Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi / Cilt: 19, Sayı: 1, Haziran 2017, 137-152

Toplumsal ve Yönetsel Alanda Bilişim Teknolojilerinin Kriminal Etkileri[1]

DOI NO: 10.5578/jss.57198

Hüseyin KOÇAK[*]
Ali Nazmi DANDİN[**]

Geliş Tarihi: 08.04.2016
Kabul Tarihi:16.05.2017

Özet

Bilişim alanındaki gelişmeler ve özellikle 1990'lı yıllarda internetin tüm dünyada yaygın şekilde kullanılmaya başlamasıyla hayatın neredeyse her alanında devrim olarak nitelendirilebilecek değişiklikler yaşanmıştır. Kuşkusuz bilişim devriminin olumlu etkilerinin yanı sıra toplumlar ve devletler üzerinde olumsuz etkileri de görülmüştür. Bu etkilerin başında bilişimin suç yaratıcı ve suçun işlenmesini kolaylaştırıcı etkisinin olduğu rahatlıkla söylenebilir. Bilişim teknolojileri terör faaliyetlerinden, endüstriyel casusluğa kadar çok değişik alanlarda kullanılmaktadır. Kişisel mahremiyet sosyal medyayı kullanan birey için her an ihlal edilebilir konumdadır. Devletin, ticaretin, sağlığın, iletişimin, kamusallığın ve kısacası neredeyse tüm yaşam alanının elektronikleştiği günümüzde işlerini görmek isteyen her birey günden güne e-kaderini yaşamaya mahkûm olmaktadır. Bu mahkûmiyet herkesi potansiyel bilişim suçu mağduru yapmaktadır. Bu çalışmada bilişim devrimi ve kriminal etkileri üzerinde durulmuştur. Bunun yanı sıra bilişim suçlarına ilişkin bir tanım geliştirilmiş ve bilişim suçlarının tasnifine çalışılmıştır. Son olarak bilişim suçlarıyla mücadele açısından ülke ekseninde önerilere yer verilmiştir.

Anahtar Kelimeler: *Bilişim, Bilişim Suçları, Bilişimin Kriminal Etkisi, Bilişim (Bilgi) Devrimi.*

The Criminal Effects of Information Technologies in Social and Administrative Area

Abstract

There have been so many changes in almost all fields of life which can be described as a revolution with the development of information technology and the start of widespread use of the internet all over the world, especially in the 1990s. Without a doubt, the information revolution has also had negative effects on societies and governments besides its positive effects. It can be said that the fact that

[1] Bu çalışma 13. KAYFOR Kamu Yönetimi Kongresi kapsamında 16.10.2015 tarihinde sunulan bildirinin gözden geçirilmiş halidir.

[*] Doç. Dr. Afyon Kocatepe Üniversitesi, Sosyoloji Bölümü, kocak@aku.edu.tr

[**] Afyon Kocatepe Üniversitesi, Sosyal Bilimler Enstitüsü, Yüksek Lisans Öğrencisi. alinazmidandin@gmail.com

information encourages crime and makes easier to commit a crime is the leading one among the negative effects. Information technology has been used wide range from terrorist activities to industrial espionage. Personal privacy is violable for the people using social networks at any moment Because today everything has turned into electronics at almost all fields of life such as government, trade, health, communication and publicity, every people who want to do their job are obliged to experience their own e-destiny unfortunately. This obligation has made everyone potential cyber crime victim. This study is specifically concerned with the information revolution and its criminal effects. In addition to this, a definition has been improved for cybercrime and cybercrimes have been classified. Finally, there have been some suggestions on the struggle with the cybercrime country-wide.

Keywords: *Information Technology, Cybercrime, Criminal Effects of Information Technology, Information Revolution*

Giriş

Günümüz insanı elinde, zihninde ya da bir başka yerde saklayamadığı her türlü veriyi artık milimetrik aletler içerisine sığdırabilmektedir. Ayrıca, her türlü veriyi kompakt, sağlam, hızlı ve etkin bir şekilde depolayabilmekte, iletebilmekte ve işleyebilmektedir. Bugün bilişim alanındaki gelişmeler insanlığa olan büyük etkileri nedeniyle bilişim devrimi olarak adlandırılmaktadır. Toplumlar, bu devrimin ilerleyişini takibe çalışmak ve olumsuz etkilerinden zarar görmemek ya da kaçınılmaz etkilerinden en az zararla kurtulmak uğraşındadırlar.

Bilişim teknolojilerinde yaşanan ve süratle meydana gelen gelişmeler birçok alanda yeni yaşam şekilleri ortaya koymuştur. Bilişim teknolojilerinin gelişmesi ve özellikle internet kullanımının yaygınlaşması ile birlikte bireysel ve toplumsal hayatta meydana gelen değişimler sadece olumlu olarak gözlenmemekte, olumsuz birçok etkiyi de içerisinde barındırmaktadır.

Kuşkusuz, bilişim devriminin olumsuz yanlarından biri de, ortaya çıkardığı yeni suç tipleridir. Yine bilişim devrimi yeni suç tipleri yaratmanın yanı sıra var olan suçların işlenmesini de kolaylaştırabilmektedir. Bu makalede öncelikle kavramsal düzeyde bilişim devrimi ve bilişim devrimiyle ilişkili kavramlar açıklanmakta, ardından bilişim devriminin etkilerinden ve özellikle suç yaratıcı etkilerinden söz edilerek, bilişim suçlarının ve bilişim suçları süjelerinin genel özelliklerine değinilmektedir. Bildirinin sonunda konuya ilişkin çeşitli saptamalar, analizler ve önermeler yer almaktadır.

1. Bilişim Kavramı ve Bilişim Devrimi

Tüm dünyada ve özellikle Batılı ülkelerde belgeleme tekniğinin gelişmesiyle birlikte bilişim, ayrı bir disiplin olarak kabul görmüştür. Bu kabul ile birlikte bilişim kavramı, insanların teknik, ekonomik, mali, sosyal, kültürel, hukuksal veya toplumsal yaşamın benzeri birçok alanında sahip oldukları verilerin saklanması, saklanan bu verilerin elektronik olarak

işlenmesi, organize edilmesi, değerlendirilmesi ve yüksek hızlı veri, ses veya görüntü taşıyan iletişim araçları ile aktarılması anlamında kullanılmaktadır (Erdağ, 2010: 277). Bu haliyle bilişim, insanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve rasyonel şekilde işlenmesi bilimi olarak da tanımlanabilir (Akarslan, 2012:27).

Sözlük anlamıyla devrim; belli bir alanda hızlı, köklü ve nitelikli değişikliktir (tdk.gov.tr, 2015). Devrim bazen sadece onu yaratan toplumun içerisinde etkili olabileceği gibi bazen de küresel düzlemde radikal değişikliklere yol açar. Örneğin Fransız Devrimi, oluşturduğu felsefe ve düşünce sistematiği ile tüm dünyayı etkilemiş; yönetim, özgürlük ve insan hakları gibi alanlarda yeni boyutlar ortaya koymuştur. 1980'li yıllarda mikro bilgisayarların geliştirilmesi ve bilgisayar sistemlerinin internet ile birbirine bağlanıp kullanımlarının yaygınlaşmasıyla birlikte insanoğluna küresel bir iletişim kapısı açılmıştır. Bilgisayar ve internet ile birlikte gelişen bilişim alanının, toplumlara, bireylere ve ekonomi anlayışına kazandırdığı farklı boyut ve oluşturduğu radikal değişim sürecinin devrim niteliğinde olduğu söylenebilir. Bu sürece rahatlıkla "bilişim devrimi" denilebilir (Alaca, 2008:24).

Teknoloji devriminin somut olarak görüldüğü 1970 ve 1980'li yıllar iki kutuplu bir dünya düzenine şahit olmuştur. Bu dönemde kutupların lokomotif ülkeleri silah sanayi ve uzay teknolojileri alanında yarışmışlardır. Bu yarışta alt yapı ve destek sağlamak amacıyla kullanılmak istenen bilgi ve iletişim teknolojileri alanında hızlı bir gelişme kaydedilmiştir. Telekomünikasyon ve bilgi işlem teknolojilerindeki hızlı ve etkin seyreden gelişmeler anında haberleşmeye ve verilerin anında iletimine imkân sağlamıştır. Oluşturulan iletişim ağı sayesinde sesli, görüntülü ve yazılı veriler her noktaya dijital olarak ulaştırılabilmiştir. Bugün kablosuz teknoloji ile daha ergonomik bir yapıda yararlanılabilen internet sistemi ile iletişim ağı tüm dünyaya yayılmıştır (Atasoy, 2007:166).

İnsanın, bilgiyi saklama, paylaşma ve ona kolayca ulaşma arzusu ve gereksiniminden ortaya çıkan internet, birçok bilgisayar sistemini TCP/IP protokolüyle birbirine bağlayan ve hızla büyüyen küresel bir iletişim ağıdır. Diğer bir ifadeyle, değişik bilgisayarların ortak bir dil çerçevesinde birbirlerine elektronik olarak bağlanması (Network) suretiyle, insanların bilgi paylaşımına imkân veren küresel bir ağdan ibarettir (İçişleri Bakanlığı, 2006: 7-8). Bu küresel ağ bugün itibariyle dünyanın farklı pek çok yerindeki milyarlarca bilgisayarı birbirine bağlamaktadır (Tekeli, 2011:183). Bilişim teknolojilerinden olan bilgisayar ve internet sayesinde insanlığın bilgiye ulaşması kolay, ucuz, hızlı ve güvenli bir hal almıştır (İçişleri Bakanlığı, 2006:8).

İletişim teknolojileri arasında sayılabilecek film, slayt, televizyon, uydu, teleteks, veri aktarma ağı ve benzeri teknolojilerin bilgisayar ve özellikle internet kanalı ile kombine edilerek kullanılmaya başlaması bilişim teknolojilerinin küreselleşmesine neden olmuştur (Avcıoğlu, 2011:21-22).

Bilgi güçtür ilkesinden hareketle, bilgi ve bilgiye dayalı gelişmelerin tarihin her döneminde toplumları üstünlük anlamında birbirinden ayırdığı söylenebilir (Koçak, 2011:39). Günümüzde, toplumlar, onları üstünlük anlamında ayıran nitelikli bilgi bilişim alanında yoğunlaşmamış ise o toplumun gelişmişliğinden söz edilememektedir. Bilişim teknolojilerini üreten az sayıdaki ülkenin üretemeyen toplumlara nazaran üstünlük sağladığı rahatlıkla söylenebilir (Ege, 2008:46).

Bilişim teknolojilerinin gelişmesi ve özellikle bilgisayar ile internet teknolojilerinin bulunup yaygın şekilde kullanılmaya başlamasıyla birlikte toplumların ekonomik, sosyal, kültürel ve hukuksal yaşamlarında köklü değişiklikler meydana gelmiştir. Bu değişiklikler çok hızlı, nitelikli ve devam eden değişikliklerdir. İnsanoğlu bilişim teknolojileri ile birlikte artık dünyanın öbür ucundaki herkesle iletişim kurabilmekte, dünyanın öbür ucundan mal ya da hizmet satın alabilmekte ve hatta eğitim, sağlık, adalet, güvenlik gibi alanlara dair hizmetleri bu kanaldan sağlayabilmektedir.

2. Bilişimin Toplumsal ve Yönetsel Alanlardaki Kriminal Etkileri

Bilişim devriminin bir parçası olan bilişim teknolojilerinin ve özellikle internetin yaygın kullanımı, bireysel ve toplumsal yaşamda büyük etkiler doğurmuştur. Bilişim teknolojileri bugün tıp, ekonomi, eğitim, iletişim, ticaret, adalet, güvenlik ve bunun gibi birçok alanda kullanılmakta ve yeni alışkanlıklar ortaya koymaktadır. Bu yeni yaşam şekli de kuşkusuz her alanda olumlu ve olumsuz olmak üzere etkilerini gün yüzüne çıkarmıştır. Bilgi ve iletişim teknolojilerinin insanoğluna sağladığı birçok faydalarla birlikte yeni suç tipleri yarattığı ve suç işleme imkânı sağladığı hususu da unutulmamalıdır.

Bilgisayar teknolojisinin hızla gelişmesi, boyutunun küçülmesi ve maliyetinin azalmasıyla birlikte kullanıcı sayısında büyük bir artış yaşanmıştır. Bu gelişmeye paralel olarak eski yöntemler terk edilmiş ve hemen hemen her alandaki kayıtlar bilişim teknolojileri ile yapılmaya başlanmıştır. 1990'lı yıllarda internetin de büyük bir gelişme kaydederek dünyadaki bilgisayar kullanıcılarını birbirine bağlamasıyla suça meyilli kişi ve gruplar için yeni suç alanları doğmuştur (Durmaz, 2006:76'dan aktaran Alaca, 2008:21).

Bilişim teknolojilerinin gelişimine paralel olarak her geçen gün yeni suç işleme araç ve yöntemleri ortaya çıkmaktadır. Yeni ortaya çıkan suç işleme yöntemlerine karşı önlemler alındığı anda, daha gelişmiş ve farklı bir

suç işleme yöntemi ile karşı karşıya kalınmaktadır. Teknolojide yaşanan gelişmeler suçun işleniş yöntemlerinin, araçlarının ve çeşitlerinin sürekli gelişimine ve değişimine neden olmaktadır. Özellikle internet; uyuşturucu ticareti, insan kaçakçılığı ve terör gibi organize suç faaliyetleri açısından iletişim aracı olma, bilgi kaynağı sağlama, eleman kazanma, propaganda yapma ve finansal servis aracı olma gibi nitelikleriyle kolaylıklar sağlamaktadır. Kolluk güçlerinin tespitlerine karşı önlem olarak e-posta, anlık mesajlaşma, internet telefonu gibi internet iletişim araçlarının anonimlik sağladığının fark edilmesi, bu teknolojileri organize suç örgütlerinin kullanımına açmaktadır (Tekeli, 2011:184).

İnternetin her kurum ve kuruluş için vazgeçilmez bir araç olmasıyla birlikte resmi kurum ve kuruluşların bilgisayarları bu ağa bağlanmış durumdadır. Bu sebeple suç işlemeye meyilli kişilerin hedefi haline gelmişlerdir. Örnek vermek gerekirse bugüne kadar güvenliği en üst seviyede tutan kurumlar arasında bilinen Amerika Bileşik Devletleri Savunma Bakanlığı (Pentagon), NATO, NASA ile bazı askeri ve endüstriyel araştırma laboratuvarlarının bilişim sistemleri bilgisayar korsanlığı eylemlerinin kurbanı olmuştur. Şirketin ana sunucularına girilmesi sonucu kullanıcılar iki gün boyunca Microsoft'un sitelerine giriş yapamamışlardır (Kurt, 2004'den aktaran Alaca, 2008:22). Türkiye'de de 2010 yılında ortaya çıkan ÖSYM'nin yaptığı çeşitli sınavlarda soru ve cevaplarının bilişim sistemleri aracılığıyla elde edilip para karşılığı satıldığı iddiaları önemli bir örnek oluşturmaktadır (Karagülmez, 2011:7).

Bilişim suçlarının failleri açısından daha fazla koruma altında olan büyük şirketler ve sistemlerle uğraşmaktansa, bireysel kullanıcıların hedef alınması daha kolay gözükmektedir. Bir bilişim sisteminin etkisiz hale getirilmesi o teknolojiye hâkim olmayı gerektirmektedir. Dolayısıyla bu gereklilik, suçluları daha kolay olana yöneltmekte ve daha çok kullanıcılara yönelik tuzaklar hazırlatmaktadır (Tekeli: 2011:84).

Depolama, işleme ve iletme imkânı veren bilişim sistemleri yoğun şekilde bilgi barındırmaktadır. Bu bilgi yoğunluğu birçok kolaylık sağlarken bir yandan da bilişim sistemlerinin zayıf yanı olarak karşımıza çıkmaktadır. Büyük miktarda bilginin toplanması ve bilgi-işlem sırasında yapılan hatalar, bu bilgilere ulaşmak ve bu hatalardan istifade etmek isteyenler için bulunulmaz bir fırsat olmaktadır (Alaca, 2008: 38-40). Yine bilgi yoğunluğu, muhtemel saldırılara karşı riske edilen bilgi miktarı ve bilginin niteliği açısından da tehlike arz etmektedir.

Bilişim sistemlerinin bilgi saklama kapasiteleri çok yüksektir. Bilgiyi saklama maliyeti çok düşük olmasına rağmen bilgiye erişim çok hızlı şekilde gerçekleştirilebilmektedir. İçeriğindeki veriler üzerinde hiçbir iz, silinti ve kazıntı bırakmadan değişiklik yapabilme olanağı bulunmaktadır. Bilişim sistemlerinde yoğun şekilde bilgi saklanabilmesi, bilgilerin yeniden

derlenebilmesi ve bilgilerin elektronik ortamda iletilebilmesi gibi özellikler suç yaratıcı faktörler olarak karşımıza çıkmaktadır (Alaca, 2008:39). Bunun yanında bilişim sistemlerindeki kontrol mekanizmasındaki eksiklikler de suçun işlenmesini kolaylaştırmaktadır. Saklama, iletme ve işleyebilme noktasında elde edilen hız, saldırılara karşı her zaman avantaj sağlayamamaktadır.

Bilişim sistemlerinin verilen komutları hiçbir sorgulamaya tabi tutmadan uygulaması nedeniyle, mantık dışı ve dolandırıcılık içeren komutları fark edememektedir. Komutların insan yerine bilgisayardan geldiğinde bilgisayarın hata yapmayacağına olan inanç yüzünden bunlara daha fazla güvenilmesi, para transferlerinin çok uzak mesafelerde, çok kısa sürelerde ve çok büyük miktarlarda yapabilmesi de bilişim sistemlerinin zayıf yanları arasında gösterilebilir. Suçların anonim şekilde işlenmesine olanak tanıması hususu da bilişim sistemlerinin bir diğer zayıf yanı olarak ortaya çıkmaktadır. Bu sistemlerde işlenen suçlarda mağdurun çoğu zaman belli olmaması, suçun sisteme karşı işlenmesi söz konusudur. Fail kimin malını aldığını bilmemekte, mağdur sistem olarak gözükmektedir. Bu durum ise failin tespitinde sorunlarla karşılaşılmasına neden olmaktadır (Alaca, 2008:38-40).

Bilişim suçlarının mağduru bazen bir kişi, bazen bir kurum, bazen ise toplumun tamamı olabilmektedir (Akarslan, 2012:37). Mağdurun belirlenmesi noktasındaki sıkıntılar da bilişim suçlarının anonim işlenme özelliğini güçlendirmektedir.

Bilişim suçlarını diğer suçlardan ayıran kimi özellikler şu şekilde sıralanabilir; zaman veya yer ile sınırlı olmadan meydana gelmesi, kolayca tanımlanabilecek sınırlara sahip olmaması, ülke ve yargı sınırlarını aşması, kanunlaştırma ve delillendirmenin güç ve dikkate değer teknik bilgi gerektirmesi, bu alanda suç tanımlarının tam manasıyla yapılamamış olması (Çakır ve Sert, 2011:145-146).

Bilişim suçlarını işleyenlerin genel olarak 20-30 yaşları arasındaki gençlerden oluştuğu gözlemlenmiştir. Bunun yanında faillerin genel itibariyle erkeklerden oluşan teknik bilgi düzeyi yüksek kişiler olduğu tespit edilmiştir. Bazı duygusal ve psikolojik sebeplerin de bu kişileri bilişim suçu işlemeye ittiği yapılan çalışmalarla ortaya çıkarılmıştır (Demirbaş, 2005:267'den aktaran Tulum, 2006:46). Amerika'da yapılan çalışmalar bilişim suçları faillerinin normal insanlara nazaran daha uyanık, sabırsız, çabuk motive olan, cüretkâr, maceraperest ve teknolojik iddialaşma içinde bulunan kişiler olduğunu ortaya koymuştur (Bequai, 1998:579-582'den aktaran Tulum, 2006:47).

Yakalanma riskinin çok az olması, bilişim suçunun sonucunda çok yüksek kazancın kolay ve risksiz olarak temin edilmesi, bilişim suçlarının

yeni suç tipleri olması nedeniyle gerekli kanun ve düzenlemelerin eksik ve yetersiz olması bilişim suçlarının faillerini cesaretlendiren hususlardır. Bazen fiillerinin deşifre olunmaması için ihbar edilmeyeceğinden, bazen ise bu fiilleri karşılayacak ceza normunun bulunmamasından cesaretle, bilişim suçlarının failleri eylemlerinin yaptırımsız kalacağına güvenle hareket etmektedir (siberkolluk.com, 2015).

Bilişim suçlarının failleri suç sayılan eylemlerinin haksızlık içeriğinin bulunmadığını düşünebilmektedirler. Örneğin Türkçe karşılığı bilgisayar korsanları olarak kullanılabilecek olan hackerlar; *"Sistemlere, donanıma ve bilgisayarlara erişim kısıtlanamaz. Bireyler, bir sistemin, teknolojinin nasıl işlediğini öğrenmekte özgürdürler." "Bilgi özgürdür. Bilginin üretilmesi, üretilen bilginin yaygınlaştırılması üzerinde bir kısıtlama kabul edilemez." "Otoriteye güvenmeyin. Baskı her zaman otoriteden kaynaklanır. Güç tek bir noktada toplanmamalıdır." "Eserleriniz, yaptıklarınız, başarınızı sizi değerli kılar. Her değerlendirme geçersizdir." "Bilgisayarlar kullanılarak güzel ve iyi şeyler yapılabilir." "Bilgisayarlar yaşamınızı olumlu yönde geliştirir."* şeklinde etik kurallar benimsemişlerdir (Akdeniz, 2013: 13). Bu etik değerlerden de anlaşılacağı üzere, bir bilgisayar korsanı için belli kurallar dâhilinde hack eyleminin haksızlık içeriği olamaz. Oysa hack eylemi çoğu ülkenin ceza mevzuatında suç olarak tanımlanmış durumdadır.

Yapılan araştırmalar bilişim suçlarının faillerinin genel olarak; işten çıkarılma veya işteki çeşitli hoşnutsuzluklar, politik amaç gütmeleri, sadece eğlenmek istemeleri, cinsel tatmin isteği, ciddi psikolojik rahatsızlıklar, öfke ve intikam alma duygusu (vandalizm, sabotajlar, yağma gibi), mali zorluklar ve para sağlama isteği, bilgisayarı aşabilme duygusu (operatör makine ilişkisinden kaynaklanan sorunlar da dahil) sebepleriyle suç işlediklerini göstermektedir (Alaca, 2008: 50-51).

İşlenen bilişim suçlarının %95'lere varan kısmı mağdurların kamuoyundan saklanmak istemeleri nedeniyle gün yüzüne çıkmamaktadır. Özellikle şirket seviyesinde işlenen bilişim suçları kolluk araştırması yüzünden ticari sırların ortaya çıkması ya da prestij kaygısı gibi sebeplerle kamuoyundan saklanmaktadır. Bunun yanında mağdur şirketlerin küçük zararları olağan olarak kabul eden ticari yaklaşımları da bilişim suçlarının açığa çıkmasını engelleyebilmektedir (Demirbaş, 2005:268'den aktaran Tulum, 2006:52).

Endüstriyel casusluktan terör eylemlerine kadar her alanda kullanılabilen bilişim araçları, kişilerin mahrem alanlarına dair de bir tehdit unsuru haline gelmiştir. Birçok ünlü siyasetçi, oyuncu, sporcu, sanatçı ya da sıradan insanın mahrem alanına dair görüntüler rahatlıkla internet ortamında milyonların önüne serilebilmektedir. Örneğin 2014 yılında birçok Hollywood yıldızının uygunsuz fotoğrafları bilgisayar korsanları tarafından

"iCloud" isimli veri depolamaya yarayan bilişim sistemine girilerek elde edilmiş ve 4Chan sitesinde yayınlanmıştır (medyafaresi.com, 2015).

Bilişim suçlarının işlenmesi noktasında truva atı, bukalemun, yerine geçme, mantık bombaları, artık depolama, gizli dinleme, bilgi aldatmacası, salam tekniği, süper darbe, ağ solucanları, virüsler, spam iletiler ve phishing (kimlik avı) gibi yol ve yöntemler geliştirilmiştir (Turhan, 2006:47-57).

3. Bilişim Suçları ve Nitelikleri

Bilişim suçlarının tanımı, ne ulusal hukuk düzenlemelerinde ne de uluslararası hukuk düzenlemelerinde yer almaktadır. Bu düzenlemelerde herhangi bir tanım yapılmaksızın bilişim suçu olarak nitelendirilen eylemlere suç tipi olarak yer verilmesi tercih edilmiştir. Öğretide ise bilişim suçu kavramının pek çok tanımı yapılmış ancak bir tanım üzerinde uzlaşmaya varılamamıştır. Bir tanım yapılmasından çok bu kavram altında hangi suç tiplerinin düzenlenmiş olduğu önem kazanmıştır. Bilişim suçlarına ilişkin genel ve kapsayıcı bir tanım yapılmasının zorluğuna ve bu konudaki çekincelere rağmen bilişim suçu Dülger tarafından, "verilere karşı ve/veya veri işlemle bağlantısı olan sistemlere karşı, bilişim sistemleri aracılığıyla işlenen suçlar" şeklinde tanımlanmıştır (Dülger, 2005).

Dönmezer bilişim suçlarını; "Bilgisayarın kötüye kullanılması, bilgileri otomatik işleme tabi tutulmuş ve verilerin nakline ilişkin kanuna ve meslek ahlakına aykırı davranışlar" olarak tanımlamıştır (Dönmezer, 1989:504). Yazıcıoğlu ise bilişim suçlarını "ceza kuralları uyarınca, bilgisayarın konusunu veya vasıtasını yahut simgesini oluşturduğu suç içeren fiiller" olarak tarif etmektedir (Yazıcıoğlu, 1997:142). Ersoy da bilişim suçlarını "bilişim araçları ile işlenen veya bilişim araçlarına karşı işlenen suçlar" olarak ifade eder (Ersoy, 1994:151).

Bilişim teknolojilerinin sadece kullanılmasıyla birlikte herhangi bir veri ya da bilişim sistemine zarar verilmeden de bilişim suçu işlenebilir. Örneğin sadece bir metin içeren e-posta göndermek suretiyle hakaret, tehdit, cinsel taciz, intihara yönlendirme ve benzeri suçlar işlenebilir. Bu hallerde 5651 ve 5070 sayılı yasalardan hareketle "bilişim sistemleri tarafından üzerinde işlem yapılabilen, taşınıp saklanabilen her türlü değer" olarak ifade edilebilecek veri ya da bilişim sistemine herhangi bir saldırı gerçekleştirilmemiş olmasına rağmen bilişim araçları kullanılarak bilişim suçu işlenmiş olacaktır.

Bilgisayar; verilerin saklanması, işlenmesi ve iletilmesi bakımından en yaygın bilişim sistemi olarak kullanılan araçlardandır. Öğretide ve uygulamada aynı anlamda kullanıldıkları görülse de, bilişim ve bilgisayar aynı şey demek değildir. Verilerin işlenmesi (veri-işlem) ve bu işlemin sonuçlarının aktarılması (veri-iletişim) olarak tanımlanabilecek olan bilişim, bilgisayara oranla onu da kapsar nitelikte bir kavramdır. Bilgisayar,

matematiksel ve mantıksal işlem dizileriyle hazırlanmış programlar çerçevesinde verileri otomatik olarak işleme tabi tutan sistemlerin ortak adıdır. 5237 sayılı Türk Ceza Kanunu'nun 243. maddesinin gerekçesinde bilişim sistemi, eksik şekilde bilgisayardan hareketle "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" şeklinde tanımlanmıştır (Erdağ, 2010:277-278). Buradan hareketle bilişim suçlarının tanımında sadece bilgisayarı ya da bilişim sistemlerini suç aracı görerek tanımlama yapmak kısıtlı bir alanda konuyu ele almamıza neden olacaktır. Taşınabilir bellek, CD, GPS sistemleri gibi araçların teknik olarak bilgisayar ya da bilişim sistemi olmadığı söylenebilir ise de, bu araçların bilişim teknolojileri içerisinde olduğu açıktır. Bunun yanında bilişim teknolojileri alanındaki süratli ve tahmin edilemeyen gelişmelerin varlığı karşısında bilişim suçu tanımında bilgisayar ya da bilişim sistemleri ile kısıtlanmak yerinde bir davranış değildir.

Yine bilişim araçları kullanılarak işlenen suçların bilişim suçu olduğu varsayımı hatalıdır. Örneğin, failin "akıllı telefon" diye adlandırılan ve bir bilişim sistemi olarak görülen cep telefonunu mağdura fırlatıp isabet sonucu onu yaralaması olayında kasten yaralama suçu işlenmiş olacak ancak, olayda bir bilişim suçu söz konusu olmayacaktır. Buradan hareketle bilişim araçları kullanılarak bilişim suçunun işlenebilmesi için bilişim aracının kendine özgü özelliklerinin fiilde kullanılması gerekecektir. Buna örnek olarak failin akıllı telefonu ile virüs içerikli bir e-postayı mağdurun e-posta hesabına iletmesi gösterilebilir.

Benzer bir biçimde bilişim araçlarına karşı işlenen suçların da bilişim suçu olduğu varsayımı kanaatimizce hatalı olabilir. Örneğin failin mağdura ait tablet bilgisayarı bilerek kırıp parçalaması olayında mala zarar verme suçu oluşuyor olmasına rağmen, bilişim suçunun varlığından bahsetmek mümkün değildir.

Açıklananlar ışığında bilişim suçlarının "bilişim araçlarının kendine özgü (sui generis) özellik ya da özelliklerinin kullanılarak işlenebilen suçlar" olarak tanımlanması uygun olacaktır.

Bilişim alanındaki gelişmeler her geçen gün karşımıza yeni suç tipleri çıkarırken bir yandan da bilişim araçları klasik suçların işlenmesini kolaylaştırabilmektedir. Bu nedenle bilişim suçları doğal (saf) bilişim suçları ve yapay (suni) bilişim suçları olarak ikiye ayırıp incelenebilir.

Yasal tanımına göre işlendiği sırada bilişim araçlarının kullanılması zorunlu olan suçlara doğal bilişim suçları, bilişim araçlarının kullanılması zorunlu olmamakla beraber bilişim araçları kullanılarak da işlenebilen suçlara ise yapay bilişim suçları denilebilir.

3.1. Doğal Bilişim Suçları

Doğal bilişim suçundan söz edilebilmesi için kanun koyucu suç tanımını yaparken o suçun işlenmesinde bilişim araçlarının kullanılmasını zorunlu kılmaktadır. Bu zorunluluk bizzat suçun temeli şeklinde ortaya konulabileceği gibi nitelikli haller ya da cezayı artıran veya azaltan nedenlerde de olabilir.

Hakaret suçu açısından bir değerlendirme yapıldığında 5237 sayılı Türk Ceza Kanunu'nun 125/2 maddesinde hakaret fiilinin mağduru muhatap alan sesli, yazılı veya görüntülü bir iletiyle işlenmesi halinde failin cezalandırılacağı hüküm altına alınmıştır. Burada sesli, yazılı ya da görüntülü bir iletiden bahsedildiğinden düzenlemenin doğal bilişim suçuna işaret ettiği düşünülebilir. Her türlü veriyi içeren iletiler doğal olarak internet, bilgisayar, telefon ve benzeri bilişim araçlarıyla mağduru muhatap alabilir. Ancak bahse konu düzenleme açısından failin örneğin mektup yoluyla da hakaret suçunu işleyebilmesi gündeme gelebileceğinden suçun işlenmesinde bilişim araçlarının kullanılmasının zorunluluk arz etmediği ortadadır. Bu sebeple bahse konu düzenleme açısından hakaret suçunun doğal bilişim suçu olmadığını kabul etmek gerekir.

Doğal bilişim suçuna doğrudan bir örnek vermek gerekirse, ilk olarak 5237 sayılı kanunun 243. maddesinde yer alan bilişim sistemine girme suçu akla gelecektir. Yasa koyucu bu düzenleme ile hukuka aykırı şekilde bilişim sistemine girilmesini ve orada kalmaya devam edilmesini cezalandırma yoluna gitmiştir. Bu düzenleme açısından failin bilişim araçlarını kullanması zorunluluk arz etmektedir.

5237 sayılı yasa kapsamında sayılan doğal bilişim suçları şunlardır:

- Bilişim sistemine girme (madde 243)
- Sistemi engelleme, bozma, verileri yok etme veya değiştirme (madde 244)
- Banka veya kredi kartlarının kötüye kullanılması (madde 245)
- Bilişim sistemlerinin kullanılması suretiyle hırsızlık (madde 142/2-e)
- Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık (madde 158/1-f)

3.2. Yapay Bilişim Suçları

Doğal bilişim suçları dışında kalan suçların bilişim araçları kullanılarak da işlenebilmesi mümkün olabilir. İlk etapta bu suçların soyut anlamda bilişim suçu olduğundan söz edilemez. Somut anlamda suç ile karşılaşıldığında somut olayda doğal bilişim suçları dışında kalan bir suçun işlenmiş olmasına rağmen bilişim araçlarının suçta kullanılması halinde o suçun artık yapay bilişim suçu olduğundan söz edilebilir.

Örneğin öldürmek kastıyla trafik ışıklarının bağlı olduğu bilişim sistemine girerek trafik ışıklarının kırmızıyı göstermesi gerekirken araç

kullanan mağduru yanıltarak yeşil ışık yanmasına ve trafik kazasına sebebiyet verip mağdurun ölümüne neden olan fail açısından durum böyledir. Fail kasten öldürme suçunun icrasını gerçekleştiren kişi olmasına ve kasten öldürme suçunun soyut manada bilişim suçu olmamasına rağmen somut fiil ile birlikte kasten öldürme suçu yapay bilişim suçuna dönüşmüştür.

5237 sayılı yasa kapsamında sayılan ve doğal bilişim suçları dışında kalan suçların somut fiil ile birlikte yapay bilişim suçuna dönüşmesine şu örnekler verilebilir:

- Hakaret (Failin sosyal paylaşım sitesi hesabından sinkaflı küfürler içeren iletileri mağdurun sosyal paylaşım sitesi hesabına mesaj yolu ile göndermesi)
- İntihara yönlendirme (Failin internet sitesi kanalı ile birçok insana ulaşıp intihara özendirici yayınlar yapması)
- Müstehcenlik (Failin çocuk pornosu içerikli fotoğrafları bilgisayarında saklaması)
- Haberleşmenin engellenmesi (Failin mağdurun internet kullanımını ve dolayısıyla haberleşmesini engelleyebilmek amacıyla akıllı telefonuna kablosuz ağ kullanımını engelleyen yazılım yüklemesi)
- Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması (Bir banka çalışanı olan failin tacir olan mağdura ait kredibilite bilgisini bankaca kullanılan bilişim sisteminden edinip rakip şirket yetkililerine vermesi)

"Doğal bilişim suçu-yapay bilişim suçu" ayrımı bilişim suçlarının kapsamını özellikle neredeyse tüm klasik suçların bilişim araçlarıyla birlikte işlenebilmesiyle birlikte yapay bilişim suçları alanına doğru genişletiyor olsa da, faydacı bir yaklaşımla soruşturma ve kovuşturmaların titizlikle ele alınıp incelenmesi anlamında önem arz etmektedir. Klasik suçların takip yöntemleri bilişim suçlarının delillendirilmesinde maalesef yetersiz kalmaktadır. Bilişim suçları uzman kolluk, uzman bilirkişi, uzman savcılık ve uzman mahkemeler nezdinde ele alınmak zorundadır. Bu zorunluluk hayat bulduğu takdirde faydacı bir bakış açısıyla yapay bilişim suçlarını da içine alan bilişim suçlarının uzman birimlerce takip edilmesi doğal olarak toplum lehine olacaktır.

4. Örnek Olaylar

İnternet ağları hareketlerinin toplumsal bağlama göre farklı şekillerde ortaya çıkardığı özerklik uzamı; örgütlenme, tartışma ve ayağa kalkma çağrılarıyla kentlerde başlayıp devam etmiştir (Castells, 2013:99). Hatta kimi yazarlarca sivil toplum ve gazeteciliğin bilişim teknolojilerinin faal olarak yararlanıldığı ülkelerde radikal bir demokratik geçişe ya da

demokratik kurumların ciddi bir biçimde pekişmesine neden olabileceği iddia edilmektedir (Howard, 2011:200'den aktaran Castells, 2013:100).

Bilişim neredeyse her alana nüfuz etmiş durumdadır. Bilişim teknolojileri bugün devletlerce manipülasyon aracı olarak bile kullanılabilmekte, toplumlara yön verme çabalarında kullanılarak toplum mühendisliği hareketinin bir aracı olabilmektedir (Avcıoğlu, 2011:17).

Örneğin Wikileaks organizasyonunun Amerikan gizli belgelerini internet kanalı ile tüm dünya ile paylaşması; Amerika Bileşik Devletleri'nin mahremiyetine yapılan bir saldırı mı, yoksa diğer ülkelerdeki Amerikan imajının düzeltilmesine yönelik bir proje mi olduğu yönünde büyük tartışmalara neden olmuştur (Yılmaz, 2010).

Bugün tüm dünyayı ve özellikle Ortadoğu coğrafyasını derinden etkileyen ve "Arap Baharı" diye adlandırılan, başta Tunus ve Mısır'da gelişen halk hareketlerinin dahi dijital bir devrim olup olmadığı tartışılmaktadır.

Hangi tarafta durulursa durulsun, bilişim teknolojileri kanalıyla dünya siyasetine yön verecek şekilde casusluk ya da manipülasyona yönelik eylemlerde bulunulduğu söylenebilir.

Bilişim ve siber güvenlik bugün gelişmiş devletlerin bile en büyük sorunlardan biri haline gelmiştir. Barack Obama ikinci kez Amerikan başkanı seçilmesinin ardından yapmış olduğu ilk konuşmasında ülkesinin önemli meselelerine değinmiş, özellikle siber güvenlik alanında kongreden hükûmetine daha fazla yetki vermesini istemiştir (turkishny.com, 2015). Amerikan kamu kurumlarına yönelik olarak IŞİD gibi terör örgütlerinin siber saldırılar düzenlemiş olması, Sony şirketinin Kuzey Kore'yi kötüleyen "Röportaj" isimli bir filmi gösterime sokmak istemesi nedeniyle internet sitesinin hacklenmesi gibi olaylar Amerika Bileşik Devletleri gibi süper güç olarak tanımlanabilecek bir ülkeyi dahi kaygılandırmıştır. Bu kaygılar ekseninde siber güvenlik alanında hukuk yaratma çabaları 2015 yılı itibariyle bu süper güç ülkede de hız kazanmıştır. Bugün Amerika Bileşik Devletleri siber güvenlik alanında yaklaşık 15 milyar dolar para harcamayı göze almış durumdadır (aa.com.tr, 2015).

Sonuç

Siyasal, sosyal ve ekonomik alanda köklü değişikliklere neden olan bilişim, hukuk alanında da birçok değişikliğe neden olmuştur. Bilişim, özellikle ceza hukuku alanında yeni suç tipleri doğurmuş ve var olan suçların işlenmesini kolaylaştırmıştır. Maalesef bilişim teknolojileri alanında yaşanan hızlı gelişmelere paralel olarak hukukun gelişmesi mümkün olamamaktadır.

Bilişim suçları alanındaki değişimlerin bireysel suçlarla sınırlı kalmayacağı, örgütlü ve uluslararası yapılarla daha büyük hukuki menfaatlere yönelebileceği ve hatta devleti zafiyete uğratabilecek bir hal

alabileceği öngörülmektedir. Öte yandan başta terör olmak üzere ülkeler arası ekonomik rekabetin yakın gelecekte bilişim teknolojileri aracılığıyla gerçekleşeceği açıktır. Protesto gerekçesiyle hedef ülkelerin kamusal belgelerine yönelen siber saldırıların bu tespitin sinyalleri olduğu söylenebilir. Bilişimin suç alanında etkin kullanımı ile birlikte geleceğin dünyasında suçların bilişim suçları ve diğerleri şeklinde bir ayrıma tabi tutulacağı muhtemel gözükmektedir (TBMM, 2012: 841-843).

Yeni suç türlerinin ortaya çıkmasıyla birlikte ceza hâkimi, hukuk hâkimi kadar serbestiye sahip değildir. Ceza hâkimi, önüne kanunda tarif edilmeyen hukuksuz bir eylem geldiğinde suçta ve cezada kanunilik ilkesinin bir sonucu olarak hukuk hâkimi gibi hukuk yaratma yoluna gidemez. Bu durumda ceza hâkimince eylemin cezalandırılması mümkün olmayacaktır (Yarsuvat, 2011:1). Kanun koyucunun bilişim teknolojilerinin doğurduğu suçlar açısından güçlü tahminlerde bulunup önceden düzenleme yapması mümkün gözükmemektedir. Ancak bilişim teknolojilerinin klasik suçların işlenmesinde her zaman kullanılabileceği düşünülürse, klasik suçların işlenmesinde bilişim araçlarının kullanılması genel bir ağırlaştırıcı neden olarak ceza kanunlarında kendisine yer bulabilir.

Kuşkusuz bilişim araçlarının suçta kullanılması faile genellikle anonim özelliklerinden dolayı kolay saklanma imkânı tanımaktadır. Bunun yanında fail, fiziki hareketlere nazaran dijital ortamda daha kolay hareket edebilmektedir. Bilişim araçlarının sırf kendine has özelliklerinin kullanılması suretiyle işlenen klasik suçlarda failin hareketlerinin haksızlık içeriğinin olağan suç işleme yollarına nazaran daha fazla olduğu söylenebilir. Bu sebeple haksızlık içeriğinin fazla olduğu doğal bilişim suçları dışında kalan ve bilişim araçlarının kullanılmasıyla beraber yapay bilişim suçuna dönüşen eylemlerin, haksızlık içeriğinin fazlalığı nedeniyle genel bir ağırlaştırıcı neden şeklinde düzenleme içinde değerlendirilmesi yoluna gidilebilir. Bu sayede cezanın caydırıcı etkisinden faydalanılarak bilişim araçlarının suçta kullanılması kısmen de olsa engellenmiş olacaktır.

Anonim yapıda olan bilişim araçları ve özellikle internet teknolojisi suçta kullanıldığı zaman genel olarak soruşturmalar ve kovuşturmalar açısından yabancı unsur ortaya çıkmaktadır. Türkiye'de işlenen bilişim suçları açısından fail, kullanılan araç ya da hizmet sağlayıcı bilişim teknolojilerini tüketen bir yapıda olduğumuzdan çoğu zaman yabancı olmakta, delillerin toplanması ülkeler arası adli yardımlaşmayı gerektirmektedir. Bu durum açısından adli makamların işlettikleri adli yardım süreci aylar ve hatta yıllar almakta, deliller kaybolmakta ya da ulaşılamaz hale gelmektedir. Bilişim suçlarıyla mücadele açısından maalesef klasik suçlara ilişkin yöntemler yetersizdir. Bu sebeple bütüncül bir bakış açısıyla sorunun çözümü yoluna gidilmek zorundadır. Mücadele ekseninde

devlet, tüm kurumlarıyla ve hatta uluslararası alanda her türlü işbirliğini sağlamak zorundadır.

Bilişim suçları açısından ülkede uzman bilirkişi eksiği çok dikkat çekicidir. Kamuoyunda "Balyoz Davası", "Ergenekon Davası" ve "17-25 Aralık Operasyonları Darbe Girişimi" olarak bilinen, ülke gündemine damgasını vuran dava ve soruşturmalarda elde edilen dijital deliller hakkında düzenlenen ülkenin farklı kurumlarının birbirinden farklı bilirkişi raporları adalete olan güveni büyük ölçüde sarsmıştır.

Bilirkişi eksiği açısından devlet öncelikle üniversitelerinde adli bilişim uzmanı yetiştirmek ve uluslararası standartlarda adli bilişim laboratuvarları kurmak zorundadır. Kurulan laboratuvarların da bilirkişinin bağımsızlığı ve tarafsızlığı ilkesinden hareketle mali, idari ve bilimsel manada özerkliğinin sağlanması zorunludur.

Türkiye açısından bütüncül yaklaşımın bir gereği olarak öncelikle yeterli eğitimi almış ve her türlü teknik donanıma sahip kolluk birimleri, bilirkişi kurumları ve yargı teşkilatı oluşturulmak zorundadır. Her ne kadar bugün uzman kolluk birimlerinin edinilmesi bakımından Siber Suçlarla Mücadele Daire Başkanlığı gibi kurumların oluşturulmuş olmasına rağmen, iş yükü karşısında sayıca ve teknik bilgi açısından yetersizlikleri nedeniyle bu kurumların etkin çalışamaz konumda oldukları ve yeteri kadar ülkede teşkilatlanamadıkları açıktır.

Bilişim suçlarıyla mücadele kapsamında günümüz koşulları göz önüne alındığında; güncel ve yeterli bir mevzuatın oluşturulması, teknik, eğitimli ve donanımlı adli bilişim personeli ile uzman savcılık ve ihtisas mahkemelerinin bulunması, güvenli yazılım ve diğer gereklerin birlikte gerçekleştirilmesi birer zorunluluk olarak gözükmektedir.

Kaynakça

Akarslan, Hüseyin. 2012. Bilişim Suçları, Seçkin Yayıncılık, Ankara.

Akdeniz, Gökşin. 2013. "Hacker Etiği", Ali Rıza Keleş, Yetkin Sal (Ed.), Hack Kültürü ve Hacktivizm: Yeni Bir Siyaset Biçimi, Alternatif Bilişim, İstanbul, s. 9-15.

Alaca, Bahaddin. 2008. Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları ile), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Atasoy, Fahri. 2007. "Kültürler Üzerinde Bilişim Devriminin Etkileri", Modern Türklük Araştırmaları Dergisi, C: 4, S: 2, s. 163-178.

Avcıoğlu, Gürcan Şevket. 2011. Küresel Bilgi Teknolojileri ve Küresel Değerler, Çizgi Kitabevi, Konya.31

Bahaddin Alaca. 2008. Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle), Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Ankara.

Castells, Manuel. 2013. İsyan ve Umut Ağları İnternet Çağında Toplumsal Hareketler, Çev: Ebru Kılıç, Koç Üniversitesi Yayınları, İstanbul.

Çakır, Hüseyin, Ercan Sert. 2011. "Bilişim Suçları", Oğuzhan Ömer Demir, Murat Sever (Ed.), Örgütlü Suçlar ve Yeni Trendler, Polis Akademisi Yayınları, Ankara, s. 143-170.

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

Dülger, Murat Volkan. 2005. "Türk Ceza Kanunu'nda Yer Alan Bilişim Suçları ve Eleştirisi", http://www.dulger.av.tr/pdf/ytkbilisimsucelestirisi.pdf (19.09.2015)

Ege, Göknur Bostancı. 2008. "Dijital Ayrım", Ege Üniversitesi Sosyoloji Dergisi, S: 19, s. 43-57.

Erdağ, Ali İhsan. 2010. "Bilişim Alanında Suçlar (Türk ve Alman Hukukunda)", Gazi Üniversitesi Hukuk Fakültesi Dergisi, S: 2, s.275-303.

Ersoy, Yüksel. 1994. "Genel Hukuki Koruma Çerçevesinde Bilişim Suçları", Ankara Üniversitesi SBF Dergisi, C: 49, S: 3, s. 149-183.

http://www.aa.com.tr/tr/dunya/obama-siber-guvenlik-paketini-imzaladi/75089, (27.09.2015)

http://www.medyafaresi.com/haber/kim-kardashian-ve-rihannanin-ciplak-fotograflari-hacklendi/583266, (28.09.2015)

http://www.siberkolluk.com/bilisim-suclari-genel-ozellikleri.html, (28.09.2015)

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.560513443bc8a4.02956117, (25.09.2015)

http://www.turkishny.com/special-news/56-special-news/114161-birligin-durumu-konusmasinda-obamadan-ekonomi-recetesi#.VggzKMvtmkp, (27.09.2015)

İçişleri Bakanlığı. 2006. wwwe…, Arem Yayınları, Ankara.

İsmail Tulum. 2006. Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Karagülmez, Ali. 2011. Bilişim Suçları ve Soruşturma-Kovuşturma Evreleri, Seçkin Yayıncılık, Ankara.

Koçak, Hüseyin. 2011. "Kablosuz İletişim ve İnternet Teknolojilerindeki Yeniliklerin Toplumsal Yaşama Katkıları", Türkiye Sosyal Araştırmalar Dergisi, Yıl:15, S: 3, s.37-48.

TBMM. 2012. Bilgi Toplumu Olma Yolunda Bilişim Sektöründeki Gelişmeler ile İnternet Kullanımının Başta Çocuklar, Gençler ve Aile Yapısı Üzerinde Olmak Üzere Sosyal Etkilerinin Araştırılması Amacıyla Kurulan Meclis Araştırması Komisyon Raporu, TBMM, Ankara.

Tekeli, Ömer. 2011. "Bilişim Suçlarıyla Mücadelede Polisin Yeri", Sayder Dış Denetim Dergisi, S. 2011 Temmuz-Ağustos-Eylül, s.183-192.

Tulum, İsmail. 2006. Bilişim Suçları ile Mücadele, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul.

Turhan, Oğuz. 2006. Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar), Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği, Planlama Uzmanlığı Tezi, Ankara.

Yarsuvat, Duygun. 2011. "Hukuk'ta Bilgisayar Kullanımı ile Ortaya Çıkan Sorunlar ve Türk Hukuku", http://www.yarsuvat-law.com.tr/articles/article7.pdf, (26.09.2015)

Yazıcıoğlu, Yılmaz. 1997. Bilgisayar Suçları Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile, İstanbul.

Yılmaz, Sait. 2010. "Wikeleaks'ı Okumak", https://www.academia.edu/7649344/Wikileaksi_Okumak, (04.04.2016)