BİLİŞİM SUÇLARI

Ebru ALTUNOK
Milli Eğitim Bakanlığı,
Milli Eğitim Denetçi Yardımcısı

Ali Fatih VURAL
Stajyer Avukat

ÖZET: *Bu yazıda insanlık tarihi açısından düşünüldüğünde geçmişi çokta uzun sayılamayacak ancak gelişim evresi açısından hayatımıza oldukça hızlı bir şekilde giren bilişim kavramı çerçevesinde işlenen suçlar kavramsal açıdan incelenmiş, tarihi gelişimi ve tasnifine yer verilmiştir. Bu konudaki yasal düzenlemelere değinilerek bilişim suçlarına karşı açılabilecek davalar ve bilişim suçları müeyyideleri incelenmeye çalışılmıştır.*

ANAHTAR KELİMELER: *Bilişim, Bilişim Hukuku, Bilişim Suçları, Mukayeseli hukukta bilişim suçları, Etik Korsanlık.*

Giriş

İçinde bulunduğumuz 21. Yüzyılın "Bilgi Çağı" olarak nitelendirilmesinin yanında, bilgi alış verişinin salise-lerle kısıtlanması insanoğlunun bilgiye olan açlığının yanı sıra yaşamını sürdürmesinin tek yolu olarak önümüze çıkmaktadır. Bu çerçevede bilişim teknolojileri insanı şaşırtan boyutlarda büyüyerek örümcek ağı gibi tüm dünyayı kaplamakta, hayatımızın her alanına nüfuz ederek durmaksızın geniş bir konsepte yayılmaktadır.

Artık bilgisayarlar insan hayatının içinde büyük oranında olup bilgisayarsız yapılan bir iş neredeyse kalmamıştır. Ancak bilişim teknolojilerinde son noktaya gelindiğini söylemek, ABD Patent Dairesi Başkanı Charles H. Duell'in 1899'da söylediği iddia edilen "icat edilebilecek her şey icat edildi" cümlesindeki hataya düşmemize sebep olacaktır. Günümüzde insanlar adeta anestezik olarak hayatlarını en ince ayrıntısına kadar siber bir ortama aktarmaktadır. Gelecekte ise her türlü işlemin bilgisayar aracılığıyla yapılması kaçınılmazdır. Bu durum bilgi dünyası ile teknoloji dünyası arasındaki köprüyü kurarak hayatımızı kolaylaştıran bilişim kavramının insan haklarının ihlal edilmesine de zemin hazırlamasını beraberinde getirmektedir. Tarihsel gelişim evresi boyunca bilişim sektöründe meydana gelen marjinal faydası yüksek gelişmeler ve

beraberinde getirdiği sorunlarla ortaya çıkan bilişim suçları kötü niyetli kişilere karşı kullanıcıları koruma amacıyla yasa koyucuları yeni hukuki düzenlemelere gitmeye zorlamış ve yeni bir hukuk dalı oluşturulması zorunluluğunu belki de ortaya çıkartmıştır.

Kavramsal Açıdan Bilişim ve Bilişim Suçları

Türk Dil Kurumu sözlüğünde bilişim, *"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi, enformatik…"* veya *"insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla, düzenli ve ussal biçimde işlenmesi bilimi. Bilgi olgusunu, bilgi saklama, erişim dizgeleri, bilginin işlenmesi, aktarılması ve kullanılması yöntemlerini, toplum ve insanlık yararı gözeterek inceleyen uygulamalı bilim dalı. Disiplinlerarası özellik taşıyan bir öğretim ve hizmet kesimi olan bilişim bilgisayar da içeride olmak üzere, bilişim ve bilgi erişim dizgelerinde kullanılan türlü araçların tasarlanması, geliştirilmesi ve üretilmesiyle ilgili konuları da kapsar. Bundan başka her türlü endüstri üretiminin özdevimli olarak düzenlenmesine ilişkin teknikleri kapsayan özdevin alanına giren birçok konu da, geniş anlamda, bilişimin kapsamı içerisinde yer alır."* şekillerinde ifade edilmektedir.[1]

Aydın tarafından ise bilişim, *"bilginin ve iletişim yapısı özellikleri; bilginin aktarılması, organize edilmesi, saklanılması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir."* şeklinde tanımlanmaktadır.[2]

Milattan önce sayma işlemine yarayan abaküsler ve 1800'lü yıllarda üretilen hesap makinelerinden sonra, 30 ton ağırlığında, 18000 vakum tüpünden oluşan ve bugünkü bilgisayarların atası olan dünyanın ilk sayısal bilgisayarı ENIAC'ın II. Dünya Savaşı sırasında ABD ordusu tarafından geliştirilmesi ile bilişim teknolojileri serüveni başlamıştır.[3] Ticari anlamda satışı yapılan ilk bilgisayar UNIVAC ise 1952 yılında piyasaya sunulmuş, 1960'lı yıllardan sonra ise elektron tüplerinin yerini önce transistörler, daha sonra da yüzlerce transistörün birleşimi olarak tarif edilebilecek entegre devreler almıştır.[4]

1957 yılında Sovyetler Birliği'nin Sputnik uydusunu uzaya göndermesinin ardından ABD ortaya çıkabilecek bir savaş veya karışıklık halinde dünyanın çeşitli yerlerine yerleştirilmiş savaş sistemlerini bir bilgisayar ağı ile yönetme kararı sonucu oluşturulan modelin,[5] 1970'lerde ABD'li mühendisler tarafından geliştirilmesi ile günümüzde bilgisayar ağı olarak bilinen yapının temelleri atılmıştır.

Zaman içerisinde bu bilgisayar ağı, ordu ve akademik birimler ile sınırlı kalmayarak milyonlarca bilgisayar içeren **Bilgisunar** (*Internet* veya *Genel ağ*) oluşmuştur. 1990'larda İsviçre'nin CERN araştırma merkezinde geliştirilen **Küresel ağ** (*World Wide Web*, *WWW*) adlı iletişim kuralları, *e-posta* gibi uygulamalar ve ethernet gibi ucuz donanımsal çözümler ile bilgisayar ağları yaygınlık kazanmıştır. 21. yüzyılda bilgisayarlar bir kol saatine sığacak ve küçük bir pil ile çalışacak duruma gelmiştir. Bilişim teknolojilerindeki değişim, dönüşüm ve gelişimin sınırları günümüzde insanoğlunun sınırsız olan hayal gücüne eşdeğer boyuta ulaşmıştır. Ancak bu gelişim ve dönüşüm bilişim suçları kavramını da beraberinde getirmiştir.

Bilişim suçları konusunda herkesin ittifak ettiği bir tarif yoksa da en geniş kabul gören tarif Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun Mayıs 1983 tarihinde Paris Toplantısı'nda *"Bilgileri otomatik işleme tabi tutan veya verilerin nakline yarayan bir sistemde gayri kanuni, gayri ahlaki veya yetki dışı gerçekleştirilen her türlü davranış"* olarak tanımlanmıştır.[6]

1 http://tdkterim.gov.tr/bts/ Er. Tar. 20/09/2011

2 Aydın, E.(1984). Bilişim Genel Sistemleri ve Sibernetik Terimleri Sözlüğü. S.256. İstanbul: Mistaş-Beytur A.Ş.

3 Aydın, E.(1992). Bilişim Suçları ve Hukukuna Giriş. S.3. Ankara: Doruk Yayınları

4 http://tr.wikipedia.org/wiki/Bilgisayar%C4%B1n_tarih%C3%A7esi, Er.Tar. 20/09/2011

5 Avşar, B. Z. ve Öngören, G.(2009). İnternet Hukuku. Ankara: TOBB Yayınları

6 Özel, C. (2002). Bilişim-İnternet Suçları. Er.Tar.20/09/2011, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

Bilişim alanında işlenen suçların tam ve doğru istatistiklerini elde etmenin zorluğu ve neden olduğu gerçek zararın hesaplanamamasındaki zorluklar ile bu alanda yetişilemeyen gelişme ve genişlemeler bilişim suçlarının kâfi derecede tanımlamasını engellemektedir. Bilişim suçları ile ilgili bir çerçeve çizmek mümkün olmadığı için bu suçlar "çizgisiz çerçeveli suçlar" olarak adlandırılmaktadır. Karagülmez'e göre bilişim suçu, bilişim sistemlerine yönelik veya bilişim sisteminin kullanıldığı suç olarak tanımlanmaktadır.[7]

Dünya bilişim suçları olgusu ile 1960'lı yılların sonunda tanışmıştır. Kişisel verilerin toplu olarak işleme tabi tutulduğu veri bankalarının oluşmasıyla gizliliğe karşı sorunlar ve tehditler başlamış ve ilk olarak bilgisayar manüpülasyonu, sabotaj ve casusluk suçları görülmüştür. 1970'lerde bilişim ağlarının kullanılmaya başlamasıyla hackleme türünden bilgisayar korsanlığı fiilleri, 1980'lerde kişisel bilgisayarın kullanımının yaygınlaşmasıyla program korsanlığı fiilleri artış göstermiştir. Aynı süreçte ATM'lerin bankacılık işlemlerinde kullanılmaya başlanması banka kartları ile ilgili suçları beraberinde getirmiştir. World Wide Web ile birlikte yasal ve yasal olmayan pek çok işlemde hayal bile edilemeyecek hızla kullanılmaya başlanmış, ticari ve kişisel bilgiler başta olmak üzere pek çok değer, dünya genelinde ülke sınırı tanımadan saldırıya açık hedef haline gelmiştir.[8]

Bilişim suçları farklı kaynaklarda bilgisayarın amaç veya araç olması, malvarlığı haklarının ihlali, bilişim sistemleriyle bağlantı, bilgisayar kullanımı, suçu işleyen fail gibi kriterler doğrultusunda farklı tasnif edilmiştir. Bilişim suçlarına ilk olarak rastlanılan ABD doktrininde suçlar 12 başlık halinde incelenmiştir. Bunlar;[9]

1. Verilere veya hizmetlere karşı gerçekleştirilen hırsızlıklar
2. Mülkiyete karşı hırsızlıklar
3. Giriş İhlalleri
4. Veri sahtekârlığı
5. Şahıslardan kaynaklanan hatalar(İnsan hataları neticesi oluşan ihlaller)
6. Gasp
7. Sır aleyhine ihlaller
8. Sabotajlar
9. Maddi kısımlara yönelik hırsızlıklar
10. Vakalarda gerçekleştirilen sahtekârlıklar
11. Bankamatik(ATM) kartları konusundaki hırsızlıklar
12. Manyetik kartların şifreleri hususunda gerçekleştirilen eylemler

Avrupa Birliği İle Birleşmiş Milletler Komisyonu ortak raporunda ise 6 ana bölümde incelenmiştir. Bunlar;[10]

1. Bilgisayar Sistemleri ve Servislerine Yetkisiz Erişim ve Dinleme

Bilgisayar sistemine erişim, bilgisayar sisteminin tamamına veya bir bölümüne, bu eylem için hazırlanmış programlar, çeşitli virüs programları, gizli yazılımlar yolu ile ulaşılmasıdır. Kişilerin özel hayatının gizliliğinin korunması çerçevesinde, dinleme, izin alınmaksızın kişisel veya şirket bilgisayarına erişimin Türk Ceza Kanunu'nun Bilişim Alanında Suçlar Başlığı altındaki 243. maddesinde suç olduğu belirtilmiştir.

2. Bilgisayarların Sabote Edilmesi

Bilgisayar içerisinde yer alan bilgilerin, sistem içerisine izinsiz girilerek silinmesi değiştirilmesi ve yok edilmesidir. Bilgisayarın sabote edilmesi, teknolojik imkânlardan faydalanmak suretiyle uzaktan sisteme erişilerek yapılabileceği gibi, fiili olarak bilgisayar başında da yapılabilmektedir. Bilgisayarın Sabote Edilmesi Türk Ceza Kanunu'nun 243/ 3 maddesi ve 244/1 ve 2 maddelerinde tanımlanmış ve müeyyide altına alınmıştır. Ancak bilgisayar virüsleri, solucanlar ve zombi programları Türk Ceza Kanunu tarafından suç olarak sayılmamıştır.

3. Bilgisayar Kullanılarak Dolandırıcılık

Kişilerin bilgisayar veya teknolojik araçlar kullanılmak marifetiyle aldatılması, kandırılması veya şaşırtılmasıdır. Türk Ceza Kanunu'nda yer alan şekli ile dolandırıcılık "Hileli davranışlarla bir kimseyi aldatıp,

7 Karagülmez, A.(2010). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri. S.40. İstanbul: Seçkin Yayınları

8 Karagülmez, A.(2010). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri. S.41. İstanbul: Seçkin Yayınları

9 Avşar, B. Z. ve Öngören, G.(2009). İnternet Hukuku. S.96. Ankara: TOBB Yayınları

10 Şener,K. http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-nelerdir.html Er.Tar. 20/09/2011

onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaktır" Kredi kartlarının kopyalanması, Bilgisayardan izinsiz olarak elde edilen verilerin kopyalarının oluşturulması, bu bilgi ve kopyaların kullanılarak hesaplardan para aktarımı, bu bilgiler ile üçüncü kişiler ile iletişim kurularak onları kandırmak örnek olarak verilebilir. Türk Ceza Kanunu bu tip suçları 158/1 fıkrası f bendi, 244/3 fıkrası ve 245/1 fıkrasında hüküm ve müeyyide altına almıştır.

4. Bilgisayar Kullanılarak Sahtecilik

Sahtecilik genel anlamıyla, bir şeyin aslına benzetilmesi yoluyla kişilerin kandırılmasıdır.

Bir web sitesinin benzerinin yapılması veya başka kişilerin adına web sitesi hazırlanarak diğer kişilere buradan mesajlar göndermek ,iletişim kurulmasını sağlamak , sahte mail (fakemail) ve Phishing yöntemleri ile kişilerin özel bilgilerini elde etmek , sahte olarak evrak oluşturmak , sahte bilet satmak vb.. bilgisayar kullanılarak sahtecilik yapılmasına örnek verilebilir. Türk Ceza Kanunu'nda bu suçlara ilişkin net tanım mevcut olmasa da 158/f bendi bu suçlarda uygulama alanı bulacaktır.

5. Kanun Tarafından Korunan Bir Yazılımın İzin Alınmadan Kullanılması

Fikir ve Sanat Eserleri Kanunu tarafından koruma altına alınmış bir yazılımın sahibinin izni dışında kopyalanması, çoğaltılması, satılması, dağıtılması ve kullanılması yasaktır. Fikir ve Sanat Eserleri Kanunu bir yazılımı yasal yollardan satın alan kişiye, bu yazılımın yedekleme amaçlı olarak 1 adet kopyasını alma hakkı vermektedir. Yazılımın bir adetten fazla kopyasının alınması, yazılımın kiralanması, satılması yasaktır.

6. Yasaya Aykırı Yayınlar

Yasadışı yayınların internet üzerinde veya bilgisayar sistemleri üzerinde, web siteleri, e-mail, forum ve benzeri teknolojik iletişimde kullanılan her türlü araç ile topluma iletilmesi ve vatanın bölünmez bütünlüğüne karşı hazırlanmış web siteleri, toplum ahlakına aykırı içerikler, kişi veya kurumlara karşı yapılan sövme ve hakaret içerikli yayınlar suç teşkil etmektedir.

Avrupa Ekonomik Topluluğu ise bir tavsiye kararında bu suçları beşe ayırmıştır.[11] Bunlar sırası ile;

1. Bilgisayarda mevcut olan kaynağa veya herhangi bir değere gayri meşru şekilde ulaşarak transferini sağlamak için kasten bilgisayar verilerine girmek, bunları bozmak, silmek, yok etmek,
2. Bir sahtekârlık yapmak için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,
3. Bilgisayar sistemlerinin çalışmasını engellemek için kasten bilgisayar verilerine veya programlarına girmek, bozmak, silmek, yok etmek,
4. Ticari manada yararlanmak amacı ile bir bilgisayar programının yasal sahibinin haklarını zarara uğratmak,
5. Bilgisayar sistemi sorumlusunun izni olmaksızın, konulmuş olan emniyet tedbirlerini aşmak sureti ile sisteme kasten girerek müdahalede bulunmaktır.

Birleşmiş Milletler 10. Kongresinde ise bilişim suçları siber suçlar başlığı altında, dar anlamda ve geniş anlamda siber suçlar olmak üzere iki alt başlıkta değerlendirilmiştir. Dar anlamıyla siber suçlar; yetkisiz ve izinsiz erişim(Hacking), verilere yönelik suçlar, bilişim ağlarına yönelik suçlar, sanal tecavüz olarak kategorilendirilmiştir. Geniş anlamda ise; bilişim ortamında cinayet, tehdit ve şantaj, hakaret ve sövme, taciz ve sabotaj, pornografi, röntgencilik, manüpilasyon, dolandırıcılık, hırsızlık, sahtekârlık, sanal/siber terör maddeleriyle ele alınmıştır.[12]

Bilişim suçlarının işlendiği en önemli alan olan internetin gelişimiyle, özel hayatın gizliliğinin korunması kapsamında "veri mahremiyeti" ya da diğer bir ifadeyle "enformasyon mahremiyeti "ne karşılık gelen, özel hayatın gizliliğin korunmasının bir yönü olarak karşımıza çıkan kişisel verilerin korunması da oldukça güçleşmiştir.[13]

11 Özel, C. (2002). Bilişim-İnternet Suçları. Er.Tar.20/09/2011, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

12 Avşar, B. Z. ve Öngören, G.(2009). İnternet Hukuku. S.96. Ankara: TOBB Yayınları

13 Ketizmen M.(2008). Türk Ceza Hukukunda Bilişim Suçları. S.193 Ankara: Adalet Yayınları

"Bilişim suçlarının işlendiği en önemli alan olan internetin gelişimiyle, özel hayatın gizliliğinin korunması kapsamında "veri mahremiyeti" ya da diğer bir ifadeyle "enformasyon mahremiyeti"ne karşılık gelen, özel hayatın gizliliğin korunmasının bir yönü olarak karşımıza çıkan kişisel verilerin korunması da oldukça güçleşmiştir"

Ayrıca, Elektronik Ticaret kapsamında internet üzerinden, bilgisayar desteği ve telekomünikasyon teknolojisi kullanılarak mal satılması ve hizmet sunulması, ürünlerin ve hizmetlerin tanıtılması ve bunların ticari amaçlarla piyasaya arz edilmesi, satışların yapılması ve satış bedellerinin tahsil edilmesi de bu alanı suça açık hale getirmiştir.[14] İnternet yoluyla girişilen ilişkilerde sözleşmenin kurulması elektronik imza haricinde şekil serbestîsi olduğu sürece mümkün olup yazılı şekle tabi sözleşmeler elektronik imza yoluyla yapılabilmektedir. 5070 sayılı Elektronik İmza Kanununda "*Başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri"* şeklinde tanımlanmakta, 5.maddesinde *"Güvenli elektronik imza, elle atılan imza ile aynı hukuki sonucu doğurur*" denilmektedir. Bu kanunda elektronik imza kapsamında ele alınan suçlar ise imza oluşturma verilerinin izinsiz kullanımı suçu, elektronik sertifikalarda sahtekârlık suçu, idari suçlar şeklindedir.[15]

Bilişim suçları değişik şekillerde işlenebilir. Hakim Kurt'a göre bilişim suçlarının işlenme şekilleri aşağıdaki gibidir.[16]

14 Avşar, B. Z. ve Öngören, G.(2010). Bilişim Hukuku. S.180 İstanbul : Türkiye Bankalar Birliği Yayınları

15 http://www.mevzuat.adalet.gov.tr/html/1328.html, Er. Tar. 20/09/2011

16 Kurt, L.(2005). Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. S.60-77 İstanbul: Seçkin Yayınları

1) Çöpe Dalma (Scavenging)

Çöplenme veya atık toplama olarak adlandırılan yöntem, bilişim sisteminde gerçekleştirilen veri-işlem sonunda kalan bilgilerin depolanmasıdır. Bu bilgiler öncelikle, çıktı birimlerince üretilen ve daha sonra çöpe atılan kâğıt, mürekkep şeridi gibi malzemeler üzerinde kalan bilgilerin toplanmasıyla elde edilmektedir. Diğer bir teknik ise bilişim sisteminin belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgileri, gelişmiş yöntemlerle tekrar geri getirmektedir.

2) Gizlice Dinleme (Eavesdropping):

Bilişim sistemlerinin veri taşımada kullandığı ağlara girilerek veya bilişim sistemlerinin yaydığı elektromanyetik dalgaların yakalanarak verilerin elde edilmesi yöntemidir.

3) Veri Aldatmacası (Data Diddling):

Veri sistemlerine veri girilirken yanlış veriler girilmesi veya girildikten sonra değiştirilmesidir. Bilişim suçları alanında uygulanan basit, güvenli ve yaygın bir suç tekniğidir. Veri aldatmacası, bilişim sistemlerine verilerin girilmesi sırasında müdahaleler, verilerin değiştirilmesi sırasında yapılan müdahaleler, bilginin alınması sırasında yapılan müdahaleler olarak gruplandırılabilir.

4) Truva Atı (Troyan Horse):

Truva atı, görünüşte yararlı bir işlevi yerine getirdiği düşünülen ancak bunun dışında bilişim sistemine zarar verecek gizli kod da içeren bir programdır. Genellikle internette ücretsiz yazılım sağlayan web sitelerinde ya da elektronik posta yoluyla kullanıcılara ulaştırılmaktadır. Truva atı; sisteme bulaştıktan sonra, sistemin açılması ile beraber kendisini belleğe yükler ve sistem ağlarının açıklarını kullanarak, programı yerleştiren tarafın isteklerine cevap verir.

5) Tarama (Scanning):

Değeri her seferinde, sıralı bir diziyi takip ederek değişen verilerin, hızlı bir biçimde bilişim sistemlerine girilmek suretiyle, sistemin olumlu cevap verdiği durumların raporlanması için yapılan işlemlerdir.

6) Süper Darbe (Super Zapping):

Süper Darbe yazılımları, bütün güvenlik kontrollerini atlatarak sisteme müdahale eden programlardır.

7) Salam Tekniği (Salami Techniques):

Bu teknik çok fazla sayıda kaynaktan, çok az sayıda değerlerin transferini esas alır. Genel olarak, tekniğin uygulanmasında Truva atı programları kullanılır. Bu yöntem özellikle bankacılık alanında kullanılmaktadır.

8) Gizli Kapılar (Trap Doors):

İşletim sistemleri normal şartlar altında yetkisiz şekilde girişe veya herhangi bir program ya da kod çalıştırmasına ve değiştirilmesine izin vermeyecek şekilde tasarlanmaktadır. İşletim sistemlerini ve programları hazırlayan programcılar, ilerde ortaya çıkabilecek durumlara karşı hatta bulma amacıyla kod ekleyebilmek veya ara program çıktısı alabilmek amacıyla programa istediğinde "trap doors" adı verilen durma mekanizmaları eklerler. Bu gizli kapıların program ve işletim sistemi tamamlandığında temizlenmesi gerekir. Ancak bazı durumlarda hata sonucu olarak ya da ileride kullanılmak amacıyla gizli kapılar kapatılmaz. Bu durumlarda gizli kötü niyetli kişiler tarafından kullanılabilmektedir.

9) Eşzamansız Saldırılar (Asynchronous Attacks):

Bilgisayarın aynı anda birden fazla işlemi yürütmesine eşzamanlı çalışma denmektedir. Bilgisayar belirli durumlarda eşzamanlı çalışma yerine işlemleri belirli sırada yürüterek, bir işlemin başlamasını diğer bir işlemin sonucuna göre belirlemesine ise eşzamansız çalışma adı verilmektedir.

10) Ağ Solucanları (Network Worms) :

Ağ solucanları, herhangi bir kullanıcı müdahalesine ihtiyaç duymadan kendi kendini çalıştırabilen ve kendisi bir kopyasını ağa bağlı olan diğer bilişim sistemlerine de kopyalayabilen bir programdır. Ağ solucanları çoğunlukla bilgisayar virüsleri ile karıştırılmaktadır. Fakat ağ solucanları, bilgisayar virüsleri gibi sisteme zarar verme zorunluluğu olmadan da sistemin içinde dolaşabilmektedir.

Ağ solucanları bilişim ağında ulaştıkları bir sistemin güvenlik duvarıyla karşılaştıklarında, tahmin edilmesi kolay şifreleri ve verileri kullanarak, genellikle kullanılan şifrelerden oluşan bir sözlükten anahtarları deneyerek, duvarı aşmaya çalışmakta ve iyi oluşturulmamış güvenlik duvarlarını aşarak sistemlere girerek eylemlerine başlamaktadırlar.

11) Bilgisayar Virüsleri:

Bilgisayar virüsleri işletim sisteminin ve makine dilinin verdiği olanaklar kullanılarak yazılan, kendi kendisini çoğaltabilen, kopyalarını çeşitli yöntemlerle başka bilişim sistemlerine ulaştırarak bu sistemleri de etkileyebilen yazılımlardır.

12) Sırtlama (Pıggybacking):

Fiziksel ya da elektronik yollarla kullanılmasıyla bilişim sistemlerine yetkisiz olarak girme tekniğidir.

13) İstem Dışı Alınan Elektronik İletiler (Spam):

Spam teknik olarak, internet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi olarak ifade edilebilmektedir.

14) Mantık Bombaları (Logic Bombs):

Mantık bombaları, bilişim sistemlerinde veya ağlarında, daha önceden belirlenmiş özel durumların gerçekleşmesi durumunda zarar verici sonuçlar yaratan programlardır.

15) Yerine Geçme (Masquerading):

Yetkisi olmayan veya sınırlı erişim yetkisi olan bir kişinin, parola veya erişim kodunun yazılması veya ona özgü niteliklerin taklit edilmesi şeklinde yapılmasına denmektedir.

16) Kredi Kartı Sahtekârlıkları

Elektronik ortamda kredi kartı sahtekarlığında; sahte müracaat, sahte kart, hacking, fishing, web link, wireless network hırsızlığı gibi yöntemler kullanılmaktadır.

16) Diğer

Tavşanlar, Bukalemun, Sahte İleti(Fake Mail), Yazılım Bombaları, Kurtlar, Bug Ware gibi yöntemlerde bilişim suçları işlenme şekilleri arasında sayılmaktadır.

5237 Sayılı Türk Ceza Kanununda Bilişim Suçları:

Türk Hukukunda Bilişim suçları yönüyle diğer ülkelerden farklı bir yol izlenmemiş, ayrı bir kanuni düzenleme yapılmamış, ancak temel ceza kanunu içinde ele alınmıştır. Türk Ceza Kanununda bilişim suçlarına aşağıdaki maddelerde yer verilmiştir;[17]

- 135. Madde: "Kişisel verilerin kaydedilmesi suçu"
- 136. ve 137. Maddeleri: "Kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu"
- 138. Madde: "Verileri yok etme suçu"
- 243. Madde: "Hukuka aykırı olarak bilişim sistemine girme ve sistemde kalmaya devam etme suçu"
- 244. Madde: "Sistemi engelleme, bozma, verileri yok etme veya değiştirme"
- 245. Madde: "Banka veya kredi kartlarının kötüye kullanılması"

Bunların dışında TCK'da bilişim sistemleri aracılığı ile işlenebilecek ancak salt bilişim suçu nitelendirilemeyecek suçlar da mevcuttur[18]. Bunlar:

- 81. ve 82. Maddeleri: "Kasten Öldürme Suçu "
- 84. Madde: "İntihara azmettirme"
- 86. ve 87. Maddeleri: "Kasten yaralama"
- 91. Madde: "Organ ve doku ticareti"
- 96. Madde: "Eziyet suçu"
- 105. Madde: "Cinsel taciz"
- 106. Madde: "Tehdit"
- 107. Madde: "Şantaj"
- 123. Madde: "Kişilerin huzur ve sükununu bozma suçu"
- 124. Madde: "Haberleşmenin engellenmesi"
- 125. Madde: "Hakaret suçu"
- 132. Madde: "Haberleşmenin gizliliğini ihlal suçu"
- 133. Madde: "Kişisel konuşmaların dinlenmesi ve kayda alınması suçu"
- 134. madde "Özel hayatın gizliliğini ihlal suçu"
- 142. Madde: 2.fıkrası e bendi "Bilişim sistemlerinin kullanılması süretiyle nitelikli hırsızlık"
- 148. ve 149. Maddeleri: "Yağma suçu"
- 157. ve 158. Maddeleri: "Dolandırıcılık"
- 170. Madde: "Genel güvenliğin kasten tehlikeye sokulması"
- 179. Madde: "Trafik güvenliğini tehlikeye sokma"
- 213. Madde: "Halk arasında korku ve panik yaratmak amacıyla tehdit"
- 214. Madde: "Suç işlemeye tahrik"
- 215. Madde: "Suçu ve suçluyu övme"
- 216. Madde: "Halkı kin ve düşmanlığa tahrik ve aşağılama"
- 217. Madde: " Kanunlara uymamaya tahrik"
- 225. Madde: "Hayasızca hareketler"
- 226. Madde: "Müstehcenlik"
- 227. Madde: "Fuhuş"
- 228. Madde: "Kumar oynanmadı için yer ve imkan sağlama"
- 237. Madde: "Fiyatları etkileme"
- 239. Madde: "Ticarî sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması "
- 258. Madde: "Göreve ilişkin sırrın açıklanması"
- 267. Madde: "İftira"
- 271. Madde: "Suç uydurma"
- 281. Madde: "Suç delillerini yok etme, gizleme veya değiştirme"
- 282. Madde: "Suçtan kaynaklanan malvarlığı değerlerini aklama"
- 285. Madde: "Gizliliğin ihlali"
- 286. Madde: "Ses veya görüntülerin kayda alınması"
- 288. Madde: "Adil yargılamayı etkilemeye teşebbüs"
- 299. Madde: "Cumhurbaşkanına hakaret"
- 300. Madde: "Devletin egemenlik alametlerini aşağılama"
- 301. Madde: "Türklüğü, Cumhuriyeti, Devletin kurum ve organlarını aşağılama "
- 304. Madde: "Devlete karşı savaşa tahrik"
- 318. Madde: "Halkı askerlikten soğutma"
- 319. Madde: "Askerleri itaatsizliğe teşvik"
- 323. Madde: "Savaşta yalan haber yayma"
- 327. Madde: "Devletin güvenliğine ilişkin bilgileri temin etme"

17 http://www.tbmm.gov.tr/kanunlar/k5237.html, Er. Tar. 20/09/2011

18 Ergin,İ. (2005). Polis Bilişim Sempozyumu Bildiriler "Yeni Türk Ceza Kanunu'nda Bilişim Suçları". S.23-29. Ankara: EGM Yay.

- 329. Madde: “Devletin güvenliğine ilişkin bilgileri temin etme”
- 330. Madde: “Gizli kalması gereken bilgileri açıklama “
- 331. Madde: “Uluslararası casusluk”
- 334. Madde: “Yasaklanan bilgileri temin”
- 335. Madde: “Yasaklanan bilgilerin casusluk maksadıyla temini”
- 336. Madde: “Yasaklanan bilgilerin casusluk maksadıyla temini”
- 337. Madde: “Yasaklanan bilgileri siyasal veya askerî casusluk maksadıyla açıklama”
- 340. Madde: “Yabancı devlet başkanına karşı suç”
- 342. Madde: “Yabancı devlet temsilcilerine karşı suç”

Bilişim Suçları İle ilgili Yasal Düzenlemeler

Bilişim suçlarının niteliği, hızlı işlenebilmesi, uluslararası sonuçlar doğurması bu suçlarla ilgili yasal düzenlemeleri yapma ihtiyacını ortaya çıkarmıştır. Bilgisayarın vatanı olan ABD’de ilk düzenleme yapılmış ve “Bilgisayar ve Hukuk”(Compiters and the Law) adıyla ayrı bir dal olarak ele alınmıştır. Bilişim suçları ile ilgili yapılan düzenlemelerde iki yöntem ön plana çıkmaktadır. Birinci yöntemde bilişim suçları ayrı bir kanunla özel olarak düzenlenmektedir. ABD’nin de dâhil olduğu Anglo Sakson hukuk sisteminde bu yol izlenmiştir. İkinci yöntemde ise ayrı bir düzenlemeye gidilmeyip mevcut düzenlemelerle konu incelenmeye çalışılmıştır. Bu guruptaki ülkelerden bazıları mevcut düzenlemeler içinde ayrı bir bölümde bilişim suçlarını düzenlerken, bazıları ise mevcut yasalar içerisinde ancak hangi hukuki yarar ihlal edildi ise bu hukuki yararı ihlal eden suçun düzenlendiği bölümde incelenmiştir. Şili, Danimarka, Fransa, Yunanistan, İngiltere, İtalya, Japonya, Kanada, Avusturya, İsveç, Norveç gibi ülkeler Mevcut ceza yazası içerisinde yer alan bir bölüm halinde düzenleme yapan ülkeler arasında olup bunların başında Fransa gelmektedir. Türk Ceza Kanununda da Fransız ceza mevzuatının etkisinde kalınarak böyle bir düzenleme yoluna gidilmiştir. Bazı ülkelerde ise mevcut ceza kanununda değişiklik yapılarak bilişim suçuyla ilgili düzenleme yapılmaktadır. Örneğin Alman ceza hukukunda “mala karşı işlenen suçlarda” düzenlenen maddesinin nitelikli hali bilgisayarla girilmek suretiyle mevcut programların bozulması olarak verilmiştir. Sahtecilik, Dolandırıcılık ve Hırsızlık suçları içinde aynı şeyler söylenebilmektedir. Federal sistemle yönetilen ABD’de bilişim suçlarıyla ilgili her eyalette farklı bir düzenleme olduğu gibi tüm ülkeyi kapsayan düzenlemeler de bulunmaktadır. İlk Federal Kanun 1984 tarihli “ Bilgisayar Sahtekârlığı ve Bilgisayarların Kötüye Kullanılması Kanunu” ‘dur. Bu kanundaki düzenlenen suç tipleri;[19]

- Atom enerjisi, savunma veya dış politika konularında gizli belgeleri elde etmek ve bunları ABD aleyhine veya başka ülke yararına kullanmak amacıyla yetkisiz olarak bilgisayarlara girme eylemi,
- Finansal bilgiler elde etmek amacıyla gayri meşru surette bilgisayarlara girilmesi veya bunların kullanılması
- Hükümet tarafından kullanılan bilgisayarlardaki bilgilerin tahribi, değiştirilmesi veya yok edilmesidir.

Bilişim Suçlarına Karşı Açılabilecek Hukuki Davalar

Bilişim suçu kapsamında yapılan saldırılara ve hak ihlallerine karşı gerek savcılığa şikâyette bulunup ceza davası gerekse hukuk davası açılabilmektedir. Medeni Kanun’un 24. ve 25. maddeleri ile Borçlar Kanunu’nun 48. ve 49. maddeleri, her tür yayınlardan dolayı zarara uğrayan kişileri çeşitli hukuk davaları ile bu saldırıya karşı korumaktadır.[20]

Bu davalar:

Yasaklama ve Önleme Davası:

Bu dava, henüz olmayan, fakat yakında yapılacak saldırılar için açılmaktadır. Önleme davasına çok benzeyen diğer mücadele “ihtiyati tedbir” olayıdır. HUMK 103. Maddesi’ne göre, geciktirilmesinde tehlike olan veya önemli zarar doğacağı anlaşılan hallerde, yargıç, tehlike ve zararı önlemek için gereken tedbirlere karar verebilmektedir. Yasaklama ve önleme davasının açılması için haksız bir saldırı konusunda belirtiler

19 Kurt, L.(2005). Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması. S.87-94 İstanbul: Seçkin Yayınları

20 Avşar, B. Z. ve Öngören, G.(2010). Bilişim Hukuku. S.303-313 İstanbul : Türkiye Bankalar Birliği Yayınları

bulunması yeterli olup, ayrıca saldırıda bulunmaya hazırlanan kişinin kusurlu olması aranmamaktadır. İnternette bir sitenin yakında A şirketinin gerçeğe aykırı biçimde çevreyi kirleteceği veya B bankasının hesaplarına girmek için şifre kırıcının dağıtılacağı duyurusuna karşı bu dava açılarak gerekli önlemlerin alınması mahkemeden istenebilmektedir.

Kaldırma Davası

Bu dava, mali ve kişilik haklarına yönelmiş ve sürmekte olan saldırılara karşı açılmaktadır. Bu davanın açılabilmesi için, internette yapılan yayın veya iletilen mesajlardaki saldırının haksız olması yeterlidir. Ayrıca saldırganın kusuru gerekmez. Hatta bir zarar meydana gelmese bile salt haksız saldırının varlığı karşısında bu dava açılabilir. Zarar meydana gelmişse de davacı hem saldırının kaldırılmasını hem de maddi ve manevi tazminatta isteyebilir. Eğer saldırı kalktıktan sonra zarar ortaya çıkmışsa, bu zararın giderilmesi ayrı bir tazminat davasıyla istenebilir.

Tespit Davası

Tespit ya da saptama davası, haksız bir yayının ve açıklamanın yapılmış, yapılmakta ya da yapılacak olduğunu belirleme amacıyla açılır. Bu davada sadece, hukuka aykırı bir saldırının saptanması istenir. Örneğin; mahkeme A sitesindeki B şahıslı kişi hakkında yazılan haber gerçeklere aykırı mıdır değil midir diye tespit eder. Ayrıca tespit kararının yayın organlarında ilan edilmesini de isteyebilir.

Esasen, bu davanın uygulamada çok önemi yoktur. Çünkü kişilik hakkına yapılan saldırıya yönelik olarak açılan öteki davalarda, az çok bir tespit kısmı bulunmaktadır. Önleme, kaldırma ve tazminat davalarında, yargıcın her şeyden önce haksız bir saldırının bulunup bulunmadığını saptanması gerekir ki, maddi veya manevi tazminat verilsin, saldırı yasaklansın. Bu davanın sonucu, aynı anda verilecek kararın ilanı ya da üçüncü kişilere bildirilmesi isteğini içeriyorsa işe yarayabilecektir.

Maddi Tazminat Davası

Bu dava parayla ölçülebilen zararı giderme amacı güder. Bu davanın şartları, haksız bir saldırı bulunulması, saldırıda bulunanın kusurlu olması, saldırı dolayısıyla parayla ölçülebilen bir zararın doğması, zararla saldırı arasında illiyet bağının bulunması olarak sayılır.

Manevi Tazminat Davası

Manevi hakları; internet yayınları veya mesajları yoluyla saldırıya ve zarara uğrayan kişi, uğradığı manevi zararı azaltmak için Medeni Kanun'un 25. maddesi ve Borçlar Kanunu'nun 49. maddesinde ifade olunan manevi tazminat davasını açabilir. Manevi zarar daha çok kişinin manevi acılar duyma, ağır bir ruhsal sarsıntı geçirme, yaşama sevincini yitirme, toplum içine çıkamayacak derecede utanç duyma gibi farklı şekillerde karşımıza çıkar. Manevi tazminat olarak ödenecek paranın tutarını, takdir yetkisine dayanarak hakim belirler.

Kınama ve Kararın Yayını Davası

Bu davanın dayanağı Borçlar Kanunu'nun 49. maddesindeki "Hakim, bu manevi tazminatın ödenmesi yerine, diğer bir tazmin sureti ikame veya ilave edilebileceği gibi, tecavüzü kınayan bir karar vermekle yetinebilir ve bu kararın basın yolu ile ilanına da hükmedilir" düzenlemesidir. Burada mahkeme iki yoldan birini seçebilir. Ya maddi ve manevi tazminat artı diğer bir tazmin şekli kararı verir ya da maddi ve manevi tazminat vermeyip, kınama artı kararın bir iletişim organında ilanına karar verir.

Bilişim Suçlarının Müeyyidesi:

TCK'da veri, program veya diğer herhangi bir unsuru ele geçirme, program veya diğer herhangi bir unsuru ele geçirme cürmü için TCK'da hem hürriyeti bağlayıcı ceza, hem de para cezası öngörülmüştür. Bilişim Alanında Suçlar başlığı altında aşağıdaki müeyyideler yer almaktadır.[21]

Bilişim sistemine girme

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.

21 http://www.tbmm.gov.tr/kanunlar/k5237.html, Er.Tar. 20/09/2011

(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.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

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 beşbin güne kadar adlî para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

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

(2) 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 yedi yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246. - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Madde metninde hürriyeti bağlayıcı cezanın alt sınırı bir yıl, üst sınırı üç yıl olarak belirtilmiştir. Mukayeseli hukukta hürriyeti bağlayıcı cezaların süresi bakımından değişik uygulamalar göze çarpmaktadır. Örneğin; Yeni Fransız Ceza Kanununda(m.323-1) bir yılı aşmayacak şekilde, Avustralya Ceza Kanununda (m. 76B-1) 6 ay, Belçika Ceza Kanununda (550-b) 3 aydan 1yıla kadar, Danimarka Ceza Kanununda (m.263) 6 ayı aşmayacak şekilde, Yunan Ceza Kanununda (370C-2) 3 aya kadar, Polonya Ceza Kanununda (m.267) 2 yıla kadar olacak şekilde çeşitli cezalar düzenlenmiştir.[22]

Etik Korsanlık (Ethical Hacher) Kavramı

Bilişim suçlarındaki korkunç artış, bilişim sistemlerini kullanan kurum ve kuruluşları yeni güvenlik arayışlarına itmiştir. Bilişim sistem güvenliğinin test edilmesi, yoklanması ve kontrol edilmesinin gündeme gelmesi ise Ethical Hacher kavramını ortaya çıkarmıştır.

Bu konudaki ilk örnek; Amerikan Hava Kuvvetleri bilişim suçları araştırması ünitesi yöneticisi James Christy'nin askeri bilişim sistemlerinin güvenliğini test etmek için bir hacker takımı yerleştirmesidir. Bu takımın 15 saniyede Pentangon'un erişimi yasak olan bilişim sistemine girdikleri rapor edilmiştir. Birçok şirket ve kamu kurumları kendi bilişim sistemlerini test etmek için bu yolu kullanmaktadır. Daha önce bilişim korsanlığı yapmış suçluların hacker olarak kullanılması daha başarılı kontrol edilmesini sağlamaktadır. Bu çerçevede ABD de "Digital Millennium Copyright Act "adlı kanununda Ethical Hacher ile ilgili düzenlenme yapılmıştır. Kanunun 1201. maddesiyle koşullarına uygun olarak yapılabilecek Ethical Hacher testi bir bakıma yasal statüye bağlanmıştır. Türk Ceza Kanunda ise bilişim sistemlerini tahrip resen takibi gerektiren suçlardandır. Ancak, kişinin test etme fiilinde, suçun unsurları bakımından suç oluşmaz şeklinde nitelemeler yapılabilse de bu yaklaşım tarzı yüzeysel kalacaktır[23]

22 Yenidünya, A.C. ve Değirmenci, O. (2002). Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları. S.82-83 İstanbul: Legal Yay.

23 Karagülmez, A.(2010). Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri. S.74-80. İstanbul: Seçkin Yayınları

Sonuç:

Bilişim teknolojilerinde faydalı olduğu kadar suç teşkil edebilecek unsurları da beraberinde getiren inkâr edilemez bir gelişim ve değişim söz konusudur. Bilişim suçları üzerine yapılacak araştırmaların hiçbiri, bilişimdeki hızlı gelişim düşünüldüğünde bilişim suçlarını yeterince kapsamayacaktır. Günümüzde bilişim teknolojik bir devrim olma niteliği yanında suçla da birlikte anılan bir kavram haline gelmiştir.

Bu çerçevede değerlendirildiğinde;

- Bilişim suçlarının yasa koyucular tarafından kapsamlı bir şekilde ele alınmasının gereği kaçınılmaz hale gelmiştir.
- II. Dünya Savaşından sonra hızlı bir şekilde hayatımızın içine giren bu "yeni "dünya" düzeninde yasa koyucu ve uygulayıcılarının toplumun belirli dinamiklerini korumak sürdürmek zorundadır. Bu durum beraberinde yeni düzenleme ve uygulamaların ve belirli müeyyidelerin gerekliliğine yol açmıştır.
- Bilişim alanında oluşturulacak yeni düzenlemelerin insan ve toplumların hak ve özgürlüklerini koruyucu bir biçimde sürdürülebilirlik ilkeleri esaslarına dayanarak düzenlenmeleri ve evrenselleştirmeleri gerekmektedir.
- Dünya çapında bir standart oluşturulması gerekliliği ütopik olarak değerlendirilemeyecektir.
- Bilişim sistemlerinin suç doğuran yapısı ve suçu tetikleyici özelliğinin önüne geçmek için yasal tedbir ve uygulamalara ihtiyaç vardır.
- Bilişim suçlarına karşı yeni yaklaşımlarla önleyici, tedbir alıcı ve koruyucu uygulamaların yasa koyucularca hüküm altına alınması zorunluluktur.

Kaynaklar:

Aydın, E.(1984). **Bilişim Genel Sistemleri ve Sibernetik Terimleri Sözlüğü.** S.256. İstanbul: Mistaş-Beytur A.Ş.

Aydın, E.(1992). **Bilişim Suçları ve Hukukuna Giriş.** S.3. Ankara: Doruk Yayınları

Avşar, B. Z. ve Öngören, G.(2010). **Bilişim Hukuku**. S.180 İstanbul : Türkiye Bankalar Birliği Yayınları

Avşar, B. Z. ve Öngören, G.(2009). **İnternet Hukuku**. Ankara: TOBB Yayınları

Ergin,İ. (2005). **Polis Bilişim Sempozyumu Bildiriler "Yeni Türk Ceza Kanunu'nda Bilişim Suçları".** S.23-29. Ankara: EGM Yay.

Karagülmez, A.(2010). **Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri**. S.40. İstanbul: Seçkin Yayınları

Ketizmen M.(2008). **Türk Ceza Hukukunda Bilişim Suçları.** S.193 Ankara: Adalet Yayınları

Kurt, L.(2005). **Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması.** S.60-77 İstanbul: Seçkin Yayınları

Özel, C. (2002). **Bilişim-İnternet Suçları.** Er.Tar.20/09/2011, http://www.hukukcu.com/bilimsel/kitaplar/bilisim_internet_suclari.htm

Şener, K.(2011). **Bilişim Suçları Nelerdir?**. Er.Tar.20/09/2011, http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-nelerdir.html

Yenidünya, A.C. ve Değirmenci, O. (2002). **Mukayeseli Hukukta ve Türk Hukukunda Bilişim Suçları.** S.82-83 İstanbul: Legal Yay.

http://tdkterim.gov.tr/bts/ Er. Tar. 20/09/2011

http://tr.wikipedia.org/wiki/Bilgisayar%C4%B1n_tarih%C3%A7esi, Er.Tar. 20/09/2011

http://www.mevzuat.adalet.gov.tr/html/1328.html, Er. Tar. 20/09/2011

http://www.tbmm.gov.tr/kanunlar/k5237.html, Er. Tar. 20/09/2011