T.C.
POLİS AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ
ADLİ BİLİMLER ANABİLİM DALI

BİLİŞİM SUÇLARI, BİLİŞİM YOLUYLA İŞLENEN SUÇLAR VE ADLİ BİLİŞİM AYRIMI

YÜKSEK LİSANS TEZİ

Hüseyin AKARSLAN

Danışman
Doç. Dr. Mehmet ÖZCAN

Ankara – 2011

T.C.

POLİS AKADEMİSİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

ADLİ BİLİMLER ANABİLİM DALI

BİLİŞİM SUÇLARI, BİLİŞİM YOLUYLA İŞLENEN SUÇLAR VE ADLİ BİLİŞİM AYRIMI

YÜKSEK LİSANS TEZİ

Hüseyin AKARSLAN

Bu tez 11../ 03./ 2011 tarihinde aşağıdaki jüri tarafından Oybirliği/~~Oyçokluğu~~ ile kabul edilmiştir.

Jüri Başkanı: Doç. Dr. Mehmet ÖZCAN .....

Üye: Prof. Dr. Şeref SAĞIROĞLU .....

Üye: Doç. Dr. Mehmet ARICAN .....

T.C.
POLİS AKADEMİSİ BAŞKANLIĞI
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yüksek lisans tezi olarak sunduğum bu çalışmayı bilimsel ahlak ve geleneklere aykırı düşecek bir yol ve yardıma başvurmaksızın yazdığımı, yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, bunlardan her seferinde yollama yaparak yararlandığımı belirtir; bunu şerefimle beyan ederim.

Enstitü veya başka herhangi bir mercii tarafından belli bir zamana bağlı kalmaksızın, tezimle ilgili bu beyana aykırı bir durumun tespit edilmesi durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara katlanacağımı bildiririm.

01.06.2011

Hüseyin AKARSLAN

ÖNSÖZ

Meslek hayatım boyunca üzerinde çalıştığım başlıca konular olan "bilişim teknolojileri ve suç" kavramları ne yazık ki gün geçtikçe daha çok iç içe girmeye başlamaktadır. Ve daha yeni gelişen bir konu tam olarak anlaşılmadan ve çözülemeden bir yenisi gündeme gelmektedir.

Uzun yıllardır bu alandaki uygulamaların içindeki birisi olarak, bilişim teknolojileri ve suç dünyası arasındaki teknik terminolojinin tam olarak oturtulamadığı ve yanlış kullanımların olduğunu görmekteydik. Bu nedenle böyle bir çalışma yapmanın teknik terminolojiye katkı yapmasının yanı sıra suç ve suçluyla mücadeleye de yarar sağlayacağı düşüncesindeyiz.

Polis Akademisi bitirme tezimde de yine bilişim suçları konusu üzerine birlikte çalıştığım ve danışmanlığımı yapan değerli hocam sayın Doç. Dr. Mehmet ÖZCAN'a hem bilimsel hem de insani katkılarından ötürü sonsuz şükranlarımı sunarım.

Bütün çalışmalarım boyunca beni destekleyen değerli eşime de anlayışı ve sabrından dolayı teşekkür ederim.

ÖZET

Akarslan, Hüseyin, (2011), Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı, Yüksek Lisans Tezi, Danışman: Doç. Dr. Mehmet Özcan, 184 sayfa

Çalışmanın ana konusu "bilişim suçları, bilişim yoluyla işlenen suçlar ve adli bilişim" kavramlarıdır. Bu kavramlar birbirleriyle ilişkili olmasına karşın aynı şeyi ifade etmemektedir. Ancak kavramların içeriği tam olarak bilinmeyen kişilerce (konuyla doğrudan ya da dolaylı ilgili olan) yanlış anlamlarda kullanılmakta ve algılanmaktadır. Bu yanlış kullanım ve algılama da, uygulamaya yanlış ve standart dışı uygulamalar olarak yansımaktadır.

Çalışmamızda öncelikle kavramlar ulusal ve uluslar arası literatüre göre detaylarıyla ve örnekleriyle anlatılmaya çalışılmıştır. Daha sonra birbirleriyle olan benzerlik ve farklılıkları vurgulanmıştır. Burada sadece teorik bir yaklaşım izlenmemiş ayrıca uygulamadan örnekler de verilmiştir.

Sonuç olarak çalışmamızda, kavramların tam olarak ne ifade ettiği anlatılırken, uygulamada nasıl yanlışlıklar yapıldığına da değinilerek, olması gereken durum ortaya konulmaya çalışılmıştır.

Anahtar Kelimeler: Bilişim Bağlantılı Suçlar, Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar, Bilişim Hukuku, Adli Bilişim

ABSTRACT

Akarslan, Hüseyin, (2011), Differences Between Computer Crimes, Computer Related Crimes and Computer Forensics, MA Dissertation, Supervisor: Assoc. Prof. Dr. Mehmet Özcan, 184 pages

The main subject of the study is "computer crimes, crimes through computers and computer forensic" terms. Despite these terms are related each other, they don't have the same meaning. But anyone (who is related with these subject directly or indirectly) that doesn't know these terms exactly, uses and understands these terms incorrectly. The incorrect using and understanding causes wrong and non-standard applications through the subject.

In our study, firstly the terms are explained in national and international literature with details and examples. Then we emphasis the similarities and the differences of these terms with each other. Not only we followed therotical approach but also we gave some examples from practice.

Consequently, it is attempted to describe how the situation should be by indicating what the concepts really refer to while touching the wrong doings in the process of implementation.

Key Words: Computer Related Crimes, Computer Crimes, Crimes Through Computers, IT Law, Computer Forensic

İÇİNDEKİLER

İKİNCİ BÖLÜM

BİLİŞİM TEKNOLOJİLERİNİN SUÇ DÜNYASINDA KULLANILMASI VE ADLİ BİLİŞİM

ÜÇÜNCÜ BÖLÜM
BİLİŞİM SUÇLARI VE BİLİŞİM YOLUYLA İŞLENEN SUÇLARIN KARŞILAŞTIRILMASI

KISALTMALAR

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

AKSSS : Avrupa Konseyi Siber Suç Sözleşmesi

BM : Birleşmiş Milletler

C : Cilt

CBS : Coğrafi Bilgi Sistemi

CMK : Ceza Muhakemesi Kanunu

CSI : Bilgisayar Güvenliği Enstitüsü

DOS : Servis Dışı Bırakma

EGM : Emniyet Genel Müdürlüğü

EİK : Elektronik İmza Kanunu

FBİ : Federal Soruşturma Bürosu

FSEK : Fikir ve Sanat Eserleri Kanunu

OECD : Ekonomik İşbirliği ve Kalkınma Örgütü

S : Sayfa

SS : Sayfa Sayısı

TCK : Türk Ceza Kanunu

TY : Tarih Yok

Y11.CD : Yargıtay 11. Ceza Dairesi

Y6.CD : Yargıtay 6. Ceza Dairesi

YCGK : Yargıtay Ceza Genel Kurulu

TABLOLAR

ŞEKİLLER

GİRİŞ

Teknolojinin gelişmesiyle sosyal hayatın her alanına etki eden bilişim teknolojileri, bu önemli etkilerinden birisini de şüphesiz "suç ve suçlu dünyasına" yapmıştır. Suç ve suçlu dünyasındaki gelişmelerle mücadele etmek için hem suçu önlemede hem de suçu aydınlatmada yeni adımlar atılması gerekmektedir. Ancak bilişim teknolojilerinin çok hızlı gelişimi karşısında hukuk sistemleri yeteri kadar hızlı reaksiyon verememektedir.

Ülkemizde de bilişim teknolojileri suç dünyasının en önemli aktörlerinden birisi haline gelmiştir ve her geçen gün özellikle olumsuz etkileri daha çok konuşulmaya başlanmıştır. Ancak bu durumla mücadele edebilmek için çabalayan güvenlik birimleri, adliyeler, araştırmacılar, mühendisler ve hukukçular konuya daha çok kendi çerçevelerinden bakmışlar ve kendi literatürlerine göre sorunu tanımlamışlardır. Sonuçta literatür birliği sağlanamadığı için kavramlar farklı anlaşılmıştır.

Araştırmanın Konusu ve Problemi

Bilişim teknolojileri ve suç dünyası deyince ilk akla gelen terimler olan "bilişim suçları", "bilişim yoluyla işlenen suçlar" ve "adli bilişim" gibi kavramlar birbirine çok karıştırılmaktadırlar. Evet, bu kavramların birbirleriyle olan bağlantıları ve yakınlıkları çok nettir ancak aralarındaki çizgiyi ve farklılıkları iyi tespit etmek gerekmektedir. Çalışmamızın konusu da bu hedefe yöneliktir. Bu ayrımın sağlıklı bir şekilde yapılmasının faydaları ve yapılmaması durumunda ortaya çıkabilecek zararları da çalışmamızda tartışılmıştır.

Bu kavramlarla ilgili olarak yapılan hataların teorik boyutu olduğu gibi günlük hayata yansıması olan pratik boyutu da vardır. Teorik olarak bu alanda yapılan akademik ve bilimsel çalışmaların üç temel problemi karşımıza çıkmaktadır. Birincisi bu alanda yapılan çalışmaların yeterli sayıda olmadığını görmekteyiz. İkincisi ise az sayıdaki çalışma içerik açısından eksik durumdadır. Üçüncüsü ve en olumsuzu ise bu çalışmalarda ilgili kavramların yanlış kullanılmasıdır.

Örneğin *Dülger*, "Bilişim Suçları"[1] başlıklı kitabında "özel hayata ve hayatın gizli alanına karşı suçlar bölümünde düzenlenen suç tiplerini" de "Yeni Türk Ceza Kanunu'nda düzenlenen bilişim suçları" başlığı altında anlatmıştır. *Ergün*, "Siber Suçların Cezalandırılması ve Türkiye'de Durum"[2] başlıklı kitabında yine "kişisel verilerle ilgili suçların yanı sıra, haberleşmenin engellenmesi suçu, siber hakaret suçu, siber hırsızlık suçu, müstehcenlik suçu" gibi suçları "Türk Hukuku'nda siber suçlar" başlığı altında tartışmıştır. Benzer bir yaklaşımı *Ketizmen*, "Türk Ceza Hukukunda Bilişim Suçları"[3] başlıklı kitabında izlemiş ve kişisel verilerin korunmasına ilişkin suçların bilişim sistemleri aracılığıyla işlenmesinden dolayı bu suçların da "bilişim alanında suçlar" başlığı altında incelenmesi gerektiğini belirmiştir. Bu gibi çalışmalarda "bilişim suçu" ve "bilişim yoluyla işlenen suç" ayrımı net olarak ortaya konulamamıştır.

Diğer taraftan *Karagülmez*, "Bilişim Suçları ve Soruşturma Kovuşturma Evreleri"[4] kitabında, *Kurt*, "Açıklamalı İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunu'ndaki Uygulaması"[5] kitabında ve *Taşdemir*, "Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçları"[6] kitabında "bilişim suçu" ve "bilişim yoluyla işlenen suç" ayrımına uygun yaklaşımlar izlemişlerdir.

Yukarıda örnek olarak verdiğimiz çalışmalarda ortak bir literatür birliğinin sağlanamadığını açıkça görmekteyiz. Bunun temel sebebi olarak çalışmalarda kaynak olarak yabancı yayınlar kullanılırken ülkemizdeki mevcut durumun daha az dikkate alındığını ve suç türleri değerlendirilirken uluslar arası hukuki düzenlemelerin temel alındığını görmekteyiz. Öğretideki bu eksiklikler yargımla süreçlerine de paralel olarak yansımaktadır.

Teknik bir alanda suçla mücadele edilebilmesi için konuya teknik literatüre uygun yaklaşmak gerekmektedir. Bu mücadelenin bir parçasını oluşturan uzmanlar

[1] Dülger, Murat Volkan, (2004), *Bilişim Suçları*, Ankara: Seçkin Yayınevi
[2] Ergün, İsmail, (2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Ankara: Adalet Yayınevi
[3] Ketizmen, Muammer, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, Ankara: Adalet Yayınevi
[4] Karagülmez, Ali, (2009), *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara: Seçkin Yayınları
[5] Kurt, Levent, (2005), *Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Ankara: Seçkin Yayınları
[6] Taşdemir, Kubilay, (2009), *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçu*, Ankara: Ütopyagrafik

kendi uzmanlık alanlarına göre kavramları tanımlamak yerine belli bir yeknesaklık içinde kalmaları önemli bir husustur. Konuyla doğrudan veya dolaylı ilgililerin kendi bakış açılarına paralel olarak ortaya koydukları çalışmalar ve geliştirdikleri uygulamalar belli bir standarda kavuşturulmalıdır.

Araştırmanın Amaç ve Önemi

Çalışmamızın amacı başta "bilişim suçları", "bilişim yoluyla işlenen suçlar" ve "adli bilişim kavramlarını" net olarak tanımlamaktır. Ayrıca bu kavramların birbirleriyle olan ilişkileri ve dünyada ve ülkemizde konuya yönelik yaklaşımların ne olduğu çözümlenmesi gereken soru(n)lardır.

Özellikle "bilişim suçu" kavramı çok geniş manada yorumlanarak, neredeyse içinde bilişim teknolojileri ile doğrudan veya dolaylı bir bağlantısı olan bütün suçlar bilişim suçu olarak algılanmaktadır. Bu yanlış algılamanın konuyla doğrudan ilgili olmayan kişiler tarafından yapılması kabul edilebilir bir durum olabilir ancak konuyla doğrudan ilgili ve bu alanda çalışan kişilerin bu yanlışa düşmesi çok sıkıntılı bir durumdur. Çünkü "bilişim bağlantılı suçlar" yani "bilişim suçları" ve "bilişim yoluyla işlenen suçlar" ceza hukukunun konusudur. Yani insanların gerçekleştirdikleri eylemleri yüzünden "ceza" aldıkları bir konudur. Bu nedenle çok hassas olunması gereken ve kesinlikle en ufak bir hataya düşülmemesi gereken bir alandır.

Kavramlar ve olgular konunun uygulayıcıları tarafından yanlış algılanır ve buna göre yorumlanırsa buradan hukuken sakat uygulamalar ortaya çıkacaktır ve çıkmaktadır. Ülkemizde bir siyasi liderin gizli kamera görüntülerinin ortaya çıkması ve internette yayılması eyleminde bilişim suçları savcısının görevlendirilmesi bu yanlış uygulamaların bir örneğidir.[7] İlk bakışta bu durum bazılarına göre olağan bir uygulama olarak yorumlanabilir. Ancak konunun uzmanı kişilere göre sadece bir olayın içinde bir kamera görüntüsü ve internet ortamı olduğu için gerçekleştirilen eylemi "bilişim suçu" olarak algılamak yanlış bir tutumdur. Nitekim bahse konu

[7] Toprak, İlhan, (2010), "Kaset Orijinal Çıktı", http://yenisafak.com.tr/Gundem/?i=259244, (Erişim Tarihi: 04.01.2011)

somut olayda "özel hayatın gizliliğini ihlal" ve "kişisel verilerin kaydedilmesi" gibi suçlardan bahsedilebilmektedir.[8]

Adli bilişim kavramının İngilizce "computer forensic" teriminden dilimize çevrildiğini ve tam olarak bu terimi karşılamadığını anlatmıştık. Bunun sebebi ise dilimizde "forensic" kelimesinin karşılığının olmamasıdır. Genelde "mahkemeyle ilgili" olarak dilimize çevrilen bu kelime on beşinci yüzyılda Eski Roma'da halka açık bir şekilde kurulan mahkeme alanlarını ifade eden "forum" kelimesinden türetilmiştir ve "mahkemeye uygun", "açığa kavuşturma" gibi anlamlar ifade etmektedir.[9] Bu gibi teknik terimleri başka toplumlardan almak zorunda kaldığımız için dilimize çevirirken ve kullanırken bu tür sıkıntıları yaşamamız kaçınılmaz bir durumdur.

"Adli bilişim" kavramı da yine bu alanda sıklıkla hataya düşülen bir teknik terimdir. En kısa tanımıyla dijital delil elde etme süreci olan "adli bilişim" özellikle "adalet" ve "bilişim" kavramlarının bir araya gelmesiyle oluştuğu sanılarak adaletle ilgili her türlü bilişim teknolojisi uygulamasının "adli bilişim" kapsamında olduğu algısı yaygın görülen bir hatadır. Bu nedenle bu kavram da çalışmamız da net olarak tanımlanması ve açıklanması gereken bir terim olarak ele alınmıştır. Çünkü "adli bilişim" kavramını "bilişim bağlantılı suçlardan" ayrı düşünmek mümkün değildir.

Araştırmanın Yöntemi

"Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı" başlıklı bu çalışmada konuyla ilgili olan kitap, makale, konferans, sempozyum, kongre notları, eğitim dokümanları, ulusal ve uluslar arası haberler, dergiler ve daha önce yapılmış tezler incelenmek suretiyle sosyal bilimlerde nitel araştırma yöntemlerinden literatür taraması ile gerçekleştirilmiş betimsel bir çalışmadır. Çalışmanın üzerinde durduğu konuların doğası gereği (bilişim teknolojilerinin uluslar arası boyutu) özelikle uluslar arası kaynaklardan da yaralanılmıştır.

---

[8] gazetevan.com , (2010), "Deniz Baykal'ın Gizli Kamera Video Görüntüleri İddiasına Savcılık Soruşturması Sürüyor", http://www.gazetevan.com/Deniz_Baykalin_gizli_Kamera_Seks_Video_goruntuleri_iddiasina_savcilik_sorusturmasi_suruyor___yenii-1444h.htm, (Erişim Tarihi: 04.01.2011)

[9] Online Etymology Dictionary, (t.y.), "forensic", http://www.etymonline.com/index.php?search=forensic&searchmode=none, (Erişim Tarihi: 06.01.2011)

Üç bölümden oluşan çalışmamızın birinci bölümünde "bilişim", "bilişim suçu" ve "bilişim yoluyla işlenen suç" kavramları teorik olarak etraflıca anlatılmıştır. Konuyla ilgili temel kaynaklarda ve diğer akademik çalışmalarda farklı anlatımlar olmakla beraber, bu alanda yaptığımız diğer araştırmalar ışığında bize göre olması gereken durum ve yaklaşım sergilenmiştir. Bilişim suçları konusunun ilk ele alındığı yıllarda literatür birliğinden bahsetmek pek mümkün değildir. Çünkü yeni ortaya çıkan ve araştırılmaya başlanan bir alan olduğu için tam olarak oturmuş bir literatür bulunmamaktaydı. Sonraki dönemlerde bu problem kısmen çözüldüyse de halen güncel kaynaklarda bazı farklı yaklaşımlar bulunmaktadır. Biz çalışmamızda konuyla ilgili en güncel bilgiler doğrultusunda ilgili kavramları açıklamaya çalıştık.

İkinci bölümde "bilişim teknolojilerinin suç dünyasında kullanılması" ve "adli bilişim" konuları incelenmiştir. Konu her iki boyutuyla yani hem suç işlemek için hem de suçla mücadele etmek için bilişim teknolojilerinin nasıl kullanıldığı yönüyle ele alınmıştır. Başka çalışmalarda "bilişim suçu işleme metotları, yöntemleri, teknikleri… gibi " adlarla anlatılan konu çalışmamızda "suç işlemek için kullanılan bilişim teknolojileri" başlığı altında anlatılmıştır. Çünkü bu teknikler sadece "bilişim suçu" işlemek için değil "bilişim yoluyla işlenen suçlarda" da kullanılmaktadır.

Suçla mücadelede ve suçu aydınlatmada kullanılan bir bilişim teknolojisi olan "adli bilişim" konusu da bu bölümde anlatılmıştır. Yine şimdiye kadar bu alanda yapılan hiçbir çalışmada değinilmeyen ancak güncel olarak tartışılmaya başlanan bir konu olan "anti adli bilişim" teknikleri de kısaca ele alınmıştır.

Üçüncü bölümde çalışmamızın asıl amacı olan kavramların karşılaştırılması farklı yönleriyle yapılmış ve örneklerle anlatılmaya çalışılmıştır. Sonuç olarak "bilişim suçlarının" ve "bilişim yoluyla işlenen suçların" neden ve nasıl birbirinden ayrılması gerektiği ortaya konulmaya çalışılmıştır. Bu ayrımı ortaya koyarken genel mantığının yanı sıra özellikle hukuki durumlar ve uygulamalar ele alınmıştır. Çünkü "bilişim bağlantılı suçlar" hukuk alanın bir konusu olduğu için en önemli çıkış noktası burasıdır. Ülkemizdeki ve dünyadaki istatistikî bilgiler de uygulamanın bir göstergesi olduğu için konu bu yönüyle de ele alınmıştır.

Yine üçüncü bölümde "adli bilişimin" bu alanda ne kadar önemli bir süreç olduğu anlatılmakla beraber suç türleriyle veya başka kavramlarla birbirine

karıştırılmaması gerektiği vurgulanmıştır. Uygulamadan örnekler verilirken "bilişim suçları", "bilişim yoluyla işlenen suçlar" ve "adli bilişim" sürecinin uygulamada nasıl gerçekleştiği vurgulanmaya çalışılmıştır.

Çalışmanın hedef aldığı ve ortaya koymaya çalıştığı durum aslında üçüncü bölümdeki Şekil 7 (Bilişim Bağlantılı Suçlar ve Adli Bilişim Ayrımı) ve Şekil 8 (Bilişim Bağlantılı Suçlar ve Adli Bilişim Ayrımı Hukuki Çerçevesi) ile net olarak ifade edilmeye çalışılmıştır. Önceki bölümlerde detaylarıyla anlatılan tanımlar ve kavramlar bu iki şekildeki terimlerin tanınması ve ayrımın hangi dayanaklarla yapıldığının anlaşılması içindir.

Sonuç olarak varmaya çalıştığımız nokta sorunun tanımlanması ve çözümün ortaya konulmasıyla birlikte bu alanla doğrudan veya dolaylı ilgililerin çalışmamızda anlatılanlara paralel uygulamalar da bulunmasıdır. "Sonuç ve öneriler" bölümünde bunun nasıl sağlanacağına yönelik çözüm önerileri de anlatılmıştır.

BİRİNCİ BÖLÜM

BİLİŞİM, BİLİŞİM SUÇU VE BİLİŞİM YOLUYLA İŞLENEN SUÇ KAVRAMLARI

1.1. BİLİŞİM, BİLİŞİM SİSTEMİ VE TEMEL KAVRAMLAR

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

Bilişim sistemi, en basit şekliyle, veri veya bilgileri alan, bu verileri işleme tabi tutabilen, sonuçları ya da verileri çıktı şeklinde verebilen elektronik makinelerdir. Bu sistemin bileşenleri, başlangıçtan itibaren sırasıyla; "girdi", "bilgi işlemleri" ve "çıktı " şeklinde üçe ayırabilir. Girdi, bilgisayar dilinde, belli özelliği olan öğelerin oluşturduğu bir kümeyi; bilgi işlemleri, girdi ile başlayan programın amaca uygun olarak işlendiği bölümü; çıktı ise, bir önceki bölümde işlenen bilgilerin okunabilir, anlamlı kümesidir.[11] 5237 sayılı TCK'da bilgisayar sözcüğünü karşılığı olarak daha kapsayıcı bir biçimde "bilişim sistemi" kavramı kullanılmaktayken, 765 sayılı eski TCK'da bilgisayar sözcüğünün karşılığı olarak "bilgileri otomatik işleme tabi tutan sistem" ifadesi kullanılmıştır.[12]

Konuyla ilgili diğer bir kavram olan "bilişim alanı" ise, "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemlerdir" şeklinde tanımlanmaktadır.[13] Bilişim sistemi ve bilişim alanı gibi

---

[10] Tavukçuoğlu, Cengiz , (2004), *Bilişim Terimleri Sözlüğü*, Ankara:Asil Yayınları, s.55.
[11] Karagülmez, (2009), a.g.e., s.123.
[12] Dülger, (2004), a.g.e., s.42.
[13] Erdağ, Ali İhsan, (t.y.), "Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Alanında Suçlar", http://www.ceza-bb.adalet.gov.tr/makale/140.doc, (Erişim Tarihi: 16.08.2010).

kavramların günlük hayattaki uygulaması bilgisayarlar ve internet olarak karşımıza çıkmaktadır. Bunun yanında son yıllarda daha çok kullanılmaya başlayan elektronik posta, alan adı, IP numarası, internet servis sağlayıcı, internet erişim sağlayıcı, yer sağlayıcı, toplu kullanım sağlayıcı gibi kavramlar internetle ilgili bilinmesi gereken temel kavramlardır.

1.1.1. Bilgisayar

Bilgisayar, "insanlar tarafından hazırlanıp yüklenen programlar yardımıyla bilgileri belirli düzende saklamak, işleyerek yeni sonuçlar üretmek, üretilen bilgileri başka yerlere iletmek, başka yerlerdeki bilgilere ulaşmak gibi amaçlarla kullanılan makineler" ya da "dış ortamdan aldığı verileri, üzerine yüklenen programlar aracılığıyla depolayan, işleyen, yeni sonuçlar üreten, ürettiği sonuçları kullanıcıya sunan, veri iletişimini sağlayan makine" olarak tanımlanmaktadır.[14] Bilgisayarlar soyut ve somut unsurlardan oluşur. Gözle gördüğümüz bütün fiziki parçalarına "donanım", bu parçaların ne şekilde çalışacağını belirleyen fiziki olmayan soyut kısmına ise "yazılım" denilmektedir.[15] Bilgisayarlarda bilgiler veri (data) şeklinde saklanır. Veri, bilginin, iletişim, yorum ya da işlem için uygun olarak formülize edilmiş şekilde gösterilmesidir. Bilgisayar tarafından üretilen ve işlenebilen bilgi elemanı için kullanılan genel terimdir.[16]

Bilgisayarın gelişiminde dört unsur hiç değişmemiştir. Bunlar;[17]

1. Bilginin Girişi (Giriş birimleri: Klavye, fare, kamera, tarayıcı, faks-modem vb.)
2. Bilginin saklanması (Hafıza: Sabit disk, disket, cd-rom vb.)
3. Bilginin işlenmesi (Beyin: Merkezi işlem birimi - Central Processing Unit - CPU)
4. Bilginin çıkışı (Çıkış birimleri: Ekran, Yazıcı, Çizici)

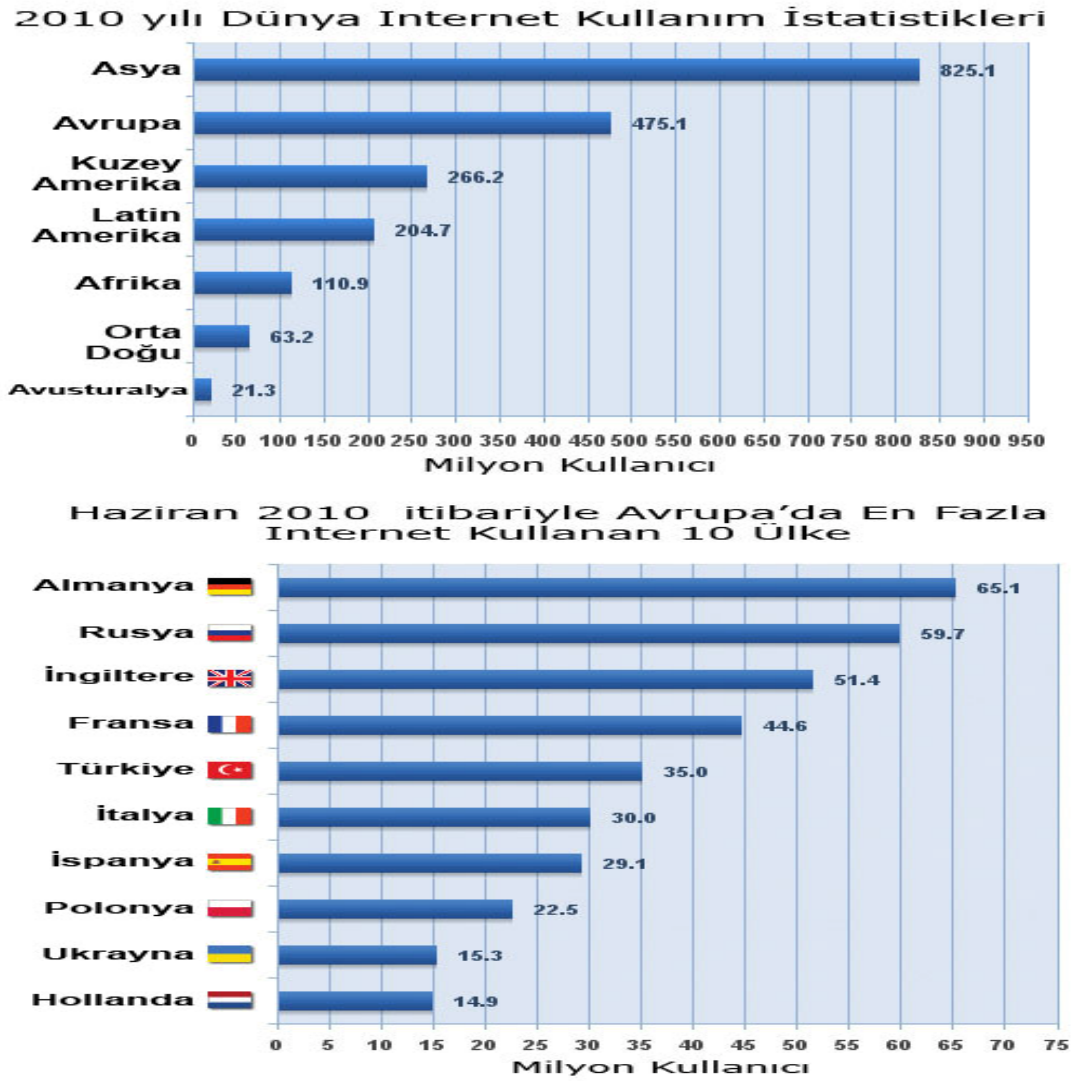
Yukarıda sayılan özellikler bilgisayar benzeri aygıtlarda da görülmektedir. Bunlar bazen gelişmiş cep telefonları ya da kişisel dijital ajandalar olabilmektedir.

---

[14] Dülger, (2004), a.g.e., s.38.
[15] Kurt, (2005), a.g.e., s.31.
[16] Tavukçuoğlu, (2004), a.g.e., s.332.
[17] bilgisayarnedir.com, (t.y.), "Bilgisayar Nedir ?", http://www.bilgisayarnedir.com/bilgisayar-nedir.html, (Erişim Tarihi: 19.08.2010).

1.1.2. İnternet ve İlgili Terimler

Kaynaklarını paylaşmak üzere birbirine bağlanmış iki veya daha fazla bilgisayarın oluşturduğu yapıya bilgisayar ağı denir. Bilgisayar ağlarının birbirine bağlanması sonucu ortaya çıkan, herhangi bir sınırlaması ve yöneticisi olmayan uluslararası bilgi iletişim ağına ise İnternet denmektedir.[18]



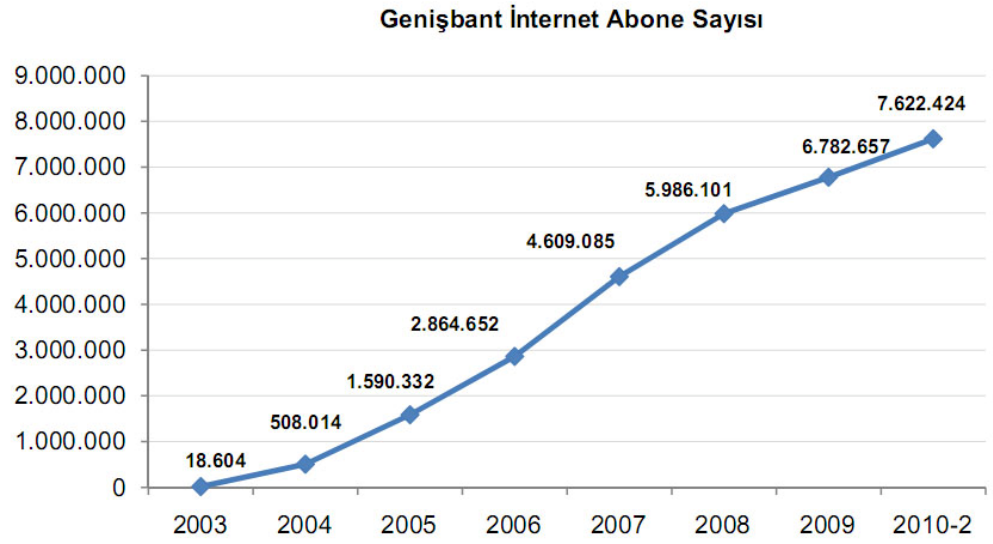
Şekil 1 - Dünya'da ve Ülkemizde İnternet Kullanımı İstatistikleri.[19]

Bilişim suçlarının zaman içerisinde dünyada ve ülkemizde hızla artmasının en önemli faktörlerinden biri olan internet kullanımı ve abone sayısı ülkemizde de hızla artmaktadır.

---

[18] Türk Dil Kurumu, (2010), "Genel Ağ", http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=genel+a%F0, (Erişim Tarihi: 27.08.2010)

[19] internetworldstats.com, (2010), "World İnternet Usage Statistics", http://www.internetworldstats.com, (Erişim Tarihi: 02.11.2010).



Yöntemler Bazında Diğer İnternet Abone Sayıları

	2010-1	2010-2
Çevirmeli Bağlantı (Dial Up)	124.121	120.385
Tümleşik Hizmet Sayısal Ağı (ISDN BA ve PA)	14.237	15.422
Uydu Haberleşme	9477	9624
Metro Ethernet	3648	3667
Kiralık Devre	1182	1243
Elektrik Hatları Üzerinden Genişbant Erişim (PLC, BPL)	662	1434
Çerçeve Röle (Frame Relay)	306	312
Sanal Özel Şebeke (VPN)	139	137
Eşzamansız İletim Modu (ATM)	74	91
Diğer	1744	1823
TOPLAM	**155.590**	**154.138**

Şekil 2 - 2010 Yılı İkinci Çeyreği İtibariyle Ülkemizde İnternet Abone Sayıları.[20]

Elektronik postanın kısaltması olan e-posta, internetin günümüzdeki en yaygın kullanımlarından biridir. E-posta, internete erişimi olan herkesin yazılı mesaj, dosya ve resimleri dünyanın herhangi bir yerindeki herhangi bir kişiye neredeyse

[20] Bilgi Teknolojileri ve İletişim Kurumu, (2010), "Pazar Verileri", http://www.btk.gov.tr/Yayin/Yayinlar.htm, (Erişim Tarihi: 23.10.2010).

anında göndermesine olanak tanımaktadır.[21] İnternetteki elektronik posta trafiğinin ciddi bir kısmını istenmeyen elektronik postalar (spam) teşkil etmektedir. İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi "spam" olarak adlandırılır.[22]

IP adresi ya da numarası, internet de dahil olmak üzere, TCP/IP ağındaki uç noktalara tahsis edilen benzersiz bir kimlik numarasıdır. IP adresi, her birisi 0-255 aralığında değişen dört sekizli rakamdan oluşmaktadır.[23] Alan adları IP adresi denilen, bilgisayarların birbirini tanımasını sağlayan numara sisteminin daha basitleştirilmiş ve akılda kalması için kelimelerle ifade edilmiş halidir.[24] Örneğin bilgisayarpolisi.com i sayfasına erişmek isteyen birisi aslında 188.124.16.13 IP numaralı bilgisayara bağlanmaktadır.

İnternet servis sağlayıcısı (ISS) veya internet erişim sağlayıcı genellikle bir ücret karşılığı internet erişimi sağlayan bir şirkettir. Bir ISS'ye bağlanmanın en yaygın yolları telefon hattı (çevirmeli) veya geniş bant bağlantısı (kablolu veya DSL) kullanmaktır.[25]

İnternet ortamında hizmet ve içerikleri barındıran sistemleri sağlayan veya işleten gerçek veya tüzel kişilere yer sağlayıcı denilmektedir. İnternet salonu ve benzeri umuma açık yerlerde belirli bir ücret karşılığı internet toplu kullanım sağlayıcılığı hizmeti veren veya bununla beraber bilgisayarlarda bilgi ve beceri artırıcı veya zekâ geliştirici nitelikteki oyunların oynatılmasına imkân sağlayan gerçek veya tüzel kişilere ticari amaçla internet toplu kullanım sağlayıcı denilmektedir.[26]

---

[21] yahoo.com, (2010), "E-Posta Yardım", http://help.yahoo.com/l/tr/yahoo/mail/about/about-48033.html, (Erişim Tarihi: 13.10.2010).
[22] spam.org.tr, (2010), "Spam Nedir?", http://www.spam.org.tr/nedir.html, (Erişim Tarihi: 14.10.2010)
[23] ipnumaram.com, (2010), "IP Adresi Nedir?", http://www.ip-numaram.com/ipadresi.html, (Erişim Tarihi: 16.10.2010).
[24] birhost.net, (2008), "Alan Adı (Domain Name) Nedir? Neden Alan Adına İhtiyacım Var?", http://www.birhost.net/edestek/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=48, (Erişim Tarihi: 19.10.2010).
[25] microsoft.com.tr, (t.y.), "İnternet Servis Sağlayıcısı (ISS) nedir?" , http://windows.microsoft.com/tr-TR/windows-vista/What-is-an-İnternet-Service-Provider-ISP, (Erişim Tarihi: 22.10.2010)
[26] İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik, Tanımlar, Madde 3.

1.2. BİLİŞİM SUÇLARI

1.2.1. Bilişim Suçu Kavramı

Bilişim teknolojilerinin hızla gelişmesi ve buna paralel olarak hayata etkisi her geçen gün daha da artmaktadır. Bu artış ve gelişme suç dünyasına da yansımaktadır. Suç dünyasında bilişim teknolojilerinin ilk kez kullanıldığı zamanlardan beri bu alanda bir sınır çizmek, konuyu belli tartışma kalıplarına sığdırmak hep zor olmuştur. Ayrıca bilişim teknolojilerinin gelişmişliği ve kullanım yaygınlığı dünyanın farklı bölgelerinde ve farklı ülkelerinde değişkenlik göstermektedir. Bu ve benzeri sebeplerden dolayı evrensel bir "bilişim suçu" tanımı dahi yapılamamaktadır. Hatta terim olarak "bilişim suçu" yerine "bilgisayar suçu", "siber suç", "ileri teknoloji suçu", "yüksek teknoloji suçu", "sanal suç", "internet suçu", "bilgisayar bağlantılı suç", "bilişim sistemi aracılığıyla işlenen suç", "elektronik suç" gibi terimler kullanılmaktadır.

Bu tanım ve kapsam sorunu nedeniyle bilişim suçlarına "çizgisiz çerçeveli suç" da denilmektedir.[27] Ülkemizde artık terim olarak "bilişim suçu" kavramı yerleşmiştir. Bununla birlikte birçok ülkede olduğu gibi ülkemizde de "bilişim suçunun" tanımı yapılmak yerine bu alanda değerlendirilen eylemlerin (suçların) tanımı yapılmıştır.

Genel olarak bir tanım yapılmak istenirse, bilişim suçu, verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar şeklinde tanımlanabilir.[28]

Literatürde geçen diğer tanımlar incelendiğinde "bilişim teknolojileri kullanılarak işlenen suçlar", "bilgisayar/bilişim sistemleri kullanılarak işlenen suçlar" gibi çok geniş kavramların da kullanıldığı görülmektedir. Çerçeveyi bu kadar geniş tutmak "bilişim suçu" ile "bilişim yoluyla işlenen suç" kavramlarının ayrımını mümkün kılmamaktadır. Ancak uygulamada böyle bir ayrım vardır ve tanımlamaların bu ayrımın ruhuna aykırı olmaması gerekmektedir. Tanımlar yapılırken suç oluşturacak eylemlerin hem teknolojik hem de hukuki yönleriyle ele alınması bu problemi ortadan kaldıracaktır.

---

[27] Karabal, Mustafa; Peker, Bekir ve Savran, Ali, (2004), "Bilişim Suçları Ve Türk Polis Teşkilatı", http://www.turkhukuksitesi.com/makale_128.htm, (Erişim Tarihi: 07.10.2010)
[28] Dülger, (2004), a.g.e., s38.

1.2.2. Bilişim Suçlarının Yapısı ve Özellikleri

Bilişim suçlarının yapı bakımından kendine özgü özelliklerinin başında suçun işlendiği ortama dikkat çekmek gerekmektedir. Bilişim ortamının olmadığı bir durumda bilişim suçundan bahsedilemeyecektir. Bununla birlikte bilişim suçunun işlenebilmesi için gerekli olan bilişim ortamının temel elemanlarını üç kategoride sıralayabiliriz.[29]

Bunlardan birincisi bilgisayarlar ya da benzeri cihazlardır. Özellikle "benzeri cihazlar" olarak kullandığımız kavramı oluşturan unsurlar her geçen gün hızla artmaktadır. Başta akıllı cep telefonları ve avuç içi bilgisayarlar[30] olmak üzere benzeri mobil cihazlar bilişim suçlarının unsurları haline gelmektedir. İkincisi bu cihazlar arasında veri iletişiminin sağlanabilmesi için gerekli bir iletişim ortamıdır. Nitekim bu iletişim ortamı da gelişen teknoloji ile birlikte değişmektedir. İnternetin yaygınlaşması ve sonrasında kablosuz ağlar ve 3G[31] gibi mobil iletişim teknolojilerinin kullanımının artması bilişim suçlarının da artmasına sebep olmuştur. Son olarak bilişim ortamının tamamlanabilmesi için bilişim cihazlarının çalışması için gereken enerjinin (elektrik) sağlanması gerekir.

Bilişim suçlarının özelliklerinin en başında işlenebilmesindeki kolaylık ancak tespit edilmesi ve cezalandırılmasındaki zorluktan bahsetmek gerekir.[32] Kriminojenik (suç yaratıcı) faktörler (fırsatları) açısından bilişim ortamı çok müsaittir. Bu uygun ortamın yine bilişim teknolojileri ile giderilmeye çalışılması da başka bir olumsuz durum olarak karşımıza çıkmaktadır. [33]

---

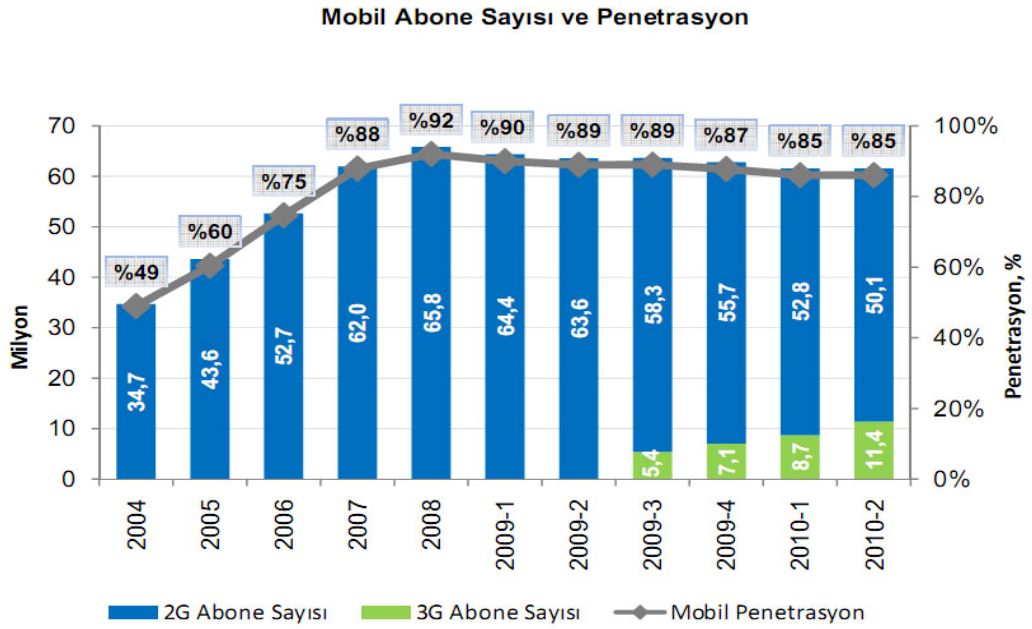
[29] Karagülmez, Ali, (t.y.), "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", http://www.caginpolisi.com.tr/46/7-8-9-10.htm, (Erişim Tarihi: 03.09.2010).

[30] "Dijital Özel Sekreter" anlamına gelen "Personal Digital Assistant" tanımının kısaltması olan PDA'ler, boyutları avuç içine sığacak kadar küçük, başta kişisel bilgilerin saklanabildiği ve iletişim özelliğine sahip elektronik cihazlardır. PDA için, yaygın olarak "avuç içi bilgisayar" ya da "cep bilgisayarı" denilen cihazların genel adı da denebilir.
http://www.teknosa.com/msib21/formlar/teknodanismandetay.aspx?cguid={4074f107-28dc-4e13-8d27-d7344f40e0f0}, (Erişim Tarihi: 21.09.2010).
Akıllı Cep Telefonu (Smartphone) ise Cep telefonunun sağladığı klasik özelliklere, bilgisayar dünyasının bir ürünü olan PDA'lerin özelliklerinin de eklenmesiyle tasarlanan gelişmiş mobil iletişim cihazlarıdır. http://www.genpatech.com/id_3325, (Erişim Tarihi: 21.09.2010)

[31] 3. Nesil GSM Hizmetleri (3G ya da 3N) üçüncü nesil kablosuz telefon teknolojilerine verilen genel addır. 3G'nin 2G'ye göre getirmiş olduğu en büyük yenilik taban olarak alınan verinin ses değil sayısal veri olmasıdır. Buna ek olarak, 3G sisteminde cihazlar bant genişliğini sadece veri alışverişi sırasında işgal ederler. 2003 yılında Avrupa'da, 2009 yılında ülkemizde kullanılmıştır.
(http://www.3gnedir.com, Erişim Tarihi: 21.09.2010).

[32] Kurt, (2005), a.g.e., s56.

[33] Aydın, Emin, (1992), *Bilişim suçları ve Hukukuna Giriş*, Ankara: Doruk Yayınları, s.14.



Şekil 3 - Ülkemizde 3G ve Diğer Mobil İnternet Teknolojilerini Kullanan Abone Sayıları[34]

Suçlu profili açısından da bilişim suçlarının kendine has özellikleri vardır. Genel olarak bilişim suçluları bilişim teknolojilerinde uzman kişilerdir ve eğer maddi çıkar sağlamak amacıyla bu suçları işliyorlarsa çoğu zaman organize çalışmaktadırlar. Bununla birlikte az seviyede teknik bilgiye sahip suçlular da büyük zararlar ortaya çıkaran suçlar işleyebilmektedirler.

1.2.3. Bilişim Suçlarını Klasik (Geleneksel) Suçlardan Ayıran Özellikler

Belki binlerce yıldır işlenen klasik (geleneksel) suçların yanında bilişim suçu çok yeni bir kavram olarak karşımıza çıkmaktadır. Klasik suçlardan kasıt geçmişten günümüze kadar hukuki dayanaklarıyla birlikte cezai yaptırımları olan adam öldürme, yaralama, hırsızlık, kundaklama, gasp, tehdit gibi suçlardır. Bu nedenle bilişim suçları klasik suçlarla az da olsa benzerlik göstermekle beraber büyük ölçüde farklılıklar göstermektedir. Bu farklılıklardan en çok öne çıkanları maddeler halinde sıralayacak olursak;

1. Bilişim suçlarının çerçevesini çizmek ve kapsamını belirlemek çok zordur. Teknolojinin gelişmesi ve yaygınlaşması bu durumu daha da zorlaştırmaktadır.[35]

[34] Bilgi Teknolojileri ve İletişim Kurumu, (2010), "Pazar Verileri", http://www.btk.gov.tr/Yayin/Yayinlar.htm, (Erişim Tarihi: 23.10.2010).

2. Sürekli değişen ve hızla artan bir suç türü olduğu için bilişim suçları ile mücadele etmek de çok zor olmaktadır.

3. Bilişim suçları zaman ve mekân kavramından bağımsız gerçekleşir ve anlık olurlar. [36]

4. Dünyada globalleşmeye bağlı olarak ekonomi ve uluslar arası yapıdaki bozulmalarla birlikte bilişim suçları klasik suçlara göre anormal oranlarda artış göstermektedir.[37]

5. Bilişim suçlarının mağduru bazen bir kişi, bazen bir kurum, bazen ise toplumun tamamı olabilmektedir.

6. Bilişim suçları klasik suçlardan farklı olduğu için klasik polisiye yöntemlerle önlenmesi mümkün değildir. Dolayısıyla bu suçlarla mücadele edecek güvenlik güçlerinin de belli bir teknik bilgisi olmak zorundadır.

7. Bilişim suçlarının önlenmesinde ve faillerin yakalanmasında kurumlar arası işbirliği kaçınılmazdır. Hatta bazı durumlarda uluslar arası işbirliği gerekmektedir.[38]

8. Bilişim suçları bir ülkenin teknolojiye ve e-devlet uygulamalarındaki otomasyona bağımlılıklarıyla doğru orantılıdır. Yani bilişim teknolojilerini çok az kullanan ülkeler için bilişim suçları ciddi bir tehdit değildir.[39]

9. Bilişim sistemleri ile işlenilen suçlarda suç ile ilgili deliller farklı şekil ve formatlarda suç sonrasında dijital delil olarak bulunabilmektedir.[40] Dijital delil toplama ve delillendirme süreci de klasik suçlarda elde edilen delillerden farklıdır. Dijital delilleri muhafaza etme ve mahkemeye sunma çok hassas bir süreçtir ve bozunmaya müsaittir.

---

[35] Karabal, Mustafa; Peker, Bekir; Karakaya, Musa ve Savran, Ali, (2004), *Barışın Köprüsü İnternet*, Konya: Akademilenyum Yayınları, s.82.
[36] Kurt, Levent, (2005), *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* TODAİE, Yayınlanmış Yüksek Lisans Tezi, Ankara, s.56
[37] Karagülmez , (2009), a.g.e., s.60.
[38] Dokurer, Semih, (t.y.), "Ülkemizde Bilişim Suçları Ve Mücadele Yöntemleri", http://bilisimsurasi.org.tr/dosyalar/17.doc, (Erişim Tarihi: 29.07.2009).
[39] Özeren, Süleyman, (2006), Siber Terörizm [Ders Notları], Polis Akademisi, Ankara
[40] Ekizer, Hakan, (2007), "Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği)" , http://ekizer.net/index.php?option=com_content&task=view&id=16&Itemid=43, (Erişim Tarihi: 21.10.2010).

10. Bilişim suçunun sonucunda çok yüksek kazancın kolay ve risksiz olarak temin edilebildiği durumlar ortaya çıkmaktadır.[41]

11. Klasik suçlarda da mağdurların şikâyetçi olmaması nedeniyle işlenen suçların bir kısmı istatistiklere yansımamaktadır ancak bu durum bilişim suçlarında daha sık görülmektedir. Mağdurlar potansiyel olarak kötü bir etkiye maruz kalmamak, müşterilerin güvenini kaybetme korkusu, şöhretlerine bir zarar gelme korkusu, algılama eksikliğine sahip olmak, kanunları yeterince bilmemek, kanunlara ya da uygulayıcılarına yeterince güvenmemek gibi sebeplerden ötürü çoğu zaman şikâyetçi olmamaktadırlar. [42]

12. Bilişim suçlarının ortaya çıkmasıyla birlikte klasik suçları kapsayan hukuki dallardan ayrı olarak yeni ihtiyaçlara cevap verebilecek "bilişim hukuku" adında ayrı bir dal ortaya çıkmıştır. Ancak bilişim hukuku her zaman için ceza hukukunun bir kolu olmayabilmektedir aynı zamanda özel hukuka ilişkin durumlarda da öne çıkmaktadır.

1.2.4. Bilişim Suçlarının Tasnifi

Bilişim suçlarıyla ilgili kaynaklar incelendiğinde tasnif konusundan farklı yaklaşımların olduğunu görmekteyiz. Bu farklılıkların sebebi tasnif yapılırken değişik unsurların dikkate alınmasından kaynaklanmaktadır. Dikkate alınan unsurlar suçun işleniş şekli, hukuki metinler ve uluslar arası düzenlemelerdir.

Avrupa Konseyi Siber Suç Sözleşmesi'ne göre bilişim suçları, bilgisayar veri veya sistemlerinin gizliliği, bütünlüğü ve kullanıma açık bulunmasına yönelik suçlar, bilgisayarlarla ilişkili suçlar, içerikle ilişkili suçlar ve fikri mülkiyet haklarının ihlali ile ilgili suçlar şeklinde sınıflandırılmıştır.[43]

Birleşmiş Milletler tarafından İtalya'da düzenlenen "Symposium on The Occasion of The United Nations Convention Against Transnational Organized Crime" sempozyumu bünyesinde 14 Aralık 2000 tarihinde düzenlenen "The Challenge of Borderless Cyber Crime" panelinde bilişim suçları ile ilgili bir takım

[41] Tulum, İsmail, (2006), *Bilişim Suçları ile Mücadele,* Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Isparta, s.32.
[42] Karagülmez , (2009), a.g.e., s. 55.
[43] Avrupa Konseyi, (2001), "Convention on Cybercrime" , http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, (Erişim Tarihi: 17.10.2010).

fiillerin üye ülkeler tarafından cezai müeyyide ile karşılanması tavsiye edilmiştir. Bunlar; bilişim sistemlerine yetkisiz giriş, bilgisayar veya bilişim sistemlerinin hukuka aykırı olarak kullanımına engel olunması, bilişim sistemleri içerisindeki verilerin değiştirilmesi veya tahrip edilmesi, veri veya program gibi soyut birtakım değerlerin ele geçirilmesi, bilişim sistemleri ile sahtekârlık fiilleridir.[44]

Avrupa Topluluğunda ise bilgisayar suçları şöyle tasnif edilmektedir;[45]

- Bir kaynağın veya herhangi bir değerin gayri kanuni olarak transferini sağlamak için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek;
- Bir sahtekârlık yapabilmek için kasten bilgisayar verilerine ve/veya programlarına girmek, bozmak, silmek ve/veya yok etmek;
- Bilgisayar ve/veya telekomünikasyon sistemlerinin çalışmasını engellemek amacıyla kasten bilgisayar verilerine ve/veya programlarına yahut bir bilgisayar sistemiyle bir bağlantı bir bağlantı sağlayan mekanizmaya girmek, bozmak, silmek ve/veya yok etmek,
- Piyasaya sürmek ve ticari olarak yararlanmak amacıyla bir bilgisayar programının yasal malikinin sahip olduğu hakları zarara uğratmak,
- Bir bilgisayar ve/veya telekomünikasyon sistemi sorumlusunun izni olmaksızın veya mevcut emniyet tedbirlerini aşarak bu sistemlere kasten girmek veya müdahalede bulunmaktır.

Bilişim suçları ile ilgili diğer bir sınıflandırma da şu şekilde olabilir; [46]

- Veri Suçları (a-Verilerin durdurulması, b-Verilerin değiştirilmesi, c-Verilerin çalınması),
- Ağ Suçları (a-Ağ engellenmesi, b-Ağ sabotajı),
- Yetkisiz Giriş Suçları (a-Bilişim sistemine izinsiz giriş, b-Virüs yayma),
- İlgili Suçlar (a-Bilgisayar yoluyla sahtecilik, b-Bilgisayarla bağlantılı dolandırıcılıklar)

[44] Pallı Hayati, (2008), *Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları*, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Kayseri, s.68.
[45] Kurt, (2005), a.g.e., s.78.
[46] A.g.e., s.79.

Bilişim suçlarının tasnifi konusundaki yaklaşımlar incelendiğinde genel olarak ayrımın bilişim teknolojilerinin "amaç" ve "araç" olarak kullanılmasından çıktığını görmekteyiz. Çalışmamızın da temel çıkış noktasını oluşturan bu ayrımın sonucu olarak genel bir tasnif yapmak istersek;

- Bilişim Suçları
- Bilişim Yoluyla İşlenen Suçlar

Şeklinde bir ayrımın yapılması hemen hemen bütün görüşlerle örtüşmektedir.

1.2.5. Türk Ceza Kanununda Bilişim Suçları

Bilişim suçları kavramı ilk kez 765 sayılı Türk Ceza Kanunu'nda değişiklik ve ekleme yapan 06.06.1991 tarih ve 3756 sayılı kanunla literatüre girmiştir. Söz konusu düzenlemeler 765 sayılı Türk Ceza Kanunu'nu ortadan kaldıran ve 01.06.2005 tarihinde yürürlüğe giren 5237 sayılı yeni Türk Ceza Kanunu'ndaki hükümler uygulanmaya başlayıncaya kadar yürürlükte kalmıştır.[47]

Günümüzde halen 5237 sayılı Türk Ceza Kanunu'ndaki düzenlemeler geçerlidir ve uygulamada bazı durumlarda yetersiz kaldığı düşünülse de kısmen oturmuş durumdadır. Bilişim Suçları Türk Ceza Kanunu'nun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde 243, 244, 245 ve 246. maddelerinde düzenlenmiştir.

1.2.5.1. Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Orada Kalmaya Devam Etme Suçu (TCK Madde 243)

(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.

[47] Kurt, (2005), a.g.e., s.79.

Bu madde Avrupa Konseyi Siber Suçları Sözleşmesi'nin ikinci maddesinde yer alan "kanunsuz erişim" suçunun karşılığı şeklinde düzenlenmiştir.[48] Buna göre;

Her bir taraf devlet bir bilgisayar sisteminin tamamı veya herhangi bir bölümüne haksız ve kasıtlı olarak erişilmesini suç kapsamına almak için gerekli kanuni düzenlemeyi yapmalı gerekli önlemleri almalıdır. Taraf devlet bu suçun oluşması için erişimin güvenlik önlemleri ihlal edilerek ya da bilgisayar sistemine bağlı diğer bir bilgisayar sistemi aracılığıyla bilgisayar verisini almak ya da başka kötü niyetlerle kullanmak şartına bağlayabilir.

Bilişim sistemine hukuka aykırı erişimin cezalandırılmasıyla korunan hukuki değer karma nitelik taşımaktadır. Bu suçla öncelikli olarak, bireylerin özel hayatlarının gizliliği, sırlarının dokunulmazlığı ve haberleşme özgürlükleri korunmaktadır. Çünkü bilişim sisteminde yer alan unsurlar, sistem sahibinin hukukça korunan özel alanına ait olduğundan hak sahibinin rızası bulunmadıkça bu alana yetkisiz erişilmemelidir. Böyle bir fiil aynı zamanda "özel hayatın gizliliği" başlıklı Anayasanın 20nci maddesine de aykırılık teşkil eder.[49]

Özellikle son yıllarda e-devlet uygulamalarının da yaygınlaşmasıyla birlikte ülkemizde bilişim sistemlerinin güvenliğinin kanuni yaptırımlarla desteklenmesi kaçınılmaz bir kamu ihtiyacıdır, bu madde bu ihtiyaca cevap vermeye çalışmaktadır.

Madde metninde geçen "kimse" sözcüğü suçun failinin herkes olabileceğini ifade etmektedir. Hukuka aykırı olarak "bilişim sistemine girme ve sistemde kalma" suçu fail açısından bir özellik göstermemektedir.[50] Ancak daha öncede bahsettiğimiz gibi bilişim suçları açısından failin belli bir teknik bilgi ve kapasiteye sahip birisinin olması kaçınılmazdır. Suçun mağduru da yine herkes olabilmektedir.

Maddenin gerekçesi incelendiğinde sisteme, hukuka aykırı olarak giren kişinin belirli verileri elde etmek amacıyla hareket etmiş bulunmasının önemi yoktur. Sisteme, doğal olarak, haksız ve kasten girilmiş olması suçun oluşması için yeterlidir.[51] "Sistemde kalmaya devam etmek" tanımlamasının suçun tamamlayıcı unsuru haline getirilmesi,

---

[48] Ankara Emniyet Müdürlüğü, (t.y.), "Bilgisayar Suçları Sözleşmesi", http://www.ankaraemniyet.gov.tr/index.php?id=601, (Erişim Tarihi: 26.10.2010).
[49] Kızıltan, Mehmet Burak, (2007), *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme Ve Bozma Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.68.
[50] Dülger, (2004), a.g.e., s.214.
[51] Türk Ceza Kanunu Gerekçesi.

kötü niyeti olmayıp da kısa süreliğine giriş yapan, araştırma amacı taşıyan, ya da yazılımının başarısını test etmek isteyen kişilerin yaptıkları sisteme girme eylemlerini de çok katı bir düzenleme ile münhasıran suç saymama düşüncesindendir. Ancak bu tür bir durum suça teşebbüs olarak değerlendirilecektir.[52]

İlke olarak kanuni unsuru gerçekleştiren bir hareket hukuka aykırıdır ancak ceza hukuku hukuka aykırılığa bir takım istisnalar getirerek, kanuni unsuru tamamlayan bazı fiillerin hukuka uygun olacağını belirlemiştir. Bunlar; Kanunun hükmü ve amirin emri (TCK m. 24/1), Meşru savunma ve zorunluluk hâli (TCK m. 25), Hakkın kullanılması ve ilgilinin rızası (TCK m. 26).[53] Burada da "bilişim sistemine girme ve orada kalmaya devam etme" eylemi hukuka aykırı olmak zorundadır. Örneğin bir suç soruşturmasında güvenlik görevlilerinin terör propagandası yapan bilişim sistemlerine girmeleri ve hatta verilerle ilgili işlemler yapmaları hukuka aykırılık teşkil etmez.

Suçlar, kural olarak ancak kasten işlenebilir. Kast, kişi ile işlediği suçun maddî unsurları arasındaki psikolojik bağı ifade etmektedir. Kast, suçun icrası sırasında var olmalıdır. Kast suçun kanuni tanımındaki maddi unsurların somut olayda gerçekleşmekte olduğunu gösterir. [54] "Bilişim sistemine girme ve orada kalmaya devam etme" suçunda da failin bilerek ve isteyerek hareket etmesi arandığı için bu suç tipinin taksirle işlenmesi mümkün değildir. Ancak yasa koyucu bu suç tipini oluşturan eylemlerin fail tarafından yapılması sırasında sistemin içerdiği verilerin taksirle yok edilmesi ya da değiştirilmesi durumunu ağırlaştırıcı neden olarak öngörmüştür.[55]

Kanunda suç olarak tanımlanmış bir fiilin icrasına başlanılmakla birlikte bu fiilin icrası henüz tamamlanmamış olabileceği gibi, icrası tamamlanmakla birlikte kanuni tarifteki netice gerçekleşmemiş olabilir. Buna teşebbüs halinde kalmış suç denir. Teşebbüsten dolayı bir fiilin cezalandırılabilmesi için, fiilin icrasının tamamlanamamış olması, ya da neticenin gerçekleştirilememiş olmasının kanun

[52] Kurt, (2005), a.g.e., s.148.
[53] "Ceza Hukuku", http://tr.wikipedia.org/wiki/Ceza_hukuku, Erişim Tarihi: 17.10.2010
[54] Akpınar, Gürsel, (t.y.), "Yeni Tck'na Göre Suçun Unsurları Bağlamında Kast, Taksir Ve Kast-Taksir Kombinasyonu", http://www.ceza-bb.adalet.gov.tr/makale/178.doc, (Erişim Tarihi: 12.10.2010).
[55] Dülger, (2004), a.g.e., s.221.

koyucunun bir yaptırımına bağlanılmış olması gerekmektedir.[56] "Bilişim sistemine girme ve orada kalmaya devam etme" suçunda da teşebbüs mümkündür, örneğin bir bilişim sistemine girmek için hazırlık yapılması ancak iletişimin kopması eylemin teşebbüs aşamasında kalmasına sebep olacaktır. Ancak bu durum için bir yaptırım kanunen düzenlenmemiştir.

5237 sayılı TCK, iştirak müessesesini, tamamıyla yeniden düzenlemiştir. Bu bağlamda, iştirak kategorilerini üç temel noktada toplamış, uzun süredir eksikliği duyulan "dolayısıyla faillik (dolaylı faillik)" müessesesini tanzim etmiş, bağlılık kurallarını düzenleyerek, sirayet meselesini köklü bir çözüme kavuşturmuştur.[57] Suça iştirak türleri faillik, azmettirme ve yardım etme durumları "bilişim sistemine girme ve orada kalmaya devam etme" suçu açısından mümkündür.

Suçun içtimai Türk Ceza Kanunu'nun 42, 43 ve 44. maddelerinde düzenlenmiştir. Birleşik suç iki suçtan meydana gelen bir suç tipidir, şöyle ki, bu iki suçtan biri diğerinin ya unsurunu ya da ağırlatıcı sebebini teşkil eder. Demek oluyor ki, bu iki suç arasında bir bağlantı varsa da, bu bağlantı, suçlardan birinin, diğerinin diğer suçun unsurunu veya ağırlatıcı sebebini teşkil etmesini gerektirmektedir. İşte bu halde unsur veya ağırlatıcı sebebi teşkil eden suç bir tek birleşik suç teşkil etmek suretiyle kaynaşırlar ve faile sadece en ağır neticeyi kapsayan suçun cezası verilir.[58] "Bilişim sistemine girme ve orada kalmaya devam etme" suçu ileriki konularda değineceğimiz "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun unsuru şeklinde karşımıza çıkarken yine ileriki konularda değineceğimiz bilişim yoluyla işlenen suçların bir kısmında ise ağırlaştırıcı sebep olarak karşımıza çıkmaktadır.

Zincirleme suç bir suç işleme kararının değişmeden, kanunun aynı hükmünün, başka zamanlarda da olsa, birkaç defa ihlalidir. Karar ve ihlal edilen hak bakımından birlik ve zaman bakımından birbirinden ayrı fiillerde çokluk varsa, zincirleme suç vardır. Zincirleme suçun mevcudiyeti için maddi bakımdan, kanunun aynı hükmünün birden fazla ihlali ve manevi bakımdan da ihlallerin aynı suç işleme kararını (kast)

[56] Gürgen, Ahmet Cemal, (2005), "Teşebbüs", http://www.ceza-bb.adalet.gov.tr/makale/169.doc (Erişim Tarihi: 19.10.2010).
[57] Darende, M. İhsan, (2005), "Yeni TCK'da İştirak", http://www.turkhukuksitesi.com/makale_182.htm, (Erişim Tarihi: 23.10.2010).
[58] Hafızoğulları, Zeki, (t.y.), "5237 Sayılı Türk Ceza Kanununda Bileşik Suçun Tanımı Hakkında", http://www.zekihafizogullari.com/Makaleler/TCK%20Bilesik%20Suc.doc, (Erişim Tarihi: 27.10.2010).

taşıması lazımdır.[59] Zincirleme suç açısından da "bilişim sistemine girme ve orada kalmaya devam etme" uygulamada sıklıkla görünmektedir.

243. maddenin ikinci fıkrasında suçun bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde hafifletici neden ortaya çıkmaktadır. Burada bedeli karşılığı yararlanılabilen sistemlerin halka açık olmasından dolayı böyle bir yaklaşım sergilenmiştir.[60] Üçüncü fıkrada ise suç nedeniyle sistemin içerdiği veriler yok olur veya değişirse suçun ağırlaştırıcı sebebi olarak karşımıza çıkmaktadır.

1.2.5.2. Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi Suçu (TCK Madde 244)

(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 beş bin güne kadar adlî para cezasına hükmolunur.*

Bu madde Avrupa Siber Suçlar Sözleşmesi'nin dördüncü maddesinde yer alan "Veriye Müdahale" suçunun ve beşinci maddesinde yer alan "Sistem Engellemeleri" suçunun karşılığı şeklinde düzenlenmiştir. Bu maddelere göre;

Her bir taraf devlet, bir kimsenin bilgisayar verisine hakkı olmadığı halde, bilerek ve isteyerek zarar verme, silme, bozma, değiştirmeye ya da ortadan kaldırma fiilleri işlemesini suç olarak düzenlemek üzere gerekli kanuni düzenlemeyi yapmalı

[59] Kılıç, Savaş, (t.y.), "Müteselsil Suç Kavramı", http://www.hukukcu.com/bilimsel/kitaplar/kilic_muteselsilsuc/endeks.htm, (Erişim Tarihi: 27.10.2010).
[60] Gürler, Cemalettin, (2007), "Bilişim Sistemlerine Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri", http://www.emo.org.tr/ekler/111f133fa0ea545_ek.pdf?dergi=2, (Erişim Tarihi: 16.10.2010).

ve gerekli diğer önlemleri almalıdır. Taraf devlet 1. paragrafta belirtilen durumun oluşmasını ciddi zarar oluşma olasılığına bağlı tutma hakkına sahiptir. Her bir taraf devlet veri yükleyerek, aktararak zarar vererek, silerek, bozarak, değiştirerek veya müdahale ederek bilgisayar sisteminin kullanımında hakkı olmadığı halde bilerek ve isteyerek bilgisayarın sisteminin çalışmasını sekteye uğratma fiilini ulusal kanununda suç olarak düzenlemeli ve gerekli diğer düzenlemeleri yapmalıdır. [61]

Bu madde ile bilişim sisteminin sadece soyut kısmı yani veriler değil aynı zamanda somut kısmı yani donanımlar ve cihazlar da koruma altına alındığından, korunan hukuksal değer karma bir nitelik göstermektedir. Maddenin gerekçesi incelendiğinde bilişim sistemlerine yöneltilen ızrar fiillerinin özel bir suç hâline getirildiğinden bahsetmektedir.[62] Ancak burada failin kastı bilişim sisteminin verilerini bozmak ya da sistemin işleyişini engellemek olmadığı durumlarda yani sadece donanımlara zarar vermek kastı olduğunda "mala zarar verme suçu (TCK Madde 151)" uygulanacaktır.[63]

Her gerçek kişi "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun faili olabilir. Ancak suç tüzel kişi yararına işlenebilir. Suç yalnızca bir bütün halinde bilişim sistemini değil aynı zamanda verilere zarar verilmesi fiillerini de içermektedir. Bu nedenle kişinin, başkasının haklarına zarar vermeksizin herhangi bir bilişim sisteminde bulunan kendisine ait verilere zarar vermesi halinde suç oluşmayacaktır. Bazen bilişim sisteminin sahibi ile verilerin sahibi birbirinden farklı kişiler olabilir. Bu durum failin belirlenmesinde sorun yaratabilir. Eğer fiil bilişim sistemine yönelik olarak gerçekleştirilmişse sistemin kendisinin, bilişim sisteminin içerdiği verilere yönelik gerçekleştirilmişse bu verilerin, hem bilişim sistemine hem de verilere karşı gerçekleştirilmişse her ikisinin de ayrı ayrı mülkiyet, kullanım ve tasarruf haklarının kime ait olduğunu ve zararı kimin meydana getirdiğini açıkça ortaya koymak gerekir. Her gerçek veya tüzel kişi suçun mağduru olabilir.[64]

---

[61] Ankara Emniyet Müdürlüğü, (t.y.), "Bilgisayar Suçları Sözleşmesi", http://www.ankaraemniyet.gov.tr/index.php?id=601, (Erişim Tarihi: 26.10.2010).
[62] Türk Ceza Kanunu Gerekçesi
[63] Dülger, (2004), a.g.e., s.231.
[64] Soyaslan, Doğan, (2009), *Bilişim Alanında Suçlar*, *Prof. Dr. Mualla Öncel'e Armağan,* Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayını, s.1572.

Yasa, gösterdiği hareketlerden herhangi birinin yapılması halinde suçun meydana geleceği hükmünü koymuşsa suç seçimlik hareketli bir suçtur. Seçimlik hareketli suçun meydana gelebilmesi için yasada gösterilen hareketlerden bir tanesinin yapılması yettiği için yasanın öngördüğü hareketlerden birkaçını birbiri ardından yapan kimse o suçu bir defadan çok işlemiş olmaz ve eyleme içtima hükümleri uygulanmaz.[65] "Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçu da seçimlik hareketli bir suçtur yani kanun metninde belirtilen eylemlerden birisinin yapılması yeterlidir. Bilişim sisteminin engellenmesi geçici olarak hizmet verememe ya da iyi performansla hizmet verememedir, bozma ise kalıcı olarak bu sistemin zarar görmesidir. Hem engelleme hem de bozma soyut olarak yani dijital veri boyutunda olabileceği gibi somut olarak donanımsal olarak da olabilir. Maddenin ikinci fıkrasında sadece bilişim sisteminin soyut boyutu güvence altına alınmıştır. Veriler üzerinde yapılan her türlü hukuka aykırı işlem yasal yaptırıma bağlanmıştır.

"Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun gerçekleşebilmesi için hukuka aykırı bir durum olması gerekir. Örneğin 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi Ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" çerçevesinde mahkeme kararıyla site erişimlerinin engellenmesi TCK 244. madde kapsamında değerlendirilemeyecektir.[66]

Kast, suçun kanunî tanımındaki unsurların bilerek ve istenerek gerçekleştirilmesidir.[67] Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçu da genel kasıt ile işlenen bir suç türüdür. Ancak maddenin üçüncü fıkrasında suçun "bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi" ve dördüncü fıkrasında suçun işlenmesi suretiyle "kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması" eylemleri ağırlaştırıcı sebepler olarak karşımıza çıkmaktadır. Bu eylemler kast açısından ayrı olarak değerlendirilmelidir. Maddede belirtilen eylemler taksirle işlenmeyecek eylemlerdir.

---

[65] Alacakaptan, Uğur, (1975), *Suçun Unsurları*, Ankara: Sevinç Matbaası, s.47.
[66] Telekomünikasyon İletişim Başkanlığı, (2010), "Sıkça Sorulan Sorular" http://www.tib.gov.tr/kat/sss, (Erişim Tarihi: 17.10.2010).
[67] Türk Ceza Kanunu Madde 21.

"Bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun teşebbüs aşamasında kalması mümkündür ancak daha öncede bahsettiğimiz gibi suçun seçimlik hareketli bir suç olmasından dolayı eylemlerden birinin yerine getirilmesi suçun oluşmasında yeterli olacaktır, bu durumda teşebbüsten bahsetmek mümkün değildir.

Suça iştirak konusunda 244. madde açısından özel bir durum olmamakla birlikte "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun zincirleme ve mütemadi şekilde işlenmesi mümkündür. Ayrıca daha önce bahsettiğimiz 243. maddede tanımlanan "Bilişim sistemine girme ve orada kalmaya devam etme" suçu 244. maddenin geçit suçu olabildiği gibi 244. maddede tanımlanan "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçu da başka suçların geçit suçu olabilir.[68]

TCK 244. maddesinin dördüncü fıkrasında geçen "tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlaması" eylemi bazı kaynaklarda farklı bir suç türü olarak "bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama" suçu şeklinde değerlendirilmiştir. Ancak maddenin gerekçesi de incelendiğinde bahse konu eylemin "bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi" suçunun ağırlaştırıcı sebebi olduğu ve "fiilin daha ağır cezayı gerektiren başka bir suç oluşturmaması" durumunda TCK 244. maddenin uygulanacağını açıkça belirtmiştir. Ayrıca gerekçede eylemin "dolandırıcılık, hırsızlık, güveni kötüye kullanma veya zimmet suçunu oluşturması hâlinde, bu fıkra hükmüne istinaden cezaya hükmedilmeyeceği" de örnek olarak belirtilmiştir.

1.2.5.3. Banka veya Kredi Kartlarının Kötüye Kullanılması Suçu (TCK Madde 245)

(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

[68] Dülger, (2004), a.g.e., s.242.

başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.

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

(4) Birinci fıkrada yer alan suçun;

a) Haklarında aykırılı 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,

d) Zararına aykırı olarak işlenmesi halinde, ilgili akraba hakkında cezaya hükmolunmaz.

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

İlk defa 5237 sayılı Türk Ceza Kanunu'nda banka ve ya kredi kartlarının kötüye kullanılmasına yönelik bir suç tanımı bilişim alanında suçlar başlığı altında düzenlenmiştir. Ancak burada dikkat edilmesi gereken kredi kartları suçlarının sadece bilişim sistemi yoluyla işlenmemesidir. Çalıntı bir kredi kartının başka bir pos[69] cihazında kullanılmasında da bu madde geçerlidir. Suçta bilişim sistemleri kullanılarak kartın oluşturulması, kart bilgilerinin bilişim sistemleri kullanılarak ele geçirilmesi veya elde edilmiş kartın bilişim sistemleri aracılığı ile menfaat temini amacıyla kullanılması durumunda bilişim suçları başlığı altında yer almalıdır görüşleri daha şimdiden yukarıda ki fıkraya muhalefet eder biçimde ortaya

[69] Pos (Point of Sale) cihazı kredi kartlarının işlem yapabilmesi için sokulduğu cihazdır. Bu cihazlar, kısaca pos veya pos aleti olarak da bilinir. Kredi kartı üreten her bankanın müşterilerine kolaylık olması amacıyla, üye işyerleri aracılığıyla POS cihazı ile hizmet vermesi gerekmektedir.

çıkmaktadır.[70] Ancak maddenin gerekçesine bakıldığında banka ve ya kredi kartlarının hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarının konusu olmaması için ve duraksamaları ve içtihat farklılıklarını önlemek amacıyla tüm fiillerin bir madde çatısı altında toplanması amaçlanmıştır.[71]

Maddenin gerekçesine göre korunan hukuki yarar banka veya kredi kartlarının hukuka aykırı olarak kullanılması suretiyle bankaların veya kredi sahiplerinin zarara sokulmasını, bu yolla çıkar sağlanmasını önlemek ve failleri cezalandırmaktır.[72]

"Banka ve ya kredi kartlarının kötüye kullanılması" suçunun faili herkes olabilmektedir ancak dördüncü fıkrada sadece birinci fıkradaki suç açısından şahsa bağlı cezasızlık nedenleri gösterilmektedir. Suçun mağduru ile suçtan zarar gören kimse arasında farklılıklar vardır. Gerçekten, belirli bir suçtan, onun mağdurundan başka, diğer bir kimse de hukuken korunan bir hakkın ihlali dolayısıyla zarara uğramış olabilir ve bu zararın tazmini istemek hakkı da doğabilir. Bu suçta asıl mağdur malvarlığında eksilme olan kart sahibi iken ilgili banka da suçtan zarar gören taraf olabilmektedir.[73]

TCK 245. maddesinde üç ayrı suç düzenlenmiştir. Maddenin ilk fıkrasında, ne şekilde ele geçirilmiş olursa olsun, başkasına ait bir banka veya kredi kartını elinde bulunduran kimsenin, kart sahibinin veya kartın kendisine verilmesi gereken kimsenin rızası olmaksızın, söz konusu kartı kullanarak veya kullandırtarak kendisine ya da bir başkasına çıkar sağlarsa cezalandıracağı yaptırıma bağlanmıştır. İkinci fıkrada ise, başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretmek, satın almak, satmak, devretmek kabul etmek suç olarak kabul edilmiştir. Maddenin üçüncü fıkrasında ise, ikinci fıkradaki eyleme bağlı olarak, yani sahte olarak üretilmiş olan ya da üzerinde sahtecilik yapılan bir kredi kartını kullanmak yoluyla kendisine ya da başkasına yarar sağlamak eylemi yaptırıma bağlanmıştır. Suçun oluşabilmesi için, belirtilen eylemlerden en az birinin

[70] Ekizer, Hakan, (2007), "Yeni TCK'da Bilişim Suçları", http://ekizer.net/index.php?option=com_content&task=view&id=13&Itemid=43, (Erişim Tarihi: 14.10.2010).
[71] Türk Ceza Kanunu Gerekçesi.
[72] Türk Ceza Kanunu Gerekçesi.
[73] Taşdemir, (2009), a.g.e., s.319.

gerçekleştirilmesinin gerekli olduğu anlaşılmaktadır ki bu suç seçimlik hareketli bir suçtur.[74]

Maddede "kendisi veya başkası lehine hukuka aykırı yarar sağlayan kimse" ifadesine yer verilmemiş "kendisine veya başkasına yarar sağlayan kişi" ifadesi kullanılmıştır. Buna göre failin suç oluşturan hareketlerini yaparken bunun neticesinde elde ettiği yararın "hukuka aykırı" olduğunu bilmesi gerekmeyecektir.[75]

Suça teşebbüs mümkün olduğu "banka ve ya kredi kartlarının kötüye kullanılması" suçu seçimlik hareketli bir suç olduğu için maddede geçen eylemlerden birinin yapılması suç işlenmesi için yeterlidir. İştirak açısından özel bir durum gözükmemektedir. Zincirleme işlenebilen bir suç olan 245. maddede "banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse" denilerek uygulama ve içtima sorunları giderilmek istenmiştir. Daha önce bahsettiğimiz 243. madde ve 244. maddede geçen suçlar da bu suçun geçit suçu olabilirler.

1.2.5.4. Bilişim Alanında Suçlarda Tüzel Kişilerin Sorumluluğu (TCK Madde 246)

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

TCK 20. maddeye göre;

(1) Ceza sorumluluğu şahsidir. Kimse başkasının fiilinden dolayı sorumlu tutulamaz.

(2) Tüzel kişiler hakkında ceza yaptırımı uygulanamaz. Ancak, suç dolayısıyla kanunda öngörülen güvenlik tedbiri niteliğindeki yaptırımlar saklıdır.

TCK 20. maddenin gerekçesine göre de "Özel hukuk tüzel kişilerinin suç faili sayılıp sayılmaması ile işlenen bir suçtan dolayı bunlar hakkında bir yaptırıma hükmedilmesi sorununu birbirinden ayırmak gerekir. Suç ve ceza politikası gereği olarak ancak gerçek kişiler suç faili olabilir ve sadece gerçek kişiler hakkında ceza yaptırımına hükmedilebilir. Bu anlaşılış, Anayasamızda da güvence altına alınan ceza sorumluluğunun şahsîliği kuralının bir gereğidir. Ancak, işlenen suç dolayısıyla özel

[74] Taşkın, Şaban Cankat, (2008), *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.75.
[75] Dülger, (2004), a.g.e., s.262.

hukuk tüzel kişileri hakkında güvenlik tedbiri niteliğinde yaptırımlara hükmedilebilecektir."[76]

TCK 60. maddeye göre "faaliyet izninin iptali" ve "müsadere" olmak üzere iki çeşit tüzel kişiler hakkında uygulanacak güvenlik tedbiri öngörülmüştür, bu güvenlik tedbirleri "bilişim alanında suçlar" için de geçerlidir.[77]

1.3. BİLİŞİM YOLUYLA İŞLENEN SUÇLAR

Bilişim yoluyla işlenen suçlar klasik (geleneksel) suçların bilişim yoluyla işlenmesidir. Bir suçun işlenmesinde bilişim teknolojilerinin araç olarak kullanılması neticesinde meydana gelen suçlardır. Toplumsal olaylar, terör ve ideolojik nedenlerle işlenmiş suçlar, ölümlü veya yaralamalı trafik kazaları dâhil trafik suçları ile kaçakçılık ve organize suçlar dışında kalan, teşekkül halinde işlenenler de dâhil olmak üzere kişiler ve/veya mal varlığına karşı işlenen suçlara asayiş suçları denilmektedir.[78] Ülkemizde işlenen suçların büyük bir kısmı asayiş suçları içerisine girmektedir ve bu suçların da hemen hemen hepsi bilişim yoluyla işlenmektedir. Bu suçlara "bilişim yoluyla işlenen asayiş suçları" denilmektedir.[79]

Bilişim yoluyla işlenen asayiş suçlarının gelecekte daha da çoğalması kaçınılmazdır. Günümüzde bilişim yoluyla işlenen asayiş suçlarına bakacak olursak;

- İntihara Yönlendirme (TCK Madde 84)
- Çocukların Cinsel İstismarı (TCK Madde 103)
- Cinsel Taciz (TCK Madde 105)
- Tehdit (TCK Madde 106)
- Şantaj (TCK Madde 107)
- Haberleşmenin Engellenmesi (TCK Madde 124)
- Hakaret (TCK Madde 125/2)
- Haberleşmenin Gizliliğini İhlal (TCK Madde 132)

[76] Türk Ceza Kanunu Gerekçesi.
[77] Karagülmez, (2009), a.g.e., s.230.
[78] Asayiş Dairesi Başkanlığı, (2010), "Asayiş Suçu Kavramı", http://www.asayis.pol.tr/asayis_sucu.asp, (Erişim Tarihi: 28.10.2010).
[79] Asayiş Dairesi Başkanlığı, (2009), "Bilişim Yoluyla İşlenen Asayiş Suçları", Hizmet İçi Sunum.

- Özel Hayatın Gizliliğini İhlal (TCK Madde 134)
- Kişisel Verilerin Kaydedilmesi (TCK Madde 135)
- Verileri Hukuka Aykırı Olarak Verme Veya Ele Geçirme (TCK Madde 136)
- Nitelikli Hırsızlık (TCK Madde 142)
- Nitelikli Dolandırıcılık (TCK Madde-158/1-F)
- Müstehcenlik (TCK Madde 226)
- Fuhuş (TCK Madde 227)
- Kumar Oynanması İçin Yer Ve İmkân Sağlama (TCK Madde 228)

Bilişim yoluyla işlenen asayiş suçları Türk Ceza Kanununda düzenlenmiştir ancak bilişim yoluyla işlenen suçların bazıları başka kanunlarda düzenlenmiştir. Bunlar;

Fikir ve Sanat Eserleri Kanununda Düzenlenen Suçlar;

- Manevi, Mali veya Bağlantılı Haklara Tecavüz (FSEK Madde 71)
- Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri (FSEK Madde 72)

Elektronik İmza Kanununda Düzenlenen Suçlar;

- İmza Oluşturma Verilerinin İzinsiz Kullanımı (EİK Madde 16)
- Elektronik Sertifikalarda Sahtekârlık (EİK Madde 17)

1.3.1. Türk Ceza Kanunu'nda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

1.3.1.1. İntihara Yönlendirme (TCK Madde 84)

(1) Başkasını intihara azmettiren, teşvik eden, başkasının intihar kararını kuvvetlendiren ya da başkasının intiharına herhangi bir şekilde yardım eden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) İntiharın gerçekleşmesi durumunda, kişi dört yıldan on yıla kadar hapis cezası ile cezalandırılır.

(3) Başkalarını intihara alenen teşvik eden kişi, üç yıldan sekiz yıla kadar hapis cezası ile cezalandırılır.

Özellikle internet insanların hiç tanımadıkları insanlarla rahat bir şekilde çok samimimi diyaloglara girebildikleri bir ortamdır. Bu ortamda sağlanan iletişim ile insanları farklı düşünce ve davranışlara yönlendirecek etkileri yapmak mümkündür. Çocuk ve gençler, bilgisayar ve internet kullanırken çok çeşitli riskler ve güvenlik tehditleri ile karşı karşıyadır. Bir ebeveynin ya da eğitimcilerin görevi, çocuğa sadece bilgisayar ve internet gibi ortamları tanıtmak ve bu ortamlara erişimlerini sağlamak olarak tanımlanamaz. Normal olarak bir ebeveynin, kendi çocuğunun kendisi olmadan evin dışında, nerede, kiminle olduğunu bilmesi gerekiyorsa; başıboş ve uçsuz bucaksız bir ortam olarak nitelendirilebilecek İnternette çocukların kontrolsüz bir şekilde bırakılmaması, oldukça tehlikeli sonuçlara maruz kalmamak için gereklidir.[80] Avrupa Birliği'nin "Safer İnternet Plus" programı tarafından desteklenen "eu kids online" projesi nihai raporunun yönetim özeti incelendiğinde de "İnternet ve intihar" önlenmesi gereken bir risk olarak belirtilmiştir.[81] İnternet üzerinden "intihara yönlendirme" suçunun nasıl işlendiğini anlamak için yaşanan örneklere bakmak yeterli olacaktır.

İngiltere'de "Bebo" isimli bir sosyal paylaşım sitesine üye olan yedi gencin bir yıl içinde intihar etmesi, ülkede panik havası yaşatmıştır. On yedi yaşındaki Natasha Randall'ın[82] kendini asmasından bir gün sonra daha önce aynı site üzerinden görüştüğü iki genç daha intihar girişiminde bulunmuştur.[83]

ABD'de çocuklar "net kabadayılığı" (cyberbullying) nedeniyle intihara yönlenmektedirler. Net kabadayılığı günlük hayatta yapılan zorbalıkların internet ortamına taşınmasıdır. Burada hakaret edici mesajlar, resimler ya da küçük düşürücü

[80] Ulusoy, Zebayir, (t.y.), "Bilgisayar Ve İnternetin Çocuklar Üzerindeki Olumsuz Etkileri Ve Alınabilecek Önlemler", http://www.kayram.net/edergi/15/internet.pdf, (Erişim Tarihi: 13.10.2010).
[81] Livingstone, S ve Haddon, L, (2009), "EU Kids Online: Final Report", http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf, (Erişim Tarihi: 11.10.2010).
[82] news.sky.com, (2008), "Bebo Suicide Cult Fears After Seven Deaths Welsh Town Bridgend", http://news.sky.com/skynews/Home/Sky-News-Archive/Article/20080641301942, (Erişim Tarihi: 16.10.2010).
[83] sabah.com.tr, (2008), "Web Tarikatta 7 İntihar, 2 Girişim" http://arsiv.sabah.com.tr/2008/01/24/haber,7E629FA6E6514F50BEAE1A62882138EE.html, (Erişim Tarihi: 16.10.2010).

videolar söz konusu olmaktadır.[84] Yine aynı durum nedeniyle İngiltere'nin Cheltenham kentinde Holly Grogan adlı 15 yaşındaki bir genç kız, kız arkadaşlarının Facebook sayfasına yazdığı kötü sözlere dayanamayıp intihar etmiştir.[85] Bununla birlikte insanların özel görüntülerinin internet ortamında paylaşılması sonucu intihara yönelmelerde mevcuttur.[86] Ülkemizde de görevli bir kurmay albayın eşinin sözde yasak ilişkisinin internet üzerinde yayınlanması nedeniyle intihar ettiğini medyadan takip etmiş bulunuyoruz.[87]

1.3.1.2. Çocukların Cinsel İstismarı (TCK Madde 103)

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

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

b) Diğer çocuklara karşı sadece cebir, tehdit, hile veya iradeyi etkileyen başka bir nedene dayalı olarak gerçekleştirilen cinsel davranışlar, Anlaşılır.

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

(3) Cinsel istismarın üstsoy, ikinci veya üçüncü derecede kan hısmı, üvey baba, evlat edinen, vasi, eğitici, öğretici, bakıcı, sağlık hizmeti veren veya koruma ve gözetim yükümlülüğü bulunan diğer kişiler tarafından ya da hizmet ilişkisinin sağladığı nüfuz kötüye kullanılmak suretiyle veya birden fazla kişi tarafından birlikte gerçekleştirilmesi hâlinde, yukarıdaki fıkralara göre verilecek ceza yarı oranında artırılır.

---

[84] guvenliweb.org.tr , (2009), "Online Bilgiler Geleceğinizi Etkiliyor", http://www.guvenliweb.org.tr/aileler/content/online-bilgiler-gelece%C4%9Finizi-etkiliyor, (Erişim Tarihi: 16.10.2010).

[85] nydailynews.com , (2009), "Parents of Holly Grogan, 15, Blame Facebook For Teen's Suicide", http://www.nydailynews.com/news/world/2009/09/21/2009-09-21_parents_of_holly_grogan_15_blame_facebook_for_teens_suicide.html, (ErişimTarihi: 17.10.2010).

[86] ntvmsnbc.com , (2010), "Facebook'taki fotoğrafları ölüm getirdi", http://www.ntvmsnbc.com/id/25062133, (Erişim Tarihi: 17.10.2010)

[87] ntvmsnbc.com , (t.y.), "Ölüme götüren kareler", http://video.ntvmsnbc.com/olume-goturen-kareler.html, (Erişim Tarihi: 17.10.2010).

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

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

(6) Suçun sonucunda mağdurun beden veya ruh sağlığının bozulması halinde, on beş yıldan az olmamak üzere hapis cezasına hükmolunur.

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

"Çocukların cinsel istismarı" suçunda bilişim teknolojilerinin en çok kullanıldığı alan ne yazık ki çocuk pornografisidir. Avrupa Konseyinin Bilişim Suçları Sözleşmesinde çocuk pornografisi, *"bir küçüğün cinsel olarak kullanılmasını, küçük gibi görünen bir kişinin cinsel olarak kullanılmasını, bir küçüğü temsil eden gerçekçi bir imajın cinsel olarak kullanılmasını görsel olarak içeren pornografik materyaldir."* şeklinde tanımlanmıştır. Bu tanımda geçen "küçük" den kasıt 18 yaşın altındaki herkestir. Taraf devletler buna karşın, 16 yaşından az olmamak üzere daha düşük bir yaş sınırı belirleyebilmektedir. Ayrıca sözleşmenin dokuzuncu maddesinde "Çocuk Pornografisi ile Bağlantılı Suçlar" başlığı altında bu suçla mücadelede sözleşmeye taraf ülkelerin yapması gerekenler sıralamıştır;

"*Her bir Taraf devlet, bir hak olmaksızın kasıtlı;*

a) Bilgisayar sistemi vasıtasıyla dağıtmak amacıyla çocuk pornografisi üretmek,
b) Bilgisayar sistemi vasıtasıyla çocuk pornografisini temin edilebilir hale getirmek veya göstermek,

c) Bilgisayar sistemi vasıtasıyla çocuk pornografisini aktarmak veya dağıtımını yapmak,
d) Kendisi veya başkası için bilgisayar sistemi vasıtasıyla çocuk pornografisi temin etmek,
e) Bir bilgisayar sisteminde veya bilgisayar veri depolama ortamında çocuk pornografisine sahip olmak

Fiillerinden sorumlu tutulması için gerekli kanuni düzenlemeyi yapmalı ve ihtiyaç duyulan önlemleri almalıdır." [88]

Çocuk pornografisi konusunda üzerinde durulması gereken kavram pedofilidir. Pedofili en az altı aylık bir süre boyunca kişide ergenlik dönemine girmemiş bir çocukla ya da çocuklarla cinsel etkinlikte bulunmayla ilgili yoğun, cinsel yönden uyarıcı fantezilerinin, cinsel dürtülerinin ya da davranışlarının yineleyici biçimde ortaya çıkması olarak tanımlanmıştır. Pedofili bireylerin büyük çoğunluğu erkeklerdir. Çocuğun cinsel istismarı sözel istismar, cinsel organlarını gösterme, çocukları soyma ve seyretme, müstehcen yayınlara konu etme, gibi çok çeşitli şekillerde ortaya çıkabilmektedir. Pedofili olgularının eylemlerinde genellikle zor kullanmadığı, aksine önce masum dokunma sonra uygunsuz dokunma, açık resimler gösterme, porno izletme gibi birçok eylem gözlemlenmektedir. Bu bireyler için internet ortamı bilgi edinme, mağduru belirleme ve ilişki kurma, fantezi geliştirme, diğer sapkınlığı olan kişilerle bağlantı kurma gibi birçok istek ve ihtiyaçlarını karşılamak için bir araç olmaya başlamıştır. Pedofilikler, çocuğun cinsel istismarı eylemlerinde çocuk pornosu ya da internet kullananlar ve kullanmayanlar olarak da iki gruba ayrılabilmektedir. İnternet ortamında utanma ve kaygının az olması kişilerin normalde sınırlayacağı diyaloglara veya yaşantılara girmesinin önünü açarak bilmediği kişilerle yakınlık kurmalarına yol açabilmektedir.[89]

"Bilişim yoluyla çocukların cinsel istismarı" suçlarından elde edilen resim ve video gibi dijital delillerde, çocuklarla cinsel ilişki, çocuklara karşı şiddet, çocuklara karşı şiddet ve zorla cinsel ilişki, birden fazla çocuğun birbirleri ile cinsel ilişkisi, cinsel ilişki ve ya şiddet olmadan sadece çocuğun cinsel bölgelerinin gösterilmesi, cinsel bölgeler gösterilmeden sanat amaçlı çekilmiş görüntüler, reşit olan bir şahsın çocuk gibi gösterilmesi, çizgi film ve ya bilgisayar animasyonları ile üretilmiş çocuk görüntüleri ile karşılaşılmaktadır.[90]

Teknolojik gelişmeler ve özellikle internetin bu denli yaygınlaşması, çocuk pornografisi ticaretine küresel bir kimlik kazandırmış olup, akıl almaz bir hızla

[88] Avrupa Konseyi, (2001), "Convention on Cybercrime", http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm, (Erişim Tarihi: 17.10.2010).
[89] Erdoğan, Ayten, (2010), "Pedofili: Klinik Özellikleri, Nedenleri ve Tedavisi", http://www.cappsy.org/archives/vol2/no2/cap_02_08.pdf, (Erişim Tarihi: 19.10.2010).
[90] Dokurer, Semih, (t.y.), "Bilişim Suçları Laboratuarlarında Çocuk Pornografisi İncelemeleri", http://www.dokurer.net/files/documents/ChildpornExamining.pdf, (Erişim Tarihi: 19.10.2010).

gelişmesine neden olmuştur. Son yıllarda çocuk pornografisi, ticaret anlamında da dengeleri değiştirmiş ve pazarda en çok eğilim gösterilen sanayilerden biri olarak yerini almıştır. Mücadele bağlamında birçok sıkıntı ile karşılaşılmaktadır. Temel olarak bilişim suçlarında yaşanan sıkıntılar, çocuk pornografisi için de geçerli olup, ek olarak psikolojik, toplumsal ve sosyal anlamda da sıkıntılar bulunmaktadır. Özellikle işin içerisinde insan faktörünün bulunması ve çocukları kapsaması açısından da mücadele, ayrı bir hassasiyet ve önem kazanmaktadır.[91]

1.3.1.3. Cinsel Taciz (TCK Madde 105)

(1) Bir kimseyi cinsel amaçlı olarak taciz eden kişi hakkında, mağdurun şikâyeti üzerine, üç aydan iki yıla kadar hapis cezasına veya adlî para cezasına hükmolunur.

(2) Bu fiiller; hiyerarşi, hizmet veya eğitim ve öğretim ilişkisinden ya da aile içi ilişkiden kaynaklanan nüfuz kötüye kullanılmak suretiyle ya da aynı işyerinde çalışmanın sağladığı kolaylıktan yararlanılarak işlendiği takdirde, yukarıdaki fıkraya göre verilecek ceza yarı oranında artırılır. Bu fiil nedeniyle mağdur; işi bırakmak, okuldan veya ailesinden ayrılmak zorunda kalmış ise, verilecek ceza bir yıldan az olamaz.

"Cinsel taciz" suçunun bilişim yoluyla en çok işlenen türü sözlü cinsel tacizdir. Sözlü cinsel taciz; hoş olmayan ve süreklilik arz eden kur yapmalar, istenmeyen aşırı özel ilgi, müstehcen imalı sözler veya şakalar, giyime ve görünüme yönelik cinsel içerikli sözler, cinsel isteklerini dile getiren konuşmalar, iş yeri dışında sosyal faaliyetle ilgili devamlı ve ısrarlı önerilerde bulunma, terfi karşılığında cinsel birliktelik teklifleri, açıkça cinsel talepte bulunma şeklinde gerçekleşmektedir.[92]

Bu eylemlerin büyük çoğunluğu internet üzerinden iletişim esnasında yapılmakla birlikte cep telefonlarından kısa mesaj göndermek suretiyle de yapılmaktadır.[93] İnternet üzerinden e-posta ile sohbet (chat) ile anında mesajlaşma[94]

---

[91] Uzunay, Yusuf ve Koçak Mustafa, (2005), "İnternet Üzerinden Çocuk Pornografisi Ve Mücadelede Yaşanan Sıkıntılar", http://nash.ii.metu.edu.tr/~yuzunay/Download/jop05.pdf, (Erişim Tarihi: 20.10.2010).

[92] Karayel, Ayhan, (2006), *Retrospektif Bir Çalışma: 2001-2005 Yılları Arasında Adana İl Emniyet Müdürlüğüne Yansıyan Cinsel Taciz Vakalarının İncelenmesi*, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Adana, s.6.

[93] cnnturk.com , (2010), "Cumhuriyet Savcısı Gök'e Cinsel Taciz'den Ceza", http://www.cnnturk.com/2010/turkiye/10/26/cumhuriyet.savcisi.goke.cinsel.tacizden.ceza/594377.0/index.html, (Erişim Tarihi: 22.10.2010).

ile internet sayfalarındaki içerikler ve tartışma forumları aracılığıyla bu eylemler gerçekleştirilmektedir.

1.3.1.4. Tehdit (TCK Madde 106)

(1) Bir başkasını, kendisinin veya yakınının hayatına, vücut veya cinsel dokunulmazlığına yönelik bir saldırı gerçekleştireceğinden bahisle tehdit eden kişi, altı aydan iki yıla kadar hapis cezası ile cezalandırılır. Malvarlığı itibarıyla büyük bir zarara uğratacağından veya sair bir kötülük edeceğinden bahisle tehditte ise, mağdurun şikâyeti üzerine, altı aya kadar hapis veya adlî para cezasına hükmolunur.

(2) Tehdidin;

a) Silahla,

b) Kişinin kendisini tanınmayacak bir hale koyması suretiyle, imzasız mektupla veya özel işaretlerle,

c) Birden fazla kişi tarafından birlikte,

d) Var olan veya var sayılan suç örgütlerinin oluşturdukları korkutucu güçten yararlanılarak,

İşlenmesi halinde, fail hakkında iki yıldan beş yıla kadar hapis cezasına hükmolunur.

(3) Tehdit amacıyla kasten öldürme, kasten yaralama veya malvarlığına zarar verme suçunun işlenmesi halinde, ayrıca bu suçlardan dolayı ceza verilir.

"Bilişim yoluyla tehdit" suçundan bahsederken günümüzde en çok kullanılan aracın internet olduğunu görüyoruz.[95] Bu amaçla internet unsurlarından en çok e-postalar ve anından mesajlaşma programlarının kullanıldığını görmekteyiz.[96]

---

[94] Anında mesajlaşma, bir bilgisayar programı sayesinde, üye olarak, listenize eklediğiniz kişilerle gerçek zamanlı görüşme olanağıdır. Program özelliğine bağlı olarak görüntülü ve sesli görüşme olanağı da olabilir.En bilinen anında mesajlaşma programları MSN Messenger, Pidgin, Kopete, ICQ, Yahoo Messenger ve Google Talk'dır. Aslında anında mesajlaşmanın geçmişi İnternetten önceye dayanır. Anında mesajlaşma ilk olarak CTSS ve Multics gibi işletim sistemlerinde görülmüştür. Günümüzde ise bazı anında mesajlaşma yazılımları video konferans, Voice Over IP özelliği de sunmaya başladı. (Wikipedia.org).

[95] Gökçen, Ahmet, (t.y.), "E-Posta, MSN Messenger İle Tehdit Edilirsek Veya Hakarete Uğrarsak Ne Yapabiliriz?", http://www.uzmantv.com/eposta-msn-messenger-ile-tehdit-edilirsek-veya-hakarete-ugrarsak-ne-yapabiliriz, (Erişim Tarihi: 22.10.2010).

[96] turkhukuksitesi.com, (2007), "İnternet Üzerinden E-Posta Ve MSN Yoluyla Tehdit Suçu İşlenmesi", http://www.turkhukuksitesi.com/showthread.php?t=11094, (Erişim Tarihi: 23.10.2010).

1.3.1.5. Şantaj (TCK Madde 107)

(1) Hakkı olan veya yükümlü olduğu bir şeyi yapacağından veya yapmayacağından bahisle, bir kimseyi kanuna aykırı veya yükümlü olmadığı bir şeyi yapmaya veya yapmamaya ya da haksız çıkar sağlamaya zorlayan kişi, bir yıldan üç yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.

(2) Kendisine veya başkasına yarar sağlamak maksadıyla bir kişinin şeref veya saygınlığına zarar verecek nitelikteki hususların açıklanacağı veya isnat edileceği tehdidinde bulunulması halinde de birinci fıkraya göre cezaya hükmolunur.

"Şantaj" suçunun bilişim yoluyla işlenmesinde iki yöntemin kullanıldığını görüyoruz, birincisi şantaj yapmak amacıyla özel bilgilerin ve ya görüntülerin bilişim teknolojileri kullanılarak elde edilmesi ikincisi ise şantaj amaçlı kullanılacak materyallerin İnternet ortamı kullanılarak yayınlanmasıdır.[97] Burada şantaj eylemlerinde kullanılan içeriklerde özellikle müstehcen görüntüler sıklıkla kullanılmaktadır.[98]

1.3.1.6. Haberleşmenin Engellenmesi (TCK Madde 124)

(1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi halinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi halinde, ikinci fıkra hükmüne göre cezaya hükmolunur.

Maddenin gerekçesine bakıldığında; "bu suçun konusu, belirli kişiler arasındaki haberleşmedir, haberleşmenin yapıldığı araç önemli değildir" denilmektedir.[99] Günümüzde en çok kullanılan haberleşme araçları ise İnternet ve mobil iletişimdir yani cep telefonlarıdır.[100] Bilişim yoluyla haberleşmenin engellenmesi bazen geçici olarak bu

[97] ntvmsnbc.com , (2010), "Pornoyla Şantaj!", http://www.ntvmsnbc.com/id/25082652/ , (Erişim Tarihi: 23.10.2010).
[98] haberturk.com, (2010), "İnternette Şantaj İddiası", http://www.haberturk.com/yasam/haber/532319-İnternette-santaj-iddiasi, (Erişim Tarihi: 24.10.2010).
[99] Türk Ceza Kanunu Gerekçesi
[100] guvenliweb.org.tr , (2009), "Mobil İletişim ve İnternet", http://www.guvenliweb.org.tr/guvenlik/content/mobil-ileti%C5%9Fim-ve-internet, (Erişim Tarihi: 24.10.2010).

iletişim araçlarının devre dışı bırakılması ve ya kalıcı olarak iletişim sisteminin işleyişini engelleme şeklinde karşımıza çıkmaktadır.

Özellikle son yıllarda "sinyal boğucu" (sinyal karıştırıcı, sinyal bozucu, jammer) denilen aletlerle kanuna aykırı olarak haberleşmenin engellenmesi sağlanmaktadır. Bazı durumlarda güvenlik amaçlı (uzaktan bomba patlatılmasını engellemek gibi) olarak hukuka uygun bir biçimde kullanılan bu cihazlar üçüncü kişilerin iletişiminin engellenmesine sebep olabilmektedir.[101]

1.3.1.7. Hakaret (TCK Madde 125)

(1) Bir kimseye onur, şeref ve saygınlığını rencide edebilecek nitelikte somut bir fiil veya olgu isnat eden veya sövmek suretiyle bir kimsenin onur, şeref ve saygınlığına saldıran kişi, üç aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Mağdurun gıyabında hakaretin cezalandırılabilmesi için fiilin en az üç kişiyle ihtilat ederek işlenmesi gerekir.

(2) Fiilin, mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde, yukarıdaki fıkrada belirtilen cezaya hükmolunur.

(3) Hakaret suçunun;

a) Kamu görevlisine karşı görevinden dolayı,

b) Dini, siyasi, sosyal, felsefi inanç, düşünce ve kanaatlerini açıklamasından, değiştirmesinden, yaymaya çalışmasından, mensup olduğu dinin emir ve yasaklarına uygun davranmasından dolayı,

c) Kişinin mensup bulunduğu dine göre kutsal sayılan değerlerden bahisle,

İşlenmesi halinde, cezanın alt sınırı bir yıldan az olamaz.

(4) Hakaretin alenen işlenmesi halinde ceza altıda biri oranında artırılır.

(5)Kurul hâlinde çalışan kamu görevlilerine görevlerinden dolayı hakaret edilmesi hâlinde suç, kurulu oluşturan üyelere karşı işlenmiş sayılır. Ancak, bu durumda zincirleme suça ilişkin madde hükümleri uygulanır.

[101] ntvmsnbc.com , (2008), "Sinyal Boğuculara Yasal Düzenleme Geliyor", http://www.ntvmsnbc.com/id/24934116, (Erişim Tarihi: 24.10.2010).

Maddenin gerekçesine göre, "kişiyi muhatap alan mektup, telgraf, telefon ve benzeri araçlarla yapılan hakaret de, huzurda hakaret olarak cezalandırılmalıdır" denilmektedir.[102] O halde başta İnternet olmak üzere diğer bilişim teknolojileri kullanılarak da kişilere hakaret edilebilmektedir.

İnternet marifetiyle hakaret e-posta, sohbet ve ya anında mesajlaşma ile kişiler arasında olabildiği gibi internet sayfaları üzerinden alenen de işlenebilmektedir. Nitekim dördüncü fıkraya göre de bu durum ağırlaştırıcı sebep olarak karşımıza çıkmaktadır. Son yıllarda giderek yaygınlaşan kişilerin, sosyal gruplar kurarak, her türlü yazılı, görsel paylaşım yapabileceği sosyal ağlar[103] aracılığı ile de hakaret suçu sözlü ve görsel olarak işlenebilmektedir.[104]

1.3.1.8. Haberleşmenin Gizliliğini İhlal (TCK Madde 132)

(1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması halinde, ceza yarı oranında artırılır.

Daha önce bahsettiğimiz şantaj suçunda olduğu gibi "haberleşmenin gizliliğini ihlal" suçunda da bilişim teknolojileri hem haberleşmenin içeriğini ele geçirmek amacıyla kullanılmakta hem de ele geçirilen içeriğin üçüncü kişilerle paylaşımında kullanılmaktadır. Ele geçirilen haberleşmenin kaynağı bazen yüz yüze yapılan konuşmalar olduğu gibi bazen de İnternet ortamı ve cep telefonları ile

[102] Türk Ceza Kanunu Gerekçesi.
[103] milliyet.com.tr , (2009), "Sosyal Ağ Nedir?",
http://blog.milliyet.com.tr/Blog.aspx?BlogNo=197465, (Erişim Tarihi: 25.10.2010).
[104] ntvmsnbc.com , (2010), "Facebook'ta Hakarete İlanlı Özür",
http://www.ntvmsnbc.com/id/25086314/ (Erişim Tarihi: 25.10.2010).

yapılan görüşmeler de olabilmektedir. Ülkemizde farklı konum ve seviyedeki devlet görevlilerinin de haberleşmeleri kanuna aykırı olarak ele geçirilip kamuoyu ile paylaşıldığı vakalara rastlanılmaktadır.[105]

1.3.1.9. Kişiler Arasındaki Konuşmaların Dinlenmesi ve Kayda Alınması (TCK Madde 133)

(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.

(2)Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adlî para cezası ile cezalandırılır.

(3)Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması halinde de, aynı cezaya hükmolunur.

Bu suçun bilişim teknolojiler kullanılarak en çok karşımıza çıkan formu uygulamada "ortam dinlemesi" olarak adlandırılan eylemdir. Ortam dinleme belli bir ortamdaki konuşmaların dinlenmesi ve hatta kayda alınmasıdır.[106] Bunun için spesifik üretilmiş bilişim cihazları kullanılabildiği gibi son günlerde bilgisayarlar ve cep telefonlarına yüklenen casus programlar vasıtasıyla da bu işlem gerçekleştirilebilmektedir.[107]

[105] haberaktuel.com , (2008), "Bir Savcının Gizli Ses Kaydı Youtube'da Teşhir Edildi", http://www.haberaktuel.com/bir-savcinin-gizli-ses-kaydi-youtubeda-teshir-edildi-haberi-115365.html, (Erişim Tarihi: 25.10.2010).
[106] zaman.com.tr , (2009), "Telefonunuzdan Ortam Dinlemesi Yapılıyor Olabilir!", http://www.zaman.com.tr/haber.do?haberno=833402, (Erişim Tarihi: 26.10.2010).
[107] Öztürkçi, Halil, (2009),"İphone'unuz Sizi Ele Veriyor", Ankara Bilgi Güvenliği Konferansı, 24 Aralık 2009, Ankara.

1.3.1.10. Özel Hayatın Gizliliğini İhlal (TCK Madde 134)

(1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, cezanın alt sınırı bir yıldan az olamaz.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi halinde, ceza yarı oranında artırılır.

"Özel hayatın gizliliğini ihlal" suçunda hem birinci fıkrada hem de ikinci fıkrada tanımlanan eylemler bilişim teknolojileri kullanılarak yapılabilmektedir. İnternet üzerinde kurulan sosyal ağlar ve paylaşım siteleri aracılığıyla bilgi paylaşımının yaygınlaşması, beraberinde özel hayatın gizliliği ilkesinin zedelenmesi ve bireyler doğrudan ya da dolaylı olarak zarar görmesi sorununu doğurmuştur.[108] İnternet aracılığıyla özel hayatın gizliliğinin ihlaline yönelik müdahale çeşitlerinden bazıları; elektronik postalar ile, bilişim korsanlığı faaliyetleri ile, intermet sayfalarındaki yayınlar ile ve kişisel verilerin toplanması ve rıza dışında kullanımı ile gerçekleştirilmektedir. [109]

1.3.1.11. Kişisel Verilerin Kaydedilmesi (TCK Madde 135)

(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.

Maddenin gerekçesinde; "Söz konusu suç tanımında kişisel verilerin bilgisayar ortamında veya kağıt üzerinde kayda alınması arasında bir ayırım gözetilmemiştir. Bu bakımdan, söz konusu suç tanımı ile Avrupa Konseyi bünyesinde hazırlanan Türkiye'nin de 28 Ocak 1981 tarihinde imzalamakla taraf olduğu "Kişisel Nitelikteki Verilerin

---

[108] stratejikboyut.com , (t.y.), "İnternet, Özel Hayatın Gizliliği Ve Hukuki Boşluklar", http://www.stratejikboyut.com/haber/İnternet,-ozel-hayatin-gizliligi-ve-hukuki-bosluklar--28234.html, (Erişim Tarihi: 26.10.2010).

[109] Kahraman, Ezgi, (2009), *Özel Hayatın Gizliliği*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.70.

Otomatik İşleme Tâbi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme"nin ilgili hükümlerine geçerlilik tanınmıştır" denilmektedir.[110] İnternet yoluyla yapılan kişilik hakları ihlalleri arasında en geniş kapsamlı olanı, kişisel veriler bağlamında karşımıza çıkmaktadır. Esasen başta bankacılık olmak üzere pek çok alanda işlemleri hızlandırmak ve güvenilir kılmak amacıyla kişisel verilerin toplanması ve ilgililerin yararlanmasına sunulması bir zorunluluktur. Ancak toplanan verilerin korunması, bu verilerden yararlanılarak kişilerin özel hayat alanına tecavüz yapılmasının engellenmesi ve kişilik hakları ihlallerinin önlenmesi gerekir.[111]

İnternet'in yaygınlaşması ve yaygınlaşan bu araç sayesinde kişilerle ilgili bilgilerin yaygınlaşması ve erişimin çok kolaylaşması bu verilerin hukuka aykırı olarak yetkisiz ve çoğu durumda kötü niyetli kişilerin eline geçmesine neden olmaya başlamıştır.[112] Devlet – birey ilişkileri açısından özel hayatın gizliliği, devletin niteliğine ilişkin önemli bir göstergedir. Özel hayatın olmadığı ya da aşırı sınırlandırıldığı bir devletin demokratik olduğu söylenemez. Bu açıdan, modern toplumlarda özel hayatın gizliliği ya da genel olarak özgürlükler çok da yeni olmayan fakat boyutları değişen bir tehditle karşı karşıyadır. Temel hak ve özgürlüklerin korunması önemi bir yana kamusal ve özel faaliyetlerin sürdürülebilmesi açısından kişisel verilere de ihtiyaç var. Bu kapsamda belirli şartlar altında kamu ve özel sektörde kişisel verilerin işlenmesine izin verilmesi kaçınılmaz olmaktadır. Kişisel verilerin işlenmesine izin verildiğinde makul beklenti özellikle devletin bu tür verilerin güvenliğini sağlaması yolundadır.[113]

1.3.1.12. Verileri Hukuka Aykırı Olarak Verne veya Ele Geçirme (TCK Madde 136)

(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Maddenin gerekçesine bakıldığında "madde hükmü ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına

[110] Türk Ceza Kanunu Gerekçesi
[111] Tiftikçi, Mehmet, (1999), "Özel Hukuk Ve İnternet", http://inet-tr.org.tr/inetconf5/tammetin/hukuk.html, (Erişim Tarihi: 27.10.2010).
[112] Sırabaşı, Volkan, (t.y.), "Kişisel Verilerin Gizliliği", http://www.fenafil.com/hukuk/İnternet/kisisel_veriler.htm, (Erişim Tarihi: 27.10.2010).
[113] Ketizmen, Muammer ve Ülküderner, Çağlar, (t.y.), "E-Devlet Uygulamalarında Kişisel Verilerin Korun(ma)ması", http://inet-tr.org.tr/inetconf12/bildiri/2.pdf, (Erişim Tarihi:27.10.2010).

vermek, yaymak veya ele geçirmek, bağımsız bir suç olarak tanımlanmıştır" denilmektedir. Burada dikkat edilmesi gereken nokta hukuka uygun olarak kaydedilmiş olan kişisel verileri hukuka aykırı olarak verme ve ya ele geçirme suç olarak tanımlanmıştır. Aslında uygulamada en çok da karşılaşın durum budur. Özellikle dünyada birçok İnternet kullanıcısının ziyaret ettiği ve ücretsiz hizmetlerinden yararlandığı internet sayfalarının sahibi olan uluslar arası şirketlerin ziyaretçi bilgilerini reklam şirketleri[114] ve istihbarat birimleriyle paylaştığı iddia edilmektedir.[115] Bununla birlikte devlet tarafından tutulan başta Türkiye Cumhuriyeti kimlik numarası ve bilgileri gibi kişisel veriler de zaman zaman suçluların eline geçmektedir.[116]

1.3.1.13. Nitelikli Hırsızlık (TCK Madde 142/2 e)

(2)Suçun

e) Bilişim sistemlerinin kullanılması suretiyle

Her ne kadar bentte, "bilişim sistemlerinin" kullanılarak hırsızlık suçunun işlenmesi, bu suçun nitelikli hali olarak kabul edilmiş ise de; bilişim sistemleri kullanılmak suretiyle haksız bir yarar elde edilmesi durumunda daha çok dolandırıcılık veya diğer bilişim suçları gündeme gelebilir ise de; hırsızlık suçunun oluşması çoğu durumda mümkün gözükmediği için, hükmün uygulama alanı oldukça sınırlı gözükmektedir.[117]

Her ne kadar bilişim sistemleri kullanılarak hırsızlık suçunun işlenmesinin çoğu durumda mümkün olmadığı kabul edilmekte ise de bir bilişim sistemi kullanılarak taşınır malların çalınmasını sağlamak da mümkündür. Örnek vermek gerekirse bir binanın güvenlik sisteminin bir bilişim sistemine bağlı olması durumunda bu sisteme girilmek suretiyle güvenlik sisteminin devre dışı

[114] hurriyet.com.tr , (2009), "Facebook Kişisel Bilgileri Satacak", http://www.hurriyet.com.tr/teknoloji/10944027.asp, (Erişim Tarihi: 28.10.2010).
[115] turkhukuksitesi.com , (2010), "Google'ın Amerikan İstihbarat Örgütü National Security Agency İle İlişkisi", http://www.turkhukuksitesi.com/showthread.php?t=47116, (Erişim Tarihi: 28.10.2010).
[116] cnnturk.com , (2010), "70 Milyonun Kimlik Bilgilerini Ele Geçirdiler", http://www.cnnturk.com/2010/turkiye/07/27/70.milyonun.kimlik.bilgilerini.ele.gecirdiler/584821.0/index.html, (Erişim Tarihi: 28.10.2010).
[117] Erdem, M. Ruhan, (t.y.), "Yeni Türk Ceza Kanunu'nda Malvarlığına Karşı Suçlar", http://www.ceza-bb.adalet.gov.tr/makale/119.doc, (Erişim Tarihi: 28.10.2010).

bırakılmasından yararlanılarak binadaki taşınır malların çalınması durumunda bu bent uygulama alanı bulacaktır.[118]

1.3.1.14. Nitelikli Dolandırıcılık (TCK Madde 158/1 f)

(1) Dolandırıcılık suçunun;

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

Dolandırıcılık eylemlerine hemen her ülkede ve her kültürde rastlamak mümkündür. Ancak, son yıllarda özellikle bilişim sektöründeki gelişmeler nedeniyle dolandırıcılık eylemleri teknolojik yöntemlerin kullanıldığı daha karmaşık bir yapı haline gelmiştir. Dolandırıcılık amacıyla kurulan çete ve şebekeler ise daha organize halde çalışmaktadır. Dolandırıcıların veya dolandırıcılık amacıyla kurulmuş olan çetelerin hedefinde "şahıslar" olduğu gibi kurumlar da yer almaktadır. Bankacılık, dolandırıcılık eylemlerine en çok hedef olan sektörlerin başında gelmektedir. Bankalar, teknolojik altyapılarının kurulmasında ve bankacılık işlemlerinin gerçekleştirilmesinde güvenliğe son derece önem vermektedirler. Dolandırıcılık girişimleri ortak noktası, ele geçirilmek istenen değerin nakit para olmasıdır. Eylem girişimi, İnternette müşterilerin bilgilerinin casus yazılımlarla ele geçirilmesi ve ele geçirilen tutarın banka şubeleri veya otomatik para ödeme makineleri (ATM) yoluyla banka dışına çıkartılmasıdır.[119]

Bilişim yoluyla nitelikli dolandırıcılığın en yaygın görünüm şekli olan interaktif dolandırıcılık istatistiklere bakıldığında ülkemizde hızla artmaktadır. Bu artış teknolojik gelişmelere paralellik göstermekte ve bunu önlemede ne kadar güvenlik tedbiri alınırsa alınsın teknolojinin getirdiği avantajlar suçluların işlerini ve saklanabilmesini kolaylaştırmaktadır.[120]

---

[118] Sayar, Filiz, (2008), *Hırsızlık Suçu ve Yeni Türk Ceza Kanunu*, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İzmir, s.101.
[119] Ergüç, Seher, (2008), *Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar Ve Bilişim Suçları Hukuku*, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.4.
[120] Gürçam, Ufuk, (2008), *İnteraktif Dolandırıcılık*, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Eskişehir, s.147.

1.3.1.15. Müstehcenlik (TCK Madde 226)

(1) a) Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,

b) Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,

c) Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,

d) Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,

e) Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,

f) Bu ürünlerin reklamını yapan,

Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Müstehcen görüntü, yazı veya sözleri basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden kişi altı aydan üç yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

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

(4) Şiddet kullanılarak, hayvanlarla, ölmüş insan bedeni üzerinde veya doğal olmayan yoldan yapılan cinsel davranışlara ilişkin yazı, ses veya görüntüleri içeren ürünleri üreten, ülkeye sokan, satışa arz eden, satan, nakleden, depolayan, başkalarının kullanımına sunan veya bulunduran kişi, bir yıldan dört yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır.

(5) Üç ve dördüncü fıkralardaki ürünlerin içeriğini basın ve yayın yolu ile yayınlayan veya yayınlanmasına aracılık eden ya da çocukların görmesini,

dinlemesini veya okumasını sağlayan kişi, altı yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.

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

(7) Bu madde hükümleri, bilimsel eserlerle; üçüncü fıkra hariç olmak ve çocuklara ulaşması engellenmek koşuluyla, sanatsal ve edebi değeri olan eserler hakkında uygulanmaz.

İnternet müstehcenlik için sıklıkla kullanılan bir ortamdır. Bu konudaki istatistiklere bakıldığında internet kullanıcılarının ciddi bir kısmı yaklaşık %42 si interneti müstehcen içerikli görüntülere ulaşmak için kullanmaktadır. 2006 yılında yapılan bir araştırmaya göre internetteki internet sitelerinin %12 si yaklaşık 4.2 milyonu müstehcen içeriklidir ve internette bir sektör haline gelen bu alanın mali boyutu yaklaşık 4.9 milyar dolardır ve Microsoft, Google, Amazon, eBay, Yahoo, Apple, Netflix gibi bilişim dünyasının devleriyle yarışacak seviyededir.[121]

Ülkemizde de İnternet müstehcenlik suçunu tanımlayan eylemler için kullanılmaktadır. Mahkeme kararıyla Telekomünikasyon İletişim Başkanlığı tarafından erişimi engellenen sitelerin %69.3'ü müstehcenlik yüzünden engellenmiştir.[122]

1.3.1.16. Fuhuş (TCK Madde 227)

(1) Çocuğu fuhşa teşvik eden, bunun yolunu kolaylaştıran, bu maksatla tedarik eden veya barındıran ya da çocuğun fuhşuna aracılık eden kişi, dört yıldan on yıla kadar hapis ve beş bin güne kadar adlî para cezası ile cezalandırılır. Bu suçun işlenişine yönelik hazırlık hareketleri de tamamlanmış suç gibi cezalandırılır.

(2) Bir kimseyi fuhşa teşvik eden, bunun yolunu kolaylaştıran ya da fuhuş için aracılık eden veya yer temin eden kişi, iki yıldan dört yıla kadar hapis ve üçbin güne

[121] toptenreviews.com , (t.y.), "İnternet Pornography Statistics", http://İnternet-filter-review.toptenreviews.com/İnternet-pornography-statistics.html, (Erişim Tarihi: 29.10.2010).
[122] Telekomünikasyon İletişim Başkanlığı, (2010), "Erişim Engelleme İstatistikleri", http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010.pdf, (Erişim Tarihi: 29.10.2010).

kadar adlî para cezası ile cezalandırılır. Fuhşa sürüklenen kişinin kazancından yararlanılarak kısmen veya tamamen geçimin sağlanması, fuhşa teşvik sayılır.

(3) (Mülga)

(4) Cebir veya tehdit kullanarak, hile ile ya da çaresizliğinden yararlanarak bir kimseyi fuhşa sevk eden veya fuhuş yapmasını sağlayan kişi hakkında yukarıdaki fıkralara göre verilecek ceza yarısından iki katına kadar artırılır.

(5) Yukarıdaki fıkralarda tanımlanan suçların eş, üstsoy, kayın üstsoy, kardeş, evlat edinen, vasi, eğitici, öğretici, bakıcı, koruma ve gözetim yükümlülüğü bulunan diğer kişiler tarafından ya da kamu görevi veya hizmet ilişkisinin sağladığı nüfuz kötüye kullanılmak suretiyle işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(6) Bu suçların, suç işlemek amacıyla teşkil edilmiş örgüt faaliyeti çerçevesinde işlenmesi halinde, yukarıdaki fıkralara göre verilecek ceza yarı oranında artırılır.

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

(8) Fuhşa sürüklenen kişi, tedaviye veya psikolojik terapiye tâbi tutulabilir.

Fuhuş suçunu düzenleyen Türk Ceza Kanunu'nun 227. maddesinin birinci, ikinci ve dördüncü fıkrasında belirtilen eylemler bilişim teknolojileri kullanılarak işlenmektedir. Özellikle İnternet fuhşa ortam sağlanması teşvik ve aracılık için kullanılmaktadır. "Eskort, partner" gibi isimlerle kategorilere ayrılan intermet sayfaları aracılığıyla organize olarak fuhuş hizmeti pazarlanmaktadır.[123] Ayrıca para karşılığı ilişkiye girmek için müşteri arayanlar da interneti kullanmaktadırlar.[124] İnternet üzerinden "şantaj" suçunun işlendiğinden bahsetmiştik. Bazı durumlarda bu şantaj eylemi karşıdaki kişiyi fuhşa zorlamaya kadar gitmektedir. Önce müstehcen görüntüleri çekilen kişiler bununla şantaj yapılarak fuhşa zorlanmaktadır.[125]

[123] .radikal.com.tr , (2010), "Sanal Fuhuş Tuzaklarla Dolu" http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetay&ArticleID=1025020&Date=23.10.2010&CategoryID=117, (Erişim Tarihi: 29.10.2010).
[124] memurlar.net , (2005), "Fuhuş Yapan TRT Spikeri Fantezi Kurbanı", http://www.memurlar.net/haber/27191, (Erişim Tarihi: 29.10.2010).
[125] cnnturk.com, (2008), "Eskişehir'de İnternetten Şantaj İddiası", http://www.cnnturk.com/2008/yasam/diger/03/07/eskisehirde.İnternetten.santaj.iddiasi/435622.0/index.html, (Erişim Tarihi: 29.10.2010).

1.3.1.17. Kumar Oynanması İçin Yer ve İmkân Sağlama (TCK Madde 228)

(1) Kumar oynanması için yer ve imkân sağlayan kişi, bir yıla kadar hapis ve adlî para cezası ile cezalandırılır.

(2) Çocukların kumar oynaması için yer ve imkân sağlanması halinde, verilecek ceza bir katı oranında artırılır.

(3) Bu suçtan dolayı, tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

(4) Ceza Kanununun uygulanmasında kumar, kazanç amacıyla icra edilen ve kar ve zararın talihe bağlı olduğu oyunlardır.

Maddenin dördüncü fıkrasında tanımlanan kumar oynamak eylemi Türk Ceza Kanunu'na göre suç sayılmamaktadır ancak Kabahatler Kanunu'nun 34. maddesinde düzenlenmiş ve idari para cezası ile cezalandırılmıştır. Kumar oynanması için yer ve imkân sağlanmasında internet çok müsait bir ortamdır. Özellikle ülke dışındaki yer sağlayıcılar üzerinden yayınlanan internet sayfaları aracılığıyla kumar oynanmaktadır. Hem kumar oynayanlar hem de oynatanlar için gizlilik açısından internet en müsait ortam haline gelmiştir.[126]

1.3.1.18. Diğer Suçlar

Türk Ceza Kanunu'nda bilişim yoluyla işlenen suçlardan bahsederken uygulamada en çok karşılaşılan ve bugün için mümkün görünenlerden bahsettik. Ancak bunların dışında "uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (190), halk arasında korku ve panik yaratmak amacıyla tehdit (213), suç işlemeye tahrik (214), suçu ve suçluyu övme (215), halkı kin ve düşmanlığa tahrik veya aşağılama(216), kanunlara uymamaya tahrik (217), suç işlemek amacıyla örgüt kurma (220), göreve ilişkin sırrın açıklanması (258), iftira (267), gizliliğin ihlali (285), cumhurbaşkanına hakaret (299), devletin egemenlik alametlerini aşağılama (299), Türk milletini, Türkiye cumhuriyeti devletini, devletin kurum ve organlarını aşağılama (301) Halkı askerlikten soğutma (318) gibi suçlar da bilişim yoluyla işlenebilmektedir.[127]

---

[126] ntvmsnbc.com, (2008), "İnternette Kumara İki Yıl Sonra Ceza Geldi", http://arsiv.ntvmsnbc.com/news/434195.asp, (Erişim Tarihi: 29.10.2010).
[127] Çekiç, Burak, (2006), *İnternet Aracılığıyla İşlenen Suçlar*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, ss.205-209.

1.3.2. Fikir ve Sanat Eserleri Kanunu'nda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

Fikir ve Sanat Eserleri Kanunu'nun ikinci maddesinde "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," ifadesi ile bilgisayar programlarını ilim ve edebiyat eserli arasında tanımlamıştır. Ayrıca kanunun altıncı maddesinde "bir bilgisayar programının uyarlanması, düzenlenmesi veya herhangi bir değişim yapılması;" da eser olarak kabul edilmiştir.

1.3.2.1. Manevi, Mali veya Bağlantılı Haklara Tecavüz (FSEK Madde 71)

(1)Bu Kanunda koruma altına alınan fikir ve sanat eserleriyle ilgili manevi, mali veya bağlantılı hakları ihlal ederek:

1. Bir eseri, icrayı, fonogramı veya yapımı hak sahibi kişilerin yazılı izni olmaksızın işleyen, temsil eden, çoğaltan, değiştiren, dağıtan, her türlü işaret, ses veya görüntü nakline yarayan araçlarla umuma ileten, yayımlayan ya da hukuka aykırı olarak işlenen veya çoğaltılan eserleri satışa arz eden, satan, kiralamak veya ödünç vermek suretiyle ya da sair şekilde yayan, ticarî amaçla satın alan, ithal veya ihraç eden, kişisel kullanım amacı dışında elinde bulunduran ya da depolayan kişi hakkında bir yıldan beş yıla kadar hapis veya adlî para cezasına hükmolunur.

2. Başkasına ait esere, kendi eseri olarak ad koyan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır. Bu fiilin dağıtmak veya yayımlamak suretiyle işlenmesi hâlinde, hapis cezasının üst sınırı beş yıl olup, adlî para cezasına hükmolunamaz.

3. Bir eserden kaynak göstermeksizin iktibasta bulunan kişi altı aydan iki yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

4. Hak sahibi kişilerin izni olmaksızın, alenileşmemiş bir eserin muhtevası hakkında kamuya açıklamada bulunan kişi, altı aya kadar hapis cezası ile cezalandırılır.

5. Bir eserle ilgili olarak yetersiz, yanlış veya aldatıcı mahiyette kaynak gösteren kişi, altı aya kadar hapis cezası ile cezalandırılır.

6. Bir eseri, icrayı, fonogramı veya yapımı, tanınmış bir başkasının adını kullanarak çoğaltan, dağıtan, yayan veya yayımlayan kişi, üç aydan bir yıla kadar hapis veya adlî para cezasıyla cezalandırılır.

Bu Kanunun ek 4 üncü maddesinin birinci fıkrasında bahsi geçen fiilleri yetkisiz olarak işleyenler ile bu Kanunda tanınmış hakları ihlâl etmeye devam eden bilgi içerik sağlayıcılar hakkında, fiilleri daha ağır cezayı gerektiren bir suç oluşturmadığı takdirde, üç aydan iki yıla kadar hapis cezasına hükmolunur.

Hukuka aykırı olarak üretilmiş, işlenmiş, çoğaltılmış, dağıtılmış veya yayımlanmış bir eseri, icrayı, fonogramı veya yapımı satışa arz eden, satan veya satın alan kişi, kovuşturma evresinden önce bunları kimden temin ettiğini bildirerek yakalanmalarını sağladığı takdirde, hakkında verilecek cezadan indirim yapılabileceği gibi ceza vermekten de vazgeçilebilir.

Manevi haklar, eseri kamuya sunma hakkı, adın belirlenmesi hakkı ve eserde değişiklik yapılmasını men etme hakkıdır. Manevi haklarla mali haklar arasında hakların devri açısından farklılık bulunmaktadır. Manevi haklar eser sahipliğinden doğan mutlak ve münhasır yetkiler olmaları nedeniyle miras yoluyla intikal etmedikleri gibi, devir yönünden ölüme bağlı tasarruflara konu olmazlar ve sağlar arası işlemlerde de devir edilmeleri mümkün bulunmamaktadır. Bununla birlikte, manevi hakların kullanılma yetkisinin devredilmesi mümkündür. Mali haklar ise; süre, yer ve muhteva itibariyle sınırlı veya sınırsız, karşılıklı veya karşılıksız olarak eser sahibi veya mirasçıları tarafından başkalarına devredebileceği gibi, sadece kullanma yetkisi de başkasına devredilebilir.[128]

Mali hak, fikri çalışma ürünü olan eserden ekonomik fayda sağlamak konusundaki yetkileri ifade eder. Eserden ekonomik yararlanmanın koşullarını belirleyen ve eser sahibinin izni olmadığı sürece bu yararlanmayı eser sahibine özgüleyen kurallar bütünü, mali hakları oluşturur. Bütün modern hukuk sistemlerinde olduğu gibi, üçüncü kişilerin eserden yararlanmaları, FSEK'te yer alan sınırlamalar dışında hukuka aykırıdır.[129]

---

[128] Bıçak, Vahit, (t.y.), "Bilim veya Edebiyat Eseri Sahiplerinin Hakları", http://www.caginpolisi.com.tr/75/5-6-7-8.htm, (Erişim Tarihi: 30.10.2010).
[129] Bayamlıoğlu, İbrahim Emre, (2007), *Fikir Ve Sanat Eserleri Hukukunda Teknolojik Koruma*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Doktora Tezi, İstanbul, s.247.

FSEK kapsamında korunan eser sahibinin haklarına ve eser sahibinin hakları ile bağlantılı haklara internet yoluyla tecavüz edilmesi halinde, tecavüze uğrayan hakların, FSEK kapsamında korunmaması düşünülemez. FSEK kapsamında korunan haklar, maddi ortamda tecavüze uğrayabileceği gibi, sanal ortamda da tecavüze uğrayabilir. Bir eser İnternette haksız şekilde çoğaltılabilir, umuma iletilebilir veya hak sahibinin rızası alınmaksızın eserinde değişiklik yapılabilir. İnternet, fikri ve sınaî haklar açısından potansiyel olarak yeni ve büyük bir ticaret ortamı yaratmak yanında, bu hakların kolayca ihlal edilebilirliği açısından da önemli bir risk oluşturmaktadır. Fikir ürünlerinin izinsiz olarak internette erişime açık tutulması, eserin bir arama motorunda bulundurulması, internette çoğaltma uygulamada rastlanılan olumsuz durumlardır.[130]

Günümüz teknolojisinin akıl almaz biçimde gelişmesi, olumlu sonuçlarının yanında her teknolojik gelişmede olduğu gibi bir takım olumsuz sonuçlara da sebep olabilmektedir. Bu noktada, özellikle bilgisayar ve İnternetin günümüzün vazgeçilmez araçları olması karşısında, bu araçların kötüye kullanılması suretiyle eser sahipleri ve bağlantılı hak sahiplerinin haklarının ihlali daha kolay ve daha pratik şekilde gerçekleştirilebilmektedir. Üstelik bu yöntemlerin kullanılması, diğer yöntemlere nazaran daha ucuz ve hedef kitlesi de daha büyüktür. Örneğin, İnternette bir internet sayfasında yer alan bir eserin bu sayfadan indirilerek çoğaltılması ya da hak sahiplerinin rızası olmaksızın bu eseri yüzlerce ve hatta binlerce kişiye bir anda gönderilmesi mümkündür. Bunun gibi, İnternette yer alan bilimsel bir makalenin üzerinde değişiklikler yapılması veya bu makalenin sahibinin adının değiştirilmesi suretiyle bir başka ad altında başka bir sitede yayınlanması gayet kolaydır.[131] İnternetin günümüz insanının hemen her alanda kullanımına girmesi sonucu fikri ürünler de kendilerine bu sanal âlemde yer bulmaya başlamış ancak bu durum, madden cisimlenmemiş eserlerin ve icraların korunmasında hak sahiplerine tanınan geleneksel yöntemlerin giderek başarısız olmasına yol açmıştır.[132]

---

[130] Baştürk, İhsan, (2006), *Genel Olarak Fikir Ve Sanat Eserleri Ve Bunlara İnternet Yoluyla Tecavüz İle Sonuçları*, Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.135.

[131] Özderyol, Teknail, (2006), *Fikir Ve Sanat Eserleri Kanununda Düzenlenen Suçlar*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.1.

[132] Gündem, Onur, (2006), *Fikir Ve Sanat Eserleri Kanununda Eser Sahibinin Haklarına Bağlantılı Haklar, Bu Hakların Sınırlandırılması Ve Korunması*, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Kırıkkale, s.51.

1.3.2.1. Koruyucu Programları Etkisiz Kılmaya Yönelik Hazırlık Hareketleri (FSEK Madde 72)

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

Bir bilgisayar programının kopyalanarak hukuka aykırı olarak çoğaltılmasını önlemek amacıyla ilave programlar kullanılmaktadır. İlave programlarla korunmak istenen bir bilgisayar programını etkisiz kılmaya yönelik program veya teknik donanım üretmek, satışa arz etmek ve ya kişisel kullanım amacı dışında elinde bulundurmak suç sayılmaktadır. Bu donanım ve programların kişisel kullanım amacıyla elde bulundurulması suç teşkil etmemektedir.[133]

1.3.3. Elektronik İmza Kanunu'nda Düzenlenen Bilişim Yoluyla İşlenen Suçlar

Elektronik İmza Kanunu'nda düzenlenen suç türlerini incelmeden önce kanunda geçen tanımlara değinmek gerekmektedir. Kanunun ikinci maddesine göre;

Elektronik veri: Elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları, **Elektronik imza:** Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi, **İmza sahibi:** Elektronik imza oluşturmak amacıyla bir imza oluşturma aracını kullanan gerçek kişiyi, **İmza oluşturma verisi:** İmza sahibine ait olan, imza sahibi tarafından elektronik imza oluşturma amacıyla kullanılan ve bir eşi daha olmayan şifreler, kriptografik gizli anahtarlar gibi verileri, **İmza oluşturma aracı:** Elektronik imza oluşturmak üzere, imza oluşturma verisini kullanan yazılım veya donanım aracını, **İmza doğrulama verisi:** Elektronik imzayı doğrulamak için kullanılan şifreler, kriptografik açık anahtarlar gibi verileri, **İmza doğrulama aracı:** Elektronik imzayı doğrulamak amacıyla imza doğrulama verisini kullanan yazılım veya donanım aracını, **Zaman damgası:** Bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, elektronik sertifika hizmet sağlayıcısı tarafından elektronik imzayla doğrulanan kaydı, **Elektronik sertifika:** İmza sahibinin imza doğrulama

[133] Karagülmez , (2009), a.g.e., s.155.

verisini ve kimlik bilgilerini birbirine bağlayan elektronik kaydı, **Kurum:** Telekomünikasyon Kurumunu, ifade eder.

Elektronik imza terimi, genellikle, elektronik ortamdaki irade beyanlarının tümü için kullanılan bir tanımdır. Geniş bir tanım yapmak gerekirse, elektronik imza, bir belgeyi imzalama niyetinde olan bir kişi tarafından sahiplenilmiş ya da icra edilmiş bir belgeyle/kayıtla mantıksal bir şekilde ilişkilendirilmiş veya eklenmiş bir süreç, elektronik bir ses veya sembol anlamına gelir.[134] Ancak kanunun konusunu oluşturan elektronik imzalar hukuken elle atılan imza ile aynı hukuki sonucu doğuran güvenli elektronik imzalardır.[135] Kanunun dördüncü maddesine göre güvenli elektronik imza; münhasıran imza sahibine bağlı olan, sadece imza sahibinin tasarrufunda bulunan güvenli elektronik imza oluşturma aracı ile oluşturulan, nitelikli elektronik sertifikaya dayanarak imza sahibinin kimliğinin tespitini sağlayan, imzalanmış elektronik veride sonradan herhangi bir değişiklik yapılıp yapılmadığının tespitini sağlayan imzalardır.

E-imzaların sağladığı başlıca önemli işlevleri kimlik doğrulama, gizlilik, veri bütünlüğü ve inkâr-edilememezliktir.[136]

1.3.3.1. İmza Oluşturma Verilerinin İzinsiz Kullanımı (EİK Madde 16)

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

(2)Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu suçta korunan hukuksal değer kamunun güvenci ve inancıdır. Burada zarar uğrayan kimseler mağdur olmayıp "suçtan zarar gören" konumundadırlar.[137]

---

[134] Sevim, Tuğrul, (2006), *Elektronik İmza Uygulamasında Kullanılan Zorunlu Ve İhtiyari Dokümanlar,* Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.5.
[135] Elektronik İmza Kanunu Madde 5.
[136] Erol, Hüseyin, (2006), *Kurumsal Ağlarda Açık Anahtar Altyapısı Tabanlı Elektronik İmza Uygulaması*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara, s.56.

Maddede suç sayılan eylemler açıkça belirtilmiş olup, bu eylemlerden birisinin yapılması suçu oluşması için yeterli olacaktır bu nedenle on altıncı maddede tanımlanan suç seçimlik hareketli bir suçtur. Maddenin ikinci fıkrasında kendisine güvenilen konumunda olan "elektronik sertifika hizmet sağlayıcısı çalışanları" tarafından bu suçun işlenmesi ağırlaştırıcı sebep olarak karşımıza çıkmaktadır.

1.3.3.2. Elektronik Sertifikalarda Sahtekârlık (EİK Madde 17)

(1) Tamamen veya kısmen sahte elektronik sertifika oluşturanlar veya geçerli olarak oluşturulan elektronik sertifikaları taklit veya tahrif edenler ile bu elektronik sertifikaları bilerek kullananlar, iki yıldan beş yıla kadar hapis ve yüz günden az olmamak üzere adlî para cezasıyla cezalandırılır.

(2) Yukarıdaki fıkrada belirtilen suçlar elektronik sertifika hizmet sağlayıcısı çalışanları tarafından işlenirse bu cezalar yarısına kadar artırılır.

Bu maddede elektronik imzanın sahtekârlık boyutu suç olarak tanımlanmıştır. Sahte bir şekilde üretilen elektronik sertifikalar ve kullanımı suç olarak kabul edilmiş ve bir yaptırıma bağlanmıştır. Bununla birlikte yine kendisine güvenilen konumunda olan "elektronik sertifika hizmet sağlayıcısı çalışanları" tarafından bu suçun işlenmesi ağırlaştırıcı sebep olarak düzenlenmiştir.

1.4. BİLGİSAYAR VE İNTERNET KULLANIMINDAN KAYNAKLANAN MAĞDURİYETLER

Bilişim suçlarının ve bilişim yoluyla işlenen suçların yanı sıra bazı durumlarda vatandaşlar hukuki bakımdan ortada bir suç olmamasına rağmen bazı mağduriyetler yaşamakta ve bununla ilgili olarak emniyet birimlerine ve savcılıklara şikâyetlerde bulunmaktadırlar. Bilişim teknolojilerinin günlük hayattaki yeri ve yaygınlığı arttıkça bu tür durumlarla karşılaşılması doğaldır.

Örneğin bir kişinin sıklıkla kullandığı bir internet sitesinin (sohbet, video, tartışma forumu gibi) yöneticileri tarafından kişinin geçici olarak engellenmesi veya tamamen yasaklanması kişiyi mağdur etmektedir. Burada hukuki olarak bir suçtan söz edilemese bile ortada bir mağduriyet vardır ve hatta kişi bu inançla savcılığa gelip şikâyet dilekçesi dahi verebilmektedir.

---

[137] Dülger, (2004), a.g.e., s.308.

Benzer durumlar artık sadece genç yaştakilerin ilgilenmediği orta yaş grubundaki kişilerin de sıklıkla ilgi gösterdiği çevrimiçi oyunlarda ve sanal dünya ortamlarında da yaşanmaktadır. Oyun esnasında kural dışı muamelelere maruz kalanlar ya da oyundaki bir özelliğini yitirenler de emniyet birimlerine gelerek şikâyetlerde bulunmaktadırlar. Bununla birlikte bir işyerinde veya arkadaşının bilgisayarında taşınabilir belleğini kullandığı için bilgisayarına zararlı yazılımlar bulaşanlar da mağduriyetler yaşamaktadır.[138]

Şekil 4 – Bilgisayar ve İnternet Kullanımından Kaynaklanan Mağduriyetler

Bu konuyla ilgili ilginç bir örnekte Belçika'da yaşanmıştır. "Second Life (İkinci Hayat)" isimli internet sitesinde sanal ortamda insanlar karakterlerini oluşturmakta ve sanal bir dünyada yaşamaktadırlar. Burada sanal karakterler arasında tecavüze uğradığını iddia eden bir bayanın şikâyeti Belçika savcıları tarafından dikkate alınmış ve soruşturma başlatılmıştır.[139]

[138] Akarslan, Hüseyin, (2009), "Türkiye'de Sayılarla Bilişim Suçlar", *İstanbul Bilgi Güvenliği Konferansı '09*.
[139] Duranske, Benjamin, (2007), "Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life", (http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/, (Erişim Tarihi: 03.11.2010).

İKİNCİ BÖLÜM

BİLİŞİM TEKNOLOJİLERİNİN SUÇ DÜNYASINDA KULLANILMASI VE ADLİ BİLİŞİM

2.1. SUÇ DÜNYASI VE BİLİŞİM TEKNOLOJİLERİ

Bilişim teknolojilerinin, bireysel ve toplumsal yaşamın hemen hemen tüm boyutlarını etkilediğini söylemek günümüzde bir sav olmaktan çıkmış ve genel geçer bir görüş haline gelmiştir. Söz konusu etkileri genel olarak bir taraftan olumlu etkiler ve olumsuz etkiler, diğer taraftan doğrudan etkiler ve dolaylı etkiler olarak sınıflamaya çalışmak olanaklıdır. Olumlu etkilerin, ağırlıklı olarak doğrudan gözlenebilir ve ekonomik olarak hesaplanabilir olmaları nedeni ile sınıflanmaları ve tartışılmalarının çok daha kolay olmasına karşın, olumsuz etkiler için net bir sınıflama ve tartışma yapabilmek çok kolay değildir. Bunun temel nedeni, olumsuz etkilerin ağırlıklı olarak sosyal, kültürel ve dolaylı olmaları ve bu nedenle üzerlerinde daha öznel değerlendirmelerin yapılabiliyor olmasıdır.[140]

İşte bu olumlu ve olumsuz etkilerin suç dünyasına da yansımış olması kadar doğal bir sonuç olamaz. Artık hayatımızın bir parçası olan bilişim teknolojileri yine hayatımızın başka bir parçası olan suç ve suçlu dünyasıyla etkileşim içerisindedir. Bu etkileşimi üç temel kategoriye ayırabiliriz. Bunlardan birincisi bilişim teknolojilerinin suç işlemede bir araç olarak kullanılmasıdır. Suç işlemek için yeni yöntemler ve kolaylıklar arayan suçlular için bilişim teknolojileri günümüzde ciddi bir alternatif haline gelmiştir. İkincisi ise bizzat bilişim teknolojilerinin suç işlenirken hedef alınması ve maddi manevi çıkar sağlamak için ulaşılmak istenen bir amaç haline gelmesidir. Tarihsel süreç içinde değerlendirildiğinde bilişim teknolojilerinin önce suçun aracı daha sonra ise amacı, hedefi haline geldiğini görmekteyiz. Üçüncü durum ise bilişim teknolojilerinin suçla mücadele için kullanılmasıdır. Bilişim teknolojilerinin güvenlik görevlilerine sunduğu avantajların suçu önlemede kullanıldığı gibi suç işlendikten sonra suçu aydınlatmada da kullanıldığını görmekteyiz. Suç dünyası içinde her zaman bir yarış içinde olan suçlular ve güvenlik

[140] Çelik, Levent, (t.y.), "Bilişim Teknolojilerinin Sosyal Yaşam Üzerindeki Etkileri", http://www.pegem.net/akademi/sempozyumbildiri_detay.aspx?id=8152, (Erişim Tarihi: 03.11.2010).

görevlileri artık yeni bir kulvarda "bilişim dünyasında" bu yarışlarına devam etmektedirler, önde olanın kazanacağı bu yarış daha çok uzun sürecek gibi gözükmektedir.

2.2. SUÇ İŞLEMEK İÇİN KULLANILAN BİLİŞİM TEKNOLOJİLERİ

Konuyla ilgili kaynaklara bakıldığında suç işlemek için kullanılan bilişim teknolojilerinden, "bilişim suçu işlenirken kullanılan yöntemler", "bilişim suçu işleme metotları", "bilişim suçlularının kullandığı teknikler" gibi başlıklarla bahsedilmektedir. Ancak bunun eksik bir yaklaşım olduğunu düşünmekteyiz. Çünkü kullanılan teknik ve yöntemlerin bilişim suçlarının yanında bilişim yoluyla işlenebilen klasik suçlarda da kullanıldığını görmekteyiz. Kullanılan yöntem ve teknikleri anlatmadan önce "bilgi güvenliği" kavramına değinmek yerinde olacaktır. Çünkü bu yöntem ve tekniklerin hedefi bilgi güvenliğidir.

2.2.1. Bilgi Güvenliği

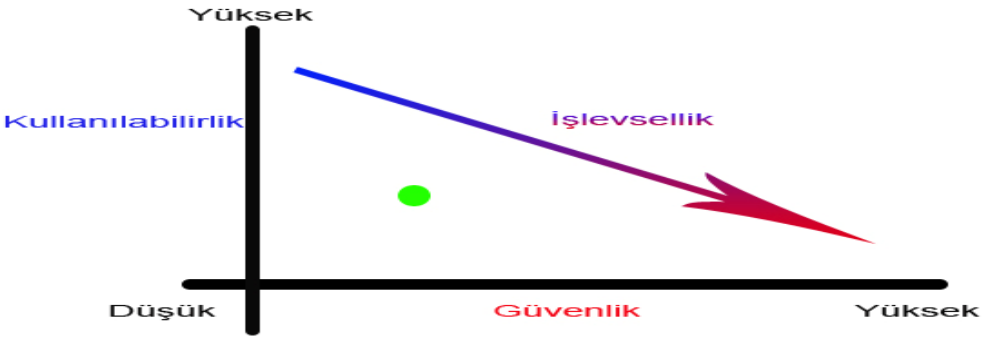
Sözlük anlamına bakıldığında; "bilgi güvenliği, bilginin kime ait olduğu belirlenmiş, bütünlüğü korunarak ve gizliliği sağlanmış olarak iletimi ve saklanması. Bilginin yetkilendirilmemiş aktarımlara, değişimlere, örselenmesine ya da açığa vurulmasına karşı korunması" şeklinde tanımlanmıştır.[141] Bilgi güvenliğinden bahsederken, bilginin "gizliliği", "bütünlüğü", "erişilebilirliği" ve "kurtarılabilirliği" üzerinde yoğunlaşmak gerekir. Bilgininin gizliliğinden kasıt sadece ona erişmeye yetkili kişi ya da kişilerin erişebilmesidir. Bilginin bütünlüğü bilginin kısmen ve ya tamamen tahrife uğramamasıdır. Erişilebilirlik istenildiği zaman bilgiye erişebilmektir. Kurtarılabilirlik ise bilginin kaybedilmesi durumunda tekrar üretilebilmesi için gerekli önlemlerin alınmasıdır.[142]

Bilgi güvenliğinin bilişim dünyasındaki yansıması da "bilişim güvenliği" olarak karşımıza çıkmaktadır. Bilgi güvenliğine benzer şekilde bilişim güvenliği gizliliğe, orijinalliğe, güvenilirliğe ve kullanılabilirliğe dayanır. Pratik uygulamalarda güvenlik ve kullanılabilirlik ters orantılıdır. Bilişim sistemlerinde güvenlik ne kadar

[141] Tavukçuoğlu, (2004), a.g.e., s.46.
[142] Güngören, Bora, (2008), "Bilgi Güvenliği Nedir?", http://www.emo.org.tr/ekler/1440ca9ca2c5e0b_ek.pdf?dergi=2, (Erişim Tarihi: 03.11.2010).

yüksek tutulursa kullanılabilirlik o kadar düşecektir, kullanılabilirliği arttırdığınızda güvenlik seviyesi de o ölçüde düşecek ve güvenlik zafiyetleri ortaya çıkacaktır.[143]

Bilişim güvenliği konusunda bilinmesi gereken bir gerçekte bu alanda kusursuz bir güvenliğin sağlanamayacağıdır. Yani en güncel güvenlik standartları bile zaman içinde yeni zafiyetler doğuracaktır. Bir bilişim sisteminde olması gereken ideal güvenlik seviyesini tespit etmek için, güvenlik üçgeni dediğimiz diyagrama bakmak gerekecektir. Standart yaklaşıma göre üçgenin ortasında durmak yeterlidir. Ancak bilişim sisteminin kurulma amacı, verdiği hizmet, fiziki donanımı ve karşılaşılabilecek güvenlik riskleri gibi sistemin kendine has özellikleri de dikkate alınarak üçgende kenarlara kayılabilir.



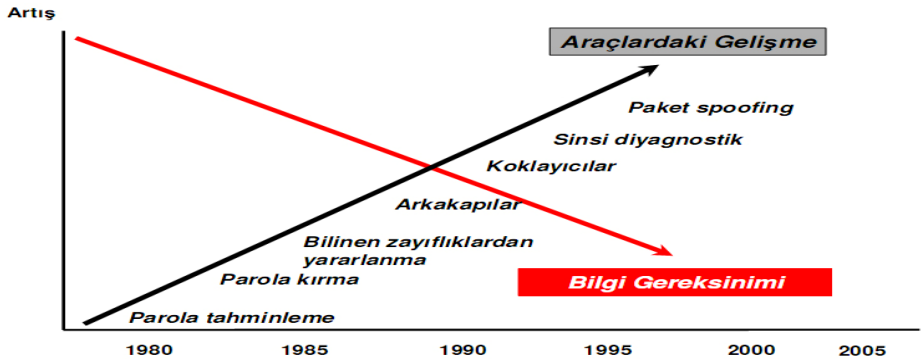
Şekil 5 - Bilişim Güvenliği Üçgeni.

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da o denli artacaktır. Bu duyarlılık arttıkça da bilgisayar sistemlerine ve ağlarına yönelik olarak gerçekleştirilecek olan saldırıların sonucunda; para, zaman, saygınlık ve değerli bilgi kaybı da artacaktır. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda ise kaybedilen insan hayatı bile olabilir.[144]

Bilişim güvenliğine yönelik ilk ortaya çıkan saldırılar daha çok basit etkisi ve olasılığı düşük teknikler olmasına karşın süreç içerisinde yöntemlerin karmaşıklığı ve

[143] Burlu, Kamil, (2010), *Bilişimin Karanlık Yüzü*, Ankara: Nirvana Yayınları, s.2.
[144] Pro-G ve Oracle, (2003), "Bilişim Güvenliği", http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, (Erişim Tarihi: 03.11.2010).

etkileri artmıştır. Buna karşın bu yöntemleri kullanabilmek için gereken bilgi düzeyi düşmüştür ve bu bilgi düzeyine ulaşmak daha da kolaylaşmıştır.[145]



Şekil 6 - Bilgi Güvenliğine Yönelik Saldırı Teknikleri Ve Bilgi Düzeyi.[146]

2.2.2. Bilişim Güvenliğine Yönelik Saldırılar (Hacking, Cracking)

Bilişim sistemlerine yönelik saldırılara genel olarak "hacking" denmektedir. Ancak "hacking" terimi aslında "cracking" teriminin yerine kullanılır hale gelmiştir ve artık hem kamuoyu hem de medyada bu şekilde kullanılmaya devam edilmektedir. "Hacking" terimi; bilişim dünyasının yer altındaki (gizli kalmış) kişilerin kendi yeteneklerini geliştirmek amacıyla bilgisayar sistemlerinin en derin teknik detaylarıyla uğraşır hale gelmesi eylemine denmektedir. "Cracking" ise illegal bir amaç için yine illegal olarak bir bilişim sistemine erişim sağlamak ve verilere müdahale etmek ve ya bilişim ürünlerine yönelik (yazılımlar) illegal müdahalelerde bulunmaktır.[147]

"Hacking" dünyasından ve terimlerinden bahsedilirken "jargon file (argo dosyası)" konusuna değinmek gerekmektedir.[148] Argo dosyası başta internet olmak üzere bilişim teknolojilerindeki birçok yeniliği bilişim dünyasına kazandıran MIT (Massachusetts Institute of Technology)'de geliştirilmiştir. İlk sürümü 1973-1975 yıllarında yayınlanan Argo dosyası bir tür sözlük şeklindeydi. Bu argo sözlüğü, kültürün kendini tanımlamakta kullandığı önemli belgelerden birisi haline gelmiş ve

---

[145] Kara, Mehmet ve Bahşi, Hayrettin, (2010), TÜBİTAK-UEKAE, "Bilişim Sistemleri Güvenliği Araştırmalarının Yönü", http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, (Erişim Tarihi: 03.11.2010).
[146] Koltuksuz, Ahmet, (2007), *Adli Bilişime Giriş*, Adli Bilişim Kursu [Ders Notları], İzmir Yüksek Teknoloji Enstitüsü, İzmir, s.6.
[147] Schell, Bernadette ve Martin, Clemens, (2006), "Webster's New World Hacker Dictionary", Indianapolis USA:Wiley Publishing, ss.73-148.
[148] Jargon File resmi web adresi ve güncel versiyonu: http://www.catb.org/jargon/

1983 yılında "The Hacker's Dictionary" (Bilişim Korsanı'nın Sözlüğü) adı altında yayınlanmıştır. Bu kitap artık basılmamakla beraber, yenilenmiş ve genişletilmiş bir sürümü olan "New Hacker's Dictionary (Bilişim Korsanı'nın Yeni Sözlüğü)" halen yayınlanmaktadır.[149]

Bilişim sistemlerine yönelik saldırılarda saldırganlar beş aşamalı bir yolu takip etmektedirler. Bunlar sırasıyla keşif, tarama, erişimi sağlama, erişime devam etme ve izleri temizlemedir. Keşif evresi hazırlık evresidir amaç saldırı yapılacak hedef hakkında olabildiğince bilgi toplamaktır. Tarama ön saldırı evresidir saldırgan hedef sisteme ulaşmada kullanacağı bilgisayar ağına ya da diğer bağlantılara yönelik zafiyetleri belirlemeye çalışır. Erişimi sağlama artık hazırlıklar tamamlanmış kullanılacak yöntem belirlenmiş ve sonunda hedef sisteme erişilmiştir. Erişime devam ettirme saldırganın sisteme sahip olma evresidir ve saldırının başkaları tarafından anlaşılmaması için çalışılır. İzleri temizleme evresi son evredir, saldırgan artık hedefine ulaşmıştır ancak daha sonra yaptığı işin anlaşılmaması için hedef sistemde kendisiyle ve ya eylemiyle ilgili izleri silmek durumundadır.[150] Bundan sonraki bölümlerde anlatılacak teknik ve yöntemler bu aşamaları gerçekleştirmek içindir diyebiliriz.

2.2.3. Zararlı Yazılımlar

Zararlı (kötücül) yazılımlar İngilizce "malware" yani "malicious software" teriminin kısaltmasından türetilmiştir. Genel olarak kullanıcısının bilgisi dışında gizlice bir bilgisayar sistemine erişebilmek için kullanılan yazılımlardır. Uzmanlar tarafından zararlı yazılımların ortak özellikleri davetsiz (istenmeyen), düşmanca ve rahatsız edici olarak tanımlanmaktadırlar.[151]

Zararlı yazılımlar üretilme amaçlarına göre değil kullanım amaçlarına ve özelliklerine göre isimlendirilirler. Bilgisayar virüsleri, solucanlar (worms), truva

[149] Raymond, Eric S., (2002), "İlk Hacker'lar", http://www.belgeler.org/howto/hacker-history_earlyhacker.html, (Erişim Tarihi: 12.11.2010).
[150] Burlu, (2010), a.g.e., s.9.
[151] Moir Robert, (2003), "Defining Malware:FAQ", http://technet.microsoft.com/en-us/library/dd632948.aspx, (Erişim Tarihi:04.11.2010).

atları (troajan horses), casus yazılımlar (spyware), reklam yazılımları (adware) ve kök kullanıcı takımları (rootkit) en bilenen zararlı yazılımlardır.[152]

2.2.3.1. Bilgisayar Virüsleri

Bilgisayar dünyasındaki olumsuz gelişmelerde ilk akla gelen durum bilgisayar virüsleridir. Bilgisayar virüsleri özel olarak yazılmış küçük birer programdır. Yani, her hangi bir iş, oyun, müzik programı gibi bilgisayar programcıları tarafından yazılmış birer programdır. Farklı olan yönleri diğer programlara kendilerini bulaştırabilmeleridir ve bu şekilde çoğalıp yayılırlar.[153]

Bilgisayar kullanıcılarının birincil sorunu kuşkusuz; virüslerdir. 1982 yılına gelindiğinde Rich Skrenta adlı lise öğrencisi tarafından arkadaşlarına şaka amacıyla hazırlanan ve Apple DOS 3.3 işletim sistemine disketten yayılan ilk virüs yazılmıştır. Bu gelişmelerden sonra 1986'da Pakistan'ın Lahora kentinde yaşayan Basit ve Amjad Farooq Alvi isimli iki kardeş tarafından bir virüs daha yaratılmıştır. Bu virüsün adı "Brain" idi. Açıklanan tarih 1986 olmasına rağmen birçok kişi bunun 1981 tarihinde bulunduğunu ve ilk virüs olduğunu iddia etmektedirler.[154] Uzmanlar, bilgisayar virüsünün evriminde en önemli değişimin, virüs programı yazma hobisinden maddi çıkar sağlama amaçlı sanal suçlara geçiş olduğunu belirterek, ilk bilgisayar virüsünün ortaya çıkışının üzerinden onlarca yıl geçmesinin ardından yüz elli binin üzerinde virüs programının yazıldığını kaydediyorlar.[155] Ancak zararlı yazılımların milyonlarca olduğunu söylemek yanlış olmaz.

Virüsler, disket, cd, İnternet, e-posta gibi yolları kullanarak bilgisayara bulaşırlar. Boot sektör virüsü bulaşmış bir disketle bilgisayar açılırsa virüs sabitdisk'in boot sektörüne bulaşabilir. 2000'li yıllarda virüslerin en çok kullandığı yöntem ise e-posta yoludur. Bu yöntemde virüslü bilgisayar bazen kendi kendine

---

[152] wikipedia.org , (2010), "Malware", http://en.wikipedia.org/wiki/Malware, (Erişim Tarihi:05.11.2010).
[153] Bahtiyar, Ziya, (2003), *Virüsler ve Güvenlik*, İstanbul: Pusula Yayınları, s.2.
[154] chip.com.tr, (2009), "Bilgisayar Virüslerinin Tarihçesi", http://www.chip.com.tr/blog/simyager/bilgisayar-viruslerinin-tarihcesi_3041.html , (Erişim Tarihi:05.11.2010).
[155] ntvmsnbc.com, (2006), "Bilgisayar Virüsü 20 Yaşında", http://arsiv.ntvmsnbc.com/news/358295.asp, (Erişim Tarihi: 05.11.2010)

kaydedilen e-posta adresine posta göndererek virüsün başka bilgisayarlara bulaşmasını sağlamaktadır.[156]

Virüslerin bulaştığı bilgisayarlara verebileceği zarar türleri; [157]

- Bilgisayarınızda hata ve uyarı mesajları almanıza neden olabilir.
- Bilgisayarınızın kilitlenmesini, kapanmasına ve açılamaz hale gelmesine yol açabilir.
- Bilgisayarınızda erişmek istediğiniz bir dosyaya erişiminizi engelleyebilir.
- Dosyalarınızın tamamını ve/veya bir kısmını kullanılmaz hale getirebilir.
- Bilgisayarınıza yerleşerek durağan kalır ve sizin yaptığınız işlemlerin veya bilgilerin (İnternet bankacılığı işlemleri, kredi kartı bilgileri) yetkisiz üçüncü kişilerin tarafından bilinmesine hatta bu kişiler tarafından bilgisayarınıza uzaktan erişime yol açabilir.

2.2.3.2. Bilgisayar Solucanları

Son yılların en popüler virüs benzeri programı olan "worm" ya da Türkçesiyle "kurtçuklar/solucanlar", virüslere oldukça benzer özelliklere sahip oldukları için virüslerle karıştırılmaktadır. Birçok yerde de virüs olarak anılmaktalar. Virüslerle olan temel farkları yayılmak için bulaşmak zorunda oldukları bir dosyaya (konak) ihtiyaç duymamalarıdır. Bunlar bir anlamda bulaşmadan kopyalanma yoluyla çoğalırlar, yayılırlar. Yayılmak için ağları kullanırlar. Bu ağ (network), kurumsal bir ağ (LAN/WAN) olabileceği gibi internet ya da intranet[158] olabilmektedir.[159] Bu nedenle solucanlardan bahsedilirken çoğu zaman "ağ solucanları" da denmektedir.

Standart bir bilgisayar virüsü bir sisteme girdiği zaman bir sistem dosyasını veya ulaşabildiği bir dosyayı gelecekte herhangi bir zamanda kullanılmak üzere

---

[156] Boun.edu.tr, "Virüsler", http://www.cc.boun.edu.tr/viruses_tur.html, (Erişim Tarihi: 05.11.2010).
[157] Tekeli, Ömer, (2005), "Virus Nedir? Korunma Yolları Nelerdir?", http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=55&KKey=103, (Erişim Tarihi: 05.11.2010).
[158] Intranet, sadece belirli bir kuruluş içindeki bilgisayarları, yerel ağları (LAN) ve geniş alan ağlarını (WAN) birbirine bağlayan, çoğunlukla TCP/IP tabanlı bir ağdır. Intranet'ler, şirket(ler) içi tele-konferans uygulamalarında ve farklı birimlerdeki kişilerin bir araya gelebildiği iş gruplarının oluşturulmasında da kullanılırlar. Günümüzde bazı şirketlerdeki intranet'lerden (bazı emniyet tedbirleri ile) İnternet çıkışı da yapılmaktadır. Bu sayede, her iki yönde de ileti trafiği kontrol edilebilmekte ve güvenlik sağlanmaktadır.
http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/64.html, (Erişim Tarihi: 9.11.2010).
[159] Bahtiyar, (2003), a.g.e., s.46.

değiştirir. Bu değiştirme genellikle virüs bilgisayarın neresinde olursa olsun aktif hale getirilebileceği bir komutun dosyaya eklenmesiyle olur. Virüsler ile solucanlar arasındaki yapılacak karşılaştırmada dikkat edilecek en önemli nokta, kullanıcı tarafından virüs aktif hale getirilinceye kadar virüsün bilgisayarda hareketsiz kalmasıdır. Oysa solucan bu açıdan bakıldığında çok daha güçlüdür. Bir solucan bilgisayara girdiği zaman eğer yapabilirse bulaşabileceği internet alanlarını arayan bir programı başlatır. Bir solucanın yüklediği bu programın başlayabilmesi için herhangi bir kullanıcının işlem yapmasına ihtiyacı yoktur. Dahası solucan internet üzerinde gezer ve kendini ekleyebileceği yeni kurban bilgisayarlar arar. Solucanın çalışması için kullanıcının bir hareketine ihtiyaç duymadığı gibi yayılmak için de herhangi bir harekete ihtiyaç duymaz.[160]

Solucanlar özellikle yayılmasının çok hızlı ve kolay olmasından dolayı suç dünyasında kullanılmaktadır. Binlerce bilgisayarı ve kullanıcısı olan büyük şirketler ve finans kurumlarının bilişim sistemlerine yönelik yapılan illegal girişimler için solucanlar tercih edilmektedir. Geniş bir alanı hedef alan bu saldırılarda takip de çok zor olmaktadır.[161]

2.2.3.3. Truva Atları

Truva atları ismini herkes tarafından bilinen tarihteki truva atından almaktadır ve aynı plan ve yöntem üzerinde çalışırlar. Bir truva atı (trojan horse), legal bir program içindeki illegal talimatlar ya da bir işi yapıyormuş gibi görünüp kullanıcısından habersiz işlemler yapan zararlı bir programdır. Genel olarak bir truva atı iki bölümden oluşur, istemci ve sunucu bölümü. Sunucu tarafında hedef seçilen kişinin bilgisayarında, istemci tarafı ise diğer bilgisayarda yani uzaktan illegal olarak erişen ve yöneten kişinin bilgisayarında çalışır. Truva atları sıklıkla bilişim sistemlerine yönelik yapılan saldırılarda kullanılsa da bazen legal olarak bilişim sistemlerinden sorumlu teknik personel tarafından da kullanılabilmektedir.[162]

---

[160] Özdilek, Ali Osman, (2003), "Kurtlar Ve Zombiler : Worm'ların ve Ddos Ataklarının Hukuki İncelemesi", http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.htm, (Erişim Tarihi : 9.11.2010).

[161] Akarslan, Hüseyin, (2006), "Adanalı Hacker", http://www.bilgisayarpolisi.com/index.php?sayfa=makaleoku&kategori=3&id=76, (Erişim Tarihi: 09.10.2010).

[162] Yılmaz, Davut, (2005), *Hacking Bilişim Korsanlığı ve Korunma Yöntemleri*, İstanbul: Hayat Yayınları, s.380.

Truva atları diğer kötücül yazılımlar gibi kendi başlarına işlem yapamazlar. Truva atlarının zararlılığı kullanıcının hareketlerine bağlıdır. Truva atları kendilerini kopyalayıp dağıtsalar bile her kurbanın programı (truva atını) çalıştırması gerekir. Bu yüzden Truva atlarının zararlılığı bilgisayar sistem açıklarına veya ayarlarına değil ileriki konularda bahsedeceğimiz toplum mühendisliğinin (sosyal mühendislik) başarılı uygulamalarına bağlıdır.[163] Truva atları da diğer birçok zararlı yazılımda olduğu gibi kullanıcılar tarafından internette ve ya e-posta yolu ile ücretsiz kullanabilecekleri basit programlar ya da ekran koruyucular gibi küçük ama ilgi çekici uygulamalar aracılığı ile bilgisayarlara bulaşmaktadırlar.

Truva atları bilişim sistemlerinden yaralandıkları güvenlik zafiyetlerine ve nasıl zarar verdiklerine göre yedi türde gruplandırılabilirler. Bunlar; uzaktan erişim sağlayan truva atları, başka bir bilgisayar veri gönderen truva atları, verilere zarar veren truva atları, hedef bilgisayarı vekil sunucu haline getiren truva atları, hedef sistemi basit dosya gönderme-alma (FTP) sistemi haline getiren truva atları, güvenlik programlarını etkisiz hale getiren truva atları ve hedef sistemi hizmet veremez hale getiren (Dos) truva atlarıdır.[164]

2.2.3.4. Casus Yazılımlar ve Reklam Yazılımları

Casus yazılımlar (spyware) ve reklam yazılımları (adware) bilgisayarınıza geldikten sonra bilgisayarınızda farklı etkiler ile casusluk yapan veya sizi rahatsız eden yazılımlardır. Bu rahatsızlık yöntemlerden en popülerleri; bilgisayarınızdaki verileri, gezdiğiniz siteleri belli bir merkeze gönderme ve reklam gösterme, internetten reklam indirme şeklinde karşımıza çıkmaktadır. Uygulamalara bakıldığında bu yazılımların temel iki amaç için kullanıldığını görmekteyiz. Birincisi milyonlarca kişinin bilgisayar kullanımı ile ilgili istatistikleridir ve bu istatistikler bazı firmalar için çok değerli olabilmektedir. İkincisi ise yazılımın bulaştığı program vasıtasıyla

[163] wikipedia.org , (2010), "Kötü Virüs", http://tr.wikipedia.org/wiki/Kötü_virüs, (Erişim Tarihi: 10.11.2010).
[164] webopedia.com , (t.y.), "What is a Trojan Horse?", http://www.webopedia.com/TERM/T/Trojan_horse.html, (Erişim Tarihi: 10.11.2010).

istem dışı olarak İnternet üzerinden reklamları tıklatmaktır. Bu tıklamalarda büyük reklam gelirleri sağlayabilmektedir.[165]

Bazı kötü niyetli kişiler tarafından casus yazılımlar kullanılarak istenilen bilişim sistemlerinden bilgiler çalınacağı vaadiyle dolandırıcılık da yapılmaktadır. Ülkemizde de benzer bir durumla karşılaşılmıştır, para karşılığı casus yazılımlarını kullandırarak hedeflenen bilişim sistemlerine erişilebileceğini iddia eden dolandırıcılara yönelik operasyonlar yapılmıştır.[166]

Son yıllarda casus yazılımlar cep telefonlarının da gelişmesiyle birlikte bu alanda kullanılmaya başlandı. Cep telefonlarına yüklenen casus yazılımlar sayesinde telefon konuşmalarını dinleme, ortam dinlemeleri, kısa mesajlara erişim gibi işlemler yapılabilmektedir. Bu yazılımlar tek başına satıldığı gibi, yazılımların yüklü olduğu cep telefonları da satılmaktadır.[167]

Reklam yazılımları ve casus yazılımları genel olarak ayrı ayrı geliştirilse de bazı zararlı yazılımlar her iki özelliği de barındırmaktadır.[168] Bu yazılımların bilgisayarda aktif hale gelmesi için kullanıcı tarafından kurulum yapılması ya da bu işlemin onaylanması gerekmektedir, kullanıcılar dikkatsizlikle ya da ilgi çekici bir internet içeriğine erişmek amacıyla bu hataya düşebilmektedirler. Yazılımların bulaştığı bilgisayarlarda tespit gerçekten zor olmaktadır ve sıradan anti virüs programları da yetersiz kalmaktadır.[169]

2.2.3.5. Kök Kullanıcı Takımı (Rootkit)

Son yıllarda en çok kendinden söz edilen zararlı yazılım türü olan kök kullanıcı takımı, hedef bilişim sisteminin dosya ve süreçlerini gizlemek veya değiştirmek suretiyle manipüle eden uygulamalardır. Farklı seviyelerde çalışan root (üst düzey

---

[165] İstanbul Üniversitesi Bilgisayar Bilimleri Uygulama ve Araştırma Merkezi, (t.y.), "Casus Yazılım Ne Demek?", http://bilisim.istanbul.edu.tr/index.asp?grp=makaleler&no=1, (Erişim Tarihi: 10.11.2010).

[166] EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, (t.y.), "Sanal Dedektiflik Operasyonu", (http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=64&KKey=119, Erişim Tarihi: 10.11.2010).

[167] PowerProNet Bilişim, (t.y.), "Türkiye'nin En Profesyonel Casus Yazılım Sitesi", http://www.powerpronet.net, (Erişim Tarihi: 10.11.2010)

[168] wikipedia.org , (2010), "Adware", http://en.wikipedia.org/wiki/Adware, (Erişim Tarihi: 11.11.2010).

[169] microsoft.com , (t.y.), "How to Protect Your Computer from Spyware and Adware", http://www.microsoft.com/windowsxp/using/security/expert/honeycutt_spyware.mspx, (Erişim Tarihi: 11.11.2010).

yetki) kit (araç - program), sistem açıklarını sömüren kullanıcının, sistem yönetici tarafından tespit edilme olasılığını minimuma indirger, hatta engeller. İlk olarak Unix işletim sistemleri için geliştirilmiş ancak daha sonra diğer işletim sistemlerinde de kullanılmıştır.[170]

Kök kullanıcı takımlarının iki önemli özelliği vardır. Birincisi etkiledikleri bilişim sisteminde üst seviye kullanıcı yetkilerini gerektiren komutları çalıştırabilmeleridir. İkincisi ise kendilerine diğer üst seviye yetkilere sahip kullanıcılardan gizleyebilmeleridir.[171]

2.2.3.6. Mantık Bombaları – Yazılım Bombaları – Zaman Bombaları

Mantık bombaları tek başlarına bir program halinde bulunan ve ya başka programlara bulaşmış kötücül yazılımlardandır. Mantık bombaları belli bir mantığa göre çalışır ve aktif olması için programsal olarak belli bir işlemin daha önce yapılması gerekir, yani mayına basmak gibi.[172]

Yazılım bombaları, en yaygın kötücül yazılımlardandır. Sisteme bulaştıkları anda verileri yok etmeye başlarlar. Bu işlemleri sırasında kullanıcı tarafından fark edilmezler ve erişebildikleri kadar geniş etkide verilere zarar verirler.[173]

Zaman bombaları aynı gerçek dünyadaki saatli bombalar gibi davranırlar. Bir bilgisayar sistemine bulaştıkları anda harekete geçmezler belli bir zamanın dolmasını ya da belli bir tarihin, saatin gelmesini beklerler. 1999 yılında yayılan WIN.CIH (Çernobil) virüsü buna örnek verilebilir. Virüs sadece her yılın 26 Nisan tarihinde aktif oluyor ve bilgisayarlara ciddi zararlar veriyordu.[174]

2.2.3.7. Bukalemunlar – Tavşanlar

Truva atlarına çok benzeyen bukalemunlar, diğer alışılagelmiş, güvenilir programlar gibi davranmakla beraber, gerçek birtakım hile ve aldatmalar içerirler. Bir

---

[170] Elbahadır, Hamza, (2010), *Hacking Interface*, İstanbul:Kodlab Yayınları, s.237.
[171] Bozağaç, Cumhur Doruk, (2006), *Ghostware And Rootkit Detection Techniques For Windows [Windows İşletim Sistemi İçin Ghostware Ve Rootkit Yakalama Teknikleri],* Bilkent Üniversitesi Mühendislik ve Gen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara, s.3.
[172] tech-faq.com , (t.y.), "Logic Bomb", http://www.tech-faq.com/logic-bomb.html, (Erişim Tarihi: 12.11.2010)
[173] Aydın, (1992), a.g.e., s.51.
[174] verikurtarma.org , (t.y.), "WIN.CIH (Çernobil) virüsü Hakkında", http://verikurtarma.org/verikurtarma_cih.htm, (Erişim Tarihi: 12.11.2010).

bukalemun, şifreleri için giriş iletilerini taklit edecek şekilde dâhiyane bir biçimde programlanır. Bukalemun, sisteme giren bütün kullanıcıların adlarını ve şifrelerini gizli dosyaya kaydeder ve daha sonra sistemin bakım için geçici bir süre kapatılacağına ilişkin bir mesaj verir. Daha sonra bukalemunun yaratıcısı, kendi özel şifresi ile sisteme girer ve kaydedilen kullanıcı isimlerin ve şifrelerini alır.[175]

Tavşanlar girdikleri sistem içinde sürekli hızla yürüyen, yerleştiği bellek veya diskteki alanı koloni kurmak suretiyle sürekli dolduran, sistemin bilgi işleme gücünü zayıflatan, bilgisayar veya sisteme sürekli gereksiz komutlar veren kendi kendilerine yetip, virüsler gibi asalak olmayan programlardır.[176]

2.2.4. Gizli - Arka Kapılar (Back Doors)

Arka kapılar bir bilgisayar sistemine yönelik normal kimlik doğrulama (kullanıcı adı ve şifre gibi) yöntemini devre dışı bırakarak başka bir yöntemle illegal olarak sisteme giriş yapma ve verilere erişme metodudur.[177] Ancak arka kapılar bazı durumlarda illegal olmayabilir örneğin bir bilişim sisteminin düzgün çalışmaması ihtimaline karşılık programcı tarafından her zaman müdahale edilebilmesi için de kullanılabilir.[178] Arka kapılar bir önceki konuda bahsettiğimiz zararlı yazılımlar aracılığıyla da açılabilir ve kullanılabilirler.

2.2.5. Yemleme – Oltalama Yöntemi (Phishing)

Özellikle çevrimiçi (online) dolandırıcılıkta suçlular tarafından en çok tercih edilen ve mağdurlarının da gün geçtikçe arttığı bir dolandırıcılık yöntemi olan "phishing" İngilizce "Password" (Şifre) ve "Fishing" (Balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuştur.[179]

---

[175] evbilgisayari.com , (t.y.), "E-Mail ve İnternet Güvenliğinizi Sağlayın!", http://www.evbilgisayari.com/İnternet-genel/18011-e-mail-İnternet-guvenliginizi-saglayin.html, (Erişim Tarihi: 12.11.2010).
[176] Kurt, (2005), a.g.e., s.75.
[177] wikipedia.org , (2010), "Backdoor (computing)", http://en.wikipedia.org/wiki/Backdoor_(computing), (Erişim Tarihi: 12.11.2010)
[178] Tavukçuoğlu, (2004), a.g.e., s.31.
[179] wikipedia.org, (2010), "Yemleme", http://tr.wikipedia.org/wiki/Yemleme, (Erişim Tarihi: 14.11.2010).

Yemleme yönteminde amaç kurbanın kişisel verilerini ele geçirmektir. Bu kişisel veriler basit e-posta veya internet kullanıcı adı ve şifreleri olabileceği gibi, kredi kartı ve bankacılık bilgileri olmak üzere mali bilgiler de olabilmektedir.[180]

Gerçeğinin neredeyse yüzde yüz aynısı gibi hazırlanmış sahte intermet sayfaları ve bir kamu kurumu ya da finans kuruluşundan geliyormuş gibi gösterilen sahte e-postalar yemleme yönteminin temel araçları olarak karşımıza çıkmaktadır.[181] Sahte e-postalar bir bankadan geliyormuş gibi gösterilip kişinin bilgilerinin güncellenmesi istenmektedir. Kişi bilgilerini güncelleyip e-postaya cevap verdiğinde hesap bilgileri ve kimlik bilgileri üçüncü kişilerin eline geçmektedir. Diğer bir yöntem ise çevrimiçi işlemlerin yapıldığı bir bankanın internet sayfasının gerçeğe çok yakın kopyasının yapılarak müşterilerin bu sahte internet adresine yönlendirilmesi ile gerçekleşmektedir, bu yönlendirme işlemi de bazen e-posta gönderilerek olabilmektedir. Sahte internet sayfasında işlem yapabilmek amacıyla kullanıcı adı ve şifresini giren kurbanın bilgileri yine üçüncü şahısların eline geçecektir.[182]

2.2.6. Tarama (Scanning)

Bilişim dünyasında "port (giriş - delik)" terimi hem fiziksel hem de sanal bir yapı ifade etmektedir. Fiziksel olarak bilgisayarların girdi ve çıktı birimleri örneğin yazıcı gibi bu girişler vasıtasıyla bilgisayara bağlanırlar. Sanal anlamda giriş ise veri iletişimi açısından işletim sistemleri ve ağ cihazlarındaki iletişimin hangi sanal yoldan (kullanılan iletişim protokolündeki veri yapısının özelliğine göre verilen bir numara – mantıksal bağlantı noktası)[183] yapılacağını ifade eder.[184]

Bilişim sistemlerinde güvenlik amacı ile sadece belli programların ve servislerin iletişimi için bazı girişler açık durumdadır. Bir sisteme saldırı yapmak isteyen kişi de sadece bu açık girişleri kullanabilecektir. Giriş tarama işlemi bir

[180] Karadeniz, Tacettin, (2005), "Türkiye'de Phishing", http://www.olympos.net/belgeler/turkiyede-phishing-126266.html, (Erişim Tarihi: 14.11.2010).
[181] turk.internet.com , (2004), "Online Dolandırıcılık (Phishing) Artıyor", http://www.turk.internet.com/portal/yazigoster.php?yaziid=10920, (Erişim Tarihi: 14.11.2010)
[182] garanti.com.tr, (t.y.), "Phishing (Olta) Saldırıları", http://www.garanti.com.tr/tr/bireysel/subesiz/İnternet_bankaciligi/guvenlik /phishing.page, (Erişim Tarihi: 14.11.2010).
[183] Tavukçuoğlu, (2004), a.g.e., s.250.
[184] Atakan, Mustafa, (2001), "Port Nedir?", http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/32.html, (Erişim Tarihi: 14.11.2010)

bilişim sistemindeki açık girişleri tespit etme sürecidir.[185] Bu işlem için geliştirilmiş programlar olduğu gibi tek tek deneme yöntemi ile de giriş taraması yapılabilmektedir. Giriş taramasının yanında bir de "zafiyet taraması" yöntemi vardır. Bu yöntemle sistemdeki açık girişleri yanı sıra, işletim sistemi ve kurulu durumdaki programların da güvenlik zafiyetleri özel geliştirilmiş yazılımlar sayesinde taranarak tespit edilebilmektedir.[186]

2.2.7. Şifre Kırıcılar

Bilişim teknolojilerinin kullanılmaya başlandığı ilk dönemlerde şifre kırma işlemleri basit olarak tahmin etme ve deneme yanılma yolu ile olmaktaydı. Ancak günümüzün gelişmiş bilişim sistemlerinde bu tür yöntemlerle bir sistemin şifresini kırmak pek mümkün değildir. Bunun yerine bu iş için geliştirilmiş yazılımlarla ve "kaba kuvvet (brute force)" denilen yöntemlerle sistemlerin şifreleri kırılmaya çalışılmaktadır.[187]

Aslında temel mantık yine deneme yanılma yöntemidir ancak geliştirilen programlar bu işlemi çok hızlı hale getirmektedir. Programlar öncelikle hedef sistem üzerinde dünyada en çok kullanılan şifreleri ve kendi hazır şifre listelerindeki şifreleri denemektedirler. Daha sonra ise ellerindeki şifre alternatiflerinin farklı varyasyonları ile şifreyi kırmayı denemektedirler.[188]

2.2.8. Dos Saldırıları ve Köle Bilgisayarlar

Bilişim sistemlerinin verdikleri hizmete göre bir fiziki yani donanımsal kapasiteleri ve yazılımsal kapasiteleri vardır. "Dos (Denial of Service)" saldırıları bu kapasitenin tamamının kullanılarak sistemin hizmet veremez (servis dışı) hale getirilmesidir. "DDos (Distributed Denial of Service)" ise Dos ataklarının dağınık bir şekilde çok sayıda kişi (bilgisayar) tarafından yapılmasıdır.[189]

---

[185] Shirey, R., (2000), "İnternet Security Glossary", http://tools.ietf.org/html/rfc2828, (Erişim Tarihi: 14.11.2010).
[186] wikipedia.org, (2010), "Vulnerability Scanner", http://en.wikipedia.org/wiki/Vulnerability_scanner, (Erişim Tarihi: 14.11.2010)
[187] wisegeek.com, (t.y.), "What Is Password Cracking?", http://www.wisegeek.com/what-is-password-cracking.htm, (Erişim Tarihi: 14.11.2010).
[188] techtarget.com, (2000), "What is Brute Force Cracking?", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci499494,00.html, (Erişim Tarihi: 14.11.2010).
[189] Özdemircili, Özgür, (t.y.), "Denial of Service Saldırılarının Önlenmesi", http://www.enderunix.org/docs/dos-saldirilari.pdf, (Erişim Tarihi: 14.11.2010).

Dos ve DDos saldırıları en çok internet sayfası yayınlanan sunuculara yönelik yapılmaktadır böylece internet sayfaları erişilemez hatta bütün sunucu hizmet veremez hale gelebilmektedir. İnternet sunucularına yönelik yapılacak Dos saldırıları temelde iki türden oluşur; kaba kuvvet saldırıları (Flood) ve tasarımsal/yazılımsal eksikliklerden kaynaklanan zafiyetlerden yararlanılarak yapılan saldırılar. Kaba kuvvet tipi saldırılarda sunucu üzerinde ne çalıştığına bakılmaksızın eş zamanlı olarak binlerce istek gönderilir ve sunucunun kapasitesi zorlanır. Bir kişi ya da birden fazla kişi anlaşarak belli bir hedefe eş zamanlı yüzlerce, binlerce istek gönderir ya da bu işi hazır köle (zombi) bilgisayarlara devredilerek etki gücü çok daha yüksek Dos saldırıları gerçekleştirilir.[190]

Bilişim sistemlerine yönelik saldırılarda saldırganlar kimlikleri gizlemek ve ya saldırının etkisini artırmak için başka bilgisayarları zombi bilgisayar olarak kullanmaktadırlar. Burada kişisel bilgisayarlar, kötücül yazılımlar ve güvenlik zafiyetlerinden faydalanılarak ele geçirildikten sonra saldırganın istekleri doğrultusunda, kullanıcısı farkında olmadan kullanılırlar.[191]

Ülkemizde de başta çocuk pornografisi olmak üzere bir suçta aracı olarak köle bilgisayarlar kötü niyetli kimseler tarafından kullanılmaktadır.[192] Hollanda da köle bilgisayarlara polis tarafından ilginç bir müdahale edilmiştir. Polis tespit ettiği köle bilgisayarlara yine bilgisayara bulaştırılan kötücül yazılımı kullanarak illegal bir yöntemle erişerek kullanıcıları uyarmıştır.[193]

2.2.9. Gizlice Dinleme – Ağı Koklama (Sniffing)

Gizlice dinleme bir bilgisayar ağında iletişim halindeki veriye erişmektir. Veri trafiğinin akmasına engel olunmadan verinin bir kopyası ağı gizlice dinleyen (koklayan) kişinin bilgisayarına yönlendirilir. Bir paket (ağ üzerinde veriler paketler

---

[190] guvenlikegitimleri.com, (t.y.), "Web Sunuculara Yönelik DOS/DDOS Saldırıları", http://www.guvenlikegitimleri.com/new/calismalar/web_ddos.pdf, (Erişim Tarihi: 14.11.2010)

[191] Şıracı, Sertel, (2009), "Zombi Bilgisayarlar Ve Bilişim Suçu", (http://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zombi-bilgisayarlar-ve-biliim-sucu.html, (Erişim Tarihi: 14.10.2010).

[192] Pehlivan, İlker, (2010), "Türkiye'deki 'Zombi Bilgisayar'lar 2 Milyonu Geçti, Sayı Hızla Artıyor", http://www.radikal.com.tr/Radikal.aspx?aType=RadikalHaberDetay&ArticleID=998855&Date=26.05.2010&CategoryID=101, (Erişim Tarihi: 14.11.2010).

[193] ntvmsnbc.com , (2010), "Polis Zombi Bilgisayarları 'Hack'ledi", http://www.ntvmsnbc.com/id/25145670, (Erişim Tarihi: 14.11.2010).

halinde taşınır) koklayıcı ağ üzerindeki tüm trafiği kontrol etmek için bilgisayar içerisine yerleşir ve kendi kendine çalışır. Bunlar yazılımsal ya da donanımsal olabilir.[194]

2.2.10. Sahte (Fake) – İstenmeyen (Spam) Elektronik Postalar

Sahte e-postalarda amaç kurbanın e-posta şifresini öğrenmektir. Bunun için öncelikle e-posta şifresi ele geçirilmek istenen kişiye sanki e-posta hizmetini aldığı internet sayfasından (Hotmail, Gmail, Mynet… gibi) geliyormuş gibi e-posta gönderilir. Bunun yapılabilmesi için e-posta başlık bilgileri değiştirilir, başlık bilgileri e-postanın kimden geldiği, kime gideceği, tarihi gibi birçok detaylı bilgiyi içerir.[195] Bu gönderilen sahte e-postayı cevaplamak için kişi yine sahte hazırlanmış bir internet adresine yönlendirilir ve kurban kullanıcı adı ve şifresini girdiğinde üçüncü kişilerin eline geçer.

İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi "istenmeyen e-posta (spam)" olarak adlandırılır. İki tür istenmeyen e-posta vardır, birincisi İnternet üzerinden belli tekniklerle çok sayıda e-posta adresinin toplanması ve bunlara e-posta gönderilmesidir. İkincisi ise MMF (Make Money Fast – Kolay Para Kazanın) iletileri; zincir iletiler ya da piramit benzeri pazarlama yapıları ile ilgili gelen iletilerdir. Burada kişi para kazanacağını zannederek e-postayı kendi arkadaşlarına gönderir ve onlarda kendi e-posta listesindeki kişilere, böylece e-posta çok sayıda kişiye ulaşmış olur.[196]

2.2.11. Klavye Dinleme Sistemleri (Keylogger)

Klavye dinleme sistemleri yazılımsal olabildiği gibi donanımsal da olabilirler. Görevleri kullanıldıkları bilgisayarda klavyede basılan her tuşu tespit etmek ve bunu ya kaydetmek ya da anında başka üçüncü bir kişiye göndermektir.[197] Çok amaçlı

---

[194] Akgün, Fatma; Buluş, Ercan ve Şen, Şenol, (t.y.), "Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler Ve Korunma Yollarının İncelenmesi", http://www.emo.org.tr/ekler/0cc088a48f313ab_ek.pdf, (Erişim Tarihi: 14.11.2010).
[195] Tschabitsche , Heinz , (2010), "What Email Headers Can Tell You About the Origin of Spam", http://email.about.com/cs/spamgeneral/a/spam_headers.htm, (Erişim Tarihi: 16.11.2010).
[196] spam.org.tr, (t.y.), "Spam Nedir", http://www.spam.org.tr/nedir.html, (Erişim Tarihi: 16.11.2010)
[197] wisegeek.com, (t.y.), "What is a Keylogger?", http://www.wisegeek.com/what-is-a-keylogger.htm, (Erişim Tarihi: 16.11.2010).

kullanılmaktadırlar. Özel bilgileri gizlice kaydetmek, kullanıcı adı ve şifreleri çalmak, birisinin bilgisayarında yaptığı işlemleri takip etmek en çok kullanım alanlarıdır.

2.2.12. Sahte Kişilik Oluşturma ve Kişilik Taklidi Yoluyla Dolandırıcılık

Hile yoluyla kendisine veya bir başkasına menfaat sağlamak ya da zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır. Bu metotta gerçek kişilere ait bilgiler kullanılarak 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.[198]

Günümüzde sosyal paylaşım ağlarında "sahte profil" oluşturma sık rastlanan bir problemdir. Kötü niyetli kişiler başkaları adına sahte profil oluşturarak, o kişinin arkadaşları ile iletişime geçerek dolandırıcılık yapmaktadırlar. Sahte profil oluşturma eylemlerinde yurt dışındaki uygulamalarda sahte profil oluşturan kişiler yüklü miktarda para cezasına çarptırılmaktadırlar.[199]

2.2.13. Hile – Aldatma (Spoofing)

İnternette aldatma, IP numarasındaki değerlerin olduğundan farklı gösterilmesi olarak bilinir. IP aldatmacası dışında bilinen aldatma türleri şunlardır; "dns aldatmacası", "icq aldatmacası", "arp aldatmacası".[200] Bütün aldatma eylemlerindeki genel amaç iletişimde olunan tarafları kandırmaktır. Bu kandırma bazen kendi kimliğini gizlemek amacıyla yapılırken bazen de iletişim ortamında aslında başkasına giden bir iletinin aldatma yapan kişiye gelmesini sağlamaktır.

---

[198] Tavukçuoğlu, (2004), a.g.e., s.54.
[199] bilisimhukuk.com, (2009), "Facebook'ta sahte profil oluşturma davası sonuçlandı.", http://www.bilisimhukuk.com/2009/07/facebookta-sahte-profil-olusturma-davasi-sonuclandi/, (Erişim Tarihi: 16.11.2010).
[200] angelfire.com , (t.y.), "Spoofing Nedir?", http://www.angelfire.com/biz3/zurnayiz/spoofing.html, (Erişim Tarihi: 16.11.2010).

2.2.14. Sosyal Mühendislik

Bilgisayar güvenliği terimleriyle "sosyal mühendislik" insanlar arasındaki iletişimdeki ve insan davranışındaki açıklıkları tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir. Bu tanım çerçevesinde iletişim kavramından kasıt, kişiler arasında, kişiyle kurum arasında ya da kurumlar arasındaki etkileşimdir. İnsan davranışlarındaki açıklıklarsa, insanların gündelik sergiledikleri, niyetlerinden bağımsız hareketlerin güvenlik açısından istenmeyen durumlara sebep olması ihtimalleridir.[201]

Sosyal mühendislik kullanılarak hedef kişi ve ya kurumun normal yollarla ulaşılamayacak bilgilerine ulaşılabilmektedir. Sosyal mühendisliği kullanan ilk bilgisayar korsanlarından olan Kevin Mitnick 15 Şubat 1995'te FBI tarafından yakalanmıştır. Büyük şirketlerin bilgisayar ağlarına izinsiz girmekten suçlu bulunarak beş yıl hapis cezası almıştır. Cezası 21 Ocak 2000'de, bilgisayarlara yaklaşma yasağı 21 Ocak 2003'te bitmiştir.[202] Kevin Mitnick, eylemlerini bilişim teknolojilerine hâkim olmasının yanı sıra çok iyi bir sosyal mühendis olması sayesinde yapabilmiştir. Yaptıklarını ve yöntemlerini de "Aldatma Sanatı" isimli kitabında detaylarıyla anlatmıştır. Kitaba göre bilgi güvenliğinin en zayıf halkası insandır ve bilgi güvenliğine yönelik yapılan saldırılarda sosyal mühendislik kullanılarak yani insan unsuru kandırılarak gizli bilgilere ulaşılabilir.[203]

Sosyal mühendislik dört aşamada gerçekleşmektedir. Birinci aşamada kişi hedef aldığı kişi ya da kurumla ilgili bilgi toplar. Daha sonra topladığı bilgilerle birlikte hedefle iletişime geçer ve bu bilgileri de kullanarak hem daha fazla bilgiye ulaşır hem de amacı doğrultusunda kullanabileceği araçları tespit eder. Kişi artık elindekiler sayesinde uygulamaya geçer ve erişmek istediği bilgilere erişir. Son olarak erişilen bilgiler istismar edilerek diğer amaçlara ulaşılabilir. Bu amaçlar bazen ciddi maddi kazançlar olabilir.[204]

---

[201] Bican, Can, (2008), "Sosyal Mühendislik Saldırıları", TUBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=183&Itemid=6, (Erişim Tarihi: 16.11.2010).
[202] wikipedia.org, (2010), "Kevin Mitnick", http://tr.wikipedia.org/wiki/Kevin_Mitnick, (Erişim Tarihi: 16.11.2010).
[203] Mitnick, Kevin D. ve William L. Simon, (2005), *Aldatma Sanatı*, Ankara: Odtü Geliştirme Vakfı Yayıncılık, s.3.
[204] Demir, Nurullah, (2010), "Web Güvenliği", http://www.yeniasya.com.tr/2010/10/12/ilim-teknik/default.htm, (Erişim Tarihi: 16.11.2010).

2.3. SUÇ İŞLEMEK İÇİN BİLİŞİM TEKNOLOJİLERİNİ KULLANANLAR

Bilişim teknolojilerini suç işlemek ve ya illegal eylemler yapmak için kullanan kişilerin sayısı gün geçtikçe artmaktadır. Ancak bu kişileri tek bir başlık altında toplamak ve hepsini aynı isimle etiketlemek mümkün değildir. Bu kişiler teknik seviyeleri, hedefleri, kullandıkları yöntemleri ve daha birçok özellikleri açısından birbirlerinden ayrılmaktadırlar. Suç işlerken bilişim teknolojilerini kullananlar aslında çok geniş bir yelpazenin parçalarıdır.

Bilişim güvenliği literatüründeki terimlerle kamuoyunun ve medyanın kullandığı terimler farklı anlamlar taşımaktadır. Kamuoyunda ve medyada en çok kullanılan tabir olan "hacker" terimi aslında farklı bir anlama gelmektedir. Ancak genel olarak kötü niyetli kişiler için kullanılan "bilişim korsanı" ifadesi hem dünyada hem ülkemizde kabul görmektedir.

2.3.1. Bilişim Korsanları (Hacker) ve Sistem Kırıcılar (Cracker)

"Hacker" ve "cracker" kavramları farklı anlamlarda olmasına rağmen iki kavram birbiri içerisine girmiş bulunmaktadır. Yaygın kullanımına bakıldığında genel olarak bir bilgisayar sistemine izinsiz girme "hacking" ve bu işi yapana da "hacker" denir. "Cracker" ise lisanslı bir yazılımı kıran ve lisansız olarak kullanılmasını sağlayan kişilerdir.[205]

"Bilişim korsanları (hacker)" kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işe adamış kişilerdir. İşletim sistemleri bu kişilerin uzmanlık alanlarına girdiğinden, esas amaçları bu sistemleri daha güvenli bir hale getirebilmek ve açıklarını keşfetmeye çalışmaktır. Asla ama asla kasıtlı olarak bir zarar verme eyleminde bulunmazlar. Test amacıyla yaptıkları iş bir "sistem kırıcı (cracker)" gibi sistemi kırmaya çalışmaktır. Ama sistem kırıcılar gibi amaç içeriden bir şeyler çalmak veya zarar vermek değil onlardan önce savunma mekanizmalarını kontrol altına almaya çalışmaktır. Bilişim korsanları ve sistem kırıcılar niyet açısından birbirlerinden ayrılırlar.[206]

---

[205] Yılmaz, (2005), a.g.e., s.15.
[206] Güven, Mehmet, (2004), "İnternette Güvenlik ve Hacker Cracker Meselesi", Ankara: Grafik Yayınları, s.20.

Aslında bilişim korsanlarının yaptığı eylem olan "hack" etme kelimesi ya da felsefesi sadece bilişim dünyasına has bir yaklaşım olmadığı düşünülmektedir. Sadece bilişim sistemleri değil sosyal sistemler, toplumlar ya da soyut olgular da "hack" edilebilir yani kırılabilir (eksik yönleri ortaya çıkartılabilir) olarak kabul edilmektedir.[207]

Sistem kırıcıların, bilişim korsanlarının kötü niyetli olanları olduğundan bahsetmiştik. Sistem kırıcıları bu niyete iten motivasyonların başında ise kendisine veya başkasına yarar sağlama isteği gelmektedir. Bununla birlikte birisine zarar verme ve bir meydan okuma göstergesi olarak da bu eylemlere girişmektedirler.[208]

Gerçek hayattaki korsanların amaçlarından (maddi fayda sağlama) ve yöntemlerinden (saldırma) yola çıkılarak bilişim dünyasında da "siber korsan" terimi kullanılmaktadır. Siber korsan genel olarak kötü niyetli kişiler için kullanılan bir terim olmasının yanında bilişim dünyasında "korsanlık" telif haklarına yönelik illegal saldırılara denilmektedir. Bu girişimler bazen bilgisayar yazılımlarına olduğu gibi, bazen de filim (VCD, DVD) ve müzik (MP3) materyallerine yönelik olabilmektedir.[209]

Bilişim korsanlarını suç işlemeye iten nedenler arasında, geleneksel olarak bireyleri suç işlemeye götüren nedenlerden farklı bir neden görmek pek mümkün değil. İntikam alma duygusu, güce sahip olma, açgözlülük, şehvet, macera veya "yasak meyveyi tatma" arzusu gibi geleneksel olarak bireyleri suç işlemeye götüren nedenler siber dünyada da geçerlidir. Sistemi kırma eylemlerinin birçoğu macera arayan kişiler tarafından, bilinmeyeni keşfetme güdüsüyle işlenir. Bilişim alanında suç işleyebilmek için gerekli teknolojik bilgi düzeyinin yüksekliği göz önüne alınırsa, karmaşık yapıdaki bilgisayar güvenlik sistemlerine zarar verme yoluyla, suç faillerinin kendilerini ispatlama güdüsü veya bir meydan okuma güdüsü ile hareket ettikleri de unutulmaması gereken bir motivasyondur. Ayrıca aşırı merak, kendini tatmin etme, kendi başına bir şeyleri başarma, kendine güven gibi olumlu bir takım güdülerle sistemi kırma fiili gerçekleştirilebileceği gibi, anti-sosyal kişiliğin dışa

[207] İzTV, "Yeni Çağın "Korsanları": "Hacker"lar" Belgeseli, İzTV, http://www.iztv.com.tr/program.aspx?id=682, (Erişim Tarihi: 20.11.2010)
[208] Sjoholm, Hans, (1997), "What is Cracker?", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html, (Erişim Tarihi: 20.11.2010).
[209] wikipedia.org , (2010), "Copyright infringement", http://en.wikipedia.org/wiki/Computer_pirates, (Erişim Tarihi: 20.11.2010).

yansıması, gerçek yaşamda kendi varlığını kabul ettirememe, dışlanma veya uyumsuzluk gibi nedenler ve bireyin kendini sanal âlemde kabul ettirme güdüleri de bu eylemi yapmaya iten etkenler arasında sayılabilir.[210]

2.3.1.1. Beyaz, Siyah ve Gri Şapkalı Bilişim Korsanı

"Hacker" kelimesinin "cracker" yerine kullanılmasıyla birlikte en azından bütün bilişim korsanlarının aynı kefeye konulmaması için kendi içinde sınıflara ayrılmıştır. Beyaz, siyah ve gri şapkalı bilişim korsanları birbirlerinden net çizgilerle ayırmak her zaman mümkün olmamakla birlikte, niyetleri ve yaptığı eylemlere göre bir ayrıma tabi tutulmaktadırlar. Bununla birlikte bir bilişim korsanı bazen beyaz şapkalı iken sonrasında gri veya siyah şapkalı bilişim korsanı haline gelebilmektedir.

Beyaz şapkalı bilişim korsanları iyi niyetlilerdir. Amaçları zarar vermek değildir ancak güvenlik zafiyetlerini test etmek gibi amaçlarla bilişim sistemlerine saldırabilirler. Beyaz şapkalı bilişim korsanları için "Etik hacker" tabiri de kullanılmaktadır.[211] Etik bilişim korsanları özel eğitimlerle yetiştirilen ve teknik seviyeleri çok yüksek kişilerdir. Bu kişiler kötü niyetli bilişim korsanlarının saldırılarına karşı savunma yapmak ve sorumlu oldukları bilişim sistemlerini öncesinde bu saldırılara karşı hazırlamaktır.[212] İş dünyasından "bilgi (bilişim) güvenliği uzmanı (danışmanı)" olarak isimlendirilen beyaz şapkalı bilişim korsanları genellikle belli bir şirketin ya da kurumun bilişim güvenliğinden sorumlu olurlar. Normal olarak, savunma yapabilmeleri için saldırı tekniklerini de bilmeleri gerekecektir.[213]

Siyah şapkalı bilişim korsanları ise "sistem kırıcılar" olarak tanımlanan grubun mensuplarıdır. Siyah şapkalı bilişim korsanları bilişim teknolojileri alanındaki yetenek ve donanımlarını kötü niyetleri için kullanırlar. Eylemleri büyük ölçüde suç oluşturur ve amaçları maddi çıkar sağlamaktır. Özellikle banka hesaplarına erişerek başka hesaplara para transferi yapmak ve ya bu bilgileri kara

---

[210] Özcan, Mehmet, (t.y.), "Hacker'lar, Teknolojinin Yaramaz Çocukları", http://dosyalar.hurriyet.com.tr/hacker/mozcan.asp, (Erişim Tarihi: 20.11.2010)
[211] wikipedia.org, (2010), "White Hat", http://en.wikipedia.org/wiki/Ethical_Hacking, (Erişim Tarihi: 20.11.2010).
[212] eccouncil.org , (t.y.), "Certified Ethical Hacker", http://www.eccouncil.org/certification/certified_ethical_hacker.aspx, (Erişim Tarihi: 20.11.2010)
[213] Akçay, Bilal, (2010), "Bilişim Güvenliği Uzmanı / Yöneticisi", http://www.bilalakcay.com/wordpress/2008/07/bilgisayar-muhendisi-ne-ith-yapar-bilithim-guvenlidhi/, (Erişim Tarihi: 20.11.2010).

borsada başkalarına satmak, bilişim sistemlerine ve bilgisayar ağlarına illegal erişmek siyah şapkalı bilişim korsanlarının en çok başvurduğu yöntemleridir.[214]

Gri şapkalı bilişim korsanları ise beyaz ve siyah şapkalıların arasında kalmış bir gruptur. Bazen beyaz şapkalı bazen siyah şapkalı gibi davranabilirler. Amaçları zarar vermek veya para kazanmak olmasa da illegal yöntemlerle bilişim sistemlerine müdahale edebilirler. Bilişim sistemlerine illegal olarak müdahale ederek sistemlerin açıklarını tespit ettiklerinde sistemin sorumluları ile para karşılığında bu deneyimlerini ve çözüm önerililerini paylaşmaktadırlar.[215]

2.3.2. Telefon Kırıcı (Phreaker)

Telefon kırıcılar, telefon iletişim teknolojilerinin gelişmesiyle ortaya çıkmıştır. Eylemleri telefon hatlarına illegal olarak erişerek saatlerce ücretsiz görüşme yapmaktır. Bu eylemlerini her zaman ücretsiz konuşma yapmak için değil bazen de telefon hatlarının nasıl bir yapısı olduğunu öğrenmek için de yapmışlardır. Daha sonra telefon hatlarının başka iletişimler için (İnternet, faks … gibi) kullanılmasıyla yaptıkları eylemlerin şekli ve verdiği zararları artmıştır.[216]

2.3.3. Özenti (Lamer)

Özentiler, kendini hacker zanneden fakat sadece önceden yazılmış program veya basit yollarla hacking yapan veya yapmaya çalışan ve bununla övünen kişilere hackerlar tarafından verilen isimdir. Ayrıca lamer, terminolojide zavallı, basit, özenti manasına gelmektedir.[217] Amaçları bilişim sistemlerine yönelik illegal eylemlerden çok bu alanda ün yapmak ve arkadaşları arasında dikkat çekmektir.[218]

Genellikle lamerler lise çağında eğitim gören öğrencilerden oluşmaktadır. Yukarıda belirttiğimiz arkadaş grubunun dikkatini çekme amacı genellikle okul arkadaşlarına yönelik bir tutum olarak karşımıza çıkmaktadır.

---

[214] hackingalert.com, (t.y.), "Black Hat Hackers", http://www.hackingalert.com/hacking-articles/black-hat-techniques.php, (Erişim Tarihi: 22.11.2010).
[215] Harris, Shon, (2008), "Gray Hat Hacking : The Ethical Hacker's Handbook", ABD: The McGraw-Hill, s.74.
[216] tech-faq.com, (t.y.), "Phone Phreaking", http://www.tech-faq.com/phone-phreaking.html, (Erişim Tarihi: 22.11.2010).
[217] turkcebilgi.com , (t.y.), "Lamer", http://www.turkcebilgi.com/lamer/, (Erişim Tarihi: 22.11.2010).
[218] lamerism.com, (t.y.), "Lamerism", http://www.lamerism.com, (Erişim Tarihi: 22.11.2010).

2.3.4. Betik Kerataları (Script Kiddie)

Bilişim korsanı olmamalarına rağmen bazı kaynaklara göre en tehlikeli ve en çok korkulması gereken kişiler bunlardır. Betik kerataları da özentiler gibi bilişim korsanlarına özenirler, fakat özentileri aksine bir miktar bilgi sahibidirler. Betik keratalrı çoğunlukla sistemlere / kişilere saldırmaya, hasar vermeye ve ele geçirdikleri bilgileri kötü amaçlarla kullanmaya çalışırlar. Onlar için bir güvenlik sistemini delmek araç değil, amaçtır. Bilişim korsanlığı dünyasının anarşistleri olarak tanımlanabilirler. Ev kullanıcılarına yapılan basit saldırıların sorumluları genelde betik keratalarıdır. İnternette kolayca bulunabilen çeşitli hazır programları kullanırlar. Başkaları tarafından bir saldırının nasıl yapılacağını adım adım anlatan dokümanları okur ve uygularlar. Kullandıkları programların nasıl çalıştığını anlamazlar ve teknik detayları bilmezler.[219]

2.3.5. Çaylak (Newbie)

"Newbie" kelimesi bir işe ve ya bir okula yeni başlayan çaylak anlamında kullanılan bir terimdir. Bilişim dünyasında da "newbie" terimi bir yazılım diline ve ya bir bilişim teknolojisi alanında yeni olan kişiler için kullanılmaktadır.[220] Bilişim güvenliği alanında da çaylaklar betik keratalrından bir basamak üstte artık kendini öğrenmeye adamış bilişim korsanı adayları olarak adlandırılmaktadırlar.[221]

2.3.6. Eylemci Bilişim Korsanı (Hactivist)

"Hacktivist" terimi "hacker" ve "activist" kelimelerinin bir araya gelmesinden türetilmiştir. Genel anlamda aktivizm, toplumsal değişme ya da politik değişiklik meydana getirmek için kasıtlı bir biçimde yapılan eylem olarak tanımlanabilir. Bu eylem çelişmeli tartışmalarda taraflardan birini desteklemek ya da muhalefet etmektir.[222] Eylemci bilişim korsanları aktivizm eylemlerini bilişim teknolojilerini kullanarak yapanlardır. Politik amaçlar doğrultusunda "sistemi kırma" eylemlerinin

[219] Şumlu, Selim, (2006), "Hacker Dünyası", *PcNet Dergisi*, S.103. (Nisan 2006).
[220] learnthat.com, (t.y.), "Free Definitions : Define newbie. What is newbie?", http://www.learnthat.com/define/view.asp?id=2294, (Erişim Tarihi: 22.11.2010).
[221] Güven, (2004), a.g.e., s.12.
[222] wikipedia.org, (2010), "Aktivizm", http://tr.wikipedia.org/wiki/Aktivizm, (Erişim Tarihi: 22.11.2010).

gerçekleştirilmesidir.[223] Ancak bu eylemler gerçekleştirilirken bilişim teknolojileri araç olabileceği gibi hedef de olabilirler. Bir siyasi partinin internet sayfasına yönelik bir saldırı buna örnek verilebilir.

2.4. TEMEL GÜVENLİK ÖNLEMLERİ

Bilişim bağlantılı suçların mağduru olmamak için öncelikle bu alanda farkındalık çok önemlidir. Bilişim teknolojilerini kullanırken ya da internet ortamından faydalanırken en az gerçek dünyada olduğu kadar dikkatli olmak gerekmektedir. Bireysel ev kullanıcıları dahi özel saldırıların hedef olmasa bile her zaman için bir risk taşımaktadırlar. Bu riski ciddi oranda azaltmak alınacak basit önlemlerle ve duyarlı olmakla mümkündür. Ancak gerekenler yapılmadığında mağdur olmak çok doğal olacaktır.

Ticari kuruluşlar için ise temel güvenlik önemleri yeterli olmayacaktır çünkü onları hedef alanlar bu alanda uzman kişiler olacağından güvenlik önlemlerini de alacak kişilerin bu alanda uzman kişiler olması gerekecektir. Ayrıca kurum içi bir güvenlik politikası geliştirilmesi gerekmektedir.

Kötücül ve casus yazılımlara karşı tedbirli olmak için alınan önlemler bir alışkanlık haline getirilmelidir. İşletim sistemleri ve üzerlerindeki koruma yazılımları güncel tutulmalıdır. Mümkün olduğunca lisanlı yazılım kullanılmalıdır. Yasal olmayan siteler ziyaret edilmemelidir. Her zaman parola kullanılmalıdır ve bu parolalar tahmin edilebilecek be basit olmamalıdır. Umuma açık internet toplu kullanım sağlayıcı mekânlardaki bilgisayarlarda çevrimiçi bankacılık işlemleri gibi önemli işlemler yapılmamalıdır. Çevrimiçi alış veriş güvenilir sitelerden yapılmalıdır. Çocuklar bilgisayar güvenliği ile ilgili bilgilendirilmelidirler. [224]

Bilgisayar virüslerinin zararlı etkilerinden korunmak için özellikle internet sitelerinden indirilen şüpheli programları çalıştırmadan önce bu amaç için geliştirilmiş anti-virüs programları kullanılarak kontrol edilmelidir.[225]

---

[223] thehacktivist.com, (t.y.), "What Is Hacktivism?", http://www.thehacktivist.com/whatishacktivism.pdf, (Erişim Tarihi: 22.11.2010).
[224] Canbek, Gürol ve Sağıroğlu, Şeref, (2006), *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri* , Ankara: Grafiker Yayınları, ss.307-312.
[225] metu.edu.tr, (t.y.), "Bilgisayar Virüsleri", http://www.po.metu.edu.tr/links/inf/css25/bolum14.html, (Erişim Tarihi: 05.11.2010).

Truva atı bulaşan bir bilgisayarda bunun tespiti gerçekten zordur. Tespit edilirse eğer ilk yapılacak işlem çalışan truva atının çalışmasını engellemek ve mümkünse silmektir. Eğer normal yollarla silinemiyor ve ya da bulaştığı dosya silinmemesi gereken bir dosya ise o zaman güncel bir anti virüs programı ile temizlenmelidir.[226]

Arka kapılardan etkilenmemek için öncelikle kullanılan işletim sistemlerinin bütün güncel yamalarının yüklü olması gerekmektedir ve ek olarak güncel durumdaki bir anti virüs programına ihtiyaç vardır. Zararlı yazılımlarda olduğu gibi arka kapılar da İnternetten indirilen programlar, dokümanlar, e-postalar aracılığıyla sistemi etkileyebilirler.[227]

Dünyada yemleme saldırıları sırasıyla en fazla; ödeme sayfalarına, finansal kurumların sayfalarına, açık artırma ve çevrimiçi alışveriş sayfalarına yönelik yapılmaktadır.[228] Hukuk sistemimizde bu eylemler TCK Madde 158/1'e göre "Nitelikli Dolandırıcılık" suçunun konusunu oluşturmaktadır.[229] Bu saldırıların kurbanı olmamak için hassas olunması gereken nokta; "her türlü çevrimiçi dolandırıcılık, sahtekârlık ve virüslere karşı en büyük korunma aracının, bu konuda bilinçli ve bilgili olmak olduğunun" unutulmamasıdır.[230]

2.5. ADLİ BİLİŞİM

En genel tanımıyla adli bilişim (computer forensic) dijital (elektronik) delil elde etme sürecidir. İngilizce bir terim olan "computer forensic" dilimize çevrilirken "adli bilişim" olarak çevrilmekte ve bu şekilde yaygın olarak kullanılmaktadır. Ancak bazı görüşlere göre bunun yerine "bilgisayar kriminalistiği" terimi de kullanılmaktadır. Konuyla ilgili tanımlara bakacak olursak;

---

[226] Lau, Hon, (2002), "Backdoor.Trojan - Removal", http://www.symantec.com/security_response/writeup.jsp?docid=2001-062614-1754-99&tabid=3, (Erişim Tarihi: 10.11.2010).
[227] essentialcomputersecurity.com, (t.y.), "Computer Protection: Backdoors", http://www.essentialcomputersecurity.com/Backdoors.html, (Erişim Tarihi: 13.11.2010).
[228] antiphishing.org, (2010), "Phishing Activity Trends Report", http://www.antiphishing.org/reports/apwg_report_Q1_2010.pdf, (Erişim Tarihi: 14.11.2010).
[229] Koç, Serhat, (2009), "Phishing ile Kredi Kartı Bilgisi Hırsızlığı ve TCK'daki Yansıması", http://www.hukukcu.com/modules/smartsection/item.php?itemid=285, (Erişim Tarihi: 14.11.2010)
[230] guvenliweb.org.tr , (2009), "Phishing", http://www.guvenliweb.org.tr/guvenlik/content/phishing, (Erişim Tarihi: 14.11.2010).

Adli bilişim, yargıya intikal etmiş bir olayla ilgili olarak potansiyel kanuni delillerin belirlenmesi için bilgisayar soruşturması ve analiz tekniklerinin bir uygulamasıdır.[231]

Adli Bilişim; elektromanyetik-elektro optik ortam(lar)da muhafaza edilen ve/veya bu ortamlarca iletilen; ses, görüntü, veri/bilgi veya bunların birleşiminden oluşan her türlü bilişim nesnesinin, mahkemede sayısal (elektronik-dijital) delil niteliği taşıyacak şekilde: Tanımlanması, elde edilmesi, saklanması, incelenmesi ve mahkemeye sunulması çalışmaları bütünüdür.[232]

Adli bilişim, elektronik ortamlardan elde edilen bulguların, çeşitli teknik donanım ve yazılımlar kullanılarak hukuki delillere dönüştürülme süreci olarak tanımlanabilir. Bu yönüyle adli bilişimin hukuki boyutundan ziyade, teknik yönü ön plana çıkmaktadır. Zira elektronik sistemlerdeki bulguların, bunlardan ayrıştırılarak birer hukuki delile dönüştürülme süreci, oldukça zahmetli, son derece teknik bilgi gerektiren ve uzmanlık isteyen bir iştir.[233]

Adli Bilişim (Computer Forensics), bilişim öğeleri kullanılarak işlenen suçların adli kurumlar tarafından aydınlatılabilmesi için bilimsel yöntemler kullanılarak, çeşitli sayısal medyalar üzerinde bulunan, suçla ilgili sayısal delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan bir delil inceleme disiplinidir. E-keşif ise, bilgisayar ve diğer teknolojik cihazlardan hukuk sürecinde kullanılacak bilgilerin toplanmasıdır.[234]

Yukarıdaki tanımlar incelendiğinde adli bilişimin dijital (elektronik, sayısal) deliller üzerine kurulmuş bir disiplin olduğunu görmekteyiz. Bu nedenle adli bilişim sürecine değinmeden önce dijital (elektronik, sayısal) delil kavramının ne olduğunu detaylarıyla ortaya koymak gerekmektedir.

---

[231] sayisaldelil.net, (t.y.), "Adli Bilişim", http://sayisaldelil.net/?page_id=19, (Erişim Tarihi: 30.11.2010).
[232] Koltuksuz, (2007), a.g.e., s.43.
[233] Tan, Aydoğan, (2010), "Adli Bilişim (Computer Forensic)", http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html, (Erişim Tarihi: 30.11.2010).
[234] e-kesif.com, (t.y.), "E-Keşif ve Adli Bilişim", http://www.e-kesif.com/2008/05/adli-bilisim-nedir.html, (Erişim Tarihi: 30.11.2010).

2.5.1. Dijital (Elektronik, Sayısal) Deliller

Sözlük anlamına göre delil "insanı aradığı gerçeğe ulaştırabilecek iz, emare" olarak tanımlanmaktadır. Hukuk literatüründe ise uyuşmazlığa neden olan fiilin veya olgunun suç olup olmadığı konusunda kolluk, savcı veya yargıcın bir kanaate varmasını sağlayan, bir hukukî ihtilafı çözmeye yarayan ve ikamesi hukuk tarafından yasaklanmamış her şeye delil denilmektedir. Taraflar bakımından "ispat", hâkim bakımından "sabit görme", maddî husus bakımından "sübut" denilen faaliyetler için kullanılan vasıtalara "ispat vasıtası" veya kısaca delil denir.[235]

Dijital delil, dijital ortamlarda sayısal olarak bulunan ispatlayıcı özelliği bulunan anlamlı bilgi olarak, tanımlanmaktadır.[236]

Dijital deliller temel delil şartlarının sağlamanın yanında suça delil niteliği sağlayan ve mahkemelere sunulabilecek dijital veri saklayabilen ve/veya elektronik devre akımları ile çalışan disk, disket, CD, bilgisayarlar, cep telefonları, PDA cihazları, taşınabilir bellekler, sim kartlar, bir bilgisayara ait dahili ve harici donanımlar gibi çeşitli elektronik cihazlardır. Elektronik cihaz oldukları için "elektronik delil" kavramı da kullanılmaktadır.[237]

Dijital delil, bilişim sistemlerinin veya bilgileri otomatik olarak işleme tabi tutma yetisine sahip elektronik cihazların veri depolama medyaları üzerinde bulunan, suç ile ilgili delil niteliği taşıyabilecek ve suçun aydınlatılmasını sağlayacak elektronik verilerdir.[238]

Elektronik deliller, elektronik cihazlarda depolanan ve ya iletişim halinde olan, suç soruşturması açısından değeri olan bilgi ve ya veridir. Elektronik deliller de DNA ve parmak izi gibi gizli delillerdir. Doğal olarak içinde bulundukları fiziksel ortamları görebiliriz. Bu delilleri görünür hale getirmek için bazı donanım ve yazılımlara ihtiyaç duyulmaktadır. Dijital deliler yapıları gereği hassastırlar ve

---

[235] Demirkaya, Vural, (2009), *Delil Güvenliği*, Polis Akademisi Güvenlik Bilimleri Enstitüsü Yayınlanmış Yüksek Lisans Tezi, Ankara, s.6.
[236] swgde.org, (2009), "Digital Evidence", WGDE/SWGIT Digital & Multimedia Evidence Glossary, http://www.swgde.org/documents/current-documents/2009-05-22 SWGDESWGIT Digital Multimedia Evidence Glossary v2.3.pdf, (Erişim Tarihi: 30.11.2010).
[237] Dokurer, Semih, (2008), *Adli Bilişim, Ses Görüntü ve Data İncelemeleri*, Ankara: Adalet Yayınevi, s.141.
[238] Ekizer, A. Hakan, (2007), "Adli Bilişim", http://ekizer.net/index.php?option=com_ content&task=view&id=16&Itemid=1, (Erişim Tarihi: 30.11.2010).

değişmeye, bozulmaya ya da yok olmaya açıktırlar. Bu nedenlerle diğer delillerden ayrılmaktadırlar.[239]

2.5.1.1. Dijital Delilerin Bulunduğu Ortamlar

Dijital deliller, birçok tipte karşımıza çıkmaktadır. Bunlar veri dosyaları, kurtarılmış silinmiş dosyalar, kayıp alanlardan kurtarılmış veriler, dijital fotoğraf ve videolar, sunucu kayıtları, e-posta, internet geçmişi, internet sayfaları, abone kayıtları gibi doğrudan bilgisayar sistemleriyle alakalı deliller olabileceği gibi, günümüzde gömülü bilgisayar sistemlerine sahip bir mikro dalga fırından elde edilebilecek ve bir kundakçılık olayında fırının belirli bir zamanda yangın çıkarmak için programlandığını ortaya çıkarabilecek veriler de dijital deliller olarak karşımıza çıkmaktadır.[240]

Dijital delilerin bulunabileceği donanımlara bakacak olursak;

- Bilgisayarlar, monitörler ve diğer çevre birimleri
- Sabit ve taşınabilir diskler
- Hafıza (ram)
- Disketler, CD vd DVD ler
- Usb bellekler
- Manyetik teypler
- RFID çipleri
- Cep telefonları ve cep bilgisayarları
- Smart kartlar, hafıza kartları
- Tarayıcılar, yazıcılar
- Fax ve fotokopi makineleri
- Dijital telefonlar
- Ses kaydedici ve medya oynatıcı cihazlar
- Fotoğraf makineleri ve kameralar
- Ağ iletişim cihazları (modem, switch, firewall … gibi)

[239] US Department of Justice – National Instute of Justice, (2001), "Electronic Crime Scene Investigation – A Guide For First Responders", http://www.ncjrs.gov/pdffiles1/nij/187736.pdf, (Erişim Tarihi: 30.11.2010).
[240] Uzunay, Yusuf ve Bıçakçı, Kemal, (t.y.), "A3D3M : Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", http://www.emo.org.tr/ekler/4843973f9b66701_ek.pdf, (Erişim Tarihi: 30.11.2010).

– E-kitap okuma cihazları

Bu donanımlar günümüz teknolojisine göre belirlenmektedir ancak gelişen ve değişen teknolojiye göre dijital verileri muhafaza eden veya ileten donanımların sayısının artması doğaldır. Dijital delil elde etme sürecinde de bu gelişmeler yakından takip edilmelidir. Örneğin 3G teknolojisinin kullanılmaya başlanmasıyla birlikte 3G modemler dijital delil ihtiva eden cihazlar listesine girmiştir. Bu nedenle suç soruşturmasında 3G modemle karşılaşıldığında dijital delillerin elde edilebilmesi için hazırlıklı olunması gerekmektedir.

2.5.1.2. Dijital Deliller ve Olay Yeri

Bir suç işlenirken bilişim cihazları kullanılmışsa, olay yeri incelemesinde öncelikle temel olay yeri prensiplerine uyulmalıdır. Bu prensipler yapılması gerekenler ve yapılmaması gerekenler olarak ikiye ayrılabilir. Yapılması gerekenler;[241]

- Güvenlik ve sağlık tedbirleri alınmalıdır.
- Devam eden olaya müdahale edilmelidir.
- Olay derhal genel kolluk birimine iletilmelidir.
- Yaralılar sağlık kuruluşuna sevk edilmelidir.
- Olayın failleri olay yerindeyse yakalanmalı ve muhafaza edilmelidir.
- Olay yerinde bulunan sanık ve tanıklar belirlenmelidir.
- Olay yeri şeritle çevrilmelidir.
- Olay yeri kapalı alan ise kapı kilitli tutulmalıdır.
- Olay yerinde kalabalık uzaklaştırılmalıdır.
- Desteğe ihtiyaç varsa yardımcı ekip çağırılmalıdır.
- Olay yerinden ayrılan mağdur ve şüphelilerin kimlik ve eşkâlleri belirlenmelidir.
- Mağdur ve faillerin nereye gönderildiklerini ve ya kaçtıkları ilgililere bildirilmelidir.
- Olay yerinde görev alan uzman personelin görevi bitince olay yerinden çıkması sağlanmalıdır. (ilk yardım görevlisi, bomba uzmanı vb.)
- Olay yerine girilecekse eldiven ve galoş giyilmelidir.
- Delillerin yeri değişmişse uzman ekibe bilgi verilmelidir.
- Savcının, soruşturmacının veya uzman ekibin gelmesi beklenmelidir.

[241] Erdoğan, Mustafa, (2009), "Olay Yeri Güvenliği Ve Olay Yerinin Korunması", Olay Yeri İnceleme [Ders Notları], Güvenlik Bilimleri Enstitüsü, Ankara.

- Olay yerinde bulunan kişiler ve yaptıkları kayıt altına alınmalıdır.

Bilişim bağlantılı bir suçta olay yerinde yukarıda belirtilen prensiplere uyulmasının yanı sıra bazı özel durumlara dikkat edilmelidir. Bir önceki başlıkta dijital delillerin nerede bulunacağından bahsetmiştik. Olay yerinde dijital delillerin bulunacağı ortamların başında bilgisayarlar gelmektedir. Bu nedenle ilk müdahale esnasında yapılacaklar bilgisayarların durumlarına göre değişmektedir. Olay yerine müdahale esnasında beş farklı durumla karşılaşılabilir ve bilgisayarın açık veya kapalı olmasına göre izlenecek süreçler standart bir prosedüre bağlanmıştır. Bunlara sırasıyla bakacak olursak;[242]

Durum 1: Monitör açık ve ekranda internet sayfaları, e-posta hesapları gibi o anda çalışan uygulamalar mevcut ise;

- Ekran görüntüsü fotoğraflanır ve ekranda görünenler dokümante edilir.
- Bilgisayar açıkken yapılması gereken diğer işlemler yapılır.

Durum 2: Monitör açık ve ekranda ekran koruyucu veya bir resim görüntüsü mevcut ise;

- Yavaşça fare hareket ettirilir ancak tuşlara ve kaydırma düğmesine dokunulmaz.
- Ekranda bir değişiklik olursa not edilir.
- Ekran görüntüsü fotoğraflanır ve ekranda görünenler dokümante edilir.
- Bilgisayar açıkken yapılması gereken diğer işlemler yapılır

Durum 3: Monitör açık ancak ekran siyah ise;

- Yavaşça fare hareket ettirilir ancak tuşlara ve kaydırma düğmesine dokunulmaz.
- Giriş ekranı veya başka bir uygulama çalışacaktır.
- Ekrandaki değişiklikler not edilir.
- Ekran görüntüsü fotoğraflanır ve ekranda görünenler dokümante edilir.

[242] US Department of Justice – National Instute of Justice, (2001), "Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders", http://www.ncjrs.gov/pdffiles1/nij/227050.pdf, (Erişim Tarihi: 01.12.2010).

- Bilgisayar açıkken yapılması gereken diğer işlemler yapılır

Durum 4a: Monitör kapalı ve ekran siyah ise;

- Monitör tuşu kapalı konumda ise açık konuma getirilir.
- Giriş ekranı veya başka bir uygulama çalışacaktır.
- Ekrandaki değişiklikler not edilir.
- Ekran görüntüsü fotoğraflanır ve ekranda görünenler dokümante edilir.
- Bilgisayar açıkken yapılması gereken diğer işlemler yapılır

Durum 4b: Monitör kapalı ve ekranda hiçbir şey görünmüyorsa;

- Monitör tuşu kapalı konumda ise açık konuma getirilir.
- Giriş ekranı veya başka bir uygulama çalışmayacaktır.
- Ekranda bir değişiklik olmadığı not edilir.
- Boş ekran fotoğraflanır.
- Bilgisayar kapalıyken yapılması gereken diğer işlemler yapılır.

Durum 5: Monitör açık ve ekran siyah ise;

- Yavaşça fare hareket ettirilir ancak tuşlara ve kaydırma düğmesine dokunulmaz.
- Ekranda bir değişiklik olmazsa ekranın elektrik kaynağına bağlı olup olmadığı kontrol edilir.
- Ekran halen siyah durumda ise bilgisayar kasasının ışıklarının yanıp yanmadığına ve bilgisayar fanının çalışıp çalışmadığına bakılır.
- Bilgisayarın kapalı olduğu anlaşıldıktan sonra bilgisayar kapalıyken yapılması gereken diğer işlemler yapılır.

2.5.1.2.1. Bilgisayar Kapalı İse Yapılması Gerekenler

Olay yerinde müdahale edilen bilgisayar **masaüstü**, **mini masaüstü** veya **sunucu** bilgisayar ise;

1. Bilgisayara bağlı olan bütün kablolar ve çevre birimleri, fotoğraflanır, dokümante edilir ve şeması çizilir.
2. Bilgisayara bağlı bütün kablolar ve usb bellekler gibi modüler parçalar numaralandırılarak etiketlenir ve fotoğraflanır.
3. Elektrik kabloları ve uzatma prizleri bilgisayardan ve duvardan sökülür.
4. Data kabloları ve usb bellekler sökülerek, söküldükleri yerlere göre karşılıklı numaralandırılır ve etiketlenirler.
5. Eğer disket okuyucu varsa girişi bantlanır. CD ve DVD okuyucuların içi boş olduğundan emin olduktan sonra onlar da bantlanır.
6. Kasanın açma kapama düğmesi açık konuma getirilmemesi için bantlanır.
7. Bilgisayarın marka, model ve seri numarası not edilir. Ayrıca kullanıcısı tarafından bilgisayar üzerine yazılmış veya etiketlenmiş bir işret varsa not edilir.
8. Bilgisayar, çevre birimleri ve bütün kablolar mevzuata uygun olarak mühürlenir.
9. Bütün deliller taşınma ve muhafaza esnasında bozulmaması için dikkatlice paketlenir.

Olay yerinde müdahale edilen bilgisayar **dizüstü** bilgisayar ise;

1. Bilgisayara bağlı olan bütün kablolar ve çevre birimleri, fotoğraflanır, dokümante edilir ve şeması çizilir.
2. Bilgisayara bağlı bütün kablolar ve cihazlar etiketlenip fotoğraflanır.
3. Şarj cihazı ve pil dikkatlice bilgisayardan ayrılır ve güvenli bir yere konur.
4. Bütün kablolar ve cihazlar sökülerek, söküldüğü yerle karşılıklı olarak etiketlenir ve dokümante edilir.
5. Eğer disket okuyucu varsa girişi bantlanır. CD ve DVD okuyucuların içi boş olduğundan emin olduktan sonra onlar da bantlanır.
6. Açma kapama düğmesi bantlanır.

7. Bilgisayarın marka, model ve seri numarası not edilir. Ayrıca kullanıcısı tarafından bilgisayar üzerine yazılmış veya etiketlenmiş bir işret varsa not edilir.
8. Bilgisayar, çevre birimleri ve bütün kablolar mevzuata uygun olarak mühürlenir.
9. Bütün deliller taşınma ve muhafaza esnasında bozulmaması için dikkatlice paketlenir.

2.5.1.2.2. Bilgisayar Açık İse Yapılması Gerekenler

Genel olarak kabul edilen yöntem hemen bilgisayarın fişinden çekilerek kapatılmasıdır ancak bazı durumlarda bu uygulanmaz. Bilgisayarın kapatılmaması gereken durumlar ve izlenmesi gereken prosedürü bir önceki konuda bahsetmiştik.

Bilgisayarın hemen fişi çekilerek kapatılması gereken durumlar;

- Ekranda bilgisayardaki bazı verilerin silindiğine ve ya kopyalandığına işaret eden görüntüler varsa.
- Bilgisayarın diskine yönelik zarar verici bir aktivitenin olduğuna yönelik belirtiler varsa.
- Eğer bilgisayar Microsoft Windows tabanlı bir iletim sistemi çalıştırıyorsa bilgisayarı fişinden çekerek kapatmak, en son bilgisayarı kullanan kullanıcıyı, sisteme giriş zamanını, en son kullanılan doküman ve komutları ve daha birçok değerli bilginin saklanmasını sağlayacaktır. Bu bilgiler adli bilişim süreci açısından çok önemli olduğu için bilgisayar fişi çekilerek kapatılmalıdır.

Bilgisayarın hemen fişi çekilerek kapatılmaması gereken durumlar;

- Ekranda delil niteliği taşıyabilecek görüntüler varsa.
- Ekranda sohbet sayfası açıksa, metin dokümanı açıksa, uzak veri tabanı bağlantısı varsa, anında mesajlaşma programı açıksa, çocuk pornografisi veya kaçakçılık ile ilgili bir sayfa varsa, finansal dokümanlar açıksa, veri kriptolama veya açıkça bir illegal aktivite varsa.

- Müdahale edilen cihaz mobil cihaz veya cep telefonu ise kapatılmadan bulunduğu durumda muhafaza edilmelidir.
- Gelişmiş bilgisayarlarda, sunucu sistemlerde veya ağ iletişim cihazlarında fişin çekilerek kapatılması ciddi veri kayıplarına yol açabilir. Bu tür durumlarda bu sistemlerin uzmanları tarafından ilk müdahale yapılmalıdır.

2.5.1.3. Dijital Delilerin Muhafazası ve Taşınması

Yapısı gereği dijital delileri ihtiva eden ortamların çok hassas olduğunu ve bozulmaya, değişmeye ve yok olmaya müsait olduğundan bahsetmiştik. Bu nedenle el konulan eşyanın türüne göre muhafaza etme ve taşıma prosedürleri vardır. El konulan eşyanın türüne göre dikkat edilmesi gereken noktalar şunlardır.[243]

- Bilgisayar kasaları dikkatle taşınmalıdır. Arabaya dik olarak sarsıntılar etkilenmeyecek şekilde yerleştirilmelidir. Arabanın hoparlörleri, ısıtma sistemi, pencereden, polis telsizi gibi manyetik alanlardan uzak tutulmalıdır.
- Monitörler arabanın arka koltuğunda kırılgan yüzeyleri yumuşak yüzeye gelecek şekilde taşınmalıdır.
- Sabit diskler manyetik alanlardan korunması gereken en hayati eşyalardır. Anti statik poşetlerle taşınmalıdır ya da kalın karton içinde veya havalı poşetle de taşınabilir.
- Disketler, hafıza kartları, usb bellekler, CD ler de manyetik alanlardan uzak tutulmalıdır. Kesinlikle bükülmemelidir. Disketler ve CDlerin üzerine direkt olarak etiket yapıştırılmamalıdır.
- Cep bilgisayarları ve mobil cihazlar manyetik alandan uzak tutulmalıdır.
- Klavye, fare, modem gibi aygıtlar plastik poşetlerde üzerinde ağır bir şey olmayacak şekilde taşınmalıdır.
- Bütün eşyalar DNA ve parmak izine yönelik olarak korunmalıdır.

[243] ACPO Association of Chief Police Officers - E-Crime Working Group and Metropolitan Police Service, (t.y.), "Good Practice Guide for Computer-Based Electronic Evidence", , http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf, (Erişim Tarihi: 01.12.2010).

- Parmak izi tespiti için alüminyum tozu kullanılmamalıdır çünkü alüminyum tozu elektronik cihazlara zarar verebilmektedir.
- Tüm eşyalar oda sıcaklığında ve normal nemli ortamda tutulmalıdır. Fazla veya çok az sıcaklık ve nem el konulan eşyalara zarar verebilir.
- Bilgisayar kasasında piller sayesinde bazı bilgiler yongalarda saklanır. Bu bilgilere ulaşmak için piller bitmeden müdahale edilmelidir.

2.5.2. Adli Bilişim Süreci

Adli bilişim (dijital delil elde etme) sürecine yönelik farklı yaklaşımlar geliştirilmiştir. Temelde birbirine yakın yaklaşımlar olmanın yanı sıra izlenecek yöntemler farklı aşamalarda tanımlanmıştır.

Dijital delilleri belirli metot ve prosedürlere uyun olarak araştırabilmek için bir takım ortak süreçlere ihtiyaç duyulmaktadır. Bu süreçlerden birisi de on iki basamaklı dijital delil araştırma süreç modelidir.[244] Bu modeldeki basamaklar sırasıyla; **1. vaka alarmı ve suçlama** (sürecin başlaması için gerekli olan hukuki durum), **2. değer değerlendirmesi** (genel olarak problemin önemi belirlenmeye çalışıldığı aşama), **3. olay/suç yeri protokolleri** (bir hataya sebebiyet verilmemesi için ilgili protokoller ve prosedürler tespit edilir), **4. tanımlama ve toplama** (söz konusu suç veya vaka ile ilgili potansiyel delillerin toplanması), **5. koruma** (delillerin muhafazası), **6. kurtarma** (silinmiş, gizlenmiş, şekli değiştirilmiş veya mevcut işletim sistemi veya dosya sistemi ile görüntülenemeyen verilerin ortaya çıkarılması), **7. ayrıştırma** (verilerin türlerine göre ayrılmasıdır), **8. indirgeme** (anlam ifade eden verilerin diğerlerinden ayrılmasıdır), **9. organizasyon ve araştırma** (bir önceki basamakta indirgenmiş verileri organize etmek, gruplamak, etiketlemek ve anlamsal birimlere yerleştirme işlemidir), **10. analiz** (önceki aşamalarda elde edilen verilerin ayrıntılı bir şekilde incelenmesidir), **11. raporlama** (yapılan çalışmaların ve elde edilen bulguların raporlanması), **12. ikna etme ve tanıklık** (adli makamlar önünde rapordaki bulguların sunulması ve ilgili sorulara yanıt verilmesi).

[244] Uzunay, Yusuf, (2002), "Dijital Delil Araştırma Süreci", http://www.caginpolisi.com.tr/50/14-15-16-17-18.htm, (Erişim Tarihi: 01.12.2010).

Diğer bir yaklaşımda adli bilişim süreci altı basamakta sıralanmıştır.[245] Bu yaklaşıma göre sırasıyla yapılması gerekenler; **1. olay yeri güvenliği sağlanır** (dijital delillerin bulunduğu ortam ve delillerin güvenlik altına alınmasıdır), **2. delillerin toplanması** (korunan ortamlardan delillerin elde edilmesidir), **3. tanıklara mülakat yapılması** (dijital delillerin tespit edilebilmesinden önce ne aranacağının bilinmesi için bilgi toplanır), **4. önceden tespit edecek sistemlerin tesis edilmesi** (suç işlenmeden önce saldırı tespit sistemlerinden elde edilen veriler), **5. laboratuar aşaması** (toplanan delillerin laboratuar ortamında analizidir), **6. raporlama** (bulguları yetkililere iletme işlemi).

Başka bir adli bilişim metodolojisi beş basamaktan meydana gelmektedir.[246] Bu basamaklar sırasıyla; **1. delil kaynaklarının belirlenmesi** (dijital delil elde edilebilecek ortamlar ve aygıtlar tespit edilir), **2. koruma** (delillerin muhafazası), **3. ortaya çıkarma** (delil niteliği olan veriler tespit edilir), **4. inceleme** (verilerin analiz edilmesidir), **5. raporlama** (elde edilen bulguların adli makamlara iletilmesidir).

Dijital soruşturma standart uygulama prosedürüne göre adli bilişim süreci farklı beş basamakta değerlendirilmiştir.[247] Bu basamaklar sırasıyla; **1. hizmet talebi** (dijital delil elde etme yöntemlerinin kullanılması için bir suç oluşması ve adli olarak harekete geçilmesi), **2. ön analiz** (delil toplanabilecek yerlerin tespiti ve hazırlık), **3. veri toplama** (delil niteliği olabilecek verilerin toplanmasıdır), **4. veri analiz** (toplanan verilerin analiz edilmesi aşamasıdır), **5. veri raporlama** (elde edilen bulguların ilgili birimlere rapor edilmesidir).

Yukarıdaki yaklaşımlar incelendiğinde adli bilişim sürecinin aslında dört ana basamakta gerçekleştiğini görmekteyiz.[248] Bunlar sırasıyla; **1. elde etme** (acquisition), **2. tanımlama** (identification), **3. değerlendirme** (evaluation), **4. sunum** (presentation). Bazı yaklaşımlarda bu basamaklar kendi içinde de alt basamaklara ayrılmışlardır ancak genel olarak adli bilişim sürecinin incelenmesi ve

---

[245] Middleton, Bruce, (2002), *Cyber Crime Investigator's Field Guide*, ABD: Auerbach Publications, s.16.
[246] Gordon , Gary R. ; Hosmer , Chet D. ; Siedsma , Christine ve Rebovich, Don, (2003), "Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime", U.S. Department of Justice, s.42.
[247] Kleiman, Dave, (2007), *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators*, ABD: Syngress Publishing, s.36.
[248] Kateeb, Bassel ve Altimus, Tim, (t.y.), "Computer Forensics", http://www.sis.pitt.edu/~jjoshi/TELCOM2813/Spring2005/FinaleKateebAltimus.ppt, (Erişim Tarihi: 02.12.2010).

prosedürün standart hale getirilmesi için en azından bu dört basamağın ayrı ayrı incelenmesi yeterli olacaktır.

2.5.2.1. Elde Etme (Acquisition)

Elde etme aşaması önceki konularda bahsedilen dijital delillere yönelik olay yeri çalışmaları ile başlar. Dijital delil muhteva etmesi muhtemel bilişim cihazlarına standart kurallara göre müdahale edilir ve delillerin bozulmaması ve değişmemesi için özel bir muhafaza ve taşıma prosedürü uygulanır. El konulan eşyalar inceleme yapmak için laboratuara getirildikten sonra mühürleri açılır ve veri elde etmek için ilk müdahaleler yapılır.

Delil ihtiva etmesi muhtemel bilgisayar sistemleri üzerindeki incelemeler, sistemin veri depolama birimlerinin birebir alınmış kopyaları üzerinde gerçekleştirilmelidir. İnceleme için alınan birebir kopyaya adli bilişimde "**imaj** (Forensic Image)" adı verilmektedir. Kopya yani imaj alma işlemi, incelemeye tabi hedef sistem üzerindeki verilerin bit bazında kopyalanması ile gerçekleştirilmelidir. Sistem üzerindeki verilerin sektör sektör birebir yansısının alınması yani düşük seviyede kopyalanması ancak geçerli bir imajın alınması anlamına gelmektedir. Çeşitli kopyalama yazılımları ile yapılan kopyalarda sadece sistem üzerinde var olan dosyalar kopyalama işlemine tabi tutulduğu için geçerli bir imaj alma söz konusu değildir. Düşük seviye bit bazında kopyalamada sistem üzerinde veri depolama biriminin sektör bazında yansısı alındığı için, veri depolama birimi üzerindeki boş veri alanları, silinmiş veri alanları ve disk yapısı olduğu gibi klonlanmaktadır.[249]

Bu klonlama işleminde en çok dikkat edilmesi gereken konu delillerin bozulmamasıdır. Veri depolayan donanımlara yönelik bütün müdahaleler "yazma koruma (write block)" yönteminin kullanılmasıyla yapılmalıdır. Yazma koruma işlemi kopyası alınacak disk veya benzeri donanımın üzerindeki verilere hiçbir müdahale edilmeden sadece veri okuma işlemi yapılarak imaj alınmasını

[249] Ekizer, A. Hakan, (2007), "Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği.)", (http://ekizer.net/index.php?option=com_content&task=view&id=16&Itemid=1, Erişim Tarihi: 02.12.2010).

sağlayacaktır. Bunun için yazılımsal çözümler kullanılsa da her zaman için tavsiye edilen yöntem donanımsal çözümlerdir.[250]

İmajı alınan donanımın delil niteliğinin bozulmadığı ve elde edilen imaj dosyasının kesinliği "hash değeri"[251] hesaplanarak ortaya konur. Hash değeri hesaplama işlemi belli bir verinin belli bir algoritmaya göre verdiği sonuçtur. Bu sonuç verideki en ufak bir değişiklikte değişecektir ve elde edilen sonuç benzersizdir (unique). İmajı alınan donanımdaki bütün verilerin hash değeri, imaj dosyasının hash değeri ile eşleştiğinde delil bütünlüğünden ve doğrulamasından bahsedilebilir.

2.5.2.2. Tanımlama (Identification)

Bu safhada öncelikle yapılması gerekenler planlanır. Bu planlama bahse konu olayın iyi anlaşılması ve nelerin arandığının net bilinmesi ile başarılı olur. Nelerin aranacağını bilen uzman bundan sonra arayacağı verileri nerede arayacağını tespit etmelidir. Örneğin bir e-posta görüşmesini arıyorsa bunun bilgisayarın diskinin neresinde saklandığını bilmelidir.

Bir önceki safhada bahsedilen elde etme işleminde aslında ham veriler elde edilmiştir. Tanımlama safhasında bu ham verilerin mümkün olduğu kadar tamamı anlamlı verilere dönüştürülür. Burada silinmiş veya diskin kullanılmayan alanlarında artık olarak kalmış veriler üzerinde de çalışılır. Tabi ki bu teknik işlemi gerçekleştirebilmek için özel donanım ve yazılımlar kullanılır. Ham verilerin anlamlı verilere dönüştürülmesinden sonra (örneğin dağınık halde olan verilerin bir araya getirilerek yarısı belli olan bir resim dosyası elde edilmesi gibi) elde edilen veriler türlerine göre sınıflandırılmalıdırlar. Bu sınıflandırma bütün safhanın başarılı olması için önemlidir.[252]

Tanımlama aşamasında uzman tarafından yapılan araştırmada belli prosedürler standart olarak uygulanmaya çalışır. Bunlara bakacak olursak;[253]

---

[250] forensicswiki.org, (2010), "Write Blockers", http://www.forensicswiki.org/wiki/Write_Blockers, (Erişim Tarihi: 02.12.2010).
[251] accuhash.com, (t.y.), "What is Checksum?", http://www.accuhash.com/what-is-checksum.html, (Erişim Tarihi: 02.12.2010).
[252] King, Gerard L., (2006), "Forensics Plan Guide", SANS Institute, http://www.giac.org/certified_professionals/practicals/gcfa/283.php, (Erişim Tarihi: 02.12.2010)
[253] Palmer, Adrian T.N., (t.y.), "Computer Forensics: The Six Steps", Kroll Ontrack Computer Forensics, http://www.krollontrack.co.uk/publications/UK EE Newsletter I1 V3 AP CF.pdf, (Erişim Tarihi: 02.12.2010), s.2-3.

- İnternet ve e-posta kayıtları gibi kullanıcının en son yapmış olduğu işlemler tespit edilerek belli bir sıralamada şema oluşturulur.
- Planlama aşamasında olayla ilgili aranacak "anahtar kelimeler" ve "önemli tarihler" elde edilen veriler içerisinde aranır.
- Elde edilen önemli doküman dosyalarının önceki versiyonları aranır.
- Elde edilen önemli dosyaların erişim, değiştirme ve oluşturma tarih ve saatleri incelenir.
- Elde edilen önemli dosyaların el konulan bilgisayarda mı üretildiği yoksa başka bir yerden mi kopyalandığı incelenir.
- İnceleme esnasında en çok karşılaşılan ve yoğun olarak gözlenen durumlar tespit edilir.

2.5.2.3. Değerlendirme (Evaluation)

Bu safhada artık elde edilen delillerden hangilerinin suçu aydınlatmada kullanılacağı ve hangilerinin adli makamlara sunulacağına karar verilir. Bazı kaynaklarda bu safha tanımlama safhasındaki analiz işlemleri içinde değerlendirilmiştir. Çünkü bu safhadaki işlemlerde bir tür analiz işlemidir ancak çok spesifik olarak bahse konu olayla bağlantılı deliller tespit edilirler. Aslında uzmanın ne kadar uzman olduğu ve soruşturmacı kimliği bu safhada kendisini gösterir. Birçok adli bilişim uzmanı elde ettiği veriler üzerinden analiz yapabilir ancak deneyimli olanları değerlendirme sürecinde başarılı olabilirler.[254]

Değerlendirme aşamasında yapılan analizlere bakacak olursak;[255] **İçerik analizi:** Tespit edilen veriler içinden belirlenen anahtar kelimelere göre içeriğin taranması, eşleştirme ve "serbest metin" analiz tekniklerini ifade etmektedir. **Görsel analiz:** İnsanların resim, video, çizelge gibi görsel materyalleri görsel olarak yorumlama ve anlama melekelerinin, aynı içerikteki metin açıklamalarını

[254] ACPO Association of Chief Police Officers, Natioanal High Tech Crime Unit, (t.y.), "Good Practice Guide for Computer Based Electronic Evidence V. 3.0", http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, (Erişim Tarihi: 02.12.2010).

[255] Öztürk, Mustafa İlker, (2007), *Bilişim Cihazlarındaki Sayısal Delillerin Tespiti Ve Değerlendirilmesinde İş Akış Modelleri*, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara, ss.80-88.

okumaktan daha yüksek olduğu gerçeğinden hareketle olay ve olaya ait tüm maddi unsurların bir ekranda görsel motiflerle ifade etme tekniğine dayanmaktadır. **Mükerrerliklerin tespiti ve eşleştirme**: Bazen gereksiz verilerin temizlenmesi, bazı durumlarda da aynı tür verilerden gizli ilişkilerin tespit edilmesi maksadıyla bu teknik kullanılmaktadır. **İlişki analizi:** Özellikle telefon görüşmeleri ve mali kayıtların incelemesinde sıklıkla kullanılan bir yöntemdir. **Küme analizi:** Yığın veriler içerisinden yoğunlaşan ilişkilerin tespit edilmesi, bağlantı veya düğüm noktalarının tespit edilerek soruşturmanın yönlendirilmesi maksadıyla kullanılmaktadır. **CBS (Coğrafi Bilgi Sistemi) analizi:** Soruşturmanın her aşamasında olay, adres gibi coğrafi değeri olan bilgilerin harita üzerinde gösterilmesi maksadıyla kurumun var olan Coğrafi Bilgi Sistemi ile bütünleşmiş çalışabilen bir analiz tekniğidir. Olay – zaman analizi: Elde edilen her tür delilin ve verinin olay ile ilişkisini zaman esasına göre sıralanması ve sonuçlarının görsel olarak gösterimi esasına dayanmaktadır. **Akış (mal – para) analizleri:** Suçun maddi unsurları ile fail arasındaki ilişkinin kurulması maksadıyla akış analizleri tekniği kullanılmaktadır. **Örgütlü suç analizi:** Suçların ve faillerinin örgütlü bir suç emareleri taşıyıp taşımadığının tespiti maksadıyla kullanılır.

2.5.2.4. Sunum (Presentation)

Bu safhaya gelindiğinde artık dijital deliller tespit edilmiş ve olayla bağlantıları ortaya çıkarılmıştır. Bundan sonra yapılması gereken yapılan çalışmaların ve elde edilen bulguların soruşturmacı makamlara ve ya adli makamlara bir rapor halinde sunulmasıdır.

Rapor yazımına geçmeden önce soruşturmacı (ya da adli bilişim uzmanı) tarafından neden adli bilişim sürecine gerek duyulduğunu ortaya koyacak noktalar tam olarak anlaşılmalıdır.[256] Bunlara bakacak olursak;

- Adli bilişim süreci ile dava arasında anlaşılabilir bir teori kurulmalıdır.
- Suçta kullanılan teknolojik imkânlar belirlenmelidir. Bu teknolojik yöntemler suçla bire bir ilintilimidir yoksa suçu aydınlatamayacak kadar az bir öneme mi sahiptir?

[256] US Department of Justice – National Instute of Justice, (2001), "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors", http://www.ncjrs.gov/pdffiles1/nij/211314.pdf, (Erişim Tarihi: 03.12.2010) ss.33-34.

- Adli bilişim sürecinde elde edilen dijital deliller, suçun kaynağı ve hedefimidir ya da sadece araç olarak mı kullanılmıştır?
- Suçta hedef olarak ya da araç olarak kullanılan bilgisayar teknolojilerinin mimarisi nedir? (Donanımlar, işletim sistemi, iletişim sistemi nedir?)
- Dijital delilleri ihtiva eden suç eşyaları tek bir adreste mi bulunmaktadır yoksa dağınık lokasyonlardamı?
- Adli bilişim süreci bittiğinde başka incelemelerin de (yeni bir adli bilişim süreci) yapılması gerektiği sonucuna varılmış mıdır?
- Adli bilişim sürecin başlatıldığı olayın hukuki konusu nedir ve kanunda hangi yaptırımlar tanımlanmıştır?

Yukarıda belirtilen konular tam olarak anlaşıldıktan sonra adli bilişim sürecinin son safhası olan rapor yazmaya geçilebilir. Adli bilişim uzmanı, tüm inceleme sürecini ve tespitlerine (kanaat, tespit veya bilgi niteliğindeki araştırma sonuçları) nasıl ve nereden ulaştığını raporunda ifade edebilmelidir. Bununla birlikte raporun taşıması gereken özellikler şunlardır;[257]

- Rapor metni kısa cümlelerle, sade ve anlaşılabilir bir dille yazılmalıdır. Teknik ifade ve terimler Türkçe kullanılmalı ya da anlamı parantez içinde yazılmalıdır.
- Rapor metninde ve eklerde, incelenmiş olan delillere referansta bulunulurken, raporun "tetkike verilen eşya" kısmında kullanılan tanımlayıcı özelliklerin aynısı kullanılmalıdır.
- Raporda delil inceleme safhaları belirtilmeli ve konu bütünlüğü olan aşamalar bütünlük ifade eden paragraflar şeklinde yazılmalıdır.
- Çok sayıda ve farklı tiplerde medya (sabit disk, disket, cep telefonu, hafıza kartları, CD'ler vs.) içeren incelemelerde, "tetkik konusu sabit disk", "söz konusu disket" gibi bir önceki cümlede geçen "nesneye" atıfta bulunmak, raporun akıcılığını ve anlaşılırlığını kolaylaştırır.

[257] Balı, Yunus, (2008), *Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği, Ses* Görüntü ve Data İncelemeleri, Ankara: Adalet Yayınevi, ss. 232-233.

- Raporda, inceleme sürecinin akış aşamaları ve delil inceleme sürecinin adımları gibi önemli safhaları belirtmek gerekir. Böylece raporda sunulan bilginin nasıl elde edildiği açıklığa kavuşturulmalı, inceleme sürecinin güvenilirliği ortaya konulmalı ve delil bütünlüğünün korunduğu vurgulanmalıdır.
- Rapor yazılırken, incelmeye konu her bir medya (sabit disk, CD vs.) ayrı ayrı düşünülmeli ve ona göre raporda yazılmalıdır. Hangi medyadan ne elde edildiği hususu çok önemlidir.

2.5.3. Adli Bilişim Sürecinin Hukuki Alt Yapısı

Hukuk sistemimiz içerisinde adli bilişim incelemeleri Ceza Muhakemesi Kanunu'nun 134. maddesinde düzenlenmiştir. Bu maddeye göre;

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstemesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

2.5.4. Adli Bilişim Sürecinde Karşılaşılan Problemler

Adli bilişim sürecinde en çok karşılaşılan problemlere bakacak olursak;[258]

- Ülkemizde delillere el koyma sürecinde işlemler yapılırken nelere dikkat edileceği hususu ile standartlar ve sorumluluklar henüz herhangi bir mevzuatta net olarak belirtilmemiştir.
- Bilgisayar veya ağ sistemlerinin incelenmesinde hâkim ya da savcıların geniş yetkilere sahip olmasına rağmen, teknik anlamda yeterli bilgiye sahip olmamaları ve onları bu konuda yönlendirecek standartların bulunmaması nedeniyle, zaman zaman ehliyet sahibi olmayan kişileri bilirkişi olarak atadıkları görülmektedir.
- Adli bilişim uzmanı olabilmek, bu alanda yetkin sayılabilmek için sadece bilişim sistemleri konusunda ileri seviyede bilgi sahibi olmak yeterli olmayacak kriminalistik bilimindeki gibi özel uygulamaların nasıl yürütüleceğinin bilinmesi ve bununda bilirkişi olabilecek şekilde yetki belgesiyle belgelendirilmesi gerekmektedir.
- Dava ile ilgilenen hâkim/savcı, raporun sonuç bölümüne bakarak karar vermektedir. Mahkemede davacı ve hükümlülerin rapora bir itirazı olduğunda yeniden inceleme için bilirkişi ya da kriminal laboratuarlarına gönderilmektedir.
- Cihazlar öncelikle yerinde incelenmesi ve bunun yeterli olmadığı durumlarda özel aparatlar ile yedeği alınarak bu yedekler üzerinde inceleme yapılması mümkün olduğunda ideal olanıdır. Mevzuatımızda bazı eksikliklerle birlikte konu ile ilgili hükümler bulunmasına rağmen, bunların kimi zaman uygulanmadığı görülmüştür.

2.5.5. Adli Bilişim Delillerini Kimler Kullanabilir?

Adli bilişim delillerinin kullanıldığı alanlara bakacak olursak;[259]

---

[258] Çicek, İlker, (2008), *Ülkemizde Adli Bilişim Laboratuarı Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları*, Haliç Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, ss. 15-17.

[259] Keser B., Leyla, (2002), *Adli Bilişim (Computer Forensic)* , Ankara: Yetkin Yayınevi, ss.76-77.

- Savcılık makamı, suç teşkil eden dokümanların bulunabileceği farklı suç çeşitlerinde bilgisayar delillerini kullanabilecektir: Örneğin; adam öldürme, uyuşturucu madde ticareti, finansal dolandırıcılık, zimmete kayıt geçirme ve çocuk pornografisi gibi. Özel Hukuk davalarında da örneğin: dolandırıcılık, boşanma, ayrımcılık ve taciz davaları ile ilgili olarak bulgular içeren bilgisayar sistemi üzerindeki şahsi ve iş kayıtlarının kullanılması mümkündür.
- Sigorta Şirketlerinin de kazada yapılmış bir hilenin, kundakçılığın ve iş yeri kaza tazminatlarının, bilgisayar delillerini kullanarak masraflarını hafifletmesi mümkündür.
- Kolluk görevlileri, araştırma öncesi yapılacak hazırlıklarda ve bilgisayar ekipmanlarına el konulma aşamasından sonraki, değerlendirme konularında sık sık yardım talep etmektedirler.
- Şirketler: cinsel taciz, zimmete para geçirme, hırsızlık veya ticari sırların ve diğer kurum içi/gizli bilgilerin ihlaline ilişkin delilleri tespit etmek için adli bilişim uzmanına müracaat etmektedirler.
- Bireyler de bazen haksız fesih, cinsel taciz veya yaş ayrımcılığı davalarında destek olması amacıyla adli bilişim uzmanlarına müracaat etmektedir.

2.5.6. Bilirkişilik Müessesi ve Adli Bilişim

Adli bilişim süreci hukuk sistemimiz içinde bilirkişilik müessesinin içinde yer alan bir konudur ve bu alanda özel eğitim almış adli bilişim uzmanları dijital deliller açısından bilirkişilik vasıflarına sahiptirler.

Adli olaylarda bilgisinden yararlanılan kişilere bilirkişi denir. Yargıçların ele aldıkları davada çözümlenmesi özel bilgiyi ya da tekniği gerektiren olaylarla karşılaştıklarında, bu konularda yetenekli gördükleri kişilere, başvurup, onların konu ile ilgili raporlarını göz önünde tutarak davayı çözümlerler. Bilirkişi görüşü bir delil değil, delillerin değerlendirilmesi vasıtasıdır.[260]

Ceza Muhakemesi Kanunu'nun 62-73. maddelerinde ve Hukuk Usulü Muhakemeleri Kanunu'nun 275-286. maddelerinde bilirkişilik müessesi ile ilgili

[260] Hancı, Hamit, (2003), *Bilirkişilik ve Çapraz Sorgu*, Ankara: Seçkin Yayıncılık, s.9.

düzenlemeler yapılmıştır. Ayrıca diğer kanunlarda da kendi konuları ile ilgili olarak bilirkişilik düzenlemeleri vardır.

Bilirkişilik resmi ve özel olmak üzere ikiye ayrılmaktadır. Kanunda düzenlenen şekliyle resmi kurumlar kendi alanlarında resmi bilirkişi kabul edilirler ve muhakeme süreci açısından önceliklidirler.[261] Özel bilirkişiler ise hâkim veya savcılar tarafından (ya da il adlî yargı adalet komisyonu tarafından) bahse konu dava ile ilgili olarak resmi bilirkişiler olmadığı durumlarda görevlendirilirler.

Adli bilişim süreci açısından Adli Tıp Kurumu, Polis Kriminal Laboratuarları ve diğer Emniyet Birimleri, Üniversiteler ve Tübitak gibi teknik kurumlar resmi bilirkişilik yapmaktadırlar. Özel bilirkişiler ise daha çok adli bilişim eğitimi almış bilgisayar uzmanlarından seçilmektedirler.

2.5.7. Delil Hukuku Açısından Adli Bilişim

Delil hukuku açısından dijital deliller ve adli bilişim süreci üzerinde durulması gereken önemli bir noktadır. Klasik anlamda delillerin üç boyutu vardır bunlar delilin kendisi, kaynağı ve muhtevasıdır. Bir parmak izi delilinde bu üç boyut net olarak görülebilirken dijital delillerde bu durum biraz daha karmaşıktır. Bu nedenle dijital deliller ceza muhakemesinde kâğıt üzerine çıktı şeklinde hazırlanarak "veri tespit eden belge" niteliğine kavuşturularak kullanılırlar. "Veri tespit eden belge" kısa tanımıyla, bilişim cihazlarında saklanan bilginini (verinin) kâğıt üzerine basılmış halidir diyebiliriz.[262]

Delillerin özellikleri açısından dijital delilleri değerlendirirken "ilgililik" özelliği bakımından sadece bilişim suçlarıyla ilgilidir demek yanlış olacaktır. Çünkü hem bilişim yoluyla işlenen suçlarda hem de klasik suçlarda dijital deliller somut olayla ilgili olabilirler. Örneğin bir cinayet olayında katille maktulün internet üzerinden yaptıkları iletişimleri doğrudan suçla ilgili bir delil olabilir.

"Faydalılık" açısından dijital deliller ve adli bilişim süreci bilişim bağlantılı suçlarda kesinlikle faydalıdır ve kovuşturma sırasında başvurulması hayatidir. Ancak

[261] Bulut, Erhan, (2001), "Bilirkişi Seçimi Ve Bilirkişi Raporlarının Bağlayıcılığı", http://www.mevzuatdergisi.com/2001/11a/02.htm, (Erişim Tarihi: 15.12.2010).
[262] Bıçak, Vahit, (2010), *Suç Muhakemesi Hukuku*, Ankara: Seçkin Yayınevi, s.399.

bir takım klasik suçlarda elde edilen dijital delillerin somut olayın çözülmesinde yüksek oranda faydalı olacaktır demek mümkün değildir.

Hem "ilgilik" açısından hem de "faydalılık" açısından adli bilişim süreci ve elde edilen dijital delillerin ciddi bir dezavantajı da vardır. Adli bilişim sürecinde tek bir bilgisayarından bile yüksek sayılarda anlamlı veriler çıkartılabilir ve adli bilişim uzmanın burada somut olayla doğrudan ilgili ve faydalı olanlarını tespit etmesi gerekecektir. Eğer adli bilişim uzmanı dava konusu olaya yeterince hâkim değilse bu eleme işlemini sağlıklı yapamayacaktır ve mahkeme sürecini olumsuz etkileyecektir.

"Akılcılık" ve "gerçeklik" bakımından dijital delillerle ilgili olumsuz bir durum bulunmamaktadır. "Müştereklik" özelliği açısından diğer delil türlerine göre dijital delillerde avantajlı bir durum mevcuttur. Çünkü daha soruşturma aşamasında dahi dijital delilleri ihtiva eden ve kopyası alınan bilgisayar disklerinin bir kopyası da bilgisayar sahibine verilmektedir. Dijital delillerin çoğaltılabilme özelliği bu anlamda bir avantajdır. Örneğin delil niteliği olan ve soruşturma (ya da kovuşturma) makamlarında bulunan bir suç eşyasını failin ya da mağdurun temin ederek kendi istedikleri bir uzmana inceletmesi mümkün değildir ancak dijital delillerde böyle bir avantaj vardır. İddia makamlarınca aleyhinde delil olarak ortaya konulan bir bilgisayar diskini eğer isterse şüpheli taraf da başka bir uzmana inceletebilir ve buradan elde edeceği bilgiler (farklı bir sonuç elde ettiyse) doğrultusunda savunmasını hazırlayabilir

Ceza muhakemesi açısından delillerin en önemli özelliği olan "kanuna uygun elde edilmiş olma" dijital deliller ve adli bilişim süreci açısından çok hassastır. Çünkü dijital delilleri elde ederken kanuna uygun davranmanın yanında bu süreçteki standart tekniklere de harfiyen uymak gerekmektedir. Dijital delillerin bozulmaya çok müsait olduğundan bahsetmiştik eğer delil elde etme süreci (adli bilişim) esnasında uyulması gereken teknik kurallara uyulmazsa deliller kolaylıkla bozulabilir. Türk Ceza Kanunu'nun 281. maddesinin ilk iki fıkrasına göre;

> *(1) Gerçeğin meydana çıkmasını engellemek amacıyla, bir suçun delillerini yok eden, silen, gizleyen, değiştiren veya bozan kişi, altı aydan beş yıla kadar hapis cezası ile cezalandırılır. Kendi işlediği veya işlenişine iştirak ettiği suçla ilgili olarak kişiye bu fıkra hükmüne göre ceza verilmez.*

(2) Bu suçun kamu görevlisi tarafından göreviyle bağlantılı olarak işlenmesi halinde, verilecek ceza yarı oranında artırılır.

Dijital delillerin toplanması ve muhafazası bu alandaki uzman kişiler tarafından yapılmadığı takdirde ilgili kamu görevlileri için ciddi sıkıntılar ortaya çıkarabilir.

Bununla birlikte dijital delillerin değiştirilmesi çok kolay olmakla birlikte uzman kişiler tarafından yine bu değişiklikleri tespit etmek de mümkündür.[263] Ancak bu yönüyle adli bilişim süreci ve dijital delillere yönelik ciddi eleştiriler getirilmektedir. Konunun uzmanları göre dijital deliller kesindir ve delil bütünlüğünü sağlamak teknik yöntemlerle mümkündür fakat teknik standartlara ve kurallara uyulmadığı takdirde bu eleştiriler son derece haklıdır. Özellikle bilişim bağlantılı suçlarda çok önemli olan adli bilişim süreci iyi eğitim almış deneyimli teknik uzmanlar tarafından yürütülmelidir. Çünkü bilişim bağlantılı suçlarda dijital deliller "doğrudan delil" niteliğinde olduğu için bu delillerin bozulması mahkeme sürecinin ciddi anlamda sekteye uğramasına sebep olacaktır.

Delil hukuku açısından dijital delillerin yapısı gereği, dijital veriler üzerinde çok kolay bir şekilde değiştirme, silme ve yenisini oluşturma gibi işlemlerin yapılabilmesi bu delillerin bütünlüğünü sağlamayı çok zorlaştırmaktadır. Dijital delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabileceği için doğrulama problemi ortaya çıkabilecektir. Dijital delillendirme işlemindeki dijital delilin sahibi, onu ele geçiren şahıslar delilin alındığı medya, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların daha sonradan inkâr edilememesi için adli bilişim süreci kusursuz yönetilmelidir. Dijital deliller oluşturulduktan ve yedeklendikten sonra, bu delilleri üçüncü bir şahıs inceleyebilmelidir.[264]

2.5.8. Anti Adli Bilişim

"Anti adli bilişim" teknikleri, adli bilişime karşı ortaya çıkmıştır ve adli bilişim sürecini kısmen sekteye uğratmak ya da tamamen başarısız kılmaya yönelik

[263] milliyet.com.tr, (2011), "Yanlış Yapan Cezasını Çeker", http://www.milliyet.com.tr/-yanlis-yapan-cezasini-ceker-/siyaset/sondakika/27.01.2011/1344802/default.htm, (Erişim Tarihi: 27.01.2011).
[264] Uzunay, Yusuf, (2008), "Olay Yerinden Alınan Dijital Delillerin Hukuki Kabul Edilebilirliğini Arttırmak", http://akademikguvenlik.wordpress.com/2008/07/11/olay-yerinden-alinan-dijital-delillerin-hukuki-kabul-edilebilirligini-arttirmak/, (Erişim Tarihi: 28.01.2011).

çalışmalardır. Adli bilişim süreci sonunda dijital delillerden elde edilen verilerin miktarını ve kalitesini azaltmaya yönelik girişimleridir.[265]

Anti adli bilişim tekniklerini incelediğimizde bunun iki boyutu olduğunu görmekteyiz. Birincisi dijital delillerden yola çıkarak suçluya ulaşmayı zorlaştırmak, ikincisi ise suçluya ulaşılsa bile bunu ispat etmeyi zorlaştırmaktır.

Anti adli bilişim teknikleri dört kategoride toplanmaktadır. Bunlar; veriye zarar verme, veriyi gizleme, veriyi şifreleme ve veri kontrolü. Veri kontrolünden kasıt daha sonra dijital delil olabilecek verilerin kalıcı olarak kaydedilmeden (uçucu) kullanılmasıdır.[266] Suçlular bu dört kategorideki tekniklere suç işlemeden önce, suç işlerken veya suç işledikten sonra başvurmaktadırlar.

Anti adli bilişim tekniklerine karşı da adli bilişim sürecinin başarılı olabilmesi için "anti – anti adli bilişim" tekniklerinin geliştirilmesi gerekmektedir. Bunun için bu alandaki gelişmeler yakından takip edilmelidir, adli bilişim programlarının zafiyetleri giderilmelidir ve adli bilişim sürecinde bütün işlemler belli alışkanlıklar doğrultusunda ezbere yapılmamalıdır.[267] Anti adli bilişim alanında yapılan çalışmalara bakıldığında dijital delilleri gizlemek yerine bunların hukuki geçerliliğini olumsuz etkilemeye yönelik girişimler de bulunmaktadır. Bu nedenle bu girişimlere karşı dijital delillerin hukuki geçerliliğini zayıflatmayacak teknik ve hukuki önemler alınmalıdır.

---

[265] Erbes, Robert, (2004), "Anti Forensics", http://infohost.nmt.edu/~sfs/Students/RobertErbes/Presentations/anti-forensics.ppt, (Erişim Tarihi: 29.01.2011).

[266] Wiele, Tom Van de, (t.y.), "BCIE Training – ICT Anti-Forensics", http://www.bcie.be/Documents/BCIE_Training03_ICT_Anti-Forensics_291106_TVdW.pdf, (Erişim Tarihi: 29.01.2011).

[267] Martin, Lockheed, (2005), "Anti - Forensics", http://www.cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005.pdf, (Erişim Tarihi: 29.01.2011).

ÜÇÜNCÜ BÖLÜM

BİLİŞİM SUÇLARI VE BİLİŞİM YOLUYLA İŞLENEN SUÇLARIN KARŞILAŞTIRILMASI

Bu bölüm çalışmamızın ana konusunu içermektedir. Birinci ve ikinci bölümde değinilen konular bu bölümün anlatılabilmesi için açıklanmıştır. Bölüm başlığında geçen karşılaştırma yaklaşımı farklılıkları ortaya koyacağı gibi benzerlikleri ve yanlış anlaşılan (yanlış kullanılan) konuları da özetleyecektir.

"Bilişim suçları" ve "bilişim yoluyla işlen suç" kavramlarını karşılaştırırken ilk göze çarpan noktanın her iki kavramda da "suç" kelimesinin geçmesi olmalıdır. Bu nedenle karşılaştırma yapılacak çerçeveyi "suç" literatürü (suç bilimi - kriminoloji) ve hukuki düzenlemeler çizecektir.

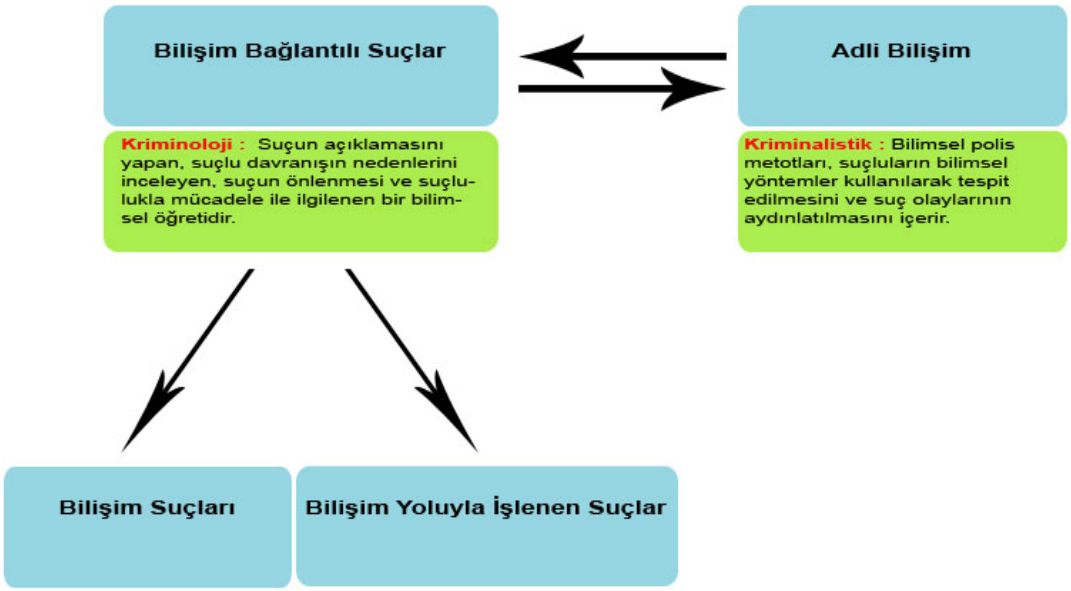
Suç bilimi açısından kavramlara bakıldığında daha çok evrensel geçerliliği olan değerlendirmeler yapılabilir. Ancak hukuki açıdan bakıldığında daha özele inmek ve ülkelerin hukuk sistemlerine göre konuyu ele almak gerekecektir. Her ne kadar genel geçerli hukuki değerler olsa da kanunlar açısından ülkelerin düzenlemeleri farklılıklar göstermektedir. Ancak bu alanda yapılan uluslar ararsı düzenlemelerin daha evrensel olduğunu söyleyebiliriz.

"Bilişim suçları" ve "bilişim yoluyla işlenen suçlar" hem istatistikî açıdan hem de suçla mücadele açısından ayrı ayrı incelenmelidir. Çünkü bu açıdan da dikkate değer farklılıklar vardır.

Teorik olarak incelenen bir konunun en iyi şekilde anlaşılabilmesi için uygulamadan örnekler verilmesinin en iyi yöntem olacağı kanısındayız. Bu nedenle ülkemizdeki ve dünyadaki uygulamalardan örnekler verilerek "bilişim suçu", "bilişim yoluyla işlenen suç" ve "adli bilişim" kavramlarının pratik hayattaki yansımalarına değinilecektir. Böylelikle kavramlar daha iyi anlaşılarak uygulamada yaygın düşülen hatalardan kaçınılacağı düşüncesindeyiz.

3.1. GENEL OLARAK

Birinci ve ikinci bölümde detaylarıyla anlatılan konuları kategorize etmek istersek aşağıdaki şekliyle bir diyagramın ortaya çıktığını görebiliriz.



Şekil 7 – Bilişim Bağlantılı Suçlar ve Adli Bilişim Ayrımı

Bilişim teknolojilerinin suç dünyasında kullanılmasıyla birlikte "bilgisayar bağlantılı suçların"[268] ortaya çıktığını söyleyebiliriz. Ancak bunu ikiye ayırmak gerekmektedir. Bunlardan birincisi suçun hedefi olarak bilişim teknolojilerinin alınması yani "bilişim suçları" ikincisi ise klasik suçlarda araç olarak bilişim teknolojilerinin kullanılması sonucu yeni karşılaşılan bir kavram olan "bilişim yoluyla işlenen suçlar."[269]

Adli bilişim, bilişim bağlantılı suçların çözülmesinde bilişim teknolojilerinin kullanılmasıdır ve bu suçlarda kesinlikle başvurulması gereken bir süreçtir. Ancak bu kavramı da doğru kullanmak ve bir suç türü gibi algılamamak gerekmektedir.

Bilişim bağlantılı suçlar işlenirken elbette bilişim teknolojileri kullanılacaktır. Ancak kullanılan bu yöntemleri de doğrudan doğruya bir suç türü gibi algılamamak gerekmektedir. Nitekim bazı teknikler olumlu amaçlar içinde kullanılmaktadır. Bilişim suçları teknolojik gelişmelere paralel olduğu için devamlı değişmektedir ve çerçevesi çok geniştir bu nedenle kanuni metinlerde bu suçları geniş bir şekilde

[268] UNODC – United Nations Office on Drugs and Crime, (2005), "Computer Related Crime", http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf, (Erişim Tarihi: 06.12.2010).

tanımlanmak yerine hangi eylemlerin bu suçları oluşturduğu ve yaptırımlarının neler olduğu kanunlarda yazılmıştır.

3.2. HUKUKİ AÇIDAN

"Suç**"** kelimesi hukuk terimi olarak, "devletçe yasalarla tanımlanıp yaptırıma bağlanmış olan kurallara aykırı davranış" şeklinde tanımlanmaktadır.[270] Hukuk sistemi içerisinde suçlar adli yaptırımları olan cürümler ve idari yaptırımları olan kabahatler şeklinde de ikiye ayrılmaktadır.

Ceza hukuku, suç ve ceza kavramlarını inceleyen kamu hukuku bölümüdür. Genel ve özel ceza hukuku olarak ikiye ayrılır. Genel ceza hukukunun konusu suç kavramının maddi ve manevi unsurlarıyla tanımı, ceza hukukuna hâkim olan genel ilkeler, ceza kavramının tanımı, suçu ortadan kaldıran nedenler, cezayı azaltan ve ortadan kaldıran nedenler gibi bütün suçlar için geçerli olan ilke ve teorilerdir. Özel ceza hukukunun konusu ise ülkenin kanunlarına göre suç sayılan eylemlerin neler olduğu, bunların kapsam ve sınırları, birbirlerinden ayrılan yönleri ile bu suçlara öngörülen cezalardır.[271]

Hukuk devleti ilkesi, bireylerin temel hak ve özgürlüklerini yalnızca ceza hukuku aracılığıyla korumakla kalmamakta, aynı zamanda ceza hukukuna karşı da korumaktadır. Hukuk devleti ilkesinin bu anlamda şüphesiz ki en önemli aracı, kanunsuz suç ve ceza olmaz ilkesidir. Kimsenin işlediği zaman kanunlarına göre suç sayılmayan bir fiilden ötürü cezalandırılamaması hukuk devleti ilkesinin birey açısından bir güvencesini oluşturmaktadır. Kanunun açıkça suç saymadığı bir fiilden dolayı kimse cezalandırılamayacağı gibi, kanunun açıkça koyduğu bir cezadan daha ağır bir ceza ile de kimse cezalandırılamayacaktır. Başka bir ifade ile bu ilke, bireyin, özgürlüğünün sınırlarını önceden bilerek davranışlarının sonuçlarının ne anlama gelebileceği çıkarımını yapmasıdır. Toplumsal barışın sağlanması ve devamı açısından da kanunilik ilkesinin önemi büyüktür.[272]

---

[270] Büyük Türkçe Sözlük, Türk Dil Kurumu, (t.y.), "Suç", http://tdkterim.gov.tr/bts/arama/?kategori=verilst&kelime=su%E7, (Erişim Tarihi: 08.12.2010)
[271] wikipedia.org, (2010), "Ceza Hukuku", http://tr.wikipedia.org/wiki/Ceza_hukuku, (Erişim Tarihi: 08.12.2010).
[272] Bostancı, Gülşah, (2007), *Avrupa İnsan Hakları Sözleşmesi Bağlamında Türk Ceza Hukukunda Suçta Ve Cezada Kanunilik İlkesi*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul, s.4.

Suçlarla ilgili karşılaştırma ve yorum yaparken ilk olarak bakılması gereken yer hukuki metinler olan kanun maddeleridir. Ancak burada mevcut durum sorgulanmalıdır. Yani kanun maddelerinde net olarak belirtilen eylemler ve cezaları dışındaki yorumlar doğru olmayacaktır.

3.2.1. Hukuk Sistemimiz Açısından

Ülkemiz hukuk sisteminde suçlar 5327 sayılı Türk Ceza Kanunu'nda düzenlenmiştir. Ancak bütün suçların bu kanunda düzenlendiğini söylemek yanlış olur. Türk Ceza Kanunu'nun 5. maddesinde bu durum düzenlenmiştir;

(1) Bu Kanunun genel hükümleri, özel ceza kanunları ve ceza içeren kanunlardaki suçlar hakkında da uygulanır.

Türk Ceza Kanunu dışındaki özel kanunlarda da suçlar ve cezaları düzenlenmiştir. Özel ceza kanunlarında ve ceza içeren kanunlarda suç tanımlarına yer verilmesinin yanı sıra, çoğu zaman örneğin teşebbüs, iştirak ve içtima gibi konularda da Türk Ceza Kanunu'nda benimsenen ilkelerle çelişen hükümlere yer verilmektedir. Böylece, ceza kanununda benimsenen genel kurallara aykırı uygulamaların yolu açılmakta ve temel ilkeler dolanılmaktadır. Tüm bu sakıncaların önüne geçebilmek bakımından, ayrıca hukuk uygulamasında birliği sağlamak ve hukuk güvenliğini sağlamak için, diğer kanunlarda sadece özel suç tanımlarına yer verilmesi ve bu suçlarla ilgili yaptırımların belirlenmesi ile yetinilmelidir. Buna karşılık, suç ve yaptırımlarla ilgili olarak Türk Ceza Kanunu'nda belirlenen genel ilkelerin, özel kanunlarda tanımlanan suçlar açısından da uygulanmasının temin edilmesi gerekmektedir. Aksi yöndeki düzenlemelerin hukuk devleti ve eşitlik ilkelerine aykırılık oluşturacaktır.[273]

Birinci bölümde detaylarıyla anlatıldığı gibi "bilişim suçları" Türk Ceza Kanunu'nun 243, 244, 245 ve 246. maddelerinde düzenlenmiştir. Yine birinci bölümde vurguladığımız gibi aslında klasik suçlardan birçok yönüyle ayrılan özel bir suç türüdür. Ancak kanun koyucular bu şekilde bir düzenlemenin yeterli olacağı kanısıyla başka bir özel kanunda düzenleme yapmamışlardır. Gelişen teknolojiyle birlikte gelecek dönemlerde çok farklı boyutlara ulaşması muhtemel olan bilişim suçları açısından ayrı özel bir kanunda düzenleme yapılması gündeme gelebilir.

[273] Türk Ceza Kanunu Gerekçesi.

Mevcut durum açıktır ve bilişim suçlarından bahsederken sadece Türk Ceza Kanunu'nun ikinci kitabının "Topluma Karşı Suçlar" başlıklı üçüncü kısmında, "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde 243, 244, 245 ve 246. maddelerinde düzenlenen suçlardan bahsetmek gerekmektedir.

Bilişim yoluyla işlenen suçların, klasik suçların veya özel kanunlarda tanımlanmış suçların bilişim teknolojiler yardımıyla işlenmesi olduğundan önceki bölümlerde bahsetmiştik. Burada dikkat edilmesi gereken nokta suçun işleniş şeklinin (modus operandi) değiştiğidir. Yeni bir suç türü olarak ortaya çıkmamış ve ayrı bir düzenleme de yapılmamıştır. Ancak bazı suçların nitelikli hali olduğu için güncel değişiklikler yapılmıştır.

Başta Türk Ceza Kanunu'nda düzenlenen suçlar olmak üzere birçok suç bilişim yoluyla işlenebilmektedir. Bununla birlikte birinci bölümde detaylarıyla anlatılan Fikir ve Sanat Eserleri Kanununda ve Elektronik İmza Kanununda düzenlenen bazı suç türlerinin bilişim teknolojileri kullanılmadan işlenmesi neredeyse mümkün değildir.

Bilişim suçları ve bilişim yoluyla işlenen suçlar arasında hukuki yönden yapılan bu ayrımı aşağıdaki diyagramda net olarak görebiliriz;

Şekil 8 - Bilişim Bağlantılı Suçlar ve Adli Bilişim Ayrımı Hukuki Çerçevesi

Bilişim yoluyla işlenen suçlar listelenirken güncel durum dikkate alınmaktadır. Ancak gelecekte bu listenin daha da uzayacağı çok açıktır. Hem Türk Ceza Kanunu'ndaki başka suçların hem de özel kanunlarda düzenlenen başka suçların önümüzdeki yıllarda bilişim teknolojileri marifetiyle işlenebileceği ihtimali çok yüksektir.

Bilişim bağlantılı suçlarda suçu aydınlatmanın en önemli ayağını oluşturan dijital delil elde etme ya da adli bilişim sürecini de ikinci bölümde detaylarıyla anlatmıştık. Bu süreçte hukuk sistemimiz içinde ceza muhakemesinin nasıl yapılacağı hususundaki kurallar ile bu sürece katılan kişilerin hak, yetki ve yükümlülüklerini düzenleyen Ceza Muhakemesi Kanunu'nun 134. maddesinde "bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma" başlığı altında düzenlenmiştir.

3.2.2. Mukayeseli Hukuk Açısından

Kısaca farklı ülkelerin aynı konulardaki farklı kanuni düzenlemelerini karşılaştırmaya, değerlendirmeye veya kıyaslamaya hukuk terminolojisinde mukayeseli (karşılaştırmalı) hukuk denilmektedir.

Ülkemizdeki düzenlemelere benzer olarak bazı ülkelerde mevcut yasalarda bilişim bağlantılı suçlar düzenlenmiştir. Ancak bazılarında ise bilişim bağlantılı suçlar ayrı bir alan olarak kabul edilmiş ve özel kanunlarda düzenlenmiştir.

Roma Hukuku sistemi Kıta Avrupa'sı ülkelerinin uyguladığı ve Türkiye'nin de uyguladığı bir sistemdir. Kıta Avrupa'sı sistemlerinde hukuku yasa koyucu yapar. İçtihatlar (yargı kararları) tamamlayıcı normlardır. Anglo-Sakson hukuk sistemi ise İngiliz ve Amerikan ülkelerinde uygulanan hukuk sistemidir. 11.ci yüzyılda İngiltere'de gelişmiştir. Roma hukuk sistemi gibi hukuku bölümlere ayırmaz. Hukuk yaratıcısı olarak yargıçları görürler. Bu nedenle yargıçlar (içtihat) hukuku da demek mümkündür. Ortak hukuk sisteminde gelişme ve teknolojinin getirdiği yenilikler ve yeni gelişmeler nedeni ile zaman içinde ortaya çıkan eksiklikler (boşluklar) çıkarılan kanunlar ile giderilmeye çalışılmıştır.[274]

3.2.2.1. Amerika Birleşik Devletleri

Bilgisayar teknolojilerinin ve İnternetin geliştirildiği ülke olan Amerika Birleşik Devletleri'nin bilişim bağlantılı suçlarla mücadele için yürürlüğe koyduğu hukuki düzenlemeler şüphesiz en dikkate değer düzenlemelerdir.

Amerika Birleşik Devletleri'ndeki bilişim bağlantılı suçlar alanındaki ilk federal kanun 1984 tarihli "Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Kanunu (Counterfeit Access Device and Computer Fraud and Abuse Act)" olup 1986 yılında Computer Fraud and Abuse Act olarak adlandırılan değişiklikle mevcut üç adet suça, üç yeni suç daha eklemiştir. Bunların dışındaki Kanunları, 1986 tarihli "Elektronik Haberleşme Gizlilik Yasası (Electronic Communications Privacy Act)", 1997 tarihli "İnternette Kumarın Önlenmesi Yasası (İnternet Gambling Prohibition Act)", 1998 tarihli "Çocukların Çevrimiçi Yayınlardan Korunması Yasası (Child Online Prevention Act)", 2001 tarihli "Anti

[274] hukuki.net, (2009), "Hukuk Sistemleri", http://wiki.hukuki.net/Hukuk_sistemleri, (Erişim Tarihi: 09.10.2010).

Terörizm Yasası (USA-Patriot Anti-Terrorism Act)" olarak saymak mümkündür. Ayrıca 1992 yılında bilişim teknolojisine dair gelişmelerin kamusal eğitim ve hizmetlerde, sağlık tedbirleri ve endüstride kullanılabileceğini garantiye alan Bilgi ve Teknoloji Yasası (Information and Technology Act of 1992) kabul edilmiş, hemen ardından, Ulusal Bilgi Altyapısı Yasası (National Information Infrastructure Act) çıkarılmıştır.[275]

Bunların dışında siber suçlarla ilgili hükümler içeren kanunlar ve federal düzenlemeler şunlardır;[276]

- 2003 yılında çıkartılan "Çocukların İstismarına Yönelik Soruşturma Çözümleri ve Yöntemler Yasası (Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act)"
- 2002 yılında çıkartılan "İç Güvenlik Yasası (Homeland Security Act)"
- 2001 yılında çıkartılan "Vatanseverlik Yasası (USA Patriot Act)"

ABD Federal Kanunları'nın 18. numaralı "Suçlar ve Ceza Muhakemesi" başlıklı bölümünde federal suç olarak düzenlenen eylemler;[277]

- Madde 1029, Erişim Cihazlarıyla Yapılan Dolandırıcılık Ve İlgili Aktiviteler (Fraud And Related Activity In Connection With Access Devices)
- Madde 1030, Bilgisayar Yoluyla Dolandırıcılık Ve İlgili Aktiviteler (Fraud And Related Activity In Connection With Computers)
- Madde 1362, İletişim Hatlarının, İstasyonların Ve Sistemlerin Korunması (Communication Lines, Stations, Or Systems)
- Madde 2510, Kablolu, Elektronik Ve Sözlü İletişim Engellenmesi (Wire And Electronic Communications Interception And Interception Of Oral Communications)

[275] Kurt, (2005), a.g.e., s.99.
[276] Computer Crime & Intellectual Property Section, Department of Justice, (t.y.), "Computer Crime Legal Resources", http://www.justice.gov/criminal/cybercrime/cclaws.html, (Erişim Tarihi: 09.10.2010).
[277] Cornell University Law School, (t.y.), "Title 18 - Crimes And Criminal Procedure", http://www.law.cornell.edu/uscode/18/usc_sup_01_18.html, (Erişim Tarihi: 09.10.2010).

- Madde 2701, Kablolu Ve Elektronik İletişim Kaydedilmesi Ve Kayıtlara Erişilmesi (Stored Wire And Electronic Communications And Transactional Records Access)
- Madde 3121, Arama, Yönlendirme, Adresleme Ve Sinyal Bilgilerinin Kaydedilmesi (Recording Of Dialing, Routing, Addressing, And Signaling Information)

Görüldüğü üzere Amerika Birleşik Devletleri'nde bilişim suçları ve bilişim yoluyla işlenen suçlar ayrı ayrı ele alınmış ve farklı kanuni düzenlemeler yapılmıştır. Bununla birlikte güncel suç türlerine ve eylemlerine göre mevcut mevzuata eklemeler yapılmaktadır.

3.2.2.2. İngiltere

İngiltere'de Bilişim Suçları, 29.08.1990 tarihinde yürürlüğe giren "Bilgisayarın Kötüye Kullanılması Yasası (Computer Misuse Act)" ile düzenleme altına alınmıştır. Bu yasa üç ana bölüm ve bunların alt dalları olan on sekiz alt bölümden oluşmaktadır. Bu ana bölümler üçe ayrılmakta ve ilk ana bölümde bazı suç tipleri düzenlenmekte, ikinci ana bölümde ceza muhakemesi hukukuna ilişin düzenlemeler getirilmekte, üçüncü ana bölümde ise konuyla ilgili bazı genel düzenlemeler getirilmektedir. Suç tiplerinin düzenlendiği birinci bölüme genel olarak bakıldığında, bunun da üç alt bölüme ayrıldığı; birinci alt bölümde bilgisayardaki yazılım ya da verilere yetkisiz giriş, ikinci alt bölümde farklı suçların işlenmesini kolaylaştırmak ya da yardımcı olmak amacıyla bilgisayarlara yetkisiz erişim ve üçüncü alt bölümde bilgisayarda bulunan yazılım ya da verilerin yetkisiz olarak değiştirilmesi eylemlerinin suç haline getirildikleri görülmektedir. Ayrıca İngiliz hukukunda bilişim suçlarını düzenleyen bu yasa dışında özellikle pornografi ve çocuk pornografisi alanına ilişkin düzenlemeler yapılmıştır.[278]

İngiliz hukuk sisteminde özel bir kanunda bilişim suçlarının ve bilişim yoluyla işlenen suçların düzenlendiğini görmekteyiz. Kanun kapsamında sadece bilişim suçları düzenlenmemiş ayrıca diğer suçlarda bilişim teknolojilerinin kullanılmasına yönelik düzenlemeler de yapılmıştır. Buna ek olarak suç ve cezalarını

[278] Dülger, (2004), a.g.e., s.97.

düzenleyen diğer kanunlarda da güncel değişiklikler yapılarak teknolojik gelişmeler mevcut hukuki sisteme entegre edilmiştir.

Amerika Birleşik Devletleri ile aynı hukuk sistemine sahip olan İngiltere'de de bilişim alanındaki suçlara yönelik kanuni düzenlemeler benzer şekilde ortaya koyulmuştur.

3.2.2.3. Almanya

Ülkemizde olduğu gibi Almanya'da da bilişim suçları ayrı bir yasada değil, öncelikle Ceza Kanunu içerişinde düzenlenmiştir. Bunun yanında konuyla ilgili başka yasalar da bulunmaktadır. Ancak bizim ceza kanunumuz gibi belli bir bölümde düzenlenmemiş farklı maddelerde ayrı ayrı düzenlenmiştir.

Alman Ceza Kanunu'ndaki bilişim bağlantılı suçlarla ilgili düzenlemeler iki başlıkta toplanabilir:[279]

- İnternet/bilgisayar suçluluğu konusunda özel olarak düzenlenen maddeler; 11/3, 176, 176a, 184, 202a (veri casusluğu), 263a, 269, 271, 274/2, 303a (veri değiştirme), 303b (bilgisayar sabotajı), 303c.
- Suç tanımlarında kullanılan ibareler nedeniyle bilişim suçlarına da uygulanabilecek olan maddeler; bilgisayar dolandırıcılığıyla ilgili 263a, ispat gücüne sahip verileri sahte evrak oluşturacak şekilde değiştirme veya bunları kullanmayla ilgili 269, verilerin işlenmesinde yanıltmayla ilgili 270, dolaylı olarak sahte evrak oluşturmayla ilgili 271, ispat gücü olan verilen başkası zararına silme, gizleme, kullanılamaz hâle getirme veya değiştirmeyle ilgili 274/2, verileri değiştirmeyle ilgili 303a, bilgisayar sabotajıyla ilgili 303b.

Alman hukuk sistemi de bizim hukuk sistemimizdekine benzer bir şekilde bilişim suçları ve bilişim yoluyla işlenen suçlar ceza kanunlarında düzenlenmiştir. Ayrıca özel kanunlarda yer alan bilişim teknolojilerinin kullanılmasıyla işlenebilecek suçlarla ilgili de düzenlemeler mevcuttur.

[279] Karagülmez, (2009), a.g.e., s.115.

3.2.2.4. Fransa

Fransa'da bilişim suçları ayrı bir fasıl şeklinde düzenlenmeden önce bu tarz eylemler Fransız Ceza Kanunu'ndaki hırsızlık (md.379), inancı kötüye kullanma (md.408) ve dolandırıcılık (md.405) gibi mal aleyhine işlenen bazı suçlarla karşılanmaya çalışılmıştır. Teknolojik gelişmeler karşısında bir kısım kanuni düzenlemeler yapılması ihtiyacı ortaya çıkmış ve sırasıyla gizliliğin korunmasına ilişkin 6 Ocak 1978 tarih ve 78-17 sayılı "relative a l'informatique, aux fichiers et aux libertes" adlı kanun ile telif hakkı korunmasına ilişkin 3 Temmuz 1985 tarih ve 85660 sayılı "relative aux droits d'auteur et aux phonogrammes et la videeogrammes et des enterprises de comminication audiovisuella" adlı kanun ihdas edilmiştir.[280]

1 Mart 1993 tarihinde yürürlüğe giren Yeni Fransız Ceza Kanunu'nda bilişim bağlantılı suçlar "mal aleyhine suç ve cürümler" başlıklı birinci kitabın "mala karşı diğer tecavüzler" başlıklı ikinci babının "bilgileri otomatik işleme tâbi tutmuş sistemlere yönelik saldırılar" başlıklı üçüncü faslı içerisindeki 323-1 ilâ 323-7. maddelerinde önceki düzenlemeden farksız biçimde yer almıştır. Yeni Kanunda yalnızca, sahte bilgisayar belgesi oluşturma ve bunu kullanma suçları, sahtecilik suçuyla genel düzenleme kapsamında değerlendirilmiştir. Yeni Fransız Ceza Kanunu'nun başka maddelerinde de bilişimle ilgili bazı düzenlemeler yer almıştır. Buna göre, 226-16 ila 226-24 maddelerde kişilik haklarının bilişim sistemi aracılığıyla ihlâli, 226-8. maddesinde bireylerin resim veya sözlerinin rızasına aykırı şekilde montajı, 227-23. maddesinde küçüğün resminin pornografik olarak kullanılması, 227-24. maddesinde küçükler tarafından görülmeye elverişli şiddet ve pornografik nitelikli mesaj yayımlanması suç olarak düzenlemiştir.[281]

Fransız hukuk sistemi de bizim hukuk sistemimizdeki gibi bilişim suçları ve bilişim yoluyla işlenen suçlar ceza kanunlarında düzenlenmiştir.

3.2.2.5. Japonya

Japonya'da Ceza Kanunu 22.06.1987 tarihinde değiştirilerek, bilişim suçlarına ilişkin hükümler kanuna eklenmiştir. Ayrıca 13.02.2000 tarihinde de "İnternete Haksız Girmenin Yasaklanması Hakkındaki Kanun" yürürlüğe girmiştir. Japon Yasa

[280] Tulum, (2006), a.g.e., s.60.
[281] Karagülmez, (2009), a.g.e., s.111-113.

Koyucu, aynı Almanya'da olduğu gibi "korunan hukuksal değeri" dikkate alarak yasal düzenlemeyi yapmıştır.[282]

3.2.2.6. İsrail

İsrail, 1995 yılında yürürlüğe giren Bilgisayar Kanunu ile bilişim suçlarını düzenleme altına almıştır. Ayrıca İsrail hükümeti, bilişim suçları ile mücadele konusunda başta Amerika Birleşik Devletleri olmak üzere, birçok Avrupa ülkesiyle işbirliği anlaşması imzalamış bulunmaktadır.[283]

Özetlemek gerekirse bilişim bağlantılı suçlar farklı ülkelerin hukuk sistemlerinde farklı şekillerde düzenlenmiştir ancak bazı ülkelerin düzenlemeleri birbirine benzemektedir. Bilişim bağlantılı suçlarla ilgili düzenlemelerde ülkelerin üç temel özelliğine göre bu düzenlemeleri farklılık göstermektedir. Bunlar;

1. Ülkenin mevcut hukuk sistemi (Kıta Avrupası – Anglo Sakson)
2. Ülkenin teknolojik gelişmişliği ve bilişim teknolojilerinin günlük hayattaki yeri ve yaygınlığı
3. Ülkelerin bilişim teknolojilerinin suç dünyasında kullanılmasıyla yaşadıkları tecrübeleri ve suçu önleme yolundaki çalışmaları.

3.2.3. Uluslar Arası Düzenlemeler Açısından

Bililim bağlantılı suçlar İnternet ortamının da kullanılmasıyla suç yeri açısından belki de tüm dünyaya yayılabilen tek suçtur. Başka organize suç türleri de birden fazla ülkede işlenebilmektedir ama bu sayı birkaç ülkeden (özellikle komşu ülke) fazla değildir. Ancak bilişim bağlantılı suçlar aynı anda onlarca ülkede birden işlenebilir.

Uluslar arası niteliği olan suçlarla mücadelede herhangi bir ülkenin güvenlik birimleri yeterli olamayacağı gibi tek bir ülkenin kanuni düzenlemeleri de yeterli olmayacaktır. Nitekim bu tür suçları önlemede başarılı olabilmek için uluslar arası işbirliği kaçınılmazdır. Uluslar arası işbirliği için de en az iki ülke arasında bu

[282] Yaycı, Esra, (2007), "*Bilişim Suçları*", Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara, s.60.
[283] Yaycı, a.g.e., s.58.

işbirliğine zemin hazırlayacak yazılı anlaşmaların veya sözleşmelerin olması gerekecektir.

Günümüzde neredeyse her ülke bir uluslar üstü (supranasyonal) topluluğun (Birleşmiş Milletler, Avrupa Birliği vb.) üyesi durumundadır. Topluluğa üye ülkeler arasında birçok alanda (özellikle uluslar arası sorunlarda) işbirliğini sağlayan sözleşmelere imza atılmaktadır. Suçla mücadele de bu alanlardandır.

Uluslararası ilişkilerdeki gelişmeler ve bu ilişkilerde yaşanan yoğunluk, gerek siyasal, gerekse hukuksal düzeyde kimi sorunları da beraberinde getirmektedir. Bu sorunlar, devletlerin uluslararası düzeyde sahip oldukları mutlak egemenlik anlayışlarını bir ölçüde terk etmeleri, ya da egemenliklerini "özgür iradeleriyle" kısıtlamaları sonucunda çözüme kavuşabilir. Bu açıdan bakıldığında, uluslararası sorunlara bulunacak siyasal ve hukuksal çözümler, her aşamada "devletlerarası işbirliğini" zorunlu kılar.[284]

Bilişim bağlantılı suçlarla mücadele de uluslar arası işbirliğinin zorunlu olduğu bir alan olduğu için bu doğrultuda özellikle uluslar üstü kurumlar tarafından üye ülkeleri bağlayıcı nitelikte hukuki düzenlemeler yapılmaktadır. Bu düzenlemelere topluluklara üye ülkeler bazı çekincelerinden dolayı hemen taraf olamayabilmektedir. Bazı durumlarda da sözleşmelere taraf olan ülkeler kendi hukuki sistemlerinde gerekli düzenlemeleri yapmadıklarından sözleşmelerde hedeflenen aktif işbirliği tam sağlanmaktadır.

3.2.3.1. Avrupa Konseyince Yapılan Çalışmalar

Merkezi Strasbourg'da (Fransa) bulunan Avrupa Konseyi'ne 47 devlet üyedir. Avrupa Konseyi (İngilizce: Council of Europe; Fransızca: Conseil de l'Europe) 1949 yılında Avrupa çapında insan hakları, demokrasi ve hukukun üstünlüğünü savunmak amacıyla Avrupa çapında kurulmuş hükümetler arası bir kuruluştur. Avrupa Birliği'nden farklı bir örgütlenmedir. Konsey, çocuk hakları, uyuşturucu bağımlılığı, hoşgörüsüzlük, azınlıkların korunması, biyoetik ve gençlere daha geniş eğitim fırsatı sağlanması alanlarında Avrupa vatandaşlarının artan kaygılarına cevaplar getirmiştir. Avrupa Konseyi'nin geniş kapsamlı girişimleri çoğu kez, ulusal yasal uygulamaları

[284] edubilim.com, (2008), "Topluluk Hukukunun Uluslar Üstü (Supranasyonal) Niteliği", http://www.edubilim.com/ana/odev-arsivi/hukuk/1-topluluk-hukukunun-uluslarustu-supranasyonal-niteligi/details.html, (Erişim Tarihi: 09.12.2010).

birbiri ile ve Konsey'in standartları ile uyumlu kılmak için hazırlanan sözleşmeler şeklini alır. Bu anlaşmalar Bakanlar Komitesinin üye devletlere yönelik olan ve ortak sorunlara çözüm bulmakta kesin etki sağlayan kararları ve tavsiyeleri ile desteklenir.[285]

Avrupa Konseyi İnternet suçları ile ilgili ilk çalışmalarını 80'li yılların sonlarına doğru gerçekleştirmiştir. Konsey bilgisayar suçlarıyla ilgili Uzmanlar Komitesi atamıştır. Konseyin böyle bir çalışma başlatmasının amacı ceza kanunları ile düzenlenmesi gerekli olan eylemlerin hangileri olduğunu açık bir şekilde tespit etmek, sivil özgürlük ve güvenlik kavramları arasındaki uyuşmazlığın nasıl aşılacağı konusunda üye ülkelere yol göstermektir Avrupa Konseyi 1995 yılında ceza usul yasalarının bilişim teknolojileri ile birleştirilmesiyle ilgili problemleri ele almıştır. 11 Eylül 1995 tarihinde Bakanlar Komitesi tarafından ele alınan metin ile bilişim teknolojilerinin getirdiği yeniliklere uygun olarak ceza usul yasalarındaki soruşturma ve el koymaya ait hükümlerin revize edilmesi, elektronik delil, şifreleme sistemlerinin kullanılması, uluslar arası işbirliği başlıkları altında kurallar belirlemiştir. [286]

Avrupa Konseyi'nin siber suçlar alanındaki en kapsamlı çalışması ise bizim de 11 Kasım 2010 tarihinden imzaladığımız "Avrupa Konseyi Siber Suç Sözleşmesi (Convention on Cybercrime)" olmuştur.

Sözleşmenin amacı önsöz bölümünde açıklanmıştır. Buna göre sözleşme devletler arasında işbirliği çerçevesinde toplumları siber suçlara karşı korumak için ortak yasal düzenlemelerin yapılmasını ve ortak bir cezai politikanın öncelikli olarak kabul edilmesini hedeflemektedir.[287]

Sözleşmede başlıkları halinde bölümler ayrılmış ve altlarında maddeler sıralanmıştır. Sözleşmedeki başlıklara bakacak olursak;

---

[285] Avrupa Konseyi (t.y.), "Biz Kimiz?", http://www.avrupakonseyi.org.tr/bizkimiz.htm, (Erişim Tarihi: 10.12.2010).
[286] Yıldız, Sevil, (t.y.), "Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi", http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/Sevil%20YILDIZ/YILDIZ,%20SEV%C4%B0L.pdf, (Erişim Tarihi: 10.12.2010).
[287] Avrupa Konseyi, (2001), "Convention on Cybercrime", http://conventions.coe.int/treaty/en/treaties/html/185.htm, (Erişim Tarihi: 10.12.2010).

Bölüm 1: Ceza Hukuku

1. Bilgisayar sistemlerinin ve verilerinin ulaşılabilirliği, bütünlüğü ve güvenliğine yönelik suçlar
2. Bilgisayar bağlantılı suçlar
3. İçerikle ilgili suçlar
4. Telif haklarının ihlaline bağlı suçlar

Bölüm 2: Usul Hukuku

1. Genel hükümler
2. Depolanan bilgisayar verilerinin hızlıca muhafaza altına alınması
3. Üretim emri
4. Depolanan bilgisayar verilerinin aranması ve zaptı
5. Bilgisayar verilerin gerçek zamanlı toplanması

Bölüm 3: Uluslar Arası İşbirliği

1. Uluslar arası işbirliği ile ilgili genel prensipler
2. Suçlu iadesine yönelik prensipler
3. Karşılıklı yardımlaşmaya yönelik genel prensipler
4. Uluslar arası işbirliği sözleşmelerinin olmadığı durumlarda karşılıklı işbirliği taleplerine yönelik prosedürler

Bölüm 4: Özel Hükümler

1. Geçici önlemlere yönelik karşılıklı işbirliği
2. Soruşturma yetkisine yönelik karşılıklı işbirliği
3. 7/24 Bağlantı

Sözleşmede başlıklar halinde sıralanan konulara baktığımızda hem bilişim suçlarına yönelik hem de bilişim yoluyla işlenen suçlara yönelik düzenlemelerin olduğunu görmekteyiz. Ayrıca adli bilişim sürecine ve soruşturma (kovuşturma) sürecine yönelik düzenlemelerinde yer aldığını görmekteyiz. Bu bakımdan gerçekten detaylı bir sözleşmedir.

Avrupa Konseyi Siber Suç Sözleşmesini incelediğimizde "İnternet Ortamında Ceza Sorumluluğunun Avrupa Ana İlkeleri" olarak da isimlendirilebilen dört ilkeden bahsedilebilir,[288] bunlar;

1. İlke: Suçlarla ilgili ceza sorumluluğunun sınırlarının çizilmesinde başta düşünce ve ifade özgürlüğü ile iletişim özgürlüklerin gereklerine uyulması

2. İlke: Bilgisayarla işlenen veya bilgisayarla ilişkili suçların belirlenip düzenlenmesinde ortak bir minimum standarda uyulması

3. İlke: Eylemin hukuka aykırı olması

4. İlke: Eylemin kasten işlenmesi

28 Ocak 2003 tarihinde Avrupa Konseyi Siber Suç Sözleşmesine ek olarak "Bilgisayar Yoluyla Irkçılık ve Yabancı Düşmanlığı Suçları (Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems)" isimli bir protokol imzaya açılmıştır.[289]

Avrupa Konseyi Siber Suç Sözleşmesi'ni konseye üye kırk yedi ülkenin yanı sıra Arjantin, Avustralya, Kanada, Şili, Kosta Rika, Dominik Cumhuriyeti, Japonya, Meksika, Filipinler, Güney Afrika ve Amerika Birleşik Devletleri de imza atmışlardır.[290]

3.2.3.2. OECD Tarafından Yapılan Çalışmalar

14 Aralık 1960 tarihinde imzalanan Paris Sözleşmesi'ne dayanılarak kurulan İktisadi İşbirliği ve Kalkınma Teşkilatı, savaş yıkıntıları içindeki Avrupa'nın Marshall Planı çerçevesinde yeniden yapılandırılması amacıyla 1948 yılında kurulan Avrupa Ekonomik İşbirliği Örgütü'nün (OEEC) yerini almıştır. Önceleri Avrupa İktisadi İşbirliği Örgütü (OEEC) adı altında, Marshall Planı'nın uygulanmasını kolaylaştırmak amacıyla kurulan bu örgütün adı 30 Eylül 1961'de Ekonomik İşbirliği

[288] Ergün, (2008), a.g.e., ss.60-61.
[289] Avrupa Konseyi, (2001), "Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", http://conventions.coe.int/treaty/en/treaties/html/189.htm, (Erişim Tarihi: 10.12.2010).
[290] Avrupa Konseyi, (2001), "Convention on Cybercrime - List of declarations, reservations and other communications", http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, (Erişim Tarihi: 10.12.2010).

ve Kalkınma Örgütü (OECD) şeklinde değiştirilmiştir. OECD, ülkeleri yönlendirmek için çeşitli etkileme araçları kullanır. OECD, üye ülkelerle irtibatı sağlamak ve sürekli etkileşim halinde olmak için üye ülkelerde temsilcilikler açmaktadır. Temsilcilikler, ya merkezi yönetimde yer alan üst düzey kamu kurumlarında açılmış ya da üst düzey kamu kurumlarıyla ilişkilendirilmiştir. OECD, sadece kendisine üye olan 34 ülkeyle ilişki yürütmemekte, üye olmayan birçok ülkeyle de ilişkileri bulunmaktadır.[291]

Ülkemizin de üyesi olduğu OECD aslında bilişim bağlantılı suçlar açısından ilk uluslar arası çalışmaların yapıldığı topluluktur. Bu çalışmaların amacı bilişim alanındaki suçlarda ülkelerin ceza yasalarının belli bir standardı ve paralelliği yakalamasını sağlamaktı. 1983 yılında başlayan çalışmalar 1986 yılında sonuçlanmış ve "Computer-Related Crime: Analysis of Legal Policy (Bilgisyar Bağlantılı Suç: Hukuki Politikaların Analizi)"[292] başlıklı bir rapor hazırlanmıştır. Raporda ülkelerin ceza kanununda en azından suç olarak tanımlanması gereken dört eyleme değinilmiştir. Bunlar;

1. Bilgisayar yoluyla dolandırıcılık ve sahtecilik
2. Bilgisayar programlarını ve verilerini değiştirme
3. Telif hakları
4. Bilgisayarların veya iletişim sistemlerinin iletişiminin veya diğer fonksiyonlarının engellenmesi

Ayrıca OECD tarafından 1992 yılında "OECD Guidelines for the Security of Information Systems and Networks (Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri)"[293] yayınlanmıştır.

Bilgi sistem ve ağlarını geliştiren, sahip olan, yöneten, hizmete sunan ve kullanan hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar için bilgi

[291] Dış Ekonomik İlişkiler Kurulu, (t.y.), "İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)", http://www.deik.org.tr/pages/TR/DEIK_CokTarafliKuruluslar.aspx?ctID=4&IKID=10, (Erişim Tarihi:11.12.2010).
[292] wikisource.org , (2010), "International Review Of Criminal Policy - Nos. 43 And 44/Regional Action", http://en.wikisource.org/wiki/International_review_of_criminal_policy_-_Nos._43_and_44/Regional_action, (Erişim Tarihi:11.12.2010).
[293] Organisation for Economic Co-operation and Development , (t.y.), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security", http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00&&en-USS_01DBC.html, (Erişim Tarihi:11.12.2010).

sistemlerinin güvenliğine ilişkin rehber ilkeler önerilmektedir. Üye ülkelerin; "Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeler: Güvenlik Kültürüne Doğru" adlı ilkeler uyarınca bir güvenlik kültürünü benimseyerek ve teşvik ederek mevcut politika, uygulama, önlem ya da prosedürlerini değiştirmelerini ya da yenilerini oluşturmalarını, rehber ilkeleri uygulamak için ulusal ve uluslar arası düzeyde işbirliği yapmalarını, koordinasyon sağlamalarını, güvenlik kültürünü teşvik etmek ve tüm kullanıcıları sorumluluk alarak Rehber İlkelerini kendilerine düşen rollere uygun bir şekilde uygulamak amacıyla gerekli adımları atmaya teşvik etmek için Rehber İlkelerini hükümetler, iş çevreleri, diğer örgütler ve bireysel kullanıcılar da dâhil olmak üzere tüm kamu ve özel sektöre dağıtmalarını amaçlamaktadır.[294]

OECD tarafından yapılan çalışmaların tarihleri de dikkate alınarak değerlendirildiğinde çok genel prensipler üzerine kurulu olduğunu görmekteyiz. Son yıllarda yapılan diğer uluslar arası düzenlemelerin ise daha spesifik ve yaşanan sorunları çözmeye odaklı olduğunu görmekteyiz.

3.2.3.3. G8 Tarafından Yapılan Çalışmalar

G8 ülkeleri tarafından 1975'ten beri yıllık ekonomi zirveleri düzenlemektedirler. G8 Uluslararası hükümetler formu olup, Kanada, Fransa, Almanya, İtalya, Japonya, Rusya, İngiltere ve Amerika dünya ekonomisinin yaklaşık %65 ini temsil ederler. Grubun aktiviteleri yıl bazında konferanslar ve politik araştırmaları içerir. Üye ülkelerin hükümet başkanlarının yıllık zirve toplantısına katılması ile doruğuna ulaşır. Her yıl G8'in üye devletleri grubun başkanlık görevini üzerine alır. Başkanlığı elinde bulunduran, grubun gündemini belirler ve o yılki toplantı için ev sahipliği yapar.[295]

G8 bünyesinde kurlu olan alt çalışma gruplarından birisi de "Yüksek teknoloji Suçları Alt Çalışma Grubu"[296] dur. Bu alt grubun kurulma amacı G8 ülkelerinin bilgisayarlar, bilgisayar ağları ve diğer teknolojik alanlarda işlenen suçlarda ortak bir önleme, soruşturma ve kovuşturma politikasını tesis etmektir.

---

[294] Organisation for Economic Co-operation and Development, (2002), "Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri – Güvenlik Kültürüne Doğru", http://www.oecd.org/dataoecd/42/59/32493366.PDF, (Erişim Tarihi: 11.12.2010).
[295] wikipedia.org , (2010), "G8", http://tr.wikipedia.org/wiki/G8, (Erişim Tarihi: 11.12.2010).
[296] justice.gov, (2004), "Meeting of G8 Justice and Home Affairs Ministers", http://www.justice.gov/criminal/cybercrime/g82004/g8_background.html, (Erişim Tarihi: 11.12.2010).

1997 yılında G8 ülkelerinin iç işleri bakanları Washington'da bir araya gelmişler ve ileri teknoloji suçlarıyla mücadele için on tane prensip kararı almışlardır.[297] Bu kararlara bakacak olursak;

1. Bilgi teknolojilerini kötüye kullananlar için güvenli alanlar olmamalıdır.
2. İleri teknoloji suçlarının nerede işlendiğinde bakılmaksızın üye ülkeler tarafından soruşturma ve kovuşturma evresinde koordine sağlanmalıdır.
3. Güvenlik kuvvetleri ileri teknoloji suçları ile mücadele için eğitilmeli ve yeterli donanımla donatılmalıdır.
4. Bilgisayar sistemlerinin ve verilerin erişilebilirliği, güvenliği ve bütünlüğü kanuni düzenlemelerle koruma altına alınmalıdır ayrıca illegal erişim ve zarar vermeler için ciddi cezalar getirilmelidir.
5. Suç soruşturmasında hayati öneme sahip olan elektronik delillere kolay erişim ve koruma altına alma kanunen düzenlenmelidir.
6. Uluslar arası ileri teknoloji suçlarında dijital delillerin toplanması ve takası karşılıklı işbirliği politikalarıyla sağlanmalıdır.
7. Bir ülke diğer bir ülkenin halka açık elektronik verilerine erişmede izine gerek duymamalıdır.
8. Suç soruşturmasında ve kovuşturmasında dijital delillerin toplanmasıyla ilgili adli bilişim standartları geliştirilmeli ve bu alanda istihdam yaratılmalıdır.
9. Mümkün olduğu ölçüde, bilgi ve iletişim sistemleri, bilgisayar ağlarının kötüye kullanımını engelleyecek ve tespit edecek şekilde dizayn edilmeli ve suçluların izlerini takip etmeyi ve delil toplamayı kolaylaştırmalıdır.
10. Bu alandaki çalışmalar gereksiz emek sarf etmemek için diğer ilgili uluslar arası kurumların da koordinesinde yürütülmelidir.

G8 ülkeleri dünyanın en zengin ve gelişmiş ülkeleri kabul edildiğinden teknolojiye paralel olan bilişim bağlantılı suçlarla mücadelede önderlik beklenen topluluklardandır. Nitekim bu alandaki suçlarla belki de en önce karşılaşan ülkeler

[297] Goodman, Marc D. ve Brenner, Susan W., (2002), "The Emerging Consensus on Criminal Conduct in Cyberspace", http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php, (Erişim Tarihi: 11.12.2010).

olduğu için benzer uluslar arası işbirliği ve koordine amaçlı düzenlemelere örnek olacak çalışmalar yürütmüşlerdir.

3.2.3.4. Birleşmiş Milletler Tarafından Yapılan Çalışmalar

Birleşmiş Milletler Örgütü ya da kısaca Birleşmiş Milletler (BM), 24 Ekim 1945'te kurulmuş dünya barışını, güvenliğini korumak ve uluslar arasında ekonomik, toplumsal ve kültürel bir iş birliği oluşturmak için kurulan uluslararası bir örgüttür. Birleşmiş Milletler kendini "adalet ve güvenliği, ekonomik kalkınma ve sosyal eşitliği uluslararasında tüm ülkelere sağlamayı amaç edinmiş küresel bir kuruluş" olarak tanımlamaktadır. Uluslararası İlişkilerde, kuvvet kullanılmasını ilk olarak evrensel düzeyde yasaklayan ilk antlaşma Birleşmiş Milletler Antlaşması'dır. Örgüte üye 192 ülke vardır. Örgütün yönetimi New York'ta bulunan genel merkezinden yürütülür ve üye ülkelerle her yıl düzenli olarak yapılan toplantılar yine bu genel merkezde gerçekleştirilir. Örgüt yapısal olarak idari bölümlere ayrılmıştır; Genel Kurul, Güvenlik Konseyi, Ekonomik ve Sosyal Konsey, Yönetim Konseyi, Genel Sekreterlik ve Uluslararası Adalet Divanı. Örgütün en göz önündeki mercisi Genel Sekreterdir.[298]

15 Kasım 2000 tarihinde BM tarafından sınıraşan organize suçlarla mücadele etmek için "The United Nations Convention against Transnational Organized Crime (Birleşmiş Milletler Sınıraşan Organize Suçlarla Mücadele Sözleşmesi)" hazırlanmıştır.[299] Türkiye tarafından da sözleşme 4803 numaralı "Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek Kara, Deniz Ve Hava Yoluyla Göçmen Kaçakçılığına Karşı Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun" ile kabul edilmiştir.[300]

---

[298] wikipedia.org, (2010), "Birleşmiş Milletler", http://tr.wikipedia.org/wiki/Birle%C5%9Fmi%C5%9F_Milletler, (Erişim Tarihi: 12.12:2010).

[299] United Nations Office on Drugs and Crime, (t.y.), "United Nations Convention against Transnational Organized Crime and its Protocols", http://www.unodc.org/unodc/en/treaties/CTOC/index.html, (Erişim Tarihi: 12.12:2010).

[300] "TBMM: Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek Kara, Deniz Ve Hava Yoluyla Göçmen Kaçakçılığına Karşı Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun", http://www.tbmm.gov.tr/kanunlar/k4803.html, (Erişim Tarihi: 12.12.2010).

Daha önceden de bahsettiğimiz gibi bilişim bağlantılı suçların sınır araşan özelliği açısından bu düzenleme önem arz etmektedir. Sözleşmenin teknolojik suçlarla ilgili maddelerine bakacak olursak;[301]

Madde 27: Yasa Uygulamada İşbirliği

(3) Taraf Devletler modern teknolojinin kullanılması yoluyla işlenmiş sınıraşan örgütlü suçlarla mücadele etmek amacıyla, olanakları dâhilinde işbirliğinde bulunmak için çaba göstereceklerdir.

Madde 29: Eğitim ve Teknik Yardım

(1) Her Taraf Devlet, gerekli olduğu ölçüde, savcılar, sorgu hakimleri ve gümrük personeli ve bu Sözleşmede belirtilen suçların önlenmesinden, ortaya çıkarılmasından, kontrolünden sorumlu diğer personel dahil, yasa uygulayıcı personeli için özel eğitim programlan başlatacak, yürütecek ve geliştirecektir. Bu tür programlar personelin başka ülkede veya kuruluşta görevlendirilmesini ve personel değişimlerini kapsayabilir. Bu tür programlar, iç hukuka uygun olduğu ölçüde ve özellikle aşağıdakileri içerecektir:

(h) Bilgisayarların, telekomünikasyon ağlarının veya modern teknolojinin diğer biçimlerinin kullanılması vasıtasıyla işlenen sınıraşan örgütlü suçla mücadelede kullanılan yöntemler;

Birleşmiş Milletler bünyesinde çalışan kurullardan biri de Ekonomok ve Sosyal Konsey'e bağlı "Commission on Crime Prevention and Criminal Justice (Birleşmiş Milletler Suçun Önlenmesi ve Ceza Adaleti Komisyonu)"[302] dur. Bu komisyon tarafından 1992'den itibaren her yıl bir kongre düzenlenmektedir. Kongrelerde ele alından konulardan birisi de siber suçlardır. Bu alanda çalıştaylar düzenlenmekte ve üye ülkelere tavsiye niteliğinde kararlar alınmaktadır.[303]

[301] Türkiye Büyük Millet Meclisi, (2003), "Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesi", http://www.unicankara.org.tr/doc_pdf/sinirasan.doc, (Erişim Tarihi: 12.12.2010).
[302] United Nations Office on Drugs and Crime, (t.y.), "The Commission on Crime Prevention and Criminal Justice", http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html, (Erişim Tarihi: 12.12.2010).
[303] Computer Crime Research Center, (2003) "UN recommendations on fighting cybercrime", http://www.crime-research.org/news/13.05.2005/1225/, (Erişim Tarihi: 12.12.2010).

Komisyon tarafından 12-19 Nisan tarihleri arasında Brezilya'da "On İkinci Birleşmiş Milletler Suçu Önleme ve Ceza Adaleti Kongresi" düzenlenmiştir.[304]

Bu kongrede siber suçlar gündeme alınmış[305] ve Rusya ve Çin tarafından desteklenen bir antlaşma teklifi getirilmiştir. Antlaşma Birleşmiş Milletler bünyesinde siber suçları önleme amacını taşıyan bir işbirliği antlaşmasıydı. Ancak antlaşma AB, ABD ve Kanada tarafından kabul edilmeyerek Birleşmiş Milletler tarafından reddedilmiştir. Antlaşmayı kabul etmeyen ülkeler buna gerekçe olarak daha önceden imza attıkları ve on yıla yakındır yürürlükte olan "Avrupa Konseyi Siber Suç Sözleşmesi'ni" gerekçe göstermişler ve yeni bir antlaşmaya gerek olmadığını iddia etmişlerdir.[306]

3.2.3.5. Europol ve Interpol Tarafından Yapılan Çalışmalar

Avrupa Polis Ofisi ya da kısaca Europol, Avrupa Birliği üyesi ülkeler ile birliğin ortaklık kurduğu diğer ülkelerin güvenlik güçleri arasında, uluslararası organize suçlar ve terörizm konusunda iş birliği ve etkili çalışma ortamı sağlamak amacıyla kurulmuş bir birimdir. [307] Interpol, Uluslararası Polis Teşkilatı (ing. International Criminal Police Organization - Interpol), 1923 yılında uluslararası polis işbirliği sağlamak amacıyla kurulmuştur. Interpol, Birleşmiş Milletler'den sonra, dünyanın ikinci büyük uluslararası örgütüdür; şu anda 184 üye ülkeye sahiptir.[308]

Interpol bünyesinde kurulan ve uzun yıllardır siber suçlar alanında hizmet veren bir çalışma grubu vardır.[309] Çalışma grubu Avrupa, Afrika, Asya – Güney

---

[304] United Nations Office on Drugs and Crime, (t.y.), "Previous Sessions And Documents Of The Commission On Crime Prevention And Criminal Justice", http://www.unodc.org/unodc/commissions/CCPCJ/session/index.html, (Erişim Tarihi: 12.12.2010).
[305] United Nations Office on Drugs and Crime, (2010), "Item 8 Of The Provisional Agenda: Recent Developments İn The Use Of Science And Technology By Offenders And By Competent Authorities İn Fighting Crime, İncluding The Case Of Cybercrime", http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf, (Erişim Tarihi: 12.12.2010).
[306] Ballard, Mark, (2010), "UN rejects international cybercrime treaty", http://www.computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm, (Erişim Tarihi: 12.12.2010)
[307] Europol, (t.y.), "EUROPOL, the European Police Office", http://www.europol.europa.eu/, (Erişim Tarihi: 12.12.2010).
[308] Interpol, (t.y), "Interpol", http://www.interpol.int/, (Erişim Tarihi: 12.12.2010).
[309] Interpol, (2010), "Information Technology Crime", http://www.interpol.int/public/TechnologyCrime/default.asp, (Erişim Tarihi: 12.12.2010).

Pasifik ve Latin Amerika olmak üzere dört farklı bölgesel grupta çalışmalarına devam etmektedir.[310]

Europol bünyesinde "Avrupa Birliği Siber Suç Görev Gücü" adında bir platform 2010 yılında kurulmuştur. Platform özellikle İnternet üzerinden işlenen siber suçlarla mücadele konusunda çalışmalar yapmakta ve projeler üretmektedir.[311]

3.2.4. Doğrudan ve Dolaylı Bilişim Suçu Kavramları

Bazı kaynaklarda "bilişim suçu" ve "bilişim yoluyla işlene suç" ayrımı yerine "doğrudan bilişim suçu" ve "dolaylı bilişim suçu" ayrımı kabul edilmektedir. Burada Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlıklı bölümünde düzenlenen suçlar için "bilişim suçu" ancak Türk Ceza Kanunu'nun diğer suçlarının nitelikli ve ağırlaştırıcı sebebi olan bilişim yoluyla işlenmesi halinde "dolaylı bilişim suçu" kavramı kullanılmaktadır.[312]

Bize göre bu yaklaşım içinde bazı çelişkileri barındırmaktadır. "Dolaylı bilişim suçu" kavramı tercih edilirken bir suçun yine "bilişim suçu" olduğu kabul edilmektedir. Ancak bir suçun bilişim teknolojileri kullanılarak işlenmesinin o suçu "bilişim suçu" olarak nitelendirilmesini mantıklı kılmamaktadır. Evet, hem ülkemizde hem de dünyada artık bilişim suçları dışındaki bazı suçlarda çok yoğun şekilde bilişim teknolojileri kullanılmaktadır. Özellikle "çocuk pornografisi" ve "internet üzerinden kumar" gibi suçlarda internet ortamından faydalanıldığı için bilişim suçları ile karıştırılmaktadır.

Mevcut durumda bu gibi birkaç suç için "dolaylı bilişim suçu" terimini kullanmak pek de sakıncalı değil gibi gözükebilir. Fakat gelecekte bugüne nazaran daha birçok suçun bilişim teknolojileri ve özellikle de internet ortamında işlenebileceğini düşündüğümüz zaman suçların büyük bir kısmını "dolaylı bilişim suçu" olarak nitelendirmek tabi ki mantıklı olmayacaktır.

---

[310] Interpol, (2010), "Regional Working Parties", http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp, (Erişim Tarihi: 12.12.2010).
[311] Europol, (2010), "European Union Cybercrime Task Force", http://www.europol.europa.eu/index.asp?page=news&news=pr100622.htm, (Erişim Tarihi: 12.12.2010).
[312] Parlar, Ali, (2011), *Türk Ceza Hukuku'nda Bilişim Suçları*, Ankara: Bilge Yayınevi, Önsöz.

Peki, neden bazı kaynaklarda böyle bir ayrıma gidilme gereği duyulmuştur? Bize göre bu durumun birkaç sebebi olabilir. Bunlardan bazıları şunlar olabilir;

- Bazı güncel suçlarda bilişim suçu olmamasına rağmen çok yoğun miktarda bilişim teknolojileri kullanılmaktadır ve bu durum konuyla doğrudan ilgili uygulayıcıları dahi şaşırtabilmektedir.
- "Bilişim bağlantılı suçlar" farklı ülkelerin mevzuatlarında farklı şekillerde düzenlenmektedir. Başka ülkelerde "bilişim suçu" olarak kabul edilen eylemler bizim hukuk sistemimizde geleneksel suçların bilişim yoluyla işlenmesi ve geleneksel suçun ağırlaştırıcı sebebi olarak düzenlenmektedir. Çalışmalarından yabancı kaynaklardan yararlananlar bu durumda dolayı yanılgıya düşebilmektedir.
- Özellikle konunun doğrudan uygulayıcısı olmayan ama dolaylı olarak ilgilenen hukukçular, bilgi güvenliği uzmanları, mühendisler, akademisyenler ve basın, yayın mensupları bu alanda ortaya koydukları haberlerde, çalışmalarda, konuşmalarında olması gereken duruma göre değil kendi donanımlarına göre kavramları kullanmaktadırlar. Bu gibi durumlarda bu kaynaklardan faydalanılarak yapılan araştırmalarda yanılgıya sık düşülmektedir.

Aslında hukuk sistemimiz açısından "doğrudan ve dolaylı bilişim suçu" kavramları illa da kullanılacaksa bunun kullanılabileceği bir alan vardır. "Bilişim Alanda Suçlar" başlığı altında düzenlenen ve çalışmamızın birinci bölümünde detaylarıyla açıkladığımız suçlardan "Hukuka Aykırı Olarak Bilişim Sistemine Girme ve Orada Kalmaya Devam Etme (TCK Madde 243) suçu" ve "Bilişim Sisteminin İşleyişinin Engellenmesi, Bozulması, Verilerin Yok Edilmesi veya Değiştirilmesi (TCK Madde 244)" suçu "doğrudan bilişim suçu" olarak kabul edilebilir. "Banka veya Kredi Kartlarının Kötüye Kullanılması (TCK Madde 245)" suçu "dolaylı bilişim suçu" olarak kabul edilebilir.

Eğer bir ayrım yapılacaksa bu tür bir ayrıma girilmesi daha gerçekçi olacaktır. Çünkü 245. maddede

> *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,…

İfadesi geçmektedir. Burada bir kişinin başkasına ait bir kredi kartını çalarak herhangi bir yerden alışveriş yapması, suçlu tarafından hiçbir bilişim teknolojisi kullanılmamasına rağmen "bilişim suçu" olarak kabul edilmektedir. Bu suç türünün neden "bilişim suçu" olarak kabul edildiğini ve neden Türk Ceza Kanunu'nun "Bilişim Alanında Suçlar" başlığı altında düzenlendiğini yine birinci bölümde detaylarıyla anlattık.

3.3. SORUŞTURMA VE KOVUŞTURMA EVRELERİ AÇISINDAN

Bilişim suçları ve bilişim yoluyla işlenen suçlar soruşturma ve kovuşturma evreleri açısından da benzerlikler ve farklılıklar ihtiva etmektedir. Bu benzerlik ve farklılıkların net olarak anlaşılması sağlıklı bir yargılama sürecinin ilk gereği olarak karşımıza çıkmaktadır.

Öncelikle üzerinde durulması gereken konu bilişim suçları ve bilişim yoluyla işlenen suçlarda soruşturma ve kovuşturmada görevli birimler farklılıklar arz etmektedir. Soruşturma aşamasında emniyet birimleri içerisindeki farklı birimler bilişim suçları ve bilişim yoluyla işlenen suçlarda soruşturmada görev alırlar. Bilişim suçlarıyla ilgili kaçakçılık ve organize suçlarla mücadele birimleri altında görev yapan bilişim suçları bölümü soruşturmada görev alırken bilişim yoluyla işlenen suçlarda yine suçun türüne göre ilgili emniyet birimi görev almaktadır. Örneğin bilişim yoluyla işlenen asayiş suçlarında asayiş birimleri, bilişim yoluyla işlenen terör suçlarında terörle mücadele birimleri soruşturma evresinde görev almaktadırlar.

Adliyeler açısından da benzer bir ayrım ilin durumuna göre mevcuttur. Özellikle büyük illerde sadece bilişim suçlarıyla ilgilenen savcılar bulunmaktadır ancak nüfusu küçük illerde savcı sayısı da buna paralel olarak az olduğundan aynı savcı hem bilişim suçlarında hem de bilişim yoluyla işlenen diğer suçlarda soruşturma evresini yürütmektedir.

Kovuşturma açısından durum biraz daha farklıdır. Büyük illerde mahkemeler (ceza mahkemeleri) aynı mahkemenin kovuşturma yetkisine giren suç yükünü göre eşit dağıtılmaktadır. Bu yüzden sadece bilişim suçlarında kovuşturma yapmakla görevli bir mahkeme bulunmamaktadır. Zaten nüfusu küçük illerdeki mahkemeler

için de böyle bir ayrım mümkün değildir. Yargıtay'da ise dairelerin (ceza daireleri) sorumlu oldukları suçlar madde madde dağıtılmış bulunmaktadır. Ancak bir ceza dairesi birden fazla suçla ilgili görevlidir. Örneğin mevcut durumda bilişim suçları ile ilgili görevlendirilmiş daire on birinci ceza dairesidir ve bu daire dolandırıcılık, resmi belgede sahtecilik, hileli iflas gibi başka birçok suç türüyle ilgili de görevlendirilmiştir.[313]

Soruşturma evresinin en önemli ayağını oluşturan delil toplama açısından hem bilişim suçlarında hem de bilişim yoluyla işlenen suçlarda bilişim ortamı ortak olduğu için benzer uygulamalar mevcuttur. Adli bilişim süreci her iki suç türünde de uygulanması kaçınılmaz bir delil toplama yöntemidir. Bunun yanında internet ortamına bağlı deliller (IP adresleri, e-posta trafikleri, anında mesajlaşma kayıtları gibi) açısından yargı kurumları ile özel sektör işbirliği her iki durumda da gereklidir.

Bilişim suçlarının yapısı gereği organize ve uluslar arası olarak işlendiğinden bahsetmiştik. Aynı boyut klasik suçların bilişim yoluyla işlenmesinde de karşımıza çıkmaktadır. Bu nedenle genel olarak bilişim bağlantılı suçlarda ulusal işbirliğinin yanı sıra uluslar arası işbirliği hem soruşturma hem de kovuşturma evresinde önem kazanmaktadır.

Mağdur ve faili belirlemede bilişim suçlarında yaşanan sıkıntılar bilişim yoluyla işlenen suçlar da kısmen daha azdır. Çünkü bilişim yoluyla işlenen suçlarda failin hedefi daha net olarak tespit edilebildiğinden buna göre mağdur(lar) da net tespit edilebilmektedir. Ancak bilişim suçlarında bilişim sistemleri hedef alındığından bu bilişim sistemlerinden faydalanan birçok kişi bir anda mağdur olabilmektedir.

Bilişim suçlarında faillerin yakalanması zaman ve mekân açısından çok sıkıntılı olabilmektedir çünkü bu suçlar zamandan ve mekândan bağımsız gerçekleşebilmektedir. Aynı durum klasik suçların bilişim yoluyla işlenmesinde yani bilişim yoluyla işlenen suçlarda da ciddi bir dezavantaj olarak soruşturma ve kovuşturma evresini etkilemektedir. Örneğin cinsel taciz suçunda fail ile mağdur zaman ve mekân açısından aynı yerde dururken bu suçun bilişim yoluyla işlenmesi

[313] Yargıtay, (t.y.), "Yargıtay On Birinci Ceza Dairesi", http://www.yargitay.gov.tr/content/view/43/43/, (Erişim Tarihi: 16.12.2010).

(örneğin e-posta yoluyla) durumunda mağdurdan yola çıkarak zaman ve mekân açısından failin yerini tespit etmek çok daha zor olabilmektedir.

Soruşturma ve kovuşturma evresinde görevli birimlerin bilişim suçlarında uzman hale gelmesinin yanı sıra bilişim yoluyla işlenen suçlarla mücadele ederken de bilişim teknolojileri konusunda birimlerin genel bir bilgi birikimine sahip olması faydalı olacaktır.

3.4. İSTATİSTİKÎ AÇIDAN

Bilişim teknolojilerinin suç dünyasında kullanımının zaman içinde nasıl değiştiğinden önceki bölümlerde etraflıca bahsetmiştik. Bu nedenle bu alandaki istatistiklerde bilişim bağlantılı suçlarda değişiklikler nedeniyle standart bir halde değildir.

İstatistiklerin tutulduğu zaman, istatistikleri tutan ülkenin hukuki düzenlemeleri veya istatistikî verileri toplayan kuruma (özel ya da kamu) göre değişik istatistikî sonuçlar elde edilmiştir.

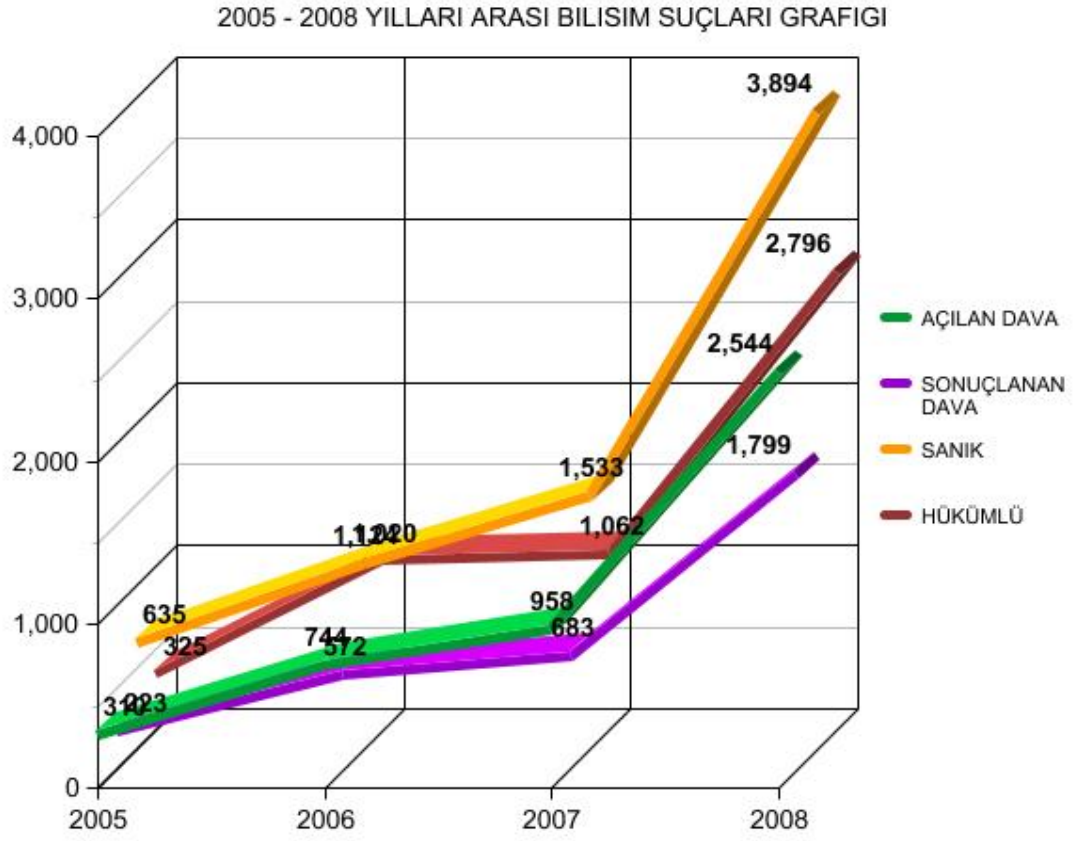
3.4.1. Ülkemiz İstatistikleri Açısından

Ülkemizde bilişim suçları ile ilgili olarak emniyet birimleri kendi istatistiklerini tutarken adliyeler tarafından da açılan ve karara bağlanan davalarla ilgili olarak ayrı ayrı istatistikler tutulmaktadır. Ancak bilişim yoluyla işlenen suçlara yönelik adliyeler tarafından ayrı bir istatistik tutulmamaktadır. Sadece suç hangi suçu oluşturuyorsa o suçun toplam sayıları üzerinden istatistikler mevcuttur. Örneğin "intihara yönlendirme" suçunun sayısı bilinmekte ancak bunun ne kadarının bilişim yoluyla işlendiği istatistikî olarak tutulmamaktadır.

Ancak emniyet birimleri tarafından ilgili şubeler sorumluluk alanlarına giren suçların ne kadarının bilişim yoluyla işlendiğinin istatistiklerini tutmaktadırlar. Bununla birlikte suç aracı olarak kullanılan eşyalar arasında bilişim ürünlerinin de kullanılma durumları suç veritabanlarında tutulmaktadır.

2005 – 2008 yılları arasındaki adliyelere yansımış olan bilişim suçları istatistiklerine bakacak olursak;[314]

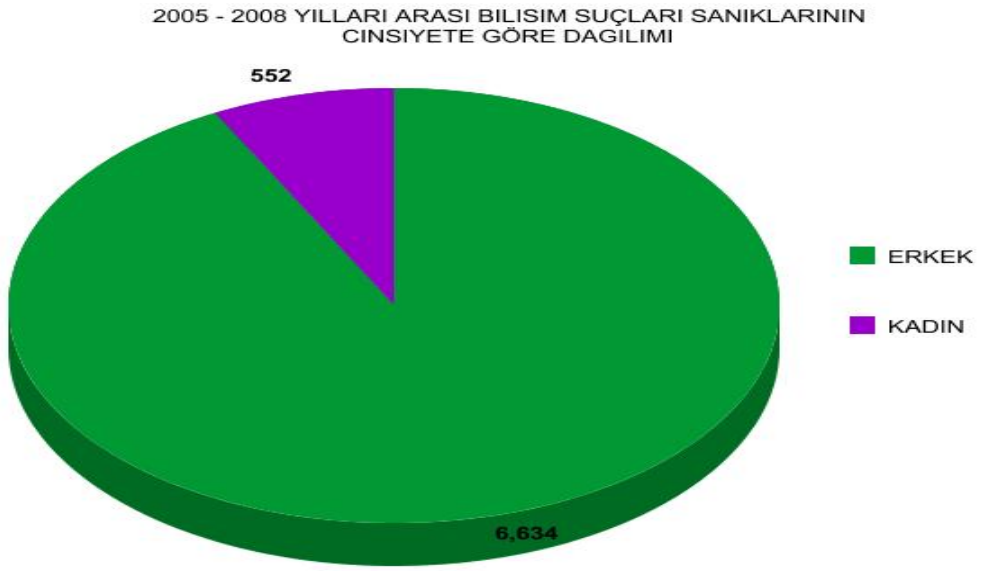
Tablo 1 - 2005 - 2008 Yılları Arası Bilişim Suçları İstatistikleri									
A: Açılan **B**: Karara Bağlanan			**2005**		**2006**		**2007**		**2008**	
			A	***B***	***A***	***B***	***A***	***B***	***A***	***B***
Dava Sayısı			310	223	744	572	958	683	2544	1799
Cinsiyete Göre Dağılım	**Toplam**		635	325	1124	1020	1533	1062	3894	2796
	Erkek		603	298	1042	956	1397	982	3592	2536
	Kadın		32	27	82	64	136	80	302	260
Yaş Grubu	**12 - 14**	**Erkek**	21	0	4	37	3	5	19	18
		Kadın	2	0	0	0	0	0	4	2
	15 - 17	**Erkek**	33	2	35	80	41	53	86	99
		Kadın	1	0	0	2	6	4	18	11
	18 +	**Erkek**	549	296	1003	839	1353	924	3487	2419
		Kadın	29	27	82	62	130	76	280	247



Şekil 9 – 2005 – 2008 Yılları Arası Bilişim Suçları Grafiği

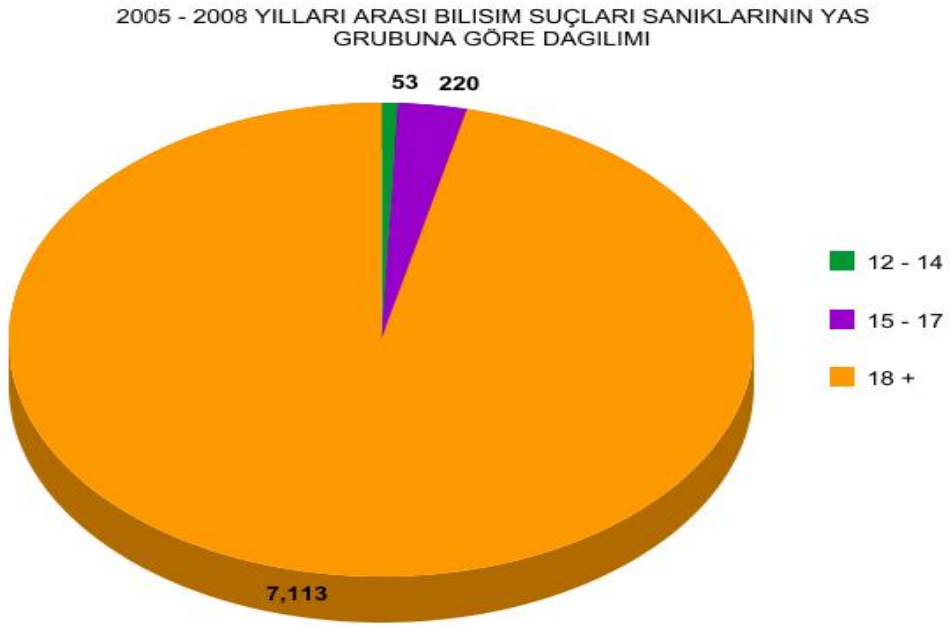
[314] Türkiye İstatistik Kurumu, (2010), "Adalet İstatistikleri", http://www.tuik.gov.tr/VeriBilgi.do?tb_id=1&ust_id=12, (Erişim Tarihi: 16.12.2010).

2005 – 2008 yılları arasında bilişim suçlarındaki ve bu suçu işleyenlerdeki artışı net olarak görmekteyiz. Grafikte dikkat edilmesi gereken diğer bir önemli husus da yükselen artış oranları olmaktadır.



Şekil 10 – 2005 – 2008 Yılları Arası Bilişim Suçları Sanıklarının Cinsiyete Göre Dağılımı

2005 – 2008 yılları arasında işlenen bilişim suçlarının sanıkların cinsiyetlerine baktığımızda büyük oranda erkeklerin olduğunu görüyoruz. Ancak az da olsa kadınların da bu suçun faili olabildiklerini söyleyebiliriz.



Şekil 11 - 2005 – 2008 Yılları Arası Bilişim Suçları Sanıklarının Yaşa Göre Dağılımı

2005 – 2008 yılları arasında işlenen bilişim suçlarının sanıkların yaş grubuna göre dağılımına baktığımızda büyük kısmının on sekiz yaşından büyük kişiler olduğunu görmekteyiz.

765 sayılı Türk Ceza Kanunu'nda bilişim suçları sadece bir maddede (525. madde) düzenlenirken 2006 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile bilişim alanındaki suç türleri üç maddede düzenlenmiştir. 2006 – 2008 yılları arasındaki bilişim alanında işlenen suçların maddelere göre dağılımına bakacak olursak;[315]

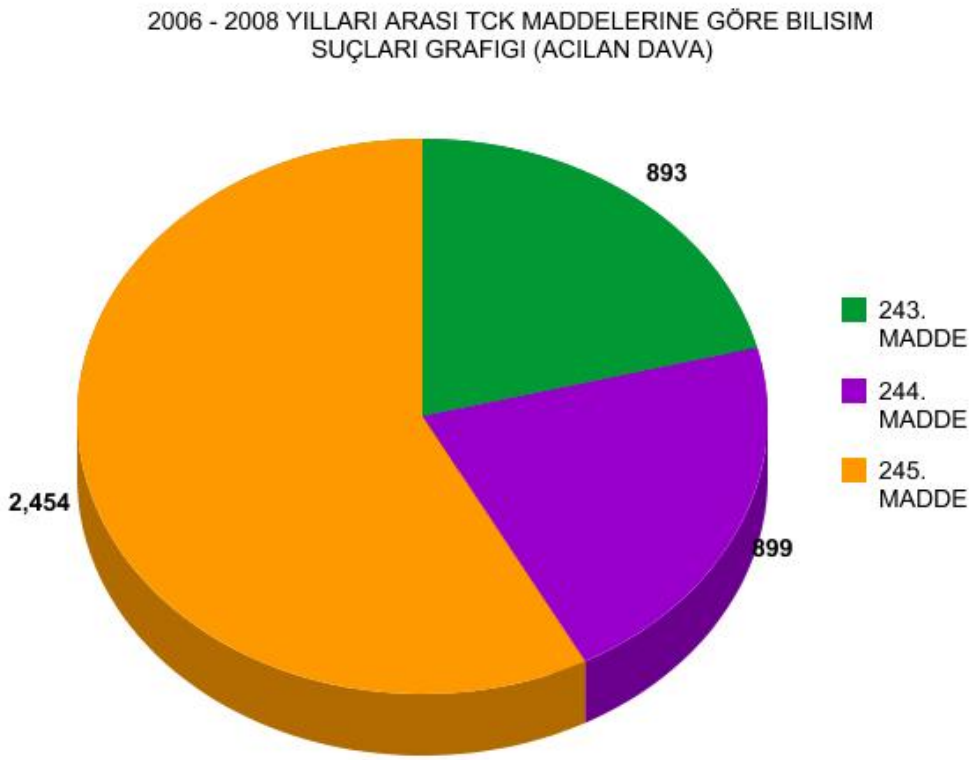
Tablo 2 – 2006 – 2008 Yılları Arası İşlenen Bilişim Suçlarının Maddelere Göre Dağılımı

A: Açılan **B**: Karara Bağlanan				**2006**		**2007**		**2008**	
				A	***B***	***A***	***B***	***A***	***B***
243. Madde	**Dava Sayısı**			137	236	271	170	485	247
	Cinsiyete Göre Dağılım	**Toplam**		189	493	429	255	791	466
		Erkek		183	467	398	237	732	424
		Kadın		6	26	31	18	59	42
	Yaş Grubu	**12 - 14**	**Erkek**	3	36	3	0	4	1
			Kadın	0	0	0	0	0	1
		15 - 17	**Erkek**	11	73	12	6	5	16
			Kadın	0	1	0	1	1	1
		18 +	**Erkek**	169	358	383	231	723	407
			Kadın	6	25	31	17	58	40
244. Madde	**Dava Sayısı**			47	54	104	61	748	380
	Cinsiyete Göre Dağılım	**Toplam**		59	80	145	106	1110	584
		Erkek		57	74	134	98	1023	534
		Kadın		2	6	11	8	87	50
	Yaş Grubu	**12 - 14**	**Erkek**	0	0	0	1	5	9
			Kadın	0	0	0	0	0	0
		15 - 17	**Erkek**	0	1	6	12	28	13
			Kadın	0	0	0	0	2	0
		18 +	**Erkek**	57	73	128	85	990	512
			Kadın	2	6	11	8	85	50
245. Madde	**Dava Sayısı**			560	282	583	452	1311	1087
	Cinsiyete Göre Dağılım	**Toplam**		876	447	959	701	1993	1746
		Erkek		802	415	865	647	1837	1578
		Kadın		74	32	94	54	156	168
	Yaş Grubu	**12 - 14**	**Erkek**	1	1	0	4	10	8
			Kadın	0	0	0	0	4	1
		15 - 17	**Erkek**	24	6	23	35	53	70
			Kadın	0	1	6	3	15	10
		18 +	**Erkek**	777	408	842	608	1774	1500
			Kadın	74	31	88	51	137	157

[315] Türkiye İstatistik Kurumu (2010), "Adalet İstatistikleri", http://www.tuik.gov.tr/VeriBilgi.do?tb_id=1&ust_id=12, (Erişim Tarihi: 16.12.2010).

İstatistiklerde maddelere göre sıralan suçların kanunda geçen isimleri, "Bilişim Sistemine Girme (243. Madde), Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme (244. Madde), Banka Veya Kredi Kartlarının Kötüye Kullanılması (245. Madde)" şeklindedir.

2006 – 2008 yılları arasında işlenen bilişim suçlarının maddelere göre dağılımına bakacak olursak;



Şekil 12 - 2006 – 2008 Yılları Arası İşlenen Bilişim Suçlarının Maddelere Göre Dağılımı

Grafiğe bakıldığında "bilişim sistemine girme" ve "sistemi engelleme, bozma, verileri yok etme veya değiştirme" suçlarının birbirlerine yakın oranda olduğunu ancak "banka veya kredi kartlarının kötüye kullanılması" suçunun bunların iki katı civarında olduğunu görmekteyiz.

Bilişim yoluyla işlenen suçlara yönelik olarak adliyeler tarafından tutulan özel bir istatistik olmadığından bahsetmiştik ancak Emniyet Genel Müdürlüğü tarafından bilişim yoluyla işlenen asayiş suçlarının istatistikleri tutulmaktadır.

Birinci bölümde bilişim yoluyla işlenebilen suçlardan bahsetmiştik. İstatistiklere bunların hepsi yansımamıştır çünkü adliyeler gibi güvenlik birimleri de suçların istatistiklerini tutarken işleniş şekillerine göre tutmamaktadır.

2008 yılı ve 2009 yılının ilk on ayına ait bilişim yoluyla işlenen asayiş suçları istatistiklerine bakacak olursak;[316]

EMNİYET GENEL MÜDÜRLÜĞÜ

2008 YILI VE 2009 YILI OCAK-EKİM AYLARINDA TÜRKİYE GENELİ POLİS SORUMLULUK ALANINDA MEYDANA GELEN BİLİŞİM YOLU İLE İŞLENEN ASAYİŞ SUÇLARININ DAĞILIMI

OLAY TÜRÜ	OLAY SAYISI	
	2008 YILI	2009 YILI OCAK-EKİM
Bilişim Yoluyla Cinsel Taciz (TCK 105)	215	276
Bilişim Yoluyla Tehdit (TCK 106)	1075	1320
Bilişim Yoluyla Şantaj (TCK 107)	36	24
Bilişim Yoluyla Hakaret	275	298
Bilişim Yoluyla Verileri Hukuka Aykırı Olarak Verme veya Ele Geçirme(TCK 136)	23	23
Bilişim Yoluyla Dolandırıcılık (158/f)	381	524
Bilişim Yoluyla Fuhuş	5	0
Bilişim Yoluyla Müsteheenlik (226/1,2,3,4,5)	43	20
Bilişim Yoluyla Kumar Oynanması İçin Yer ve İmkan Sağlama (TCK 228)	143	108

NOT 1: Yukarıda belirtilen olaylara ait istatistiki bilgiler; 2008 yılından itibaren müstakilen derlenmeye başlanmıştır.

2: 2009 yılı Kasım ayı verileri henüz derlenmemiştir.

3: 4982 sayılı Bilgi Edinme Hakkı Kanununun 29. maddesi "Bu kanunla erişilen bilgi ve belgeler ticarî amaçla çoğaltılamaz ve kullanılamaz" hükmünü, Bilgi Edinme Hakkı Kanununun Uygulanmasına İlişkin Esas ve Usuller Hakkındaki Yönetmeliğin 42. Maddesi de, "Kanunda ve bu yönetmelikte belirtilen usul ve esaslar çerçevesinde erişilen bilgi ve belgeler ticari amaçla çoğaltılamaz, kullanılamaz, erişimi sağlayan kurum ve kuruluştan izin alınmaksızın yayınlanamaz. Bu madde hükmüne aykırı olarak erişilen bilgi veya belgeleri ticari amaçla çoğaltanlar, kullananlar veya yayınlayanlar hakkında kanunların cezai ve hukuki sorumluluğa ilişkin hükümleri uygulanır." hükmünü amirdir.

Tablo 3 – 2008 – 2009 Yılı Ocak – Ekim Aylarında Türkiye Geneli Polis Sorumluluk Alanında Meydana Gelen Bilişim Yoluyla İşlenen Asayiş Suçlarının Dağılımı

İstatistiklere bakıldığından ilk olarak göze çarpan durum daha yıl tamamlanmamasına rağmen birçok suçta artış olduğu görülmektedir. Buna bağlı olarak bir sonraki yılda da (2010) benzer oranda artış olduğunu tahmin etmek gerçekçi olacaktır.

[316] Emniyet Genel Müdürlüğü, (2009), "Bilgi Edinme Birimi", http://bilgiedinme.egm.gov.tr/, Bilgi edinme başvurusuna 17.12.2009 tarihinde cevap olarak istatistikler gönderilmiştir. Aralık 2010 itibariyle istatistik sisteminde yapılan yeni çalışmalar nedeniyle olumsuz cevap verilmektedir.

Burada bir suçun bilişim yoluyla işlenme oranına bakacak olursak, örneğin "Cinsel taciz" suçunda adliye istatistiklerine göre 2008 yılında 8358 tane dava açılmıştır.[317] Emniyet Genel Müdürlüğü istatistikleriyle karşılaştırıldığında cinsel taciz suçlarının yaklaşık % 3'ü bilişim yoluyla işlendiği gözükmektedir. Tabi bu istatistiklere Jandarma sorumluluk bölgesinde işlenen suçlar katılmadığından bu oranın en azından % 4 – 5 civarında olması gerektiği tahmin edilebilir. Bu oranın teknolojiye paralel olarak zaman içinde artması da kuvvetle muhtemeldir.

3.4.2. Dünya Geneli İstatistikler Açısından

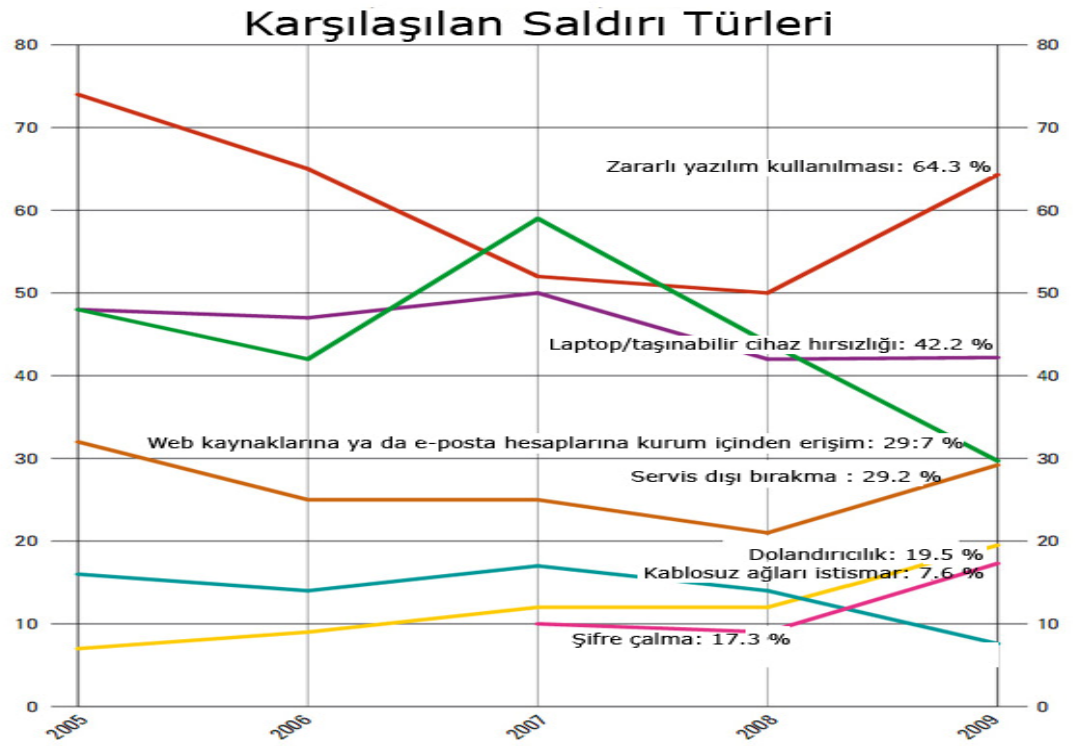
Suç dünyasında bilişim teknolojilerinin kullanımına dair dünya çapında yapılan istatistiklerde veya diğer bazı ülkelerde yapılan istatistiklerde standart bir format bulunmamaktadır. Bazı ülkeler kendi yasal düzenlemelerine göre veya adli sistemlerine göre istatistikler tutarken, bazı ülkelerde de bilişim suçu işlenirken kullanılan yöntemlere göre istatistikler tutulmaktadır.

Bilgi Güvenliği Enstitüsü (Computer Security Institute - CSI)[318] bilişim bağlantılı suçlarla ilgili veya kullanılan metotlarla ilgili dünya geneli istatistiklerin derlenip düzenlendiği ve sunulduğu en geniş çaplı organizasyondur. Organizasyon bilgi güvenliği sektöründe hizmet veren firmaların ortaklaşa bilgi paylaşımı ile çalışmaktadır ve yılda bir defa konferans düzenlemektedir. Yaklaşık otuz yıldır bilgi güvenliği sektöründe hizmet vermekte ve her yıl düzenledikleri konferansta yıllık bilgi güvenliği raporu yayınlanmaktadır.

Bilgi Güvenliği Enstitüsü (Computer Security Institute – CSI) tarafından yapılan 2009 yılı araştırmalarına[319] göre bilişim teknolojilerinin suç işlenmesinde kullanılmasına yönelik son beş yılda en çok kullanılan metotlar aşağıdaki grafikte görüldüğü üzere yedi sınıfta kategorize edilmiş ve ölçülmüştür. Bunlar: zararlı yazılım kullanılması (malware infection:), laptop/taşınabilir cihaz hırsızlığı (laptop/ mobile device theft), internet kaynaklarına ya da e-posta hesaplarına kurum içinden erişim (insider abuse of net access or e-mail), servis dışı bırakma (denial of service),

[317] Türkiye İstatistik Kurumu (2010), "Adalet İstatistikleri", http://www.tuik.gov.tr/VeriBilgi.do?tb_id=1&ust_id=12, (Erişim Tarihi: 16.12.2010).
[318] Computer Security Institute, (t.y.), "Computer Security Institute – CSI", http://www.gocsi.com/about, (Erişim Tarihi:18.12.2010).
[319] Computer Security Institute, (2009), "14th Annual CSI Computer Crime and Security Survey Executive Summary", http://gocsi.com/survey_2009, (Erişim Tarihi: 18.12.2010).

dolandırıcılık (financial fraud), şifre çalma (password sniffing), kablosuz ağları istismar (exploit of wireless network).



Şekil 13 - Bilişim Teknolojilerinin Suç İşlenmesinde Kullanılmasına Yönelik Son Beş Yılda En Çok Kullanılan Metotlar

En çok kullanılan yedi metodun dışındaki ölçülen diğer on beş metot da şunlardır; kurum içi köle bilgisayarlar (Bots / zombies within the organization), yemleme (Being fraudulently represented as sender of phishing messages), çalınan veri ile veya saldırı tehdidi ile şantaj (Extortion or blackmail associated with threat of attack or release of stolen data), internet sitesi hackleme (Web site defacement), halka açık internet sitelerinin istismar edilmesi (Other exploit of public-facing Web site), DNS sunucuları istismar (Exploit of DNS server), internet gezginlerini istismar etmek, (Exploit of client Web browser), sosyal ağları (facebook, myspace vb.) istismar (Exploit of user's social network profile), anında mesajlaşmayı istismar (Instant messaging abuse), kurum içi saldırılar (Unauthorized access or privilege escalation by insider), kurum dışından sistem zafiyetlerini tarama (System penetration by outsider), mobil cihazların çalınması kişisel verilerin çalınması ya da illegal erişim (Theft of or unauthorized access to PII or PHI due to mobile device theft/loss), mobil cihazların çaldırılması sonucu fikri mülkiyet haklarını ihlal (Theft

of or unauthorized access to intellectual property due to mobile device theft/loss), diğer nedenlerle kişisel verilerin çalınması ya da illegal erişim (Theft of or unauthorized access to PII or PHI due to all other causes), diğer nedenlerle fikri mülkiyet haklarının ihlali (Theft of or unauthorized access to intellectual property due to all other causes). Aşağıdaki istatistikte yukarıda bahsedilen yirmi iki metodun son beş yıldaki yüzde oranları verilmiştir.[320]

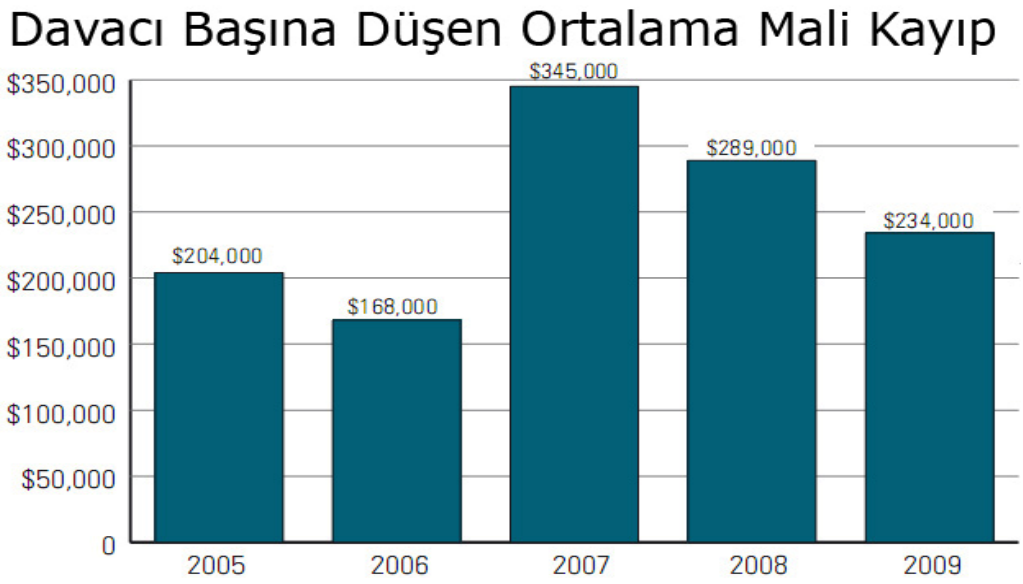
Karşılaşılan Saldırı Türleri

Atak Tipleri	2005	2006	2007	2008	2009
Zararlı yazılım kullanılması	74%	65%	52%	50%	64%
Kurum içi köle (zombi) bilgisayarlar			21%	20%	23%
Yemleme			26%	31%	34%
Şifre Çalma			10%	9%	17%
Dolandırıcılık	7%	9%	12%	12%	20%
Servis dışı bırakma	32%	25%	25%	21%	29%
Çalınan veri ile veya saldırı tehdidi ile şantaj					3%
Web sitesi hackleme	5%	6%	10%	6%	14%
Halka açık web sitelerinin istismar edilmesi					6%
Kablosuz ağların istismar edilmesi	16%	14%	17%	14%	8%
DNS sunucuları istismar			6%	8%	7%
Web gezginlerini istismar					11%
Sosyal ağları (facebook, myspace...) istismar					7%
Anında mesajlaşmayı istismar			25%	21%	8%
Web kaynaklarına ya da e-posta hesaplarına kurum içinden erişim	48%	42%	59%	44%	30%
Kurum içi saldırılar					15%
Kurum dışından sistem zafiyetlerini tarama					14%
Laptop/taşınabilir cihaz hırsızlığı	48%	47%	50%	42%	42%
Mobil cihazların çalınması kişisel verilerin çalınması ya da illegal erişim				8%	6%
Mobil cihazların çaldırılması sonucu fikri mülkiyet haklarını ihlal				4%	6%
Diğer nedenlerle kişisel verilerin çalınması ya da illegal erişim				8%	10%
Diğer nedenlerle fikri mülkiyet haklarının ihlali				5%	8%
2009 CSI Computer Crime and Security Survey				2009: 185 Respondents	

Şekil 14 - Bilişim Teknolojilerinin Suç İşlenmesinde Kullanılmasında Kullanılan Metotlar

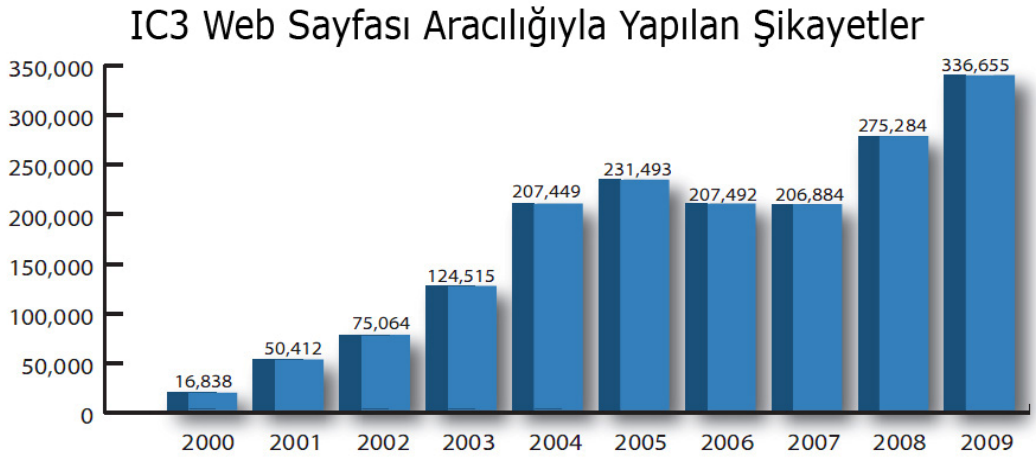
[320] Computer Security Institute, (2009), "14th Annual CSI Computer Crime and Security Survey Executive Summary", http://gocsi.com/survey_2009, (Erişim Tarihi: 18.12.2010).

Bilgi Güvenliği Enstitüsü (Computer Security Institute – CSI) tarafından siber suçların mağduru olan kişilerin kişi başı ortalama mali kayıpları da istatistikî olarak hesaplanmıştır.[321] Bunlara bakacak olursak;



Şekil 15 - Siber Suçların Mağduru Olan Kişilerin Kişi Başı Ortalama Mali Kayıpları

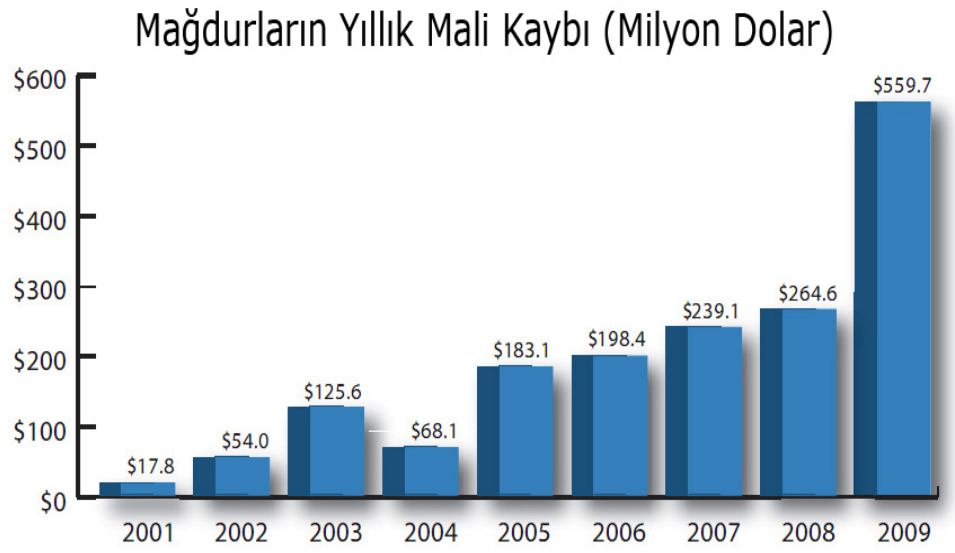
Amerika Birleşik Devletleri Adalet Bakanlığı'na bağlı İnternet Suçları Şikâyet Birimi (IC3) tarafından yıllık istatistikler tutulmaktadır.[322] 2000 – 2009 yılları arasında yapılan şikâyetlerin sayısına bakacak olursak;



Şekil 16 - Amerika Birleşik Devletleri Adalet Bakanlığı'na Bağlı İnternet Suçları Şikâyet Birimi'ne 2000 – 2009 Yılları Arasında Yapılan Şikâyetler

[321] Computer Security Institute, (2009), "14th Annual CSI Computer Crime and Security Survey Executive Summary", http://gocsi.com/survey_2009, (Erişim Tarihi: 18.12.2010).
[322] İnternet Crime Complaint Center – USA Department of Justice, (2010), "2009 Internet Crime Report", http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf, (Erişim Tarihi:18.12.2010).

2001 – 2009 yılları arasında sanal suçların ortaya çıkardığı mali kayba (milyon dolar) bakacak olursak;

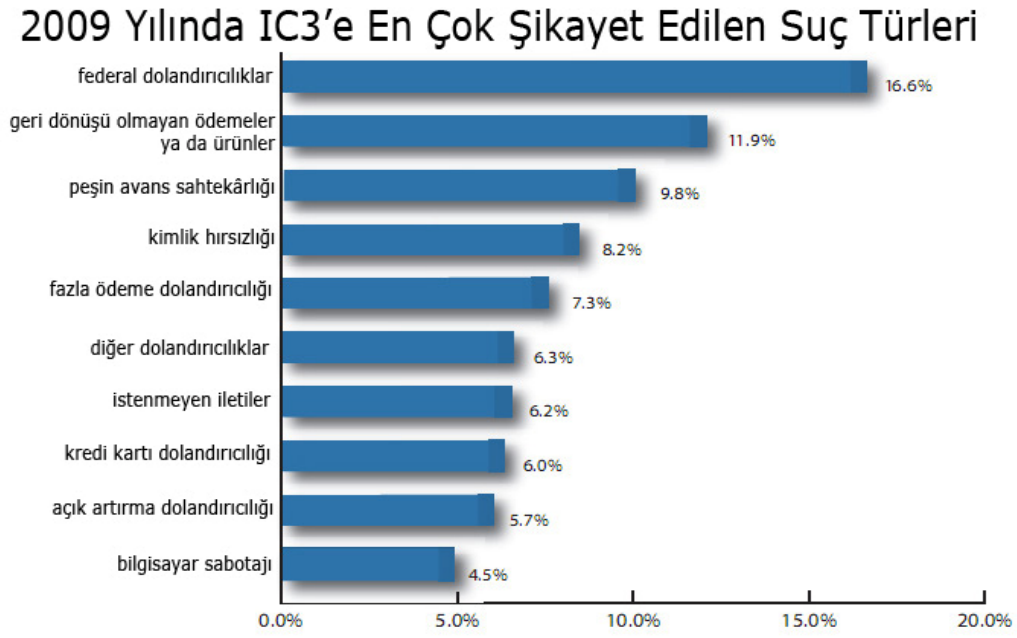


Şekil 17 - Amerika Birleşik Devletleri 2001 – 2009 Yılları Arasında Sanal Suçların Ortaya Çıkardığı Mali Kayıp

Amerika Birleşik Devletleri Adalet Bakanlığı'na bağlı İnternet Suçları Şikâyet Birimi tarafından tutulan sanal suçların istatistiklerinde on adet suç türü değerlendirilmiştir.[323] Bu suç türleri; federal dolandırıcılıklar (fbi scams), geri dönüşü olmayan ödemeler ya da ürünler (non-delivery merchandise/payment), peşin avans sahtekârlığı (advanced fee fraud)[324], kimlik hırsızlığı (identity theft), fazla ödeme dolandırıcılığı (overpayment fraud)*, diğer dolandırıcılıklar (miscellaneous frauds), istenmeyen iletiler (spam), kredi kartı dolandırıcılığı (credit card fraud), açık artırma dolandırıcılığı (auction fraud), bilgisayar sabotajı (computer damage),

[323] İnternet Crime Complaint Center – USA Department of Justice, (2010), "2009 İnternet Crime Report", http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf, (Erişim Tarihi:18.12.2010).
[324] Bu tür dolandırıcılığın dünya suç literatüründeki tanımı "Advance Fee Fraud". Yani "Peşin Avans Sahtekârlığı". Bu yöntemde, oldukça zeki ve donanımlı dolandırıcılık çeteleri, ağlarına düşürdükleri kurbanları milyarlar vaadiyle sömürüyor. Sömürmenin şekli kimi zaman avukatlık parası, kimi zaman vekalet parası, evrak parası oluyor... Bu dolandırıcılıkta başı Nijerya Çeteleri çekiyor. Zaten Amerikan Federal Soruşturma Bürosu'nun (FBI) da dolandırıcılık bölümünde bu çeteler "419 Fraud" başlığıyla yer alıyor. 419 kodu, Nijerya yasalarındaki bu tür suçlara yönelik hükmü düzenleyen ilgili madde. http://www.patronlardunyasi.com/haber/En-zengin-Turk-FBI-listesinde/86795, (Erişim Tarihi: 18.12.2010).
* Fazla Ödeme Dolandırıcılığı yönteminde dolandırıcı kurbana yanlışlıkla yüksek miktarda ödeme yapmaktadır ve ödemesi gerekenden fazla olan miktarı da nakit olarak geri istemektedir. Ödeme karşılıksız çıkmaktadır ancak dolandırıcı nakit parayla ortadan kaybolmaktadır. http://www.youtube.com/watch?v=cRTU72kAkLA, (Erişim Tarihi: 18.12.2010).

Bu suçlardan en çok işlenenlere ve toplam suçların yüzde kaçını oluşturduğuna bakacak olursak;



Şekil 18 - Amerika Birleşik Devletleri Adalet Bakanlığı'na Bağlı İnternet Suçları Şikâyet Birimi'ne 2009 Yılında En Çok Şikayet Edilen Suç Türleri

Yukarıdaki suç türlerine bakıldığında birçoğunun mali boyutu olan dolandırıcılık suçları olduğunu görüyoruz. Aslında bu suçlara genel olarak "bilişim yoluyla dolandırıcılık" demek mümkündür.

İngiltere'nin 2006 – 2008 yılları arasında işlenen sanal suçlar istatistiklerine bakacak olursak[325] 2008 yılında toplam 3,5 milyona yakın bilişim bağlantılı işlenen suç rapor edilmiştir. Ayrıca diğer rakamlar;

Tablo 4 – İngiltere 2006 – 2008 Yılları Sanal Suçlar İstatistikleri

Kategori	**2008**	**2007**	**2006**	**07/08 Oran**
Kimlik Hırsızlığı ve Dolandırıcılığı	86900	84700	92000	+ %2.6
Mali Dolandırıcılık	207700	203700	207000	+ %1.9
Bilişim Yoluyla Taciz	2374000	2240000	1944000	+ %6.0
Bilgisayar Suçları (Virüsler Hariç)	137600	132800	144500	+ %3.6
Bilişim Yoluyla Cinsel Suçlar	609700	617500	850000	- %1.3
Toplam	**3415900**	3278700	3237500	+ %4.2

[325] Garlik, (2010), "The Garlik UK Cybercrime Report", https://www.garlik.com/cybercrime_report.php, (Erişim Tarihi: 29.12.2010).

3.5. UYGULAMADAN ÖRNEKLER

3.5.1. Bilişim Suçları ve Bilişim Yoluyla İşlenen Suçlar

Bilişim suçları ve bilişim yoluyla işlenen suçların kovuşturma evresinde de farklı yaklaşımlar görülmektedir. Uygulamada karşılaşılan aksaklıkları ve düzeltmeleri görebilmek için güncel Yargıtay kararlarını incelemek yerinde olacaktır.

3.5.1.1. Örnek 1: Yargıtay 11. Ceza Dairesi, Esas No: 2008/18190, Karar No: 2009/30-58, Tarih: 26.03.2009[326]

> *...*
>
> *Sanığın hırsızlık ve banka kartını kötüye kullanma suçlarından cezalandırılmasına karar verilen somut olayda, Yargıtay Ceza Genel Kurulu'nca çözümlenmesi gereken uyuşmazlıklar;*
>
> *1- Bankamatikten para çekmek için gelen kişilerin banka kartlarını, kurulan bir düzenekle ele geçirerek bu kişilerin hesaplarından para çekme şeklinde gerçekleşen bir eylemde; banka veya kredi kartlarının kötüye kullanılması suçunun yanında hırsızlık suçunun da oluşup oluşamayacağının belirlenmesi,*
>
> *2- Banka kartlarının kötüye kullanılması suçunun yanında hırsızlık suçunun da oluştuğuna karar verilmesi halinde ise, sanık hakkında TCY'nin 145.*[327] *maddesinin uygulanma koşullarının bulunup bulunmadığı ile ilgili araştırma yapılmasının gerekip gerekmediği, noktalarında toplanmaktadır.*
>
> *Sanık Cumayi'nin, bankamatiklere gelenlerin banka kartını ele geçirebilmek için bir düzenek kurduğu, düzenek nedeniyle işlem yapamayan ve kartları ATM (asynchronous transfer mode) cihazına takılan mağdurların yanına giderek şifrelerini yeniden girmelerini istemek suretiyle şifrelerini öğrendiği, banka kartı bankamatik cihazına sıkışan mağdurların uzaklaşması üzerine kartı tornavida ile çıkarttığı, ele geçirdiği banka kartı ile başka bir*

---

[326] Yargıtay, (2010), "Ceza Genel Kurulu 2010/11-17 E., 2010/65 K.", http://emsal.yargitay.gov.tr/VeriBankasiIstemciWeb/DokGosterMainServlet?dokumanId=95%203%20ICM8%20ICMNLSDB15%20UYAPVERIBANKASI59%2026%20A1001001A10L20B51211C8408218%20A10L20B51211C840821%2014%201162&aranan=&dokumanTuru=YARGITAYKARARI, (Erişim Tarihi: 02.01.2011).

[327] Madde 145- (1) (Değişik: 29/6/2005 – 5377/16 md.) Hırsızlık suçunun konusunu oluşturan malın değerinin azlığı nedeniyle, verilecek cezada indirim yapılabileceği gibi, suçun işleniş şekli ve özellikleri de göz önünde bulundurularak, ceza vermekten de vazgeçilebilir.

bankamatik cihazından mağdurların hesabından para çektiği, bu bağlamda; 07.10.2008 tarihinde E... 1. Etap Ö... İş Merkezi yanında bulunan ATM'de mağdur Bektaş'ın banka kartını bu şekilde ele geçirerek başka bir ATM cihazından 100 Lira çektiği, yine 01.11.2008 tarihinde E... 2. Etap K... İş Merkezi önünde bulunan ATM'den mağdur Ahmet'in kartını aynı yöntemle ele geçirdiği, kendisinden şüphelenip takip eden mağdurun sanığın başka bir ATM'den para çektiğini görünce polise haber verdiği, sanığın bir süre sonra üzerinde mağdura ait hesaptan çektiği 600 Lira ile yakalandığı, yapılan yargılama sonucunda yerel mahkemece sanığın mağdur Bektaş'a yönelik hırsızlık suçundan 5237 sayılı TCY'nin 141/1, 53 ve 63. maddeleri uyarınca 1 yıl hapis, banka kartının kötüye kullanılması suçundan 5237 sayılı TCY'nin 245/1, 168/2, 52, 53 ve 63. maddeleri uyarınca 2 yıl hapis ve 12.000 Lira adli para cezası, mağdur Ahmet'e yönelik hırsızlık suçundan ise, 5237 sayılı TCY'nin 141/1, 53 ve 63. maddeleri uyarınca 1 yıl hapis, banka kartının kötüye kullanılması suçundan ise, 5237 sayılı TCY'nin 245/1, 168/1, 52, 53 ve 63. maddeleri uyarınca 1 yıl 4 ay hapis ve 8.000 Lira adli para cezası ile cezalandırılmasına karar verildiği, sanık müdafilerinin temyizi üzerine dosyayı inceleyen Özel Daire'ce hükmün onanmasına karar verildiği, Yargıtay C.Baş-savcılığı'nın ise "sanığın her bir müştekiye yönelik eylemden dolayı banka veya kredi kartının kötüye kullanılması suçunun yanında hırsızlık suçunun oluşmayacağı, oluştuğunun kabulü halinde ise bu suç yönünden 5237 sayılı TCY'nin 145. maddesinin uygulanması gerektiği" görüşüyle itiraz yasa yoluna başvurduğu anlaşılmaktadır.

...

Bu açıklamalar ışığında birinci uyuşmazlık konusu değerlendirildiğinde;

5237 sayılı TCY'nin 245/1. maddesindeki banka veya kredi kartlarını kötüye kullanma suçu bileşik suç olarak düzenlenmemiş olup, yasa maddesinde geçen "her ne surette olursa olsun" ifadesi banka veya kredi kartlarının sadece hukuka uygun yollardan ele geçirilmesini kapsamaktadır. Bunun sonucu olarak; sanığın kurduğu düzenek ile ATM makinesine para çekmek için gelen mağdurların şifresini de öğrenmek suretiyle ele geçirdiği, ekonomik değeri bulunduğunda kuşku bulunmayan menkul mal niteliğindeki

banka kartı ile başka bir ATM cihazına gidip para çekmesi şeklinde gerçekleştirdiği eylemlerinde, ***banka veya kredi kartının kötüye kullanılması suçu yanında hırsızlık suçu da oluşmaktadır****.*

...

Bu açıklamalar ışığında ikinci uyuşmazlık konusuna ilişkin olarak somut olay değerlendirildiğinde;

Sanığın ATM makinesine para çekmek veya işlem yapmak için gelen kişilerin banka kartını ele geçirebilmek için bir düzenek kurduğu, bankamatiğe taktığı bu düzenek nedeniyle işlem yapamayan ve kartları bankamatiğe sıkışan kişilerin yanına yardım etme görünümü altında yaklaştığı, şifrelerini öğrenebilmek amacıyla şifrelerini yeniden girmelerini istediği, böylece şifrelerini öğrendiği, sanığın kurduğu düzenek nedeniyle banka kartı ATM cihazına sıkışan mağdurların telefon etmek için uzaklaşması üzerine banka kartını tornavida ile çıkarttığı, ele geçirdiği banka kartı ile başka bir bankamatikten mağdurların hesabından para çektiği anlaşılmakta olup, bu şekilde gelişen olayda, ***suçun işleniş şekli itibariyle 5237 sayılı TCY'nin 145. maddesinin uygulanma koşullarının bulunmadığı sonucuna ulaşılmaktadır****.*

Emsal kararda hem bir bilişim suçunun hem de geleneksel suçun birlikte işlendiğini görmekteyiz. Bir banka kartının ATM cihazından para çekmek amacıyla çalınması durumunda hırsızlık suçu oluşmaktadır. Asıl amaç banka kartı ile çekilebilecek parayı çalmak dahi olsa, sadece banka kartının çalınması hırsızlık suçunu oluşturmaktadır. Ani banka kartının çalınması, "banka veya kredi kartının kötüye kullanılması" suçunun geçiş suçu olarak kabul edilmeyip ayrı bir suç olarak kabul edilmiştir.

Öte yandan haksız olarak ele geçirilen banka kartı ile ATM cihazından para çekme eyleminde banka veya kredi kartlarının kötüye kullanılması ile haksız yarar elde edilmesi, bilişim alanında suçlar altında düzenlenmiş bir suç türüdür. Ancak burada haksız yarar sağlanırken çekilen para suçun asıl hedefi olmakla beraber bu paranın çekilmeden önce bankaya ait olması ve banka kartlarının haksız olarak ele geçirilmesi için ATM cihazına düzenek yerleştirilmesi eylemlerinde bankanın da mağdur olup olmadığı başka bir tartışma konusunu oluşturmaktadır. Hem bu örnekte

hem de bir sonraki başlıkta bahsedilecek ikinci örnekteki gibi somut olaylarda bankalar her zaman kendilerini konunun dışında kabul etmektedirler. Suçlu karşısında hakkını arayan mağdura destek olmamaktadırlar.

Ülkemizde özellikle sanal banka mağdurlarının sayısı gün geçtikçe artmaktadır. Bu mağdurların genel şikâyet konusu haklarını aramada bankaların duyarsız olmasıdır ve bu amaçla bir dernek çatısı altında toplanmışlardır.[328]

3.5.1.2. Örnek 2: Yargıtay Ceza Genel Kurulu, Esas No: 2009/11-193, Karar No: 2009/268, Tarih: 17.11.2009[329]

…

Sanık Volkan ile firari Saim'in birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın İnternet bankacılık şifresini kullanmak suretiyle, katılanın Ş... bank Ankara K. Şubesindeki hesabından 10.750 YTL'yi İnternet kanalı ile Ş ... bank-İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale ettikleri ve aynı gün banka şubesinden çektikleri olayda,

Sanığın eyleminin, 765 sayılı TCY'nin ikinci kitap, onbirinci babta düzenlenen bilişim alanında suçlar bölümünün 525/b-2 maddesinde düzenlenen suçu oluşturduğu yönünde herhangi bir uyuşmazlık bulunmamaktadır.

Yargıtay Ceza Genel Kurulu'nca çözümü gereken uyuşmazlık, sanığın 765 sayılı TCY'nin 525/b-2. maddesine uyan eyleminin, suç tarihinden sonra yürürlüğe giren 5237 sayılı TCY'nin 244/4. maddesine mi, yoksa 142/2-e maddesine mi, uyan suçu oluşturduğuna ilişkindir

5237 sayılı TCY'nin kişilere karşı suçların düzenlendiği, ikinci kitap, ikinci kısım, onuncu bölümünde yer alan malvarlığına karşı suçlar bölümünde bulunan hırsızlık suçunun temel şekli 5237 sayılı TCY'nin 141. maddesinde; zilyedinin rızası olmadan başkasına ait taşınır bir malı, kendisine veya

[328] Sanal Banka Mağdurları Derneği, (t.y.), "Sanal Banka Mağdurları Derneği", http://www.sanalbankamagdurlari.com, (02.01.2011).
[329] Kazancı Hukuk Programları, (2010), "Ceza Genel Kurulu 2009/11-193 E., 2009/268 K", http://www.kazanci.com/cgi-bin/highlt/ibb/highlight.cgi?file=ibb/files/cgk-2009-11-193.htm, (Erişim Tarihi: 02.01.2011).

başkasına bir yarar sağlamak maksadıyla bulunduğu yerden almak şeklinde düzenlenmiş, aynı Yasa'nın 142. maddesinin 2. fıkrasının (e)bendinde de; suçun, bilişim sistemlerinin kullanılması suretiyle işlenmesi nitelikli hal olarak yaptırıma bağlanmıştır.

...

Uyuşmazlık konusu, Yargıtay Ceza Daireleri arasında farklı yorumlanmış olup; Yargıtay Onbirinci Ceza Dairesi'nin 22.01.2008 gün ve 8423-117, 28.02.2008 gün ve 22-1141, 28.02.2008 gün ve 23-1160, 26.09.2007 gün ve 5875-7637 sayılı kararlarında, eylemin 5237 sayılı TCY'nin 244/4. maddesinde düzenlenen suçu oluşturduğu kabul edilmiş iken,

Yargıtay Altıncı Ceza Dairesi'nin 02.06.2008 gün ve 555-12249 sayılı kararında ise benzer eylemin, 5237 sayılı TCY'nin 142/2-e maddesinde düzenlenen nitelikli hırsızlık suçunu meydana getirdiği kabul edilmiştir.

...

Bu bilgiler ışığında somut olay değerlendirildiğinde;

Sanık Volkan'ın; firari Saim ile birlikte hareket ederek, daha önceden haksız bir şekilde ele geçirdikleri katılan firmanın İnternet bankacılık şifresini kullanmak suretiyle, katılanın Ş bank Ankara K. .. Şubesindeki hesabından 10.750 YTL'yi Ş ... bank-İstanbul Z Şubesinde sanık Volkan adına açtırdıkları hesaba havale edip, aynı gün banka şubesinden çekmek şeklinde gerçekleştirdiği eylemdeki kastı, katılan firmanın banka hesabında bulunan, taşınır nitelikteki parayı bilişim sistemini kullanmak suretiyle kendi banka hesaplarına geçirmeye, katılanın rızasına aykırı olarak malvarlığında azalmaya neden olmaya; başka bir anlatımla var olan veriyi başka bir yere göndermekten ziyade, bu verinin temsil ettiği parayı alarak mal edinmeye yöneliktir. Kaldı ki sanığın katılanın İnternet bankacılık hesabında bulunan parasına ulaşmak için bilişim sistemlerini araç olarak kullanmaktan başka alternatifi de yoktur. Dolayısıyla olayımızda, 5237 sayılı TCy'nin 142/2-e maddesinde düzenlenmiş bulunan "bilişim sistemi kullanılmak suretiyle hırsızlık" suçunun gerçekleştiği kabul edilmelidir. ***Şu halde, sanığın eyleminin 5237 sayılı TCY'nin 142/2-e maddesindeki nitelikli hırsızlık***

suçunu oluşturduğunun kabul edilmesi karşısında; 244. maddenin 4. fıkrası uyarınca uygulama yapma olanağı da bulunmamaktadır.

Öte yandan 5252 sayılı Yasa'nın 9/3. maddesi uyarınca sanık yararına olan hükmün, önceki ve sonraki yasaların ilgili bütün hükümlerinin somut olaya uygulanarak ortaya çıkan sonuçların birbirleriyle karşılaştırılması suretiyle bulunacağının gözetilmemesi, ***765 sayılı Yasa ile yapılan uygulama açıkça sanık yararına olduğundan, sonuca etkili görülmemiştir.***

...

Bilişim suçları, 765 sayılı TCK'da 525/a, 525/b, 525/c ve 525/d maddeleri olmak üzere toplam 4 maddeden oluşmakta, 525 a/b ve c maddelerinde beş değişik suç söz konusu olduğu halde, 525/d maddesinde yeni bir suç düzenlenmeyip fer'i ceza öngörülmekte idi.

01 Haziran 2005 tarihinde ise, 5237 saydı TCK'ya onuncu bölümde bilişim alanında suçlan kapsayacak temel hükümler getirilmiştir. "Bilişim sistemlerine izinsiz girilmesi (m. 243)", "bilişim sistemlerindeki verilere müdahalelerde bulunulması (m. 244)", "bilişim sistemleri aracılığıyla haksız yarar sağlanması (m. 244/)", "banka veya kredi kartlarının kötüye kullanılması (m. 245)" gibi suçlar, bilişim suçları olarak düzenlenmiştir.

Bu suçlar dışında, bilişim teknolojilerinin getirdiği olanaklar dolayısıyla ortaya çıkan ve bilişim teknolojileri de aracı kılınarak işlenebilen "haberleşmenin gizliliğini ihlal (m. 132)", "haberleşmenin engellenmesi (m. 124)", "eğitim ve öğretimin engellenmesi (m. 112)", ve "kamu kurumu veya kamu kurumu niteliğindeki meslek kuruluşlarının faaliyetlerinin engellenmesi, (m. 113)" gibi bilişim suçlan da yer almaktadır.

Yine 5237 sayılı TCK'da çeşitli bölümlerde bilişim sistemleriyle işlenmesi olanaklı suç tiplerine de yer verilmiştir. Yasa'nın 135. maddesinde" kişisel verilerin kaydedilmesi', 136. maddesinde "kişisel verileri hukuka aykırı olarak verme veya ele geçirme', 138. maddesinde" verileri, yok etmeme" 142. maddesinin 2. fıkrasının b bendinde nitelikli hırsızlık suçu ile 158. maddenin

1. fıkranın f bendindeki nitelikli dolandırıcılık suçu bağımsız suç tipleri şeklinde düzenlenmişlerdir.

*5237 sayılı TCK'nın **bilişim alanında suçlara ilişkin hükümlerini eleştirmemek mümkün değildir**. Kanun, bu alandaki suçların düzenlenmesi bakımdan madde hükümlerinin kaleme alınışından suç siyasetine, suçların düzenlenme şeklinden, uygulanamayacak hükümler içermesine, madde metni ile madde gerekçelerinin birbirinden farklı olmasına, bilişim alanında özel bir bölüm bulunmasına rağmen sistemin dışına çıkılarak genel hükümler içinde de düzenlemelere yer verilmeye çalışılmasına, miktarları itibariyle anlamsız cezalar içermesinden (m. 243/1-2)sonuçları ile orantılı olmayan ağır cezalar barındırmasına kadar çeşitli çarpıklıkları da bünyesinde taşımaktadır.*

Emsal kararı özetleyecek olursak haksız bir şekilde elde edilen internet bankacılığı şifreleri ile "sistemi engelleme, bozma, verileri yok etme veya değiştirme" eylemi sonucunda "bilişim yoluyla hırsızlık" suçu meydana geldiği için bu suçtan yargılanma yapılmaktadır. Bir önceki örnekte bir bilişim suçunun işlenmesi için geleneksel bir suçun (hırsızlık) geçiş suçu olarak işlendiğini (bu suçtan da yargılama yapılmıştır) görmüştük. Bu örnekte ise geleneksel bir suçun (hırsızlık) bilişim teknolojisiyle işlenen güncel bir versiyonunu (bilişim yoluyla hırsızlık) işlenebilmesi için bir bilişim suçunun (bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu) geçiş suçu olarak işlendiğini görmekteyiz.

Ancak suçun işlendiği zamanda geçerli olan 765 sayılı eski TCK'nda bilişim yoluyla hırsızlık suçu düzenlenmediğinden ve bu durum sanığın aleyhine olduğundan eylem "bilişim alanında suçlar" kapsamında değerlendirilmiştir. Benzer olaylar 5237 sayılı TCK yürürlüğe girdiği tarihten itibaren işlenmiş olsaydı "bilişim yoluyla hırsızlık suçundan" yargılama yapılacaktı.

Bilişim suçlarıyla ilgili Yargıtay içtihatlarına bakacak olursak[330];

[330] Kazancı Hukuk Programları, (2010), "Kazancı - Mevzuat ve İçtihat Bilgi Bankası Programı", http://www.kazanci.com, (Erişim Tarihi: 02.01.2011).

Tablo 5 – Bilişim Alanında Suçlarla İlgili Yargıtay Kararları Listesi			
Madde	**İlgili Yargıtay Dairesi**	**Karar Tarihi**	**Emsal ve Karar Numarası**
243	Y11.CD	26.3.2009	E. 2008/18190 K. 2009/3058
244	Y6.CD	10.11.2005	E. 2003/18552 K. 2005/9931
244	Y11.CD	20.9.2006	E. 2006/2696 K. 2006/7334
244	Y11.CD	16.4.2007	E. 2005/6376 K. 2007/2551
244	YCGK	19.6.2007	E. 2007/6-136 K. 2007/150
244	Y11.CD	18.9.2007	E. 2007/6963 K. 2007/5533
244	Y11.CD	27.9.2007	E. 2007/6709 K. 2007/6012
244	Y9.CD	27.9.2007	E. 2007/6709 K. 2007/6012
244	YCGK	9.10.2007	E. 2007/11-44 K. 2007/200
244	Y11.CD	22.1.2008	E. 2007/8423 K. 2008/117
244	Y11.CD	9.6.2008	E. 2008/5591 K. 2008/5863
244	Y11.CD	1.7.2008	E. 2006/1800 K. 2008/7126
244	Y11.CD	1.7.2008	E. 2006/2734 K. 2008/7125
244	Y11.CD	27.1.2009	E. 2008/15441 K. 2009/80
244	Y11.CD	28.5.2009	E. 2009/3019 K. 2009/6644
244	Y11.CD	7.10.2009	E. 2009/1616 K. 2009/11328
244	Y11.CD	12.10.2009	E. 2008/11060 K. 2009/11936
244	YCGK	17.11.2009	E. 2009/11-193 K. 2009/268
244	Y11.CD	24.11.2009	E. 2007/849 K. 2009/14539
245	Y11.CD	26.4.2006	E. 2006/1856 K. 2006/3468
245	Y11.CD	30.5.2006	E. 2006/2513 K. 2006/4870
245	Y11.CD	5.6.2006	E. 2006/2428 K. 2006/5098
245	Y11.CD	14.6.2006	E. 2006/3035 K. 2006/5495
245	Y6.CD	26.6.2006	E. 2006/3750 K. 2006/6651
245	Y11.CD	12.7.2006	E. 2006/3327 K. 2006/6649
245	Y11.CD	20.9.2006	E. 2006/5243 K. 2006/7374
245	Y11.CD	25.9.2006	E. 2006/5514 K. 2006/7524
245	Y11.CD	30.10.2006	E. 2006/5208 K. 2006/8493
245	Y11.CD	5.12.2006	E. 2006/7207 K. 2006/9886
245	Y11.CD	13.12.2006	E. 2006/8164 K. 2006/10200
245	Y11.CD	9.1.2007	E. 2006/5949 K. 2007/1
245	Y11.CD	29.1.2007	E. 2006/8430 K. 2007/282
245	Y11.CD	7.3.2007	E. 2007/199 K. 2007/1473
245	Y11.CD	12.3.2007	E. 2005/8843 K. 2007/1582
245	Y11.CD	14.3.2007	E. 2007/480 K. 2007/1683
245	Y11.CD	2.4.2007	E. 2006/8242 K. 2007/2283
245	Y11.CD	13.6.2007	E. 2007/2649 K. 2007/4142
245	Y11.CD	17.7.2007	E. 2007/5557 K. 2007/5170
245	Y11.CD	24.9.2007	E. 2007/6874 K. 2007/5826
245	Y11.CD	27.9.2007	E. 2007/6530 K. 2007/6017
245	Y11.CD	12.11.2007	E. 2007/7255 K. 2007/7837
245	Y11.CD	6.2.2008	E. 2006/367 K. 2008/574
245	Y11.CD	20.2.2008	E. 2007/8458 K. 2008/915
245	Y11.CD	5.3.2008	E. 2007/7660 K. 2008/1296
245	Y11.CD	18.3.2008	E. 2006/1891 K. 2008/1623

245	YCGK	27.5.2008	E. 2008/11-127 K. 2008/147
245	YCGK	27.5.2008	E. 2008/11-87 K. 2008/150
245	Y11.CD	11.6.2008	E. 2008/3819 K. 2008/5910
245	Y11.CD	17.6.2008	E. 2006/3811 K. 2008/6336
245	Y11.CD	17.6.2008	E. 2006/3995 K. 2008/6351
245	Y6.CD	17.6.2008	E. 2007/14075 K. 2008/13647
245	Y11.CD	4.7.2008	E. 2008/5042 K. 2008/7221
245	Y11.CD	17.9.2008	E. 2008/12914 K. 2008/8887
245	Y11.CD	23.9.2008	E. 2008/9636 K. 2008/9181
245	Y11.CD	24.9.2008	E. 2008/8860 K. 2008/9215
245	Y11.CD	9.10.2008	E. 2006/3768 K. 2008/10124
245	Y11.CD	3.11.2008	E. 2006/4791 K. 2008/10984
245	Y11.CD	3.12.2008	E. 2006/4682 K. 2008/12691
245	Y11.CD	4.2.2009	E. 2008/15452 K. 2009/488
245	Y6.CD	17.3.2009	E. 2008/11599 K. 2009/5135
245	Y11.CD	9.4.2009	E. 2009/630 K. 2009/4067
245	Y11.CD	6.5.2009	E. 2008/20909 K. 2009/5303
245	Y11.CD	4.6.2009	E. 2009/4462 K. 2009/6890
245	Y11.CD	6.7.2009	E. 2009/13310 K. 2009/8701
245	Y11.CD	8.10.2009	E. 2009/14916 K. 2009/11372
245	Y11.CD	24.11.2009	E. 2007/849 K. 2009/14539
245	Y11.CD	7.12.2009	E. 2009/18692 K. 2009/14758
245	Y11.CD	16.2.2010	E. 2009/22078 K. 2010/1382
245	YCGK	30.3.2010	E. 2010/11-17 K. 2010/65
245	Y11.CD	29.4.2010	E. 2009/15793 K. 2010/4885
245	Y11.CD	3.5.2010	E. 2007/8741 K. 2010/5625
245	Y11.CD	26.5.2010	E. 2010/4953 K. 2010/6357
245	Y11.CD	21.6.2010	E. 2010/4547 K. 2010/7082
245	Y11.CD	20.9.2010	E. 2010/9643 K. 2010/9400

Yukarıda listesi verilen içtihatlar incelendiğinde, hem ilk derece mahkemelerinin hem de Yargıtay'ın gerek bilişim suçlarında gerekse bilişim yoluyla işlenen suçlarda ciddi çelişkiler içinde olduğunu görmekteyiz. Benzer eylemlerle işlenen suçlarda farklı mahkemelerin hem esas yönünden hem de usul yönünden farklı uygulamalarda bulunduğunu gibi, farklı Yargıtay daireleri de farklı içtihatlar geliştirmiştir. Bununla birlikte somut olaylarda aynı daire üyeleri dahi farklı görüşlerde bulunmaktadırlar.

Birinci derece mahkemeleri ve Yargıtay tarafından bilişim bağlantılı suçlarla ilgili olarak yaşanan görüş ayrılıklarını maddeler halinde sıralayacak olursak;

1. Gerçekleştirilen eylemin bir "bilişim suçu" mu yoksa "bilişim yoluyla işlenen suç" mu olduğu tam tespit edilememektedir.

2. Özellikle “bilişim yoluyla işlenen suçlarda” yargılama yapılırken aynı zamanda “bilişim suçu” da işlendiği kabul edilerek yargılama yapılıp yapılmaması konusunda farklı içtihatlar vardır.
3. Birden çok mağdurun olduğu “bilişim bağlantılı suçlarda” hem mağdurlar hem de mağdur oldukları konular net tespit edilememektedir.
4. 2006 yılında Türk Ceza Kanunu’nun değişmesiyle birlikte yargılamada ciddi aksaklıklar yaşanmıştır. Çünkü bahse konu eylem işlendiği tarihte eski ceza kanunu yürürlükte olduğu davalarda hangi kanunun sanığın lehine olduğu tam olarak tespit edilememiştir.
5. İçtihatlarda konu edilen bazı davalar incelendiğinde eylemin hangi suç türüne girdiği yanlış tespit edildiğinden yargılama yanlış mahkemelerde sürdürülmüş ve Yargıtay tarafından bozulmuştur.

Yukarıda maddeler halinde sıralan problemlere bakıldığında halen “bilişim bağlantılı suçlarla” ilgili olarak yargılama sürecinin tam olarak yerleşmediği görülmektedir. Nitekim benzer davalarda Yargıtay tarafından dahi farklı içtihatlar geliştirilmesi de ilk derece mahkemelerini farklı uygulamalara sevk edebilecektir.

Bilişim teknolojilerinin gelişmesiyle birlikte adliye mensuplarının bu alandaki suçlarda yetersiz kalmasının bir diğer sebebi olarak da ilgili kanun maddelerinin yetersiz olduğu da yine Yargıtay içtihatların da geçmektedir.

Örnek 2 de değindiğimiz Emsal kararın bir bölümünde şu açıklamalar yer almaktadır;

Bilişim suçları, öğretide ve uygulamada öncelikle;

a)Doğrudan bilişim suçu (gerçek bilişim suçları)

b)Dolayısıyla bilişim suçu (bilişim bağlantılı suçlar)biçiminde tasnife tabi tutulmuştur. Türk Ceza Kanununda da bu sistem kabul edilmiştir. Şöyle ki:

Bilişim sisteminden amaç, verileri toplayıp yerleştirdikten sonra bunları otomatik işleme tabi tutma olanağını veren manyetik sistemlerdir. Bilişim alam ise, bilgileri depo ettikten sonra bunları otomatik olarak işleme tabi tutan sistemlerden oluşan alanlardır. Ceza Yasasının 2. Kitap, 3. Kısım, 10. Bölümünde 'Bilişim Alanında Suçlar' başlığında 243. maddede' Bilişim

Sistemine Girme; 244. maddede 'Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme' 245. maddede 'Banka veya Kredi Kartlarının Kötüye Kullanılması' düzenlenmiştir.

Dolayısıyla bilişim suçları ise, klasik suçların bilişim sistemlerinden yararlanılarak işlenmesi olup, bu suçların nitelikli şekli olarak o suçla ilgili bölümlerde yer almaktadır. TCK'nın 112, 113, 125, 132, 133, 134, 135, 136, 138, 142/2-e, 158/1-f, 213-218, 226, 228 vs maddelerinde yazılı suçların bilişim sistemleri kullanılarak işlenmesi mümkündür. Bu suçlardan davayı ilgilendiren ve sanığın eylemine uygun bulunan suç, TCK'nın 142/2-e maddesinde öngörülen 'bilişim sistemlerinin kullanılması suretiyle hırsızlık' suçu olup, bu suç üzerinde durulacaktır.

Bu açıklamalarda öğretideki yaklaşımların Yargıtay içtihatlarında önemle dikkate alındığını açıkça görmekteyiz. Çalışmamızda sık sık altınız çizdiğimiz "bilişim bağlantılı suçların" bir alt kolu olan "bilişim yoluyla işlenen suçlar" burada "dolayısıyla bilişim suçu" ya da "bilişim bağlantılı suç" olarak öğretiden alınmıştır. Görüldüğü üzere öğretideki yanlış yaklaşımlar yargı sürecini de etkilemektedir.

3.5.2. Adli Bilişim

Adli bilişim sürecinin uygulamada nasıl işlediğini en iyi anlamın yolu bu alanda yapılan örnekleri incelemek olacaktır. Dünyada adli bilişim işlemleri sayesinde çözülmüş çok kritik davalar bulunmaktadır. Bu örnekleri incelemek adli bilişimin hem nasıl hayata geçirildiğini hem de suçu aydınlatmada ne kadar etkili bir teknik olduğunu ortaya koymaktadır.

3.5.2.1. Örnek 1: BTK Davası

Dennis Rader, Wichita, Kansas'ta (ABD) 1974-1991 yılları arasında tam 10 cinayet işlemiştir. Cinayetlerde polisin elindeki tek delil tahtalar üzerine kazılmış imzası (BTK – Bind, Torture and Kill – Bağla, İşkence et ve Öldür) ve olay yerinde bulunan DNA örnekleridir. Ancak yıllarca süren soruşturma neticesinde herhangi bir sonuç elde edilememiştir.[331]

[331] Robinson, Bryan, (2004), "The 'BTK' Case: Inside the Mind of a Serial Killer", http://abcnews.go.com/US/News/story?id=294705&page=1, (Erişim Tarihi: 03.01.2011).

BTK cinayetlerini işlerken bunların duyulmasını, ünlü olmayı ama bir sır olarak kalmayı planlıyordu. Uzun bir süre sessizliğini korusa da belli zamanlarda hep Kansas'taki medya gruplarıyla iletişime geçiyor ve kendine göre mesajlar veriyordu. Bunun yanı sıra defalarca mektup gönderiyor ve adeta onlarla oynuyordu. Tüm bu yaptıklarına rağmen yakalanmadığı için bir süre sonra BTK'nın bir polis olabileceği bile tartışılmış ve hatta şüphelenilen polis departmanındaki bütün polislerin DNA örnekleri alınıp olay yerinden elde edilenlerle karşılaştırılmıştır. Ama bir sonuca varılamamıştır.[332]

Tüm bu çalışmalar devam ederken BTK yine kendince bir oyun kurgulamaktadır. Şubat 2005 de Wichita televizyonlarından biri olan KSAS'a bir mor renkte, şeffaf bir disket yollar. Disketin üzerinde 3 X 5 cmlik bir etiket vardır ve içerisin de sadece "test.rtf" adında bir metin dosyası bulunmaktadır. Dosyanın içerisinde de "Disketin üzerindeki etiketi okuyun!" yazmaktadır.[333]

İlk başlarda bundan bir şeyler çıkartamayan polis disketin dijital olarak incelenmesi için "Çöl Fırtınası" operasyonunda görev almış eski bir asker olan ve 1998 yılında beri Wichita polis departmanında bilişim suçları bölümünde görev yapan 39 yaşındaki Randy Stone'a başvurur. Randy Stone diskette ve içindeki dosyada yaptığı çok ayrıntılı incelemelerde disketin Wichita'nın Christ Lutheran Kilisesi'nde kullanıldığına ve bir önceki kullanıcısının "Dennis" adında bir isimle oturum açtığını tespit eder. Randy Stone hemen Wichita'nın Christ Lutheran Kilisesi'nin resmi internet sitesine girer ve orada çalışanların listesine bakar. Çalışanlardan birisinin adı "Dennis Rader" dır. Dennis Rader hemen yakalanır ve DNA örnekleriyle olay yerinden alınan örnekler eşleşmiştir.[334] Sonuç olarak otuz bir yıldır çözülemeyen dava neredeyse on beş dakika içinde çözülmüştür.

3.5.2.2. Örnek 2: Scott W. Tyree Davası

Bir gece Alicia Kozakiewicz ortadan kaybolur, Pittsburgh'taki evlerinde anne babası ve erkek kardeşiyle birlikte yemek yedikten sonra odasına çekilir ve on üç yaşındaki

[332] wikipedia.org, (2010), "Dennis Rader", http://en.wikipedia.org/wiki/Dennis_Rader, (Erişim Tarihi: 03.01.2011).
[333] trutv.com, (t.y.), "The BTK Story", http://www.trutv.com/library/crime/serial_killers/unsolved/btk/25.html, (Erişim Tarihi: 03.01.2011).
[334] Reagan, Brad, (2006), "Computer Forensics: The New Fingerprinting", http://www.popularmechanics.com/technology/how-to/computer-security/2672751, (Erişim Tarihi: 03.01.2011).

kız bir daha geri dönmez. Ebeveynleri odasını kontrol ettiklerinde ne bir not ne de bir zorlanma belirtisi görmezler.[335]

Bir taraftan komşuları çevredeki boş arazileri ve dereleri araştırırken Pittsburgh polisi de ailesi ve arkadaşlarıyla iki gün boyunca görüşür ancak bir sonuç elde edemez. FBI ajanı Denise Holtz davayı devraldığında soruşturma odak noktasından oldukça uzaklaşmıştır. Holtz'un bütün bildiği: Alicia şiir yazan utangaç bir çocuktur ve onur duyulan başarılı öğrencilerden birisidir. Son zamanlarda sıkıntı içindedir. Tek bir ipucu vardır: Arkadaşları Alicia'nın sık sık İnternet Sohbet odalarında vakit geçirdiğini söylerler.[336]

Holtz büronun bilgisayar uzmanlarından birisi olan FBI dijital delil inceleme uzmanı Tony Pallone ile görüşür. Pallone, Alicia'nın bilgisayarındaki sabit diskin analiz için imajını alır ve adli bilişim işlemi için hazırlıklarını tamamlar.

Alicia'nın kişisel internet sayfasına bakıldığında, Pallone onun kendisini "goddessofall" olarak isimlendirdiğini ve ilgi alanlarını da sihirbazlık, hipnoz ve mitoloji olarak listelediğini görür, böylece sabit diskindeki verilerde hep bu kelimeleri arayarak bu karışık karakteri daha da netleştirebilecek ipuçlarına ulaşır. Bazı ilginç bilgiler bulur: atık dosya kayıtları bilgisayarın en son işlemlerinde Alicia'nın "sadist ve mazoşist" adında bir sohbet odasını ziyaret ettiğini gösterir. Daha da kötüsü, Pallone atık dosya parçalarından Alicia'nın endişelendirecek bir takma ad kullanan "dcsadist" diye birisiyle sohbet ettiğini fikrine varır. Pallone, internette bu takma adı kullanan birisinin olup olmadığını araştırır ancak bir sonuç bulamaz.[337]

Pallone yoğun bir tempoyla laboratuarında çalışmasını bırakırken dedektiflerde sonunda Alicia'yı arama işlerine mola vermişlerdir. İsmini vermek istemeyen Tampalı bir adam FBI ile iletişime geçer ve "Pittsburgh Post-Gazette" gazetesinin internet sitesinde kayıp kız olarak resmi çıkan çocuk hakkında bir şeyler biliyor olabileceğini söyler. İhbarcı internette bir kızı yakaladığını iddia eden bir

[335] Fuoco, Michael A., (2002), "Missing Teen Found Safe But Tied Up İn Virginia Townhouse", http://www.post-gazette.com/regionstate/20020105missingp1.asp, (Erişim Tarihi: 03.01.2011).
[336] Jackmon, Tom, (2002), "Girl Chained In Herndon Is Reunited With Family", http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A2747-2002Jan5&notFound=true, (Erişim Tarihi: 03.01.2011).
[337] Etzel, Jack, (t.y.), "Is Your Child Safe? Kidnapped! A Victim Is Inspired By Her Own Horrific Story", http://www.northhillsmonthly.com/200703/perspective.php, (Erişim Tarihi: 03.01.2011).

grup ile karşılaştığını söyler. İhbarcıya "Galiba birini ele geçerdim" diye yazar adam ve duvara zincirlenmiş ağlayan bir kızın da videosunu göstermiştir. İhbarcı adamın kuzey Virginia'da yaşadığını ve "master for teen slave girls (küçük köle kızların efendisi)" adıyla bilindiğini düşünüyordur.[338]

İhbarcı adamın takma adını söylediğinde Pallone'ın ortağı Tim Huff ofise gelmiştir. Laboratuardaki altı kişi daha internet ortamında ve sohbet odalarında bu takma adı kullanan olup olmadığını aramak için Pallone'a katılır. Huff belki de adamın "master for teen slave girls" takma adını kullanmak yerine bazı internet kısaltmalarını kullanmış olabileceğini düşünür. Takım üyeleri bu adın varyasyonlarını aramaya başlarlar ve dakikalar içinde ajanlardan birisi Yahoo sohbet odalarında birisinin profil adının "master4teen_slavegirls" olduğunu tespit eder. Profili incelendiğinde de çevrimiçi kişilerden birisi de "dcsadist" takma adını kullanmaktadır.

Kızın bilgisayarından elde ettikleri bilgilerle ihbarcının verdiği isim eşleşir ve büyük bir ihtimalle Alicia'yı kaçıran adam kesinleşmiştir. Ama profilde nerede yaşadığı yazmıyordur. Holtz Yahoo ile iletişime geçip profile bağlanan kullanıcının IP adresini öğrenmeye çalışır ve Vatanseverlik Sözleşmesinin[339] 212. bölümü gereği Yahoo'dan IP adresini öğrenmek için faks yollar.

Yahoo, Pittsburgh laboratuarına IP adresini bildirir. Servis sağlayıcı Verizon'dan IP adresinin sorgulanması istenir. Verizon Holtz'a müşterinin adını ve adresini, 38 yaşındaki Scott William Tyree[340], Herndon, Va. olarak kayıtlarında geçtiğini bildirir. Tyree'nin adresi doğrulandıktan sonra Holtz Washington D.C. de.ki bölge ofisi ile bağlantı kurar ve bir grup ajan Tyree'nin evine gönderilir.

---

[338] Reagan, Brad, (2006), "Computer Forensics: The New Fingerprinting", http://www.popularmechanics.com/technology/how-to/computer-security/2672751, (Erişim Tarihi: 03.01.2011).

[339] Ekim 2001 de kabul edilen Vatanseverlik Sözleşmesi'nden önce, firmalar devletle işbirliği yapılması gerektiğinde müşterileri ile ilgili tuttukları bilgileri kolluk kuvvetleriyle paylaşabilmeleri için adli kararlara ihtiyaç vardı aksi takdirde cezalandırılacaklardır. Ancak 212. bölüm sivillerin güvenliğini ilgilendiriyordu ve "ölüm tehlikesi veya ağır yaralanma" durumları söz konusu olduğunda şirketlere bu anlamda bir serbestlik tanınmıştı. Bu dava sözleşmenin ilk uygulamalarından birisidir. ("Usa Patrıot Act" - http://en.wikipedia.org/wiki/USA_PATRIOT_Act, Erişim Tarihi: 03.01.2011).

[340] Roddy, B. Dennis ve Schimitz, Jon, (2002), "Suspect Scott Tyree: 'A Classic Long-Haired Computer Guy'", http://www.post-gazette.com/regionstate/20020105tyreep2.asp, (Erişim Tarihi: 03.01.2011).

Tyree'nin varoşlardaki kasaba evine ajanlar silahları ile birlikte girerler. Üst kattaki yatak odasında Alicia bağlanmış ve tavandaki bir halkaya zincirlenmiş olarak bulunana dek ev boş gibi gözüküyordur. Zincirler sadece onun banyoya gidebileceği kadar uzundur. Tyree Alicia'yı kaçmaya çalışırsa ona zarar vereceği şeklinde uyarmıştır ve yakındaki bir bilgisayar firmasında çalıştığını söylemiştir.[341]

Sonuç olarak adli bilişim teknikleri sayesinde çok kritik bir olay çözülmüş ve muhtemel bir can kaybı önlenmiştir. Bu tür olayların yaşandığı tarihten itibaren günümüze kadar bilişim teknolojilerinin günlük hayatımızı yeri çok daha artmıştır. Bu nedenle birçok suç türünde, suçu aydınlatma ve muhtemel zararlarını önlemede adli bilişim tekniklerinin kullanılması daha elzem gibi görünmektedir.

Adli bilişim süreci ile ilgili verdiğimiz iki örnekte dikkat edilmesi gereken husus iki somut olayda da ne bir "bilişim suçu" ne de bir "bilişim yoluyla işlenen suç" mevcuttur. Evet, her iki olayda da bilişim bağlantılı durumlar vardır ve olaylar bu bağlantılar sayesinde çözülmüştür ancak yine de bu suçlara bilişim suçu diyemeyiz. Çalışmamızın genelinde de anlatmaya çalıştığız konulardan birisi de budur. Bir somut olayda bilişim teknolojilerinin yoğun bir şekilde kullanılması o eylemi "bilişim suçu" yapmamaktadır.

[341] Reagan, Brad, (2006), "Computer Forensics: The New Fingerprinting", http://www.popularmechanics.com/technology/how-to/computer-security/2672751, (Erişim Tarihi: 03.01.2011).

SONUÇ

Bilişim teknolojileri ve suç dünyası karşılaştırıldığında, teknolojinin hep bir adım önde olması sebebiyle ne suçla mücadelede ne de yargılama sürecinde taşların tam olarak yerine oturmadığını görmekteyiz. Bu alandaki istatistiklere baktığımızda ise gelecekte bu durumun ciddi sıkıntılar yaratacağını öngörmek mümkündür. Özellikle "bilişim bağlantılı suç", "bilişim suçu", "bilişim yoluyla işlenen suç" ve "adli bilişim" gibi konuların arasındaki bağlantı ve farklılıklar net olarak anlaşılmalı ve bu doğrultuda uygulamalar geliştirilmelidir.

Geniş tabiriyle siber suçlar farklı meslek grupları tarafından farklı anlaşılmakta ve farklı anlamlarda kullanılmaktadır. Emniyet birimleri, hâkimler, savcılar, avukatlar, akademisyenler, mühendisler, bilişim uzmanları, bilgi güvenliği uzmanları gibi konuyla direkt ya da doğrudan ilgili çevreler ne yazık ki tam olarak aynı dili konuşmamaktadırlar. Normal olarak her grup konuya kendi açısından bakmaktadır. Bu durumun doğal sonucu olarak suç ve suçluyla mücadele yeteri kadar başarılı olamamaktadır.

Bilişim bağlantılı suçların yapısı gereği uluslar arası boyutu olduğundan etraflıca bahsettik. Bu nedenle sadece bir ülkenin kendi içindeki kurumlarının dahi ortak bir dili kullanması ve işbirliği içinde olması ne yazık ki yeterli olmamaktadır. Bu alanda mücadele eden ülkelerin verimli bir işbirliği gerçekleştirebilmeleri için kendi aralarında da ortak bir dili geliştirmeleri gerekmektedir. Bu amaçla yapılan düzenlemelerin genel olarak benzer olmasının yanında daha standart hale getirilmesi uluslar arası işbirliği için elzem gözükmektedir.

Bunun devamında ise ülkeler bilişim bağlantılı suçlarla ilgili kendi hukuki düzenlemelerini yaparken uluslar arası düzenlemelere paralel hareket etmelidir. Ancak ülkemizde de olduğu gibi her ülke kendi özel durumlarına göre mevzuatlarını düzenlemektedir. Ülkemizde banka ve ya kredi kartlarının kötüye kullanılması suçunda hiçbir bilişim teknolojisi kullanılmasa bile bilişim suçu kapsamında değerlendirilmektedir. Bunun nedenlerinden birinci bölümde bahsedilmiştir. Üçüncü bölümde değerlendirilen istatistiklerde de bu suçun diğer bilişim suçlarına göre çok daha fazla işlendiği görülmektedir. Bu suçların mali boyutunun da diğer bilişim

suçlarına oranla çok daha fazla olduğunu düşünürsek ülkemiz bilişim suçları mevzuatının buna özel bir yer vermesi doğaldır.

Yine üçüncü bölümde mukayeseli hukuk açısından bilişim bağlantılı suçları irdelenirken farklı ülkelerin farklı hukuki düzenlemeleri olduğu görülmüştür. Her ne kadar uluslararası düzenlemelerde bir çerçeve çizilmeye çalışılsa da her ülke kendi özel durumuna göre davranmaktadır.

"Bilişim suçu ve bilişim yoluyla işlenen suç ayrımı" ceza muhakemesi açısından üzerinde önemli durulması gereken bir konudur. Böyle bir ayrıma gitmek yerine bu tür suçların hepsini bilişim suçu kapsamında birleştirmek birbirlerinden çok farklı statüsü olan suçları aynı yaptırımla cezalandırmayı gerektireceğinden adilane olmayacaktır. Bunun yanında bu ayrım yapılmadığı zaman bilişim suçlarının kapsamı gelecekte sağlıklı bir yargılama yapılamayacak kadar genişleyecektir.

Bir suçu, bilişim suçu veya bilişim yoluyla işlenen suç kapsamında değerlendirirken çıkış noktamız bilişim teknolojilerinin araç veya amaç olarak kullanılması ayrımıdır. Eğer bir suçta bilişim teknolojileri "hedef" ise orada "bilişim suçundan" bahsetmek gerekir yok eğer bilişim teknolojileri başka bir suçu işlemek için "araç" olarak kullanılıyorsa "bilişim yoluyla işlenen suçtan" bahsedebiliriz. Bu çıkış noktası genel olarak bu ayrımı yapmak için yeterlidir ancak bazı karmaşık olaylarda yeterli olmayabilir. Bu gibi durumlarda mağdurun mağduriyet konusuna bakılmalıdır.

Bilişim suçları ve bilişim yoluyla işlenen suçların soruşturma ve kovuşturma evreleri açısından da benzerlik ve farklılıkları bulunmaktadır. Bu suçlarla ilgili olarak sağlıklı bir yargılama sürecinin yürütülebilmesi için bu benzerlik ve farklılıkların da doğru bilinmesi ve uygulamada da buna göre davranılması gerekmektedir. Özellikle soruşturma evresinin hızlı tamamlanabilmesi için bilişim suçları ve bilişim yoluyla işlenen suçların iyi tahlil edilmesi gerekmektedir.

"Bilişim suçu ve bilişim yoluyla işlenen suç ayrımının" adalet sistemimiz tarafından tam olarak benimsenmesi için öncelikle savcılar, hâkimler ve avukatlar bu alanda eğitilmelidir. Bu tür suçlarda uzmanlaşabilmek için eğitim yanında tecrübe de çok önemlidir ancak özellikle hâkimler tarafından bu tecrübe kazanılana kadar yargılama sürecinin sağlıklı yürümesi için bu alanda araştırma yapan uzmanların da teknik öğretiye eksik ve yanlış katkılar yapmaması gerekmektedir.

Bu alandaki diğer bir sıkıntı da hiç şüphesiz ilgili hukuki düzenlemelerdir. Ceza kanunları sık sık değiştirilmemesi gereken kanunlardır ancak bilişim teknolojileri hızla değişmekte ve bilişim bağlantılı suçları da değiştirmektedir. Bu nedenle bilişim bağlantılı suçlarla ilgili kanunlar hazırlanırken gelecekteki değişikler öngörülmelidir. Bununla birlikte güncel yenilikler ve değişiklikler hukuki metinlere yansıtılamasa bile adliye personeli bu yeni gelişmelere paralel olarak bilgilendirilmeli ve yönlendirilmelidir.

"Bilişim suçu ve bilişim yoluyla işlenen suç" ayrımının birbirine karıştırılmaması için ceza kanunumuzda bilişim suçu olarak tanımlanan eylemler tekrar gözden geçirilmelidir. Özellikle "bilişim alanında suçlar" başlığı altında düzenlenmesi gerektiği ileri sürülen ancak "bilişim yoluyla işlenen bir suç türü" olan "kişisel verilere yönelik suçların" durumu tekrar değerlendirilmelidir.

Hukuki açından suç oluşturmayan ancak bilgisayar ve internet kullanımından kaynaklanan mağduriyetlere de emniyet ve adalet birimleri duyarsız kalmamalıdır. Emniyet birimleri önleyici polislik çerçevesinde konuya yaklaşarak gelecekte ortaya çıkabilecek olumsuzlukları giderecek önemleri tartışmalıdır. Adalet birimleri de bu mağduriyetleri giderebilecek düzenlemelerin mümkün olup olmadığını araştırmalıdır.

Adli bilişim açısından da benzer hukuki sıkıntılar giderilmelidir. Giderek etkinliği ve önemi artan "adli bilişim" uygulamaları ile ilgili CMK'nın tek bir maddesinde yapılan düzenlemeler ciddi eksiklikler taşımaktadır. Bunun giderilmesi için mevcut madde değiştirilmeli ve yeni düzenlemeler yapılmalıdır.

Adli bilişim sürecinin hukuki dayanağı olan kanun metninde sadece "bilgisayar" teriminin geçmesi diğer bilişim cihazlarına yönelik adli bilişim incelemelerinin yapılıp yapılamayacağı eleştirisini ortaya çıkarmaktadır. Bununla birlikte inceleme yapılan bilgisayar disklerinin bir kopyasının istenmesi durumunda şüpheliye verilmesi disk içinde suça konu veriler olduğu durumlarda sıkıntı doğurmaktadır. Örneğin ilgili diskin içinde başkalarına ait kredi kartı bilgileri olsa bile şüpheli şahsa diskinin kopyası geri verilmektedir. Son olarak en çok eleştirilen diğer bir konu da bilgisayar diskinden elde edilen iletişim kayıtlarıdır. Bu kayıtlar delil olarak kullanılmaktadır ancak bazı hukukçulara göre bunun için "iletişimin tespiti, dinlenmesi ve kayda alınması" hükümlerine göre hareket edilmeli ve buna

göre ek bir mahkeme kararı alınması gerekmektedir. Bu haklı eleştirilerin giderilmesi için yeni hukuki düzenlemelerin yapılması kaçınılmazdır.

Hem bilişim bağlantılı suçlarla ilgili hem de adli bilişimle ilgili hukuki düzenlemelerdeki eksiklikler ve buna paralel yanlış uygulamalar suçluları da cesaretlendirmektedir. Klasik suçlarda cezasını ve nasıl yakalanacağını bilen suçlular için bu ciddi bir caydırıcı unsurdur. Ancak bilişim bağlantılı suçlarla ilgili hukuki düzenlemelerdeki eksiklikleri bilen suçlular bundan faydalanmaktadırlar. Adli bilişimle ilgili hukuki eksiklikler de suçlular yakalandıktan sonra suçu aydınlatmada ve ispat sırasında suçlu açısından ciddi avantajlar sağlamaktadır. İkinci bölümde bahsedilen anti adli bilişim teknikleri de bu amaca yöneliktir. Bunun giderilebilmesi için gerekli teknik ve hukuki önlemler alınmalıdır.

Emniyet birimleri içersisinde bilişim suçlarıyla mücadele eden birimler organizasyon şeması içinde daha üst seviyede konumlandırılarak ayrı birer daire başkanlığı şeklinde yapılanmalıdır. Bu birim ayrıca bilişim yoluyla işlenen suçlarla ilgili sorumlu olan birimlere de teknik destek vermelidir.

Bilişim bağlantılı suçlarla mücadele edecek birimlere ve bu alanda bilimsel çalışmalar yapanlara, konunun uzmanları tarafından verilen eğitimler ortak bir çatı altında toplanmalı ve standart bir sertifikasyon sistemi tesis edilmelidir. Bu sertifikasyon tesis edilirken ilk etapta uluslar arası sertifikasyonlar örnek alınmalıdır sonrasında ise ülkemizin kendi durumu göz önüne alınarak güncellenmelidir.

Bilişim bağlantılı suçlar ve adli bilişim konusunda çalışan araştırmacılar konuyu doğru değerlendirebilmeleri için özellikle kamu kurumları (adalet bakanlığı, savunma bakanlığı, üniversiteler, barolar) tarafından hazırlanan kaynaklardan (ulusal ve uluslar arası) faydalanmalıdırlar. Barolar yabancı dillerde hazırlanan dokümanları da toplayarak ülkemiz mevzuatına uygun güncel yayınlar hazırlamalıdırlar.

Ülkemizde bilişim bağlantılı suçlar ve adli bilişim konularında düzenlenen bilimsel etkinliklerin sayısı ve kapsamı artırılmalıdır. Özellikle de farklı meslek gruplarının ve uzmanların (yargı mensupları, akademisyenler, teknik uzmanlar ve emniyet birimleri) ortak katılımıyla gerçekleştirilen etkinlikler bu alanda ortak bir dilin oluşturulması için faydalı olacaktır. Ayrıca bu etkinlikler sonucu tespit edilen eksikliklerin hukuki açıdan giderilebilmesi için yasama organına iletilmesi sağlanmalıdır.

Bilişim bağlantılı suçlar ve adli bilişim kapsamında gerçekleştirilen bilimsel etkinlikler, fuarlar, yapılan araştırmalar, polisiye operasyonlar ve yargılamalar uygun olduğu ölçüde kamuoyuyla da paylaşılmalıdır. Böylece bu alanda bir farkındalık yaratılacağı gibi konuya ilgili duyan ve bu alanda araştırma yapmak isteyenlerin de nasıl bir yol izlemesi gerektiği de açığa kavuşturulmuş olacaktır.

Teknik terminolojide yabancı dillerden dilimize çevrilen kavramların doğru çevrilebilmesi için, Adli Tıp Enstitüsü, Bilişim ve Teknoloji Hukuku Enstitüsü ve Güvenlik Bilimleri Enstitüsü gibi kurumların bu amaçla çalışmalar yapmalıdır.

Son olarak şunu söylemek gerekir; Her geçen gün hızla ilerleyen teknolojik gelişmelerle birlikte yaygınlığı artan ve işleniş şekli değişen "bilişim bağlantılı suçlarla" mücadele edebilmek için en azından bu alanda kullanılan teknik terimlerin ortaya çıkış sürecini ve anlamlarını bilmek ve doğru kullanmak gerekmektedir. Aksi takdirde bu nedenlerden ötürü bugün yaşanan sıkıntılar ve yanlış uygulamalar gelecek dönemlerde çok daha fazla olacaktır.

KAYNAKÇA

accuhash.com, (t.y.), "What is Checksum?", http://www.accuhash.com/what-is-checksum.html, (Erişim Tarihi: 02.12.2010).

ACPO Association of Chief Police Officers - E-Crime Working Group and Metropolitan Police Service, (t.y.), "Good Practice Guide for Computer-Based Electronic Evidence", http://www.7safe.com/electronic_evidence/ACPO_guidelines_ computer _ evidence_v4_web.pdf, (Erişim Tarihi: 01.12.2010).

ACPO Association of Chief Police Officers, Natioanal High Tech Crime Unit, (t.y.), "Good Practice Guide for Computer Based Electronic Evidence V. 3.0", http://www.acpo.police.uk/asp/policies/Data/gpg_computer_based_evidence_v3.pdf, (Erişim Tarihi: 02.12.2010).

Akarslan, Hüseyin, (2006), "Adanalı Hacker", http://www.bilgisayarpolisi.com /index.php?sayfa=makaleoku&kategori=3&id=76, (Erişim Tarihi: 09.10.2010)

Akarslan, Hüseyin, (2009), "Türkiye'de Sayılarla Bilişim Suçlar", *İstanbul Bilgi Güvenliği Konferansı '09.*

Akçay, Bilal, (2010), "Bilişim Güvenliği Uzmanı / Yöneticisi", http://www. bilalakcay.com/wordpress/2008/07/bilgisayar-muhendisi-ne-ith-yapar-bilithim-guvenlidhi/, (Erişim Tarihi: 20.11.2010).

Akgün, Fatma; Buluş, Ercan ve Şen, Şenol, (t.y.), "Bilgisayar Ağları Üzerinde İletilen Verilere Zarar Vermek İçin Kullanılan Önemli Teknikler Ve Korunma Yollarının İncelenmesi", http://www.emo.org.tr/ekler/0cc088a48f313ab_ek.pdf, (Erişim Tarihi: 14.11.2010).

Akpınar, Gürsel, (t.y.), "Yeni TCK'na Göre Suçun Unsurları Bağlamında Kast, Taksir Ve Kast-Taksir Kombinasyonu", http://www.ceza-bb.adalet.gov.tr/makale/178.doc, (Erişim Tarihi: 12.10.2010).

Alacakaptan, Uğur, (1975), *Suçun Unsurları*, Ankara: Sevinç Matbaası

angelfire.com, (t.y.), "Spoofing Nedir?", http://www.angelfire.com/biz3/zurnayiz /spoofing.html, (Erişim Tarihi: 16.11.2010).

Ankara Emniyet Müdürlüğü, (t.y.), "Bilgisayar Suçları Sözleşmesi", http://www.ankaraemniyet.gov.tr/index.php?id=601,(Erişim Tarihi: 26.10.2010).

antiphishing.org, (2010), "Phishing Activity Trends Report", http://www. antiphishing.org/reports/apwg_report_Q1_2010.pdf, (Erişim Tarihi: 14.11.2010)

Asayiş Dairesi Başkanlığı, (2009), "Bilişim Yoluyla İşlenen Asayiş Suçları", Hizmet İçi Sunum.

Asayiş Dairesi Başkanlığı, (2010), "Asayiş Suçu Kavramı", http://www. asayis.pol.tr/asayis_sucu.asp, (Erişim Tarihi: 28.10.2010).

Atakan, Mustafa, (2001), "Port Nedir?", http://www.bilisimterimleri.com/bilgisayar _bilgisi/bilgi/32.html, (Erişim Tarihi: 14.11.2010).

Avrupa Konseyi (t.y.), "Biz Kimiz?", http://www.avrupakonseyi.org.tr/bizkimiz.htm, (Erişim Tarihi: 10.12.2010).

Avrupa Konseyi, (2001a), "Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", http://conventions.coe.int/treaty/en/treaties/html /189.htm, (Erişim Tarihi: 10.12.2010).

Avrupa Konseyi, (2001b), "Convention on Cybercrime - List of declarations, reservations and other communications", http://conventions.coe.int/Treaty/Commun/ ChercheSig.asp?NT=185&CM=&DF=&CL=ENG,(Erişim Tarihi: 10.12.2010).

Avrupa Konseyi, (2001c), "Convention on Cybercrime", http://conventions.coe.int /Treaty/EN/Treaties/html/185.htm, (Erişim Tarihi: 17.10.2010).

Aydın, Emin, (1992), *Bilişim suçları ve Hukukuna Giriş*, Ankara: Doruk Yayınları.

Bahtiyar, Ziya, (2003), *Virüsler ve Güvenlik*, İstanbul: Pusula Yayınları.

Balı, Yunus, (2008), *Adli Bilişim Rapor Metinlerinin Yargılama Sürecinde Kullanımı ve Anlamlandırılabilirliği*, *Ses Görüntü ve Data İncelemeleri*, Ankara: Adalet Yayınevi.

Ballard, Mark, (2010), "UN rejects international cybercrime treaty", http://www. computerweekly.com/Articles/2010/04/20/240973/UN-rejects-international-cybercrime-treaty.htm, (Erişim Tarihi: 12.12.2010).

Baştürk, İhsan, (2006), *Genel Olarak Fikir Ve Sanat Eserleri Ve Bunlara İnternet Yoluyla Tecavüz İle Sonuçları*,Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Bayamlıoğlu, İbrahim Emre, (2007), *Fikir Ve Sanat Eserleri Hukukunda Teknolojik Koruma*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Doktora Tezi, İstanbul.

Bıçak, Vahit, (2010), *Suç Muhakemesi Hukuku*, Ankara: Seçkin Yayınevi

Bıçak, Vahit, (t.y.), "Bilim veya Edebiyat Eseri Sahiplerinin Hakları", http://www.caginpolisi.com.tr/75/5-6-7-8.htm, (Erişim Tarihi: 30.10.2010).

Bican, Can, (2008), "Sosyal Mühendislik Saldırıları", TUBİTAK-UEKAE, http://www.bilgiguvenligi.gov.tr/index.php?option=com_content&task=view&id=183&Itemid=6, (Erişim Tarihi: 16.11.2010).

Bilgi Teknolojileri ve İletişim Kurumu, (2010a),"Pazar Verileri", http://www. btk.gov.tr/Yayin/ Yayinlar.htm, (Erişim Tarihi:23.10.2010).

Bilgi Teknolojileri ve İletişim Kurumu, (2010b),"Pazar Verileri", http://www. btk.gov.tr/Yayin/Yayinlar.htm, (Erişim Tarihi:23.10.2010).

bilgisayarnedir.com, (t.y.), "Bilgisayar Nedir ?", http://www.bilgisayarnedir.com/ bilgisayar-nedir.html, (Erişim Tarihi: 19.08.2010).

bilisimhukuk.com, (2009), "Facebook'ta sahte profil oluşturma davası sonuçlandı.", http://www.bilisimhukuk.com/2009/07/facebookta-sahte-profil-olusturma-davasi-sonuclandi/, (Erişim Tarihi: 16.11.2010).

birhost.net, (2008), "Alan Adı (Domain Name) Nedir? Neden Alan Adına İhtiyacım Var?", http://www.birhost.net/edestek/index.php?_m=knowledgebase&_a=viewarticle&kbarticleid=48, (Erişim Tarihi: 19.10.2010).

Bostancı, Gülşah, (2007), *Avrupa İnsan Hakları Sözleşmesi Bağlamında Türk Ceza Hukukunda Suçta Ve Cezada Kanunilik İlkesi*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

boun.edu.tr, (t.y.), "Virüsler", http://www.cc.boun.edu.tr/viruses_tur.html, (Erişim Tarihi: 05.11.2010).

Bozağaç, Cumhur Doruk, (2006), *Ghostware And Rootkit Detection Techniques For Windows [Windows İşletim Sistemi İçin Ghostware Ve Rootkit Yakalama Teknikleri],* Bilkent Üniversitesi Mühendislik ve Gen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara.

Bulut, Erhan, (2001), "Bilirkişi Seçimi Ve Bilirkişi Raporlarının Bağlayıcılığı", http://www.mevzuatdergisi.com/2001/11a/02.htm, (Erişim Tarihi: 15.12.2010)

Burlu, Kamil, (2010), *Bilişimin Karanlık Yüzü*, Ankara: Nirvana Yayınları.

Büyük Türkçe Sözlük, Türk Dil Kurumu,(t.y.), "Suç", http://tdkterim.gov.tr/bts/arama/?kategori=verilst&kelime=su%E7, (Erişim Tarihi: 08.12.2010).

Canbek, Gürol ve Sağıroğlu, Şeref, (2006), *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri*, Ankara: Grafiker Yayınları.

chip.com.tr, (2009), "Bilgisayar Virüslerinin Tarihçesi", http://www.chip.com.tr/blog/simyager/bilgisayar-viruslerinin-tarihcesi_3041.html, (Erişim Tarihi:05.11.2010).

cnnturk.com, (2008), "Eskişehir'de İnternetten Şantaj İddiası", http://www.cnnturk.com/2008/yasam/diger/03/07/eskisehirde.İnternetten.santaj.iddiasi/435622.0/index.html, (Erişim Tarihi: 29.10.2010).

cnnturk.com, (2010a), "70 Milyonun Kimlik Bilgilerini Ele Geçirdiler", http://www.cnnturk.com/2010/turkiye/07/27/70.milyonun.kimlik.bilgilerini.ele.gecirdiler/584821.0/index.html, (Erişim Tarihi: 28.10.2010).

cnnturk.com, (2010b), "Cumhuriyet Savcısı Gök'e Cinsel Taciz'den Ceza", http://www.cnnturk.com/2010/turkiye/10/26/cumhuriyet.savcisi.goke.cinsel.tacizden.ceza/594377.0/index.html, (Erişim Tarihi: 22.10.2010).

Computer Crime & Intellectual Property Section, Department of Justice, (t.y.),"Computer Crime Legal Resources", http://www.justice.gov/criminal/cybercrime/cclaws.html, (Erişim Tarihi: 09.10.2010).

Computer Crime Research Center, (2003) "UN recommendations on fighting cybercrime", http://www.crime-research.org/news/13.05.2005/1225/, (Erişim Tarihi: 12.12.2010).

Computer Security Institute, (2009), "14th Annual CSI Computer Crime and Security Survey Executive Summary", http://gocsi.com/survey_2009, (Erişim Tarihi: 18.12.2010).

Computer Security Institute, (t.y.), "Computer Security Institute – CSI", http://www.gocsi.com/about, (Erişim Tarihi:18.12.2010).

Cornell University Law School, (t.y.), "Title 18 - Crimes And Criminal Procedure", http://www.law.cornell.edu/uscode/18/usc_sup_01_18.html, (Erişim Tarihi: 09.10.2010).

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

Çelik, Levent, (t.y.), "Bilişim Teknolojilerinin Sosyal Yaşam Üzerindeki Etkileri", http://www.pegem.net/akademi/sempozyumbildiri_detay.aspx?id=8152, (Erişim Tarihi: 03.11.2010).

Çicek, İlker, (2008), *Ülkemizde Adli Bilişim Laboratuarı Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları*, Haliç Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Darende, M. İhsan, (2005), "Yeni TCK'da İştirak", http://www.turkhukuksitesi. com/makale_182.htm, (Erişim Tarihi: 23.10.2010).

Demir, Nurullah, (2010), "Web Güvenliği", http://www.yeniasya.com.tr/2010/10/12/ilim-teknik/default.htm, (Erişim Tarihi: 16.11.2010).

Demirkaya, Vural, (2009), *Delil Güvenliği*, Polis Akademisi Güvenlik Bilimleri Enstitüsü Yayınlanmış Yüksek Lisans Tezi, Ankara.

Dış Ekonomik İlişkiler Kurulu, (t.y.), "İktisadi İşbirliği ve Kalkınma Teşkilatı (OECD)", http://www.deik.org.tr/pages/TR/DEIK_CokTarafliKuruluslar.aspx?ctID=4&IKID=10, (Erişim Tarihi:11.12.2010).

Dokurer, Semih, (2008), *Adli Bilişim, Ses Görüntü ve Data İncelemeleri*, Ankara: Adalet Yayınevi.

Dokurer, Semih, (t.y.a), "Bilişim Suçları Laboratuarlarında Çocuk Pornografisi İncelemeleri", http://www.dokurer.net/files/documents/ChildpornExamining.pdf, (Erişim Tarihi: 19.10.2010).

Dokurer, Semih, (t.y.b), "Ülkemizde Bilişim Suçları Ve Mücadele Yöntemleri", http://bilisimsurasi.org.tr/dosyalar/17.doc, (Erişim Tarihi: 29.07.2009).

Duranske, Benjamin, (2007), "Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life", (http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/, (Erişim Tarihi: 03.11.2010).

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

eccouncil.org, (t.y.), "Certified Ethical Hacker", http://www.eccouncil.org/certification /certified_ethical_hacker.aspx, (Erişim Tarihi: 20.11.2010).

edubilim.com, (2008), "Topluluk Hukukunun Uluslar Üstü (Supranasyonal) Niteliği", http://www.edubilim.com/ana/odev-arsivi/hukuk/1-topluluk-hukukunun-uluslarustu-supranasyonal-niteligi/details.html, (Erişim Tarihi: 09.12.2010).

EGM Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı, (t.y.), "Sanal Dedektiflik Operasyonu", (http://www.kom.gov.tr/Tr/KonuDetay.asp?BKey=64&KKey=119, Erişim Tarihi: 10.11.2010).

e-kesif.com, (t.y.), "E-Keşif ve Adli Bilişim", http://www.e-kesif.com/2008/05/adli-bilisim-nedir.html, (Erişim Tarihi: 30.11.2010).

Ekizer, A. Hakan, (2007), "Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği.)", (http://ekizer.net/index.php?option=com_content&task=view&id=16&Itemid=1, Erişim Tarihi: 02.12.2010).

Elbahadır, Hamza, (2010), *Hacking Interface*, İstanbul: Kodlab Yayınları.

Erbes, Robert, (2004), "Anti Forensics", http://infohost.nmt.edu/~sfs/Students/RobertErbes /Presentations/anti-forensics.ppt, (Erişim Tarihi: 29.01.2011).

Erdağ, Ali İhsan, (t.y.), "Ekonomi, Sanayi ve Ticarete İlişkin Suçlar ve Bilişim Alanında Suçlar", http://www.ceza-bb.adalet.gov.tr/makale/140.doc, (Erişim Tarihi: 16.08.2010).

Erdem, M. Ruhan, (t.y.), "Yeni Türk Ceza Kanunu'nda Malvarlığına Karşı Suçlar", http://www.ceza-bb.adalet.gov.tr/makale/119.doc, (Erişim Tarihi: 28.10.2010).

Erdoğan, Ayten, (2010), "Pedofili: Klinik Özellikleri,Nedenleri ve Tedavisi", http://www.cappsy.org/archives/vol2/no2/cap_02_08.pdf, (Erişim Tarihi: 19.10.2010).

Erdoğan, Mustafa, (2009), "Olay Yeri Güvenliği Ve Olay Yerinin Korunması", Olay Yeri İnceleme [Ders Notları], Güvenlik Bilimleri Enstitüsü, Ankara.

Ergüç, Seher, (2008), *Türk Bankacılık Sisteminde İnternet Bankacılığı İle Yapılan Dolandırıcılıklar Ve Bilişim Suçları Hukuku*, Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Ergün, İsmail, (2008), *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Ankara: Adalet Yayınevi.

Erol, Hüseyin, (2006), *Kurumsal Ağlarda Açık Anahtar Altyapısı Tabanlı Elektronik İmza Uygulaması*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara.

essentialcomputersecurity.com, (t.y.), "Computer Protection: Backdoors", http://www.essentialcomputersecurity.com/Backdoors.html, (Erişim Tarihi: 13.11.2010).

Etzel, Jack, (t.y.), "Is Your Child Safe? Kidnapped! A Victim Is Inspired By Her Own Horrific Story", http://www.northhillsmonthly.com/200703/perspective.php, (Erişim Tarihi: 03.01.2011).

Europol, (2010), "European Union Cybercrime Task Force", http://www.europol.europa.eu/index.asp?page=news&news=pr100622.htm, (Erişim Tarihi: 12.12.2010).

Europol, (t.y.), "EUROPOL, the European Police Office", http://www.europol.europa.eu/, (Erişim Tarihi: 12.12.2010).

evbilgisayari.com, (t.y.), "E-Mail ve İnternet Güvenliğinizi Sağlayın!", http://www.evbilgisayari.com/İnternet-genel/18011-e-mail-İnternet-guvenliginizi-saglayin.html, (Erişim Tarihi: 12.11.2010).

forensicswiki.org, (2010), "Write Blockers", http://www.forensicswiki.org/wiki/Write_Blockers, (Erişim Tarihi: 02.12.2010).

Fuoco, Michael A., (2002), "Missing Teen Found Safe But Tied Up İn Virginia Townhouse", http://www.post-gazette.com/regionstate/20020105missingp1.asp, (Erişim Tarihi: 03.01.2011).

garanti.com.tr, (t.y.), "Phishing (Olta) Saldırıları", http://www.garanti.com.tr /tr/bireysel/subesiz/İnternet_bankaciligi/guvenlik /phishing.page, (Erişim Tarihi: 14.11.2010).

Garlik, (2010), "The Garlik UK Cybercrime Report", https://www.garlik.com/cybercrime _report.php, (Erişim Tarihi: 29.12.2010).

gazetevan.com, (2010), "Deniz Baykal'ın Gizli Kamera Video Görüntüleri İddiasına Savcılık Soruşturması Sürüyor", http://www.gazetevan.com/Deniz_Baykalin _gizli_Kamera_Seks_Video_goruntuleri_iddiasina_savcilik_sorusturmasi_suruyor__ _yenii-1444h.htm, (Erişim Tarihi: 04.01.2011).

Goodman, Marc D. ve Brenner, Susan W., (2002), "The Emerging Consensus on Criminal Conduct in Cyberspace", http://www.lawtechjournal.com/articles/2002/03_ 020625_goodmanbrenner.php, (Erişim Tarihi: 11.12.2010).

Gordon, Gary R. ; Hosmer, Chet D. ; Siedsma, Christineve Rebovich, Don, (2003), "Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime", U.S. Department of Justice.

Gökçen, Ahmet, (t.y.), "E-Posta, MSN Messenger İle Tehdit Edilirsek Veya Hakarete Uğrarsak Ne Yapabiliriz?", http://www.uzmantv.com/eposta-msn-messenger-ile-tehdit-edilirsek-veya-hakarete-ugrarsak-ne-yapabiliriz, (Erişim Tarihi: 22.10.2010).

guvenlikegitimleri.com, (t.y.), "Web Sunuculara Yönelik DOS/DDOS Saldırıları", http://www.guvenlikegitimleri.com/new/calismalar/web_ddos.pdf, (Erişim Tarihi: 14.11.2010).

guvenliweb.org.tr, (2009a), "Mobil İletişim ve İnternet", http://www.guvenliweb.org.tr/ guvenlik/content/mobil-ileti%C5%9Fim-ve-internet, (Erişim Tarihi: 24.10.2010).

guvenliweb.org.tr, (2009b), "Online Bilgiler Geleceğinizi Etkiliyor", http://www. guvenliweb.org.tr/aileler/content/online-bilgiler-gelece%C4%9Finizi-etkiliyor, (Erişim Tarihi: 16.10.2010).

guvenliweb.org.tr, (2009c), "Phishing", http://www.guvenliweb.org.tr/guvenlik/ content/phishing, (Erişim Tarihi: 14.11.2010).

Gündem, Onur, (2006), *Fikir Ve Sanat Eserleri Kanununda Eser Sahibinin Haklarına Bağlantılı Haklar, Bu Hakların Sınırlandırılması Ve Korunması*, Kırıkkale Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Kırıkkale.

Güngören, Bora, (2008), "Bilgi Güvenliği Nedir?", http://www.emo.org.tr/ekler/1440ca9ca2c5e0b_ek.pdf?dergi=2, (Erişim Tarihi: 03.11.2010).

Gürçam, Ufuk, (2008), *İnteraktif Dolandırıcılık*, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Eskişehir.

Gürgen, Ahmet Cemal, (2005), "Teşebbüs", http://www.ceza-bb.adalet.gov.tr/makale/169.doc (Erişim Tarihi: 19.10.2010).

Gürler, Cemalettin,(2007), "Bilişim Sistemlerine Karşı Suçlar Bölümünde Düzenlenen Suç Tipleri", http://www.emo.org.tr/ekler/111f133fa0ea545_ek.pdf?dergi=2, (Erişim Tarihi: 16.10.2010).

Güven, Mehmet, (2004), "İnternette Güvenlik ve Hacker Cracker Meselesi", Ankara: Grafik Yayınları.

haberaktuel.com, (2008), "Bir Savcının Gizli Ses Kaydı Youtube'da Teşhir Edildi", http://www.haberaktuel.com/bir-savcinin-gizli-ses-kaydi-youtubeda-teshir-edildi-haberi-115365.html, (Erişim Tarihi: 25.10.2010).

haberturk.com, (2010), "İnternette Şantaj İddiası", http://www.haberturk.com/yasam/haber/532319-İnternette-santaj-iddiasi, (Erişim Tarihi: 24.10.2010).

hackingalert.com, (t.y.), "Black Hat Hackers", http://www.hackingalert.com/hacking-articles/black-hat-techniques.php, (Erişim Tarihi: 22.11.2010).

Hafızoğulları, Zeki, (t.y.), "5237 Sayılı Türk Ceza Kanununda Bileşik Suçun Tanımı Hakkında", http://www.zekihafizogullari.com/Makaleler/TCK%20Bilesik%20Suc.doc, (Erişim Tarihi: 27.10.2010).

Hancı, Hamit, (2003), *Bilirkişilik ve Çapraz Sorgu*, Ankara: Seçkin Yayıncılık.

Harris, Shon, (2008), "Gray Hat Hacking : The Ethical Hacker's Handbook", ABD: The McGraw-Hill.

hukuki.net, (2009), "Hukuk Sistemleri", http://wiki.hukuki.net/Hukuk_sistemleri, (Erişim Tarihi: 09.10.2010).

hurriyet.com.tr, (2009), “Facebook Kişisel Bilgileri Satacak”, http://www.hurriyet.com.tr/teknoloji/10944027.asp, (Erişim Tarihi: 28.10.2010).

Interpol, (2010a), “Information Technology Crime”, http://www.interpol.int/public/TechnologyCrime/default.asp, (Erişim Tarihi: 12.12.2010).

Interpol, (2010b), “Regional Working Parties”, http://www.interpol.int/Public/TechnologyCrime/WorkingParties/Default.asp, (Erişim Tarihi: 12.12.2010).

Interpol, (t.y), “Interpol”, http://www.interpol.int/,(Erişim Tarihi: 12.12.2010).

İnternet Crime Complaint Center – USA Department of Justice, (2010), “2009 Internet Crime Report”, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf, (Erişim Tarihi:18.12.2010).

internetworldstats.com, (2010), “World İnternet Usage Statistics”, http://www.internetworldstats.com, (Erişim Tarihi: 02.11.2010).

ipnumaram.com, (2010), “IP Adresi Nedir?”, http://www.ip-numaram.com/ipadresi.html, (Erişim Tarihi: 16.10.2010).

İstanbul Üniversitesi Bilgisayar Bilimleri Uygulama ve Araştırma Merkezi, (t.y.), “Casus Yazılım Ne Demek?”, http://bilisim.istanbul.edu.tr/index.asp?grp=makaleler&no=1, (Erişim Tarihi: 10.11.2010).

İzTV, “Yeni Çağın "Korsanları": "Hacker"lar” Belgeseli, İzTV, http://www.iztv.com.tr/program.aspx?id=682, (Erişim Tarihi: 20.11.2010).

Jackmon, Tom, (2002), “Girl Chained In Herndon Is Reunited With Family”, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&contentId=A2747-2002Jan5&notFound=true, (Erişim Tarihi: 03.01.2011).

justice.gov, (2004), “Meeting of G8 Justice and Home Affairs Ministers”, http://www.justice.gov/criminal/cybercrime/g82004/g8_background.html, (Erişim Tarihi: 11.12.2010).

Kahraman, Ezgi, (2009), *Özel Hayatın Gizliliği*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Kara, Mehmet ve Bahşi, Hayrettin, (2010), TÜBİTAK-UEKAE, “Bilişim Sistemleri Güvenliği Araştırmalarının Yönü”, http://www.bilgiguvenligi.gov.tr/guvenlik-

teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, (Erişim Tarihi: 03.11.2010).

Karabal, Mustafa; Peker, Bekir ve Savran, Ali,(2004), "Bilişim Suçları Ve Türk Polis Teşkilatı", http://www.turkhukuksitesi.com/makale_128.htm, (Erişim Tarihi: 07.10.2010).

Karabal, Mustafa; Peker, Bekir; Karakaya, Musa ve Savran, Ali, (2004), *Barışın Köprüsü İnternet*, Konya: Akademilenyum Yayınları.

Karadeniz, Tacettin, (2005), "Türkiye'de Phishing", http://www.olympos.net/belgeler /turkiyede-phishing-126266.html, (Erişim Tarihi: 14.11.2010).

Karagülmez, Ali, (2009), *Bilişim Suçları ve Soruşturma – Kovuşturma Evreleri*, Ankara: Seçkin Yayınları.

Karagülmez, Ali, (t.y.), "Bilişim Suçlarında Delil Toplamayı Etkileyen Başlıca Konular", http://www.caginpolisi.com.tr/46/7-8-9-10.htm, (Erişim Tarihi: 03.09.2010).

Karayel, Ayhan, (2006), *Retrospektif Bir Çalışma: 2001-2005 Yılları Arasında Adana İl Emniyet Müdürlüğüne Yansıyan Cinsel Taciz Vakalarının İncelenmesi*, Çukurova Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Adana.

Kateeb, Bassel ve Altimus, Tim, (t.y.), "Computer Forensics", http://www.sis.pitt.edu /~jjoshi/TELCOM2813/Spring2005/FinaleKateebAltimus.ppt, (Erişim Tarihi: 02.12.2010).

Kazancı Hukuk Programları, (2010a), "Ceza Genel Kurulu 2009/11-193 E., 2009/268 K", http://www.kazanci.com/cgi-bin/highlt/ibb/highlight.cgi?file=ibb/files/cgk-2009-11-193.htm, (Erişim Tarihi: 02.01.2011).

Kazancı Hukuk Programları, (2010b), "Kazancı - Mevzuat ve İçtihat Bilgi Bankası Programı", http://www.kazanci.com, (Erişim Tarihi: 02.01.2011).

Keser B., Leyla, (2002), *Adli Bilişim (Computer Forensic)*, Ankara: Yetkin Yayınevi.

Ketizmen, Muammer ve Ülküderner, Çağlar, (t.y.), "E-Devlet UygulamalarındaKişisel Verilerin Korun(ma)ması", http://inet-tr.org.tr/inetconf12/bildiri/2.pdf, (Erişim Tarihi:27.10.2010).

Ketizmen, Muammer, (2008), *Türk Ceza Hukukunda Bilişim Suçları*, Ankara: Adalet Yayınevi.

Kılıç, Savaş, (t.y.), "Müteselsil Suç Kavramı", http://www.hukukcu.com /bilimsel/kitaplar/kilic_muteselsilsuc/endeks.htm, (Erişim Tarihi: 27.10.2010).

Kızıltan, Mehmet Burak, (2007), *5237 Sayılı Türk Ceza Kanununda Bilişim Sistemine Girme, Sistemi Engelleme Ve Bozma Suçları*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

King, Gerard L., (2006), "Forensics Plan Guide", SANS Institute, http://www. giac.org/certified_professionals/practicals/gcfa/283.php, (Erişim Tarihi: 02.12.2010).

Kleiman, Dave, (2007), *The Official CHFI Study Guide (Exam 312-49) for Computer Hacking Forensic Investigators*, ABD: Syngress Publishing.

Koç, Serhat, (2009), "Phishing ile Kredi Kartı Bilgisi Hırsızlığı ve TCK'daki Yansıması", http://www.hukukcu.com/modules/smartsection/item.php?itemid=285, (Erişim Tarihi: 14.11.2010).

Koltuksuz, Ahmet, (2007), *Adli Bilişime Giriş*, Adli Bilişim Kursu [Ders Notları], İzmir Yüksek Teknoloji Enstitüsü, İzmir.

Kurt, Levent, (2005a), *Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması,* TODAİE, Yayınlanmış Yüksek Lisans Tezi, Ankara.

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

lamerism.com, (t.y.), "Lamerism", http://www.lamerism.com, (Erişim Tarihi: 22.11.2010).

Lau, Hon, (2002), "Backdoor.Trojan - Removal", http://www.symantec.com/security_ response/writeup.jsp?docid=2001-062614-1754-99&tabid=3, (Erişim Tarihi: 10.11.2010).

learnthat.com, (t.y.), "Free Definitions : Define newbie. What is newbie?", http://www.learnthat.com/define/view.asp?id=2294, (Erişim Tarihi: 22.11.2010).

Livingstone, S ve Haddon, L, (2009), "EUKids Online: Final Report", http://www2.lse. ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20

Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf, (Erişim Tarihi: 11.10.2010).

Martin, Lockheed, (2005), "Anti - Forensics", http://www.cyberforensics.purdue.edu/documents/AntiForensics_LockheedMartin09152005.pdf, (Erişim Tarihi: 29.01.2011).

memurlar.net, (2005), "Fuhuş Yapan TRT Spikeri Fantezi Kurbanı", http://www.memurlar.net/haber/27191, (Erişim Tarihi: 29.10.2010).

metu.edu.tr, (t.y.), "Bilgisayar Virüsleri", http://www.po.metu.edu.tr/links/inf/ss25/olum14.html, (Erişim Tarihi: 05.11.2010).

microsoft.com, (t.y.), "How to Protect Your Computer from Spyware and Adware", http://www.microsoft.com/windowsxp/using/security/expert/honeycutt_spyware.mspx, (Erişim Tarihi: 11.11.2010).

microsoft.com.tr, (t.y.), "İnternet Servis Sağlayıcısı (ISS) nedir?", http://windows.icrosoft.com/tr-TR/windows-vista/What-is-an-İnternet-Service-Provider-ISP, (Erişim Tarihi: 22.10.2010).

Middleton, Bruce, (2002), *Cyber Crime Investigator's Field Guide*, ABD: Auerbach Publications.

milliyet.com.tr, (2009), "Sosyal Ağ Nedir?", http://blog.milliyet.com.tr/log.aspx?logNo=197465, (Erişim Tarihi: 25.10.2010).

milliyet.com.tr, (2011), "Yanlış Yapan Cezasını Çeker", http://www.milliyet.com.tr/-yanlis-yapan-cezasini-ceker-/siyaset/sondakika/27.01.2011/1344802/default.htm, (Erişim Tarihi: 27.01.2011).

Mitnick, Kevin D.ve William L. Simon, (2005), *Aldatma Sanatı, Ankara*: Odtü Geliştirme Vakfı Yayıncılık.

Moir Robert, (2003), "Defining Malware:FAQ", http://technet.microsoft.com/en-us/library/dd632948.aspx, (Erişim Tarihi:04.11.2010).

news.sky.com, (2008), "Bebo Suicide Cult Fears After Seven Deaths Welsh Town Bridgend",http://news.sky.com/skynews/Home/Sky-News-Archive/Article/20080641301942,(Erişim Tarihi: 16.10.2010).

ntvmsnbc.com, (2006), “Bilgisayar Virüsü 20 Yaşında”, http://arsiv. tvmsnbc.com/news/358295.asp, (Erişim Tarihi: 05.11.2010).

ntvmsnbc.com, (2008a), “Sinyal Boğuculara Yasal Düzenleme Geliyor”, http://www. tvmsnbc.com/id/24934116, (Erişim Tarihi: 24.10.2010).

ntvmsnbc.com, (2008b), “İnternette Kumara İki Yıl Sonra Ceza Geldi”, http://arsiv.ntvmsnbc.com/news/434195.asp, (Erişim Tarihi: 29.10.2010).

ntvmsnbc.com, (2010a), “Facebook'ta Hakarete İlanlı Özür”, http://www. tvmsnbc.com/id/25086314/(Erişim Tarihi: 25.10.2010).

ntvmsnbc.com, (2010b), “Facebook'taki fotoğrafları ölüm getirdi”, http://www. tvmsnbc.com/id/25062133, (Erişim Tarihi: 17.10.2010).

ntvmsnbc.com, (2010c), “Polis Zombi Bilgisayarları 'Hack'ledi”, http://www.ntvmsnbc.com/id/25145670, (Erişim Tarihi: 14.11.2010).

ntvmsnbc.com, (2010d), “Pornoyla Şantaj!”, http://www.ntvmsnbc.com/id/25082652/, (Erişim Tarihi: 23.10.2010).

ntvmsnbc.com, (t.y.), “Ölüme götüren kareler”, http://video.ntvmsnbc.com/olume-goturen-kareler.html, (Erişim Tarihi: 17.10.2010).

nydailynews.com, (2009), “Parents of Holly Grogan, 15, Blame Facebook for Teen's Suicide”, http://www.nydailynews.com/news/world/2009/09/21/2009-09-21_parents _f_olly_grogan_15_blame_facebook_for_teens_suicide.html, (Erişim Tarihi: 17.10.2010).

Online Etymology Dictionary, (t.y.), “forensic”, http://www.etymonline.com/index.php? search=forensic&searchmode=none, (Erişim Tarihi: 06.01.2011).

Organisation for Economic Co-operation and Development, (2002), “Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri – Güvenlik Kültürüne Doğru”, http://www.oecd.org/dataoecd/42/59/32493366.PDF, (Erişim Tarihi: 11.12.2010).

Organisation for Economic Co-operation and Development, (t.y.), “OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security”, http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00& &en-USS_01DBC.html, (Erişim Tarihi:11.12.2010).

Özcan, Mehmet, (t.y.), "Hacker'lar, Teknolojinin Yaramaz Çocukları", http://dosyalar.hurriyet.com.tr/hacker/mozcan.asp, (Erişim Tarihi: 20.11.2010).

Özdemircili, Özgür, (t.y.), "Denial of Service Saldırılarının Önlenmesi", http://www.enderunix.org/docs/dos-saldirilari.pdf, (Erişim Tarihi: 14.11.2010).

Özderyol, Teknail, (2006), *Fikir Ve Sanat Eserleri Kanununda Düzenlenen Suçlar*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Özdilek, Ali Osman, (2003), "Kurtlar Ve Zombiler : Worm'ların ve Ddos Ataklarının Hukuki İncelemesi", http://www.hukukcu.com/bilimsel/kitaplar/wormlarhukuki.htm, (Erişim Tarihi : 9.11.2010).

Özeren, Süleyman, (2006), Siber Terörizm [Ders Notları], Polis Akademisi, Ankara.

Öztürk, Mustafa İlker, (2007), *Bilişim Cihazlarındaki Sayısal Delillerin Tespiti Ve Değerlendirilmesinde İş Akış Modelleri,* Ankara Üniversitesi Sağlık Bilimleri Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara.

Öztürkçi, Halil, (2009), "İphone'unuz Sizi Ele Veriyor", Ankara Bilgi Güvenliği Konferansı, 24 Aralık 2009, Ankara.

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

Palmer, Adrian T.N., (t.y.), "Computer Forensics: The Six Steps", Kroll Ontrack Computer Forensics, http://www.krollontrack.co.uk/publications/UK EE Newsletter I1 V3 AP CF.pdf, (Erişim Tarihi: 02.12.2010).

Parlar, Ali, (2011), *Türk Ceza Hukuku'nda Bilişim Suçları*, Ankara: Bilge Yayınevi.

Pehlivan, İlker, (2010), "Türkiye'deki 'Zombi Bilgisayar'lar 2 Milyonu Geçti, Sayı Hızla Artıyor", http://www.radikal.com.tr/Radikal.aspx?aType=RadikalHaberDetay&ArticleID=998855&Date=26.05.2010&CategoryID=101, (Erişim Tarihi: 14.11.2010)

PowerProNet Bilişim, (t.y.), "Türkiye'nin En Profesyonel Casus Yazılım Sitesi", http://www.powerpronet.net, (Erişim Tarihi: 10.11.2010).

Pro-G ve Oracle, (2003), "Bilişim Güvenliği", http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, (Erişim Tarihi: 03.11.2010).

radikal.com.tr, (2010), “Sanal Fuhuş Tuzaklarla Dolu” http://www.radikal.com.tr/Radikal.aspx?aType=RadikalDetay&ArticleID=1025020&Date=23.10.2010&CategoryID=117, (Erişim Tarihi: 29.10.2010.

Raymond, Eric S., (2002), “İlk Hacker'lar”, http://www.belgeler.org/howto/hacker-history_earlyhacker.html, (Erişim Tarihi: 12.11.2010).

Reagan, Brad, (2006), “Computer Forensics: The New Fingerprinting”, http://www.popularmechanics.com/technology/how-to/computer-security/2672751, (Erişim Tarihi: 03.01.2011).

Robinson, Bryan, (2004), “The 'BTK' Case: Inside the Mind of a Serial Killer”, http://abcnews.go.com/US/News/story?id=294705&page=1, (Erişim Tarihi: 03.01.2011).

Roddy, B. Dennis ve Schimitz, Jon, (2002), “Suspect Scott Tyree: 'A Classic Long-Haired Computer Guy'”, http://www.post-gazette.com/regionstate/20020105tyreep2.asp, (Erişim Tarihi: 03.01.2011).

sabah.com.tr, (2008), “Web Tarikatta 7 İntihar, 2 Girişim” http://arsiv.sabah.com.tr/2008/01/24/haber,7E629FA6E6514F50BEAE1A62882138EE.html, (Erişim Tarihi: 16.10.2010).

Sanal Banka Mağdurları Derneği, (t.y.), “Sanal Banka Mağdurları Derneği”, http://www.sanalbankamagdurlari.com, (02.01.2011).

Sayar, Filiz, (2008), *Hırsızlık Suçu ve Yeni Türk Ceza Kanunu*, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İzmir.

sayisaldelil.net, (t.y.), “Adli Bilişim”, http://sayisaldelil.net/?page_id=19, (Erişim Tarihi: 30.11.2010).

Schell, Bernadette ve Martin, Clemens, (2006), “Webster’s New World Hacker Dictionary”, Indianapolis USA:Wiley Publishing.

Sevim, Tuğrul, (2006), *Elektronik İmza Uygulamasında Kullanılan Zorunlu Ve İhtiyari Dokümanlar,* Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Shirey, R., (2000), “İnternet Security Glossary”, http://tools.ietf.org/html/rfc2828, (Erişim Tarihi: 14.11.2010).

Sırabaşı, Volkan, (t.y.), "Kişisel Verilerin Gizliliği", http://www.fenafil.com/hukuk/İnternet/kisisel_veriler.htm, (Erişim Tarihi: 27.10.2010).

Sjoholm, Hans, (1997), "What is Cracker?", http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html, (Erişim Tarihi: 20.11.2010).

Soyaslan, Doğan, (2009), "Bilişim Alanında Suçlar", *Prof. Dr. Mualla Öncel'e Armağan,* Ankara: Ankara Üniversitesi Hukuk Fakültesi Yayını.

spam.org.tr, (2010), "Spam Nedir?", http://www.spam.org.tr/nedir.html, (Erişim Tarihi: 14.10.2010).

stratejikboyut.com, (t.y.), "İnternet, Özel Hayatın Gizliliği Ve Hukuki Boşluklar",http://www.stratejikboyut.com/haber/İnternet,-ozel-hayatin-gizliligi-ve-hukuki-bosluklar--28234.html, (Erişim Tarihi: 26.10.2010).

swgde.org, (2009), "Digital Evidence", WGDE/SWGIT Digital & Multimedia Evidence Glossary,http://www.swgde.org/documents/current-documents/2009-05-22 SWGDESWGIT DigitalMultimedia Evidence Glossary v2.3.pdf, (Erişim Tarihi: 30.11.2010).

Şıracı, Sertel, (2009), "Zombi Bilgisayarlar Ve Bilişim Suçu", (http://www.sertels.av.tr/avukat/hukuk/bilisim-hukuku/zombi-bilgisayarlar-ve-biliim-sucu.html, (Erişim Tarihi: 14.10.2010).

Şumlu, Selim, (2006), "Hacker Dünyası", *PcNet Dergisi*, (Nisan 2006).

Tan, Aydoğan, (2010), "Adli Bilişim (Computer Forensic)", http://www.edirnebarosu.org.tr/kutuphane/makaleler/89-adli-bilisim-computer-forensic.html, (Erişim Tarihi: 30.11.2010).

Taşdemir, Kubilay, (2009), *Bilişim, Banka veya Kredi Kartlarının Kötüye Kullanılması ve Dolandırıcılık Suçu*, Ankara: Ütopyagrafik.

Taşkın, Şaban Cankat, (2008), *Karşılaştırmalı Hukukta ve Hukukumuzda Bilişim Suçları*, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, İstanbul.

Tavukçuoğlu, Cengiz, (2004), *Bilişim Terimleri Sözlüğü*, Ankara: Asil Yayınları.

tech-faq.com, (t.y.a), "Logic Bomb", http://www.tech-faq.com/logic-bomb.html, (Erişim Tarihi: 12.11.2010).

tech-faq.com, (t.y.b), "Phone Phreaking", http://www.tech-faq.com/phone-phreaking.html, (Erişim Tarihi: 22.11.2010).

techtarget.com, (2000), "What is Brute Force Cracking?", http://searchsecurity. techtarget.com/sDefinition/0,,sid14_gci499494,00.html, (Erişim Tarihi: 14.11.2010).

Tekeli, Ömer, (2005), "Virus Nedir? Korunma Yolları Nelerdir?", http://www. kom.gov.tr/Tr/KonuDetay.asp?BKey=55&KKey=103,(Erişim Tarihi: 05.11.2010).

Telekomünikasyon İletişim Başkanlığı, (2010a), "Erişim Engelleme İstatistikleri", http://www.guvenliweb.org.tr/istatistikler/files/pdf/ihbar_istatistikleri_01.03.2010. pdf, (Erişim Tarihi: 29.10.2010).

Telekomünikasyon İletişim Başkanlığı, (2010b), "Sıkça Sorulan Sorular" http://www.tib.gov.tr/kat/sss,(Erişim Tarihi: 17.10.2010).

thehacktivist.com, (t.y.), "What Is Hacktivism?", http://www.thehacktivist.com/ whatishacktivism.pdf, (Erişim Tarihi: 22.11.2010)

Tiftikçi, Mehmet, (1999), "Özel Hukuk Ve İnternet", http://inet-tr.org.tr/ inetconf5/tammetin/hukuk.html, (Erişim Tarihi: 27.10.2010).

Toprak, İlhan, (2010), "Kaset Orijinal Çıktı", http://yenisafak.com.tr/Gundem/?i=259244, (Erişim Tarihi: 04.01.2011).

toptenreviews.com, (t.y.), "İnternet Pornography Statistics", http://İnternet-filter-review.toptenreviews.com/İnternet-pornography-statistics.html, (Erişim Tarihi: 29.10.2010).

trutv.com, (t.y.), "The BTK Story", http://www.trutv.com/library/crime/serial _killers/unsolved/btk/25.html, (Erişim Tarihi: 03.01.2011).

Tschabitsche, Heinz, (2010), "What Email Headers Can Tell You About the Origin of Spam", http://email.about.com/cs/spamgeneral/a/spam_headers.htm, (Erişim Tarihi: 16.11.2010).

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

turk.internet.com, (2004), "Online Dolandırıcılık (Phishing) Artıyor", http://www.turk.internet.com/portal/yazigoster.php?yaziid=10920, (Erişim Tarihi: 14.11.2010).

turkcebilgi.com, (t.y.), "Lamer", http://www.turkcebilgi.com/lamer/, (Erişim Tarihi: 22.11.2010).

turkhukuksitesi.com, (2007), "İnternet Üzerinden E-Posta Ve MSN Yoluyla Tehdit Suçu İşlenmesi", http://www.turkhukuksitesi.com/showthread.php?t=11094, (Erişim Tarihi: 23.10.2010).

turkhukuksitesi.com, (2010), "Google'ın Amerikan İstihbarat Örgütü National Security Agency İle İlişkisi", http://www.turkhukuksitesi.com/showthread.php?t=47116, (Erişim Tarihi: 28.10.2010).

Türk Dil Kurumu, (2010), "Genel Ağ", http://tdkterim.gov.tr/bts/?kategori=verilst&kelime=genel+a%F0,(Erişim Tarihi: 27.08.2010).

Türkiye Büyük Millet Meclisi, (2003), "Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesi", http://www.unicankara.org.tr/doc_pdf/sinirasan.doc, (Erişim Tarihi: 12.12.2010).

Türkiye Büyük Millet Meclisi, (2003), "TBMM: Sınıraşan Örgütlü Suçlara Karşı Birleşmiş Milletler Sözleşmesine Ek Kara, Deniz Ve Hava Yoluyla Göçmen Kaçakçılığına Karşı Protokolün Onaylanmasının Uygun Bulunduğuna Dair Kanun", http://www.tbmm.gov.tr/kanunlar/k4803.html, (Erişim Tarihi: 12.12.2010).

Türkiye İstatistik Kurumu (2010), "Adalet İstatistikleri", http://www.tuik.gov.tr /VeriBilgi.do?tb_id=1&ust_id=12, (Erişim Tarihi: 16.12.2010).

Ulusoy, Zebayir, (t.y.), "Bilgisayar Ve İnternetin Çocuklar Üzerindeki Olumsuz Etkileri Ve Alınabilecek Önlemler", http://www.kayram.net/edergi/15/internet.pdf, (Erişim Tarihi: 13.10.2010).

United NationsOffice on Drugs and Crime, (2010), "Item 8 Of The Provisional Agenda: Recent Developments İn The Use Of Science And Technology By Offenders And By Competent Authorities İn Fighting Crime, İncluding The Case Of Cybercrime", http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf, (Erişim Tarihi: 12.12.2010).

United NationsOffice on Drugs and Crime, (t.y.a), "Previous Sessions And Documents Of The Commission On Crime Prevention And Criminal Justice", http://www.unodc.org /unodc/commissions/CCPCJ/session/index.html, (Erişim Tarihi: 12.12.2010).

United NationsOffice on Drugs and Crime, (t.y.b), "United Nations Convention Against Transnational Organized Crime And İts Protocols", http://www.unodc.org/unodc/en/ treaties/CTOC/index.html, (Erişim Tarihi: 12.12:2010).

UNODC – United Nations Office on Drugs and Crime, (2005), "Computer Related Crime", http://www.unis.unvienna.org/pdf/05-82111_E_6_pr_SFS.pdf, (Erişim Tarihi: 06.12.2010).

US Department of Justice – National Instute of Justice, (2001), "Electronic Crime Scene Investigation – A Guide For First Responders", http://www.ncjrs.gov /pdffiles1/nij/187736.pdf, (Erişim Tarihi: 30.11.2010).

US Department of Justice – National Instute of Justice, (2001a), "Electronic Crime Scene Investigation: AnOn-the-Scene Reference for First Responders", http://www.ncjrs.gov/pdffiles1/nij/227050.pdf, (Erişim Tarihi: 01.12.2010).

US Department of Justice – National Instute of Justice, (2001b), "Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors", http://www.ncjrs.gov /pdffiles1/nij/211314.pdf, (Erişim Tarihi: 03.12.2010).

Uzunay, Yusuf ve Bıçakçı, Kemal, (t.y.), "A3D3M: Açık Anahtar Altyapısı Destekli Dijital Delilleri Doğrulama Modeli", http://www.emo.org.tr/ekler/ 4843973f9b66701_ek.pdf, (Erişim Tarihi: 30.11.2010).

Uzunay, Yusuf ve Koçak Mustafa, (2005), "İnternet Üzerinden Çocuk Pornografisi Ve Mücadelede Yaşanan Sıkıntılar", http://nash.ii.metu.edu.tr/~yuzunay/Download /jop05.pdf, (Erişim Tarihi: 20.10.2010).

Uzunay, Yusuf, (2002), "Dijital Delil Araştırma Süreci", http://www. caginpolisi.com.tr/50/14-15-16-17-18.htm, (Erişim Tarihi: 01.12.2010).

Uzunay, Yusuf, (2008), "Olay Yerinden Alınan Dijital Delillerin Hukuki Kabul Edilebilirliğini Arttırmak", http://akademikguvenlik.wordpress.com/2008/07/11/ olay-yerinden-alinan-dijital-delillerin-hukuki-kabul-edilebilirligini-arttirmak/, (Erişim Tarihi: 28.01.2011).

verikurtarma.org, (t.y.), “WIN.CIH (Çernobil) virüsü Hakkında”, http://verikurtarma.org/verikurtarma_cih.htm, (Erişim Tarihi: 12.11.2010).

webopedia.com, (t.y.), “What is a Trojan Horse?”, http://www.webopedia.com/TERM/T/Trojan_horse.html, (Erişim Tarihi: 10.11.2010).

Wiele, Tom Van de, (t.y.), “BCIE Training – ICT Anti-Forensics”, http://www.bcie.be/Documents/BCIE_Training03_ICT_Anti-Forensics_291106_TVdW.pdf, (Erişim Tarihi: 29.01.2011)

wikipedia.org, (2010a), “Adware”, http://en.wikipedia.org/wiki/Adware, (Erişim Tarihi: 11.11.2010)

wikipedia.org, (2010b), “Backdoor (computing)”, http://en.wikipedia.org/wiki/Backdoor_(computing), (Erişim Tarihi: 12.11.2010)

wikipedia.org, (2010c), “Copyright infringement”, http://en.wikipedia.org/wiki/Computer_pirates, (Erişim Tarihi: 20.11.2010)

wikipedia.org, (2010d), “G8”, http://tr.wikipedia.org/wiki/G8, (Erişim Tarihi: 11.12.2010)

wikipedia.org, (2010e), “Kötü Virüs”, http://tr.wikipedia.org/wiki/Kötü_virüs, (Erişim Tarihi: 10.11.2010)

wikipedia.org, (2010f), “Malware”, http://en.wikipedia.org/wiki/Malware, (Erişim Tarihi:05.11.2010)

wikipedia.org, (2010g), “Aktivizm”, http://tr.wikipedia.org/wiki/Aktivizm, (Erişim Tarihi: 22.11.2010)

wikipedia.org, (2010h), “Birleşmiş Milletler”, http://tr.wikipedia.org/wiki/Birle%C5%9Fmi%C5%9F_Milletler, (Erişim Tarihi: 12.12:2010)

wikipedia.org, (2010i), “Ceza Hukuku”, http://tr.wikipedia.org/wiki/Ceza_hukuku, (Erişim Tarihi: 17.10.2010)

wikipedia.org, (2010j), “Ceza Hukuku”, http://tr.wikipedia.org/wiki/Ceza_hukuku, (Erişim Tarihi: 08.12.2010)

wikipedia.org, (2010k), “Dennis Rader”, http://en.wikipedia.org/wiki/Dennis_Rader, (Erişim Tarihi: 03.01.2011)

wikipedia.org, (2010l), "Kevin Mitnick", http://tr.wikipedia.org/wiki/Kevin_Mitnick, (Erişim Tarihi: 16.11.2010)

wikipedia.org, (2010m), "Vulnerability Scanner", http://en.wikipedia.org/wiki/ Vulnerability_scanner, (Erişim Tarihi: 14.11.2010)

wikipedia.org, (2010n), "White Hat", http://en.wikipedia.org/wiki/Ethical_Hacking, (Erişim Tarihi: 20.11.2010)

wikipedia.org, (2010o), "Yemleme", http://tr.wikipedia.org/wiki/Yemleme, (Erişim Tarihi: 14.11.2010)

wikisource.org, (2010), "International Review Of Criminal Policy - Nos. 43 And 44/Regional Action", http://en.wikisource.org/wiki/International_review_of_ criminal_policy_-_Nos._43_and_44/Regional_action, (Erişim Tarihi:11.12.2010)

wisegeek.com, (t.y.a), "What Is Password Cracking?", http://www.wisegeek.com/what-is-password-cracking.htm, (Erişim Tarihi: 14.11.2010)

wisegeek.com, (t.y.b), "What is a Keylogger?", http://www.wisegeek.com/what-is-a-keylogger.htm, (Erişim Tarihi: 16.11.2010)

yahoo.com, (2010), "E-Posta Yardım", http://help.yahoo.com/l/tr/yahoo/mail/about/about-48033.html, (Erişim Tarihi: 13.10.2010)

Yargıtay, (2010), "Ceza Genel Kurulu 2010/11-17 E., 2010/65 K.", http://emsal.yargitay.gov.tr/VeriBankasiIstemciWeb/DokGosterMainServlet?dokumanId=95%203%20ICM8%20ICMNLSDB15%20UYAPVERIBANKASI59%2026%20A1001001A10L20B51211C8408218%20A10L20B51211C840821%2014%201162&aranan=&dokumanTuru=YARGITAYKARARI, (Erişim Tarihi: 02.01.2011)

Yargıtay, (t.y.), "Yargıtay On Birinci Ceza Dairesi", http://www.yargitay.gov.tr /content/view/43/43/, (Erişim Tarihi: 16.12.2010)

Yaycı, Esra, (2007), "*Bilişim Suçları*", Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmış Yüksek Lisans Tezi, Ankara

Yıldız, Sevil, (t.y.), "Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi", http://www.sosyalbil.selcuk.edu.tr/sos_mak/makaleler/Sevil%20YILDIZ/YILDIZ,%20SEV%C4%B0L.pdf, (Erişim Tarihi: 10.12.2010)

Yılmaz, Davut, (2005), *Hacking Bilişim Korsanlığı ve Korunma Yöntemleri*, İstanbul: Hayat Yayınları.

zaman.com.tr, (2009), "Telefonunuzdan Ortam Dinlemesi Yapılıyor Olabilir!", http://www. zaman. com.tr/haber.do?haberno=833402, (Erişim Tarihi: 26.10.2010).