapısı Kanunu", 1998 tarihli "Çocukların On-line Yayınlardan

Korunması Kanunu", 1997 tarihli "Internette Kumarın Önlenmesi Kanunu", 2001 tarihli "Anti-Terörizm Kanunu", 1996 tarihli "İletişim Ahlak Kanunu" belirtilebilir.

Görüldüğü üzere ABD'de mevzuat alanında bu suçlarla ilgili gerekli önlemler alınmış, bunun yanında kanun uygulayıcı kuvvetlerin bu suçlarla mücadeledeki hak ve sorumlulukların da gerekli düzenlemeler yapmıştır.

Fransa:

Fransa da 1998 yılında yeni teknolojiler kullanılarak işlenen suçların maliyeti 14 milyar FF düzeyine ulaşmış, 1999 yılında ise bu konuda polis ve jandarma makamlarına 3815 olay aksetirilmiştir. Bunların 2450 adedi Internet kullanılarak işlenen suçlardır. Kalan 1336 adedi ise telekomünikasyon sistemlerinin kullanımına aitir. Bu alandaki Fransız Danıştay'ının 1998 yılında Internet konulu yayınladığı raporda, mevcut mevzuatın bilgisayar ortamında işlenen suçlarla mücadeleyi de kapsayacak şekilde geliştirilmesinin yeterli olacağını belirtmiştir. Ancak, bazı özel konularda yeni hukuki çerçevelerin belirlenmesi ihtiyacı doğmuştur. 17 Mart 1999 tarihinde şifreleme sistemi kullanımına ilişkin mevzuata değişiklikler yapılmıştır. Yine 29 şubat 2000 tarihinde elektronik imzaların hukuki değer taşımasına ilişkin bir kanun kabul edilmiştir.

Teknolojik suçlarla mücadele amacıyla devletin birden fazla kurumunda özel birimler kurulmuştur.

- Başbakana bağlı Mili Savunma Genel Sekreterliği (SGDN) bünyesinde kurulan Haberleşme Sistemleri Güvenliği Merkez Birimi (DCSSI),
- Haberleşme Teknolojisi kullanılarak yapılan dolandırıcılıkların soruşturulması birimi (SEFTI),
- Bilgisayar ortamında işlenen suçların bastırılması birimi (BCRCI),
- Jandarma Genel Komutanlığı Seç Araştırmaları Enstitüsü (IRCGN),
- Fransız İstihbarat Örgütü (DST),
- İletişim ve Enformasyon ve Teknolojilerinin Kullanımı Suretiyle İşlenen Suçlarla Mücadele Bürosu.

İrlanda:

İrlanda şu anda ülkede yatırım yapan ABD firmalarının da etkisiyle bilgisayar üretimi, satışı, program yazılımı ve enformasyon teknolojisine yatırım açısından AB'nin en önde gelen ülkesi konumundadır.

İrlanda'da bilgisayar suçları ile mücadele etmek amacıyla 1991 yılında "The Computer Crime Unit-Bilgisayar Suçu Birimi" kurulmuş ve bu tür suçlarla mücadelede yetkili kılınmıştır. Temelde spesifik olarak bilgisayar suçları ile ilgili kanunlar olmasa da, 1991 yılında yasalaşan "Criminal Damage Act-Suçla İlgili Zarar Yasası" bu tür suçlarla ilgili geniş tanımlamalar yapmaktadır. 1991 yılında çıkarılan bu yasa dört temel suçu ortaya koymaktadır.

- Mülkiyete zarar verme (bilgisayarlar ve veriler dahil),
- Mülkiyete zarar vermek amacıyla tehdit etmek,
- Bilgisayara yetkisiz giriş,
- Bilgisayarlara zarar vermek niyetiyle sahip olunan her şey (ör: virüsler),

"Criminal Damage Act" haricindeki diğer kanunlar aşağıda sıralanmıştır:

1. The Copyright Act 1963, (Telif Hakkı Kanunu)

2. The Criminal Evidence Act 1992, (Suç Oluşturan Deliller Kanunu)

3. The Data Protection Act 1988, (Veri Koruma Kanunu)

4. The Postal and Telecommunications Services Act 1983, (Posta ve İletişim Servisleri Kanunu)

5. The Child Traficking and Pornography Act 1998, (Çocuk Ticareti ve Pornografi Kanunu)

Hollanda:

1993 tarihli "Computer Crime Act-Bilgisayar Suçu Yasası" yasalaşmadan önce Hollanda polisi bilgisayar suçları ile mücadele etmek amacıyla özel bir birim kurmuştur. Üç pilot bölgede yapılan başarılı uygulamalardan sonra bölgeler arası bir bilgisayar suçları ile mücadele birimi kurulmuştur. Bilgisayar suçları birimleri Adalet

Bakanlığına bağlı kriminal labaratuarları, "Information Technology and Crime Department of the National Criminal Intelligence Division-Ulusal Suçla İlgili Bölümünün Bilişim Teknolojisi ve Suç Dairesi" ve "Detective's Training Collage-Detektif Eğitim Koleji" ile birlikte çok yakın çalışmalar yapmaktadır. Konunun uzmanları, siber suçlarla ilgili olarak takip edilen yöntemin, diğer suçların işlenişiyle aynı olduğunu, kapsamlı bir uluslararası antlaşmanın olmaması ve suçun hangi ülkeden işlendiğinin tespit edilmesindeki güçlükler nedeniyle, uluslararası alanda mücadele güç olmakla beraber, tespit edilen suçlarla ilgili işbirliğinin adli yardımlaşma çerçevesinde gerçekleştirildiğini ifade etmektedirler.

İspanya:

İspanya'da siber suçlara ilişkin mevzuat Ceza Kanunu ile ilgili maddelerden ibaretir. Söz konusu suçlarla mücadelede şirketler, firmalar ve şahıslar tarafından alınan tedbirler ise bu amaçla hazırlanmış koruma amaçlı yazılımlardan öteye gitmemektedir.

İspanyol Hükümeti yasalardaki düzenlemelere ilaveten, İçişleri Bakanlığı, Emniyet Genel Müdürlüğü bünyesinde bir birim oluşturmuştur. Enformasyon Teknolojilerindeki Suçları Araştırma Birimi adı altında faaliyet gösteren emniyet görevlileri teknoloji, iletişim, telekomünikasyon ve çocuk pornografisi alanlarında işlenen suçları ve ortaya çıkan şikayetleri takip etmektedir. Sadece Madrid'de bulunan merkez büronun yanında bu sene içinde ülke çapında değişik yerlerde de yeni bürolar açılması planlanmaktadır.

İsrail:

İsrail Emniyet Müdürlüğü, bilgisayar üzerinden işlenen suçlar konusuyla 1996 yılından itibaren ilgilenmeye başlamıştır. Sahtekarlık bölümü bünyesinde Bilgisayar Suçları Bölümü kurulmuştur. Anılan bölümdeki görevliler, esasen polis olup bilgisayar konusunda eğitimden geçirilmişlerdir. Bu birim, 1995 yılında yürürlüğe giren Bilgisayar Yasası ve Polis Soruşturma ve Tutuklama Kanunu çerçevesinde görev yapmaktadır. Gerektiğinde diğer polis birimlerince yürütülen soruşturmalara yardımcı olmaktadır.

Bilgisayar üzerinden işlenen suçlara karşı polis tarafından teknik önlemler alınması söz konusu değildir. Bu alanda diğer devlet kuruluşları ve özel şirketlere yardımcı olunmamaktadır. Söz konusu kuruluşlar kendi imkanları ile korunma sistemlerini oluşturmakta ve işletmektedirler.

İsrail hükümeti, bilgisayar suçları ile mücadele konusunda başta ABD olmak üzere, birçok Avrupa ülkesiyle işbirliği anlaşması imzalamış bulunmaktadır.

İsveç:

Konuya ilişkin olarak İsveç'te mevcut yasal düzenlemeler ceza kanunu içerisinde bulunan " Bilgi Hırsızlığı " ve " Bilgi Sistemlerini İhlal Etme Bilgisayarlara Yasadışı Giriş ya da Verileri Kötüye Kullanma " şeklinde tanımlanabilecek suçlara ilişkin hükümlerdir.

İsveç'te bütün devlet kuruluşları bilgisayar güvenliği konusunda kendi önlemlerini almaktadır. Bununla beraber, 1999 yılında hükümet " Ulusal Posta ve Telekomünikasyon Ajansı " na konuyla ilgili ihtiyaçları tespit ve analiz etme talimatı vermiştir. Konu hakkında polisiye birimleri bulunup merkezi bir ekip bu tür suçları bütün ülkede takip ve mücadele etmektedir.

İsviçre:

İsviçre'de siber terörizm ve teknolojik suçlarla mücadeleye ilişkin, "Federal Ceza Yasası" ve "Haksız Rekabet Yasası" adında federal iki yasa mevcutur. "Federal Ceza Yasası" yasal olmayan yollardan teknolojik bilgi edinme, bilgi çalma ve bilgileri bozma gibi suçların cezalandırılmasını içermekte, "Haksız Rekabet Yasası" ise, ticari amaçlı bilgisayar suçlarını içermektedir.

"Federal Ceza Yasası" 143. maddesi kayıt altına alınmış veya elektronik ortamda iletişime konu olan verilerin hırsızlığına ilişkin suçun 5 yıl ve daha fazla süre için hapisle cezalandırılmasını öngörmektedir.

Aynı yasanın 143. maddesi ise, bir bilgisayar sistemine teknik yollar kullanılarak girilmesi suretiyle yapılacak veri hırsızlığının, şikayet üzerine, hapis veya para cezası ile cezalandırılmasını öngörmektedir.

Söz konusu yasanın 147. maddesine göre, bir bilgisayarın yasadışı biçimde eksik ve yanlış veriler kullanılarak etkilenmesi yoluyla sahtecilik amaçlı kullanılması ve bu sayede başkalarına maddi zarar verilmesi durumunda en fazla 5 yıl en az 3 ay hapis cezası verilmesi, suçlunun bu eylemi mesleğini icra ederken yaptığı belirlendiğinde ise 10 yıldan fazla ve 3 aydan az olmamak üzere hapis cezası verilmesi öngörülmektedir.

Norveç:

Norveç'te işlenen bilgisayar suçları ile ilgilenen makam Norveç Adalet Bakanlığı'na bağlı Polis Teşkilatı içinde özel olarak oluşturulan OKOKRIM "Ekonomik ve Çevre Suçları Araştırma ve Soruşturma Milli Otoriter" birimidir. OKOKRIM'a bağlı bilgisayar suçları birimi, bilgisayar mühendisleri, dedektifler ve savcılardan oluşan "multidiscipliner" bir merkezdir. 1993'den bu yana faaliyette olan birim, çeşitli türdeki siber saldırılarının tespiti, soruşturulması ve ortaya çıkarılması, dijital korsanlık gibi konularda büyük tecrübeye sahiptir.

İtalya:

Bilgisayar suçları konusunda en son yasal düzenleme 23 Aralık 1993 tarihinde 547 sayılı kanun ile yapılmıştır.

İtalya'da bilgisayar suçları ile mücadele için 30 Mart 1998 tarihinde Emniyet Genel Müdürlüğü bünyesinde kurulmuş olan "Posta ve İletişim Güvenliği Daire Başkanlığı" bulunmaktadır. Başkanlık bünyesinde Personel Lojistik ve Teknik olmak üzere iki bölüm mevcutur. Taşrada ise 20 ilde doğrudan başkanlığa bağlı olarak görev yapan ofisler bulunmaktadır. Operasyonel işlevi olan teknik bölüm bünyesinde oluşturulan bir çalışma grubunda mühendisler, bilişim teknisyenleri ve örgütlü suç, terörizm, çocuk pornografisi vb. konularda uzmanlaşmış dedektifler görev yapmaktadır.

Bilgisayar üzerinden işlenen suçlar konusunda, ceza yasasında tarif edilen suç teşkil eden eylemler özet olarak aşağıdadır:

• Yazılımları kısmen veya tamamen tahrip eden, değiştiren, bilgi veya iletişim - istemlerinin doğru çalışmasını engeleyen programlarla saldırıda bulunmak (1 milyon liret-500$- kadar para cezası),

• Kamu yararına kullanılan tesislerin, bilgi sistemlerinin, veri, bilgi ve yazılımlarının içeriklerini tahrip etmek ve çalışmasını kesintiye uğratmak (1 yıldan 4 yıla kadar hapis),

• Bilgi veya iletişim sistemlerine fiziki olarak veya yazılım aracılığıyla yetkisiz olarak girmek, bilgi almak, alınan bilgileri yaymak, kayıtlar üzerinde tahribat yapmak veya sisteme maksatlı olarak yeni bilgiler ilave etmek (3 yıla kadar hapis ve 10 milyon liret –5000$-kadar para cezası),

• Her türlü iletişimin engelenmesi, mahremiyetinin, ihlal edilmesi, bu amaçla çeşitli cihaz ve sistemlerin kurularak enformatik ve telematik haberleşmenin kesintiye uğratılması, araya girilmesi veya iletişimin içeriğinin değiştirilmesi,

• Gizli dokümanların içeriğinin açıklanması, gizli kalması gereken kamu veya özel dokümanların içeriğinin yasadışı olarak ele geçirilmesi ve açıklanması (3 yıla kadar hapis ve 2 milyon lirete kadar para cezası).

Bu suçlarla mücadele için Posta ve İletişim Güvenliği Daire Başkanlığı bünyesinde oluşturulan grup, sürekli olarak Internet üzerinde çalışmakta ve ilgili kanunlarda tarif edilen herhangi bir suç unsuruna rastladıklarında çeşitli yöntemlerle suçlular tespit edilerek, suç ve suçlular adli makamlara intikal ettirilmektedir. Dijital ortamda işlenen her türlü suç bu grubun görev alanına girmektedir.

Kanada:

Kanada'da ABD'den farklı olarak, siber terörist saldırılara veya Network sabotajlarına karşı önlemler almakla sorumlu bir hükümet kuruluşu olan FEDCERT (Federal Computer Emergency Response Team-Federal Bilgisayar Acil Karşılık Veren Tim) benzeri bir özel birim bulunmaktadır. Esasen, Kanada enformasyon ağırlıklı bir sisteme sahip olup da bilgisayar olaylarına karşı uluslararası koalisyon durumundaki FIRST (Forum For Incident Response Teams)' e üye olmayan ender ülkelerden biridir. Bununla birlikte, Kanada'da CANCERT (Canadian Computer Emergency Response Team) adı altında benzer işleve sahip bir özel sektör kuruluşu bulunmaktadır. Ayrıca her federal bakanlık ve kuruluşun da ayrı ayrı enformasyon teknolojisi güvenliği politikası ve yöntemleri mevcutur.

Kanada'da siber terörizm ve benzeri teknolojik suçlar halen mevcut ceza kanunu kapsamında işlem görmektedir. Ceza Kanunu'nun 1985 yılından itibaren yapılan değişikliklerle bu tür faaliyetler de suç kapsamına alınmıştır. Ceza Kanunu'nun 342. maddesi uyarınca hakkı olmadan ve sahtekarlık yoluyla elektromanyetik, akustik, mekanik veya başka bir cihaz yoluyla bir bilgisayar sistemini dolaylı veya doğrudan kesintiye uğratan herkes cezai müeyyideyi gerektiren bir suçun faili durumundadır.

Yeni Zelanda:

Teknolojik suçlarla ilgili olarak, 1961 tarihli ceza yasasının yetersizliğinin görülmesi üzerine hazırlanan "Crimes Involving Computers-Bilgisayarları Kapsayan Suçlar" başlıklı yasa değişikliği tasarısı parlamentoya sevk edilmiş ve yıl sonunda onaylanması beklenmektedir. Bununla birlikte bilgisayar suçlarına yönelik polisiye birimler oluşturulmuştur.

Hindistan:

Siber terörizm ve benzeri teknolojik suçlarla mücadele hususunda Hindistan Bilgi ve Teknoloji Bakanlığı tarafından yapılan çalışmalarda üç aşamalı bir yaklaşım izlenmiştir. Birinci aşamada, bu tür suçların önlenebilmesini teminen alınması gerekli fiziki tedbirler belirlenmiş ve kullanıcıların istifadesi için güvenlik rehberi hizmeti verilmeye başlanmıştır. İkinci aşamada, başta Savunma, Dışişleri, İçişleri Bakanlıkları olmak üzere, hassas bilgilere ve teknolojilere sahip bakanlık ve kuruluşları, siber terörizm ve teknolojik suçların yaratabileceği tehlikeler ve bunlara karşı alınacak tedbirler hakkında bilgilendirme çalışmaları başlatılmış ve müteakip aşamada oluşturulacak yasal çerçeve için söz konusu kurumların destek ve deneyimlerine başvurulmuştur. Son aşama yasal çerçevenin hazırlanmasıdır. Bu amaçla aralık 1999'da parlamentoya sunulan yasa tasarısı bahse konu suçların önlenmesi ve bu suçları yasal bir çerçeveye oturtmayı ve devletin bu alandaki kontrol zaafiyetini gidermeyi amaçlamaktadır. Siber ve teknolojik suçlarla ilgilenmek üzere "Bilgi ve Teknoloji Bakanlığı" bünyesinde özel bir grup tesis edilmiştir. Bilgisayar mühendislerinden oluşan bu grup siber ve teknolojik güvenliğin arttırılması çalışmalarını yürütmekte ve kamu kurum ve kuruluşlarının güvenlik programlarının oluşturulmasına yardım etmektedir.

Malezya:

Malezya'da siber suçlarla mücadele; Haberleşme, Multimedya ve Enerji Bakanlığı sorumluluk alanına girmektedir. Malezya'da teknolojik suçlara ilişkin kanunlar:

- Digital Signature Act, (Dijital İmza Kanunu)
- Multimedia Convergence Act,

- Computer Crime Act, (Bilgisayar Suçu Kanunu)
- Telemedicine Development Act,

Bu kanunlarda yer alan bilgisayar suçları da şöyledir:

- Bilgisayarlara izinsiz nüfuz etme, hasar verme,
- Kullanıcı şifresi alışverişi,
- Telif haklarının ihlali,
- Marka sahteciliği,
- Ticari sırları çalma,
- Çocuklara yönelik istismar ve müstehcenlik,
- Internet dolandırıcılığı,
- Internet tacizi,
- Internet'le tehdit, korku, panik, huzursuzluk yayma,

Hükümet ve özel sektör siber suçları, engeleyici teknolojiler geliştirerek, güvenlikli iletişim için uluslararası iletişim ve bilgi teknolojileri standartlarını kullanarak, gizli elektronik işlemleri şifreli olarak ve güvenlik yazılımları kullanmak suretiyle engellemeye çalışmaktadır.

Pakistan:

Pakistan Bilim ve Teknoloji Bakanlığı, ilgili diğer kuruluşlarla işbirliği halinde siber terörizm ve benzeri teknolojik suçları da kapsayacak şekilde bilgisayarlarla ilgili bütün hususları içeren bir yasa oluşturulması üzerinde çalışmaktadır.

Rusya:

Rusya'da bilgisayar üzerinden işlenen suçlar konusunda iki yıl öncesine kadar bir düzenleme bulunmamaktaydı. Ancak, G-8 ülkelerinin 1997 yılında Washington'da yaptıkları Adalet ve İçişleri Bakanları toplantısında kabul edilen bildiri ile "Ulusal Temas Noktaları" oluşturulmasına karar verilmesi üzerine, İçişleri Bakanlığı bünyesinde bir temas noktası oluşturulmuştur. "R dairesi" olarak adlandırılan bu bölüm, ülke içindeki güvenlik ve yargı organları ile ve diğer ülkelerdeki karşıtları ile doğrudan

temas halinde bulunmakta ve uzmanları 24 saat kesintisiz çalışma prensibi uygulamaktadır.

Rusya İçişleri Bakanlığı, İnternet üzerinden suç ve suçluların takibi için delillerin korunması amacıyla Internet hizmeti sağlayan servislerle işbirliği yapmakta, Internet firmalarına verilerini 6 ay saklama ve yargı makamlarının talebi olduğu takdirde söz konusu verileri ilgili makamlara sağlama zorunluluğu getirmektedir.

Singapur:

Singapur Hükümeti, bilgisayar üzerinden işlenen suçlarla mücadele için "Computer Misuse Act-Bilgisayarı Kötüye Kullanma Yasası" ile elektronik ticareti düzenlemek ve işlemleri hukuki zemine oturtmak için "Electronic Transaction Act-Elektronik İşlemler Yasası" nı çıkarmıştır. Singapur'da siber suçlarla aşağıda belirtilen kurumlar ve program aracılığıyla mücadele edilmektedir.

- Singapur Polis Gücü; Yasaların uygulanmasını sağlamaktadır.
- Infocommunications Development Agency'nin Güvenlik Dairesi; siber suçlarla mücadele için gerekli politikaları oluşturmakta ve bu konuda ilgilileri yönlendirmektedir.
- Singapur Computer Emergency Response Team (SINGCERT) ; Kamuoyunu siber saldırılar karşısında uyarmakta, gerekli önlemleri nasıl alabileceklerini bildirmekte, koruma programları tavsiye etmekte, Network önlem niteliğinde kontrol etmekte, saldırı denemeleri olup olmadığını araştırmakta ve siber saldırılardan korunma konusunda halkı ve ilgili kuruluşları bilgilendirmek için seminerler düzenlemektedir. SINGCERT, hükümet ile Singapur Ulusal Üniversitesi'nin işbirliği ile yürüttükleri bir programdır. Siber suçlar Computer Misuse Act'de şu şekilde sınıflandırılmıştır:
- Yetkisiz olarak bir bilgisayara veya sisteme girmek,
- Suça yardımcı olmak maksadıyla veya bu amaçla sisteme girmek,
- Bilgisayarda saklı bilgileri yetkisiz değiştirmek, silmek,
- Bilgisayar kullanımını önlemek ve işlemez hale getirmek,
- Yetkisiz bir bilgisayar hizmetinden yararlanmak,

- Şifreleri çalmak veya bunları açıklamak,

Yukarıda da görüldüğü gibi dünyanın bir çok yerinde ülkeler bilgisayar bilişim suçları hakkında çalışmalar başlatmış bunlarla ilgili gerekli kanuni düzenlemeler yapmış ve bu suçlarla mücadele edecek özel birimler oluşturmuştur.

Ülkemizde hukuki açıdan ideal bir yapı olmamakla birlikte mevcut kanunlar dijital ortamda işlenen suçlarla mücadele için yeterlidir. Fakat dijital ortamda işlenen suçlar kovuşturulurken uzmanlık gerektiren suçlar olduğu için bu alanda ülkemizde de özel birimlerin oluşturulması gerekmektedir. Şuan itibariyle her ne kadar dijital ortamda işlenen suçlar Emniyet Teşkilatı için bir sorun olarak görünmüyor olsa bile önümüzdeki yıllar Internet ve elektronik ticaretin hızla geliştiği ülkemizde bu alanda da suç patlaması olacağı tahmin edilmektedir.[52]

52- DOKURER, a.g.e

Sonuç:

Bilişim suçlarının tanımlanmasına bakıldığı zaman belli bir tanım üzerinde dünyada bir konsesüs oluşmamıştır. Her ülke kendi koşullarına göre tanımlamalar, hukuki ve idari yapılanmalara gitmektedir. Bununla birlikte bilgisayar suçları yada **bilişim suçları** konusunda herkesin ittifak ettiği bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda yaptığı tanımlamadır. Bu tanımlamaya göre bilişim suçları; "Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranıştır"

Bilişim suçlarının tanımını, sınıflandırılmasını, yöntem ve tekniklerini anlamadan onunla mücadele etmenin zorluğu ortadır. Çünkü bu teknik bir konu olmakla birlikte nerdeyse her gün değişebilen ve gelişebilen bir teknoloji kullanılmaktadır.

Bundan dolayı ilk önce bu suçun ne olduğunu bilmek, nasıl işlendiğini anlamak gerektiğinden tanımlamalar, sınıflandırmalar, teknik ve yöntemler incelenmiş daha sonra bu suçlarla ilgili hukuki durumlar ele alınmıştır.

Küreselleşen dünyada paralel olarak bu tip suçlarda gelişmekte, özellikle Internet'le birlikte uluslararası bir boyut kazanmaktadır. Türkiye'de işlenen bir suçun tesbiti bazen diğer ülkelerde yapılmakta bize ise sadece yakalamak düşmektedir.

Yukarıda yapılan çalışmada görüldüğü ve anlaşıldığı üzere bu suçlarla mücadele zor olmakla birlikte suçluların tesbiti, yakalanması bazı durumlarda imkansız hale gelmektedir. Bununla mücadele için mutlak suretle gerekli teknik alt yapıların oluşturulması, gerekli teknik personelin yetiştirilmesi ve sürekli eğitim altında olması gerekmektedir. Ayrıca uluslararası çalışmalarında geliştirilmesi önemli unsurlardan biri olarak karşımıza çıkmaktadır.

Sonuç olarak; Bilişim suçlarıyla mücadele hukuki olarak alt yapısı tamamlanmış ileri görüşlü, teknik donanımlara sahip kadrolarca ve tüm kurumların ortak çalışmalarıyla baş edilebilecek bir özellik taşımakta. Bunun için gerekli çalışmaların ve düzenlemelerin yeniden gözden geçirilerek bu suç türleri bir tek hukuki çatı altında toplanmalı ve teknik kadrolar yetiştirilmeli ve konuyla ilgili birimler oluşturulmalıdır.

KAYNAKÇA

AKARSLAN, Hüseyin: "Bilişim Suçu Kavramı," http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=142&Itemid=28

ASLAN, Fırat: **"** Bilişim Suçlarında Koğuşturma," http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=250

COŞKUN, Özkan: **"**Bilişim Suçlarının İşlenme Şekilleri," http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=251

.

DOKURER, Semih: Emniyet Genel Müdürlüğü, Bilgi İşlem Daire Başkanlığı, Yayınlanmamış Eser

EKER, Mehmet Akif: "Bilişim Suçları, Bilişim Suçlarıyla Mücadele, Türkiye'de Bilişim Suçları," http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=123&Itemid=28

ERSANEL, Nedret: Siber İstihbarat, Hayykitap, İstanbul, Ekim 2005

GENÇ, Gökhan: **"**Bilişim Suçlarına İlişkin Yeni Türk Ceza Kanunu'ndaki Düzenlemeler," http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=252

KODAN, Mahmut: "Bilişim Suçlarının 5846 Sayılı Fikir Ve Sanat Eserleri Kanunu Açısından Değerlendirmesi, Bilişim Suçları," http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=254

.

ÖZCAN, Mehmet: **1.** "Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu," http://www.usakgundem.com/makale.php?id=114

2. "Siber Terör Küresel Tehlike," http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=36&Itemid=29, Kaynak: aksam.com.tr, Pazar, 29 Ocak 2006

ÖZDİLEK, Ali Osman: İnternet ve Hukuk, Papatya Yayıncılık, İstanbul Eylül 2002.

ÖZEL, Cevat: **1. "**Bilişim-Internet Suçları," ,24.12.2002-Bahçe şehir Üniversitesi Sürekli Eğitim Merkezi, cevatozel@mynet.com, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

2. http//www.hukukcu.com/bilimsel/kitaplar/bilisimsuclari_TCKtasarisi.htm

ŞEKER, Güven: **"**Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması Ve Ülkemizdeki Durum," http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=295

Türk Dil Kurumu: Türkçe Sözlük**,** Ankara

YÜZER, Muharrem: **"**Bilişim Suçlarının Yapısı Ve Özelliklerine Bir Bakış,"

http://www.bilisimhukuku.org/modules.php?name=Makale&op=showcontent&id=253

ELEKTRONİK KAYNAKLAR

http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=37&Itemid=29, **Bilişim Suçları ve Siber Terörizm,** inet-tr.org.tr,

http://www.bilgisayarpolisi.com/index.php?option=com_content&task=view&id=36&Itemid=29,Kaynak: aksam.com.tr ,Pazar, 29 Ocak 2006, **Siber Terör Küresel Tehlike,**

http**://**www.egm.gov.tr, **Bilişim Suçları Genel Bilgiler,**

http://forum.flash.gen.tr/archive/index.php?t-559.html, **Bilgisayar Suçları,**

http://www.iad.org.tr/ayinkonusu04.html

http://www.iem.gov.tr/iem/?m=3&s=51#1

http://www.isbank.com.tr/interaktif/i-interaktif-guvenyontem.html