T.C.

RADYO VE TELEVİZYON ÜST KURULU

BİLİŞİM SUÇLARIYLA MÜCADELE YÖNTEMLERİ

UZMANLIK TEZİ

Uğur BOĞA

ANKARA

EKİM/2011

T.C.

RADYO VE TELEVİZYON ÜST KURULU

BİLİŞİM SUÇLARIYLA MÜCADELE YÖNTEMLERİ

UZMANLIK TEZİ

Uğur BOĞA

DANIŞMAN

Muhsin KILIÇ

ANKARA

EKİM/2011

Radyo ve Televizyon Üst Kurulu Başkanlığına

Bu çalışma, Tez Değerlendirme Komisyonu tarafından oy birliği/oy çokluğu ile Uzmanlık Tezi olarak kabul edilmiştir.

	Adı Soyadı	İmza
Başkan	: Taha YÜCEL	.....
Üye	: Volkan ÖZTÜRK	.....
Üye	: Muhsin KILIÇ	.....

ONAY
…./…./……...

Prof. Dr. Davut DURSUN
Üst Kurul Başkanı

TEZ TESLİM TUTANAĞI VE DOĞRULUK BEYANI

Radyo ve Televizyon Üst Kurulunda görev yapan Üst Kurul Uzman Yardımcısı olarak, Radyo ve Televizyon Üst Kurulu Uzman Yardımcılığı Giriş ve Yeterlik Sınavları ile Uzmanlığa Atanma, Yetiştirilme, Görev, Yetki ve Çalışma Usul ve Esasları Hakkında Yönetmeliğin 19 uncu maddesinin 4 üncü fıkrasına istinaden çıkartılan Radyo ve Televizyon Üst Kurulu Tez Hazırlama Yönergesi'ne uygun olarak hazırlamış olduğum uzmanlık tezi ilişikte sunulmuştur.

Bu uzmanlık tezindeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplayıp sunduğumu; ayrıca, bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi beyan ederim.

Bilgilerinizi ve gereğini arz ederim.

…/10/2011

Uğur BOĞA
Üst Kurul Uzman Yardımcısı

Uzmanlık Tezinin Adı:
Bilişim Suçlarıyla Mücadele Yöntemleri

EK:
-Tez (3 adet)

Tezi Teslim Alan

ÖNSÖZ

Bu tezin hazırlanmasında her türlü desteği sağlayan tez danışmanım Sayın Muhsin KILIÇ'a, çalışmalarım esnasında yardımlarını esirgemeyen Sayın Süleyman TEPE, Ahmet AKALIN, Erdem ÇAKMAK, İbrahim ESER'e, bana her konuda destek olan eşim Sayın Sibel AKARSU BOĞA, çocuklarım Umut Emre, Yusuf Emir ve Zeynep Ezgi'ye teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖNSÖZ I
İÇİNDEKİLER II
KISALTMALAR LİSTESİ IV
TABLO ve ŞEKİLLER LİSTESİ VII
GİRİŞ 1
BİRİNCİ BÖLÜM 3
1. BİLİŞİM İLE İLGİLİ TEMEL KAVRAMLAR 3
1.1. BİLİŞİM 3
1.1.1. Bilişim Kavramı 3
1.1.2. Bilişim Sistemlerinin Tarihsel Gelişimi ve Günümüzdeki Konumu 6
1.1.3. İnternet 9
1.1.3.1. İnternetin Tarihçesi 9
1.2. BİLİŞİM SUÇLARI 12
1.2.1. Bilişim Suçunun Tanımı 12
1.2.2. Bilişim Suçlarının Gelişimi 16
İKİNCİ BÖLÜM 20
2. BİLİŞİM SUÇLARININ YAPISI 20
2.1. BİLİŞİM SUÇLARININ SINIFLANDIRILMASI 20
2.1.1. Yetkisiz Erişim 20
2.1.2. Yetkisiz Dinleme 20
2.1.3. Hesap İhlali 21
2.1.4. Bilgisayar Sabotajı 22
2.1.5. Bilgisayar Yoluyla Dolandırıcılık 23
2.1.6. Banka Kartı Dolandırıcılığı 23
2.1.7. İnternet Bankacılığı Dolandırıcılığı 24
2.1.8. Girdi/Çıktı/Program Hileleri 25
2.1.9. İletişim Servislerinin Haksız ve Yetkisiz Olarak Kullanılması 26
2.1.10. Bilgisayar Yoluyla Sahtecilik 27
2.1.11. Bilgisayar Yazılımının İzinsiz Kullanımı 28
2.1.12. Kişisel Verilerin Kötüye Kullanılması 29
2.1.13. Sahte Kişilik Oluşturma ve Kişilik Taklidi 29
2.1.14. Yasadışı Yayınlar 30
2.1.15. Ticari Sırların Çalınması 30
2.1.16. Warez, Cracking ve Hacking Amaçlı Siteler 31
2.1.17. Tv Kartları ile Şifreli Yayınları Çözme 32
2.1.18. Terörist Faaliyetler 32
2.1.19. Çocuk Pornografisi 33
2.1.20. Sanal Kumar 34
2.2. BİLİŞİM SUÇLARININ İŞLENME BİÇİMLERİ 34
2.2.1. Truva 34
2.2.2. Ağ Solucanları 37
2.2.3. Bilgisayar Virüsleri 38
2.2.4. Salam Tekniği 40

2.2.5. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking) 41
2.2.6. Mantık Bombaları 41
2.2.7. Hukuka Aykırı İçerik Sunulması 42
2.2.8. Veri Aldatmacası (Data Diddling) 43
2.2.9. İstem Dışı Alınan Elektronik Postalar (Spam) 44
2.2.10. Çöpe Dalma (Scavenging) 46
2.2.11. Gizlice Dinleme (Eavesdropping-Sniffing) 47
2.2.12. Tarama (Scanning) 48
2.2.13. Süper Darbe (Super Zapping) 49
2.2.14. Gizli Kapılar (Trap Doors) 50
2.2.15. Eşzamansız Saldırılar (Asynchronous Attacks) 51
2.2.16. Sırtlama (Piggybacking) 52
2.2.17. Yerine Geçme (Masquerading) 52
2.2.18. Tavşanlar (Rabbits) 53
2.2.19. Bukalemun (Chameleon) 53
2.2.20. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme 54
2.2.21. Oltaya Gelme (Phishing) 55
ÜÇÜNCÜ BÖLÜM 58
3. BİLİŞİM SUÇLARIYLA MÜCADELE 58
3.1. ÖNLEYİCİ TEDBİRLER 58
3.1.1. Fiziksel Güvenlik 58
3.1.2. Kurumsal Güvenlik 60
3.1.3. Personel Güvenliği 61
3.1.4. İşlemsel Güvenlik 63
3.1.5. Bilgi Güvenliği Standartları 65
3.1.5.1. ISO 27000 66
3.1.5.2. ISO 27001 67
3.1.5.3. ISO 27002 70
3.1.5.4. Cobit 72
3.2. BİLİŞİM SUÇLARININ TÜRK HUKUK SİSTEMİNDEKİ YERİ 73
3.2.1. Mevcut Hukuki Durum 73
3.2.2. Hukuki Düzenlemeler 85
3.3. EGM UYGULAMALARI 86
3.3.1. Genel Çalışmalar 86
3.3.2. İdari Yapılanma 87
3.3.3. KOM Çalışmaları 88
3.4. YAŞANMIŞ ÖRNEKLER 91
3.4.1. Sanal Deprem Operasyonu (2008) 91
3.4.2. Sanal Tuzak Operasyonu (2008) 92
3.4.3. Kimlik Numarası Operasyonu (2010) 93
SONUÇ VE DEĞERLENDİRME 95
KAYNAKÇA 102
EK-1: YARGITAY KARARLARI 107
ÖZET 114
ABSTRACT 115
ÖZGEÇMİŞ 116

KISALTMALAR LİSTESİ

a.g.e.	Adı Geçen Eser
ABD	Amerika Birleşik Devletleri
ANS	İleri Ağ Hizmetleri (Advanced Network Services)
AOL	Amerika Online Şirketi (America Online Incorporated)
ARPANET	Advanced Research Project Authrotiy Net
ATM	Otomatik Para Çekme Makinesi (Automated Teller Machine)
C	Cilt
CD	Yoğun Disk (Compact Disc)
COBIT	Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (Control Objectives for Information and Related Technology)
DARPA	Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency)
DNS	Alan Adı Sistemi (Domain Name System)
DVD	Çok Amaçlı Sayısal Disk (Digital Versatile Disc)
EARNet	Avrupa Akademik Araştırma Ağı (European Academic Research Network)
e-posta	Elektronik Posta
EGM	Emniyet Genel Müdürlüğü
EİK	Elektronik İmza Kanunu
FSEK	Fikir ve Sanat Eserleri Kanunu
GPRS	Genel Paket Radyo Servisi (General Packet Radio Service)
ICCC	Uluslararası Bilgisayar ve İletişim Konferansı (International Conference on Computer and Communication)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
IP	İnternet Protokolü (Internet Protocol)
IRC	İnternet Aktarmalı Sohbet (Internet Relay Chat)
ISACA	Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association)

ISMS	Bilgi Güvenliği Yönetimi Sistemi (Information Security Management System)
ISO	Uluslararası Standartlar Teşkilatı (International Organization for Standardization)
ITGI	Bilgi Teknolojileri Yönetim Enstitüsü (Information Technologies Governance Institute)
İLSİS	İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi
İSS	İnternet Servis Sağlayıcı
Kb	Kilobit
KOM	Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı
Mb	Megabit
MCI	Microwave Communications Incorporated
MEBBİS	Milli Eğitim Bakanlığının Bilişim Sistemleri
MITS	Micro Instrumentation and Telemetry Systems
MIT	Massachusetts Teknoloji Enstitüsü (Massachusetts Institute of Technology)
MMF	Kolay Para Kazanın (Make Money Fast)
NASA	Amerikan Uzay ve Havacılık Dairesi (National Aeronautics and Space Administration)
NCP	Ağ Kontrol Protokolü (Network Control Protocol)
No	Numara
NSF	Ulusal Bilim Vakfı (National Science Foundation)
P2P	Kişiden Kişiye (Peer-to-Peer)
PC	Kişisel Bilgisayar (Personal Computer)
PIN	Kişisel Tanımlama Numarası (Personel Identification Number)
RAM	Rastgele Erişimli Hafıza (Random Access Memory)
S	Sayı
s	Sayfa
SRI	Stanford Araştırma Enstitüsü (Stanford Research Institute)
TADOC	Türkiye Uluslararası Uyuşturucu ve Organize Suçlarla Mücadele Akademisi (Turkish International Academy Against Drug and Organised Crime)

TCK	Türk Ceza Kanunu
TCP/IP	İletim Kontrol Protokolü/Internet Protokolü (Transmission Control Protocol/Internet Protocol)
UBE	Talep Edilmemiş Kitlesel e-posta (Unsolicted Bulk e-mail)
UCE	Talep Edilmemiş Ticari e-posta (Unsolicted Commercial e-mail)
UCLA	Kaliforniya Üniversitesi (University of California), Los Angeles
UCSB	Kaliforniya Üniversitesi (University of California), Santa Barbara
USDoD	Amerika Birleşik Devletleri Savunma Bakanlığı (United States Department of Defense)
VNET	Sanallaştırılmış Ağ (Virtualized Network)
YCGK	Yargıtay Ceza Genel Kurulu

TABLO ve ŞEKİLLER LİSTESİ

Tablolar

Tablo 1 - Erişimi Engellenen Site Sayıları …… 82
Tablo 2 - 2009 Yılında Meydana Gelen Bilişim Suçları Olay ve Şüpheli Sayıları 89
Tablo 3 - Yıllara Göre Bilişim Suçları Olay ve Şüpheli Sayıları …….. 90

Şekiller

Şekil 1 - ISO 27001 standardında bilgi güvenliği döngüsü …… 68
Şekil 2 - ISO 27001 döngüsünün planlama aşamasında ISO 27002 kontrollerinin seçilmesi ……..…… 69
Şekil 3 - ISO 27001 döngüsü ve ISO 27002 kontrolleri ….……...… 71
Şekil 4 - 2009 Yılı Bilişim Suçlarında Operasyon Sayılarına Göre İlk On İl …… 90

GİRİŞ

Teknolojinin 20. yüzyılla birlikte hızlı bir gelişme göstermesi, bilişim sistemlerinin de doğmasını ve bugün insanoğlu için vazgeçilemez bir boyuta ulaşmasını sağlamıştır. Öyle ki sanayi devrimi artık yerini bilişim devrimine bırakmakta, bilgiye sahip olan güce de sahip olmakta ve insanlığa liderlik etmektedir.

Bilişim teknolojileri, bugün itibariyle hayatımızın her alanına nüfuz etmiş durumdadır. Özellikle internetin yaygınlaşması ile küreselleşme hızlanmış, sınırlar kaybolmuştur. Maliyet, rekabet, iletişim gibi konularda sağladığı avantajlar ile bilişlim teknolojilerinin kullanımı her geçen gün hızlı bir şekilde artmaya devam etmektedir.

Bilişim teknolojilerindeki bu hızlı değişim toplumları da beraberinde sürüklemiş, toplumların bilgi toplumlarına dönüşmesini sağlamıştır. En ücra yerleşim yerlerinde dahi bilgiye ulaşma bir lüks olmaktan çıkmış, insanların yaşam tarzını bütünüyle bu yöne kaydırmıştır. Bilişim teknolojilerinin toplum hayatında yoğun olarak kullanılması ile beraber, bilginin saklanması ve işlenmesi gibi konular da önem arz etmeye başlamıştır.

Bilişim teknolojilerindeki hızlı gelişme, insanoğluna sunduğu yararlarla beraber, daha önce karşılaşılmayan yeni suç tiplerini de beraberinde getirmiştir. Gelişen teknoloji insanlığın faydasına kullanıldığı gibi, failler tarafından suç işlemek

üzere de kullanılmaya başlanmıştır. Bu yeni suç tipleri dinamik yapısıyla da klasik suçlardan ayrılmaktadır.

Bu bağlamda, üç bölümden oluşan "Bilişim Suçlarıyla Mücadele Yöntemleri" konulu bu tez çalışmamızın birinci bölümünde, bilişim ile ilgili temel kavramlara yer verilmiştir. Oldukça yeni bir kavram olan bilişim suçlarıyla mücadeleyi etraflıca ele alabilmek için, konuya esas temel öğelerin de tam anlamıyla anlaşılması büyük önem arz etmektedir.

İkinci bölümde ise bilişim suçlarının sınıflandırması yapılmış, bu suçların işlenme biçimleri ele alınmıştır.

Çalışmamızın üçüncü bölümünde, bilişim suçlarıyla mücadelede alınması gereken tedbirler, yapılan ve yapılması gereken hukuki düzenlemeler, Emniyet Genel Müdürlüğü çalışmaları ve bugüne kadar karşılaşılan bazı örnekler sunulmuştur.

Sonuç ve değerlendirme bölümünde ise, bütün bu bilgi ve analizler ışığında, ülkemizde bilişim suçlarıyla mücadelede uygulanması gereken yöntemlerin genel bir değerlendirmesi yapılmıştır.

BİRİNCİ BÖLÜM

1. BİLİŞİM İLE İLGİLİ TEMEL KAVRAMLAR

1.1. BİLİŞİM

1.1.1. Bilişim Kavramı

Bilişim kavramının sözlük anlamı, Türk Dil Kurumu'nun Bilim ve Sanat Terimleri Ana Sözlüğü başlığıyla internet sayfasında şöyle belirtilmiştir: "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim, bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır." [1]

Bilişimin doktrinde de değişik tanımları yapılmıştır. Değirmenci ve Yenidünya bilişimi "teknik, ekonomik, sosyal, hukuk ve benzeri alanlardaki verinin

1 Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü

saklanması, saklanan bu verinin otomatik olarak işlenmesi, organize edilmesi ve değerlendirilmesi ve aktarılmasıyla ilgili bir bilim dalı" şeklinde tanımlamışlardır. [2]

Aydın ise bilişimi, "bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler, bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi ve sibernetik, otomasyon ile insanın çalışma çevrelerinde, yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeler, işlevler süreçler ve etkinlikler" olarak vermektedir. [3]

Yazıcıoğlu'na göre ise bilişim "bilgisayardan da faydalanmak suretiyle bilginin saklanması, iletilmesi ve işlenerek kullanılır hale gelmesini konu alan akademik ve mesleki disipline verilen addır." Yazıcıoğlu, bilişim alanı kavramını da "bilgisayarları da kapsayan ve özellikle bilgisayar ve bu tür aygıtların yer aldığı bir alan" şeklinde ifade etmiştir. [4]

Dülger'in tanımına göre bilişim "insanların teknik, ekonomik, siyasal ve toplumsal alanlardaki iletişiminde kullandığı bilginin, özellikle bilgisayar aracılığıyla düzenli ve akılcı biçimde işlenmesi, her türden düşünsel sürecin yapay olarak yeniden üretilmesi, bilginin bilgisayarlarda depolanması ve kullanıcıların erişimine açık bulundurulması bilimidir." [5]

Özel ise bilişimi "bilgisayarlardan faydalanılarak bilgilerin depolanması, işlenerek başkalarının istifadesine sunulur hale getirilmesi ve iletilmesi faaliyetini,

2 A. Caner Yenidünya, Olgun Değirmenci, Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları, Legal Yayınevi, İstanbul, 2003, s.27
3 Emin D. Aydın, Bilişim Suçları ve Hukukuna Giriş, Doruk Yayınevi, Ankara, 1992, s.3
4 R. Yılmaz Yazıcıoğlu, Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile, İstanbul, 1997, s.131
5 Murat Volkan Dülger, Bilişim Suçları, Seçkin Yayınevi, Ankara, 2004, s. 47

bilgisayar ise bu faaliyetin gerçekleştirilmesinde en önemli etken olan cihaz" olarak açıklamıştır. [6]

Kardaş'ın tanımında ise bilişim kavramı "insan bilgisinin, teknik, ekonomik ve sosyal alanlardaki iletişimin otomatik makinelerde akılcı olarak işlenmesini konu alan bilim" olarak verilmiştir. [7]

Yapılan tanımlar değerlendirildiğinde bilişimin, bilginin teknoloji vasıtasıyla işlenmesi, saklanması ve aktarılması olduğu göze çarpmaktadır.

Bilişim biliminde bilgi geniş anlamlıdır ve verileri de içermektedir. Aydın bu bilim teknoloji dalını veri-işlem olarak tanımlamaktadır. [8] Ancak doktrinde daha yaygın olarak bilgi-işlem olarak isimlendirilmektedir. Kavram karmaşası, İngilizce ''data'' ve ''information'' kelimelerinin Türkçe'ye ''bilgi'' olarak çevrilmesinden kaynaklanmaktadır. İngilizce'de ki ''data-processing'' kavramının Türkçe karşılığı olarak bilgi-işlem kullanılmasına rağmen, esasen ''veri-işlem'' olması gerekmektedir. Aslen ''bilgi-işlem'' ile kastedilen veridir ve bilgi ile karıştırılmaktadır. [9]

Genel olarak tanımlara bakacak olursak bilişimi, her türlü verinin, otomatik olarak işlenmesi, saklanması, organize edilmesi, değerlendirilmesi ve aktarılması ile ilgili bilim dalı olarak tanımlayabiliriz. [10]

---

6 Cevat Özel, Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı, İstanbul Barosu Dergisi, sayı 7-8-9, İstanbul, 2001, s. 858-872
7 Ümit Kardaş, Bilişim Dünyası ve Hukuk, Karizma Dergisi, sayı 13, 2003, s. 8
8 E. Aydın, 1992, s.3
9 Yurdakul Ceyhun, M. Ufuk Çağlayan, Bilgi Teknolojileri Türkiye için Nasıl Bir Gelecek Hazırlamakta, Ankara, 1997, s.7
10 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara

Bu durumda, bilişim bilgi teknolojilerinin tümünü kapsayan bir üst kavram olarak karşımıza çıkmaktadır ve görüldüğü üzere oldukça geniş bir tanıma sahiptir. Öyle ki her bilişim sisteminde mutlaka bilgisayar olması gerekmez ancak her bilgisayar mutlaka bir bilişim sistemi olarak kabul edilebilir. [11]

Türk hukuk mevzuatında bilişim ile ilgili ilk tanımlama 1989 Türk Ceza Kanunu tasarısında yer almaktadır. 1989 Türk Ceza Kanunu tasarısında ‘’bilişim alanı’’ 342nci madde gerekçesinde ‘’...bilgileri toplayıp depo ettikten sonra bunları otomatik olarak işleme tabi tutma sistemlerinden oluşan alan...’’ olarak tarif edilmektedir. [12]

Son olarak 2007 Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısında “bilgi”, “bilgisayar”, “bilişim ağı”, “bilişim ortamı”, “bilişim sistemi”, “veri” gibi tanımlamalar yapılarak kavram karmaşasının önüne geçilmeye de çalışılmıştır. Bu tasarıda da bilişim sistemi; “bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşan veri işleme, saklama ve iletmeye yönelik sistem” olarak tanımlanmıştır.

1.1.2. Bilişim Sistemlerinin Tarihsel Gelişimi ve Günümüzdeki Konumu

Son 45-50 yıldır insanlığın hizmetinde olan bilgisayar, artık hayatımızın vazgeçilmez bir parçası olmuştur. Bankalardan kartlarla para çekebilmemiz, elektronik bilgi-işlemle, telefonlarla kaliteli görüşme yapabilmemiz ve burada sayamadığımız daha birçok kolaylık hep bilgisayar sayesinde hayatımıza girmiştir.

11 M. Dülger, 2004, s. 47
12 TCK Öntasarısı, 2. Komisyon Tarafından Yapılan Değerlendirme Sonucu Hazırlanan Metin, Ankara, Mart 1989, 342. madde gerekçesi

İlk bilgisayar askeri uygulamalarda kullanılmak üzere 1945 yılında Pensilvanya Üniversitesinde üretilmiştir. İlk bilgisayar olan ENİAC için, bugünkü çiplerin atası olan elektronik tüplerden 18.000 adet kullanılmıştır. ENIAC 30 ton ağırlığında, 167 m2 büyüklüğündeydi ve 150 KW güç harcıyordu. ENIAC saniyede 5000 toplama işlemi yapabiliyor fakat aşırı ısınma sebebiyle bir kaç dakika içinde arızalanıyordu. [13]

ENIAC'ın ardından kısa ömürlü olan DEVAC ve ticari anlamda satışa sunulan ilk bilgisayar olan UNIVAC yapılmıştır. Zamanla, elektron tüplerinin yerini önce transistörler, daha sonra da yüzlerce transistörün birleşimi olan entegre devreler almıştır. Bugünkü bilgisayarlarda kullanılan mikroçipler ise bir çok entegre devrenin birleştirilip küçültülmüş halidir.

Zamanla boyutları küçülen bilgisayarın gelişen teknolojiyle beraber fiyatları da düşmüştür. 1975 yılında üniversite ve büyük şirketler dışında kullanılabilecek kadar ucuz ilk bilgisayar ALTAIR 8800, MITS (Micro Instrumentation and Telemetry Systems) şirketi tarafından satışa sunulmuştur. ALTAIR 8800'de ekran yerine oldukça kullanışsız bir panel, klavye yerine ise bir anahtar grubu bulunmaktaydı. Kullanışlı olmasa bile ALTAIR, bilgisayarın herkes tarafından günlük hayatta kullanım için de alınabilecek kadar ucuz olabileceğini göstermesi bakımından önemli bir adımdır.

1977 yılında ilk kez piyasaya çıkan Apple bilgisayarları ise bir evin garajında iki arkadaş tarafından üretilmiştir. Ekran olarak televizyon kullanılmasına rağmen Apple'ın bir klavyesi bulunmaktaydı. Böylelikle herkesin sahibi olabileceği kişisel bilgisayarlar (PC - Personel Computer) dönemi başlamış oldu. [14]

13 M. Dülger, 2004, s. 56
14 Erkan Boğaç, Murat Songür, Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü, Hacettepe-Taş Yayınları, Ankara, 1999, s. 285

70'lerin sonuna doğru kişisel bilgisayarların elektronik sanayisinde yerinin büyük olacağı anlaşılınca, ileride bilgisayar dünyasının mavi devi olarak anılacak olan IBM, 1981 yılında ilk IBM PC'yi piyasaya sürmüştür. Dört yıl içinde bir milyon PC satılmıştır. 1980'lerin ortasında birçok firma IBM gibi bilgisayar üretmeye başlamışlardır. IBM kendi ürününe benzer ürünler üreten firmalarla rekabet etmek zorunda kalmıştır. [15]

Bilgisayarlar kullanım alanlarına göre ikiye ayrılmaktadır. Özel amaçlı bilgisayarlar, hangi amaçla yapıldıysa sadece o alanda hizmet verebilen bilgisayarlardır. Elektronik müzik aletleri, robotlar veya günlük hayatımızdaki elektronik çamaşır makineleri gibi ev araçlarını özel bilgisayarların kullanım alanlarına örnek gösterebiliriz. Genel amaçlı bilgisayarlar, programlanacak her işi yapabilen bilgisayarlardır. Aşağıda bu gruba giren bilgisayarlar sınıflandırılarak anlatılmıştır.

Kişisel Bilgisayarlar (PC veya Mikrobilgisayar): Genellikle tek kişi tarafından kullanılan bilgisayarlardır. Bu yüzden bu bilgisayarlara kişisel bilgisayar yani PC denir. Mikro bilgisayarlar 1970'li yıllardan sonra yaygınlaşmış ve birçok kullanım alanı bulmuştur.

Mini Bilgisayarlar (Frame): PC'nin aksine çok kullanıcılı bir bilgisayar türüdür. Uygun bir klavye ve ekranla en fazla 100 kişi aynı anda kullanabilir. Banka şubelerindeki bilgisayar bu tür bilgisayarlara iyi bir örnektir.

Ana bilgisayar (Main Frame): 100 kullanıcıdan daha fazlasına hizmet veren bilgisayarlardır. Çok büyük işyerlerinde kullanılır.

15 Bilgisayar Ansiklopedisi, Milliyet Yayınları, İstanbul, 1991, s.39-42

Süper Bilgisayar: Kullanıcı sayısı çok olmamakla beraber çok yüksek işlem hızı gerektiren bilimsel çalışmalarda kullanılır. Büyük üniversiteler veya NASA gibi bilimsel kurumlarda kullanılmaktadır.

1.1.3. İnternet

İnternet dünya üzerine yayılan, milyonlarla ifade edilen sayıda bilgisayarların birbirlerine bağlanması ile oluşan ağların ve bu ağların yine birbirlerine bağlanması ile oluşan çok geniş yapıdaki bir ağdır. Bu ağların her geçen gün büyümesi, yeni ağ omurgalarının bu sistemin içine katılması nedeniyle internete "ağlar arası ağ" ya da "ağların ağı" da denilmektedir.

İnternet kişilerin dünya üzerinde birbirleri ile çok geniş amaç ve içerikte iletişim kurmalarını, bilgi alışverişinde bulunmalarını sağlayan ortak iletişim altyapısıdır. Bugün için internete bağlanan bilgisayar sayısı 1 milyarı aşmış olup, internet kullanıcı sayısı ise 2 milyara yaklaşmış bulunmaktadır. [16] Bu da dünya nüfusunun %30'una tekabül etmektedir. Bu oran Avrupa ve Avustralya'da %60'lar seviyesinde iken, Kuzey Amerika'da %80'i bulmaktadır.

1.1.3.1. İnternetin Tarihçesi

İnternetin köklerini 1962 yılında J.C.R. Licklider'in Amerika'nın en büyük üniversitelerinden biri olan Massachusetts Institute of Tecnology'de (MIT) tartışmaya açtığı "Galaktik Ağ" kavramında bulabiliriz. Licklider, bu kavramla küresel olarak bağlanmış bir sistemde isteyen herkesin herhangi bir yerden veri ve programlara erişebilmesini ifade etmiştir.

16 http://www.internetworldstats.com

Licklider 1962 Ekim ayında Amerikan Askeri araştırma projesi olan İleri Savunma Araştırma Projesi'nin (DARPA) bilgisayar araştırma bölümünün başına geçmiştir. MIT'de araştırmacı olarak çalışan Lawrance Roberts ile Thomas Merrill, bilgisayarların ilk kez birbirleri ile 'konuşmasını' ise 1965 yılında gerçekleştirmiştir.

1966 yılı sonunda Lawrence Roberts DARPA'da çalışmaya başlamış ve "ARPANET" isimli proje önerisini yapmıştır. ARPANET çerçevesinde ilk bağlantı 1969 yılında dört merkezle yapılmış ve ana bilgisayarlar arası bağlantılar ile internetin ilk şekli ortaya çıkmıştır. ARPANET'İ oluşturan ilk dört merkez University of California, Los Angeles (UCLA), Stanford Research Institute (SRI), University of Utah ve son olarak University of California, Santa Barbara (UCSB) olmuştur.

Kısa süre içerisinde birçok merkezdeki bilgisayarlar ARPANET ağına bağlanmıştır. 1971 yılında Ağ Kontrol Protokolü (Network Control Protocol - NCP) ismi verilen bir protokol ile çalışmaya başlamıştır. 1972 yılı Ekim ayında gerçekleştirilen Uluslararası Bilgisayar İletişim Konferansı (ICCC- International Conference on Computer and Communication) isimli konferansta, ARPANET'in Ağ Kontrol Protokolü ile başarılı bir demonstrasyonu gerçekleştirilmiştir. Yine bu yıl içinde elektronik posta (e-mail) ilk defa ARPANET içinde kullanılmaya başlanmıştır. Ağ kontrol protokolünden daha fazla yeni olanaklar getiren yeni bir protokol, 1 Ocak 1983 tarihinde İletişim Kontrol Protokolü (Transmission Control Protocol/Internet Protocol - TCP/IP) [17] adıyla ARPANET içinde kullanılmaya başlanmıştır. TCP/IP bugün varolan internet ağının ana halkası olarak yerini almaktadır.

17 TCP/IP bilgisayarlar ile veri iletme/alma birimleri arasında organizasyonu sağlayan, böylece bir yerden diğerine veri iletişimini olanaklı kılan pek çok veri iletişim protokolüne verilen genel addır. Diğer bir ifadeyle, TCP/IP protokolleri bilgisayarlar arası veri iletişiminin kurallarını koymaktadır.

1980'li yılların ortasında ABD Savunma Bakanlığı'na bağlı Amerikan askeri bilgisayar ağı, ARPANET'ten ayrılmış, MILITARY NET adı ile kendi ağını kurmuştur. 1986 yılında Amerikan bilimsel araştırma kurumu 'Ulusal Bilim Kuruluşu' (NSF), ARPANET için ülke çapında beş büyük süper bilgisayar merkezi kurulmasını içeren kapsamlı bir öneri paketi öne sürmüş, daha sonra ARPANET Amerikan hükümetinin sübvansiyonu ile NSFNET olarak düzenlenmiştir. 1987 yılında yeniden düzenlenen internet yapılanması planı ile NSFNET yedi bölgesel nokta üzerinde 1.5 Mb/s (daha önce 56 Kb/s idi) güçlü bir omurgayı işleteceğini duyurmuştur.

NSFNET Merit olarak adlandırılan Michigan Eyaletindeki üniversitelerin organizasyonu ile NSF'in yaptığı bir anlaşma doğrultusunda işletilmeye başlanmıştır. NSFNET'in işletilmesine bir süre sonra Merit'in yanında ABD'nin dev bilgisayar firması IBM ve haberleşme firması MCI dahil olmuştur. NSFNET'in işletilmesine yönelik 1990 yılında oluşturulan bu birlik 'İleri Ağ Hizmetleri' (Advanced Network Services - ANS) olarak adlandırılmıştır. ANS'nin kuruluş süreci, ABD'de 1990'lara kadar devlet desteğinde gelişen internet omurgasının özelleştirilmesi sürecinin de başlangıcı olmuştur.

1990 yılında NSFnet ile özel şirketlerin ortak işletmesi ile başlayan özelleştirme süreci, 1995 yılı mayıs ayında NSF'nin internet omurga işletmeciliğinden tamamen çekilmesi ile tamamlanmıştır. 1995 yılından itibaren ABD internet omurga işletimi tamamen özel işleticilerin elinde bulunmaktadır. [18]

Internet 1990 yılından bugüne kadar ciddi bir oranda büyüme göstermiş, özellikle web sayfası kavramının kullanıma girdiği 1995 yılı içinde büyük bir patlama göstermiştir.

18 http://www.meb.gov.tr/belirligunler/internet_haftasi_2005/internet_tarih.htm (27.06.2010)

Bugün itibariyle internetten hemen her alanda faydalanılmakta, ürünler internetle dünyanın dört bir yanındaki tüketicilere sunulmakta, üniversiteler internet üzerinden öğrenci kaydı kabul etmekte, bazı üniversitelerde dersler ve sınavlar internet üzerinden yapılmakta, bankacılık işlemleri artık yirmi dört saat internet ile hizmete sunulmakta, tapu, nüfus, vergi gibi bürokratik işlemler internet üzerinden yapılabilmektedir.

1.2. BİLİŞİM SUÇLARI

1.2.1. Bilişim Suçunun Tanımı

Bilişim teknolojilerindeki gelişmeler, eğitimden kültüre, ticaretten eğlenceye, devlet sektöründen özel sektöre kadar birçok alanda klasikleşen anlayışı değiştirmiş ve insanlara yeni bir yaşam tarzı getirmiştir. Ancak bütün bu faydalarının yanında bir takım olumsuzluklar da, bu gelişmelerle beraber hayatımıza girmiştir. Klasik suç tanımlarına uymayan yeni bir suç türü olarak bilişim suçları karşımıza çıkmaktadır. Klasik suçların bu sanal dünyada işlenmesinin yanında daha önce hiç karşılaşılmamış suç türleri de bu çerçevede ortaya çıkmıştır.

Doktrinde bilişim suçlarıyla ilgili çeşitli tanımlamalar yapılmıştır. Dönmezer bilişim suçlarının tanımını, bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar şeklinde yapmaktadır. [19]

19 Sulhi Dönmezer, Yeni Türk Ceza Kanunu Öntasarısı - Ceza Hukuku El Kitabı, İstanbul, 1989, s.504

Parker bilişim suçları tanımını, işlendiği takdirde faile çıkar sağlayacak bir şeyler kazandıran ya da kurbana kaybettiren, aynı zamanda bilgisayar kullanımı veya teknolojisi bilgisi içeren herhangi kasıtlı bir davranış olarak vermiştir. [20]

Akbulut ise bilişim suçu olarak, verilerle veya veri işlemle konu bağlantısı olan ve bilişim sistemleriyle veya bilişim sistemine karşı işlenen suçlar biçiminde tanımlama yapmıştır. [21]

Yazıcıoğlu ise bilgisayar suçlarını, ceza kuralları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç olgusu içeren fiiller biçiminde tarif etmektedir. [22]

Bilişim ve bilgisayar arasındaki kullanım benzerliği, bilişim suçu ve bilgisayar suçu kavramlarında da mevcuttur. Aslen bilişim suçu kastedilmesine rağmen bilgisayar suçu kavramı da yaygın olarak kullanılmaktadır. Nitekim Yenidünya ve Değirmenci de bilişim teriminin bilgisayara göre daha geniş bir alanı kapsayıp bir üst kavram olduğunu belirtmekle beraber, bilişim sistemlerinin en yaygın kullanılan unsurunun bilgisayarlar olması nedeni ile "bilgisayar suçu" teriminin yaygınlık kazandığını belirtmişlerdir. [23]

Bilişim suçları, tek bir bilgisayar vasıtasıyla işlenebileceği gibi bir ağ veya internet üzerinde de işlenebilmesi haricinde, ufak bir elektrik devresi ya da bir kredi kartı kullanılarak da yapılabilmektedir. Burada dikkat edilmesi gereken nokta,

---

20 Donn B. Parker (1989), Computer Crime: Criminal Justice Resource Manual'den aktaran, Osman Nihat Şen, Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler, 1. Polis Bilişim Sempozyumu, Ankara, 2003, s.70-71
21 Berrin Bozdoğan Akbulut, Bilişim Suçları, Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, S. 1-2, C8, 2000, s. 551
22 R. Yazıcıoğlu, 1997, s.142
23 A. Yenidünya, O. Değirmenci, 2003, s. 27

bilişim teriminin bilgisayar ve bilgisayar teknolojileri ile iletişim teknolojilerini kapsadığı gibi, bilişim suçları ile kastedilenin de bahsedilen bu teknolojileri kullanarak işlenen tüm suç türleri olduğudur.

Karşımıza çıkan bir başka problem ise, gelişen teknolojiyle birlikte bilişim suçlarının da değiştiği gerçeğidir. Bu sebeple tanımlarda da görüldüğü gibi bilişim suçlarının çizgileri net olarak çizilememektedir. 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 yaygın olan, bu kavramların hepsinin genel olarak "Bilişim Suçu" adı altında adlandırılmasıdır.

Bilişim suçları, çeşitli ülkelerdeki kanun koyucular ve hukukçular tarafından da farklı yaklaşımlarla ifade edilmiştir. Herkesin üzerinde anlaştığı bir tanım yoksa da en geniş kabul gören tanım 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 davranış olarak tanımlanmaktadır.

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. [24]

Görüldüğü üzere bilişim suçları özellikle bilgisayar kullanımıyla ortaya çıkmış, ama daha çok internetin yaygınlaşmasıyla beraber hızla artmıştır. Tanımında ve yapısında henüz net bir uzlaşma sağlanamasa da, elektronik ortamda işlenmesi ve hukuka aykırılık içermesi genel anlamda kabul görmüş unsurlarıdır.

Avrupa Ekonomik Topluluğu tavsiye kararında da görüldüğü üzere, bilişim suçlarının farklı şekillerde işlenebildiği, suçun farklı görünüş biçimlerinin değişik özellikler arz ettiği ortaya koyulmuştur.

Bilişim suçları, doğası gereği insanlara sağladığı özgür iletişim platformuyla birlikte, bireylerin şeref ve haysiyetine yönelecek ihlaller açısından gerçekleştirilmesi çok kolay ancak kontrol edilmesi çok güç olan bir ortamın da ortaya çıkmasını sağlamıştır. Özellikle internet üzerinden yapılan yayınlarla ve hukuk dışı girişimlerle bireylerin hak ve özgürlüklerini hedef alan, kişisel haklarını ihlal eden bir boyuta ulaşması önemli ve çözülmesi zor bir problem olarak karşımıza çıkmaktadır. İnternetin özgür bir iletişim platformu olması ve teknik imkansızlıklar bu suçlarla mücadelede karşılaşılan en büyük güçlükler olarak göze çarpmaktadır.

Bilişim suçlarının temel özelliklerinden birisi de, suçların işlenmesinin oldukça kolay, fakat belirlenmesinin oldukça güç olmasıdır. Çoğu bilgisayar suçunun kurum içi çalışanlar vasıtasıyla ya da kurum içerisinden bilgi alınması suretiyle gerçekleştirilmesi sebebiyle, failin belirlenmesi zor ve takibi oldukça

24 C. Özel, 2001, s. 858-872

güçtür. Bilişim suçları yapısının kesin ve net olarak ortaya konulamaması, yargılamanın da en temel sorunu olarak ortaya çıkmaktadır.

1.2.2. Bilişim Suçlarının Gelişimi

Bilgisayar ve iletişim teknolojilerinin hızla gelişmesi, insan hayatında da önemli değişikliklere sebep olmuştur. İnsanların klasikleşmiş eğitim, kültür, ticaret ve benzeri anlayışları, gelişen bu yeni teknolojilerle tamamen farklı bir boyut kazanmıştır. İnsanlık tarihine farklı bir yön veren bu değişim, her alanda olduğu gibi burada da yeni suç tiplerinin ortaya çıkmasına sebep olmuş ve olmaya da devam etmektedir. Bu hızlı gelişimin imkanlarından herkes gibi suçlular da faydalanmakta ve teknolojinin getirdiği kolaylıkları kullanmaktadırlar. Özellikle 1990'lı yılların başında internetin de büyük bir gelişme kaydederek dünyadaki bilgisayar kullanıcıları arasında bağlantıyı sağlaması nedeniyle suç işlemeye meyilli kişi ve gruplara da yeni suç alanları doğmuştur. [25]

Bilgisayar teknolojisinin gelişmesi, yeni nesil bilgisayarların boyutunun küçülmesi ve maliyetlerinin azalması, bilgisayar kullanıcı sayısında da hızlı bir artışa neden olmuştur. Buna paralel olarak, hemen her alanda yapılan kayıt ve bilgi saklama işlemleri zamanla bilişim teknolojileri ile yapılmaya başlanmıştır. Bilişim teknolojilerindeki bu yaygın kullanım, bilişim teknolojilerindeki suçların da benzer doğrultuda yaygınlık kazanmasına neden olmuştur.

Gelişen teknoloji ile beraber, günümüzde kullanılan bilgisayarlar da suç kavramı ile birlikte anılan bir araç halini almıştır. İnsanlığa getirdiği yararlarla birlikte, yeni ihlal sahalarının da ortaya çıkmasına neden olmuştur.

25 Şükrü Durmaz (2006), Bilişim Suçlarının Sosyolojik Analizi, Gazi Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, Ankara, s. 76

Bilişim ile ilgili suçlar 1960'lı yılların sonuna kadar bilinmeyen bir olguydu. Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır. [26] Son yıllarda da bilişim suçları; bilgisayar programcıları, sistem programcıları, sistem analistleri, operatörleri, teknisyenleri, bilgisayar üreticileri, bilgisayar kullanıcıları, hukukçular, suç araştırmacıları, kısacası tüm bilişim uzmanlarının ve kullanıcılarının ilgisini çekmeye başlamıştır.

İnternetin her kurum ve kuruluş için vazgeçilemez bir imkan olması nedeniyle resmi kurum ve kuruluşların pek çok bilgisayarı bu ağa bağlanmış ve suç işlemeye meyilli kişilerin saldırılarına karşı hedef olmaya başlamıştır. Bilişim suçlularınca bugüne kadar, güvenliğin en üst seviyede tutulduğu bilinen kurumların, askeri ve endüstriyel araştırma laboratuarlarının bilişim sistemlerine sızılmış, pek çok değerli veri çalınmış, zaman zaman kullanıcıların önemli kurumların web sitelerine girmesi engellenmiştir.

Günümüzün kurumlarının faydalanacakları teknoloji alanındaki gelişmeler arttıkça, suçlular içinde gerekli olan teknolojik ilerlemelerin olduğu unutulmamalıdır. Bilişim suçlarında karşımıza çıkan önemli bir unsur da, suçluların doğal olarak kimliklerini gizleme çabalarıdır. Kendi kimliğini gizlemek isteyen suçlular, daha sonra ayrıntılarına gireceğimiz çeşitli tekniklerle, başka kullanıcıların bilgisayarlarını ele geçirip, gerçek kullanıcılarının haberleri bile olmadan bu bilgisayarları kendi işleyecekleri suçlar için birer platform olarak kullanmaktadırlar. Masum kullanıcıların bilgisayarlarına yapılan bu müdahalelerle hem suçsuz insanlar suça ortak edilmekte, hem oluşturulan suçların kapsamı genişletilmekte, hem de suçluların kendilerini daha iyi gizlemesini sağlamaktadır. İnternetin yayılmasıyla birlikte, sistemden sisteme geçiş yapan suçlular, uzun ve karmaşık bir yapı oluşturarak kendi izlerini kaybettirmektedirler. 2001 yılının Kasım ayında "W32.Bad Trans.B-mm" isimli solucan 50 ülkede Nimda solucanının en son

26 http://www.hukukcular.org.tr/makaleler/65-blm-suclari.html (14.04.2010)

versiyonu olarak yaklaşık 840.000 bilgisayarı etkileyerek, toplam olarak en az 7,5 milyon dolar zarara sebep olmuştur.

Genel kullanıma açık olan internet kafelerin, kablosuz internet erişim noktalarının artması, bluetooth, GPRS gibi teknolojilerin ortaya çıkmasıyla beraber, suçlu izi takip etmek neredeyse imkansız bir hal almıştır.

Sistemleri kullanmak ve yönetmek kolaylaştıkça bilişim suçları da işlenmesi uzmanlık gerektirmeyen bir hal almıştır. Öyle ki başka sistemlere müdahale edilmesini sağlayan programlar, internetten rahatlıkla bulunup indirilebilmektedir. Tek bir komut dosyasını çalıştırması bile kimi zaman bu müdahaleler için yeterli olmaktadır. Kurumların uluslararası çalışmaya başlaması, hizmetlerin globalleşmesi ile birlikte, suçlularca bilişim suçlarına olan ilgi de artmaktadır.

Bilişim suçlarıyla meydana getirilebilecek sosyal olaylara örnek olarak internet, telefon gibi haberleşme araçlarının durdurulması, şehir trafik ışıklarının kapatılması, bankacılık ve finans kurumlarının işlem yapmasının engellenmesi, ulaşım hizmetlerinin aksatılması gösterilebilir. Bunlarla birlikte kişi ve kurumlara yaşatılabilecek maddi ve manevi zararlar ise burada sayılamayacak kadar fazla olmasına rağmen, bilişim suçları toplumda halen cinayet, gasp, terör gibi suçların yanında hafife alınmakta, gereken önlem verilmemektedir. Hatta medyada bu suçu işleyenler, bilişim dahisi olarak gösterilmekte, verilen zararlar ve kişiler üzerinde bıraktığı etkiler yeterince anlaşılamamaktadır.

Görüldüğü üzere bugün bilişim suçları geniş bir yelpazeye yayılmış durumdadır. Fakat ülkemizde bilişim suçları, halen adam öldürme, gasp, terör gibi suçların yanında çok ciddi bir suç olarak değerlendirilmemektedir. Yaygın kanı bu suçları çocuk yaştaki veya genç yaştaki kişilerin bir gençlik hevesi ve merakla

işlediği yönündedir. Medyada ve internet üzerinde bilişim suçlarını işleyenler çok zeki, karizmatik insanlar olarak gösterilip efsane haline getirilmektedir. Konu böyle yansıtılırken işin başka bir yönüne ise hiç yer verilmemektedir. Suçun mağdurlarına ne olduğu, nasıl ve ne kadar zarar verildiği, verilen zararların bireyler veya kuruluşlar üzerindeki etkileri veya muhtemel etkileri, geri planda kullanılan teknikler, destekler, hukuki durumun ayrıntılı analizi gibi buzdağının görünmeyen kısmı hep göz ardı edilmektedir.

İKİNCİ BÖLÜM

2. BİLİŞİM SUÇLARININ YAPISI

2.1. BİLİŞİM SUÇLARININ SINIFLANDIRILMASI

2.1.1. Yetkisiz Erişim

Yetkisiz erişim, kişinin bir bilgisayar sistemine ya da bilgisayar ağına yetkisi olmaksızın erişmesidir. Bilgisayar sistem ve verilerinin güvenliğine (yani gizlilik, bütünlük, kullanıma açıklık) yönelik tehlikeli tehdit ve saldırılar şeklindeki temel suçları kapsamaktadır. Suçun hedefi bir bilgisayar sistemi ya da ağıdır. Erişim, sistemin bir kısmına ya da bütününe, programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli olmamakla beraber, bir kişi tarafından bir bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, dolaylı olarak uzak bir mesafeden örneğin bir modem hattı ya da başka bir bilgisayar sisteminden de olabilmektedir. [27]

2.1.2. Yetkisiz Dinleme

Yetkisiz dinleme, bir bilgisayar veya ağ sistemi aracılığıyla yapılan iletişimin yetki olmaksızın teknik anlamda dinlenmesidir.

---

27 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.5

Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferini içerir. İletişim; tek bir bilgisayar sistemi içerisinde, aynı kişiye ait iki bilgisayar sistemi, birbiriyle 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 ya da erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanımı yoluyla) elde edilmesi ile ilgilidir.

Suçun oluşması için hareketin yetkisiz ve niyet edilmiş olarak işlenmesi gerekmektedir. Uygun yasal şartlar çerçevesinde soruşturma mercilerinin yaptıkları dinlemeler bu kategoriye girmemektedir. [28]

2.1.3. Hesap İhlali

Hesap ihlali, herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının dijital hesabının kötüye kullanılmasıdır. Bu tip suçlar normalde geleneksel suçlardaki hırsızlık, dolandırıcılık suçları 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. [29]

28 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.5
29 a.g.e., s.5

2.1.4. Bilgisayar Sabotajı

Bilgisayar sabotajı mantıksal ve fiziksel olmak üzere iki şekilde görülmektedir.

a. Mantıksal (Bilgisayar verilerine zarar verme yada değiştirme)

Mantıksal bilgisayar sabotajı, bir bilgisayar ya da iletişim sisteminin fonksiyonlarını engelleme amacıyla bilgisayar verileri veya programlarının girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir. Bir bilgisayar ya da iletişim sisteminin fonksiyonlarının çalışmasını engellemek amacıyla verilerin ya da programların zaman bombası (logic-time bomb), truva atları (trojan horses), virüsler, solucanlar (worms) gibi yazılımlar kullanarak değiştirilmesi, silinmesi, ele geçirilmesi ya da çalışmaz hale getirilmesidir.

Mantıksal bilgisayar sabotajı özellikle veri ve programların bütünlüğünü bozmayı ya da mevcut verilerin değiştirilmesini amaçlamaktadır. Verilerin yok edilmesi ya da tanınmayacak şekilde değiştirilmesi, fiziksel bir cismin imhasına eşdeğerdir.

b. Fiziksel

Fiziksel bilgisayar sabotajı, bir bilgisayar ya da iletişim sistemine fonksiyonlarını engelleme amacıyla fiziksel yollarla zarar verilmesidir. [30]

30 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s.87.

2.1.5. Bilgisayar Yoluyla Dolandırıcılık

Bilgisayar yoluyla dolandırıcılık, bilgisayar ve iletişim teknolojileri kullanılarak verilerin alınması, değiştirilmesi, silinmesi yoluyla kişilerin kendisine veya başkasına yasadışı ekonomik menfaat temin etmesi veya mağdura zarar vermesidir.

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 ya da mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları suçluların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık göstermektedir.[31]

2.1.6. Banka Kartı Dolandırıcılığı

Banka kartı dolandırıcılığı, bankamatik sistemlerinden yapılan dolandırıcılık ve hırsızlık suçlarıdır. Bankamatik sistemleri (ATM - Automated Teller Machine) genelde bankalar ya da benzeri finans kuruluşları tarafından kullanılmaktadır. Bankamatik sistemleri şifreli ağ sistemlerini kullanırlar. Erişim genellikle bir kişisel tanımlama numarası (PIN - Personel Identification Number) girişi gerektiren bir kart ya da benzeri bir sistem iledir. Dolandırıcılık, bu kartların çoğaltılması, kopyalanması ya da iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur. [32]

31 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.6
32 a.g.e., s.6

Bu suç türünün işleniş biçimi incelendiğinde, sahte kimlik ve belgelerle başkasının hesabından para çekilmesi, banka ve diğer kredi kuruluşlarından verilmemesi gereken bir kredinin sahte evrak kullanılarak veya başka yöntemlerle alınması ortaya çıkabilmektedir. Bahsi geçen başka yöntemler, o çıkar amaçlı suç organizasyonunun etkinliği ölçüsünde değişmektedir. [33]

Bankaların verdiği kredi kartları ile ilgili dolandırıcılıklar da bu suçun kapsamındadır. Suçlular, banka kartları bilgilerine ulaşmak için çeşitli yöntemler kullanmaktadırlar. Bu yöntemler genellikle; alışveriş yada ATM makinelerinin kullanımı sırasında manyetik kopyalama cihazları vasıtasıyla bilgilerin alınması, yine alışveriş yada ATM makinelerinin kullanımı sırasında kart bilgilerinin izlenerek alınması, internet üzerinde bulunan online alışveriş sitelerinin kayıtları elde edilerek buradaki kart sahiplerinin spam mail yoluyla kandırılması, internet üzerindeki sohbet kanalları vasıtasıyla kart bilgilerinin alınması şeklinde olmaktadır.

2.1.7. İnternet Bankacılığı Dolandırıcılığı

İnternet bankacılığı, banka müşterilerinin internet üzerinden bankacılık hizmetleri almasının genel ismidir. Hızla yayılan internet kullanımı ve internet üzerinden alışverişin getirdiği kolaylıklar sebebiyle internet bankacılığı, giderek daha çok kullanılmaya başlanmıştır. İnternet bankacılığı, banka şubesine gitmeden, internet erişimi olan bir bilgisayar aracılığıyla yapılan bir uygulama olup birçok bankacılık işlemini kapsamaktadır. Şubelerdeki kalabalık işlem yükünü azaltan ve personel artışından koruyan, maliyetleri düşüren, kullanıcılara zaman kazandıran bu yeni bankacılık anlayışı gittikçe yaygınlaşmaktadır. Özellikle güvenlik konusunda alınan son önlemler ile hizmet oldukça güvenli hale getirilmiştir. Kredi kartına benzer olarak, sadece alışverişler için tahsis edilen miktar kadar limite sahip sanal

33 Köksal Bayraktar, Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları, Beta Yayınevi, İstanbul, 2000, s.72-73

kart uygulaması da, internet bankacılığı kapsamında verilen hizmetlerden bir tanesidir. [34]

Ancak internet şubeleri üzerinden son zamanlarda artan dolandırıcılık faaliyetleri bu teknolojinin güvenlik boyutunun sorgulanmasına neden olmuştur. Suçlular tarafından phishing [35], e-posta veya keylogger [36] programları aracılığıyla internet bankacılığı kullanıcılarının bilgileri alınmaktadır. Dolandırıcılık, kullanıcının güvenlik eksikliği veya kullanım hatasından olabileceği gibi, banka sistemlerine sızılması şeklinde de olabilmektedir. Kullanıcıların yaşadığı mağduriyetlerin engellenebilmesi için, internet bankacılığı kullanıcılarıyla beraber bankaların da gerekli güvenlik önlemlerini almaları gerekmektedir. Özellikle son yıllarda mahkemelerin, bankaların yeterli güvenlik önlemi almadıkları yönünde verdiği kararlar, bankaların bu yönde yeni güvenlik çözümleri bulma arayışını artırmıştır.

2.1.8. Girdi/Çıktı/Program Hileleri

Girdi/çıktı/program hileleri, bir bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden çıktı almak ya da sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır. Bir bilgisayar veri tabanına yanlış veri girmek yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistemde kullanılan yazılım programlarını da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

---

34 http://tr.wikipedia.org/wiki/%C4%B0nternet_bankac%C4%B1l%C4%B1%C4%9F%C4%B1 (07.06.2010)

35 Phishing: Yemleme, sözcüğü İngilizce "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing sözcüğünün Türkçe karşılığıdır. Yemleme, yasadışı yollarla bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenmeye denir. "Yemleyici" diye tanımlanan şifre avcıları, genelde e-posta vb. yollarla kişilere ulaşır ve onların kredi kartı vb. ayrıntılarını sanki resmi bir kurummuş gibi isterler. Bu "av"a karşılık veren kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır.

36 Keylogger: Kullanıcıların haberleri olmadan klavye tuş dokunuşlarını dinleme metodudur.

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:

a. Satışa açık olan ticari piyasa için yazılmış yazılımlar.

b. Yukarıda belirtilen şekilde alınmış fakat sonradan belli bir amaç için değiştirilmiş yazılımlar.

c. Belirli bir amaç için özel olarak yazılmış ve satışa yada dağıtıma açık olmayan yazılımlar. [37]

2.1.9. İletişim Servislerinin Haksız ve Yetkisiz Olarak Kullanılması

İletişim servislerinin haksız ve yetkisiz olarak kullanılması, kişinin kendisine veya başkasına ekonomik menfaat sağlamak maksadıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerine veya diğer bilgisayar sistemlerine hakkı olmadan girmesidir. Burada iletişim servisleri, değişik şekillerde art niyetli olarak kullanılmaktadır. Fiil bazen yüksek telefon faturalarının önüne geçmek için işlenmektedir. [38]

37 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.7
38 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 30

2.1.10. Bilgisayar Yoluyla Sahtecilik

Bilgisayar yoluyla sahtecilik, kişinin kendisine veya başkasına yasa dışı ekonomik menfaat temin etmek veya mağdura zarar vermek maksadıyla, bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturması veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmasıdır.

Bilgisayarlarda tutulan dokümanlarda (iş akış programları, raporlar, personel bilgileri vs) sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilmektedir. Modern yazılımların güçlendirilmiş grafik kapasitesi, ticari alandaki pek çok belgenin sahtesini yapmayı mümkün hale getirmiştir. Modern teknoloji, özellikle renkli lazer yazıcıların ve fotokopi cihazlarının gelişimi ile daha önceden üretilmesi çok zor olan belgelerin kopyalanmasını mümkün kılmıştır. [39]

Avrupa Konseyi Siber Suçlar Sözleşmesinde de "Bilgisayarlarla İlişkili Suçlar" başlığı altında bu suçlar aşağıdaki şekilde tanımlanmıştır.

Sahtecilik: Verilerin doğrudan doğruya okunabilir ve anlaşılabilir nitelikte olup olmadığına bakılmaksızın, bilgisayar verilerine yeni veriler ilave etme ve bilgisayar verilerini değiştirme, silme veya erişilemez kılma ve böylece orijinal verilerden farklı veriler meydana getirme fiilinin, söz konusu farklı verilerin hukuki açıdan orijinal verilermiş gibi değerlendirilmesi amacıyla, kasıtlı olarak ve haksız şekilde yapılmasıdır.

39 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.7

Sahtekarlık: Sahtekarlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bilgisayar verilerine herhangi bir şekilde yeni veriler ekleme, bilgisayar verilerini herhangi bir şekilde değiştirme, silme veya erişilemez kılma; sahtekârlık yoluyla kendisi veya bir başkasına haksız maddi menfaat sağlamak amacıyla, bir bilgisayar sisteminin işleyişine herhangi bir şekilde müdahale edilmesidir. [40]

2.1.11. Bilgisayar Yazılımının İzinsiz Kullanımı

Bilgisayar yazılımının izinsiz kullanımı, ulusal ve uluslararası telif sözleşmeleri ve yasalarla lisans hakkı korunan yazılım ürünlerinin yetkisiz olarak kopyalanması, çoğaltılması, yayılması ve ticari mevkiye konulmasıdır. Lisanssız yazılım kullanan her kişi aslında telif hırsızlığı yapmaktadır.

Yazılım lisans sözleşmesi belirli bir yazılım ürünü ile ilgisi bulunan ve eser sahibi tarafından izin verilmiş kullanım şartlarını ifade etmektedir. Lisans sözleşmesinde yazılıma sahip olan kullanıcının haklarını belirten ve gerekli düzenlemeleri içeren şartlar yer almaktadır. Bilinmesi gerekli en önemli husus, yazılım kullanan herkesin yasal kullanıcı olduğunu sadece programın orijinal kopyası, kullanma kılavuzu ve lisans sözleşmesi ile ispat edebileceğidir.

Lisanslı yazılım alanlar, orijinal disketlerin başına gelebilecek herhangi bir aksiliğe karşı yedekleme kopyası yapabilirler. Bunun haricinde orijinal yazılımların herhangi bir şekilde çoğaltılmış diğer kopyaları ise izinsiz kopya olarak nitelendirilmektedir. Bu davranış ise, yazılımı ve kullanım haklarını koruyan Fikir ve Sanat Eserleri Kanunu'nun (FSEK) ve lisans sözleşmesinin ihlali demektir.

40 Avrupa Konseyi Siber Suçlar Sözleşmesi, Budapeşte, 2001

Bilgisayar yazılımının izinsiz kullanımı, lisans sözleşmesine aykırı kullanma, sözleşmeye aykırı çoğaltma, sözleşmeye aykırı kiralama, taklitçilik veya izinsiz ithalat şekillerinde olabilmektedir.

2.1.12. Kişisel Verilerin Kötüye Kullanılması

Ticari ya da mesleki sırların, kişisel bilgilerin ya da değerli diğer verilerin kendisine veya başkasına menfaat sağlamak ya da zarar vermek amacıyla bu bilgilerin kullanımı, satılması ve dağıtımıdır. [41]

Müşteri bilgileri, hasta bilgileri gibi banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kendisine ya da başkasına menfaat sağlamak veya zarar vermek amacıyla kişilerin rızası dışında kullanılmasıdır. [42]

2.1.13. Sahte Kişilik Oluşturma ve Kişilik Taklidi

Sahte kişilik oluşturma ve kişilik taklidi, hile yolu ile kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek maksadıyla hayali bir kişilik oluşturulması veya bir başkasının bilgilerini kullanarak onun kişiliğinin taklit edilmesidir.

41 Abraham D.Sofaer, Seymour E.Goodman, The Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution Press, Stanford, 2001, s. 292
42 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 33

Bilgisayar sistemlerine yetkisiz erişim sağlamak ya da kullanma hakkı kazanmak amacıyla gerçek kişilerin taklidi ya da 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. [43]

2.1.14. Yasadışı Yayınlar

Yasadışı yayınların saklanmasında ve dağıtılmasında bilgisayar sistem ve ağlarının kullanılmasıdır. Kanun tarafından yasaklanmış her türlü materyalin web sayfaları, elektronik postalar, haber grupları ve her türlü veri saklanabilecek optik medyalar gibi dijital kayıt yapan sistemler vasıtasıyla saklanması, dağıtılması ve yayınlanmasıdır. [44]

2.1.15. Ticari Sırların Çalınması

Ekonomik kayıp vermek ya da yasal olmayan bir ekonomik avantaj sağlamak niyetiyle yetkisi ya da herhangi bir yasal sebebi olmaksızın uygun olmayan yollarla bir ticari sırrın elde edilmesi, kullanımı, transferi ya da ifşa edilmesidir.

43 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.9
44 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s.93

Bilişim suçları, özellikle suç bir bilgisayardaki saklanmış verileri ilgilendiriyorsa ticari sırların hırsızlığını da kapsayabilmektedir. Ticari sırların çalınması, endüstriyel casusluk olarak da bilinmektedir. [45]

2.1.16. Warez, Cracking ve Hacking Amaçlı Siteler

Warez, cracking ve hacking amaçlı siteler, belirli amaçlar veya ticari kazanç sağlamak için hazırlanmış programların ve yazılımların internet ortamında ücretsiz olarak kolayca temin edilebilmesi ve yazılım şifrelerinin kırılmasını gerçekleştirmek amacıyla oluşturulmuş sitelerdir. Bu sitelerde pek çok programa ve yazılıma ait bilgiler bulmak mümkündür.

Warez: Belirli bir amaç ve ticari kazanç amacıyla yazılmış bilgisayar programların ücretsiz ve sahibinin izni olmadan internet kullanıcılarına sunulduğu sitelerdir. Bu siteler vasıtasıyla bilgisayar programlarının tamamını veya bu programlara ait yamaları bulmak ve yüklemek mümkündür.

Cracking: Belirli bir amaç ve ticari kazanç amacıyla yazılmış bilgisayar programlarına ait yazılım şifrelerinin ücretsiz olarak internet ortamında dağıtıldığı sitelerdir. Bu sitelerde bilgisayar programlarına ait şifrelerin yanı sıra, bu programları çalıştırmak için gerekli şifreleri üreten şifre üreteci programlarını da bulmak mümkündür. Ayrıca bu siteler lisanslı programların şifreleme mantığını ve yapısını çözerek bu programların şifreleri ve anahtarları kırılmış versiyonlarını hazırlayarak çoğaltmakta ve yayımlamaktadır.

45 Interpol Computer Crime Manual'den aktaran Bilişim Suçları Çalışma Grubu Raporu, EGM, s.8

Hacking: Bilişim sistemleri üzerinde, başka sistemlere veya web sitelerine hangi yöntemler kullanılarak zarar verilebileceği, bunun için hangi sistemlerin ve programların kullanılabileceği gibi konularda yayın yapan sitelerdir. Bu suçların işlenmesi için gerekli ortamı ve programları da yayımlayabilen bu siteler, böylelikle kullanıcıları da suç işlemeye teşvik etmektedirler. [46]

2.1.17. Tv Kartları ile Şifreli Yayınları Çözme

Bilgisayar teknolojisinin gelişmesiyle birlikte değişik amaçlı kartlar da buna paralel olarak gelişme göstermiştir. Bilgisayara takılarak kullanılan Tv kartlarının analog ve sayısal yayınları almaya uyumlu hale gelmeleriyle beraber şifreli yayınları çözebilme imkanı da sağlanmıştır. Tv kartları ile birlikte kullanılan ve bu amaç için hazırlanmış şifre çözücü programlar, hem ses hem de görüntü şifrelerini bilgisayar ortamında gerçek zamanlı olarak çözerek bilgisayar üzerinde seyredebilme imkanı sunmaktadırlar. Oysa Tv kanalı sahiplerinin belirli ücretler karşılığı sattığı veya kiraladığı şifre çözücü (decoder) cihazları ile seyredilmesi gereken programlar, bu şekilde ücretsiz olarak izlenmekte ve bilişim suçu işlenmektedir. Ayrıca uydu üzerinden yapılan şifreli yayınları izlemek amacıyla kullanılan alıcılara (receiver) takılan ilave sayısal kartlar ve yüklenen yazılımlar ile şifreli yayınlar çözülebilmektedir. Şifreli Tv yayınlarını çözmeye yarayan bu programların internet ortamında kolaylıkla bulunması da mümkündür.

2.1.18. Terörist Faaliyetler

Terör örgütlerinin propaganda faaliyetlerini, birbirleri ile olan haberleşmelerini, taraftar kazanma, toplumda infial oluşturma gayretlerini,

46 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 34-35

faaliyetlerini başkalarına haklı gösterme çabalarını ve benzeri terörist faaliyetlerini yaymak için gerçekleştirdikleri web siteleri, gönderdikleri elektronik postalar bu kapsamda değerlendirilmektedir. İnternet ortamında faaliyetlerini daha özgür, hiçbir kısıtlamaya tabi olmaksızın gerçekleştiren terör örgütleri, bu web siteleri ve postalar vasıtasıyla kanunlara karşı gelmekte, hatta toplumu kendi lehlerinde yönlendirmeye çalışmaktadırlar.

Terör örgütleri daha önce kitap, doküman, broşür gazete, dergi ve el ilanları vasıtasıyla yaptıkları, terör örgütüne yardım toplamak ve gelir elde etmek, terör örgütünün aldığı kararları ve izleyeceği politikaları yayımlamak, taraftar toplamak ve eleman temin etmek, topluma nifak sokarak bölücülük yapmak ve bunun propagandasını gerçekleştirmek, devletin faaliyetlerini kötüleme, karalama ve hakaret, terör örgütünün eylemlerini yönlendirme, terör örgütünün toplumsal hareketlerini organize etme, toplum nazarında sempati oluşturmaya çalışma, geniş kitlelere hitap etme, baskı yapma ve yaratma gibi eylemlerini bilişim ortamlarına taşımışlardır. [47] Terör örgütleri bununla da yetinmeyip, kamu kurumlarının veya özel şirketlerin bilişim sistemlerine sızmaya çalışarak bu sistemleri işlemez hale getirmeye çalışmaktadırlar.

2.1.19. Çocuk Pornografisi

Çocuk pornografisi, genel anlamda 15 yaş altındaki kız ve erkek çocuklarının cinsel istismarını içeren filmler ve resimlerden oluşan, uluslararası olarak da yasaklanmış olan zararlı pornografi türüdür. Avrupa Konseyi Siber Suçlar Sözleşmesinde çocuk pornografisi, cinsel anlamda müstehcen bir eyleme reşit olmayan ya da reşit görünmeyen bir kişinin katılımını gösteren görüntüler olarak

47 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 36

tanımlanmıştır. [48] Özellikle internetin bir pornografi yayın aracı olarak hızla yaygınlaşması, bu işin kirli yönleriyle uğraşanlar tarafından çocukların daha da çok şiddete ve uygunsuz cinsel ilişkiye maruz tutulmalarına sebep olmuştur. İnternetteki sohbet gruplarının sağladığı anonimlik hakkından istifade ile bu ortamlarda bu tür materyaller fütursuzca kullanılabilmektedir. Özellikle günümüz internet paylaşım araçlarının en çok kullanılan peer-to-peer (P2P) [49] yazılımları çocuk pornografisi işinde kullanılmakta ve bu yazılımların kullanıcı sayıları günden güne artmaktadır.

2.1.20. Sanal Kumar

Şansa ve beceriye dayanan, oyun araç ve gereçleri ile veya bir kasaya karşı para veya benzeri maddi değerler karşılığı oynatılan oyunların bilişim ortamları kullanılarak gerçekleştirilmesidir. Özellikle internet kullanımıyla yaygınlaşan sanal kumar için, online kumar, e-kumar, internette kumar, online casino gibi ifadeler de kullanılmaktadır.

2.2. BİLİŞİM SUÇLARININ İŞLENME BİÇİMLERİ

2.2.1. Truva

Mitolojideki truva atına benzer şekilde, truva programları da yararlı yazılımlar gibi görünmekte, ancak gerçekte güvenliği tehlikeye atmakta ve pek çok zarara yol açmaktadırlar. Truvalar, insanların meşru bir kaynaktan geldiğini düşündükleri bir programı açmaya yöneltilmeleri yoluyla yayılır.

48 Avrupa Konseyi Siber Suçlar Sözleşmesi, Budapeşte, 2001
49 Peer-to-peer: İki veya daha fazla istemci arasında veri paylaşmak için kullanılan bir ağ protokolüdür.

Truvalar bilişim sistemlerine, herkesin kullanımına açık bilişim sistemleri ağlarından veya internet üzerinden herhangi bir web sayfasından kopyalanarak girerler. Truvalar genellikle kullanıcıları cezbedecek isimler altında bulunduklarından dolayı, kullanıcılar kolaylıkla programları sistemlerine bulaştırabilmektedirler. Bilgisayar kullanıcıları tarafından sıklıkla kullanılabilecek yararlı bir yazılıma truva atı programı da eklenebilmekte, bu yolla truvaların birçok bilgisayara ve sisteme bulaşması sağlanmaktadır. Truvaların yayılmasını hızlandırmak için bu programlar internet üzerinden ücretsiz olarak dağıtılmakta veya elektronik posta yoluyla kullanıcılara gönderilebilmektedir. Kullanıcı programın yararlı işlevlerinden istifade etmekte ve hiçbir şeyden şüphelenmemektedir. Bu yazılımı bilgisayarına yükleyen kullanıcı, yazılımın görünüşte yararlı olan tarafından faydalanmaktadır. Bu arada truva atı yazılımı da kurulmuş olduğu bilgisayarın işletim sistemi açıklarından istifade ederek, kendisini gönderenin tüm komutlarını yerine getirmektedir.

Truva atları, virüsler gibi sisteme zararlı yazılımlardır. Ancak virüsler gibi kendi kendilerine çoğalamazlar.

Bir truva atı sisteme bulaştıktan sonra, kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren tarafa bilgi gönderir veya onun isteklerine cevap verir. Bir truva atı iki kısımdan oluşur. Birinci kısım hedef bilgisayarda çalışan sunucudur. İkinci kısım ise müdahalede bulunan bilgisayarda çalışan istemcidir. Hedef bilgisayara yerleştirilen sunucu programların boyutu küçüktür. Küçük olması sayesinde, başka programların sonuna rahatlıkla eklenebilmekte ve tespit edilmesi güç olmaktadır. Sistemin çalışmasıyla aktif olmakta ve istenen bilgileri truvanın gerçek sahibine göndermektedirler.

Her truva atı programı kendisine uzaktan verilen komutlarla farklı farklı işlemler yapabilirler. İnternet üzerinde en yaygın truvalardan Back Orifice 2000

programı sayesinde; hedef bilgisayarın sabit diskleri ve harici sürücülerine girilebilir, dosyaları değiştirilebilir ya da silinebilir, bilgisayarlar arasında istenen dosyalar karşılıklı gönderilebilir, hedef bilgisayar ekranına çeşitli mesajlar gönderilebilir, hedef bilgisayar kapatılabilir, giriş şifresi gibi önemli bilgiler müdahale eden bilgisayara gönderilebilir. [50]

Truva atı içeren programlar genellikle internet üzerinden serbest olarak dağıtılmaktadırlar. Kullanıcıların birbirlerine e-posta aracılığıyla gönderdiği programlar da truva atı taşıyıcıları olabilirler. Kullanıcı bu programlardan herhangi birini çalıştırdığı anda, truva programı arka planda çalışıp kendisini gönderen bilgisayarla iletişime geçmekte, programı bulunduğu sisteme yüklemekte ve sistemin her açılışında çalıştırılmasını sağlamaktadır. Tüm bunları yaparken normal bir program gibi yapması gerekenleri de yapmakta ve kullanıcıların şüphesini çekmemektedirler. [51]

Truva saldırısı, ilk olarak 9 Aralık 1987'de Almanya'da Clasuthal-Zellerfield Üniversitesi'nde öğrencilere Christmas (Noel) adlı bir elektronik postanın gönderilmesiyle gerçekleşmiştir. Elektronik posta içeriğinde "Bırakın bu exec işlesin ve keyfinize bakın" mesajı yazmakta ve devamında tırnak işaretleriyle oluşturulmuş bir noel ağacı resmi bulunmaktaydı. Resmin altında "sadece Christmas yazın" şeklinde bir mesaj daha bulunmaktaydı. Kullanıcı "Christmas" yazması durumunda ekranda bir noel ağacı resmi oluşmaktaydı. Dosya daha sonra kullanıcı tarafından silinmesine rağmen, bilgisayarın her açılışında dosyanın bir kopyası yine bilgisayarda durmaktaydı. Program sadece noel ağacı resmi çizmemiş, bilgisayardaki elektronik adres defterini kontrol etmiş, adres defterindeki diğer kişilere de kendi kopyasını göndermişti. Bu adres defterinde üniversitedekilerden başka Avrupa Akademik Araştırma Ağı (EARNet) ile de bağlantılı bulunan

50 M. Dülger, 2004, s. 70
51 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara

elektronik adresleri bulunmakta idi. Program 15 Aralıkta IBM şirketinin dünya çapındaki özel elektronik posta ağı VNET'e ulaştı ve ağdaki işleri durma noktasına getirdi. Bu program şimdiki truva programlarının atası sayılmaktadır. [52]

2.2.2. Ağ Solucanları

Solucanlar da, virüs gibi kendisini bir bilgisayardan diğerine kopyalamak için tasarlanmıştır ancak bunu otomatik olarak yapar. İlk olarak, bilgisayarda dosya veya bilgi ileten özelliklerin denetimini ele geçirir. Solucan bir kez sisteme girdikten sonra kendi başına ilerleyebilir. Solucanların en büyük tehlikesi, kendilerini büyük sayılarda çoğaltma becerileridir. Örneğin bir solucan, e-posta adres defterindeki herkese kopyalarını gönderebilir ve sonra aynı şeyi onların bilgisayarları da yapabilir. Bu domino etkisinin getirdiği yoğun ağ trafiği işyeri ağlarını ve internetin tümünü yavaşlatabilir. Yeni solucanlar ilk ortaya çıktıklarında çok hızlı yayılırlar. Ağları kilitlerler ve genellikle internetteki web sayfaları görüntülenirken uzun süre beklenmesine yol açarlar.

Solucan, virüslerin bir alt sınıfıdır. Bir solucan genellikle kullanıcı eylemi olmaksızın yayılır ve kendisinin tam kopyalarını ağlardan başka ağlara dağıtır. Bir solucan bellek veya ağ bant genişliğini tüketebilir, bu da bilgisayarın çökmesine yol açabilir.

Solucanlar yayılmak için bir taşıyıcı programa veya dosyaya gereksinim duymadıklarından, sistemde bir tünel açıp, başka birinin uzaktan bilgisayarın denetimini eline geçirmesini sağlayabilir. Yakın geçmişteki solucanlara örnek olarak Sasser solucanı ve Blaster solucanı verilebilir. Jeffrey Lee Parson adlı 18 yaşında bir

52 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

Amerikalı gencin ürettiği Blaster solucanı, 500 binden fazla bilgisayar girmiştir. Bu virüs nedeniyle ABD'de devlet kurumlarında problemler yaşanmış, hatta kimi kurumlar bir günlüğüne kapatılmıştır. Sasser solucanının ise bulaştığı bilgisayarda kalıcı bir zarar vermediği, ancak bilgisayarı sürekli kapatıp açtığı tespit edilmiştir.

Ağ solucanları, genellikle güvenlik duvarı zayıf sistemlere girmektedirler. Sisteme girdikten sonra sistem üzerinde serbestçe dolaşan solucan, üzerinde taşıdığı bir truva programını sisteme bırakabileceği gibi, kendisi de sisteme zarar verebilmektedir. Sistem içine giren solucanlar genellikle iz bırakmamakta ve sistem içinde bulunmalarını güçleştirmektedirler. [53]

2.2.3. Bilgisayar Virüsleri

Virüs, kendini bir programa veya bir dosyaya iliştirerek bilgisayardan bilgisayara atlayabilen bir bilgisayar kodu parçasıdır. Yeni bilgisayarlara atladıkça bulaşır. Virüsler yazılımlara, donanımlara ve sistemdeki dosyalara hasar verebilir.

Bilgisayar virüsleri bulaştıkları bilişim sisteminde bulunan yazılımları çökerterek, sisteme olası en fazla zararı verecek şekilde tasarlanmışlardır. Bilgisayar virüsleri bir yazılıma ya da dosyaya fark edilmeyecek şekilde yerleşirler ve sonra kendi kendilerini kopyalayarak çoğaltırlar. Son olarak sistemleri, veri depolama üniteleri başta olmak üzere kullanılamaz hale getirirler.

Boot virüsleri, disketlerin veya sabit disklerin "boot" sektörlerine yerleşmekte ve sistem açıldığında ilk olarak disklerin "boot" adı verilen sektöründe

53 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

bulunan komutları çalıştırmaktadırlar. Boot virüsleri boot sektöründen yüklenen programın komut akışını değiştirmekte ve kendilerini de yüklemektedirler. Brain, Crazy Boot, Ping Pong gibi virüsler boot virüslere örnek olarak verilebilir.

Dosya (File) virüsleri, uzantısı ".exe", ".bat" veya ".com" olan çalıştırılabilir dosyalara bulaşmakta, dosya çalıştırılınca da devreye girip kendilerini bilgisayarların RAM belleğine yerleştirmektedirler. Bilgisayar açık kaldığı müddetçe virüs bellekte kalmakta ve çalıştırılan her dosyaya kendisini bulaştırmaktadır. Joker, Disk Killer, Walker gibi virüsler dosya virüslerine örnek olarak verilebilir.

Makro virüsleri, makro çalıştırma özelliği bulunan, başta Word, Excel gibi Microsoft Office dosyalarına bulaşmaktadırlar. Makro özelliği, programların kullanımı esnasında bazı işlerin otomatik yapılmasını sağlayan ve o uygulama için kullanılan yardımcı programlama dilidir. Bu virüsler, sadece hangi makro dili ile yazılmışlarsa o dosyaları bozabilirler. Makro virüsler, ilgili uygulamanın makro dili ile yazılmış bir şekilde, bir word ya da excel kullanarak hazırlanan dokümana yerleşmekte ve bu dokümana her girildiğinde aktif hale geçmektedirler. W97M/Class, W97M/Ethan virüsleri makro virüslerine örnek olarak verilebilir.

1948 yılında John Von Neuman tarafından geliştirilen ve kendi kendini kopyalayabilen bir program olan "automata", virüslerin atası olarak kabul edilmektedir. Bu programlar tamamen faydalı amaçlar için tasarlanmışlardır. Bu programlar 7 gün 24 saat çalışan sistemlerde geceleri dolaşarak kendilerine verilen rutin işleri gerçekleştirmekteydiler.

Akademik anlamda virüs terimi ilk olarak, 1985'te Güney Kaliforniya Üniversitesinde yüksek lisans öğrencisi olan Fred Cohen'in tezinde kullanılmıştır.

Cohen'in yazdığı bu uygulama yalnızca kendisini değişik dosyalara kopyalamak sureti ile çoğalan, zararsız, basit bir uygulama olmakla birlikte, bilgisayar kullanıcısının isteği dışında çoğaldığı için bu uygulama virüs olarak anılmaktadır. Programın bilgisayar güvenliğine karşı büyük tehdit içerdiği, bilgisayar belleklerinde bulunan verilere erişebileceği, değiştirebileceği, tahrip edebileceği, sistemi tamamen işlemez hale getirilebileceği dolayısıyla bu tür programlar yapılması, Cohen'in çalışmasının ardından yasaklanmış ama zamanla virüslerin yayılmasına engel olunamamıştır.

Bilgisayara zarar veren Brain adlı ilk bilgisayar virüsü, Pakistanlı Basit ve Amjad Farooq ALVİ adlı kardeşler tarafından Delaware Üniversitesi'nde yazılmıştır. Aslında Brain virüsü, korsanı engellemek amacıyla yazılmıştır ama zaman ilerledikçe bu amaçtan sapmıştır. Zararsız olmasına karşın, virüsü temizlemek için Delaware Üniversitesi bir hafta zaman ve önemli ölçüde insan kaynağı kullanmıştır. [54]

2.2.4. Salam Tekniği

Salam tekniği, genellikle bankalarda yaygın olarak gerçekleştirilen bir bilişim suçu metodudur. Bu yöntem ile fail, banka hesaplarında virgülden sonraki küsuratlardan sonrasını kendi belirlediği bir hesaba aktararak biriktirmektedir. Banka çalışanları ve hesap sahipleri, hesaplarda meydana gelen bu küçük miktarların hareketini fark edememekte, ancak bu küçük miktarların faile ait başka bir hesapta toplanması ile suçlular büyük miktarlarda para toplayarak hukuka aykırı yarar sağlamaktadırlar. [55] Bu tekniğin gerçekleştirilmesi için de genellikle Truva programları çeşitleri veya benzer işleve sahip yazılımlar kullanılmaktadır.

54 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s. 63-65
55 M. Dülger, 2004, s. 71

2.2.5. Sistem Güvenliğinin Kırılıp İçeri Girilmesi (Hacking)

"Hacker" deyimi ilk olarak 1960'lı yıllarda, Amerika'da ki Massachusetts Institute of Technology (MIT) laboratuarlarında, varolan programları geliştirenler için kullanılmıştır. "Hacking" deyimi de ilk olarak, bir yazılım veya sistemin yapabileceklerini öteye taşımak anlamında kullanılmakla beraber, zaman içerisinde anlamını değiştirmiş, günümüzde ise bilişim sistemleri ve sistemlerin nasıl çalıştığı hakkında bilgi almak için bu sistemlere izinsiz girmek anlamına dönüşmüştür. Hacking işlemi kimileri tarafından mevcut programları geliştirmek, programlarda varolan açıkları bulup gerekli önlemlerin alınması için bu açıkları programcılara bildirmek gibi yararlı olarak kullanılsa da, çoğunlukla sistemleri, karşıt görüşlü web sitelerini ele geçirip zarar verme gibi durumlar için de kullanılmıştır.

2.2.6. Mantık Bombaları

Mantık bombaları, bilişim sistemlerinde daha önceden belirlenen özel durumlar gerçekleşinceye kadar zararlı bir işlem yapmayan, ancak önceden belirlenen şartların sağlanması durumunda veya belirli bir tarih geldiğinde çalışmaya başlayıp sisteme zarar veren virüs programlardır. Bir çeşit truva atı gibi davranan mantık bombaları, belirlenen şartlar oluşuncaya kadar faydalı bir programmış gibi davranmaktadır. Ancak belirlenen şartlar oluştuğunda zarar vermeye başlar ve kendisini sürekli gizli tutmaya çalışan truva programlarından ayrılır.

Mantık bombalarının tek amacı içine girdikleri sisteme zarar vermek olduğundan dolayı harekete geçtiklerinde sistem için yıkıcı olmaktadırlar. Mantık bombasına örnek olarak, 1999 yılında ortaya çıkan "Çernobil Virüsü" gösterilebilir. Virüs, yazarı tarafından yerel bir bilişim konferansında yararlı bir program olarak

dağıtılmış, kısa bir süre içerisinde de Avusturya, Avustralya, İsrail, Şili, İsviçre, İsveç, ABD, Rusya ve İngiltere gibi ülkelere ulaşmıştır. Virüs programı, kurulum dosyasının çalıştırılmasıyla birlikte sisteme bulaşmaktadır. Faaliyete geçmek için her ayın 26'sını beklemektedir ve sistemi kullanılamaz hale getirmektedir. Çernobil virüsü, mantık bombasının bir alt türü olan saatli bomba şeklinde çalışmaktadır. [56]

2.2.7. Hukuka Aykırı İçerik Sunulması

Hukuka aykırı içeriklerin bilişim sistemlerinde bulundurularak veri iletim ağları aracılığı ile diğer kullanıcıların erişimine sunulması çok karşılaşılan bir bilişim suçudur. Bu içerikler, ırkçı, ayrımcı, şiddeti teşvik eden ya da kişilik haklarına tecavüz eden içerikler, insan ticareti ya da çocuk pornografisi ile ilgili içerikler olabilir. Hukuka aykırı içerik sunulması, web sayfaları, forumlar, elektronik postalar ve dosya paylaşımı aracılığı ile gerçekleştirilebilir.

Bilgi ve verileri bizzat üretmese dahi, kullanıcılara bu bilgi ve verileri kendisine ait internet sitesinde yayınlama imkânı veren içerik sağlayıcılar ilk etapta suçtan dolayı sorumlu olmasalar da, herhangi bir kullanıcısının yayınladığı hukuka aykırı içerikten haberdar edilmesi halinde erişimi engellemekle sorumludurlar.

Ülkemizde bir üniversitede idari görevleri de bulunan bir öğretim üyesine, üniversitedeki tutumunu, eğitim ve öğretim uygulamalarını tenkit eden hakaret ve tehdit içeren bir elektronik posta gönderilmiştir. Mesajda, öğretim üyesinin Ankara'da okuyan bir yakınının adım adım takip edildiği ve üniversitedeki tavır ve uygulamalarını düzeltmediği takdirde yakınına zarar verileceği şeklinde tehdit bulunmaktadır. Elektronik posta üzerinde yapılan teknik inceleme ve çalışmalar

56 M. Dülger, 2004, s. 75

sonucunda, elektronik izler takip edilmiş ve fail yakalanarak mahkemeye sevk edilmiştir. [57]

2.2.8. Veri Aldatmacası (Data Diddling)

Veri aldatmacası, veri sistemlerine veri girişi yapılırken, kasıtlı olarak yanlış verilerin girilmesi veya verilerin girildikten sonra değiştirilmesidir. Veri aldatmacası, bilişim suçları alanında en çok tercih edilen basit, güvenli ve yaygın bir suç tekniğidir.

Veri aldatmacası olarak veri-işlem dokümanlarının tahrif edilmesi, veri saklama ortamında saklanan verilerin özel araçlar ile değiştirilmesi, verilere ek başka verilerin kaydedilmesi, bazı verilerin silinmesi veya kontrol aşamalarında gösterilmemesi usulleri sayılabilir.

Veri aldatmacası tekniğinin uygulanması için kişin ileri düzeyde bilgisayar bilgisine sahip olmak gerekmez. Hatta bilişim sistemlerine müdahale yetkisi dahi olmadan, bilgisayara veri girişini yapabilecek yetenekteki herhangi bir kişi bu suçun faili olabilmektedir. Verilerin oluşturulması, kaydedilmesi, işlenmesi esnasında nezaret eden, verileri nakleden, kontrol eden veya şifreleyen kişiler bu suçu işleyebilmektedirler. Herhangi bir ağ üzerindeki bilişim sistemlerine ulaşabilen kişiler de güvenlik önlemlerini aşarak bu suçu işleyebilirler. [58]

57 Cem Beyhan, "Türkiye'de Bilişim Suçları ve Mücadele Yöntemleri", Polis Bilimleri Dergisi, Ankara, C. 4, S. 3-4, Temmuz- Aralık 2002, s. 94-95
58 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

Sabit disklerin, disketlerin veya manyetik bantların önceden hazırlanan kopyaları ile değiştirilmesi de veri aldatmacasına örnek olarak gösterilebilir.

2.2.9. İstem Dışı Alınan Elektronik Postalar (Spam)

Spam, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere zorlayıcı nitelikte gönderilmesidir. [59] Diğer bir deyişle spam, elektronik posta kutularına isteğimiz dışında, genellikle reklam amacıyla gönderilen elektronik postaları ifade etmektedir. Spam adı verilen elektronik postaları gönderen kişiye ise "spammer" denmektedir. Spammerlar oluşturdukları elektronik posta veritabanlarını kullanarak, ideolojik, pornografik ve her türlü ticari duyuru yapmak isteyen kişilerin, spam yardımıyla geniş kitlelere ulaşmasını sağlarlar. Forumlar, posta listeleri, haber grupları, tartışma grupları, yeniden iletilen elektronik postalar, web siteleri, sohbet odaları spammerların elektronik posta adresi elde etmek için kullandıkları yöntemlerdir. [60]

Spam, genellikle bir ürünün reklamı, pazarlanması ile pornografik içerikli reklam ve mesajların dünya çapında kitlelere ulaştırılması amacıyla kullanılmaktadır. [61]

İnternet kullanıcıları üzerindeki etkileri incelendiğinde iki tip spam vardır. Birinci grup spam, elektronik posta aracılığıyla doğrudan bireysel kullanıcıları hedef almaktadır. İkinci grup spam ise tartışma listelerine gönderilerek aynı anda birçok kullanıcıya ulaşmaktadır.

---

59 http://www.spam.org.tr/nedir.html (19.04.2010)
60 Ali Osman Özdilek, İnternet ve Hukuk, Papatya Yayıncılık, İstanbul, 2002, s.153
61 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s. 67

Spam, ticari içerikli olan UCE (Unsolicted Commercial e-mail, Talep Edilmemiş Ticari e-posta), mutlaka ticari olması gerekmeyen, siyasi bir görüşün propagandasını yapmak veya bir konu hakkında kamuoyu oluşturmak amaçlı gönderilen UBE (Unsolicted Bulk e-mail, Talep Edilmemiş Kitlesel e-posta) ve zincir iletiler ya da piramit benzeri pazarlama yapıları oluşturan MMF (Make Money Fast, Kolay Para Kazanın) gibi sınıflara ayrılmaktadır. [62]

Elektronik posta adreslerinin bu şekilde dağıtılması, kişilerin ev veya iş yeri adres bilgilerinin elden ele dolaşmasına benzemektedir. Kişi ve kuruluşların elektronik posta adresleri, kişisel bilgiler olarak değerlendirilmektedir ve bu bilgilerin izin alınmaksızın ticarete konu olması kişilik haklarına saldırı niteliği taşımaktadır.

Fazlaca gönderilen elektronik postalar, kurumlara da ek maliyet getirmekte, oluşan trafiği kaldırabilmeleri için kurumların gereksiz yere daha fazla donanım almalarına sebep olmaktadırlar. Örneğin AOL (America Online) şirketi, mahkeme kararıyla durduruluncaya kadar Cyber Promotions isimli kuruluştan günde 1.8 milyon spam iletisi aldığını belirtmiştir. Tipik bir kullanıcının bir spam mailini alması, tespit etmesi ve silmesi için sadece 10 saniye harcadığı bile düşünülse, bu toplamda AOL şirketi tarafından karşılanması gereken 5,000 saatlik bağlantı anlamına gelmektedir. Kaldı ki bu şekilde oluşan bir trafik, çoğu kez kurumların sistemlerini çökertmekte, internete bağlanmalarını engellemektedirler.

Spam postalar, kullanıcı ve kurumların haricinde internet servis sağlayıcılarının da yeterli hizmeti sunabilmek için fazladan yatırım yapmalarına neden olmaktadırlar. AOL'ın belirttiğine göre, günlük olarak işlem gören 15 milyon

62 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

elektronik postanın %40'ını spam oluşturmaktadır. Connecticut'ta bir araştırma şirketi olan Gartner Group'a göre, dünyada gönderilen her on postadan birinin spam olduğu tahmin edilmektedir. [63]

Ülkemiz açısından istem dışı alınan elektronik postalara özgü yasal bir düzenleme bulunmamasına karşılık, dolaylı olarak da olsa bunu engelleyebilecek hükümlerin var olduğu görülmektedir. Bu sebeple, spam ile ilgili problemlerin Tüketicinin Korunması, Haksız Rekabet ve Medeni Kanun hükümlerine göre çözümlenmesi düşünülebilir. Gönderilen e-postaların içeriğine göre Türk Ceza Kanunu'nda ele alınması da mümkündür. E-postanın içeriğinde tehdit, hakaret yasal olmayan propagandalar varsa bu takdirde bunlar ayrıca ceza davalarının konusunu oluşturmaktadırlar. [64]

2.2.10. Çöpe Dalma (Scavenging)

"Çöplenme" veya "atık toplama" olarak da adlandırılan "çöpe dalma" yönteminde, bilişim sisteminde gerçekleştirilen bir veri-işlem sonunda kalan bilgiler toplanmaktadır. Bu bilgiler öncelikle, çıktı birimlerince üretilen ve daha sonra çöpe atılan kağıt, mürekkep şeridi gibi malzemeler üzerinde kalan bilgilerin toplanmasıyla veya bilişim sisteminin belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesiyle elde edilmektedir. [65]

Çöpe atılan kağıt, mürekkep şeridi gibi malzemelerden bilgilerin alınması, fazla bir bilgi ve teknoloji gerektirmemekte, ancak bilişim sistemlerinden bilgilerin

63 A. Özdilek, 2002, s.155-158
64 Levent Kurt, Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması, Seçkin Yayınları, Ankara, 2005, s. 72
65 R. Yazıcıoğlu, 1997, s. 159

geri getirilebilmesi, bilişim sistemleri ile ilgili programlama bilgisine ve bilişim sistemine, direkt veya ağ ile ulaşılmasına ihtiyaç duyulmaktadır. Bilişim sistemlerinin ve bilgisayarların bir dosyayı silerken sadece adres tablosundan ismini silmesi, gerçek bilgisayar dosyasının silinmesinin ise üzerine yeni bilginin yazılmasından sonra gerçekleşmesi nedeniyle, silindiği düşünülen bilgiler veri depolama ünitelerinde kalabilmektedirler. Bazı programlar aracılığı ile bilginin yeniden elde edilmesi mümkündür. [66]

Bu yöntemin kullanıldığı örneklerden birisi, 1981 yılında takma ad olarak Captain Zap'i kullanan Pat Riddle'ın bilgi toplama yöntemi gösterilebilir. Captain Zap telefon şirketlerinin arkasında topladığı telefon sistemleri hakkında kitapçıklardan, şirket içi bilgi notlarından faydalanarak elde ettiği telefon numaralarıyla Amerikan Hava Kuvvetleri bilgisayarları başta olmak üzere, MIT, Pentagon ve Beyaz Saray'ın sistemlerine bağlanmış ve bu sistemlerden birçok veri elde etmiştir. [67]

2.2.11. Gizlice Dinleme (Eavesdropping-Sniffing)

Gizlice dinleme, bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak verilerin elde edilmesidir. Bilgisayar monitörlerinin yaydığı elektromanyetik dalgaların yakalanarak tekrar ekran görüntüsüne dönüştürülmesi mümkündür. Bilişim sistemlerinin merkezlerine yerleştirilecek elektromanyetik dalgaları yakalayabilen radyo vericileri aracılığı ile de veriler elde edilebilir. Araya konulan yükselticiler vasıtasıyla, elektromanyetik dalgaları çok uzaklardan yakalamak ve verileri elde etmek mümkündür.

66 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul
67 Paul Mungo, Bryan Clough, Approaching Zero Data Crime and the Computer Underworld, Çev: Emel Kurma, Sıfıra Doğru, Veri Suçları ve Bilgisayar Yeraltı Dünyası, İstanbul, 1999, s.61-69

Bilişim sistemleri arasında kullanılan ağlara veri gönderimi sırasında yapılan fiziksel müdahaleler sonucu, ağ üzerinde akan verileri elde edilmesi şeklinde de gizlice dinleme yapılabilmektedir. [68]

2.2.12. Tarama (Scanning)

Tarama, değeri her seferinde, sıralı bir diziyi takip ederek değişen verilerin, hızlı bir şekilde bilişim sistemlerine girilmek suretiyle, sistemin olumlu cevap verdiği durumların raporlanması için yapılan işlemlerdir. Sistem bir telefon numarasından başlayarak arama yapar. Aranan numara bir bilişim sistemine bağlı ise bağlantı sinyali gönderilir. İşlem her seferinde bir numara artırılarak tekrar edilir. Böylelikle belirli bir aralıkta bulunan telefon numaralarına bağlı bilişim sistemleri tespit edilmiş olur. Aynı yöntem, internete bağlı IP adres numaralarını veya IP adresleri üzerinde açık olan portları [69] bulmaya yönelik olarak da kullanılmaktadır. Özellikle port taraması, son zamanlarda bilişim suçlularının sıkça başvurdukları yöntemlerden biridir. Port taramasıyla karşı sisteme ait bilgiler elde edilerek sistemin açıklıkları bulunabilmektedir.

Şifre ile korunmuş sistemlerin şifrelerini çözmek amacıyla da şifre taraması yapılmaktadır. Özellikle sözlüklerden seçilmiş kelimeler, sadece rakamlardan veya sadece harflerden oluşan basit şifreler, şifre taraması yapan programlar tarafından rahatlıkla çözülebilmektedir. Tarama programları internet aracılığı ile kolaylıkla bulunabilmektedir. Şifre tarayıcı programlar, geçerli şifreyi bulmak için veri tabanında bulunan kelimeleri ve harf dizilerini birer birer deneyerek sistemin

68 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

69 Burada kullanılan port, bilgisayarlarda bulunan fiziksel seri ve paralel portların dışında kalan mantıksal portları ifade etmektedir. Her IP Adresi portlara yani sanal veri yollarına bölünmüştür. Bu sayede aynı anda, aynı IP Adresinden farklı programlarla veri alışverişi yapılabilmektedir.

yanıtlarını kontrol etmektedirler. Veritabanı mantıklı kelimelerden başlamak üzere, dünya genelinde en çok kullanılan şifrelerden oluşan bir sözlük niteliğindedir. [70]

Tarama programları, bilişim suçluları tarafından sistemlere saldırı düzenlemek amacıyla kullanılabileceği gibi, sistem açıklarının tespit edilip bu açıkların kapatılarak sistem güvenliğinin artırılması amacıyla da çalıştırılabilmektedir.

2.2.13. Süper Darbe (Super Zapping)

Süper darbe programları, bilişim sistemleri çeşitli sebeplerle işlemez hale geldiğinde, çok kısa bir süre içerisinde sistemin tekrar çalışmasını sağlamak üzere tüm güvenlik kontrollerini aşarak sistemde değişiklik yapılabilmesini sağlayan programlardır. İlk olarak bilgisayarlarda herhangi bir programın disketten diskete kopyalanmasına engel olan "kopya koruma" yazılımlarını atlatan bir program olarak ortaya çıkmıştır. Bu program amacı doğrultusunda bilişim sistemlerinin kilitlendiği veya işlemez hale geldiği acil durumlardan çıkılmasında kullanıldığında çok faydalı olmasıyla beraber, kötü amaçlara alet edildiği takdirde çok tehlikeli olmaktadır. Süper darbe programları, bilişim sistemlerinde büyük çapta tahribat yapmak isteyen bilişim suçlularına, tüm güvenlik önlemlerinden serbestçe geçebilmesinden dolayı çok geniş bir olanak sağlamaktadır. [71]

Amerikan Bankasında bir bilgi işlem görevlisi, sistemde meydana gelen bir hatayı düzeltmek için süper darbe programını çalıştırdığı sırada, güvenlik tedbirlerinin kaldırıldığını fark etmiş ve arkadaşlarının hesabına yüklü miktarda

70 E. Aydın, 1992, s. 82
71 a.g.e., s. 83

paralar aktarmıştır. Bu olay müşterilerinden birinin hesabındaki paranın azaldığını fark etmesi ile ortaya çıkmıştır. [72]

2.2.14. Gizli Kapılar (Trap Doors)

Tuzak kapısı, arka kapı ya da açık kapı da denilen gizli kapılar, bir sistemin yazılımını yapan kişi tarafından, yazılımın içine gizli bir şekilde yerleştirilen bir virüs yazılımıdır. Bu programın çalıştığı bilgisayara, virüsü yerleştiren kişi, uzaktan erişim yöntemiyle sistem kontrollerine yakalanmadan bilişim sistemine sızabilmektedir.

Adından da anlaşılacağı üzere uygulamayı geliştiren şirket ya da kişi tarafından bilinçli bir şekilde bırakılmış açık noktalardır. Gizli kapılar, dokümante edilmemiş gizli giriş noktaları olarak da tanımlanabilir. Çok sık rastlanılmasa da gizli kapılara örnek olarak kimlik denetimi (authentication) olan uygulamalar verilebilir. Sadece uygulama geliştiriciler tarafından bilinen bir kullanıcı adı ve şifre, sisteme ait gizli bir kapıdır. Sisteme zarar vermekten çok, genellikle teknoloji hırsızlığına ve ticari kaygılara dayanmaktadır. [73]

Gizli kapılar genellikle işletim sistemlerini veya programları hazırlayan programcılar tarafından, ilerde ortaya çıkabilecek durumlara karşı hata bulma amacıyla kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programlara eklenmektedirler. Bu gizli kapılar hataları gidermek amacıyla konulduğu için meşru amaçlıdır. Ancak gizli kapıların program ve işletim sistemi tamamlandığında temizlenmesi gerekmektedir. Bazı durumlarda hata sonucu olarak

72 R. Yazıcıoğlu, 1997, s. 156
73 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s. 62

ya da ileride kullanılmak amacıyla gizli kapılar açık bırakılır. Bu durumlarda gizli kapılar, kötü niyetli kişilerin bilişim sistemlerine sızabileceği potansiyel bir boşluk oluşturmaktadırlar. [74]

2.2.15. Eşzamansız Saldırılar (Asynchronous Attacks)

Bilgisayarların birden fazla işlemi aynı anda yürütmesine eşzamanlı çalışma denir. Bilgisayarlar belirli durumlarda eşzamanlı çalışma yerine, işlemleri belirli sırada yürütmektedirler. Bir işlemin başlaması diğer bir işlemin sonucuna göre belirlenmektedir. Bu çalışma esasına ise eşzamansız çalışma adı verilir. Örneğin yazıcıdan bir çıktı alınması işlemi esnasında, çeşitli görevlerin sırayla çağrılması gerekmektedir. İşletim sistemi bu istekleri bekletir ve yazıcı kaynakları ulaşılabilir olduğunda, istek sırasına ya da öncelik sırasına göre istekleri yerine getirir. İşletim sistemleri bu tür durumlarda, kaynaklara ulaşabilme esasına dayanan bir şekilde eşzamansız olarak çalışmaktadır. [75]

Eşzamansız çalışma esnasında, bellekte bekleyen veriler üzerinde değişiklik yapılmasına dayanan saldırı biçimine eşzamansız saldırı denmektedir. Örneğin herhangi bir programla yapılan çalışmanın sonuçlarını yazıcıdan almak için diğer işlemlerin bitmesinin beklendiği esnada, iyi programlama bilgisine sahip kişiler bellekte bekleyen bu veriler üzerinde istekleri doğrultusunda ekleme, silme veya değişiklik yapabilme imkanına sahiptirler. [76]

74 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul, s. 85
75 a.g.e., s. 86
76 R. Yazıcıoğlu, 1997, s. 158

2.2.16. Sırtlama (Piggybacking)

Sırtlama, fiziksel ya da elektronik yollar aracılığıyla bilişim sistemlerine yetkisiz olarak girme tekniğidir. Fiziksel sırtlama, bilişim sistemlerinin yetki ile erişilen kısımlarına, girişe yetkili olan bir kullanıcının giriş yetkisinin kullanılarak girilmesidir. Elektronik sırtlama ise bilişim sistemlerine bağlı kullanıcıların bağlandıkları hatlar kullanılarak, bilişim sistemlerine yetkisiz olarak erişilmesidir. [77]

2.2.17. Yerine Geçme (Masquerading)

Belli bir ağa bağlı olan bilişim sistemleri, erişim yetkileri yönünden bölümlere ayrılırlar. Sistemlere erişim imkanı her bilgisayar için eşit düzeyde olmayabilir. Erişim düzeyi sistemden sisteme farklılık gösterebilir. Sistem kullanıcıları farklı seviyelerde yetkilendirilmektedir. Kullanıcılar, sahip oldukları kullanıcı isim ve şifreleri sayesinde bilişim sistemlerinde farklı seviyelerde işlem yapabilmektedirler. Gelişen teknoloji ile birlikte, kullanıcı isim ve şifrelerinin yanında parmak izi, göz retina yapısı gibi kişisel özellikler de sistem erişimlerinde kullanılmaya başlanmıştır. Bilişim sistemlerine erişim yetkisi olan bir kişinin başkaları tarafından, kullanıcı isim ve şifresinin yazılarak veya kişisel özelliklerinin taklit edilerek sistemlere giriş yapılmasına yerine geçme denmektedir. [78]

1980'li yıllarda Triludan The Warrior isimli bir hacker, İngiliz Prestel şirketinin bilgisayarlarına girmek için yerine geçme yöntemini kullanarak, sistem yöneticisi olmuştur. Yerine geçme yönteminde, gerçek kullanıcının fiziksel olarak bulunmasına gerek bulunmamaktadır. [79]

---

77 P. Mungo, B. Clough, Çev: E. Kurma, 1999, s.83
78 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul
79 P. Mungo, B. Clough, Çev: E. Kurma, 1999, s.53

2.2.18. Tavşanlar (Rabbits)

Tavşanlar, bilişim sistemlerine, gereksiz işler yapması için sürekli olarak komut gönderen yazılımlardır. Tavşanlar hızla çoğalarak koloni kurmakta, bilgisayarların veri işleme gücünü azaltmakta ve sonuçta bilişim sistemlerini işlemez hale getirmektedirler. Tavşanların faaliyete geçebilmesi için tavşan bulaşan dosyanın çalıştırılmasına veya açılmasına gerek yoktur. Kendi kendilerine bu özelliği gösterebilmektedir. [80]

İngiltere'de 1988 yılında, "mad hacker" takma isimli bir bilişim korsanı, Queen Mary ve Hull Üniversitesi'nin bilişim sistemlerine yüklediği tavşan yazılımlar sayesinde bu sistemlerin hiç durmadan yazılar yazmasını sağlayarak sistemlerin çalışmaz hale gelmesine sebep olmuştur. [81]

2.2.19. Bukalemun (Chameleon)

Bukalemunlar, normal bir program gibi çalışır fakat aynı zamanda bir takım aldatma ve hilelerle sistemlere zarar verirler. Kullanıcı adı ve şifrelerini taklit etme özelliği nedeni ile gizli dosyalara ulaşıp, şifreleri gizli bir dosya açarak kaydetmektedirler. Daha sonra sistemin bakım nedeniyle geçici bir süre kapatılacağına dair mesaj verip, bu programı kullanan kişilerin bu gizli dosyaya ulaşarak kullanıcı isim ve şifrelerini ele geçirmesini sağlamaktadırlar. [82]

80 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul
81 P. Mungo, B. Clough, Çev: E. Kurma, 1999, s.67
82 Olgun Değirmenci (2002), Bilişim Suçları, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul

2.2.20. Web Sayfası Hırsızlığı ve Web Sayfası Yönlendirme

Yaygın olarak görülen suçlardan birisi de web sayfası hırsızlığı ve web sayfası yönlendirmedir. Bir web sitesine alan adı verilen adreslerden ulaşılır. Alan adları sunucuları (DNS) veri tabanında tutulur ve tüm dünyaya ilan edilir. Bir internet kullanıcısı web sitesine ulaşmak istediğinde, web tarayıcısı alan adının DNS sorgulamasını yaparak web sayfasının bulunduğu sunucunun IP adresini öğrenmekte ve bu IP adresinden sayfayı getirmektedir. Bir kişi web sayfası yayınlamak istediğinde önce bir alan adı almak zorundadır. Bunun için alan adı hizmeti veren servis sağlayıcılara müracaat eder. Eğer bu müracaattan önce, bir kişi daha hızlı davranıp alan adını tescil ettirirse, isim hakkı o kişinin olur. Tescil edilmiş alan adları da hackerlar veya bu bilgiye erişebilen bir internet servis sağlayıcı (İSS) çalışanı tarafından kendileri veya üçüncü bir kişi lehine olacak şekilde tescil kaydını değiştirebilirler. Bu şahıslar daha sonra tescil ettirdikleri alan adlarını yüksek ücretlerle olması gereken gerçek sahiplerine satmaya çalışmaktadırlar. Bu suç internet servis sağlayıcılarının herhangi bir şekilde internet başvurusuna ait bilgileri kötü niyetli üçüncü kişilere sızdırması şeklinde işlenebilir. Aynı zamanda servis sağlayıcısının sistemlerine bilgisayar korsanlarının girerek bilgilere erişmesi şeklinde de işlenebilir.

Almanya'da Bremen Üniversitesi Enformatik Teknoloji Merkezi'nin taşınabilir bilgisayarları için beş internet adresi Berlin'de ucuz bir internet servis sağlayıcısı olan Strato'dan ayrılmış olmasına rağmen, başvuru sürecinde bilgiler kimliği belirsiz kişilerce öğrenilmiş ve daha hızlı davranılarak beş adresten dört adedi başkaları adına kaydedilmiştir. İnternetin yaygınlaşmasıyla beraber, alan isimleri de değerlenmiş, bu da bilişim suçlularının web sayfası hırsızlığına yönelmelerine sebep olmuştur.

Web sayfası yönlendirme ise, internet sitelerinin alan adları ile IP adreslerinin tutulduğu veritabanları olan DNS sunucularda hukuka aykırı olarak değişiklik yapılarak, web sitesinin bir başka IP adresine yönlendirilmesidir. Kullanıcılar siteye ulaşmak için alan adını web tarayıcısına girerler. Ancak DNS kayıtları değiştirildiği için kullanıcı gitmesi gereken IP adresi yerine, faillerin istedikleri adrese yönlendirilir ve bambaşka bir siteye ulaşır. [83] Bu yöntem genellikle banka web sayfasına ulaşmak isteyen kullanıcılara uygulanmaktadır. Kullanıcıların yönlendirildiği web sayfası, gerçekte gidilmek istenen web sayfasına benzer şekilde tasarlanmış başka bir web sayfasıdır. Kullanıcı bu sayfa üzerinde şifrelerini girdiğinde, bilgisayar korsanı bu şifreleri elde etmektedir. Özellikle internet üzerinden alışveriş ve bankacılık işlemlerinin yaygınlaşması, suçluların bu yöntemi kullanarak banka kredi kartları bilgilerini temin edebilme eğilimlerini artırmıştır.

Bir diğer web sayfası yönlendirme tekniği ise "typing error hijacking" (yanlış yazanları kaçırma) olarak adlandırılan bir tekniktir. Bu teknikte hacker yaygın olarak bilinen yanlışları göz önüne alarak bu yanlışları yapan kullanıcıları kendi sayfasına yönlendirir. Örnek olarak Amerika Birleşik Devletleri Başkanlık sarayının internet adresi http://www.whitehouse.gov olmasına rağmen birçok kullanıcı www.whitehouse.com adresinden ulaşmaya çalışmaktadır. Fail bu yanlışı değerlendirerek, alan adını kaydettirmiş ve kendi porno sitesine yönlendirmiştir. [84]

2.2.21. Oltaya Gelme (Phishing)

Olta saldırıları, internet kullanıcılarının kullanıcı adı, şifre gibi kişisel tanımlama bilgilerini, online bankacılık ve kredi kartı numarası gibi finansal hesap erişim bilgilerini, sosyal mühendislik ve teknik hileler kullanarak elde etmeyi

83 Bahaddin Alaca (2008), Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara, s. 70-71
84 http://media.chip.com.tr/images/arsivpdf/2000-03-258.pdf (13.04.2010)

amaçlayan saldırılardır. Bilgisayar korsanları tarafından günümüzde oldukça yaygın olarak kullanılan olta atma saldırıları, şahısların bilgileri elde edilerek haksız kazanç sağlanılmaktadır.

Özellikle son yıllarda internet bankacılığının yaygınlaşmasıyla birlikte çoğu internet kullanıcısı bankacılık işlemlerini bankalarının online sayfaları üzerinden gerçekleştirmektedir. Çoğunlukla sıkı güvenlik önlemleri ile desteklenmiş online bankacılık hizmetlerinde bankanın güvenlik zafiyeti olmaksızın, bankanın adı ve uygulama sayfasının bir benzeri kullanılarak art niyetli faaliyetler bilgisayar korsanları tarafından yürütülebilmektedir.

Bunun yanında bilgisayar korsanları hedef olarak seçtikleri kişilerin e-posta hesaplarının veya online üyelik gerektiren hizmetlerinin şifrelerini elde etmek amacıyla bahse konu online hizmetin iyileştirilebilmesi veya şifre doğrulaması adı altında olta saldırılarını sıklıkla kullanmakta ve kullanıcı adları ile şifrelerini kolaylıkla elde edebilmektedirler.

Gerçekleştirilen herhangi bir olta saldırısında, içeriği sosyal mühendislik yöntemiyle alıcısını kandırmaya yönelik olarak profesyonelce hazırlanmış bir sahte elektronik posta iletisi bulunmaktadır. Gerçek sahipleri tarafından geliyormuş gibi gösterilen bu sahte elektronik postalar, birçok adrese gönderilmektedir. Elektronik postanın sahte olduğunun farkına varmayan kişiler, posta iletisindeki belirli bir linke tıklayarak yine gerçeğine benzer şekilde hazırlanmış web sayfalarına yönlendirilerek veya doğrudan posta iletisini kullanarak kişisel bilgilerini bilişim korsanlarına göndermektedirler.

Bazı durumlarda da, bilişim korsanları gönderdikleri elektronik posta iletisindeki linkin kurban tarafından tıklanmasını sağlayarak kurbanların bilgisayarlarına bir casus program indirilmesini sağlamaktadırlar. İndirilmesi sağlanan bu casus programlar, genellikle kurban kullanıcının bilgisayarındaki klavye tuş vuruşlarını kaydederek kullanıcı ismi, şifre, bankacılık bilgileri gibi kritik bilgileri karşı tarafa iletmektedirler. [85]

85 http://www.ekizer.net/index.php?option=com_content&task=view&id=15&Itemid=1 (13.05.2010)

ÜÇÜNCÜ BÖLÜM

3. BİLİŞİM SUÇLARIYLA MÜCADELE

3.1. ÖNLEYİCİ TEDBİRLER

İlerleyen konularda da detaylı olarak bahsedileceği üzere, hem suç faillerinin bulunmasının güç olması, hem de dinamik bir suç alanı olması hasebiyle suç oluştuktan sonra öngörülen cezai yaptırımların teknolojiye ayak uyduramaması, suçlular için caydırıcılığı düşürmektedir. Bilişim alanındaki suçlar ve suçluların sayısı hızla artmaktadır. Bu bağlamda, bilişim suçlarıyla mücadelenin en kolay yolu, suçun oluşmadan engellenmesidir. Alınacak küçük tedbirler, olası çok büyük zararlara engel olabilmektedir. Bu yüzden önleyici tedbirler, yani suçun oluşmadan önce suçun oluşmaması için uygulayacağımız yöntemler, bilişim suçlarıyla mücadelede oldukça önemlidir.

3.1.1. Fiziksel Güvenlik

Fiziksel güvenlik, değerli bilgilerin ve firmaların kaynaklarının korunmasında uygulanması gereken en temel ve önemli yöntemlerin başında gelmektedir. Fiziksel güvenliğin ilk adımı olarak çalışma alanlarının fiziksel güvenlik gereksinimlerinin belirlenmesi gerekmektedir. Daha sonra yapılabilecek risk analizi ile hangi bölgenin ne derecede güvenlik gereksinimine ihtiyaç duyduğu belirlenmelidir. Fiziksel güvenliğe esas öğeler; personel giriş/çıkışları, ziyaretçi

giriş/çıkışları, sistemlerin ve bu sistemlerle bağlantı kurulan kişisel ve dizüstü bilgisayarların güvenliği, kablolama güvenliği, binanın ve çalışılan ofislerin fiziksel güvenliğidir.

Bilgileri çoğaltmak, taşımak veya arşivlemek amacıyla kullanılan disket, CD, harici bellek ve diğer harici hafıza birimleri mutlaka emniyetli bir yerde muhafaza edilmeli ve kilit altında bulundurulmalıdır. Bu malzemelerin bulunduğu yerlere erişim de emniyet altına alınmalıdır. Söz konusu malzemelerin kırılması, çizilmesi veya bozulması halinde kullanılamaz duruma gelenler mutlaka yakılarak imha edilmelidir. Bilgi işlem sistemlerinde kullanılan her türlü veri taşıyıcısı, yazıcı, tarayıcı ve diğer donanımlar kayıt ve gözlem altına alınmalıdır. [86]

Bilişim sistemleri kullanılmadıkları zaman kesinlikle gözetimsiz bırakılmamalıdırlar. Sistem kullanılmadığı zaman açma-kapama anahtarı ile kapatılmalı ve diğer sistemlerle olan tüm irtibatları (network, internet vb.) kesilmeli, elektrik fişi çekilmelidir.

Bilişim sistemlerinin bulunduğu emniyetli bölgelere giriş ve çıkışlar kontrol altında olmalıdır. Kartlı giriş/çıkış, kamera gözetimi gibi güvenlik tedbirleri alınmalıdır. Sistemlerin kurulacağı yerler tespit edilirken yangın, su basması gibi olaylar hesap edilmeli, sistem için en uygun yer seçilmelidir. Sistemler kurulduktan sonra da olası tehlikeler için, ısı, duman, nem ve benzeri sensörler, yangın söndürme sistemleri kullanılmalıdır.

Verinin tutulduğu/işlendiği ortamlara fiziki erişim düzeylendirilmeli, yetkiler paylaşımlı hale getirilmelidir. Erişim yetkileri yazılı hale getirilip, görevli personelin erişebileceği güvenli ortamlarda tutulmalı, muhtemel aksaklıklar göz önünde

86 B. Akbulut, 2000, s. 545-555

tutularak her an yedek görevli personel bulundurulmalıdır. Üçüncü taraf destek hizmetleri gerektiği durumlarda, bu destek hizmeti görevli personel nezaretinde alınmalı, erişim yetkileri sınırlı tutulmalı, üçüncü taraflara herhangi bir kaydedici cihaz ile güvenlik ortamlarına giriş izni verilmemelidir.

Doğal felaketlere karşı tedbirler alınmalı, ana merkez bilgi işlem cihazları ile online senkronizasyon olan aynı (veya daha yüksek kapasiteli) konfigürasyona sahip cihazlar, farklı deprem veya doğal felaket kuşağında bulunan bölgelerde muhafaza edilmelidir. Her şartta erişebilirlilik garanti altına alınmalıdır. [87]

3.1.2. Kurumsal Güvenlik

Bir organizasyonun sadece teknik önlemler alınarak bilgi güvenliğinin ve iş sürekliliğinin sağlanmasının mümkün olmadığı günümüzde, artık tüm dünyada yaşanan canlı örneklerle ve karşılaşılan büyük kurumsal kayıplarla kendini ispatlamıştır. Bilgi güvenliği, ancak kurumsal bir yönetim yapısı olarak ele alınması ve bu yapıya üst yönetimin ve tüm çalışanların destek vermesi durumunda sağlanabilmektedir.

Gelişen teknolojinin sağladığı avantajlara ve değişen iş yapma biçim ve tekniklerine bağlı olarak kurum ve kuruluşların, iş süreçlerini ve bilgi varlıklarını sayısal ortama taşımasıyla birlikte, bilgi güvenliği stratejik öneme sahip bir konu haline gelmiştir. Stratejik bilgi güvenliği yaklaşımı, bilgi güvenliğinin her iş süreci içinde değerlendirilmesi gereken bir unsur olduğunu ortaya koymaktadır.

87 E-imza Ulusal Koordinasyon Kurulu Bilgi Güvenliği Ve Standartlar Çalışma Grubu İlerleme Raporu, 2004, http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuv1.2.pdf (20.04.2010)

Bilgi güvenliği, kurumlar için bir politika olmalı, tüm kurum çalışanları için uymaları gereken kurallar bu politika çerçevesinde tanımlanmalıdır. Tüm güvenlik önlemlerini alan bir kurumda dahi, tek bir personelin farkında olmadan oluşturacağı bir açık, yapılan tüm çalışmaların boşa gitmesine sebep olabilmekte, bilgi güvenliğini sekteye uğratabilmektedir. Sistemin hizmet kesintisine uğramaması, üretilen veya barındırılan bilgilerin bütünlüğünün korunması ve bu bilgilerin kurum dışına izinsiz çıkartılamaması için, güvenlik kurumsal bazda ele alınmalı, kurumlara has tüm iş süreçlerinde olası güvenlik açıkları değerlendirilmelidir. Bu açıkların nasıl kapatılacağı da ortaya konularak kurumun bilgi güvenliği politikaları oluşturulmalıdır.

3.1.3. Personel Güvenliği

Bilişim sistemleri üzerinde alınacak önemli güvenlik tedbirlerinden birisi de personel güvenliğidir. Bilişim sistemlerinin yönetim merkezlerinde çalışacak personelin güvenlik tahkikatı yaptırılmalı ve bu personele düzenli olarak güvenlik brifingi verilmelidir.

Bilişim sistemlerinin kullanıcıları ve yöneticilerinde bilgi sistemleri güvenliği bilinci oluşturulmalıdır. Bilişim sistemlerinde görevli personel, yetkileri ve görevleri gereğince sahip olduğu kritik bilgileri kimseyle paylaşmamalıdır. [88] Bilişim sistemlerinde mümkün mertebe güvenlik konusunda eğitimli personel çalıştırılmalı, gelişen teknolojiler hakkında personelin yetişmesi için gerekli eğitimler de ilgili personele verilmelidir.

88 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 81

Üçüncü tarafların (yazılım ve donanım destek hizmeti, temizlik hizmeti, kısa süreli çalıştırılan personel, danışmanlık hizmetleri vb.) fiziki ve elektronik erişimleri, hizmetlerin aksamayacağı ve güvenliğin tehlikeye atılmayacağı şekilde denetlenmeli, işlemler dokümante edilmelidir. Üçüncü taraflarca yapılacak her işlem sözleşme hükümlerine bağlanmalıdır. Yanlış kullanımdan doğacak sonuçlarla, diğer personel hatalarının doğuracağı risklere karşı her türlü idari ve teknik tedbirler alınmalıdır.

Personelin yetkileri hiyerarşik ve otokontrol sağlayıcı biçimde yapılandırılmalıdır. Personel işe alımlarında, ilgili yasalarda belirtilen yasal şartları taşıma şartı aranmalı, teknik yeterlilikleri (mezuniyet bilgileri, aldıkları eğitimler vs) belgelendirilmelidir.

Personel ile hizmet sağlayıcı kuruluş arasında imzalanacak iş akitlerinde gizlilik ve mahremiyet kuralları öncelikli madde olarak bulunmalıdır. İşe alma veya sözleşme şartlarında bir değişiklik oluştuğunda, özellikle personel işletmeden ayrılma aşamasında olduğunda veya sözleşme süresi sona erme aşamasında olduğunda, gizlilik anlaşmaları ve güvenlik politikaları yeniden gözden geçirilmelidir. [89]

Kullanıcı personel, bilişim sistemleri üzerinde dosya paylaşımı ve yetkilendirme konularını bilmelidir. Bilişim sisteminde alınması gereken fiziki ve işlemsel güvenlik tedbirlerini tüm personel ve sistem yöneticileri bilmeli ve en üst düzeyde uygulamalıdır.

89 E-imza Ulusal Koordinasyon Kurulu Bilgi Güvenliği Ve Standartlar Çalışma Grubu İlerleme Raporu, 2004, http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuv1.2.pdf (20.04.2010)

Sistem yöneticileri, sisteme dışarıdan müdahale olduğunda fark edebilecek, gerekli müdahaleyi yapabilecek seviyede olmalıdır. Ayrıca dışarıdan yapılacak müdahalelerin neler olabileceğini ve sisteme vereceği zararları, temel bilişim suçlarının neler olduğunu, bunların nasıl işlenebileceğini ve bunlar hakkındaki yasal mevzuatı bilmeli ve buna göre belirlenmiş tedbirleri uygulamalıdır. Tüm kullanıcılar bilişim sistemlerinde kullanılan anti-virüs ve firewall (ateş duvarı) gibi güvenlik programlarını çok iyi bilmeli, bu programları kullanarak saldırılardan korunmayı gerçekleştirebilmelidir. [90]

3.1.4. İşlemsel Güvenlik

Bilişim sistemlerinde kullanılan tüm programlar lisanslı, kaynağı ve güvenilirliği bilinen programlar olmalıdır. Lisanssız programların kullanılması suç unsuru oluşturduğu gibi güvenlik açıklarına da neden olmaktadır.

Bilişim sistemlerinde bilgisayar açılışlarına mutlaka bios [91] şifresi konulmalıdır. Bu şifre sayesinde bilgisayarın çalışmasına müdahale edilmesi önlenmiş olmaktadır. Ayrıca bios şifresinin silinmesini engellemek amacıyla bilgisayarların içinde takılı olan pilin sökülmemesi için tedbirler alınmalıdır.

Bilgisayarların bir ağa dahil olup olmadığına bakılmaksızın, sistemlerde parola koruması mutlaka aktif edilmelidir. Bilgisayarların kullanılmadığı kısa süreli durumlarda hem ekranda çalışılan bilgilerin, hem de bilişim sisteminin içindeki

90 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 81

91 Basic Input/Output System" (Temel Giriş/Çıkış Sistemi) kelimelerinin baş harflerinin birleşmesinden meydana gelen BIOS, bilgisayarın çalışması için gereken temel yapısıdır. Bilgisayar donanımlarından anakart üstünde bulunan ve konum itibariyle çok küçük olmasına karşın işlevsel yönden bilgisayarın en temel parçası olan bu aygıt, bilgisayarın açılışı sırasında yapılması gereken tüm komutları ve donanımsal olarak yapılması gereken tüm işlemleri denetleyen ve ayarlamaları yapan bir parçadır.

bilgilerin yetkisiz kişilerce görülmemesi amacıyla sisteme giriş parolasından başka, ekran koruma parolası koyulmalı ve bu parolaların sisteme giriş yetkisi olanların haricinde bilinmemesi sağlanmalı, mümkün olduğunca gizli tutulmalıdır. Bilgisayar sistemlerinin açılışına koyulan parolalar en az sekiz karakterden oluşmalı ve bu karakterler harf, rakam işaret içermeli, doğum tarihi, isim gibi kolaylıkla tahmin edilebilecek sözcükler içermemelidir.

Bilgisayarlara yüklenen işletim sistemi programlarının network uyumlu olmasına dikkat edilmelidir. Bu işletim sistemlerinin güvenliği daha üst seviyededir. Söz konusu işletim sistemlerine ait güvenlik seviyesi en az C2 seviyesinde olmalıdır. İşletim sistemlerinde kullanılan güvenlik seviyeleri A1, B3, B2, B1, C2, C1 ve D olmak üzere yedi farklı düzeydedir ve en emniyetlisi A1'dir.

Bilgisayarların disket, CD/DVD veya benzeri harici sürücülerle açılması engellenmeli hatta mümkün olan sistemlerde bu ve benzeri harici aygıt kullanımları kontrol altına alınmalıdır. Bu amaçla bilgisayarların sistem kurulum ayarlarında gerekli düzenlemeler yapılmalıdır.

Bilgisayarlarda lisanslı olarak virüs koruma ve temizleme programları kullanılmalıdır. Sistemler her açıldığında bu programlar aktif olarak çalışmaya başlamalı ve koruma yapacak şekilde ayarlanmalıdır. Anti-virüs programları düzenli olarak güncellenmeli, böylelikle yeni virüsleri de tanıyacak seviyeye getirilmelidir.

Bilgisayarlar, internet veya yerel bir ağ ortamında kullanılıyorsa, tüm sürücüler (C, D, E vb.) paylaşıma kapatılmalı ve hiç kimseye gereksiz yetki tanımlanmamalıdır. Eğer gerekiyorsa bilgi alış-verişi amacıyla uygun boş bir klasör paylaşıma açılmalı ve bu klasöre erişebilecek kullanıcılar tespit edilerek

yetkilendirilmelidir. Ayrıca ağ üzerinden paylaşıma açılan bu klasöre mutlaka erişim parolası koyulmalıdır.

Bilgisayarlar üzerindeki hizmete özel her türlü doküman, yansı ve tablolara yetkisiz kişilerin nüfuz etmesini engellemek için dosya bazında parola koruması da uygulanmalıdır. Eğer bu dosyaların bilgisayar üzerinde bulunması şart değilse, emniyetli bir harici veri taşıyıcısına aktarılarak sistemden silinmelidir. [92]

Son yıllarda özellikle internet üzerinden işlenen suçlarda ki artış dolayısıyla, internete giren kişilerin de özel önlem almaları ihtiyacı doğmuştur. Çalışılan şirkete veya şahsa ait önemli bilgilerin yer aldığı bilgisayarlar ile özel güvenlik önlemleri almadan internete bağlanılmamalıdır. İnternet ortamında %100 güvenliğin hiçbir zaman sağlanamayacağı akıldan çıkarılmamalıdır. Özellikle chat [93] ortamında bilgisayara saldırılabileceğini, chat ortamında tanışılan kişilere şahıs, aile, adres, telefon, iş vb. konularda şahsi bilgilerin verilmemesi gerektiği unutulmamalıdır. İnternet ortamında hiçbir şekilde banka kartı, kredi kartı bilgileri verilmemelidir. İnternet üzerinden yapılan yazışmalarda ve uygulamalarda, mümkün olduğunca güvenilirliği bilinen programlar kullanılmalıdır.

3.1.5. Bilgi Güvenliği Standartları

Kurumların değerli ve gizli olarak nitelendirilen veri ve bilgilerinin korunmasında, bilgi güvenliği standartları çok önemli bir görev üstlenmektedir. Kurumların, bilgi güvenliği hususunda azami ölçüde dikkatli olması, gerekli tedbirleri yerinde ve zamanında alması gerekmektedir. Bilgi güvenliği standartları

92 İsmail Tulum (2006), Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta, s. 79-80
93 Chat: Internet üzerinden belli sunuculara bağlanarak diğer insanlarla haberleşme tekniğidir.

ile kurumların bilgi güvenliğinin sürekliliği, kaynakların doğru şekilde kullanımı ve güvenlik uygulamalarının geliştirilmesi amaçlanmaktadır.

Bilgi güvenliği konusunda oluşturulmuş en önemli standartlar, Uluslararası Standartlar Teşkilatı Elektroteknik Komisyonunun (ISO/IEC) oluşturduğu 27000 ile başlayan ISO standart ailesidir.

Bilgi teknolojileri yönetimi için bir denetim aracı olan Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri (COBIT) ise Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA) ile Bilgi Teknolojileri Yönetim Enstitüsü (ITGI) tarafından 1996 yılında geliştirilmiştir.

3.1.5.1. ISO 27000

ISO 27000 standartları ISO/IEC ISMS standart ailesinin bir parçasıdır. ISO 27000 standart serisi; ISO 27001, ISO 27002, ISO 27003 vb. "Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetimi sistemleri - Genel bakış ve tanımlar" başlıklarını kapsayan uluslararası standartları içeren bir standart ailedir.

ISO 27000 bilgi güvenliği standartları, diğer pek çok teknik konuda olduğu gibi karmaşık bir terminoloji ağı geliştirmektedir. Nispeten az sayıda yazar bu terimlerin tam olarak ne anlama geldiğini belirleme zahmetine katlanmakta ve bu da standartlar konusunda kabul edilemez, karışıklığa yol açabilecek değerlendirme ve belgelendirme sürecinin değerini azaltıcı bir yaklaşım olmaktadır. ISO 9000, ISO 14000 de olduğu gibi, '000' temelli standartlar bu durumun önemini ortaya koymayı amaçlamaktadırlar.

ISO 27000 standartları, Uluslararası Standardizasyon Örgütü'nün ve Uluslararası Elektroteknik Komisyonu'nun ortaklığında kurulan Birleşik Teknik Komite'ye bağlı bir alt komite tarafından geliştirilmektedir. [94]

3.1.5.2. ISO 27001

ISO 27001 standardı, Uluslararası Standardizasyon Örgütü ve Uluslararası Elektroteknik Komisyonu tarafından Ekim 2005'te yayınlanmış bir Bilgi Güvenliği Yönetim Sistemi standardıdır. Standardın tam adı; "ISO/IEC 27001:2005 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetimi Sistemleri – Şartları" olarak geçmektedir ama genel olarak ISO 27001 belgesi standardı olarak bilinmektedir.

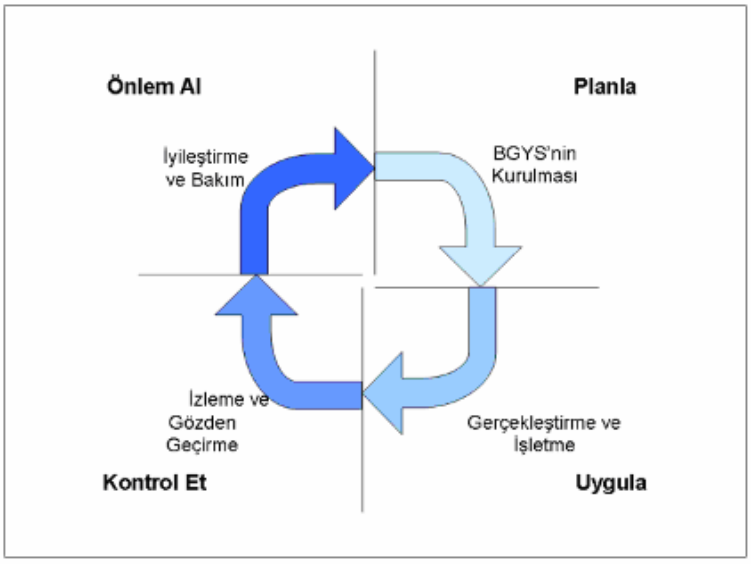
ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı, ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ana standardı olup sistem kurulumu ve belgelendirme bu standart üzerinden yapılmaktadır. Genel olarak ISO 27001 standardı aşağıdaki amaçları gerçekleştirmektedir:

- Kurumun/kuruluşun bilgi güvenlik risklerini, bilgi varlıklarına yönelik tehditleri, varlıkların açıklıklarını sistematik olarak denetlemek,
- Risk işleme planları, artık risklerin transferleri ile tutarlı bilgi güvenliği kontrollerini tanımlamak ve gerçekleştirmek, riskleri kabul edilebilir seviyelere çekmek,
- Bilgi güvenliği kontrollerinin sürekliliğini bilgi güvenliği esaslarına göre sağlamak üzere yönetim süreçlerini kabul etmek ve uygulamak.

94 http://www.isokalitebelgesi.com (12.06.2010)

ISO 27001 standardı yaşayan, dolayısı ile tehdit ve saldırılara reaksiyon gösteren ve kendini yenileyen bir bilgi güvenliği sisteminde yer alması gereken öğeleri tanımlamaktadır.

ISO 27001'de tanımlanan yaklaşım uyarınca bilgi güvenliğinin bir süreç olarak ele alınması ve sürecin planlama, uygulama, kontrol etme ve önlem alma adımlarından oluşan bir döngü şeklinde çalıştırılması gerekmektedir. [95] Yaşayan ve kendini yenileyen bir bilgi güvenliği sistemi ancak Şekil-1'de görülen bu döngünün çalıştırılması ile mümkün olabilmektedir.

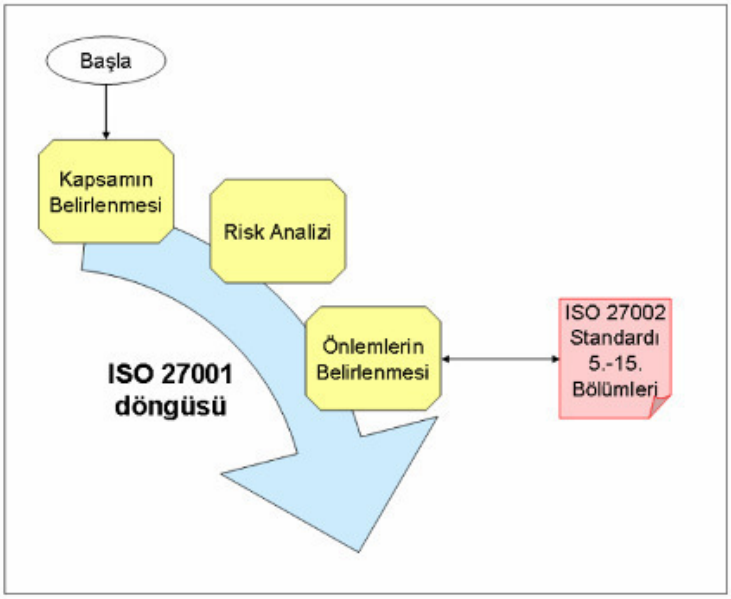


Şekil 1 - ISO 27001 standardında bilgi güvenliği döngüsü

Bu sürecin planlama adımı içerisinde, kurumda bilgi güvenliği şemsiyesi altında bulunacak varlıkların korunması için risk analizi çalışmasının yapılması gerektiği kaydedilmekte, bu çalışmanın sonuçları göz önünde bulundurularak ISO

95 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 (18.06.2010)

27002 standardında tanımlanan önlemlerden kuruma en iyi hizmet edecek olanların seçilmesi ve uygulanması talep edilmektedir. Bu durum Şekil-2'de özetlenmektedir.



Şekil 2 - ISO 27001 döngüsünün planlama aşamasında ISO 27002 kontrollerinin seçilmesi

Böylece ISO 27001 ve ISO 27002 standartları arasındaki ilişki kurulmuş olmaktadır. Şöyle ki, ISO 27001 standardında tarif edilen döngü, ISO 27002 standardından seçilen önlemler için çalıştırılarak bilgi güvenliği süreci gerçekleştirilmeye ve yaşatılmaya çalışılmaktadır.

Bilgi güvenliğinde esas olanın ISO 27001 süreci olduğu, bu süreçten kopuk, dolayısı ile ölçülmeyen, kayıtların oluşturulmadığı, tetkik ve gözden geçirmelerin yapılmadığı, düzeltici ve önleyici faaliyetlerin gerçekleştirilmediği bir sistemde önlemlerin kuruma hizmet etmeyeceği rahatlıkla söylenebilir. [96]

96 Fikret Ottekin, Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri, 2008, http://www.bilgiguvenligi.gov.tr (22.06.2010)

3.1.5.3. ISO 27002

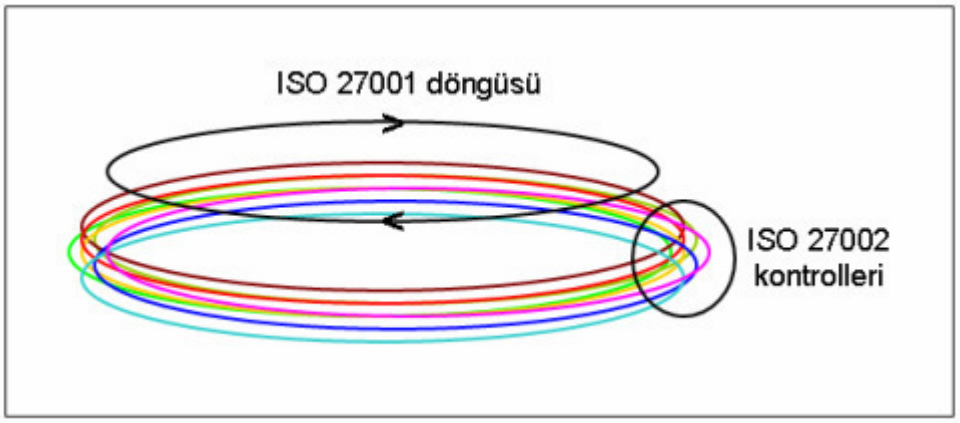
2007 Temmuzunda, diğer ISO/IEC 27000 serisi standartlarla aynı çatı altında toplamak için ISO/IEC 17799:2005 standardı ISO/IEC 27002:2005 olarak yeniden numaralandırılmış ve "Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi İçin Uygulama Kodları" olarak isimlendirilmiştir. Şu anda uygulanmakta olan standart, 2000 yılında BS (İngiliz Standardı) 77991:1999'dan kelime kelime kopyalanarak oluşturulan ISO/IEC'nin ilk basımının revize edilmiş halidir.

ISO 27002 Bilgi Güvenliği Yönetim Sistemi İçin Uygulama Kodları Standardı ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ikinci standardı olup ISO 27001 Bilgi Güvenliği Yönetim Sistemine göre sistem kurmuş firmaların performanslarını arttırmak için uyguladıkları bir standarttır. Genel olarak ISO 27002 standardı aşağıdaki amaçları gerçekleştirmektedir:

- Risklerin değerlendirilmesi
- Güvenlik politikalarının hazırlanması
- Kurumların güvenlik yönetimi organizasyonlarının kurulması
- Varlık yönetiminin kurulması
- Kurum insan kaynaklarının, alt yüklenici veya dış kaynak çalışanlarının yönetimi
- Fiziksel ve çevresel güvenliklerin sağlanması
- Erişim kontrollerinin denetlenmesi
- Güvenlik uygulamaları için kurumsal gelişim, edinme ve gereksinimlerin karşılanması
- Olay ihlal yönetiminin kurulması
- İş sürekliliği prosedür veya planlarının hazırlanması
- Teknik ve yasal mevzuata uyumluluk

ISO 27002 standardı Bilgi Güvenliği Yönetim Sistemini uygulamak, yerleştirmek ve sürekliliğini sağlamak ile sorumlu olan kişilere bilgi güvenliği yönetimi için en iyi uygulama çözümleri ile ilgili öneriler getirir.

ISO 27002 standardı, bilgi güvenliği sürecinde işletilebilecek tedbirleri içeren bir önlem havuzudur. [97] ISO 27002 standardının giriş bölümünde bilgi güvenliğinin seçilen önlemler aracılığı ile gerçekleştirileceği belirtilmekte, her önlem için uygulama, izleme ve iyileştirme çalışmalarının yapılması gerektiği belirtilerek ISO 27001 döngüsüne gönderme yapılmaktadır.



Şekil 3 - ISO 27001 döngüsü ve ISO 27002 kontrolleri

Özetle, Şekil-3'de de görüldüğü gibi, önlemler ISO 27002 standardında, önlemlerin nasıl yaşatılacağı ise ISO 27001 standardında açıklanmaktadır. [98]

97 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297 (18.06.2010)
98 Fikret Ottekin, Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri, 2008, http://www.bilgiguvenligi.gov.tr (22.06.2010)

3.1.5.4. Cobit

Kurumlarda bilgi güvenliği standartlarının sağlanabilmesi için, öncelikle bilgi teknolojileri sistemlerinin yönetim stratejilerinin neler olacağının belirlenmesi gerekmektedir. Cobit standardının amacı, yöneticilere, denetçilere ve bilgi teknolojileri kullanıcılarına iş hedeflerinin bilgi işlem hedeflerine dönüşümünü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirirken, aynı zamanda bilgi teknolojileri alt yapılarını da etkin kullanmayı sağlamaktır.

Cobit, yönetici, denetçi ve kullanıcılara bilgi teknolojileri sistemlerini anlamada, şirketlerin varlıklarını korumak için bilgi teknolojileri yönetişim modeline göre gerekli olan güvenlik ve kontrol seviyelerine karar vermede yardımcı olmaktadır.

Yöneticiler Cobit'ten, bilgi teknolojileri alanında daha etkili kararlar verme ve kuruluş için doğru yatırımlar yapma maksadıyla yararlanmaktadır. İçerdiği stratejik bilgi teknolojisi planı, bilgi mimarisi, stratejiyi işletmek için gerekli bilgi teknolojisi donanım ve yazılımları, bilgi teknolojileri performansını izleme sistemi ile Cobit karar vermeyi daha etkili hale getirmektedir. Bilgi teknolojileri kullanıcıları ise Cobit'ten, kontrol, güvenlik ve süreç yönetimi güvencesi sağlanması şeklinde yararlanmaktadır. Cobit, denetçilerin ise bilgi teknolojileri altyapısı içindeki sorunları kontrol esasları çerçevesinde belirlemelerine yardımcı olmaktadır. Ayrıca denetçilerin kendi denetim bulgularını onaylamaktadır. [99]

99 http://tr.wikipedia.org/wiki/Cobit (30.09.2010)

3.2. BİLİŞİM SUÇLARININ TÜRK HUKUK SİSTEMİNDEKİ YERİ

3.2.1. Mevcut Hukuki Durum

Türk Ceza Kanunu (TCK) - 5237

Bilişim suçları, Türk hukukunda 1990'lı yıllardan itibaren yer bulmaya başlamıştır. 1991 yılında 765 sayılı Türk Ceza Kanunu'na, 3756 sayılı Kanun'la "Bilişim Alanında Suçlar" adıyla 525/a, 525/b, 525/c ve 525/d maddelerinden oluşan bir bab eklenmiş ve bilişim suçları Türk hukukunda yasal boyut kazanmaya başlamıştır. Bu babdaki bilişim suçları, 1989 Türk Ceza Kanunu Tasarısından çok küçük değişikliklerle alınmıştır.

TCK'daki bu maddelerde ilk olarak bir kısım bilişim suçları yer aldığında, ülkemizde bilişim sistemlerinin, bilgisayarların ve internetin kullanımının sınırlı olması sebebiyle konu Türk hukukuna da yabancı idi. Zamanla bilişim sistemlerinin yaygınlaşması, bilgisayar ve internet kullanımının artmaya başlaması, özellikle bankacılık sektöründe otomatik para çekme makinelerinin (ATM) ve online bankacılık hizmetlerinin artması, bilişim suçlarını tartışılmaya değer önemli bir konu haline getirmiştir. [100]

Bilişim suçları 26.09.2004 gün ve 5237 sayılı yeni TCK'da da, "bilişim alanında suçlar" (243, 244, 245, 246. maddeler) ve "özel hayata ve hayatın gizli alanına karşı suçlar" (135, 136, 138. maddeler) bölümlerinde ele alınmaktadır. Bu bölümlerde düzenlenen suçlara konu olan fiiller özellikle bilişim sistemleriyle işlenebilir ve genellikle günümüzde bilişim sistemleri dışında işlenebilme olanakları çok kısıtlıdır. Dolayısıyla klasik suçların yanında yalnızca bilişim suçu olarak

100 Ali Karagülmez, Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara, 2005, s.123

nitelendirilebilecek suç tipleri de ortaya konulmaktadır. Sayılan suçlarla beraber, TCK'nın farklı bölümlerinde bilişim sistemleriyle işlenebilmesi mümkün olan suç tiplerine de yer verilmiştir. Ancak yeni suç işleme modellerinin ve gelişen teknolojinin sıkça görülmesi nedeniyle bu tür suçlar arasında net ve kesin bir ayrım bulunmamaktadır. [101]

Bu bağlamda bu suç tiplerini hukuki zemine oturtmak bir hayli güç olmaktadır. Kanunlarda boşluk bulunması ve istenilen seviyeye gelememesi veya mevcut kanunların yorumlanmasında yaşanan sıkıntılar uygulamada kendini göstermektedir. Nitekim ekte örnekleri verilen Yargıtay kararlarında, uygulamadaki sıkıntılar açıkça gözükmektedir.

TCK 243. madde:

"*(1) 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.*

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

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

şeklinde olup, hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçunu ele alınmıştır.

765 sayılı eski TCK'da yer almayan "Bilişim sistemine girme" suçu, böylece TCK'da düzenlenmiş, böylece verilerin ele geçirilmesi şartı aranmaksızın bilişim sistemine hukuka aykırı olarak girilmesi ve bu suretle bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmiştir. Böylelikle, bilişim sistemine her hangi bir zarar verilmese, bilişim sistemi üzerindeki veriler silinip, değiştirilmese

101 M. Dülger, 2004, s. 114

veya yetkisiz olarak girişi yapılan bilişim sisteminin çalışması engellenip, bozulmasa dahi bilişim sistemine yetkisiz olarak her ne suretle olursa olsun girilmesi ve girildikten sonra orada kalınması suç olarak sayılmıştır. [102]

Bu suç tipi ile korunmak istenilen hukuksal yarar, bilişim sisteminin güvenliğinin sağlanmasıdır. Bunun yanı sıra, bilişim sistemini kullananların çıkarlarının zedelenmemesi de korunan hukuksal yararlar arasındadır. [103]

Ekte yer alan Yargıtay kararlarından, özellikle 11. Ceza Dairesi'nin verdiği 2007/2551 nolu karar örnek teşkil edecek niteliktedir. E-posta yoluyla virüs göndererek bir şirketteki bilgisayarlara zarar verdiği iddia edilen sanık hakkında açılan dava ile ilgili olarak gelen temyiz başvurusu sonunda, Yargıtay 11 Ceza Dairesi, bilgisayar ve internet yoluyla işlenen suçlarla ilgili olarak bilgisayar aramalarının nasıl yapılacağı, dijital delillerin hangi usullerle inceleneceği ve e-postaların kaynağının nasıl araştırılması gerektiğine dair örnek bir karar vermiştir.

Bu kararda, bir e-postanın kimden geldiğinin tespiti için, ilk olarak e-postayı gönderen IP adresinin bulunması, daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin açık adres ve kimlik bilgilerinin talep edilmesi ve bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılması gerektiği hususlarına dikkat çekilmiştir.

Ek-1'de de görüldüğü üzere, Yargıtay kararlarının önemli bir bölümünde, inceleme eksikliğinden ötürü hüküm bozma kararı verilmiştir. Bilgisayarlardan ve ağlardan elde edilen dijital delillerin zaman damgası içerecek şekilde yedeğinin

102 http://www.ekizer.net/ (13.05.2010)
103 A. Karagülmez, 2005, s.167

alınması gerekmektedir. Ayrıca yapılacak inceleme ve teknik takip, şüpheye yer bırakamayacak şekilde somut olarak ortaya koyulmalıdır.

Yargıtay kararlarında hüküm bozma gerekçesi olarak öne çıkan bir diğer faktör de, TCK'nın bahsettiğimiz 243. ve birazdan değineceğimiz diğer maddelerinin, kararlar alınırken dikkate alınmaması veya yanlış yorumlanmasıdır.

TCK 244. madde:

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

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

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

(4) 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."

şeklinde olup, bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu ile bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu ele alınmıştır.

1. ve 2. fıkralarda tanımlanan bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçlarıyla korunmak istenilen hukuksal yarar, karma bir nitelik göstermektedir. Bu suç tanımlarıyla bilişim sistemlerinin yalnızca veri ve yazılımlardan oluşan soyut unsurları değil aynı

zamanda somut unsuru olan donanım kısmı da koruma altına alınmıştır. [104] Burada hem bilişim sisteminin ve hem de bu sistemin içerisinde yer alan veriler veya diğer unsurların zarar görmemesi amaçlanmaktadır. [105]

Bu maddeyle birlikte, bilişim suçuna konu olan yazılım ve verilerin koruma altına alınmasının haricinde, bilişim sistemi bütünüyle esas alınarak sistemin işleyişini bozmak, yok etmek, erişilmez kılmak da suç saymıştır. Dolayısıyla bilişim sisteminin kullanıcıları da böylelikle koruma altına alınmıştır.

Maddenin 3. fıkrasında, 1. ve 2. fıkradaki suçların ağırlatıcı nedeni düzenlenmiştir. Bu ağırlatıcı nedenin kabul edilmesinin nedeni, özel kurumlardan banka ve kredi kurumlarının bilişim suçlarında mali çıkar sağlamak amacıyla en çok hedef alınan kesimi oluşturması, kamu kurum ve kuruluşlarına ait bilişim sistemlerine yönelik suçların kişisel bir bilişim sistemine yönelik suça nazaran daha vahim sonuçlara ve zararlara neden olmasıdır.

4. fıkrada ise, 1. ve 2. fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisine veya başkasına yarar sağlaması suç olarak tanımlanmıştır. [106]

TCK 245. madde:

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

104 M. Dülger, 2004, s. 231
105 A. Karagülmez, 2005, s.187
106 Mustafa Akın, Ali Parlar, Muzaffer Hatipoğlu, Bankacılık Ceza Hukuku, Ankara, 2010, s. 678-680

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

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

(4) Birinci fıkrada yer alan suçun;

a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,

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

c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

(5) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır."

şeklinde olup, banka veya kredi kartlarının kötüye kullanılması suçu ele alınmıştır.

Bu maddeyle banka veya kredi kartlarının kötüye kullanılması eylemleri bağımsız bir suç tipi olarak düzenlenmiştir. Burada amaçlanan banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulması, bu yolla çıkar sağlanmasının önlenmesidir. Aslında hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının işlenme şekillerinin tümünü de içeren bu fiiller, duraksamaları ve içtihat farklılıklarını önlemek amacıyla bağımsız suç haline getirilmişlerdir. Bu itibarla bu suçla aynı zamanda mağdurun malvarlığının korunması da amaçlanmıştır. [107]

107 M. Akın, A. Parlar, M. Hatipoğlu, 2010, s. 701-702

TCK 246. madde:

"*(1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur*."

şeklinde olup, tüzel kişiler hakkında güvenlik tedbiri uygulanması için 243. 244. ve 245. maddelerde düzenlenen suçlarla ilgili ortak bir düzenlemeye yer verilmiştir. Buna göre, bu suçların işlenmesi suretiyle tüzel kişilerin haksız menfaat sağlamaları durumunda, bu özel hukuk tüzel kişileri hakkında bunlara özgü güvenlik tedbirlerine hükmolunmaktadır. Yasa koyucu, bu bölümde yer alan suçların (Bilişim Alanında Suçların) işlenmesi suretiyle özel hukuk tüzel kişilerin yararına haksız menfaat sağlanmasının yarattığı toplumsal tehlikeyi gözeterek, tüzel kişilerin suç işlenmesinin odak noktası olmalarının önüne geçmeyi amaçlamıştır. [108]

TCK 135. madde:

"*(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.*

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır."

şeklinde olup, kişisel verilerin kaydedilmesi suçu ele alınmıştır.

Bu maddeyle, kişisel veri olarak kabul edilen gerçek kişilerle ilgili her türlü bilgi kastedilmekte ve böylelikle de kişinin özel hayatı güvence altına alınmaktadır.

108 M. Akın, A. Parlar, M. Hatipoğlu, 2010, s. 747

TCK 136. madde:

"*(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.*"
şeklinde olup, kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu ele alınmıştır.

Bu madde, 135. maddenin bir sonraki aşamasını ele almaktadır. Özellikle internetin yaygınlaşması ve iletişimi kolaylaştırması ile bu suçun işlenmesi de çok kolay bir hal almıştır. Öyle ki, elde edilen bilgiler, internet ortamında pazarlanıp elden ele dolaşmaya başlamıştır.

Şubat 2009'da yüzbinlerce öğretmenin TC kimlik numaralarının da yer aldığı, Milli Eğitim Bakanlığının Bilişim Sistemleri (MEBBİS) projesi kapsamında uygulamaya koyduğu ve eğitim alanındaki birçok hizmetin sanal ortama taşınmasını sağlayan İl ve İlçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'ndeki (İLSİS) tüm verilerin, internette bir paylaşım sitesinde paylaşıma açıldığı ortaya çıkmıştır. Bu olaydan bir süre sonra yine benzer bir olayda, 24 Temmuz 2010 tarihinde EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına bağlı olarak İstanbul Emniyet Müdürlüğü bünyesinde çalışan Bilişim Suçları ve Sistemleri Şube Müdürlüğünün yaptığı operasyonda, 70 milyon Türkiye Cumhuriyeti vatandaşına ait adres, telefon ve kimlik bilgilerinin yer aldığı listeler bulunduran ve bu bilgileri sattıkları iddia edilen 15 kişi gözaltına alınmıştır.

Birçok kamu kurumu ve özel şirketin işlemlerini internet üzerinden gerçekleştirmesiyle birlikte, kişisel veriler daha da önemli bir hal almıştır. TC kimlik numarası bilgileriyle birlikte kamu kurumları, bankalar, sigorta şirketleri, sağlık kuruluşları, eğitim kurumları aracı kullanılarak çok daha fazla bilgiye de ulaşmak mümkündür. Kaldı ki artık sadece kimlik numarası bilgisiyle dahi birçok kişiye özel işlem yapılabilmektedir.

TCK 138. madde:

"*(1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde altı aydan bir yıla kadar hapis cezası verilir.*"

şeklinde olup, verilerin yok edilmemesi suçu ele alınmıştır.

Bu madde diğer iki maddeden farklı olarak (135 ve 136. maddeler), kişisel verilerin hukuka uygun olarak elde edilmiş olsalar bile, kanunların belirlediği süreler zarfında yok edilmemesinin de bağımsız bir suç olduğunu ortaya koymaktadır. Kişisel veri bulunduran kamu kurumlarıyla beraber, özel kurum ve kuruluşlar da bu madde kapsamı altında olup, bu verileri zamanında yok etmeye dikkat etmeleri gerekmektedir.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun - 5651

23.05.2007 gün ve 26530 sayılı Resmi Gazete'de yayımlanarak 3. ve 8. maddesi yayımı tarihinden altı ay sonra, diğer maddeleri yayımı tarihinde yürürlüğe giren, 14 madde ve bir geçici maddeden oluşan 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki Kanun ile Türk hukukunda ilk kez internet erişimine düzenleme getirilmiştir.

Kanunun öncelikle amacı, içerik sağlayıcı, yer sağlayıcı, erişim sağlayıcı, toplu kullanım sağlayıcı gibi internet aktörlerinin sorumluluklarını düzenlemek, internet servislerinin denetlenmesi yoluyla internet üzerinden zararlı içeriklerin yayılmasını engellemektir. İnternet erişiminin kanunla kontrol altına alınması ile birlikte, internet üzerinden işlenen bilişim suçlarının önemli ölçüde önüne geçilmesi ve suç unsuru içeren herhangi bir olay sonrasında suçlu ya da sorumluların daha

kolay tespit edilmesi beklenmektedir. Ayrıca kullanıcıların internet üzerinden aldatılmaları ve kötü amaçlı içeriklerden korunması da bu kanunla amaçlanmaktadır.

Kanuna göre, erişimin engellenmesi kararı, adli makamların yanısıra idari makam olan Telekomünikasyon İletişim Başkanlığı tarafından da verilebilmektedir. Erişimin engellenmesi kararı, soruşturma evresinde hakim, kovuşturma evresinde ise mahkeme tarafından verilmektedir. Soruşturma evresinde, gecikmesinde sakınca bulunan hallerde ise Cumhuriyet savcısı tarafından da erişimin engellenmesine karar verilmektedir. İçerik veya yer sağlayıcısının yurt dışında bulunması halinde ya da içerik veya yer sağlayıcısı yurt içinde bulunsa bile, içeriği çocukların cinsel istismarı ve müstehcenlik suçları oluşturan yayınlara ilişkin olarak erişimin engellenmesi kararı re'sen Telekomünikasyon İletişim Başkanlığı tarafından da verilebilmektedir.

Tablo 1 - Erişimi Engellenen Site Sayıları

Suç Türleri	**Re'sen**	**Yargı**
Kumar oynanması için yer ve imkan sağlama	69	17
Bahis / Kumar	36	3
Sağlık için tehlikeli madde temini	0	0
İntihara yönlendirme	1	0
Uyuşturucu / Uyarıcı madde kullanımını kolaylaştırma	0	1
Atatürk aleyhine işlenen suçlar hakkında kanundaki suçlar	2	50
Fuhuş	10	2
Çocukların cinsel istismarı	499	5
Müstehcenlik	422	38
Diğer	0	154
Toplam	**1039**	**270**

Tablo - 1, 23.11.2007 ve 21.11.2008 tarihleri arasında erişimi engellenen site sayısını ve erişimin engellenmesine sebep olan suç türlerini göstermektedir. [109] Bunlardan 1039'u re'sen, 270'i ise yargı kararıyla olan erişim engellemelerdir.

Son günlerde, dünya genelinde bilinen youtube.com, dailymotion.com, myspace.com gibi belli başlı sitelerin erişimlerinin engellenmeleriyle, kamuoyu bu konuyla daha çok ilgilenmeye başlamıştır. Erişim engellemelerinin, uygulamada yasakçı ve sansürcü bir çizgide gerçekleştiğini ifade eden kitle, uygulanan bu yasakların ve bürokratik engellerin, iletişimi boğacağını, yeni kuşakların girişimci, bağımsız, özgür bireyler olarak gelişmesine ve ülkenin kalkınmasına olumsuz etkileri olacağını düşünmektedirler.

İnternetin tamamen başıboş bırakılması hiç kuşkusuz sakıncalı olduğu gibi, sınırlamaların da belli ölçüler içerisinde olması gerekmektedir. Bu sınırlamaların çerçevesi çizilirken toplum değerleri, teknolojik ilerleme, hukuki boyut tümden ele alınmalı, uygulamada ortaya çıkabilecek bu ve benzeri problemler öngörülmelidir. Mevcut yasanın getirdiği düzenlemeler birçok yönden faydalı olmakla beraber, bahsedilen bu tip problemler ortak akılla değerlendirilmeli ve gerekli değişiklikler yapılmalıdır.

Fikir ve Sanat Eserleri Kanunu (FSEK) - 5846

5.12.1951 tarihli ve 5846 sayılı Fikir ve Sanat Eserleri Kanunu'nun 2. maddesinde 7.6.1995 tarihli ve 4110 sayılı Kanunla yapılan değişiklikle "herhangi bir şekilde dil ve yazı ile ifade olunan eserler ve her biçim altında ifade edilen bilgisayar programları ve bir sonraki aşamada program sonucu doğurması koşuluyla bunların hazırlık tasarımları" da "eser" sayılarak, bilgisayar programlarına yönelik bu kanun kapsamındaki fiiller de suç sayılmıştır. [110] Bu sayede fikri mülkiyet

109 http://www.tib.gov.tr/dokuman/faaliyet_raporu.pdf (19.10.2010)
110 A. Karagülmez, 2005, s.123

kapsamında olan eser kavramının içeriğine bilgisayar programları da dahil edilmiş, böylelikle bilgisayar programları üzerindeki manevi ve mali hakların kasten ihlali halinde de failin cezalandırılması öngörülmüştür.

FSEK'te 4110 sayılı yasa ile yapılan değişiklikte, Kanun'un 6. maddesine 10. bent eklenmiş ve bir bilgisayar programının uyarlanması, düzenlenmesi veya programda herhangi bir değişim yapılması da ayrı bir fikir ve sanat eseri sayılmıştır. FSEK'teki bu değişiklik Avrupa Yazılım Yönergesi'nden esinlenilerek yapılmıştır. Bu değişiklikle 14.05.1991 tarihli ve 91/250/EEC sayılı Avrupa Konseyi direktifiyle FSEK arasında uyum sağlanmıştır. [111]

5846 sayılı Fikir ve Sanat Eserleri Kanunu'na 2001 tarihli ve 4630 sayılı yasa ile "Tanımlar" başlıklı 1/B maddesinin (g),(h),(ı) bentlerinde "Bilgisayar programı", "Arayüz", "Araişlerlik" kavramlarının açıklamaları ilave edilmiştir. Fikir ve Sanat Eserleri Kanunu'na bu kavramların girmesiyle, bilişim endüstrisinin ürünleri olan bilgisayar programlarının üzerindeki fikri haklar koruma altına alınmaktadır. [112]

Elektronik İmza Kanunu (EİK) - 5070

15 Ocak 2004 tarih ve 5070 sayılı Elektronik İmza Kanunu, elektronik imza konusunda temel yasal düzenlemedir. Elektronik imza, bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti etmektedir. Bu kanun ile elektronik imzanın hukuki yapısı, elektronik sertifika hizmet sağlayıcılarının faaliyetleri, hukuki yetki ve sorumlulukları ile elektronik imzanın kullanımına ilişkin bağlayıcı temel hususlar düzenlenmektedir. Kanun yayımı tarihinden altı ay sonra yürürlüğe girmiştir.

111 M. Dülger, 2004, s. 293
112 a.g.e., s. 293

3.2.2. Hukuki Düzenlemeler

Özellikle internet kullanımının artmasıyla, bilişim suçu olayları ve bilişim suçu mağdurları sayısında hızlı bir artış meydana gelmiştir. Benzer biçimde, bilişim suçu olaylarının işlenme biçimleri de her geçen gün yeni bir boyut kazanmakta, mevcut yasalar ve yönetmelikler, bu konuda yetersiz kalabilmektedir.

Bilişim suçları, ceza kanunlarında düzenlenen birçok suç tipinin aksine statik değil dinamik bir yapı göstermektedir. Bu özelliğinin bir sonucu olarak, bu alanda yapılan düzenlemelerin, gelişen teknolojiyle paralel güncellenmesinin yapılması, yeni çıkan suç işleme şekillerinin hukuka aykırı eylem olarak hüküm altına alınması gerekmektedir. Kanunlaştırma çalışmaları mukayeseli hukukla paralel yapılmalı, uluslararası çalışmalar ile bilişim sistemlerinin teknolojik boyutu göz önünde bulundurulmalıdır. [113]

Bilişim suçları ile ilgili olarak, Adalet Bakanlığı tarafından "Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı" yayınlanmıştır. Tasarının kanunlaşması halinde, Türk Ceza Kanunu'nda düzenlenen gerek bilişim sistemleri aracı kılınarak işlenen suçlar, gerekse de bilişim alanında suçlar, kendi özel kanunu içerisinde yer bulacaktır. Bilişim ağı hizmetlerine yönelik özellikle "içerik sağlayıcı", "yer sağlayıcı", "erişim sağlayıcı", "hizmet sağlayıcı" ve "toplu kullanım sağlayıcı" gibi temel ifadelerin netleştirilmesi, bilişim suçlarıyla ilgili tanımlamaların net olarak ortaya konması, yanlış anlamaların önüne geçeceği gibi mahkemelerce mevzuattaki hükümlerin yorumlanma sorununu da engelleyecektir.

113 Olgun Değirmenci, Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi, Çağın Polisi Dergisi, Sayı 37, 2005

Bilişim suçları yasa tasarısıyla ilgili son olarak, Adalet Bakanlığının tasarı üzerinde çalıştığı ve Ulaştırma Bakanlığının da tasarıya teknik yönden destek olduğu açıklanmıştır. Bu düzenlemeyle birlikte, gazete ve televizyonlarda olduğu gibi internet sitelerinin sahip, sorumlu yazı işleri müdürleri, muhabirlerinin yaptıkları haberlerin suç olması durumunda izlenilecek yolun da tarif edileceği belirtilmiştir. Bu düzenlemelerle birlikte, internet ortamında işlenen çeşitli suçların takibi, cezalandırılması da daha kolay hale gelecektir.

3.3. EGM UYGULAMALARI

3.3.1. Genel Çalışmalar

Emniyet Genel Müdürlüğü bünyesinde 18.04.1998 tarihinde "Bilgisayar Suçları ve Bilgi Güvenliği Kurulu", bu kurula bağlı olarak da 01.03.1999 tarihinde "Bilişim Suçları Çalışma Grubu" oluşturulmuştur. Bu çalışma grubunun oluşturulma amacı bilişim alanındaki hak ihlallerini araştırmak, bu alandaki suç tiplerini belirlemek, ilgili Daire Başkanlıklarının yönetmeliklerinde gerekli düzenlemeleri yapmak olarak belirlenmiştir. Bilişim Suçları Çalışma Grubu kurulduğu 1 Mart 1999 tarihinden itibaren kendine 4 aylık bir çalışma programı belirlemiştir. Bu çalışma grubuna görev alanları itibariyle;

- Teknolojik gelişmeleri takip etmek ve bu konularda yönlendirme yapmak üzere Bilgi İşlem Daire Başkanlığı,

- Yazılım korsanlığı, bilgisayar sistemleri kullanılarak meydana gelen dolandırıcılıklar ve kredi kartları dolandırıcılığı konusunda düzenlemeler yapmak üzere Kaçakçılık ve Organize Suçlar Daire Başkanlığı,

- Dijital ortamda yayınlanan dergi, gazete ve benzeri yayınları incelemek ve bu konudaki çalışmaları yapmak üzere Güvenlik Daire Başkanlığı,

- Bilişim alanında işlenen suçlarda iz ve deliller konusunda çalışma yapmak üzere Kriminal Polis Laboratuvarları Daire Başkanlığı,

- İnterpol üyesi ülkelerle irtibatı ve karşılıklı bilgi aktarımını sağlamak üzere İnterpol Daire Başkanlığı,

- Üniversitelerle bağlantıları yapmak üzere Polis Akademisi Başkanlığı,

- Yapılacak yönetmelik çalışmalarında bulunmak üzere Hukuk Müşavirliği üyeleri dahil edilmişlerdir.

Çalışmaya son şeklini vermek üzere 07.06.1999-11.06.1999 tarihleri arasında Bilgi İşlem Daire Başkanlığı bünyesinde ortak bir görevlendirme ile bilişim suçlarının tasnifi yapılmış, Daire Başkanlıklarının görev alanları tespit edilmiş ve polisin olay yerinde bilgisayar ve bilgisayar sistemleri ile karşılaştığında yapması gerekenler çalışma grubu sonuç raporu içinde tanzim edilmiştir. [114]

3.3.2. İdari Yapılanma

Türkiye'de Emniyet Teşkilatı'nda bilişim suçları ile ilgili ilk birim, Bilgi İşlem Daire Başkanlığı bünyesinde 1997 yılında Bilişim Suçları Bürosu ismiyle kurulmuştur. 2001 yılında bu büronun adı İnternet ve Bilişim Suçları Şube Müdürlüğü olarak değiştirilmiştir. Bu birimin dışında da diğer daire başkanlıkları altında Bilgi İşlem Şube müdürlükleri kurulmuştur. Bu daireler kendi görev alanlarına giren konularda bilişim suçları ile mücadele etmektedir. Ayrıca merkez teşkilatı içinde yukarda bahsedilen Bilgisayar Suçları ve Bilgi Güvenliği Kurulu oluşturulmuştur. 2001 yılında Kaçakçılık ve Organize Suçlar Daire Başkanlığı ile Birleşmiş Milletler tarafından ortaklaşa kurulan TADOC (Turkish Academy Against Drug and Organised Crime) bünyesinde de Bilişim Suçları Araştırma Merkezi oluşturulmuştur. Bu merkez faaliyetlerinde daha çok bu suçlar ile mücadelede, ilgili birimlere yol göstermek amacıyla akademik destek niteliğinde çalışmalar yapmaktadır. Bu merkezi yapılanmanın yanında büyük illerde de bilgi işlem büroları

114 Bilişim Suçları Çalışma Grubu Raporu, EGM, s.4

kurulmuş ve bu alanda karşılaşılan sorunlar ile ciddi anlamda mücadeleye başlanmıştır.

Emniyet Genel Müdürlüğü bünyesinde Kaçakçılık ve Organize Suçlarla Mücadele Dairesi Başkanlığı koordinatör daire başkanlığı olarak belirlenmiştir. Bu koordinasyona Terörle Mücadele Daire Başkanlığı, Asayiş Daire Başkanlığı ve Güvenlik Daire Başkanlığı dahil edilmiştir. İstisnai olarak İstihbarat Daire Başkanlığı bu koordinasyondan bağımsız olarak Bilişim Suçları ile mücadele alanında faaliyet göstermektedir.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde yer alan Bilgi İşlem Büro Amirliği, 20.04.2003 tarihinden itibaren Yüksek Teknoloji Suçları ve Bilişim Sistemleri Şube Müdürlüğü adını alarak Bilişim Suçlarıyla mücadeleye başlamıştır. 5237 sayılı TCK'da yer alan ifadesiyle örtüşmesi açısından, E.G.M. Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Merkez ve İl Teşkilatı Kuruluş, Görev ve Çalışma Yönetmeliği'nde 03.01.2006 tarihinde yapılan değişiklikle; "Bilişim Suçları ve Sistemleri Şube Müdürlüğü" adını almıştır. [115]

3.3.3. KOM Çalışmaları

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, il KOM birimleri ile koordineli olarak bilişim suçlarıyla mücadele çalışmalarını yürütmektedir.

Tablo 2'de görüldüğü üzere, 2009 yılında il KOM birimleri tarafından 2871 adet operasyon gerçekleştirilmiştir. Gerçekleştirilen operasyonların, banka ve finans

115 Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Raporu, EGM, Ankara, 2006

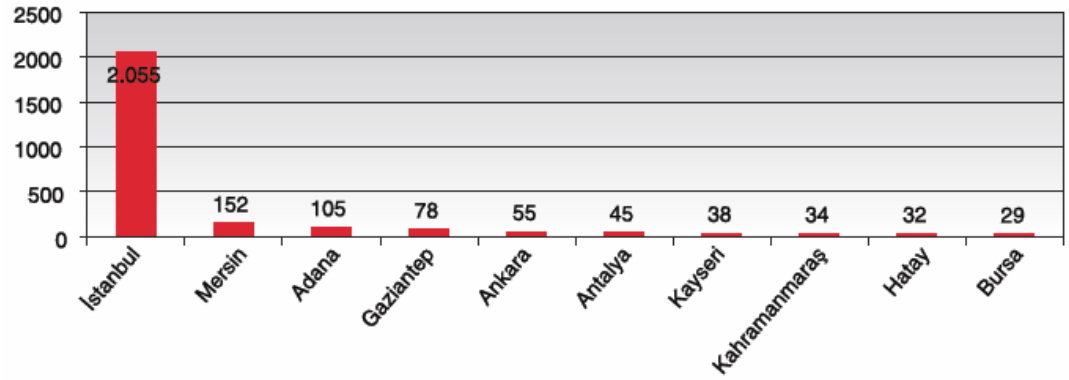
kurumlarına karşı işlenerek karşılığında maddi menfaat sağlanan suçlara karşı yoğunlukta olduğu gözlenmektedir.

Tablo 2 - 2009 Yılında Meydana Gelen Bilişim Suçları Olay ve Şüpheli Sayıları

Olay Türü	Olay	Şüpheli
Banka ve Kredi Kartı Dolandırıcılığı	1511	2176
İnteraktif Banka Dolandırıcılığı	550	1113
Bilişim Sistemlerine Girme, Sistemi Engelleme, Bozma, Verileri Yok Etme, Değiştirme	353	534
İnternet Aracılığıyla Nitelikli Dolandırıcılık	412	731
Diğer	45	116
Toplam	2871	4670

KOM Daire Başkanlığı koordinesinde gerçekleştirilen operasyonlarda, "uyuyan hesap" şeklinde tabir edilen, internet bankacılığı işlemlerine açık olmayan, üzerinde uzun süre işlem yapılmayan hesaplara ait müşteri bilgilerinin, suç örgütü üyelerince çeşitli yollarla ele geçirildiği ve ele geçirilen bu bilgiler aracılığı ile dolandırıcılık yapıldığı tespit edilmiştir. Bu bilgilerle düzenlenen sahte kimliklerle bankalara müracaat edildiği veya telefon bankacılığı aracılığı ile söz konusu hesaplara internet bankacılığı kullanıcı şifresi alındığı ve müşteriler tarafından bankaya bildirilen irtibat telefon numarasının değiştirildiği ya da ilgili telefon operatörüne sahte kimliklerle kayıp/çalıntı müracaatında bulunularak yenisinin alındığı belirlenmiştir.

KOM Daire Başkanlığı 2009 raporuna göre, bilişim suçları olay sayıları illere göre Şekil-4'de incelendiğinde, ilk sırada 2055 olay ile İstanbul, ikinci sırada 152 olay ile Mersin, üçüncü sırada ise 105 olay ile Adana yer almaktadır.



Şekil 4 - 2009 Yılı Bilişim Suçlarında Operasyon Sayılarına Göre İlk On İl

Tablo 3'de ise, KOM Daire Başkanlığı 2008 raporuna göre, 2006, 2007 ve 2008 yılları için bilişim suçları olay ve şüpheli sayıları verilmiştir. [116]

Tablo 3 - Yıllara Göre Bilişim Suçları Olay ve Şüpheli Sayıları

Olay Türü	**2006**		**2007**		**2008**	
	Olay	Şüpheli	Olay	Şüpheli	Olay	Şüpheli
Kredi Kartı Sahteciliği ve Dolandırıcılığı	310	468	594	907	830	991
Banka Dolandırıcılığı	723	1398	642	1187	1177	2114
Bilişim Suçları ve Dolandırıcılığı	178	283	416	764	560	842
Diğer	7	60	91	134	157	416
Toplam	1218	2209	1743	2992	2724	4363

116 Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Raporu, EGM, Ankara, 2009

3.4. YAŞANMIŞ ÖRNEKLER

3.4.1. Sanal Deprem Operasyonu (2008)

EGM KOM Daire Başkanlığı koordinesiyle başlatılan bir çalışmada kredi kartı dolandırıcılığı ile ilgili faaliyet gösteren bir suç şebekesinin varlığı ve bu şebekenin örgüt içi haberleşmesini IRC [117] sunucuları aracılığıyla yürüttüğü tespit edilmiştir. Devamında bu sunucuların irc.realunix.net alan adına sahip olduğu ve sisteme bağlı İngiltere, İsrail, Amerika gibi birçok ülkeden yayın yapan onlarca farklı sunucunun olduğu görülmüştür. TRaVma rumuzlu Türk vatandaşı olan bir şahsın, ana sunucuda en yetkili kişi olduğu ve uluslararası kredi kartı dolandırıcılığı yapan suç şebekesini yönettiği tespit edilmiştir.

Araştırmaların devamında banka ve kredi kartı dolandırıcılığı işlemleri ile ilgili şebekenin haberleşmesini sağlayan www.realunix.net sitesi ve aynı kişiler tarafından kullanılan irc.realunix.net sunucuları ile ilgili olarak teknik takip çalışmalarına başlanmıştır.

Uzun teknik takip çalışması sonucunda İstanbul, Şanlıurfa, Muğla, Kastamonu, Sivas, Diyarbakır, Hatay, Mersin, Kocaeli, İzmir, Çorum, Yozgat ve Ankara illerini kapsayan çalışma operasyona dönüştürülmüştür.

Yapılan eş zamanlı operasyon sonucunda, 29 şahısla birlikte çok sayıda hard disk, boş ve dolu manyetik şeritli kredi kartı, bilgisayar, kodlayıcı cihaz (banka ve

117 IRC: Internet Relay Chat kelimelerinin baş harflerinden oluşan bir kısaltma olup, dünya üzerindeki değişik kullanıcıların internete bağlı oldukları ve de aynı sunucuyu ya da birbirine bağlı sunucuların ağını seçtikleri durumunda birbirleri ile iletişim kurmalarını sağlayan bir protokoldür.

kredi kartı kopyalamaya yarayan cihaz), tapu senedi ve yüksek miktarda nakit para ele geçirilmiştir. [118]

3.4.2. Sanal Tuzak Operasyonu (2008)

Adana KOM Şube Müdürlüğü görevlilerince yapılan bir çalışmada, Adana ilinde kredi kartı dolandırıcılığı alanında faaliyet gösteren bir suç şebekesinin varlığı tespit edilmiştir. Edinilen bilgiler doğrultusunda, şahısların İngiltere'de iken mağdurlara ait kredi kartlarını kopyalamak ve bu suretle haksız kazanç elde etmek üzere şebeke kurdukları, Adana iline gelerek mağdurlara ait kredi kartı bilgilerini kopyalayacak cihazlarını yerleştirmek amacıyla işyeri aradıkları bilgilerine ulaşılmıştır.

Adana KOM Şube Müdürlüğü görevlilerinin şebekeyi çökertmeye yönelik çalışmaları esnasında şebeke içerisinde Türkiye, İngiltere ve Yunanistan vatandaşı şahısların olduğu tespit edilmiş, çalışmalar devam ederken şebeke üyesi üç kişi İstanbul ilinde sahte kredi kartlarını kullanmak üzere iken yakalanmıştır.

İngiltere vatandaşı olan şebeke üyesinin şebeke yöneticisi olduğu ve kart kopyalamaya imkan tanıyan cihazları şebeke üyelerine bizzat temin ettiği tespit edilmiştir.

Şebekeye dair bütün suç unsurları tespit edildikten sonra Nisan 2008 tarihinde "TCK Madde 245 hükmü uyarınca başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı imal etmek, sahte oluşturulan veya

118 Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Raporu, EGM, Ankara, 2008

üzerinde sahtecilik yapılan banka veya kredi kartlarını kullanmak suretiyle haksız kazanç elde etmek" suçundan yasal işlem başlatılmıştır.

Yakalanan on üç şahısla birlikte yaklaşık bin adet kopyalanmış kredi kartı, kodlayıcı cihaz ile birlikte bir miktar yerli ve yabancı para ele geçirilmiştir. [119]

3.4.3. Kimlik Numarası Operasyonu (2010)

EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına bağlı olarak İstanbul Emniyet Müdürlüğü bünyesinde çalışan Bilişim Suçları ve Sistemleri Şube Müdürlüğünün 24 Temmuz 2010 tarihinde yaptığı operasyonda, 70 milyon Türkiye Cumhuriyeti vatandaşına ait adres, telefon ve kimlik bilgilerinin yer aldığı listeler ele geçirilmiştir. Kamu kurum ve kuruluşlarının veri tabanlarına girerek Türkiye'deki 70 milyon vatandaşın adres, kimlik ve telefon bilgilerini ele geçirdiği öne sürülen 15 kişi gözaltına alınmıştır.

İstanbul Emniyet Müdürlüğü'nden yapılan açıklamada; E.K isimli kişinin liderliğinde kurulan şebekenin resmi ve yarı resmi kurumların alt yapılarında bulunan kimlik bilgisi, telefon ve adres bilgilerine, bu kurumların sistemlerine hukuka aykırı şekilde girerek eriştikleri belirtilmiştir. Ele geçirilen bu bilgiler ile içerisinde yaklaşık 70 milyon Türkiye Cumhuriyeti vatandaşına ait kimlik adres ve sabit telefon bilgilerinin bulunduğu bir data bankası hazırlandığı ifade edilmiştir.

Şüphelilerin ayrıca oluşturulan bu data bankasından sorgu yapabilmek için 'Adres programı' ve ' Telefon sorgu' adı verilen programları yazdıkları ve bu programları bazı hukuk bürolarına para karşılığı sattıkları belirtilmiştir.

119 Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Raporu, EGM, Ankara, 2009

Yaklaşık 8 ay süren çalışmaların ardından operasyon kararı alan Bilişim Suçları ve Sistemleri Şube Müdürlüğü ekipleri İstanbul, Mersin, Antalya, Muğla ve Kayseri'nin de aralarında bulunduğu 7 ilde eş zamanlı baskınlar düzenleyerek şüphelileri gözaltına almış, şüphelilerin sattıkları bilgiler karşılığında 3 milyon liralık gelir elde ettiği ifade edilmiştir. Şüphelilerin ev ve işyerlerinde yapılan aramalarda 16 harddisk, 11 dizüstü bilgisayar, 16 telefon, 20 flash bellek, 82 CD-DVD ve 15 adet hukuk bürolarına satışı yapılan 'Adres programı' ve 'telefon sorgu programı' isimli programlara ait satış sözleşmeleri ele geçirilmiştir. Hukuk bürolarının yaptıkları bu sözleşmeler EGM tarafından Adalet Bakanlığı'na gönderilmiştir. [120]

120 http://www.dha.com.tr/ (11.10.2010)

SONUÇ VE DEĞERLENDİRME

Bilişim suçlarıyla mücadeleyi, uluslararası hukuk bakımından incelersek, tam bir yeknesaklık sağlandığını söylemek çok güçtür. Ülkeler genel olarak kendi politikası ve dünya görüşüne göre düzenleme yapmaktadır. Bazı ülkelerde internete giriş izinle olabildiği gibi, bazılarında devletin kontrolünde olan tek bir servis sağlayıcı bulunabilmektedir. Bazı ülkelerde de devletin politikasına ve dünya görüşüne uymayan sitelere erişim kısmen de olsa engellenebilmektedir.

Avrupa ülkelerine baktığımızda, ülkelerin birbirinden bağımsız düzenlemeye gittikleri görülse de, düzenlemelerde ve uygulamalarda yeknesaklık için çalışmalar başlamıştır. Bilişim suçları alanında şu ana kadar yapılan en kapsamlı çalışma Avrupa Konseyi'nin oluşturduğu "Siber Suçlar Konvansiyonu"dur.

Avrupa Suç Sorunları Komitesi içinde çalışmalarını tamamlayan "Siber Suç Uzmanları Komitesi" tarafından hazırlanan Nihai Faaliyet Raporu Komitenin 18-22 Haziran 2001 tarihleri arasında yapılan 50. Genel Kurulunda onaylanmıştır. Böylece Siber Suç Sözleşmesinin (Convention On Cybercrime) ilk adımı atılmıştır.

23 Kasım 2001 tarihinde imzalanan Siber Suçlar Konvansiyonunun amacı siber suçlar alanında ülkelerin maddi ceza hukuku unsurlarını ve bağlantılı hükümlerini uyumlu hale getirmektir. Bu suçların soruşturulması ve kovuşturulması ve delillerinin elde edilmesi için gerekli olan yerel ceza usul sistemlerini, her yerde birbirinin aynı olabileceği şekilde kurabilmektir. Ulusal düzeyde alınan önlemler ile usulleri uluslar arası alanda aynı yapabilmek için devletler arasında işbirliğini kurmak zorunluluktur. Sözleşme, üye ülkelere ceza kanunları ile düzenlenmesi gerekli olan eylemlerin neler olduklarının açık bir şekilde tespitini, sivil özgürlük ve

güvenlik kavramları arasındaki uyuşmazlıkların nasıl aşılacağını göstermeyi amaçlamaktadır.

Sözleşmeyle, Avrupa Konseyine üye ülkeler arasında ortak bir ceza politikasının oluşturularak toplumun bilişim suçlarına karşı korunması, bu amaçla ulusal mevzuatlarda gerekli düzenlemelerin yapılarak uluslararası alanda da işbirliğinin geliştirilmesi amaçlanmıştır. Sözleşmeyle, bilişim alanına ilişkin olarak bir takım terimlerin tanımları yapılmakla beraber, bilişim ortamında veya bilişim sistemleri vasıta kılınarak işlenebilecek suçlar düzenlenerek bu suçların soruşturulması usulüne ilişkin bir takım hükümlere yer verilmektedir. Ayrıca sözleşmeyle uluslararası işbirliği düzenlenmekte ve bilişim ağında hizmet verenlerin yükümlülüklerine yer verilmektedir. [121]

Ülkemizin de biran önce bu sözleşmeyi imzalayarak, bilişim suçlarıyla mücadelede uluslararası anlamda önemli bir aşamayı gerçekleştirmesi gerekmektedir.

Bilişim suçları yapısı itibariyle, aynı suç için birden fazla ülkeyi ilgilendirebilmektedir. Bilişim suçlarını önlemek için, tüm dünya ülkeleri birlikte hareket etmeli, suçun ortaya çıkarılması, suçluların yakalanması için ortak çalışmalıdır. Benzer yasal düzenlemeler tüm ülkelerde yapılmalıdır. Zira suçluların bulundukları ülkeyle suçu işlediği ülke farklı olabilmektedir. Suçu işleyenler, bulundukları ülkenin yasal boşluklarını kullanmakta, böylelikle yeterli yasal düzenlemesi olmayan ülkelerde işlenen suçlar sadece o ülkeye değil, diğer ülkelere de zarar vermektedir. Teknoloji sınır tanımadığı gibi bilişim suçluları da sınır tanımamaktadır. Bilişim suçlarını birkaç ülke üzerinden gerçekleştiren bu tür failler mücadeleyi gerçekten zorlaştırmaktadırlar. Güvenlik güçleri bu suçlular ile

121 Haldun Yağan, Bilişim Suçları, Gümrük Dünyası Dergisi, Sayı 52, 2007

mücadelede daha önce hiç olmadığı kadar işbirliğine muhtaç ve karşılıklı bağımlıdırlar.

Bilişim suçları türlerinin önemli bir kısmı yasalarımızda suç olarak düzenlenmiş olmakla birlikte teknolojinin hızla ilerlemesi, internetin sürekli yaygınlaşması nedeniyle, zamanla bazı yasal boşluklar da ortaya çıkabilmektedir. Bu sebeple gelişmelerin sürekli takip edilip yasal boşlukların giderilmesi konusunda çalışmalar yapılması gerekmektedir. Ulusal hukuk kuralları teknolojik gelişmelerin gerisinde kalmamalıdır. Daha önce de bahsedildiği gibi, konuyla ilgili olarak yeni bir kanun tasarısı oluşturulmuştur. Ancak suç tiplerinin dinamik olması, her geçen gün farklı şekilde olayların vuku bulması sebebiyle, çıkarılacak kanun daha dinamik yönetmeliklerle de desteklenmeli, kolluk güçleri ve yargı bu konuda olabildiğince geniş yetkilerle donatılmalıdır.

Bilişim suçlarıyla mücadele de belki de en önemli faktör, cumhuriyet savcıları, hakimler ve de kolluk güçleri personelinin konuyla ilgili olarak yeterli bilgiye ve tecrübeye sahip olup olmadıklarıdır. Şu an için İstanbul, Ankara ve İzmir dışındaki kentlerde bilişim davalarını görecek mahkeme olmadığından, bu şehirlerdeki mahkemelerde yığılmalar olmakta, dolayısıyla mahkeme süreleri de uzamaktadır. Kaldı ki daha önce de bahsedildiği gibi, bu suç tipleri gelişen teknolojiyle birlikte her geçen gün artmakta, mevcut mahkemeler ise bu hızı yakalayamamaktadırlar. Bu dinamizmi yakalayabilmek için ülke genelinde hem Adalet Bakanlığı personeline, hem EGM personeline konuyla ilgili eğitimler sağlanmalıdır. Bununla beraber diğer kamu kurumlarındaki çalışanlara, hatta özel sektörde ya da evinde bilgisayar kullananlar için de bu farkındalık oluşturulmalı, gerektiği durumlarda işbirliği yapabilmeleri sağlanmalıdır. Acil durumlarda polisin uluslararası düzeyde işbirliği göstermesinin sağlanabilmesi için 24/7 irtibat noktası acilen tesis edilmelidir. Böylece olaylara müdahalede tek merkezden yönetim esası benimsenmeli ve disiplinler arası çalışmalar zorunlu hale getirilmelidir.

Bu eğitimlere paralel olarak, bilişim suçlarına bakacak ihtisas mahkemelerinin bir an önce oluşturulması sağlanmalıdır. Bu bağlamda, hukuk fakültelerinden başlayarak, bilişim hukuku ayrıntılı olarak ele alınmalı, bu konuda donanımlı hukukçuların yetişmesinin önü açılmalıdır. Zira Yargıtay kararları ele alındığında, Yargıtay'ın genellikle yerel mahkemelerin kararlarını bozduğu, bunun da başlıca sebebinin, bilişim suçlarıyla ilgili maddelerin yerel mahkemelerce yeterli seviyede bilinmediği veya yorumlanamadığı görülmektedir.

Davalara atanacak bilirkişilerin yetersiz olması da süreci olumsuz yönde etkilemektedir. Gerek bilgi yetersizliğinden, gerekse de bilirkişi bulunamamasından dolayı, bilişim davalarına bilirkişi olarak adliyedeki bilgisayar tamircilerinin veya tamamen ilgisiz kişilerin atandığı durumlar ne yazık ki olmuştur. Bilişim suçu içeren davaların, yetki belgesi alan adli bilişim uzmanları tarafından incelenmesi gerekmektedir. Bu kişilerin, gelişen teknolojiye ayak uydurarak, belirli aralıklarla kendilerini yenilemeleri de sağlanmalıdır.

Bugüne kadar işlenen bilişim suçlarına bakıldığında, özellikle maddi açıdan diğer suç tipleriyle kıyaslanamayacak derecelerde tahribata yol açabileceği görülmüştür. Daha önce de bahsedildiği gibi faillerinin bulunması açısından ise diğer suçlara oranla çok kısıtlıdır. Özellikle suçların sanal ortamda işlenmesi, faillerin, işini kolaylaştırmakta, arkalarında bıraktıkları izleri rahatlıkla temizlemelerini sağlamaktadır. O yüzden bilişim suçlarıyla mücadelenin temelini, bu suçların meydana gelmeden engellenmesi oluşturmaktadır.

Daha önce bahsedilen önleyici tedbirlerin, tüm kurum ve kişilerce alınması gerekmektedir. Bunu yaparken özellikle yöneticilerin konunun önemini anlamış olmaları, gerekli maddi desteğe imkan vermeleri gerekmektedir. Tasarruf yapmak için teknoloji yatırımlarını kesmeleri, kurumlara telafisi olmayan daha büyük maddi ve manevi zararlar olarak dönmektedir. Bilişim suçlarıyla mücadele için, kurumların

teknik altyapılarının güçlü olması, olası saldırıları önlemede çok önemlidir. Dışarıdan yapılacak saldırıların kurum ağ yapısına geçmeden önlenmesi, bunun için gerekli olan anti-virüs, firewall (ateş duvarı) ve diğer koruma programlarının bulunması ve güncel tutulması gerekmektedir. Özellikle veri güvenliği ve şifreleme konularında, bu konularda uzmanlaşmış birimlerden destek alarak, gerekli üst düzey önlemler alınmalıdır.

Bilişim suçlarında, faillerin tespiti için trafik verilerinin tutulmuş olması hayati önem taşımaktadır. Daha önce bahsedilen 5651 sayılı Kanunla, erişim sağlayıcılara trafik bilgilerini tutma zorunluluğu getirilmiştir. Bu veriler sayesinde failler sayısal ortamda delil bırakacak ve tespitleri daha kolay olacaktır. Bu yüzden uygulamada da bu konuya önem verilmelidir.

Teknik altyapının yanında insan kaynağı da bilişim suçlarının önlenmesinde çok önemlidir. Personel güvenliği başlığında belirtilen esaslara dikkat edilmeli, bilişim sistemlerinde çalışacak personelin seçiminde kesinlikle taviz verilmemelidir. Özellikle kurum içi personelin yapacağı kasıtlı bir saldırı, telafisi olmayan zararlar verebilmektedir. Kurum içi casusluklar son zamanlarda en çok rastlanan suç tiplerindendir. Özellikle birbirine rakip firmalarda, güvenlik önlemlerini geçip ticari sırlara ulaşabilmenin en kolay yollarından biri olarak karşımıza çıkmaktadır.

Eskiden bu tarz bir suçun işlenmesi, defter veya kayıtların fiziki olarak şirket dışına çıkarılması yahut bu defter ve kayıtların kopyasının oluşturulup kopyaların şirket dışına çıkarılmasıyla oluşmaktaydı. Fiziki ortamda işlenebilen bu suç, fiziki önlemlerle de çoğu zaman engellenebiliyordu. Ancak bilgi teknolojilerinin gelişmesi, suçun fiziki olarak işlenmesine gerek duyulmadan basit bir takım programlar tarafından çok kolay bir şekilde işlenmesini sağlamıştır. Ayrıca kurumların bilgi güvenliği ve gizliliği gibi bir politika oluşturmamış olmaları, kurum içerisindeki bilgisayarlarda ve ağ sistemlerinde hem donanım hem de yazılım

olarak bir önlem alınmamış olması, kimin hangi bilgiye ne şartlarda erişebileceğinin saptanmamış olması, gerekli kayıt ve izleme önlemlerine başvurulmamış olması gibi boşluklar da suçun işlenmesi için yeterince olanak sağlamaktadır. Bu yüzden bilgi güvenliği yönetim standartları kurumlara yansıtılmalı, riskler görülerek gerekli önlemlerin en başından alınmaları gerekmektedir.

Bilişim suçlarının bu denli yaygınlaşmasının nedenlerinden birisi de, internet kafelerin artması, alışveriş merkezleri, restoran, otel gibi umuma açık yerlerin hızla artan bir şekilde kablosuz internet imkanı sunmasıdır. Bu gibi yerlerde bilişim suçları artmakla da kalmamış, faillerin takibini oldukça güçleştirmiştir. Bu yüzden bu tip yerlerde, kurumların ve şirketlerin kendilerini de zora sokmaması açısından ağ trafik bilgilerini sıkı takip etmeleri gerekmektedir. Zira kontrolsüz bir şekilde sunulan bu imkanlar bilişim suçlularının rahatça hareket edebilecekleri ve yakalanmayacakları bir zemini oluşturmaktadır. Bu yerlerde bilgisayar kullanma veya internete bağlanma durumları için kurumsal bazda güvenlik standartları oluşturulmalı, her türlü işlemin bu yerlerde yapılmasına izin verilmemelidir.

Bilişim suçlarıyla mücadelede bir diğer önemli konu da ulusal anlamda olaylara müdahalenin nasıl yapılacağıdır. Bu konuda yapılan ve yapılacak yasal düzenlemelerle paralel bir ulusal politika oluşturulmalı, bilişim suçları oluşmadan önce ya da oluştuktan sonra kişilerin veya kurumların nasıl hareket etmesi gerektiği saptanmalıdır. Birçok kişi veya kurum karşılaştığı bir bilişim suçu karşısında ne yapması gerektiğini bilememektedir. Bu da olası delillerin yok olmasına ve faillerin bulunamamasına neden olmaktadır. Bu yüzden, devlet olarak bir saldırı acil eylem planı geliştirilmeli, strateji oluşturulmalıdır.

Bilişim suçlarıyla savaş, yalnız polisiye tedbirler alınması veya devletin bu konu ile mücadele etmesi ile çözülebilecek bir olgu değildir. Toplum olarak da bu konu ele alınmalı, gerekli bilinç oluşturulmalıdır. Bu bağlamda bilgisayar okur

yazarlığı artırılmalı, temel bilgisayar kullanıcıları bilinçlendirilmeli, alınabilecek önlemler anlatılmalıdır. Oluşturulan devlet stratejisi toplumu da kapsamalı ve bu bilinçle beraber derhal uygulamaya alınmalıdır.

KAYNAKÇA

Akbulut, Berrin Bozdoğan (1999), *Türk Ceza Hukukunda Bilişim Suçları*, Selçuk Üniversitesi, Yayımlanmamış Doktora Tezi, Konya.

Akbulut, Berrin Bozdoğan (2000), *Bilişim Suçları*, Selçuk Üniversitesi Hukuk Fakültesi Dergisi Milenyum Armağanı, C. 8, S. 1-2.

Akın, Mustafa, Parlar, Ali, Hatipoğlu, Muzaffer (2010), Bankacılık Ceza Hukuku, Ankara.

Alaca, Bahaddin (2008), *Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi*, Ankara Üniversitesi, Yüksek Lisans Tezi, Ankara.

Armstrong, Helen L., Forde, Patrick J. (2003), "Internet anonymity practices in computer crime", *Information Managament and Computer Security*, C. 11, S. 5.

Avrupa Konseyi Siber Suçlar Sözleşmesi (2001), Budapeşte.

Aydın, Emin D. (1992), *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınevi, Ankara.

Aydın, Öykü Didem, Bilişim 93, Bildiriler.

Bayraktar, Köksal (2000), *Banka Kredi Kartları ile Ortaya Çıkan Ceza Hukuku Sorunları*, Beta Yayınevi, İstanbul.

Beceni, Yasin, Siber Suçlar, http://www.hukukcu.com/bilimsel/kitaplar/yasinbeceni/bolum4.htm (14.05.2010).

Bequai, August (1998), "A Guide to Cyber Crime Investigations", *Computers and Security Report*, C. 17, S. 7.

Beyhan, Cem (2002), "Türkiye'de Bilişim Suçları ve Mücadele Yöntemleri", *Polis Bilimleri Dergisi*, C. 4, S. 3-4.

Bilgisayar Ansiklopedisi (1991), Milliyet Yayınları, İstanbul.

Bilişim Suçları Çalışma Grubu Raporu, EGM.

Boğaç, Erkan, Songür, Murat (1999), *Açıklamalı Bilgisayar ve İnternet Terimleri Sözlüğü*, Hacettepe-Taş Yayınları, Ankara.

Bulduk, Seyfi (2003), "Bilişim Suçları İle Mücadelede Yapılanma Modeli ve Personel Eğitimi", *J.Okullar K.lığı Uluslararası Terörizm ve Bilişim Suçları Konferansı, Takdim Metni*'nden aktaran, Tulum, İsmail (2006), *Bilişim Suçları İle Mücadele*, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta.

Burden, Kit, Palmer, Creole, Lyde, Barlow (2003), "Internet Crime - Cyber Crime - A New Breed of Criminal", *Computer Law and Security Report*, C. 19, S. 3.

Ceyhun, Yurdakul, Çağlayan, M. Ufuk (1997), Bilgi Teknolojileri Türkiye için Nasıl Bir Gelecek Hazırlamakta, Ankara.

Csonka, Peter (2000), "Internet Crime", *Computer Law and Security Report*, C. 16, S. 5.

Değirmenci, Olgun (2002), *Bilişim Suçları*, Marmara Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Değirmenci, Olgun (2005), "Bilişim Suçları Alanında Yapılan Çalışmalar ve Bu Suçların Mukayeseli Hukukta Düzenlenişi", *Çağın Polisi Dergisi*, S. 37.

Dijle, Hikmet (2006), *Türkiye'de Eğitimli İnsanların Bilişim Suçlarına Yaklaşımı*, Gazi Üniversitesi, Yüksek Lisans Tezi, Ankara.

Dönmezer, Sulhi (1989), *Yeni Türk Ceza Kanunu Öntasarısı - Ceza Hukuku El Kitabı*, İstanbul.

Durmaz, Şükrü (2006), *Bilişim Suçlarının Sosyolojik Analizi*, Gazi Üniversitesi, Yayımlanmamış Yüksek Lisans Tezi, Ankara.

Dülger, Murat Volkan (2004), *Bilişim Suçları*, Seçkin Yayınevi, Ankara.

E-Dönüşüm Türkiye İcra Kurulu 21. Toplantısı, Bilişim Suçlarında Yaşanan Gelişmeler, http://www.bilgitoplumu.gov.tr/Documents/1/Icra_Kurulu/071025_IK21.BilisimSuclarindaYasananGelismeler.pdf (12.06.2010).

EGM (2006-2008-2009), Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Raporu, EGM, Ankara.

Foltz, C. Bryan (2004), "Cyberterrorism, Computer Crime and Reality", *Information Managament and Computer Security*, C. 12, S. 2.

Garland, David, "Strategies of Crime Control in Contemporary Society", *British Journal of Criminology*, C. 36, S. 4.

Granville, Johanna (2003), "The Dangers of Cyber Crime and a Call for Proactive Solutions", *Australian Journal of Politics and History*, C. 49, S. 1.

http://tr.wikipedia.org (07.06.2010).

http://www.antiphishing.org (12.06.2010).

http://www.bilgiguvenligi.gov.tr (22.06.2010).

http://www.dha.com.tr (11.10.2010).

http://www.ekizer.net (13.05.2010).

http://www.hukukcular.org.tr/makaleler/65-blm-suclari.html (14.04.2010).

http://www.internetworldstats.com (18.10.2010).

http://www.iso.org (18.06.2010).

http://www.isokalitebelgesi.com (12.06.2010).

http://www.meb.gov.tr/belirligunler/internet_haftasi_2005/internet_tarih.htm (27.06.2010).

http://www.spam.org.tr/nedir.html (19.04.2010).

http://www.tib.gov.tr/dokuman/faaliyet_raporu.pdf (19.10.2010)

http://www.tk.gov.tr/eimza/doc/diger/eimza_bgs_taslak_raporuv1.2.pdf (20.04.2010).

http://www.yargitay.gov.tr/ (12.05.2010).

Interpol Computer Crime Manual.

İlkiz, Fikret (2010), "Bilişim Hukuku Kurultayı", http://bianet.org/bianet/bianet/122712-bilisim-hukuku-kurultayi (11.07.2010).

Karagülmez, Ali (2005), *Bilişim Suçları ve Soruşturma - Kovuşturma Evreleri*, Seçkin Yayıncılık, Ankara.

Karamatullah, Gari (2000), *Terörizm ve İnsan Hakları*, 1. Milletlerarası Doğu ve Güneydoğu Anadolu'da Güvenlik ve Huzur Sempozyumu, Elazığ.

Kardaş, Ümit (2003), "Bilişim Dünyası ve Hukuk", *Karizma Dergisi*, S. 13.

Katyal, Neal Kumar, *Criminal Law in Cyberspace*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030 (18.05.2010)

Köksal, Ahmet Turan, Oktay, Dilek, Eser, Serap (1999), *İnternet*, Pusula Yayıncılık, İstanbul.

Kurt, Levent (2005), *Açıklamalı - İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yayınları, Ankara.

Mungo, Paul, Clough, Bryan, "Approaching Zero Data Crime and the Computer Underworld", Çeviri: Kurma, Emel (1999), "Sıfıra Doğru", *Veri Suçları ve Bilgisayar Yeraltı Dünyası*, İstanbul.

Nykodym, Nick, Taylor, Robert, Vilela, Julia (2004), "Control of Cyber Crime: The World's Current Legislative Efforts Against Cyber Crime", *Computer Law and Security Report*, C. 20, S. 5.

Özdilek, Ali Osman (2002), *İnternet ve Hukuk, Papatya Yayıncılık*, İstanbul.

Özel, Cevat (2001), "Bilişim Suçları ile İletişim Faaliyetleri Yönünden Türk Ceza Kanunu Tasarısı", *İstanbul Barosu Dergisi*, S. 7-8-9.

Özel, Cevat (2002), "Bilişim - İnternet Suçları", http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm (13.05.2010).

Özel, Cevat, Ahi, M. Gökhan (2005), "Bilişim Suçlarında Usul Ve Sorumluluk Sistemi Üzerine Öneriler", http://hukukcu.com/modules/smartsection/item.php?itemid=74 (18.06.2010).

Parker, Donn B. (1989), *Computer Crime: Criminal Justice Resource Manual*'den aktaran, Osman Nihat Şen, *Polisin Bilişim Suçlarıyla Mücadelede Yapması Gerekenler*, 1. Polis Bilişim Sempozyumu, Ankara, 2003.

Pazarcı, Melih (1997), "Bilirkişi Raporu, Şifreli Yayınların Hukuki Konumunu Aydınlatan ki Önemli Görüş", *İstanbul Barosu Dergisi*, C.71, S.1.

Robinson, James K. (2000), "Internet as the Scene of Crime", *International Computer Crime Conference*, Norveç, http://www.justice.gov/criminal/cybercrime/roboslo.htm (21.05.2010).

Sırabaşı, Volkan (2003), *İnternet ve Radyo Televizyon Aracılığıyla Kişilik Haklarına Tecavüz (İnternet Rejimi)*, Ankara.

Sırımcıyan, Ali (2000), "Domain Hırsızları", *Chip Dergisi*, Mart 2000, S. 3.

Smith, Alan D., Rupp, William T. (2002), "Issues in Cybersecurity: Understanding the Potential Risks Associated With Hackers/Crackers", *Information Managament and Computer Security*, C. 10, S. 4.

The Niagara Regional Police Service, http://www.nrps.com/community/comprev.asp (02.05.2010).

Tulum, İsmail (2006), *Bilişim Suçları ile Mücadele*, Süleyman Demirel Üniversitesi, Yüksek Lisans Tezi, Isparta.

Türk Dil Kurumu Bilim ve Sanat Terimleri Ana Sözlüğü, http://tdkterim.gov.tr/ (13.04.2010).

Yağan, Haldun (2007), "Bilişim Suçları", *Gümrük Dünyası Dergisi*, S. 52.

Yaycı, Esra (2007), *Bilişim Suçları*, Gazi Üniversitesi, Yüksek Lisans Tezi, Ankara.

Yazıcıoğlu, R. Yılmaz (1997), *Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile*, İstanbul.

Yenidünya, A.Caner, Değirmenci, Olgun (2003), *Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları*, Legal Yayınevi, İstanbul.

Yüzer, Muharrem, *Bilişim Suçlarının Yapısı Ve Özelliklerine Bir Bakış'tan* aktaran Dilek, Halil İ. (2007), *Bilişim Suçları ve Türk Hukuk Sistemindeki Yeri*, Dicle Üniversitesi, Yüksek Lisans Tezi, Diyarbakır.

EK-1

YARGITAY KARARLARI

"Sanığın, katılanın yetkilisi olduğu Zorel Tekstil İmalat Pazarlama Sanayi ve Ticaret Limited şirketinin Türkiye Ekonomi Bankası Denizli şubesinde bulunan hesabına internet üzerinden izinsiz giriş yaptığı, ancak şirkete ait hesaba girdikten sonra bu hesapta oynama yaparak başka bir hesaba havale yapmadığının iddia ve kabul olunması karşısında sanığın eyleminin 5237 sayılı TCK'nın 243/1.maddesinde düzenlenen suçu oluşturduğu gözetilmeden yazılı şekilde (5237 sayılı TCK'nın 244/4, 35/2. maddeleri gereğince) hüküm tesisi, bozmayı gerektirmiştir."

Y. 11. C. D. 2009/3058

"E..... İnşaat Sanayi ve Ticaret Limited Şirketi'nin bilgisayarlarına virüs bulaştırması sonucu doğacak zararın, şirketin gönderdiği e-postalar aracılığıyla başka adreslere virüs göndererek başka bilgisayarlara zarar vermesi ve kendi bilgisayarlarının sistem dosyalarını silerek çalışamaz duruma getirip iş ve zaman kaybına neden olması olduğunu, virüslü veya virüssüz bir e-postayı gönderen bilgisayarı bulmanın mümkün olduğunu, e-postayı gönderen bilgisayarın IP numarası, e-postayı gönderen sunucu bilgisayarın IP numarası, gönderici ve alıcı adreslerinin, e-posta almayı ve göndermeyi sağlayan e-postanın sunucu bilgisayarlarının tuttuğu günlük kayıtlarında saklandığını, servis sağlayıcı firmaların bir süre sonra bu kayıtların olduğu dosyaları silebildiğini, bu bilgilerin servis sağlayıcı firmalardan resmi yollarla istenilerek öğrenilebileceğini, bu davada 03.01.2002 tarihinde saat 16.19'da E..... İnşaat Sanayi ve Ticaret Limited Şirketi'nin aedltd@mynet.com e-posta adresine virüslü e-posta gönderilerek bilgisayar

sistemlerine zarar verilmesinin söz konusu olduğunu, M.... şirketinin günlük kayıtları mevcutsa gönderici e-posta adresini, e-postanın yazılıp yola çıkarıldığı ilk bilgisayarın IP numarasını ve IP numarasının sahibi servis sağlayıcı firmanın isminin bulanabileceğini, servis sağlayıcı firmadan da, günlük kayıtları mevcutsa verilen tarih ve saat için bu IP numarasının kullanıcısının öğrenilebileceğini, şayet e-postanın yola çıkarıldığı sistemin IP numarası M.... şirketinden öğrenilemezse ve e-postayı gönderen adres mcde70@yahoo.de olarak bulunursa Y.... şirketinden, başka bir adres çıkarsa o e-posta adresini sağlayan servis sağlayıcıdan, bu adresi kullanan kişinin sistemde kayıtlı kimlik bilgileriyle, mevcutsa günlük kayıtlarından bu adres aracılığıyla e-posta gönderip almak için sisteme erişildiğindeki tarih ve saatler ile erişilen IP numaralarının öğrenilebileceğini ve bu kullanıcı telefonla bağlanan bir ev kullanıcısı ise bağlanılan telefon numarasından kimliğinin kolaylıkla bulunabileceğini, sonuç olarak, sanığın E..... İnşaat Sanayi ve Ticaret Limited Şirketi'nin bilgisayarlarına virüs gönderdiğinin kesin olmadığını, ancak virüs bulaştıran e-postanın gönderildiği kaynağın araştırılması gerektiğini, e-posta nedeniyle bulaşan virüsün bilgisayar sistemi bozarak iş ve zaman kaybına neden olduğunu, virüslü e-postayı gönderen bilgisayarın tespit edilmesinin, e-postanın yola çıkarıldığı bilgisayarın IP numarasının bulunmasıyla mümkün olabileceğini açıklaması karşısında, gerçeğin kuşkuya yer vermeyecek şekilde belirlenmesi açısından; öncelikle e-posta yolu ile virüs göndererek sistemine zarar verilmiş bir bilgisayarda incelemenin, olayın hemen akabinde yapılması ya da inceleme yapılacak bilgisayarın veya bilgisayara ait veri içeren ünitelerin, olaydan sonra inceleme yapılana kadar hiç kullanılmaması gerektiği, incelenecek bilgisayarın diskine bazı bilgilerin yazılması, değişmesi veya silinebilmesini önlemek ve söz konusu diskin bütünlüğünü sağlamak için bilgisayarda virüslü dosya üzerinde inceleme yaparken ilk işlem olarak, söz konusu dosyanın birebir (sector-by-sector) yedeğinin alınması (yani incelemenin orijinal dosya üzerinde yapılmaması), daha sonra ikinci olarak alınan birebir yedeğin değiştirilip değiştirilmediğini tespite yarayacak zaman ve bütünlük kontrolü imkanı sağlayan değerin (hash) belirlenmesi, bir e-postanın kimden geldiğinin tespiti için de, ilk olarak e-postayı gönderen IP adresinin bulunması (örneğin; şikayetçiye gelen e-postanın seçeneklerinden e-posta üst bilgisinin belirlenmesi ve bu üst bilginin uzman kişiler tarafından incelenmesi

veya şikayetçiye gelen e-postanın göndericisinin ya da alıcısının e-posta sunucusunun sahibi şirkete belirtilen tarih ve saatte bahse konu e-postanın hangi IP adresinden gönderildiğinin sorulması ile), daha sonra da bulunan IP adresinin belirtilen tarih ve saatte hangi abone tarafından kullanıldığının ve o abonenin açık adres ve kimlik bilgilerinin talep edilmesi, bulunan IP adresini kullanan abonenin sanıkla bağlantısının araştırılması gerektiği hususları da göz önüne alınarak, bilgisayardaki virüslü dosya veya dosyaların orijinallerinin korunup korunmadığı, birebir yedeklerinin alınıp alınmadığı hususlarının araştırılması, e-posta veya e-postaları gönderenin IP adresinin bilirkişi raporları doğrultusunda tespiti, bulunacak adresin sanıkla ilgisinin belirlenmesi, olay tarihinde katılan dışındaki diğer şirket ortakları ile Yurdanur Çavdar'ın tanık sıfatı ile dinlenmeleri ve toplanan deliller bir bütün halinde değerlendirildikten sonra sonucuna göre sanığın hukuki durumunun takdir ve tayini gerektiği gözetilmeden eksik inceleme ile yazılı şekilde beraatine hükmolunması, bozmayı gerektirmiştir."

Y. 11. C. D. 2007/2551

"1- Dolandırıcılık suçunda unsur olan kandırabilecek nitelikteki hilenin, gerçek kişiye yönelmesi ve bu kişinin hataya düşürülüp onun veya bir başkasının zararına, fiili işleyene veya başkasına haksız bir menfaat sağlanması gerekir, Somut olayda; sanığın, katılan Mücahit S'in kimlik bilgilerine göre düzenlenip kendi fotoğrafı yapıştırılmış ele geçirilemeyen sahte nüfus cüzdanını kullanarak katılan A A.Ş.nin Yenigün Şubesi'nde hesap açtırarak diğer katılan Murat Ç'ın bankada bulunan para hesabındaki var olan verileri (bilgileri) sahte kimlikle açtırdığı hesaba internet yoluyla havale edip hesap cüzdanı ibraz ederek banka şubesinden çektiğinin iddia ve kabul olunması karşısında; eyleminin, paranın sanığın açtırdığı hesaba intikaline kadar katılan Murat Ç'a yöneltilmiş hile bulunmaması ve tamamen bilişim sistemi içinde gerçekleştirilmesi nedeniyle 5237 sayılı TCK'nın 244/4 maddesine uyan suçu oluşturduğu gözetilmeden, vasıflandırılmada yanılgıya düşülerek unsurları oluşmayan banka aracı kılınmak suretiyle nitelikli dolandırıcılık suçundan mahkûmiyet hükmü kurulması,

2- Sanığın hesap açtırmak için kullandığı sahte nüfus cüzdanının elde edilememesi ve sahteciliğin iğfal kabiliyetini haiz olup olmadığının saptanamamış bulunması, aynı belgenin başka işlemler sırasında da kullanılıp aldatıcılık yeteneğinin tespit edilememesi, banka görevlilerinin ihmali davranışları sebebiyle hesabın açılmış olma ihtimali de nazara alındığında sırf sahte nüfus cüzdanı ile işlem yapılmasının iğfal kabiliyetinin varlığını kabul için yeterli olmadığı gözetilmeden yüklenen sahtecilik suçundan beraati yerine isabetsiz gerekçe ile yazılı şekilde mahkumiyet hükmü kurulması, bozmayı gerektirmiştir."

Y. 11. C. D. 2008/117

"Dolandırıcılık suçları ile ilgili hükmün temyizine gelince,

A) Dolandırıcılık suçundan unsur olan kandırabilecek nitelikteki hilenin, gerçek kişiye yönelmesi ve bu kişinin hataya düşürülüp onun veya bir başkasının zararına, fiili işleyene veya başkasına haksız bir menfaat sağlanması gerekir,

Somut olayda; sanığın, mağdurların bankalarda bulunan para hesaplarındaki var olan verileri (bilgileri) sahte kimliklerle açtırdığı hesaplara internet yoluyla göndererek, yine sahte kimliklerle bu paraları çekmek istemesinden ibaret eylemlerinin; paranın sanığın açtırdığı hesaplara intikaline kadar gerçek kişilere yöneltilmiş hile bulunmayıp eylemlerin tamamen bilişim sistemi içinde gerçekleştirildiğinden, her bir mağdura karşı işlenmiş ayrı ayrı 5237 sayılı TCK'nın 244/4 maddesine uyan suçu oluşturduğu ve paranın açtırdığı hesaplara transferiyle suçun tamamlanacağı gözetilmeden, suçun vasıflandırılmasında yanılgıya düşülerek nitelikli dolandırıcılığa teşebbüs suçundan mahkûmiyet hükmü kurulması,

B) Uygulamaya göre de;

5237 sayılı TCK uyarınca verilen adli para cezasının, belirlenecek tam gün sayısı ile bir gün karşılığı olarak takdir edilen miktarın çarpılmak suretiyle belirlenmesi yerine, sağlanan haksız menfaatin iki misli olarak hükmolunması, bozmayı gerektirmiştir."

Y. 11. C. D. 2007/6012

"Sanıkların fikir ve eylem birliği içinde hareket ederek, katılan Sadet Erbil'in Yapı Kredi Bankası Manisa Şubesindeki banka hesabına ait "interaktif bankacılık şifresini" kırarak internet aracılığı ile hesapta bulunan parasını sanıklardan Yıldırım Aydemir'in Akbank Bakırköy Şubesindeki şirket hesabına havale ederek bu hesaptan parayı çekmelerinden ibaret eylemlerinin 5237 sayılı TCK'nın 244/4. maddesinde öngörülen bilişim suçlarını oluşturduğu gözetilmeden suçların nitelendirilmesinde yanılgıya düşülerek hırsızlık suçlarından yazılı şekilde hüküm kurulması, bozmayı gerektirmiştir."

Y. 11. C. D. 2009/4877

"Dolandırıcılık suçunda unsur olan hileli davranışların gerçek kişiye yönelmesi ve bunun sonucunda onun veya başkasının malvarlığı aleyhine sanığın veya başkasının yararına haksız bir menfaat sağlanması gerekeceği, somut olayda ise; sanığın katılanın Şekerbank Uludağ Şubesinde mevcut şirket hesabına internet bankacılığı yoluyla girip hesaptaki paradan 7300,00 YTL'yi Yapı Kredi Bankası Adana Baraj Yolu Şubesinde Barış Güven sahte kimliğiyle açtırmış olduğu hesaba havale edip çekmeye çalıştığının iddia ve dosya içeriğine uygun gerekçelerle kabul edilmesi karşısında; Gerçek kişiye yönelen hile oluşturacak nitelikte bir hareketin bulunmaması nedeniyle dolandırıcılık suçunun unsurlarının bulunmadığı, fiilin 5237 sayılı TCK'nın 244/4 maddesinde öngörülen bilişim suçunu oluşturduğu gözetilmeden, suç vasfında hataya düşülerek yazılı şekilde bilişim sistemlerinin aracı olarak kullanılması suretiyle dolandırıcılık suçundan mahkumiyetine karar verilmesi, bozmayı gerektirmiştir."

Y. 11. C. D. 2009/80

"Oluşa uygun olarak sübutu kabul edilen, katılan Nazan Eroğlu'na ait Fortisbank Sefaköy Şubesindeki hesaba internet üzerinden girilerek, mevduatında bulunan 12.100 YTL parayı, fikir ve eylem birliği içerisinde hareket eden sanıklar tarafından, sanık Pınar'ın Akbank Adana Küçükesat Şubesindeki hesabına havale edilerek aynı gün paranın 10.900 YTL'sini banka şubesinden, 1000 YTL'sini banka

kartı ile çekilmesinden ibaret eylemlerinin bir bütün halinde 5237 sayılı TCK'nın 244/4. maddesinde öngörülen bilgileri otomatik işleme tabi tutmuş bir sistemi kullanarak kendisi veya başkası lehine hukuka aykırı yarar sağlamak suçunu oluşturduğu gözetilmeden nitelikli hırsızlık suçunu oluşturduğunun kabulü ile yazılı şekilde hüküm kurulması, bozmayı gerektirmiştir."

Y. 11. C. D. 2009/3058

"Sahte kredi kartı üretip kullanmak suçlarından şüpheli olarak takibe alınan sanığın olay günü benzin istasyonunda alış-veriş yaptıktan sonra güvenlik güçlerince yakalandığı, üzerinde ve aracında yapılan aramada Sezgin Taşkın adına düzenlenmiş sanığın fotoğrafı bulunan sürücü belgesi ve gerçekte Independent Bank City, Michigan United States of America bankasına ait olup üzerinde Vakıfbank logosu bulunan sonu 7486 ile biten manyetik şerit bilgileri kopyalanmış sahte kredi kartının ele geçirdiği cihetle; sanığın fiillerinin yaptırımının sahte sürücü belgesi düzenleyip kullanmak suçu yönünden 5237 sayılı TCK'nın 204/1, sahte kredi kartı üretip kullanmak suçları yönünden ise 245/2-3. madde ve fıkralarında düzenlenip anılan maddelerde suçlar için öngörülen cezaların alt sınırları itibariyle açıkça aleyhe hükümler içerdiğinden tebliğnamedeki somut uygulama yapılmadığı gerekçesiyle bozma isteyen düşünceye iştirak edilmemiş, sanıkta ele geçen sahte kredi kartının 19.06.2002 22.12.2002 tarihleri arasında birden çok alış verişte kullanılarak 10.010 YTL'lik harcama yapıldığının anlaşılması karşısında teselsül hükümlerinin uygulanmaması ve sağlanan menfaat miktarının pek fahiş olduğunun nazara alınmaması, dolandırıcılık suçunun tamamlandığı halde teşebbüs aşamasında kaldığının kabulü, uygulamaya göre de 765 sayılı TCK'nın 19. maddesi uyarınca adli para cezasının suç tarihi itibariyle 216 TL'den az olamayacağının gözetilmemesi karşı temyiz olmadığından bozma nedeni yapılmamıştır."

Y. 11. C. D. 2010/7002

"Sanıkların fikir ve eylem birliği içerisinde başkaları adına tanzim edilmiş ancak sanık Alpaslan Yılmaz'ın fotoğrafı yapıştırılmış aslı elde edilemeyen nüfus

cüzdanlarını ibraz ederek, bu kimlik bilgilerine istinaden imzaladıkları kredi kartı sözleşmeleri ile kredi kartı talebinde bulunmaktan ibaret eylemlerinin, başvuruların aynı bankaya yapılmış olması nedeniyle zincirleme şekilde işlenen 5237 sayılı TCK'nın 245/2. madde ve fıkrasındaki banka veya kredi kartının kötüye kullanılmasına teşebbüs suçunu oluşturduğu gözetilmeden, eylemlerinin özel belgede sahtecilik suçlarını oluşturduğundan bahisle yazılı şekilde karar verilmesi, bozmayı gerektirmiştir."

Y. 11. C. D. 2010/4847

"1- Sahte kredi kartı ile yapılan harcama miktarları ve tarihleri saptanarak buna göre suç tarihi ve suça konu değerin belirlenmesi gerektiği gözetilmeden gerekçeli karar başlığında suç tarihinin kredi kartı başvuru tarihi olan 01.11.2002 olarak gösterilmesi,

2- Sanığın, şikayetçi Türk Dış Ticaret Bankasından karısı Saliha Demiralp'in rızası dışında onun adına sahte olarak düzenlettirdiği kredi kartının kendisine teslimini sağlayıp bu kartla, bankanın maddi varlıklarından olan POS cihazlarını kullanarak alış-veriş yapmak suretiyle adı geçen şikayetçi bankanın zararına kendisine yarar sağladığının iddia ve kabul olunması karşısında; 5252 Sayılı Kanunun 9/3. maddesi uyarınca; suç tarihinde yürürlükte olan 765 Sayılı TCK'nın 504/3, 522, 80 ile 5237 Sayılı TCK'nın 245/2-3, 43/1. maddelerinin ayrı ayrı uygulanmasıyla bulunan sonuçların kararın gerekçe bölümünde denetime olanak verecek şekilde somut olarak gösterilip birbirleriyle karşılaştırılması suretiyle lehe Yasanın belirlenmesi yerine, uygulamalı karşılaştırma yapılmadan uygulama yeri bulunmayan 5237 sayılı TCK'nın 158/1-j maddesinin lehe olduğundan bahisle yazılı şekilde hüküm kurulması, bozmayı gerektirmiştir."

Y. 11. C. D. 2010/3229 [122]

122 http://www.yargitay.gov.tr/

ÖZET

Bilişim teknolojilerindeki gelişmeler, toplumda hemen her konuda klasik anlayışı değiştirmiş, hayatımıza yeni bir yaşam tarzı getirmiştir. Bilginin önemli bir güç haline gelmesiyle, bilişim teknolojileri de fevkalade önemli bir araç konumuna girmiştir. Bu hızlı gelişim, sosyal ve teknolojik yönden dengesiz değişimler, yeni tehlike ve tehditleri de ortaya çıkarmıştır.

Toplum bilgi toplumuna dönerken, bu gelişimin bir ürünü olarak bilişim suçları ortaya çıkmıştır. Özellikle İnternetin yaygınlaşmasıyla, suçlular arasında, çok daha kolay işlenen, tespit edilmesi ise bir o kadar zor olan bu suç tipleri hızla yayılmış, klasik suç tiplerinin yerini almıştır.

Çalışmamızın genel amacı, bilişim suçlarıyla yapılan mücadelede gelinen durum ve bundan sonrası için çözüm önerileri oluşturmaktır. Bilişim suçlarıyla mücadele ederken, teknolojinin dinamik yapısı göz ardı edilmeden esnek çözümler üretilmeli, konunun hukuki boyutuyla beraber kişilere ve kurumlara özel güvenlik tedbirleri geliştirilmelidir.

Anahtar Kelimeler: Bilişim Suçları, Siber Suçlar, Bilgisayar Suçları

ABSTRACT

Developments in information technologies has changed the classical sense in sociaty about almost every respect, and brought a new lifestyle to our lives. Information Technologies has been a very important issue, as information becoming a major force. This rapid growth, unstable social and technological changes, also revealed new threats.

While society turns to be an information society, cyber crimes occurs as a product of this development. Owing to the spread of the Internet, these crime types, being much more easily processed and difficult to determine, are quickly widespread and takes the role of classical crime types among the criminals.

The aim of our study is to create solution suggestions through the struggle against the cyber crimes. While this struggle, flexible solutions must be produced without ignoring the dynamic nature of technology and security measures must be developed special to people and institutions while thinking the legal side of issue.

Key Words: Information Technologies Crimes, Cyber Crimes, Computer Crimes

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı	: Uğur BOĞA
Doğum Yeri ve Tarihi	: Amasya 01.12.1977

Eğitim Durumu

Lisans	: Orta Doğu Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü
Yabancı Dil	: İngilizce

İş Deneyimi

Çalıştığı Kurumlar	: Radyo ve Televizyon Üst Kurulu
	: Bayındırlık ve İskan Bakanlığı
	: Türk Telekomünikasyon A.Ş.
	: Havelsan-Ehsim A.Ş.