OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 10
Cilt *Volume*:15
Sayı *Issue* :10 Yıl Özel Sayısı
Haziran *June* 2020
Makalenin Geliş Tarihi *Received Date*: 30/12/2019
Makalenin Kabul Tarihi *Accepted Date*: 24/06/2020

Türkiye'de Bilişim Suçlarının Kriminolojik Açıdan Değerlendirilmesi: Bilişim Suçlarının Hukuksal ve Sosyolojik Boyutlarının Analizi[1]

DOI: 10.26466/opus.688815

*

Furkan Yılmaz* – Fuat Güllüpınar **
* Doktora Öğrencisi, Gazi Üniversitesi Bilişim Enstitüsü, Ankara/Türkiye
E-Posta: furkanyilmaz89@hotmail.com **ORCID:** 0000-0002-9204-9180
** Doç.Dr., Anadolu Üniversitesi, Edebiyat Fakültesi, Eskişehir
E-Posta: fgullupinar@gmail.com **ORCID:** 0000-0003-3661-7232

Öz

Bilişim teknolojileri hayatımızı her geçen gün daha yoğun bir biçimde dijitalleşmektedir ancak bilişim alanındaki bu devasa gelişmeler bir yandan hayatımızı kolaylaştırırken bir yandan da beraberinde bazı önemli riskleri de getirmektedir. Bu açıdan, bilişim teknolojileri hem hayatımızı oldukça kolaylaştıran bir şekilde konforlu bir hayat sunarken, öte yandan bilişim teknolojileri her türlü suçun işlenebileceği olanak ve fırsatlar için potansiyel olarak güçlü bir mecra ve zemin haline gelmiştir. Bu çalışmada, Türk Ceza Kanunu ve diğer iç mevzuattaki bilişim suçlarına ilişkin hükümler incelenerek, başta internet kanunu olarak bilinen 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ele alınarak toplum üzerindeki etkileri sosyolojik açıdan analiz edilmeye çalışılmıştır. Bilişim suçları ile ilgili ceza kanunları kriminolojik ve sosyolojik sonuçları ve etkileri açısından incelenerek, bazı maddelerdeki dikkat çeken eksiklikler, bilişim suçlarının işlenmesini caydırma konusundaki yeterlilikleri ve yetersizlikleri açısından ele alınmıştır. Çalışmada, kanunların sosyolojik olarak ne tür ihtiyaçları karşılayabildikleri ve yaşanan olgular karşısındaki zayıflıkları ayrıntılı olarak ele alınacaktır. Son olarak, bilişim suçlarının hukuksal ve sosyolojik açıdan nasıl önlenebileceğine ilişkin bir takım önerilere de yer verilmiştir.

Anahtar Kelimeler: *Bilişim suçu, ceza kanunu, kriminoloji, suç sosyolojisi, Türkiye*

[1] *Bu çalışma Anadolu Üniversitesi Sosyal Bilimler Enstitüsüne sunulan "Türkiye'deki Bilişim Suçlarının Sosyolojik Bir Analizi: Tehditler ve Çözüm Stratejileri" başlıklı yüksek lisans tezinden yararlanılarak hazırlanmıştır.*

OPUS
Uluslararası Toplum Araştırmaları Dergisi
International Journal of Society Researches

ISSN:2528-9527
E-ISSN : 2528-9535
Yıl *Year* : 10
Cilt *Volume*:15
Sayı *Issue* :10 Yıl Özel Sayısı
Haziran *June* 2020
Makalenin Geliş Tarihi *Received Date*: 30/12/2019
Makalenin Kabul Tarihi *Accepted Date*: 24/06/2020

Criminological Evaluation of Cyber Crimes in Turkey: Analysis of Legal and Sociological Dimensions of Cybercrimes

*

Abstract

Information technologies encompass our lives in every aspect and our lives are becoming digitalized. However, these gigantic developments in the field of informatics make our lives easier and at the same time bring some important risks. In this respect, while information technologies provide a comfortable life in a way that makes our lives quite easy, on the other hand, information technologies have become a potentially strong medium and area for the opportunities where all kinds of crimes can be committed. In this study, the articles of the Turkish Criminal Code and other internal legislation on informatics were examined. The effects of the Law on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication, which are known as "The Internet Law", were analyzed from a sociological perspective. Criminal laws related to cybercrimes are examined in terms of their criminological and sociological consequences and effects, and some of the shortcomings that are noteworthy are discussed in terms of their competencies and inadequacies in deterring the committing of cybercrimes. In this study, what kind of the sociological needs can be met by the laws and weaknesses of the laws against the facts will be discussed in detail. Finally, some recommendations on how to prevent cybercrimes from a legal and sociological point of view are also included.

Keywords: *Cybercrime, penal code, criminology, sociology of crime, Turkey*

Giriş

Bilgi teknolojilerinin hızla gelişimi, bu gelişmelere aynı hızda ayak uydurabilecek bir toplum yapısı geliştirme ihtiyacını doğurmuştur. Özellikle bilişim teknolojilerinin gelişmesi sonucunda yaşanan ekonomik ve kültürel ve sosyal alandaki değişmeler, toplumun her alanında değişimini beraberinde getirmektedir. Dijital iletişim alanındaki devrimler hayatımızı geri dönülmeyecek bir biçimde değiştirdi ve değiştirmeye devam ediyor. İnternet dünyası ve bilişim teknolojilerinde yaşanan değişimler, sosyal ilişkilerimizi doğrudan etkiliyor ve sosyal hayatımızı şekillendiriyor. Fikir ve ifade özgürlüğü internet sayesinde hiç olmadığı kadar gelişti. Bu yeni özgürlük alanı, bir yandan da dev bilgi deposu ve kayıt alanı olarak gelişimini sürdürmektedir. Küreselleşme süreci de bu alanı hem genişletmiş hem de karmaşık hale getirmiştir. Küreselleşme, son yıllarda üzerinde en çok tartışılan, çok farklı anlam ve değerler yüklenen, çok farklı tanımlamalara ve nitelemelere konu olan kavramların başında yer almaktadır.

Kısacası, "dünyanın tek bir mekân olarak algılanabilecek ölçüde sıkışıp küçülmesi anlamına gelen bir süreci" (Tutar, 2002, s.2) ifadesiyle tanımlanan küreselleşme, ekonomik, siyasal, sosyal ve kültürel değerlerin ve bu değerler çerçevesinde oluşmuş birikimlerin ulusal sınırlar dışına taşarak dünya geneline yayılması şeklinde değerlendirilmektedir. Ekonomik açıdan bakıldığında, bilişim teknolojisindeki gelişmelerle birlikte, sanayi ekonomisi yerini bilgi ekonomisine bırakırken, ekonominin üçlü sacayağı olarak nitelendirdiğimiz üretim, tüketim, dağıtım ilişkileri ve ekonomik yapının tümü, bilgi temeli üzerine yeniden yapılanmış ve bilgi rekabetin temel faktörü durumuna gelmiştir (Tekin ve Çiçek, 2006).

Kültürel değişimler açısından bakıldığında, özellikle internet medyasının getirdiği özgür ve geniş alan, sosyal medyanın en büyük paylaşım alanı olmasını sağlamıştır. Bilişim teknolojilerinin gelişimi, aslında bir anlamda da toplumsal ilişkilerin ve yapılanmaların yeniden şekillenmesi şeklinde yorumlanabilir (Şehitoğlu, 2005). Her ne kadar internet üzerinden kurulan sanal gruplardaki ve cemaatlerdeki iletişimin ve ilişkilerin yüz yüze ilişkiler kadar sahici ve samimi olmadığı düşünülse de, güvensiz dışarı yerine, güvenli evde kurulan ve sürdürülen ilişkiler günümüz toplumunda tercih sebebi olabilmektedir. Hatta şöyle ki, sanal cemaatler dışarıda bir ilişki kurmak için yeterli

fiziksel gücü olmayan yaşlılar ve sakatlar için de yeni fırsatlar sunabilmektedir (Bozkurt, 1999, s.68).

Özellikle tüm insanlık tarihi boyunca, gerçekleşmiş olan toplam teknolojik gelişmenin önemli bölümünün 20. yüzyıl içerisinde gerçekleştiği göz önüne alındığında, bilişim teknolojilerinin yarattığı etkiler; toplumsal yapıların kırılganlığı ve geçişkenliği çatışmalara neden olabilmektedir (Çubukçu, 2010).

Bilişim teknolojilerinin hızlı bir şekilde gelişmesi sonucunda internet faydalarının yanı sıra art niyetli kişilere ulaşılması kolay, izlerinin diğer suçlara göre daha zor bulunacağı, sanal bir suç işleme ortamı sunmuştur (UNESCO, 2004). Teknolojiye bağlı olarak bilişim alanına kazandırılan her türlü araca bağlı olarak işlenen suç şekilleri de sürekli gelişmektedir. İnternetin özellikle hukuksal alanda pek çok davranış şekilleri ile birlikte yeni sorunları da beraberinde getirdiği söylenebilir (Özberk, 2002, s.101).

Siber suçlar ya da bilişim suçları yaygın olarak; sahte internet siteleri (phishing[2], pharming[3] amaçlı) oluşturma, kişilerin şifreleri ve kullanıcı bilgileri ele geçirme, web sitelerine ve sunucularına yönelik saldırılar düzenleme (defacement-bozma), virüs taşıyan e-postalar (spam mail) yollayarak elektronik saldırılar yapma şeklinde gerçekleştirilir. Mağdurun bilgisi ve rızası dışında ele geçirilen şifre, kullanıcı adı, resim, görüntü gibi bilgi ve dokümanlar şahsa karşı; karalama, şantaj gibi suçları işlemek üzere kullanılır.

Bilişim suçlarının kendine özgü niteliği nedeniyle fail kurbanlarından fiziksel olarak uzaktadır ama aynı zamanda işlenen fiilin suç olup olmadığı geleneksel suçlarda olduğu gibi siyah ve beyaz ayrımından ziyade gri alan içerisinde kalmaktadır (Seymour, 2013, s.27). Failler bu eylemi gerçekleştirirken kasıtlı hareket etmektedirler ve belirli bir amaca yönelme içerisindedirler. Ancak, çoğu suç faillerinin genellikle geleneksel suçlarla ilgili bir sabıkaları yoktur.

Imhof'un (2010, s.97) da işaret ettiği üzere, internet bilişim suçlarının faillerine, güç eksikliklerini kapatabilecekleri fırsatları sunmaktır. Örneğin, baskıcı bir ülkede bir hacker internet erişimine sahip olabilmektedir ve bunu, uygulayabilecekleri kontrol miktarını arttırarak kontrol oranını arttırabileceği

---

[2]Phishing (password harvesed fishing): başka bir internet sitesini taklit ederek, o siteye kullanıcı tarafından girilen parolaları ve diğer bilgileri elde etmek.

[3]Pharming: kullanıcıya ait parolaları ve diğer bilgileri elde etmek için hedefin DNS ayarları değiştirilerek, ulaşmak istediğinden farklı bir siteye yönlendirmek.

bir araç olarak görmektedir. Genel olarak, bir birey, zararlı yazımları diğer makineleri kontrol etmek amacıyla geliştirerek, mesela botnet yaratarak, saldırgan davranışlarda bulunabilir. Eğer bu birey çok büyük bir botnet yaratırsa çok fazla güce sahip olabilir. Eğer yeterince güçlü olursa büyük organizasyonlarda iletişim altyapılarını kapatmamak için bu şirketlerden dilediklerini isteyebilir. Bunu isteyebilecek güçte olmak veya bu gücün farkında olmak onların kendilerinin kontrol duygularını önemli ölçüde arttırabilir.

Bilişim alanında suçların en önemli özelliği suçlu ile mağdur arasında mekânsal mesafenin bulunmasıdır (Öztürk, 2007, s.16). Ayrıca, bilişim teknolojisinin işleyiş tarzı sebebiyle, suç çoğu zaman birçok ülkeyi ilgilendirebilmektedir (Berber, 2004, s.151). Bilişim suçları da, terörist faaliyetler, kaçakçılık, insan ticareti, organize suçlar gibi sınır aşan niteliktedir.

Ceza kanunlarının mülkiliği ilkesinin genel ilke olması, evrensellik ilkesinin ise çoğu ülkede mülkilik ilkesine göre tali ve tamamlayıcı nitelik göstermesinden dolayı bilişim suçlarının soruşturma ve kovuşturulması için uluslararası işbirliğini sağlayacak düzenlemeler hayati önem taşımaktadır (Topaloğlu, 1997, s.19). Bilişim suçlarının gelişimine ilişkin olarak yapılacak olan temellendirme de "internet ile sunulan hizmetin ulusal sınırları aşarak herhangi bir kitle haberleşme aracına kıyasla daha fazla etki yapması" bilişim suçlarının kapsamını bir hayli genişletmiştir (Gercke, 2009).

1981 yılında AET (Avrupa Ekonomik Topluluğu şimdiki adı ile Avrupa Birliği-AB) tarafından düzenlenen "Bilgisayarlaşan Toplumda İhlaller" adlı toplantıda belirlenen kavramlar, günümüzde de geçerliliğini ilk günkü öneminde korumaktadır (Akıncı ve diğerleri, 2004, s.171). 1985 yılında Avrupa Topluluğu Suç Problemleri Komitesi, bünyesinde, bilişim suçları alanında çalışmalar yapması ve üye devletlere tavsiye bulunması amacıyla bir alt komisyon oluşturulmuş (Yazıcıoğlu, 1997, s.131, Akıncı vd., 2004, s.171), yine aynı yıl içerisinde Milano'da 7'incisi düzenlenen Birleşmiş Milletler (BM) Toplantısında bilgisayar suçlarının sonuçları tartışılmıştır (Yazıcıoğlu, 1997, s.19).

Ancak bilişim suçları konusunda şu ana kadar yapılan en etkin hukuki düzenlemenin, Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde imzaya açılan Avrupa Konseyi Siber Suçlar Sözleşmesi olduğu söylenebilir. Hazırlanan sözleşmenin hedefi "ortak bir ceza politikasının oluşturulması ile toplumun siber suça karşı korunması, özellikle gerekli mevzuatın kabul edilmesi" ve uluslararası işbirliğinin geliştirilmesidir. Türkiye, Avrupa Konseyi Siber

Suçlar Sözleşmesine 10 Kasım 2010 tarihinde imza koyarak taraf olduğu hâlde, Sözleşmeyi iç hukukun parçası hâline getirecek işlemleri tamamlayıp, Sözleşmeyi iç hukuka aktaramamıştır. 22 Nisan 2014 tarihinde mecliste yürürlüğe girmiştir, ancak sözleşmenin iç hukuka entegrasyonunda ve uygulanmasında sıkıntılar devam etmektedir. Bilişim suçlarının tarihsel gelişimine baktığımızda yaklaşık 40 yıllık süre içerisinde bu duruma gelinmiştir. Bilişim suçlarının bu kadar önemli olarak kabul edilmesinin bir diğer sebebi geçmişinde meydana getirdiği tehlikelerdir.

Toplumun Dijitalleşmesi

Castells'in de işaret ettiği üzere (2013, s.1), bilgiyi temel alan teknoloji devrimi toplumun temel dinamiklerini yeniden şekillendirmiştir. İnternet ve iletişim teknolojilerindeki devrimlerle birlikte insanların iletişim biçimleri radikal bir biçimde değişmiştir. İnsanlar arası iletişimin mesafe tanımaksızın, çok boyutlu hale gelmesi sosyolojik bir varlık olan insan için hayatta büyük değişimlerin habercisidir. Denizaşırı ülkelerden görüntülü konuşmak mümkün hale gelmiştir. On binlerce kilometre uzaklıkta bulunan bir veri saniyeler içinde başka mekânlara aktarılabilmektedir. İnternetin sahip olduğu bu imkânların yanında günlük hayatımıza ilişkin birçok ihtiyacımızı da gidermekteyiz. İnternet üzerinden ödeme yapan, bilet alan, alışveriş yapan, sınava başvuran, araştırma yapanların sayısı günden güne artmaktadır.

2008'den beri Türkiye'de faaliyet gösteren E-devlet uygulaması da bu dijitalleşen hayatımızın bizlere sunduğu kolaylıklardan. Vatandaşlar E-devlet uygulaması sayesinde devletle ilgili işlerini internet üzerinden takip edebilmektedir. Vatandaşlar kişisel bilgilerine ilişkin sorgular yapabilmektedir E-devlet olanakları sayesinde yaklaşık 44 milyon kullanıcıya 625 kurumdan toplam 4905 hizmet sunulmaktadır.[4]

Kısacası hayatımıza bilişim her gün daha fazla girmekte ve hayatımız bir bakıma dijitalleşmektedir ancak bilişim alanındaki bu devasa gelişmeler bir yandan hayatımızı kolaylaştırmakta bir yandan da beraberinde bazı riskleri de getirmektedir.

[4] https://www.turkiye.gov.tr/ *(Erişim tarihi: 10.09.2019)*

Dijitalleşen Türkiye

Türkiye'deki bilişim teknolojileri alışkanlıklarına ilişkin TÜİK tarafından yapılan hane halkı araştırması yapılmıştır. 16 - 74 yaş aralığındaki bireylere yapılan 2018 yılındaki bu araştırmanın sonuçları ise şu şekildedir.[5]

Bilgisayar kullanma oranı %59,6 olup, erkeklerde %68,6 iken kadınlarda %50,6 olmuştur. İnternet kullanımı ortalama %72,9 iken, erkeklerin %80,4'ü internet kullanmaktadır. Kadınların oranı ise %65,5'dir. Türkiye genelindeki internet erişimi olan hanelerin oranı %83,8'dir. Cep telefonu veya akıllı telefona sahip olan hanelerin oranı %98,7 iken, %19,2'sinde masaüstü bilgisayar bulunmaktadır. Ayrıca %28,4'ünde tablet bilgisayar ve %32,1'inde ise internete bağlanabilen televizyon bulunmaktadır.

TÜİK, 2019 yılında ise 16 - 74 yaş aralığındaki bireylerin yanı sıra 06 – 15 yaş arasındaki çocukları da araştırmaya dahil etmiştir. Bu veriler ışığında elde edilen veriler ise şu şekildedir.[6]

İnternet kullanımı ortalama %75,3e çıkmışken, erkeklerin %81,8'i internet kullanmaktadır. Kadınların oranı ise %68,9'dur. Türkiye genelindeki internet erişimi olan hanelerin oranı %88,3'tür. Cep telefonu veya akıllı telefona sahip olan hanelerin oranı %98,7 iken, %17,6'sinde masaüstü bilgisayar bulunmaktadır. Ayrıca %26,7'sinde tablet bilgisayar ve %37,7'unda ise internete bağlanabilen televizyon bulunmaktadır.

Son olarak, bilgisayar kullanmaya başlama yaşı ortalama 8 olarak tespit edilmiştir.[7] Bu da teknolojinin git gide hayatımızın her alanında bizi içine almaya başladığının bir başka göstergesidir.

Bilişim Suçu Faillerini Suç İşlemeye İten Nedenler

Bilinen ilk bilişim suçu, 18 Ekim 1966 tarihli Minneapolis Tribune'de yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansımıştır (Kurt, 2005: 157). Bilişim suçunun

[5] *Türkiye'nin İnternet Kullanım Alışkanlıkları - TÜİK 2018 https://www.guvenliweb.org.tr/haber-detay/turkiyenin-internet-kullanim-aliskanliklari-tuik-2018 (Erişim tarihi: 10.03.2019)*

[6] *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması http://www.tuik.gov.tr/PreTablo.do?alt_id=1028 (Erişim Tarihi: 10.03.2019)*

[7] *http://www.tuik.gov.tr/PreHaberBultenleri.do?id=15866 (Erişim Tarihi: 09.09.2019)*

failleri çeşitli nedenlerle bu suçları işlemektedirler. Bu nedenleri suçun öncesindeki kişisel nedenler ve suç sonrasındaki nedenler ceza almama inancı olarak iki kategoride ele alabiliriz.

Suç öncesi nedenlere bakıldığında, bu suçu işlemedeki amaç her ne kadar maddi menfaat sağlamak gibi gözükse de; birçok diğer sebep de bu suçun işlenişinde etkili olabilmektedir. Maddi çıkarın ötesinde özellikle bilişim suçlarının kanunda tanımlanmış olan eylemlerine bakarsak, "yalnızca kişisel bir zevk almak ve tatmin olmak, yapabildim diyebilmek için hareket eden bilişim korsanlarının hukuka aykırı olarak verileri ele geçirmek gibi çeşitli eylemlerin" (Dülger, 2013, s.119) cezalandırılması amacı güdüldüğü görülmektedir.

Jordan ve Taylor (2010, s.231), korsanların bilgisayar ve ağlarına duydukları ilgi ve meraktan dolayı bu suça meyil ettiklerini ileri sürmüştür. Hatta bu merak duygusunun normal yaşantılarındaki heyecanlarından çok daha baskın olduğunu daha fazla heyecan vermesi sebebiyle çevrimiçi fiiller gerçekleştirdiğini belirtmektedir.

Clough ise bilgisayar korsanı için verinin içeriğinin bilinmesinden ziyade veriye ulaşılabilmesi daha önemli olduğunu ileri sürmüştür (aktaran Dülger, 2013, s.119). Bunun göstergesi olarak da Zone-h gibi internet sitelerinde korsanlar tarafından hacklenen sitelerin duyurularının yapılıyor olması sayılabilir. Bu şekilde fail kendini ispatlamış olmakta ve bu alanda popülarite kazanmaya çalışmaktadır. Aslında bu pek çok korsan için en önemli motivasyondur. Bu şekilde topluluk içinde kabul görülür ve hiyerarşide daha üst pozisyona gelebilir (Jordan ve Taylor, 2010, s.231). Eğer ki, siber saldırıya maruz bırakılan hedef, CIA (Central Intelligence Agency) gibi ulusal veya uluslararası arenada önemli bir yerde ise güç sahibi olabilmenin çekiciliği daha da dikkate alınması gereken bir faktördür. Açılımı Merkezi İstihbarat Teşkilatı olan CIA'in korsan saldırılar sonucu açılımı Merkezi Budalalık Teşkilatı olan CSA (Central Stupidity Agency)'ye çevrilmesi bu güç hevesinin bir göstergesidir (Jordan ve Taylor, 2010, s. 221).

Hactivizm de ise; hackleme eylemleri siyasi veya ideolojik bir amaç doğrultusunda gerçekleştirilmekte, bu ses getiren eylemler vasıtasıyla propaganda yapılmaktadır. Bu eylemlerde hedefler genellikle kamu kurumlarına veya dünya çapında faaliyet gösteren büyük şirketlere ait internet siteleri olabilmektedir.

Siber terörizm kavramı ise, terör amaçlı eylemlerin bilişim yöntemleri kullanılarak gerçekleştirilmesine denilmektedir. Özcan ise siber terörizmi "bilgi sistemleri doğrultusunda elektronik araçların bilgisayar programlarının ya da diğer elektronik iletişim biçimlerinin kullanılması amacıyla ulusal denge ve çıkarların tahrip edilmesini amaçlayan kişisel ve politik olarak motive olmuş amaçlı eylem ve etkinlikler" olarak tanımlamıştır (aktaran Dülger, 2013: 158). Bu eylemlerdeki amaç silahlı terör eylemlerinde olduğu gibi halk içinde korku ve panik yaratarak devlete ve kamu kurumlarına olan güvenin sarsılması amaçlanmaktadır.

Kimi zamanda bu suçun failleri yaptıkları eylemleri iyi niyetli olarak yaptıklarını düşünmekte, sadece sistemin açığını göstermek için yaptıklarını iddia etmektedirler. Bu şekilde iyi niyetli olup herhangi bir zarar vermek istemeyenlere 'beyaz şapkalı hacker' denilmektedir. Bunun tam tersi kastla hareket edenlere ise 'siyah şapkalı hacker denilmektedir. Her iki kast ile hareket edenlere ise 'gri şapkalı hacker' denilmektedir.

Suç sonrasındaki nedenler ele alındığında ilk öne çıkan yaptıkları işte uzman olduklarına inanmalarından dolayı asla yakalanmayacaklarını sanmaktadırlar ve "bilgisayarlar, daha önce hiçbir suçta görülmemiş bir biçimde suçu işleyenlere, kimliklerini gizleme imkânı sunmaktadır…" (Karagülmez, 2005, s.51). Kanundaki cezai karşılıklarının diğer suç tiplerine göre daha hafif oluşu da yakalandıklarında alacakları cezalardan çekinmemelerine sebep olmaktadır.

Soruşturma ve kovuşturma aşamasında delil toplama eylemlerinin oldukça zor olması, yeterli delil elde edilmesinin çok güç olacağı kanaati uyandırmaktadır. Doğru faile ulaşılsa bile fail kendisinin de mağdur olduğu, kendisine ait kimlik, kullanıcı, IP (Internet Protocol) bilgilerinin kullanıldığını iddia edebilmektedir. Çünkü bu alanın ne kadar suiistimallere açık olduğunu gayet iyi bilmektedirler.

Öte yandan failin soruşturma yapan kolluk birimlerinin bilgi ve becerilerinin düşük olduğuna ve bu yüzden kendisine asla ulaşamayacaklarına inanması işledikleri suç sonunda herhangi bir yaptırımla karşılaşmayacaklarına olan güvenlerini daha da artırmaktadır.

Bilişim Suçu Faillerinin Özellikleri

Günümüzde hemen herkes teknolojik cihazları bir şekilde kullanabilmektedir. Hatta akıllı telefonlar sayesinde her zaman yanı başında ve hayatın en mahrem anlarına dahi teknoloji girebilmektedir. İnsanların bunları kullanabilmek için belirli bir düzeyde teknolojik bilgi ve beceriye sahip olmaları gerekmektedir. Ama bu gereken bilgi temel düzeyde olmaktadır. Çünkü artık teknolojik şirketler kullanıcı dostu ara yüzler (user-friendly interface) kullanarak kullanıcıları teknik kısımdan olabildiğince uzak tutmak istemektedir. Hatta bu seviye olabildiğince aşağı çekilmeye çalışılmış, kullanılan ara yüzler için aptal dostu ara yüz (idiot-friendly interface) kavramı dahi ortaya çıkmıştır.

Bilgisayar veya diğer teknolojik cihazları kullanabilen herkes bu suç için fail olamaz, teknoloji konusunda günlük yaşantı ihtiyacının ötesinde bir bilgi ve beceriye sahip olmaları gerekmektedir. Bilişim suçlarına ilişkin yapılan araştırmalar bilişim suçu faillerinin genellikle; genç, eğitimli, teknik yeteneğe sahip ve agresif olduğunu ortaya koymuştur (Karagülmez, 2005, s.51).

Öte yandan kişisel bilgisayarların yaygınlaşmasıyla, bilişim suçu için kullanılan araçlar da yaygınlaşmış ve internetteki açık kaynaklardan ulaşmak ve video içeriklerinden anlayarak kullanmak, konuyla ilgilenen kişilerin yatkınlık düzeyine göre giderek kolay hale gelmektedir. Ama verilere ulaşmak ne kadar kolay olursa olsun bu fiilleri gerçekleştirmek için günlük kullanıcı bilgisinden fazlası gerekmektedir.

Özellikle örneğin hedef alınan banka veya kamu kurumları gibi yüksek düzeyde güvenlikle korunan sistemlere erişmek için ise gereken bilgi düzeyi en üst seviyededir. Kişisel bilgisayarların kullanımıyla birlikte bu tip sistemlere yapılan müdahaleler içeriden gerçekleşmekten daha çok dışarıdan yapılan yetkisiz erişimlerle meydana gelmeye başlamıştır (Dülger, 2013, s.122).

Bilgisayarlar ve teknolojik gelişmelerle ilgili ileri düzeyde bilgi ve beceri ya da ortalamanın üzerinde yatkınlıklarının bulunması faillerde görülen başlıca özelliklerin başında gelmektedir. Bunun yanı sıra Ksander bu özelliklerine meraklı olmayı, detaylarla ilgilenmeyi, kendi meslek veya tutkularıyla ilgili problem veya sıkıntılı konuları çözmeyi, sezgiye dayalı düşünmeye yönelmeyi ve zor konularda orijinal çözümler üretmeyi eklemiştir (aktaran Karagülmez, 2005, s.51).

Ayrıca korsanlar için erkek baskınlığı durumu mevcuttur. Genellikle toplu olarak hareket ederler ve en önemli motivasyonlarından biri de bu topluluktur. Gizliliğe önem verirler; ancak bu iki yönlüdür. Hem yakalanmamak için gizli kalmak, hem de popülarite ve bilginin yayılması için alenilik. Bir korsan grubu üyesi olan Zoetermeer "bilgisayar korsanlığı kendisi bir ödül sayılır, çünkü bazen size gerçekten heyecan verir. Ancak deneyimlerinizi başkalarıyla paylaşırsanız sizi çok daha fazla tatmin eder ve tanınmanızı sağlar… Bu grup olmasaydı işletim sistemlerine girmek için ekran başında bu kadar vakit geçirmem imkânsızdı." (Jordan ve Taylor, 2010, s.227).

Fail özelliklerine ilişkin ülkemizde yapılmış en kapsamlı çalışma Eriş tarafından gerçekleştirilen Türkiye'de Hacker Kültürü isimli doktora tezinde 258 hacker ile yaptığı görüşmedir. Bu görüşmeler sonucunda failler için ön plana çıkan özellikler, genellikle erkek oldukları, 14 - 21 yaş aralığında ve genellikle öğrenci oldukları bilgisine ulaşmıştır. Gelir düzeyleri orta alt seviyede ve eğitimi düzeyi ise lise ve üniversite düzeyindedir (Eriş, 2011).

Eriş'in de belirttiği üzere (2011) özellikle ülkemiz hackerlarının diğer ülke hackerlarından ayıran motivasyonu ise ülkü, milliyetçilik, din gibi faktörlerdir. Dünya genelinde özgürlük ve anarşist motivasyonlar ön plandayken; Türkiye'de ise bilakis milliyetçilik ve muhafazakârlık temel saikler durumundadır.

Bilişim suçu faillerinin özellikleri, caydırıcılıktan etkilenmelerine göre ele alındığında şu şekilde bir sonuç ortaya çıkmaktadır. Bilişim suçu failleri kendilerini bu işin uzmanı olarak gördükleri için, caydırıcılıktan etkilenmeleri düşüktür. Çünkü genelde bilişim suçlarıyla mücadele eden görevlilere kıyasla kendilerinin bilgilerini oldukça iyi olduğuna inanmaktadırlar. Riske attıkları şeyler ne olursa olsun yakalanma risklerinin diğer suçlara kıyasla daha düşük olmasından dolayı caydırıcılıktan etkilenme oranları düşüktür. Hackerların yaş ortalamasının 14 - 21 yaş arasında olduğu ve genel itibariyle bilişim suçu faillerinin yaş ortalamalarının düşük olduğu bilindiğinden, yine yaşlılara göre caydırıcılıktan etkilenmeleri oranı düşüktür. Ayrıca, faillerin büyük çoğunluğunun erkek olmasından dolayı da kadınlara göre caydırmaya yönelik faktörlerden etkilenmeleri düşüktür. Sosyoekonomik durumları genelde geleneksel suçlardaki gibi düşük değildir. Bu özellikleriyle caydırılma oranları yüksektirler. Genel itibariyle bilişim suçu failleri özellikleri caydırıcı etkinin çok fazla etkili olmadığı bir profil çizmektedir.

Türk Ceza Kanununda Bilişim Suçları

Bilişim suçları 5237 sayılı yeni TCK'da, Bilişim Alanında Suçlar ve Özel Hayatın Gizli Alanına Karşı Suçlar bölümlerinde ele alınmıştır. Bu bölümlerde düzenlenen suçlara konu olan fiiller özellikle bilişim sistemleriyle işlenebilir ve genellikle günümüzde bilişim sistemleri dışında işlenebilme olanakları çok kısıtlıdır. Dolayısıyla klasik suçların yanında yalnızca bilişim suçu olarak nitelendirilebilecek suç tipleri de ortaya konulmuştur. Sayılan suçlarla beraber, TCK'nın farklı bölümlerinde bilişim sistemleriyle işlenebilmesi mümkün olan suç tiplerine yer verilmiştir. Ancak yeni suç işleme modellerinin ve gelişen teknolojinin sıkça görülmesi nedeniyle bu tür suçlar arasında net ve kesin bir ayrım yoktur.

Bilişim suçları ile ilişkili olan mevzuat; bilişim suçları, Türk Ceza Kanunu, Fikir ve Sanat Eserleri Kanunu, Kaçakçılık ile Mücadele Kanunu ve Ceza Muhakemesi Kanunu olmak üzere beş ana başlık altında toplanmış ve ilgili başlıklar altında aşağıdaki gibi listelenmiştir.

Kanunda ele alınan bilişim alanındaki suçlar şunlardır:

- TCK (Türk Ceza Kanunu) (Bilişim Suçları)
  - MADDE 243. Yetkisiz erişim –Sisteme girme
  - MADDE 244. Hacking, verileri engelleme, bozma, değiştirme, yok etme
  - MADDE 245. Kredi kartı ve bankaya karşı işlenen suçlar.
  - MADDE 246. Tüzel kişiler hakkındaki tedbirler

- TCK (Bilişim Vasıtalı Suçlar)
  - MADDE 124. Haberleşmenin engellenmesi
  - MADDE 125. Hakaret
  - MADDE 132. Haberleşmenin gizliliğini ihlal.
  - MADDE 133. Kişiler arası konuşmaların dinlenmesi ve kayda alınması.
  - MADDE 135. Kişisel verilerin kaydedilmesi.
  - MADDE 136. Verileri hukuka aykırı olarak verme veya ele geçirme.
  - MADDE 138. Verileri hukuka aykırı olarak verme veya ele geçirme.

- MADDE 142. Nitelikli hırsızlık.
- MADDE 158. Nitelikli dolandırıcılık.
- MADDE 226. Müstehcenlik.

❖ Fikir ve Sanat Eserleri Kanunu
- MADDE 71. Manevi haklara tecavüz.
- MADDE 72. Mali haklara tecavüz.
- MADDE 73. Diğer suçlar.

❖ Ceza Muhakemesi Kanunu
- MADDE 134. Bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma

Bilişim alanında suçlar açısından Türk Ceza Kanununun 243, 244 ve 245. maddelerinin değerlendirilmesi

TCK gerekçesinin bilişim sistemi tanımı aslında bilişim sisteminden çok bilgisayar tarifine yakındır. Bilişim sistemi kavramı ele alınırken, daha geniş anlamda yorumlanmalı, bilgi işlemeye ve depolamaya yarayan her türlü donanımın yanı sıra farklı ülkelerde sunucuları bulunan bulut servisleri de bu kavram içinde ele almalıyız.

Bilişim sistemine girme

Türk Ceza Kanunu madde 243'teki hükümde;

Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya 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 halinde, 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. ibaresi yer almaktadır.

Birinci fıkrada korunan hukuksal değer Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde "Her taraf, iç hukukuna uygun olarak, bir bilişim sisteminin

tamamına veya bir kısmına kasten ve haksız olarak erişimi suç haline getirmek için gerekli görülen yasal tedbirleri almayı kabul eder." şeklinde de belirtildiği üzere bilişim sistemlerinin güvenliğidir.

24.03.2016 tarihinde gerçekleştirilen değişikliğe kadar Türk Ceza Kanunu'nda "… giren ve orada kalmaya devam eden kimseye…" şeklindeyken; Avrupa Siber Suç Sözleşmesi'nin 2. maddesinde ise "kasten ve haksız olarak erişimi" suç kılmaktadır. Yani bizim kanunumuzda 'girme' eyleminin tek başına bu suçu oluşturmadığı ancak ve ancak 'orada kalmaya devam etme' eylemiyle suçun sübuta ereceği anlaşılmaktaydı. Bu açıdan madde "suç = yetkisiz erişim + kalmaya devam etme" şeklinde formüle edilebilir, bunun anlamı da anlık yapılan yetkisiz erişimin suç sayılmaması gerektiğidir (Karagülmez, 2005: 167). Ancak yapılan değişiklikle "ve" tabiri yerine "veya" tabiri getirilerek bu husus düzeltilmiştir.

Maddenin ikinci ve üçüncü fıkrasında nitelikli halleri tanımlanmış, bedeli karşılığında yararlanılan sistemlere karşı işlenmesi halinde örneğin, bir internet sitesinin belirli bir ücret karşılığında müşterilerine sunmuş olduğu dergi, gazete vs. abonelik hizmetine yetkisiz erişim sağlayarak, sunuluna hizmetten yararlanmak eylemi bu suçun nitelikli halini oluşturacaktır. Ancak dikkat edilen nokta bu hal suçun artırıcı değil hafifletici

Aynı şekilde bu yapılan yetkisiz erişimden dolayı verilerin değişmesi veya silinmesi söz konusu olursa da bu suçun nitelikli hali olacak ve cezası artacaktır.

Dikkat edileceği üzere buradaki korunan değer sisteme sağlanan erişimle sınırlıdır. Bilişim sistemine girişlerin cezalandırılması için verilerin ele geçirilmesi şartı kaldırılmakta ve veri ele geçirilsin ya da geçirilmesin bilişim sistemine hukuka aykırı olarak girilmesi ve orada kalınmaya devam edilmesi yani bilişim sisteminin güvenliğinin ihlal edilmesi suç haline getirilmektedir (Dülger, 2013, s.319). Zaten verilerin ele geçirilmesine ilişkin Türk Ceza Kanunu'nun 135. maddesinde 'Kişisel verilerin kaydedilmesi' ve 136. maddesinde 'Verileri hukuka aykırı olarak verme veya ele geçirme' başlıkları altında daha ayrıntılı şekilde düzenlenmiştir.

Bu maddede suç olarak belirtilen eylemin diğer bilişim suçlarından en büyük farkı, kendi başına en sık karşılaşılan bilişim suçu olduğu gibi, diğer bilişim suçları için de araç niteliği taşımaktadır. "bu eylem öğretide geleneksel suçlardaki konut dokunulmazlığının ihlali suçuna benzetilmektedir. Bu suç yalnızca hedeflenerek gerçekleştirilebileceği gibi, bilişimle ilgili olsun ya da

olmasın başka bir suç işlemek için 'araç suç' olarak da işlenebilir. Bu yönüyle hukuka aykırı erişimin konut dokunulmazlığı suçuna daha fazla benzerlik gösterdiği ifade edilmektedir." (Erdoğan, 2012'den aktaran Dülger, 2013, s.321).

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Türk Ceza Kanunu'nun 244. madde hükmünde:

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 halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Maddenin ilk iki fıkrasında hangi eylemlerin bu suçu oluşturacağı belirtilmiştir. İlk fıkrada sistemi korumayı hedeflerken, ikinci fıkrada korunan değer sistemin içindeki verilerdir. Bu açıdan bakıldığında ilk fıkrada soyut yazılım ve veri gibi değerlerin yanında, bunu muhafaza eden sistemlerin somut yani donanımsal özelliklerinin de korunduğunu görmekteyiz.

Dülger bu kanun maddesiyle korunan değerin önemini şöyle açıklamıştır:

> *Günümüzün modern yaşam düzeninin ana konularını oluşturan ekonomi, sağlık, eğitim, bilimsel araştırmalar, idare, savunma gibi pek çok yaşamsal alanda bilişim sistemleri vazgeçilmez alanlar olmuşlar, bu alanların pek çok yerinde geri dönülmez şekilde insanların yerini almışlardır. Bu nedenle bilişim sistemlerine ve içerdiği verilere karşı yapılan saldırılar sonucu bu sistemlerin geçici süreyle de olsa çalışmaması çok büyük zararlara neden olabilmektedir. Özellikle çok iyi üretilmiş bilişim virüsleri, kurtçuklar, Truva atları gibi zarar verici yazılımlar bilişim ağlarında geometrik hızla yayılarak bunları hazırlayan ve verilere zarar vermek amacıyla sanal alana sokan faillerin dahi öngördüğünden daha fazla zarara yol açabilmektedir. Benzer bir şekilde web*

> *sitelerini çökertmek için DDoS saldırıları gibi eylemler pek çok kamu hizmetinin alınmasını önleyebilmekte ya da saldırıya uğrayan siteyi kullanan şirketin ticaret yapmasını engelleyebilmektedir. Yasa koyucu da bu büyük tehlikeyi öngörerek sisteme ve/veya verilere zarar verme eylemlerini bu maddeyle suç haline getirmiştir. (Dülger, 2013, s.386).*

Bu suçun gerçekleşmesini sağlayan eylemler ele alındığında, birinci fıkrada "… engelleyen veya bozan …" ibaresi geçmektedir. Bilişim sisteminin işleyişini engellemek ile kast edilen sistemin faaliyetlerini geçici veya sürekli olarak durdurmasına sebep olmaktır.

Engel olma fiili bilişim sisteminin geneline yönelik olabileceği gibi, onun çalışmasına destek olan, katkı sağlayan başka bir unsura da yönelik olabilir. Bu diğer unsura yapılan müdahalenin suça konu olan bilişim sisteminin işleyişini kısmen veya tamamen engellemiş olması bu suçun oluşması için yeterlidir (Karagülmez, 2005, s.188).

Bozma eylemi ise, aslında bilişim sisteminin kendisinin veya alt unsurlarından birinin yapılan yetkisiz müdahale sonucu zarar görmesi ve bunun neticesinde de sistemin genelinde sağlıksız çalışma meydana gelmesidir. Aslında nihai olarak bu eylem de bir engellemedir. Karagülmez (2005, s.189)'in de dediği gibi Türk Ceza Kanunu'nun 244. maddesinde 'bozan' ibaresi kullanılmadan da, sadece 'engelleme' ibaresi ile yetinilebilirdi. Çünkü sistemin bir kısmının veya tamamının bozulması aynı zamanda sistemin bir kısmının veya tamamının işleyişini engelleyeceğine göre bu sonuca varılması mantıklıdır.

Suçu işleniş amaçları ele alındığında, ilk fıkranın ikinci fıkradan en büyük farkı, veri kavramından ziyade sistem kavramının ön planda tutulmasıdır. İçindeki veriyi göz ardı ederek sistemlerin işlemesinin engellenmesinde amaç ne olabilir? Aslında bu kanun maddesinde genellikle doğrudan maddi menfaat temini için ileride daha detaylıca ele alınacak olan ikinci fıkranın sübuta ermesi daha olasıdır.

Birinci fıkradaki suçun bilişim sisteminin işleyişinin engellenmesi veya bozması fiilinin doğrudan maddi menfaat temini odaklı olmadığından dolayı, gerçekleştirilmesinin en büyük sebebinin 'prestij' ya da 'sesini duyurmak' olduğunu söyleyebiliriz. İnternet sitelerinin de bir bilişim sistemi olduğunu düşünürsek, sırf internet site hacklemelerinin duyurulduğu internet si-

telerinin varlığı, bu suçun gerçekten de 'prestij' maksatlı yapıldığının göstergelerinden biridir. Dünya çapında veya ulusal çapta önemli şirketlerin internet siteleri ya da devlete ait kurumların internet siteleri hacklenerek, siyasi ya da ideolojik mesajların verilmesi olayı yani 'sesini duyurma' maksatlı bu suçun işlenmesi de sıklıkla meydana gelmektedir. Bu maksatla gerçekleştirilen bu olaya hack ve aktivizm kelimelerinin birleşiminden oluşan 'hacktivizm' denilmektedir.

Diğer sebepler ise kişinin kendini deniyor olması, eğlence maksatlı ve ticari kaygılarla yapılan hedef şirketin itibarına zarar vermek amaçlı saldırılardır.

Bu maddenin ikinci fıkrasında ise verilerin bozulması, yok edilmesi, değiştirilmesi, erişilmez kılma sisteme veri yerleştirilmesi ve verileri başka yere gönderilmesi suçları yer almaktadır. Burada korunan veriler ve verilerin güvenliğidir. Ancak bu kanun maddesinde kast edilen veri, sistemin işleyişine doğrudan etkisi olmayan veriler olduğu ilk fıkradaki eyleme göre daha az ceza gerektirmesinden anlaşılmaktadır. Benzer görüşte Erdoğan da (Dülger, 2013: 389) "… bir bilişim sisteminde yer alan her veri, sistemin işleyişini bozmayacağı ve engellemeyeceği için 1. fıkradaki suça nazaran daha az ceza ile cezalandırılmaktadır. Dolayısıyla bu suç tipiyle de verilerin varlığı, düzgünlüğü, doğruluğu ve erişilebilirliği korunmaktadır. …bir başka deyişle 2. fıkra ile sistemin içinde yer alan; ancak sistemin yapı taşı olmayan veriler korunmaktadır."

Maddenin 4. fıkrasında kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde ibaresi geçmektedir. Bu eylemin gerçekleşmesinde kasıt genellikle verilere ve bu sayede de verilerin sahibine zarar vermek olabileceği değerlendirilmektedir. Çünkü bu verilerin maddi değere sahip para veya ona eş değer olabilecek kredi, kontör vs. hakkında işlenmesi durumunda Türk Ceza Kanunu'nu 142/2-e bendinde geçen bilişim sistemine girmek suretiyle nitelikli hırsızlık suçunu oluşturacağı, aynı şekilde elde edilen verilerin kişisel veri niteliğinde olması durumunda ise kanunun 136. maddesindeki Verileri hukuka aykırı olarak verme veya ele geçirme suçunu oluşturacağı değerlendirilmektedir. Ancak Yargıtay Ceza Genel Kurulu tarafından manyetik telefon kartlarının üzerindeki verilerin değiştirilerek herhangi bir ücret ödemeksizin ankesörlü telefonların kullanılmasını bu suç kapsamında değerlendirmesine yönelik 2007 yılındaki kararın gerekçesinde:

Sanığın telefon kulübelerinden topladığı kredisi bitmiş telefon kartlarına barkod ve manyetik bant yapıştırmak suretiyle kontör yükleyip bunları diğer sanık S.. T.. ile birlikte katılan Kurum' ait kulübelerde bulunan telefon cihazlarına sokup kullandıkları, bu yöntemle kısa süre içinde toplam 35210 kontörlük görüşme yapıldığı dosyadaki kanıtlardan anlaşılmaktadır…

Ankesörlü telefonlar, manyetik kart, kredi kartı ve smart kart ile çalışan hizmet telefonlarıdır. Bu telefonlar katılan Kurum tarafından ücretsiz olarak meydanlar, hastaneler, terminaller, garlar, limanlar, metro istasyonları, askeri tesisler, toplu konut alanları gibi halka açık yerlere tesis edilmekte, ARMS olarak adlandırılan merkezi bilgisayar sistemi ile yönetilmektedir. ARMS sisteminin suçun işlendiği bölgede hizmet veren ve kendisine bağlı olan 200 adet D-3 manyetik kartlı ankesör makinesinin çalışma bilgilerini, (kullanılan kontör miktarı, manyetik karta ait barkot numaraları, görüşen ve görüşülen bölgeler ve numaralar, görüşme saati ve süresi vs.) bünyesinde topladığı anlaşılmaktadır. Nitekim kopyalama yapılan manyetik kartların barkod numaraları dahi bu sayede tespit edilmiştir. Suç tarihinde kullanılan sistemin işleyiş biçimine gelince, bu sistemin kullanılabilmesi için iki unsura ihtiyaç vardır. Bunlardan birincisi, manyetik telefon kartı, diğeri ise kontör olarak adlandırılan kredidir. Bunlara sahip olunmadan, bir bilgi işlem biriminin parçası olan ve ARMS denilen sisteme bağlı bulunan ankesörlü makinelerden, Kurum'ca acil durumlarda kredisiz görüşme yapılabilmesine olanak sağlanmış bulunan sınırlı sayıdaki numara dışında görüşme yapılabilmesine olanak yoktur. Bu sistemde, manyetik kart üzerindeki barkodu okuyan makine, manyetik kart üzerinde kullanılmış kredi bilgileri bulunmadığı takdirde, okuduğu kartın kredi sınıflandırma özelliklerine göre 100, 60 veya 30 kontör kredi yüklemesi yapmak suretiyle kullanıma hazır hale getirmekte, kullanım süresince yaptığı hesaplamaların sonucuna göre kalan kredi miktarını saptayıp manyetik karta işlemektedir. Başka ifadeyle sistem, makineye takılan karttaki verilerin alınıp değerlendirilmesi suretiyle işlemektedir.

Somut olayda sanığın, kredisi bitmiş olan manyetik telefon kartları üzerinde yaptığı değişiklerle, sistemin verileri farkı algılamasını sağladığı veya başka bir deyişle sisteme farklı veri yüklediği, bu suretle bilgileri otomatik işleme tabi tutmuş bir sistemi yanıltıp boş manyetik karta kredi yüklemesini sağladığı, böylelikle hukuka aykırı yarar elde ettiği anlaşılmaktadır. Bu durumda, sanığın sabit olan eylemi, gerek suç tarihinde yürürlükte olan 765 sayılı Türk Ceza Yasası'nın 525 b maddesinin ikinci fıkrasında düzenlenen, bilgileri otomatik işleme tabi tutan bir sistemi kullanarak hukuka aykırı yarar sağlamak suçunu, gerekse suçtan

sonra yürürlüğü giren 5237 sayılı Türk Ceza Yasası'nın 244. maddesinin 4. fıkrasında yazılı suçu oluşturmaktadır…" (Yargıtay Ceza Genel Kurulu, Kt. 19.06.2007; E.2007/6-136, k. 207/150'den aktaran Dülger, 2013, s.414).

Bu karardan da anlaşılacağı üzere, suça konu müdahalenin sadece bilişim sistemine yönelik olma şartından ziyade, ona veri girişi yapan etkenlerdeki manipülenin de bilişim sistemine müdahale eylemi meydan gelecek ve bu sayede elde edilen menfaatin de bilişim sistemindeki verilerin değiştirilerek çıkar sağlama suçunu oluşturacaktır.

Banka veya kredi kartlarının kötüye kullanılması

Türk Ceza Kanunu'nu 245. maddesinde:

1. Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.
2. Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve onbin güne kadar adlî para cezası ile cezalandırılır.
3. Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beşbin güne kadar adlî para cezası ile cezalandırılır.
4. Birinci fıkrada yer alan suçun;
    a) Haklarında ayrılık kararı verilmemiş eşlerden birinin,
    b) Üstsoy veya altsoyunun veya bu derecede kayın hısımlarından birinin veya evlat edinen veya evlâtlığın,
    c) Aynı konutta beraber yaşayan kardeşlerden birinin,

Zararına olarak işlenmesi hâlinde, ilgili akraba hakkında cezaya hükmolunmaz.

5. (Ek: 6/12/2006 – 5560/11 md.) Birinci fıkra kapsamına giren fiillerle ilgili olarak bu Kanunun malvarlığına karşı suçlara ilişkin etkin pişmanlık hükümleri uygulanır." ibaresi geçmektedir.

Bu maddeyle korunan hukuksal değer, hırsızlık, dolandırıcılık, güveni kötüye kullanma ve sahtecilik suçlarında korunan hukuksal değerler ile aynıdır. Çünkü bu suç işleniş biçimine göre bu fiillerin birini veya birkaçını kapsayabilmektedir. Düzenlenen hırsızlık ve dolandırıcılık suçlarıyla malvarlığı, güveni kötüye kullanma suçuyla kişilerin birbirine duyduğu kişisel güven sahtecilik suçuyla ise devlet tarafından bireylere yüklenilen hukuk alanında inandırıcılığı olan belgelere güven korunmak istenmektedir (Dülger, 2013: 427). Ama asıl korunan değer, failin suçu işlemedeki olası saiki da göz önüne alındığında malvarlığı olduğunu söylemek yanlış olmaz.

Bu suç işleniş bakımından banka kartı veya kredi kartına yönelik olması gerekmektedir. Banka kartı: kişiye bankadaki hesabıyla ATM türü vezne işlemi gören cihazlar üzerinden doğrudan bağlantı kurması için üzerindeki manyetik şeritte verilere sahip ve verilerin doğrulanması için de şifreye ihtiyaç duyan kartlardır. Günümüzde para çekme işleminin yanında, alışverişe de imkân sağlamaktadır.

Kredi kartı: Banka tarafından müşterisine kısa süreliğine genellikle alışveriş için kredi imkânı sağlayan manyetik şeride ve günümüzde çiplere sahip kartlardır. Borçlanma imkânı sağladığı için olası maddi zarar kapasitesi daha yüksek olup, fiziki alışverişlerde imza yerine pin, internet üzerinden alışverişlerde ise son kullanma tarihi, güvenlik kodunun yanı sıra 3D[8] güvenlik kullanılması yaygınlaşmıştır.

Bu suç tipi, bu kartların fiziksel olarak elde edilmesi, bu kartların kopyalanması ve internet üzerinden alışveriş için yeterli bilgilerin elde edilmesi suretiyle gerçekleşmektedir.

Kartların fiziksel olarak elde edilmesi: Kanun maddesinde her ne suretle olursa olsun ibaresi geçtiğinden, bu eylemi geniş düşünmek gerekmektedir. Sadece hukuka aykırı olarak elde etme değil, kişinin rızası dâhilinde veya işi

[8] *3D güvenlik: internet üzerinden alışverişlerde, o işleme özel oluşturulan kodun müşteri tarafından teyidi ile sağlanan güvenlik (OTP - one time password).*

veya görevi gereği bu kartı elinde bulunduran üçüncü kişi de bu suçu işleyebilmektedir. Kişinin restoranda ödeme yapmak için kartını verdiği garsonun ya da bankalar tarafından üretilmiş olan kartı, sahibine ulaştırması için verilmiş kurye kartı elinde bulundurma açısından hukuki bir eylem içerisindedirler.

Diğer yandan ise, hukuka aykırı olarak elde etme diyebileceğimiz hırsızlık veya cebir veya tehdit kullanarak yağma ile gerçekleşmesi durumunda da bu kartın fiziksel olarak elde edilmesi mümkündür. Bir diğer yöntem ise ATM cihazlarına yerleştirilen kart yuvasında kartın sıkışmasını sağlayan düzenekler vasıtasıyla kartın fiziksel olarak elde edilmesidir.

Kartların kopyalanması: Bu yönteme 'skimming' denilmektedir, bu yöntem ATM'lere yerleştirilen düzenek veya POS cihazlarını[9] kullanan kasiyerler veya işyeri sahipleri tarafından aynı zamanda 'skimming' yapabilen başka bir cihazdan geçirilmesi ile mümkün olmaktadır. Bu kopyalama cihazları kartlarda bulunan manyetik şeridi hafızasına almaktadır. Manyetik şeritte bulunan track data 1 ve track data 2 bilgileri sahte üretilen farklı bir karda kaydedilmektedir; ancak bu kartların kullanılabilmesi için kullanıcının karta ait şifresinin de ele geçirilmiş olması gerekmektedir. Ülkemizde çipli kartların kopyalanmasına ilişkin bir olaya henüz rastlanılmamıştır.

İnternet üzerinden alışveriş için gerekli bilgilerin elde edilmesi: Bu işlem için kredi kartının üzerinde yer alan kart numarası, son kullanma tarihi ve güvenlik kodu bilgileri yeterlidir. Bu bilgilerin temini ise fiziki kartın elde edilmesi, fiziki kartın fotoğraflanması ya da phishing dediğimiz yöntemle gerçeğinin aynısı gibi görünen taklit sitelere veya kontör, fatura ödeme vb. amaçlı görünen sitelere kişinin kart bilgilerini girmesi suretiyle elde edilmektedir. Bu tip suçlara karşı alışveriş siteleri ve bankalar tarafından kullanıcıya işleme özel onay kodu gönderilmesi olan 3D güvenlik ile tedbir alınsa da bunların da aşıldığı olaylara sıkça rastlanılmaktadır.

Yasak cihaz veya programlar

Türk Ceza Kanunu'nu 245/A maddesinde:

[9]POS (Point of sale) cihazı: kredi ve banka kartlarının işlem yapabilmesi için bankayla iletişime geçen cihaz.

"(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır." hükmü geçmektedir.

Bu madde yine 24.03.2016 tarihinde eklenmiştir. Oldukça yerinde yapılan bu ekleme ile bilişim sistemine yönelik fiillerin yanış sıra bu işlemleri kolaylaştırıcı eylemler de suç sayılmıştır. Zaten Alman Ceza Kanunu'nda 202c paragrafında yer alan 'Veri Casusluğunun ve Verilerin İletilirken Ele Geçirilmesinin Hazırlığı' başlığı altında bu tür eylemler düzenlenmektedir. Bu hükümde: "… belirtilen suçların işlenmesini hazırlamak üzere, 1. verilere giriş yapmayı sağlayan şifre ve sair güvenlik kodlarını veya 2. bu tür fiilleri işlemeyi amaçlayan bilgisayar programlarını, üretir, kendisine veya bir başkasına sağlar, satar, bir başkasına verir, yayar veya sair bir şekilde ulaşılabilmesini sağlarsa bir yıla kadar hapis cezası veya adli para cezasına ile cezalandırılır." (Dülger, 2013, s.322). Bu yapılan yerinde değişiklikle bu tip hareketlerin suç sayılması sağlanmış ve caydırıcılık artırılmıştır.

Topluma karşı suçlar - genel ahlaka karşı suçlar

Madde 226. Müstehcenlik

- Bir çocuğa müstehcen görüntü, yazı veya sözleri içeren ürünleri veren ya da bunların içeriğini gösteren, okuyan, okutan veya dinleten,
- Bunların içeriklerini çocukların girebileceği veya görebileceği yerlerde ya da alenen gösteren, görülebilecek şekilde sergileyen, okuyan, okutan, söyleyen, söyleten,
- Bu ürünleri, içeriğine vakıf olunabilecek şekilde satışa veya kiraya arz eden,
- Bu ürünleri, bunların satışına mahsus alışveriş yerleri dışında, satışa arz eden, satan veya kiraya veren,
- Bu ürünleri, sair mal veya hizmet satışları yanında veya dolayısıyla bedelsiz olarak veren veya dağıtan,
- Bu ürünlerin reklamını yapan, Kişi, altı aydan iki yıla kadar hapis ve adlî para cezası ile cezalandırılır.

Bu suç türünün günümüzde en çok sirayet ettiği alan internet olmuştur. Daha çok insana, daha anonim olarak bu tip içerikler sunulabilmektedir. Özellikle çocuğun kullanılması sonucu oluşan müstehcen içeriklere ilişkin, ulusal ve uluslararası çapta tedbirler alınmaktadır. Küresel çapta mücadeleler sürdürülmektedir. Birçok uluslararası şirket, kullanıcı mahremiyetini sadece bu suç tipi için bozmakta, ABD'de yer alan NCMEC (National Center for Missing and Exploited Children) koordinesinde ihbarlar ilgili ülke birimlerine iletilmektedir. Ülkemizde ise Emniyet Genel Müdürlüğü Siber Suçlarla Mücadele Daire Başkanlığı irtibat noktası görevini yürütmektedir. Gelen ihbarları, gereği yapılmak üzere taşra birimlerine sevk etmektedir.

5846 Sayılı Fikir ve Sanat Eserleri Kanunu

Fikir ve Sanat Eserleri Kanunu'na göre, film, müzik CD'leri, yazılım programı vs. her türlü eseri tamamen veya kısmen kopyalama, çoğaltma; çoğaltılmış nüshalarını kiralama, ödünç verme, satma ve diğer yollarla dağıtma hakkı sahibine aittir. İzinsiz olarak bunları kullanmak, kopyalamak, dağıtmak ve satmak suçtur. Bunun yanı sıra, bir bilgisayar programının yetkisi olmayan kişilerce çoğaltılmasını önlemek amacıyla oluşturulmuş programları etkisiz hale getiren program veya teknik donanımları üretmek ve satmak da suçtur.

Kanundaki cezai yaptırımlar öngören maddelere kısaca baktığımızda,

Madde 71. Manevi, mali veya bağlantılı haklara tecavüz

- Yazılımı kamuya sunma hakkı,
- -Yazılım sahibinin adını belirtme hakkı,
- -Değişiklik yapılmaması hakkı,
- -Değiştirmek, kopyalamak, çoğaltmak yaymak, ticaret konusu yapmak, aracılık etmek

Madde 72. Koruyucu programları etkisiz kılmaya yönelik hazırlık hareketleri

- Bilgisayar programının hukuka aykırı çoğaltılmasının önüne geçmek amacıyla oluşturulmuş programları etkisiz hale getirmeye yönelik hareketler.

Madde 73. Diğer suçlar

Şeklinde düzenlenerek bu hakları koruma altına almayı hedeflemiştir. Bu suçların işlenmesi yıllardan beri süre gelmektedir; ancak son yıllarda bu tip

ihlallerin yapılması daha çok internet üzerinden gerçekleşmektedir. Özellikle peer-to-peer[10] paylaşım programları, film-dizi siteleri, e-kitap paylaşımı yapan siteler sıkça karşılaşılan aynı zamanda çok fazla da tercih edilen internet siteleri olarak yayın yapmaktadırlar.

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

2007 Mayıs ayında Resmi Gazetede yayınlanarak yürürlüğe giren ve internet üzerinden yapılan yayınları düzenleyen bu kanun ve üç yönetmeliği ile birlikte ülkemizde bilişim ve internet alanının hukuki yapısının düzenlenmesi yönünde büyük bir adım atılmıştır. 24 Ekim 2007 tarihinde yayınlanan ilk yönetmelikte sitelere yer sağlayıcılar ve erişim sağlayıcılara ait düzenlemeler yapılarak internet servis sağlayıcı şirketler olan TTNET, Superonline gibi şirketlerle, siteler için barınma imkânı sağlayan hosting şirketleri için düzenlemeler getirilmiştir

1 Kasım 2007 tarihinde Kişilere belli bir yerde ve belli bir süre internet ortamı kullanım olanağı sağlayan yer olarak tanımlanmış olan toplu kullanım sağlayıcılarına ilişkin düzenlemeler getirmiştir.

Son yönetmelikte ise, sitenin yayınladığı içeriklere ilişkin düzenlemelere yer verilmiş ve içerik sağlayıcıların içeriğinde suç barındıran içeriklerin kontrolü ve bunun sorumluların tespiti ve suçun soruşturulmasına ilişkin yenilikler getirilmiştir.

Ayrıca kanun bu internet sitelerinin yayınladıkları içeriklerle herhangi bir suça sebebiyet vermesi veya toplum ahlakı ve sağlığı açısından tehdit oluşturması durumunda ilgili siteye erişimin engellenmesini sağlamaktadır. İnternet sayfası üzerinden işlenebilecek olası suçların, daha sonra takip edilebilmesi ve kim tarafından nasıl gerçekleştirildiğinin bilinmesi amacıyla internet sayfalarına erişen tüm kullanıcılara ilişkin kayıtlarının tarih bilgisi ile tutulmasını ve saklanmasını istenmektedir. Tüm erişimlerinin kayıtlarının en az 6 ay en fazla 2 yıl süreyle tutulması gerekmektedir.

Alaca'nın (2008, s.78) da belirttiği gibi kanunun ilk defa düzenlediği konular;

[10]*Peer-to-peer: istemciler arasında veri paylaşmak için kullanılan bir ağ protokolüdür.*

1. İnternet ortamındaki yayınlardan kanunda katalog suçlar olarak nitelendirilen 8 suçla ilgili olarak erişim engelleme kararlarını ve

Madde 8 - (1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar verilir:

a) 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;
   - İntihara yönlendirme (madde 84),
   - Çocukların cinsel istismarı (madde 103, birinci fıkra),
   - Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),
   - Sağlık için tehlikeli madde temini (madde 194),
   - Müstehcenlik (madde 226),
   - Fuhuş (madde 227),
   - Kumar oynanması için yer ve imkân sağlama (madde 228), suçları.

b) 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar.

2. Erişimin engellenmesi kararı ve yerine getirilmesi usulleri belirlenmiştir.
3. İnternet ortamında oynanan kumar konusunda bir özel düzenleme yapılmıştır.
4. Erişimin engelleme işlemlerine itirazın usulü belirlenmiştir.
5. İnternet ortamındaki yayınlara ilişkin olarak cevap ve düzeltme hakkı getirilmiş ve bunun usul ve esasları belirlenmiştir.
6. İnternet ortamındaki yayınların ilkeleri belirlenmiştir.
7. İnternet aktörleri tanımlanarak bu aktörlerin hak, sorumluluk ve yükümlülükleri belirlenmiştir.
8. Erişim ve yer sağlayıcıların faaliyet belgesi almalarına ilişkin usul ve esaslar belirlenmiştir.
9. İnternet aktörlerinin tutmaları gereken trafik bilgilerine ilişkin bir düzenleme gelmiştir.
10. İnternet toplu kullanım sağlayıcıların yükümlülük ve sorumlulukları belirlenmiştir.
11. Ticari amaçla internet toplu kullanım sağlayıcıların izin belgeleri almalarının usulü, yükümlülük ve sorumlulukları ile denetleme usulü belirlenmiştir.

12. Ticari amaçla internet toplu kullanım sağlayıcıların sahibi veya sorumlu müdürün mülki idare amirliklerinin koordinesinde alacakları eğitim belirlenmiştir.
13. Türkiye'de internet filtreleme konusunda usul ve esaslar belirlenmektedir.
14. İnternet filtrelemesine ilişkin üretilen donanım ve yazılımın kriterleri belirlenmektedir.
15. Türkiye'de internet ortamındaki yayınlardan kanunda belirtilen 8 suça ilişkin şikâyetlerin yapılabileceği bilgi ihbar merkezi kurulmuştur.
16. İnternet kurulunun mevzuat düzenlemesi yapılmıştır.
17. Bilişim ve internet alanında uluslararası koordinasyonda bulunacak görevli kuruluş belirlenmiştir.
18. İnternet ortamındaki yayınları izleme hususu düzenlenmiştir.
19. Ticari amaçla internet toplu kullanım sağlayıcılarda hangi tür oyunların oynanabileceği hangi tür oyunların oynanamayacağı düzenlenmektedir.

5271 Sayılı Ceza Muhakemeleri Kanunu

Bilişim yolu ile işlenen suçlarda en etkin usul yöntemlerinden biri olan 5271 sayılı Ceza Muhakemesi Kanunu'nun (CMK) 134 üncü maddesinde bir suç dolayısıyla yapılan soruşturmada delil elde etmek amacıyla şüphelinin kullandığı bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilebileceği belirtilerek, dijital verilerin maddi delil haline getirilebileceği düzenlenmiştir.

Madde 134 – (1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hakim veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine karar verilir. Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

Madde 134 – (1) inci maddesinde; bilgisayar, bilgisayar programları ile bilgisayar kütükleri iadelerinin kullanılması uygulama da ikilemlere sebep olmuş, cep telefonları ve veri depolayan diğer cihazların (CD, DVD, USB Bellek vb.) durumları farklı değerlendirilerek farklı uygulamalar getirilmiştir. Avrupa Konseyi Siber Suçlar Sözleşmesinin 'Saklanan bilgisayar verilerinin aranması ve bunlara el konulması' başlıklı 19 maddesinde bilgisayar sistemi ya da bu sistemin parçası ve bunlarda saklanan veriler ile bilgisayar verilerinin saklandığı cihazlar denilerek geniş bir kapsam sunmuş ve ikilem çıkmasını engellemiştir. Ancak günümüzde bu kavramın da yetersiz kaldığı görülmekte, bunun yerine IoT teknolojileri, kablosuz veri akışları ve bulut teknolojilerini ve gelecek teknolojileri de ele alarak sayısal veri teriminin kullanılmasının daha yerinde olacağı değerlendirilmektedir.

Şüphelinin kullanmış olduğu ifadesi ile şüpheliye yer verilirken üçüncü kişilere ait dijital materyalerin ceza yargılmasında hangi usülle ele alınması gerektiği ile ilgili tereddütlere sebep olmaktadır. Uygulamada ise bu Cumhuriyet Savcısından alınan talimat ile aşılmaktadır.

25.07.2018 tarihli yapılan değişiklikle gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısına yetki verilmiştir. Bu değişiklikte oldukça yerinde yapılan bir değişikliktir. Bu yetkinin daha önceden hakim kararıyla sınırlandırılması, gece karşılaşılan ya da hakime ulaşılamadığı durumlardaki olaylarda adli makamların hareket kabiliyetini artırmıştır. Her ne kadar Cumhuriyet savcısına bu yetki tanınmış ise de, verdiği kararların hakim tarafından aksine onaylanması ve aksi karar verilmemesi de düzenlenmiştir.

Madde 134 – (2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecek olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

Şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş verilere ulaşılamaması durumunda çözümün yapılabilmesi veya kopyanın alınabilmesi için el koyma işleminin yapılacağı belirtilmiştir. Bu durum uygulama da bazı sıkıntılara yol açmaktadır. Öncelikle bir dijital materyalde yer alan bilgiler üzerinde şifre olup olmadığını belirlemek için olay yerinde inceleme yapmak gerekliliği şarttır. Diğer taraftan dijital materyallerde kullanılan işletim sistemleri kendi özelliklerine has olmak üzere bir bilgisayar kullanıcısının

normalde göremeyeceği alanlar içerir. Bu alanlarında inceleme aşamasında araştırılması gerekir.

El koyma şartlarının "Gerçekleştirilen arama neticesinde tüm verilere ulaşılamaması veya adli kopya alma işleminin gerçekleştirilememesi ya da işlemin uzun sürecek olması halinde" şeklinde sayılmasının daha yerinde olacağı değerlendirilmektedir.

Bu nedenle CMK 134'de Suç kapsamında dijital materyallere el koyma ve inceleme ile ilgili kolluk kuvvetlerinin çalışmasını kolaylaştıracak değişikler yapılması gerekmektedir.

Şekil 1. Disk kopyalama cihazı ile CMK Md. 134 uyarınca iki kopya imaj alınmasına ilişkin fotoğraf

İmajı alınan ve şüpheliye ait olan materyallerin şüpheliye veya müştekinin yazılı talebi üzerine kanunla yedeklemesi yapılan kopyanın verilmesini istenilmemesi durumunda nasıl bir yol izleneceğinin belirlenmesi gerekmektedir.

CMK 134. maddesinin 2. fıkrası kapsamında kolluk tarafından söz konusu suç materyalinden kopya alınırken şüpheli veya avukat hazır bulunup bulunmadığı kanunda belirtilmemiştir. Bu durumda yapılan işlemler hakkında

şüpheli veya avukatının çekinceler oluşturarak soruşturmanın selametini etkilemektedir. Şüpheli veya müşteki kopya alma işleminde hazır bulunmuyorsa el konulan materyallerin kopyası alınırken kamera ile kayıt altına alınması konu hakkında ileride doğabilecek sıkıntıları ortadan kaldırması için önemli bir çözüm olabilir. Bu bağlamda uygulamada iş ve işleyişin sağlanması için CMK 134. maddesi aşağıdaki hali ile uygulanması öngörülmektedir.

CMK 134. maddesinin 4. fıkrasında 21/02/2014 tarihli ve 6526 sayılı Kanunun 11 inci maddesiyle dördüncü fıkrasında yer alan "istemesi halinde, bu" ibaresi "Üçüncü fıkraya göre alınan" şeklinde değiştirilmiştir. Bu değişiklikle birlikte imajı alınan her soruşturma konusu ile ilgili olarak şüpheli veya vekiline alınan imajın kopyasının verilmesinin zorunlu hale getirdiği, bu da özellikle çocuk pornografisi veya kişisel verilerin kullanıldığı suçlarda zaten mağdur olanların ileride olası mağduriyetlerine sebep olacaktır. Bu durumların önüne geçilmesi için kopya tesliminden önce barındırdığı verilerin bizatihi suç olup olmadığına ilişkin değerlendirme neticesinde verilmesinin veya Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesinde de yer alan (Bu sözleşme, Türkiye'nin de yer aldığı taraf devletlerinin imzasıyla onaylanmıştır. Onay sonucu taraf devletler en kısa sürede iç hukukuna entegre çalışmalarını yapması gerekmektedir.) suça konusu silinerek verilmesinin uygulanması yerindedir.

Bilişim Alanındaki Kanunların Toplum Üzerindeki Etkisi

İnternet kanunu terimiyle, akıllarda 'biri bizi gözetliyor' ve 'internet sansürü' algıları oluşmaktadır. Bir nevi devletin asimetrik olan tahakkümünü yine, yeniden halka karşı kullanması durumu ortaya çıkmaktadır.

Marx'ın dikkat çektiği sistematik izleme olarak da geçen gözetim hususu aslında, emek ve sermayenin etkileşiminin sonucudur. Eski tip köleliğin yerini gözetim ve denetim faktörüyle emekten azami düzeyde faydalanılması yer almıştır. Foucault'un da bahsettiği gibi 'Panopticon hapishanesi' aslında sürekli gözetim altında olduğu hissiyatının çok güzel bir ifadesidir. Birey olarak sürekli ziyaret ettiği internet sitelerinin birileri tarafından takip ediliyor olma ihtimali, internetin kendine has özerk, denetimsiz ve anonim yapısıyla

çelişmektedir. İnternetin asıl işlevleri, toplum içinde oluşan algı yüzünden yeterince sağlıklı işlememektedir (Bozkurt, 2000).

Bilişim hukuku ya da bilişim suçları denildiğinde internetle birlikte bilişim sistemleri teknolojisi ve kullanımının günümüzde ulaşmış olduğu boyut itibarıyla ilk bakışta kuşkusuz çok geniş bir alan akla gelmektedir. Ülkemizde bilişim alanındaki yasal düzenleme çalışmaları Bilgi Teknolojileri ve İletişim Kurumunun kurulması ile birlikte çok hızlı bir şekilde gelişme göstermiştir. Bilişim alanında suçlar, ülkemiz bakımından ilk olarak, Fransız hukukunun bu konudaki düzenlemelerinden de etkilenerek 6 Haziran 1991 yılında o zamanki 765 sayılı TCK'ya yapılan eklemelerle yaptırım altına alınmıştır. 2005 yılında yürürlüğe giren 5237 sayılı yeni TCK ile bilişim alanında suçlar, bizde ve batı hukukunda yaşanan gelişmeler doğrultusunda bütünüyle yeniden düzenlenmiştir.

Ülkemizde internet üzerinden yapılan yayınlar yoluyla işlenen suçlarla mücadele için 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'a ihtiyaç duyulmuştur. Bu kanunun Anayasa madde 41'de geçen 'Ailenin korunması ve çocuk hakları' ve madde 58' de geçen 'Gençliğin korunması' amir hükümleri gereğince düzenlenmiştir. Asıl amaç internet ortamında belli başlı suçların işlenmesinin önlenerek, internet üzerinde yayınlanan zararlı içeriklerden çocuk ve gençlerin korunmasıdır.

5651 sayılı kanuna ilişkin yukarıda yer alan bölümde belirtilen içerikleri barındıran siteler için erişimin engellenmesine hükmedilebilmektedir. Ayrıca son yıllarda yapılan değişikliklerle, erişim engellenmesi hallerini genişletilmiş, özel hayatın gizliliğini ihlal ve kişilik haklarına saldırı hallerinde gerçek kişiler tarafından içeriğin kaldırılmasını talep edebilme hükmü düzenlenmiştir.

Bu sayede internet üzerinde yayınlanan içerikler neticesi mağduriyetlerin önüne geçilmesi hedeflenmiştir. Bu kanun değişikliklerinden önce bireylerin hakkını aramaları hususunda hukuki eksiklikler bulunmaktaydı, yapılan düzenlemeler sayesinde kişilerin izlemesi gereken adımlar açıkça belirtilmiştir.

Öte yandan, Kanun'da 2014 yılındaki değişikliklerden sonra medyada çokça yeni internet kanununun özgürlüklere müdahalesiyle ilgili haberlere yer verilmiştir. Bilgi Teknolojileri ve İletişim Kurumunun yetkilerinin art-

ması ve hâkim onayına sunulmadan önce gecikmesinde sakınca bulunan hallerde re'sen karar alabileceği alanların genişletilmesinden dolayı bu tip tepkilerle karşılaşılmıştır.

Kanun gereğince, bir internet sitesi erişime engellendiğinde, mağdur, suçlu, üçüncü kişi gibi kavramlar tanımlanamaz duruma gelmektedir. Bir internet sitesinde, bir kullanıcının paylaşımı kanun gereğince suç unsuru içermesi durumunda, site tamamen erişime engellendiğinde o sitenin diğer içerik sağlayanları, üyeleri ve ziyaretçileri mağdur olmaktadır. Ayrıca her erişim engelleme, diğer bireylerin düşünce ve ifade özgürlüğüne bir müdahale oluşturmaktadır.

5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'da değinilmesi gereken ilk husus ismi her ne kadar 'Suçla Mücadele' denilse de kanunun içeriği incelendiğinde suçla 2015 yılındaki değişikliklere kadar nasıl mücadele edileceği hususu netlik kazanmamıştır. 2015 Mart ayındaki değişikliklerle suçun önlenmesi ve failin tespitine ilişkin hükümler getirilmiştir.

Böyle bir kanuna toplum düzeni açısından ihtiyaç olduğu aşikârdır. Tepkilerin devletin ideolojik aygıtlarından olan medyalardan gelmesi ve bu tedbirlerden en çok etkilenecek unsurlardan biri olmasından ötürü bu tepkilerin homojen olarak toplumun tamamının kabul ettiğini varsaymak doğru olmayacaktır. Çünkü tüm tedbirler veya suça ilişkin yaptırımlar, hâkim veya mahkeme kararına ihtiyaç duymaktadır. Bu sebeple bağımsızlığı Anayasal güvence altında olan yargılama organlarına güven hususu esas olmaktadır.

Ama her ne kadar kanun esasında yargı organlarının bağımsızlığından temel alsa da, idari tedbirlerin fazlalığı bazı konularda soru işaretlerini akla getirmektedir. Öte yandan internetteki içeriklerin erişimlerinin engellenmesine ilişkin bir kanunun mevcudiyeti de ister istemez akıllara ifade özgürlüğüne ilişkin sorunları getirmektedir.

Sosyolojik olarak ele aldığımızda da bu kısıtlamaların aslında ters tepmesi de çok muhtemeldir. Kontrol teorilerinde kontrolü elinde olmayan bireyin, kontrolü eline almak için suça yönelebileceğinden bahsedilmektedir. Daha sonraki bölümlerde daha detaylı ele alınacak olsa da, kişiler bu baskılara karşı kısıtlamaları ihlal yönünde fiiller içinde bulunabilmektedirler.

Sonuç

Gelişen ve yaygınlaşan teknolojiye uyum sağlamak için her alanda yasal düzenlemeler yapmak önemli bir zorunluluktur. Özellikle teknoloji araçlığıyla yürütülen işlemlerin güvenli şekilde yapılması ve bilişim suçlarından dolayı mağduriyetinin yaşanmaması için düzenlemelerin yapılması gerekmektedir.

Batır'ın (2005, s.158) dediği gibi internet kendine has özelliklerinden dolayı gerçek dünya hukukuyla düzenlenemez, yeni hukuki düzenlemelere ihtiyaç duyulmaktadır. Çünkü gerçek dünyadaki kanunların sınırları kanunu çıkartan devletin egemenlik sınırları iken; internetin tabi olabileceği böyle bir sınır söz konusu değildir. Bu sebeple internetle ve içeriğiyle mücadeleden söz edebilmek başlı başına bir soru işaretidir.

Diğer yandan gelişen ve giderek yaygınlaşan sosyal medya; sadece bireyler için değil aynı zamanda kurumlar ve markalar için de yükselen bir yıldız haline gelmiştir. Özellikle 2000'li yılların başlarından başından itibaren sosyal medya; kurumsallaşmış şirketler ve markalar için vazgeçilmez bir iletişim aracı haline gelmiş ve artık son dönemlerde sosyal medyada varlık göstermek artık bir zorunluluk halini almıştır.

Sonuç olarak; internette gerçek anlamda bir sansürün ve denetimin uygulanması imkânsızdır. Bu durum aslında internetin tümüyle kontrol edilemezliğini ortaya koyan bir gerçektir. Fakat bu durum internetin kontrolsüz olduğu anlamına gelmemektedir. İnternetin kendi kendine oluşturduğu ve hala oluşturmaya devam ettiği bir oto kontrol mekanizması vardır. Bu bakımdan gerek bilişim ve iletişim teknolojileri genelinde, gerekse internet özelinde geliştirilecek kanuni düzenlemelerin bu özgürlüğü tehdit etmeyecek, tersine koruyacak bir anlayışla yapılması gereklidir.

Dünya genelinde bilişim sistemi üzerinden çocuğun cinsel istismarı ve çocukların kullanıldığı müstehcenlik suçu (çocuk pornografisi) gittikçe mücadelesine önem verilen suçlar olmuştur. Bundan dolayı çocukların korunması adına yasal düzenlemelerin kapsamlı bir şekilde artırılması ve çocukları baştan çıkarmaya yönelik hareket olarak açıklanan Grooming kavramı tanımlanarak Çocukların Cinsel İstismarı TCK madde 103, Cinsel Taciz TCK madde 105, Müstehcenlik TCK madde 226/3, Çocukların Kullanıldığı Müstehcenlik maddesi kapsamına eklenmesi zorunlu hale gelmiştir. Görülmektedir ki bilişim suçları ile mücadelede bilişim

teknolojileri ve hukuki düzenlemelerin beraber kullanımı sayesinde neticeye ulaşmak mümkün olacaktır.

Ayrıca Türk Ceza Kanunu'nda bilişim suçlarına ilişkin düzenlemelere yukarıda yer verilmiştir. Bu maddelerin suçları daha iyi tanımlamaları ve cezai tedbirlerin orantılı olacak şekilde caydırıcılık düzeyleri artırılmalıdır. 243. maddesinde düzenlenen bilişim sistemine girme suçunun ilk fıkrasında "…hukuka aykırı olarak giren ve orada kalan…" şeklinde düzenlenmesi suçun gerçekleşmesi için sisteme girmenin tek başına yeterli olmayacağını orada kalmanın da gerekliliği anlamını taşımaktadır. Bu düzenlemenin "…hukuka aykırı olarak giren veya orada kalan…" şeklinde düzenlenmesi daha uygun olacaktır.

Avrupa Konseyi Siber Suçlar Sözleşmesi'nde 'Saklanan bilgisayar verilerinin aranması ve bunlara el konulması' başlıklı 19. maddesinde yetkili mercilere, erişilen bilgisayar sistemindeki söz konusu verilerin erişilemez, kullanılamaz hale getirilmesi ya da silinmesi yetkisinin verilmesi gereği belirtilmiştir. Suça konu materyal içerisindeki verilerin bulunmasının suçu devam ettirebileceği, yeni mağduriyetlere yol açabileceği durumlarda bu tip verilerin silinerek şüpheliye verilmesi daha uygun olacağı değerlendirilmektedir. Özellikle çocuk pornografisi ve kredi kart bilgilerinin kullanılması suçlarında verilerin hali hazırda bulundurulmasının zaten suç olduğu ve yeni mağduriyetlere yol açabileceğinden içindeki verilerin silinmesine yetki sağlayacak düzenlemelerin iç hukukumuza entegre edilmesi gerekmektedir.

Durumsal suç önleme teorisinin en temel özelliği, suçludan ziyade suçu oluşturan faktörleri ele almasıdır. Bu sebeple muhtemel suçlu, uygun hedef ve suça karşı yetenekli bir koruyucunun yokluğu ile suçun meydana geldiğini öne süren rutin aktivite teorisini temel almaktadır.

Bu durumsal suç önlemeyi bilişim suçlarında nasıl etkili olabileceğini ortaya koymak için hangi faktörlerin etkili olduğunu irdelemek gerekir. Muhtemel suçlu, yeterli bilgi ve teknik donanıma sahip, suç işleme kastı olan kişidir. Uygun hedef olarak, teknoloji hayatının içinde olan her bir birey bu suçun mağduru olabilir. Koruyucular ise başta kolluk kuvvetleri olmak üzere bilişim suçuyla mücadele eden görevlilerdir. Bu üç faktör bilişim suçlarının durumsal önlenmesi konusunda ayrı ayrı ele alınmalıdır.

Bireyin muhtemel suçlu olabilmesi için uygun şartların oluşması gerekmektedir. Bireyin teknik bilgiye sahip olması iyi niyetli düşünüldüğünde hem birey hem toplum için artı değerdir. Bu sebeple teknik bilgi konusunda

fırsata engel olmadan söz edilemez. Diğer fırsat ise yeterli donanıma sahip olması, bu genellikle bir bilgisayar veya benzer işlevli bir cihaz ve internet bağlantısı ile sağlanmaktadır. Bu her iki öğeden de bireylerin mahrum bırakılması gibi bir durum söz konusu değildir. Ancak kişinin internete bağlanırken anonim olduğu konusunda şüpheleri varsa, suç işlemedeki motivasyonunda azalma olacaktır. Yukarıda da belirtildiği gibi muhtemel suçlu denetim mekanizmasının işlemesinden dolayı internet kafeye gittiğinde bulunma korkusu taşıyorsa, bu bir fırsat yoksunluğudur. Aynı şekilde, sınır aşan bir eylem içerisindeyse; ancak uluslararası işbirliği failin kolayca tespit edilip, yargı huzuruna çıkarabilecek düzeydeyse yine muhtemel suçlu için negatif bir durum söz konusudur. Diğer bir husus, yakalanması durumunda, alacağı cezaların yaptırım gücü de muhtemel suçlu üzerinde caydırıcı etki yaratabilecektir.

Uygun hedef adayları, teknolojiyi hayatında yer eden her bireydir. Hedefleri uygunluktan çıkartmak için, ilk uygulamaya sokulması gereken eğitim faaliyetleridir. Bireylerin, bilişim teknolojileri ve internet konusunda düzenlenecek eğitimlerle hem kendileri hem de aile bireyleri için bilinçli birer kullanıcı haline getirilmeleri gerekmektedir. Bunun yanı sıra kişisel ve kurumsal ölçekte alınacak sistemsel tedbirlerle suçun işlenme ihtimali minimize edilebilir.

Suça karşı yetenekli koruyucuların başında kolluk birimlerinin bilişim suçlarıyla mücadele birimlerinde çalışan görevlileri gelmektedir. Bu polis teşkilatında Siber Suçlarla Mücadele Daire Başkanlığı ve taşra birimleri tarafından icra edilmektedir. Temelde siber suç soruşturma, siber suç önleme ve adli bilişim olarak üç farklı alanda mücadele gerçekleştirilmektedir. Yetenekli koruyucuların varlığı ancak bu birimlerde çalışan personelin kalifiye olmasıyla sağlanabilir. Bu personelin de kendi alanlarıyla ilgili eğitilmesi gerekmektedir. Bu sayede gerek suç oluşmadan önce tedbirlerle, gerek suç sonrası soruşturma işlemlerinde, gerekse suça konu dijital materyallerin incelenerek delil olarak kabul edilip raporlanması işlemlerinde başarı oranı artacak ve muhtemel suçlu için yakalanmama ihtimali düşecektir. Diğer yandan, koruyucuların bu yeteneklerini daha etkili kullanabilmeleri için de, oldukça önemli diğer bir husus da mevzuatın sağladığı yetkidir. Tüm mücadele işlemleri belirli bir mevzuata dayanarak yerine getirilmektedir. Mevzuatın da birey bazında kişisel hak ve özgürlükleri ihlal etmeden ancak bu suçla da en etkin mücadeleyi sağlayacak şekilde optimize edilmesi gerekmektedir.

EXTENDED ABSTRACT

Criminological Evaluation of Cyber Crimes in Turkey: Analysis of Legal and Sociological Dimensions of Cybercrimes

*

Furkan Yılmaz – Fuat Güllüpınar
Gazi University, Anadolu University

The rapid development of information technologies has caused to the need to develop a legal structure that can keep pace with these developments. The changes in the economic and cultural and social areas, especially as a result of the development of information technologies, bring about its change in every area of the society. Revolutions in the field of digital communication have changed our lives irrevocably and continue to change. The changes in the internet world and information technologies directly affect our social relations and shape our social life. Freedom of opinion and expression has improved more than ever thanks to the internet. This new area of freedom continues to develop as a giant storage and saving area of information. The process of globalization has both expanded and complicated this area. Globalization is one of the most discussed concepts that have been discussed the most in recent years, with many different meanings and values, and subject to many different definitions and qualifications.

Cybercrimes or IT crimes are being commonly performed as creating fake websites (for phishing, pharming purposes), stealing passwords and user information, attacks on websites and servers (defacement-out of services), and electronic attacks by sending electronic emails (spam mail). Information and documents such as password, user name, picture, image seized outside of the victim's knowledge and consent are against the person; used to commit crimes such as smear or blackmail.

The most important feature of cybercrimes is the spatial distance between the criminal and the victim. Also, because of the way information technology works, crime can often concern many countries. Indeed, the

main feature of cybercrimes is that there is no limits. It is now one of the leading cross-border crimes such as smuggling, human trafficking and organized crime. It is less likely to detect cybercrime than traditional crime. The type and format of the evidence to reveal cybercrime, and the methods of obtaining them are different than conventional crime.

It can be said that the most effective legal arrangement on cybercrimes so far is the Council of Europe Cybercrime Convention, which was opened by the Council of Europe on 23 November 2001. The aim of the contract is to "protect the society against cybercrime by establishing a common penalty policy, in particular to adopt the necessary legislation" and to develop international cooperation. However Turkey, the Council of Europe Cybercrime Convention is a party to the case by signing on 10 November 2010, could not transfer the contract to the domestic law by completing the process that will bring it an integral part of the domestic law. It came into force on April 22, 2014 in the Assembly, but difficulties remain in the integration and implementation of the contract.

When it comes to information technology law or cybercrimes, a very large area undoubtedly comes to mind at first glance in terms of the size of information systems technology and its use with the internet. Legal regulation works in the field of information technology in our country has developed very rapidly with the establishment of the Information and Communication Technologies Authority. In the field of informatics, crimes were firstly sanctioned by the additions to the Turkish Penal Code (TCK) numbered 765 at the time, on June 6, 1991, by being affected by the regulations of French law in this regard. With the new TCK numbered 5237, which entered into force in 2005, crimes in the field of information technology were completely rearranged in line with the developments in us and western law.

In order to combat crimes committed through internet broadcasts in our country, Law No. 5651 on Regulation of Publications on The Internet and Combating Crimes Committed by Means of Such Publication was needed. This law is regulated in accordance with the provisions of the 'Protection of the family and children's rights' stated in article 41 of the Constitution and the 'Youth protection' mentioned in article 58. The main

purpose is to prevent the processing of certain crimes in the internet environment and to protect children and young people from harmful content published on the internet.

It is possible to deny the access for the sites containing the contents specified in the section above regarding the law numbered 5651. In addition, with the changes made in recent years, the provisions of access denial have been expanded, and the provision of requesting the removal of content by real persons in cases of violation of privacy and attack on personal rights has been regulated.

In this way, it is aimed to prevent victimization as a result of the content published on the internet. Before these law changes, there were legal deficiencies in individuals' right to seek their rights, thanks to the arrangements made, the steps that people should take were clearly stated.

On the other hand, after the amendments in 2014 in the Law, there are many news about intervention in freedoms in the media. Such reactions were encountered due to the increase of the powers of the Information and Communication Technologies Authority and the expansion of the areas where it can be taken ex officio in cases where there is a delay in the delay before it is presented to the approval of the judge.

In accordance with the law, when a website is blocked from access, concepts such as victims, criminals, third parties become undefined. In a website, if the sharing of a user is a crime in accordance with the law, when the site is completely blocked from access, other content providers, members and visitors of that site are victimized. In addition, each access blocking causes an intervention in the freedom of thought and expression of other individuals.

Officers who work in cybercrime units of law enforcement units are among the most prominent crime protectors. It is carried out by the Department of Cyber Crime and its provincial units in this police service. Basically, cybercrime investigation, cybercrime prevention and digital forensics are carried out in three different areas. The availability of skilled protectors can only be ensured by the qualification of the staff working in these units. These personnel also need to be trained in their fields. In this way, the success rate will increase both in measures before the crime occurs, in the post-crime investigation processes, and in the process of analyzing and accepting and reporting the digital materials subject to crime,

and the probability of not getting caught by the potential criminal will decrease. On the other hand, another important issue is the authority provided by the legislation so that the protectors can use these abilities more effectively. All combat operations are carried out based on a specific legislation. Legislation also needs to be optimized so as to ensure the most effective fight against this crime without violating personal rights and freedoms on an individual basis.

Kaynakça / References

Akıncı, H., Alıç, E. A. ve Er, C. (2004). *Türk Ceza Kanunu ve bilişim suçları*. İstanbul: Atamer.

Batır, K. (2005). İnternet ve hukuk. (Ed. M. Binark ve B. Kılıçbay) *İnternet, Toplum, Kültür* içinde (s.156-176). Ankara: Epos Yayınları

Berber Keser, L. (2004). *Adli bilişim: Computer forensic*, İstanbul: Yetkin Yayınları.

Bozkurt, V. (2000). Gözetim toplumu ve internet: Özel yaşamın sonu mu? *Birikim Dergisi*, 136, 69-74.

Castells, M. (2013). *Ağ Toplumunun Yükselişi* (3. Baskı) (Çev: E. Kılıç) İstanbul: İstanbul Bilgi Üniversitesi Yayınları.

Çubukçu, B. (2000) *Teknoloji ve endüstriyel ilişkiler*. 16.10.2016 tarihinde http://antrak.org.tr/index.php?option=com_content&task=view&id=991 adresinden erişilmiştir.

Dülger, M. V. (2004). *Bilişim suçları*. Ankara: Seçkin Yayınları.

Durmaz Ş. (2005). *Bilişim suçlarının sosyolojik analizi.* Yayımlanmamış Yüksek Lisans Tezi.Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Eriş, U. (2011) Türkiye'de hacker kültürüi *Gümüşhane Üniversitesi İletişim Dergisi 1*(2) 20.09.2015 tarihinde http://egifder.gumushane.edu.tr/article/view/5000006422/5000006851 adresinden erişilmiştir.

Gercke, M. (2009), *Europe's legal approaches to cybercrime*. 17.09.2014 tarihinde http://www.springerlink.com/index/f76171880840794.pdf adresinden erişilmiştir.

Imhof, R. (2010). *Cyber crime and telecommunications law*. Yüksek Lisans Tezi. Rochester Institute of Technology.

Jordan, T. ve Taylor, P. (2010). Bilgisayar korsanları sosyolojisi (Ed A. Giddens) *Sosyoloji* içinde (s.221-239), İstanbul: Say Yayınları, 221-239.

Karagülmez, A. (2005). *Bilişim suçları ve soruşturma:Kovuşturma evreleri.* Ankara: Seçkin Yayınları

Kurt, L. (2005). *Açıklamalı-İçtihatlı tüm yönleriyle bilişim suçları ve Türk Ceza Kanundaki uygulaması*. Ankara:Seçkin Yayınları.

Özberk, V. Ö. (2002). İnternet kullanımında ortaya çıkabilecek bazı ceza hukuku soruları. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, *4*(1), 101-159.

Öztürk, M. İ. (2007). *Bilişim cihazlarındaki sayısal delillerin tespiti ve değerlendirilmesinde iş akış modelleri*. Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Ankara.

Şehitoğlu, O. T. (2005). *Bilgisayar ve ağ üzerinden işlenen siber suçlarla mücadelenin hukuksal ve güvenlik boyutu*. Yayımlanmamış Yüksek Lisans Tezi, Ankara, Kara Harp Okulu Komutanlığı Savunma Bilimleri Enstitüsü.

Seymour, M. M. (2013). *An explanatory model of motivation for cyber-attacks drawn from criminological theories*. Unpublished MSc thesis. Maryland, ABD: University of Maryland.

Tekin, M. ve Çiçek, E. (2006) Bilgi çağında bilgi toplumu ve bilgi ekonomisi. 05.04.2015 tarihinde http://www.bilgitoplumu.blogspot.com/ adresinden erişilmiştir.

Topaloğlu, T. (2014). *Adli bilişim ve elektronik deliller* (Ed: H. Çakır ve M. S. Kılıç) Ankara: Seçkin Yayıncılık.

Tutar, H. (2000). Küreselleşme sürecinde işletme yönetimi. *Hayat Dergisi* İstanbul.

UNESCO, (2004) The COE International Convention on Cybercrime Before Its Entry Into Force. *UNESCO e-bülten Ocak-Mart 2004* 17.12.2015 tarihinde http://portal.unesco.org/culture/en/files/19556/11515912361coe_e.pdf/coe_e.pdf adresinden erişilmiştir

Yazıcıoğlu, R. Y. (1997). *Bilgisayar Suçları, kriminolojik, sosyolojik ve hukuki boyutları ile*. İstanbul: Alfa Basım Yayım Dağıtım

Kaynakça Bilgisi / Citation Information

Yılmaz, F. ve Güllüpınar, F. (2020). Türkiye'de bilişim suçlarının kriminolojik açıdan değerlendirilmesi: Bilişim suçlarının hukuksal ve sosyolojik boyutlarının analizi. *OPUS–Uluslararası Toplum Araştırmaları Dergisi, 15*(10. Yıl Özel Sayısı), 5371-5409. DOI: 10.26466/opus.688815