ISophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi
ISophos: International Journal of Information, Technology and Philosophy
Yıl/Year: 2018 • Sayı: 1

SUÇ OLGUSUNUN DEĞİŞEN YÜZÜ: SİBER SUÇLAR

CHANGİNG FACE OF THE PHENOMENON OF CRİME: CYBER CRİME

Mert Küçükvardar
Marmara Üniversitesi Sosyal Bilimler Enstisüsü
Bilişim ABD // mertkvardar@gmail.com

Anahtar Kelimeler:

Siber Evren, Siber Âlem, Siber Suçlar, Bilişim Hukuku, Siber Güvenlik.

Özet

Siber suçlar dünyayı sarsan küresel bir sorundur. "Siber" sözcüğü "bilgisayarların, iletişim teknolojilerinin ve sanal gerçekliğin kültürüyle ilişkili" olarak tanımlandığı için çok geniş bir alanı kapsar. Ayrıca internet üzerinden gerçekleşen geleneksel suçları da içerir. Bu nedenle siber suçlar, suç dünyasındaki en yeni ve en karmaşık sorunlarını içerisinde barındırır. Artık süper güç olarak tanımlanan ülkeler savunma yatırımlarının birçoğunu siber alana yapmaktadır. Siber saldırılarla, seçimlere müdahale edilebildiği, şehirlerde büyük elektrik kesintilerinin gerçekleştirilebildiği ya da iletişim sistemlerinin çökertilebildiği görülmektedir. Teknolojinin ve buna bağlı olarak internetin çok hızlı şekilde ilerlemesi bilişim alanında yaşanan suçları arttırmaktadır. Dünden bugüne, insanların eylemlerini kontrol altına alan, düzenleyen kolluk kuvvetleri ve çeşitli yasalar mevcuttur ancak siber ortamda kontrol, geleneksel ortama göre oldukça farklıdır. Kontrolün oldukça zor olması dünyanın birçok yerindeki hükümet ve kuruluşların siber alandaki suçların önüne geçilmesi ve etkin uygulamaların ortaya koyulması için gösterdikleri çabayı zorlaştırmaktadır. Siber hırsızlar artık sosyal medya gönderilerini incelemekte, GPS'leri kullanmakta ve hatta ebeveynlerin çocuklarını gözlemlemek için yerleştirdiği bebek monitörlerine bile sızabilmektedirler. Bugün sanal dünyayı kullanan tüm bireyler siber hırsızların hedefindedir.

Sanal ortama bağlı banka hesapları ya da bilgisayar sunucuları güvende değil ve hiçbir zaman da olmadı. Teknolojiye bağımlılık şimdi siber hırsızlar tarafından bir nimet olarak görülmektedir. Dolayısıyla bu alana yönelik bilgi havuzunun genişletilip aynı zamanda güncel tutulması önemlidir. İnternette gerçekleşen olayların ışık hızıyla meydana geldiği de düşünülürse etkin ve güçlü savunma sistemlerinin inşa edilmesi, konu hakkında farkındalık ve bilinç oluşturulmasının ne kadar önemli olduğu görülecektir. Bu makalede içerik analizi yönteminden hareketle, bilişim teknolojilerinin kötüye kullanılmasıyla ortaya çıkan siber suç ve buna bağlı kavramlar ile bu suçun etkileri irdelenmiştir. Elde edilen bulgular çerçevesinde siber suçlara yönelik uluslararası hukuk boyutunda daha kapsamlı düzenlemelerin yapılması ve her geçen gün etkisini arttıran siber suç olgusu üzerine farklı araştırmaların ele alınmasına yönelik tavsiyelerde bulunulmuştur.

Keywords:

CyberWorld, Cyber Space, Cybercrimes, IT Law, Cyber Security.

Abstract

Cybercrime is a global problem that affects the world. The term “cyber” contains a very broad area and related to computers, communication technologies and virtual reality culture. It also includes traditional crimes on the Internet. On account of this cybercrime, It contains the latest and most complex problems in the criminal world. Countries such as United States of America and Russia have been making the most of their defense investments in cyberspace. We witness massive cyber attacks for example, interfering with elections, major power failures in cities, or collapsing communication systems. The rapid progress of technology and the Internet shift the world and communication system. For long years, we have law enforcement agencies and various laws to control, regulate the actions of people, but in the

cyber environment control is quite different from the traditional atmosphere. Governments and organizations struggle to put forth effective practices to control cybercrime. We are now facing side effect of technology. The cyber thieves are watching our social media post, using our GPS and even hacking the baby monitors you put in to watch our kids. Today we are all aimed at cyber thieves. Our bank accounts or computer servers are not safe as it never been. Our technology addiction is now seen as a blessing by the cyber thieves. Therefore, the pool of information on cybercrime should be expanded. It is important to create an effective consciousness against cybercrime in the light of events taking place on the Internet. Content analysis technique was used in this study. Cybercrime and its related concepts and the effects of these crimes arising from the abuse of information technologies have been examined. In the framework of the findings, more comprehensive regulations on cybercrimes should be made in terms of international law. There have also been recommendations for handling different research on the cybercrime phenomenon.

1. GİRİŞ

Bilişim; elektronik cihazlar yardımıyla bilginin belirli bir düzen içerisinde gerçekleştirilip, işlenmesidir. Özellikle sosyal ve davranış bilimlerine göre daha yeni bir alandır. Bu yeni alan yaşadığımız dünyanın sınırları genişletmektedir. Artun'a göre günümüz dünyası, bir bilim ve teknoloji dünyasıdır. Bilgi patlaması, bilimsel ve teknolojik alanda kaydedilen hızlı değişme ve gelişmeler nedeniyle günümüz, bilişim çağı olarak kabul edilmektedir. Bilişim düşüncesinin yaygınlaşması ve bilgisayar kullanımının artması beraberinde zihniyet değişimini de getirmektedir (Artun, 2005, s. 321). Bilgi akışındaki hızlı dönüşümlere uyum sağlayabilmek amacıyla bilişim bilincinin oluşturulması kaçınılmazdır.

İnsanoğlu, dünya üzerinde var olduğu günden bu yana içinde bulunduğu çağın özelliklerine göre iletişim araçlarını kullanmıştır. Bu kimi zaman resim, kimi zaman yazı olarak görülmüştür. Günümüz söz konusu olduğunda ise bu iletişim araçları, teknolojik araçlarla daha güçlü ve yaygın bir duruma ulaşmıştır. Bilgisayarı olan ev sayısı artarken, internet kullanımı da buna bağlı olarak artış göstermiştir (Keskin, 2012, s. 4). Tarihsel olarak yerleşik toplum düzeninden sanayi toplumuna evirilen insanoğlu artık kendine yeni bir yön belirleyerek bilgi toplumu olma yolunda ilerlemektedir. Fakat bunu yaparken geçmişe bakıldığında çok daha hızlı bir evrimden söz etmek mümkündür. Bu

evrimde yaşanan hızlanmanın en önemli nedeni kuşkusuz bilgi ve iletişim teknolojilerinde yaşanan gelişmelerdir.

1950'li yıllarda icat edilen transistor, ardından geliştirilen mikro işlemciler, yarı iletken bellekler ve lazer teknolojisi, günümüzde kullanıma sunulan kişisel bilgisayarların temelini oluşturmaktadır. İşte o yıllarda geliştirilen bu teknolojiler şimdilerde ifade edilen bilgi toplumunun kaynağını oluşturmaktadır. Ancak süreç belirli problemleri içerisinde barındırmaktadır. Özellikle sanayi toplumundan bilgi veya sanayi ötesi topluma geçiş aşamasında da belli sıkıntıların yaşanıyor olması kaçınılmazdır (Ceyhun, 1997). Günümüzde ise bu sıkıntıların azaltılması kuşkusuz bilişimde yaşanan ilerlemeler ve bilgiye yönelik ilginin artmasından kaynaklanmaktadır. Naisbitt ise daha sonraki bölümlerde bahsedilecek olan olumsuz etkilere yol gösterici nitelikte bir söylemde bulunur ve teknolojinin bize görünmeyen bir darbe indirdiğini ifade eder:

> "Teknolojinin baştan çıkarıcı keyifleri ve vaatleri ile zehirlenmiş bir halde teknolojinin yol açacağı sonuçlara sırtımızı dönüyoruz ve geleceğin neden güvenilmez göründüğüne hayret ediyoruz. Çok azımız teknolojinin yaşamlarımızda sahip olduğu (veya olması gereken) yer, her şeyden öte teknolojinin ne olduğu konusunda tam bir anlayışa sahibiz. Teknolojiye sanki doğa kanunu gibi özel bir statü, günlük yaşamları geliştirici deneyimlerimiz, hatta doğal dünyayı giderek daha sofistike hale gelen yazılımlarla yönetmek için mutlak bir hak tanımaktayız. Biz bağlanmak, çevrimiçi olmak, çalıştırmak, çıkmak ve sonunda parçaları toplamakla meşgulken teknoloji ekonomimize darbe indirmeye doğru ilerlemektedir. Bir şeylerin doğru olmadığını hissediyoruz ancak ne olduğu üzerine parmak basmıyoruz" (Naisbitt, 2004, s. 11):

Sınırların tek bir tıklamayla aşıldığı ve genellikle herhangi bir izne gerek duyulmadan saniyelerden daha kısa bir sürede sorunları aşan pek çok teknolojinin gölgesinde, bilişim teknolojileri bireyleri interaktif bir karar verici haline getirmiştir. Sınırlar arası bir olgunun bireylere vereceği zararın ise yalnızca ulusal mevzuatlarla giderilmesi ve zararın sorumlusunun sadece ulusal yasalarla takibi elbette mümkün değildir. Teknolojilerin sağladığı imkânları suç olgusu ile birleştiren suçluların ise adalete teslimi ortak ve birbiriyle uyumlu yasalarla mümkündür. Bilişim suçları ile ilgili olarak, ülkeler tarafından atılan pek çok olumlu adımın birbirinden bağımsız ve farklı uygulamalara dönüşmesi bu olumlu gelişmeleri gölgelemektedir. Çalışmada siber suçlar ve bu suçların

çeşitleri yönelik incelemeler ile ülkelerin attığı, bahsi geçen birbirinden bağımsız düzenlemeler nedeniyle bir karmaşıklık olduğu tespit edilmiştir. Dolayısıyla konunun açıklanmasına yönelik belirli sınırlılıklar mevcuttur. Öncelikle ülkemizdeki bilişim hukuku ve adli bilişim konularıyla ilgili bilgilerin ortaya koyulması önem arz etmektedir.

2. Türkiye'de Bilişim Hukuku

Yeni teknolojiler yeni suç olanakları yaratmaktadır. Dolayısıyla siber suçları geleneksel suç faaliyetlerinden ayıran temel fark nedir? sorusu akılları karıştırmaktadır. Aslına bakıldığında temel fark; suçların dijital ortamda işlenmesidir ancak tek başına teknoloji, farklı suç eylemlerini kapsamamaktadır. Dolayısıyla temel bir ayrım için bir yetersizlik durumu söz konusudur. Artık suçlular, sahtekârlık, fikri mülkiyet hırsızlığı, kimliklerini kopyalamak veya bir kimsenin mahremiyetini ihlal etmek için bir bilgisayardan ziyade farklı şeylere ihtiyaç duymaktadır.

Yeni şeylere duyulan ihtiyaçların ışığında bilişim hukuku sürekli güncellenmesi gereken bir alandır. Bu bağlamda bilişim suçlarına yönelik ülkemizde çeşitli kanunlar mevcuttur. Yeni Türk Ceza Kanunu'nda işlenen bilişim suçlarına yönelik maddeler şu şekildedir:

> "Kişilere karsı suçlar" kısmının dokuzuncu bölümünde 'özel hayata ve hayatın gizli alanına karsı suçlar' baslığı altında m. 135 'kişisel verilerin kaydedilmesi suçu', m. 136 'kişisel verileri hukuka aykırı olarak verme veya ele geçirme suçu', m.138 'verileri yok etmeme suçu. 'Topluma karşı suçlar' kısmının onuncu bölümünde 'bilişim alanında suçlar' başlığı altında m.243 'hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu', m.244/1-2 'bilişim sisteminin işleyişinin engellenmesi, bozulması, verilerin yok edilmesi veya değiştirilmesi suçu', m.244/4 'bilişim sistemi aracılığıyla hukuka aykırı yarar sağlama suçu', m.245 'banka veya kredi kartlarının kötüye kullanılması suçu" (YTCK, 2014):

Görüldüğü üzere ceza kanununda yer alan suçlar, kişisel hayata müdahale edilmesi üzerine yoğunlaşmaktadır. Bunların yanı sıra YTCK'da bilişim sistemleri aracılığıyla işlenebilecek ancak yalnızca bilişim suçu olarak nitelendirilemeyecek suç tipleri de bulunmaktadır:

> "Bilişim alanında suçlar bölümünde ilk olarak 243. maddede 'hukuka aykırı olarak bilişim sistemine girme veya sistemde kalma suçu' düzenlenmiştir. YTCK'da yer alan bu maddeyle, yasa koyucu 'bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girme veya orada kalmaya devam etme' eylemini suç tipi haline getirmiştir."

Avrupalı devletlerin bilişim suçlarını düzenleme zamanlarına bakıldığında, Türkiye'nin bu alana adaptasyon konusunda biraz geç kaldığı söylenebilir. Bilgisayar sektörünün 1990'lı yıllarda yakaladığı büyüme trendine yönelik ülkemizde ilk tepki 1991 yılında yapılan düzenlemelerle gelmiştir. Modern anlamda 2004 yılında baştan sona yenilenen Türk Ceza Kanununun bilişim alanında suçlar kısmı da bilhassa Avrupa Siber Suç Sözleşmesi'ne paralellik sağlamak amacıyla yeniden düzenlenmiştir. Günümüzde ise son dönemde yaşanan hukuksal değişimler, TIB'e tanınan yetkilerle birlikte, devletin internet üzerinde kontrol ve yasakları artmıştır. Siber suçlarla mücadele etmek için Avrupa Birliği de siber güvenlik stratejisinin bir parçası olarak mevzuatlar uygulamakta ve operasyonel işbirliğini desteklemektedir. Avrupa Komisyonu, Ocak 2013'te faaliyete başlayan EC3'ün geliştirilmesinde önemli bir rol oynamıştır. EC3, AB içindeki siber suçlara karşı mücadelede etmeyi amaçlamakta ve üye devletlerin siber suç araştırmalarını desteklemek için Avrupa siber suçları uzmanlarını bir araya getirmektedir.

3. Adli Bilişim Kavramı

Adli Bilişim (*Computer Forensics*), hukuki ya da cezai bir soruşturmada dijital kanıtların elde edilmesi, analizi ve kullanım süreçlerini içeren bir olgudur. Kanıtların kaynağı olarak bilgisayarlarla sınırlı değildir. Dijital dosyaları depolayabilen herhangi bir ortam ya da araç adli bilişim araştırmacısı için potansiyel bir kanıt kaynağıdır. Bu nedenle, adli bilişim aynı zamanda dijital dosyaların incelenmesi üzerine yoğunlaşır. Bu işle uğraşan bireyler olay yerinde bulunan delilleri, niteliklerine uygun bilim alanlarının verilerine göre, laboratuvar ortamında inceleyip bilimsel ve teknik sonuçlar çıkarabilen gerekli teknik ve hukuki bilgiye sahip uzmanlar olarak nitelendirilmektedir. Bu uzmanlar aynı zamanda gerektiğinde olay yerinde bulunup olay yeri inceleme görevlerini üstlenmek, delillerin ön değerlendirmesini yapmak veya olay yeri inceleme görevlilerine danışmanlık yapmakla görevlidirler.

Bilişim aygıtlarının tüketiciler tarafından özellikle 1990'lardan itibaren yoğun şekilde tercih edilmesiyle siber suçlarda artış başlamıştır. Bu gelişmelerin ışığında bilgisayarlara yönelik yeni yasalar çok geçmeden yürürlüğe girmiştir. Bilgisayarlara yönelik suçları içeren ilk yasa tasarısı 1978 yılında Amerika Birleşik Devletlerinde kabul edilmiştir. Yasanın içeriği bilgisayar sistemlerinde yer alan bilgilerin izinsiz bir şekilde değiştirilmesi ya da silinmesini kapsamıştır. İlerleyen dönemlerde suçlarda görülen artış beraberinde çeşitliliği de getirmiştir (Hafner, 1996, s. 186). 2000'den itibaren bilişimle ilgili temel oluşturmaya yönelik adımlar atılmaya başlanmıştır bu amaçla Amerikan federal soruşturma bürosu (FBI) tarafından adli bilişim laboratuvarları kurulmuştur. Ülkemizde ise 2005'den itibaren kurumsal olarak özel şirketler tarafından danışmanlık hizmetleri verilmeye başlanmıştır. Siber suçları geniş bir çerçeveden ele almak için konunun teknoloji ve kullanıcı boyutundan da incelenmesi gereklidir.

4. Sınırları Ortadan Kaldırma Yarışında Bitiş Çizgisi Olmayan Teknolojiler

İnsanlık tarihi daha önce pek de eşine rastlanmamış bir hızda ve enformasyon teknolojilerinin gölgesinde ilerlemektedir. Yirminci yüzyıl, bilim ve toplum arasındaki ilişkide kırılma noktası olarak değerlendirilebilir. Birinci Dünya Savaşı›nda önemli bilim adamları askere alınmış ve çoğu siperlerde ölmüştür. II. Dünya Savaşı'nda ise durum değişmiş ve bilim adamları ülkelerinin savaşta ciddi kazanımlar elde etmelerine yardımcı olmuştur. Sonraki yıllarda hükümetler teorik araştırmalardan yola çıkarak endüstri, tarım ve tıp alanında pratik geliştirmeler yapılabileceğine inanmaya başlamaktadır. Bu inanç, antibiyotiklerin keşfi ve nükleer fiziğin atomik silahların üretimine uygulanması gibi gelişmeler tarafından desteklenmiştir. Geçmişle kıyaslandığında teknolojiyle ilişkilerimizin bugün daha keskin ayrımlarla ifade edilebildiği söylenebilir. Bu noktada, bu yeni teknolojilerin neyi ifade ettiği ve modernizme ait olan hangi dinamikleri değiştirdiği ya da ortadan kaldırdığı sorusu önem kazanmaktadır. Ayrıca bu yeni enformasyon teknolojilerinin çok hızlı bir şekilde insanların hayatlarında vazgeçilemez konuma gelmelerinin nedenlerini anlayabilmek önemlidir. Zira teknolojilerin insanların hayatlarına katmayı vaat ettiği şeylerle birlikte tehditleri de yakından incelenmesi gereklidir (Güven, 2008, s. 69).

Teknolojiyle olan ilişkilerin karmaşıklığı üzerine çözümlemelerde bulunan Naisbitt'e göre, teknolojiyle ilişkilerimizde kutuplardan ziyade bilinçli bir teknoloji şuurunun oluşturulması ve bu şuura göre teknolojiyle ilişkilerimizin, seçimlerimizin oluşması gerekmektedir. Naisbitt'in "bilinçli teknoloji" şuurun-

dan bahsettiği şey özetle şudur:

> "İnsan hayalinin yaratıcı bir ürünü olan teknolojinin, kültürel gelişmenin ayrılmaz bir parçası olduğunu ve yeni teknolojiler yaratma isteğinin esas olarak içgüdüsel olduğunu kabul etmektir. Ama aynı zamanda da, insanlığımızı kanıtlamak için işimizde ve yaşamlarımızda teknolojiyi ne zaman geri plana atacağımızı bilmektir. En iyi açıdan bakıldığında teknolojinin insan yaşamını desteklediğini ve geliştirdiğini, en kötü açıdan bakıldığında da yabancılaştığını, izole ettiğini, yozlaştırdığını ve yıprattığını kabul etmektir. Teknolojiyi ne zaman ortaya çıkaracağını ve ne zaman kapatacağını bilmektir" (Naisbitt, 2004, s. 19).

Teknolojide görülen hızlanmalar devam ettikçe ve makineler geliştikçe insana olan ihtiyaç azalmaya başlamıştır. Gelecek yıllarda, gazeteci, ofis çalışanı ve hatta bilgisayar programcıları robotlarla, akıllı yazılımlarla yer değiştirecektir. İlerleme devam ederken, mavi ve beyaz yakalı işçiler de bu değiştirmeden nasibini alacaktır. Ancak insanı ikinci plana iten teknolojilere olan inanç pek de kaybolacak gibi gözükmemektedir. Naisbitt konuyla bağlantılı olarak, inanç düzleminde ve teknolojiyle olan ilişkilerimizde değişik duygulanımlardan bahseder:

> "Bir an teknolojiden korkuyoruz, bir an geliyor gücüne hayran oluyoruz. Bir gün rakiplerimizin veya birlikte çalıştıklarımızın gerisinde kalma korkusu ile gönülsüzce kabul ediyoruz, ertesi gün ise yaşamımızı veya işimizi daha iyi hale getiren bir şey sağlarsa keyifle sarılıyoruz, sonra da bize yardımcı olmadığında hayal kırıklığına uğramış hissediyor ve rahatsız oluyoruz. Çoğumuz için teknoloji nötr olmaktan çok uzaktır. Teknolojiyle belli bir derecede hem korkuyu hem tapınmayı kapsayan büyük ölçüde incelenmemiş bir ilişki yaşamaktayız" (Naisbitt, 2004, s. 19).

Toplumda yaşayan bireyler olarak teknolojide yaşanan çok hızlı değişimlere yönelik yaşadığımız karmaşık duygular, teknolojinin hayatımıza getirdiği olanakların yanı sıra ortaya çıkardığı olumsuz durumlar da mevcuttur. Kuşkusuz bunların arasında en sık karşılaştığımız olgu siber suçlardır.

5. Yeni Bir Suç Türü: Siber Suç

Teknolojinin günlük hayatta kullanımı artık bir kolaylık ve tercih meselesinin ötesine geçip zorunluluk halini almaya başlamıştır. Hayatın internet ile

bahsi geçen ölçüde bütünleşik hale gelmesi insanları yalnızca teknolojiye daha fazla bağlamakla kalmamış aynı zamanda kişisel bilgilerin bu ortamda daha fazla yer almasına yol açmıştır. Bilgilerin sanal alanda giderek daha fazlalaşması insanları aynı ölçüde tehlikeye yöneltmiştir. Benzer şekilde kamu kurumlarının veri tabanlarında yer alan gizli bilgilerden, enerji santrallerine, su dağıtım şebekelerinden, iletişim ağlarına kadar birçok kamu kuruluşu ve hizmeti de tehlike altında kalmıştır. Siber alandaki tehdit, tehlikelerin fazlalığı ve bunların sonuçlarının ne denli büyük olabileceği konusu, göz ardı edilemez bir gerçeklik halini almıştır.

Bilgisayar ve iletişimin birlikteliğinden doğan bilişim çağında birçok kavram insanların hayatına girmiştir. Daha çok yabancı kaynaklı kaynaklardan dilimize uyarlanan çok sayıda siber suç kavramı mevcuttur. Bunlardan en temel olan *siber (cyber)* kelimesi, bilgisayar ve iletişim ağlarına yönelik, onları betimlemek için kullanılan bir sözcüktür. Çok sayıda metinde karşılaşılan *siber alan (cyberspace)* kelimesi ise farklı şekillerde de olsa birbirleriyle etkileşim halinde olan sistemlerin ve insanların oluşturduğu alanı ifade etmek için kullanılır (Klimburg, 2012). *Siber suç (cybercrime)* kelimesi ise "yasadışı olan ya da belirli taraflarca yasa dışı sayılan ve küresel elektronik ağlar aracılığıyla yürütülebilen faaliyetler" olarak tanımlanabilmektedir. Ayrıca suçun yasalar tarafından açıkça yasaklanmasının dışında bir de gayri resmi sosyal normları içeren ve istenmeyen, sakıncalı addedilen davranışları içeren bir yapısı da söz konusudur.

Tanımın kapsadığı geniş alan siber suçların değişik şekil ve içeriklerde olabileceğini ve klasik suçların siber alan ile farklı biçim ve yoğunlukta temas edebileceğini ima etmektedir. Esasında teknolojideki gelişiminin tahmin edilemezliği de böyle geniş bir tarifi zaruri kılmaktadır (Hekim & Başıbüyük, 2013, s. 136). Bilişim suçlarının ne olduğu ve bunun tarifi konusunda, farklı tanımlamalar yapılmakta ve ortaya birbirinden farklı açıklamalar çıkmaktadır. Özellikle bir taraftan gelişen teknoloji karşısında bilgisayar suçlarındaki teknik ve yöntemlerin sürekli nitelik ve şekil değiştirmesi, diğer taraftan konunun hem hukuki hem de cezai yanının bulunması herkesin üzerinde birleşeceği bir tanım yapılmasını zorlaştırmaktadır. Ancak, konuya ilişkin tanımlar ne kadar çeşitli olursa olsun temelde üç görüşten hareket edilmektedir. Bunlardan birincisi aynı zamanda en eski ve popüler olanı bilgisayar suçları ne şekilde açıklanırsa açıklansın, genelde bu suçlar ekonomik suçlar kategorisi içinde yer almaktadır. Avrupa Topluluğunun çeşitli çalışmalarında (12 Şubat 1981 tarihli ekonomik suçlar hakkındaki rapor ve 1989 tarihli bilgisayar suçları hakkındaki rapor gibi) bilgisayar suçlarının, ekonomik

suç teşkil ettiğini açıklamaktadır (Yücel, 1992, s. 4).

Bazı görüşlere göre siber suç olgusuna daha basit bir bakış açısıyla bakılmakta ve bilgisayar teknolojilerini kullanabilen bireylerin ortaya çıkardığı suiistimal davranışları olarak değerlendirilmektedir. Zira günümüzde siber suçlara yönelik anlayış genellikle bu yöndedir. Aynı zamanda gelişen teknolojiler ve ortaya çıkan farklı araçlar nedeniyle siber suç tanımının, içeriklerinin eskimesi gibi durumlar olaya bütüncül bir açıdan bakılamamasına yol açmaktadır. Bu nedenle siber suçlar daha geniş bir çerçevesinden tanımlanmalı, hukuki ve cezai düzlemde daha açık şekilde ortaya koyulmalıdır. Bu bağlamda Avrupa Topluluğunun 1983 yılında Paris'te gerçekleştirdiği toplantıda geniş bir tanım ortaya koyulmuştur. Bu tanıma göre, siber suçlar, bilgisayar ve benzeri araçlar aracılığıyla bilgilerin bir sistemden gayri kanuni, yetki dışı ve gayri ahlaki olarak aktarılması davranışlarını içermektedir. Yapılan tanım diğerlerine nazaran olayın hukuk, meslek ahlakı, ekonomik, toplumsal boyutlarını da içermesi bakımından geniş bir kesimi temsil etmektedir (Yücel, 1992, s. 4-5).

İletişim dünyasında birçok faaliyet siber ortamda yürütülmektedir. Temelde küresel çapta birbirine bağlanmış makinelerden oluşan bir ağı tanımlayan bu kavram, bilişim dünyasının en önemli parçası olarak kabul edilmektedir. Farklı kavramlarla birlikteliği olan siber ortama yönelik ilk literatür bilgisine 1980'lı yıllarda William Gibsion'un kaleme aldığı bilim kurgu romanında rastlamak mümkündür. Gibson, *"siber uzay" (cyberspace)* adını verdiği bu kavramda birbirine çeşitli nedenlerle bağlanmış bir ağda bulunan insanlara yönelik göndermede bulunmaktadır. Özellikle küresel çağda siber ortamda oldukça fazla vaka meydana gelmektedir. Son dönemlerde popülerlik kazanan *derin ağ (deep web)* gibi internetin daha alt katmanı olan ortamlarla birlikte siber suçlar, gelişim ve dönüşüm göstermiştir.

Gelişim ve dönüşümün ışığında siber ortamı oluşturan bilişim teknolojileri, saldırılarda önemli bir araç olarak kullanılabilmektedir. Saldırılar, hackerlar aracılığıyla kişisel menfaat veya internet mafyasına hizmet etmek için yapılabilmektedir. Haktivist gruplar, saldırılarını siyasi hedeflerine propaganda yapmak, seslerini duyurmak ve dikkatleri üzerlerine çekmek için yapmaktadır. Devlet destekli saldırılarda ise hedef ülkenin siber ortamına müdahale etmek, ekonomik zarar vermek ve gizli bilgilerini ele geçirmek amaçlanmaktadır. Siber ortamda yaşanılan saldırılarla genellikle başkalarına zarar vermek amaçlanmıştır ve bu durum ulusal güvenlik sorunu haline gelmiştir (Kara, 2013, s. 5). Bu güvenlik sorunları ile mücadele için "Adli Bilişim" konusu

günümüzün olmazsa olmazları arasına girmiştir. Dijital delillerin mahkeme ve soruşturma birimlerince delil niteliği taşıyabilmeleri için belirlenen kurallara uygun bir şekilde toplanıp, muhafaza edilip, uygun koşullarda incelenmesi gerekmektedir. Adli bilişim de dijital delillerin soruşturma birimi için hazırlanması ve sunulmasında, bütünlük ve güvenilirliğinin sağlanması hususunda oldukça önemli görevleri üstlenmektedir.

6. Siber Suçların Gelişimi

Siber suçların gelişimi, bilişim teknolojilerinin ve özellikle de internetin gelişimine denk bir şekilde ilerlemeye göstermiştir. Siber suçların görülmesi ve potansiyel suçluların artması, suçlu profillerinin çoğalması, konuya daha fazla önem verilmesini gerekli kılmış ve gözlerin bu alana çevrilmesine neden olmuştur. Geçtiğimiz yüzyıl içerisinde insanoğlunun keşfettiği bilgisayarları ve elektronik eşyaları birbirine bağlama (internet olgusu) fikri bizlere hem görsel, hem işitsel hem de etkileşimli bir haberleşme, bilgi yayma, bilgiyi araştırma, bunun üzerinden para kazanma, sanal ortamda alışveriş yapmayla birlikte para harcama imkânı vermiştir (Demirbaş, 2005, s. 264). Bu düşünce aslında yeni bir dönemin işaretidir ve "*Sanayi* Çağı" yerini "*Bilişim* Çağına" bırakmıştır. Yeni bir çağ dememizin sebebi ise toplumda meydana gelen köklü değişimler ve ekonomik alandaki etkileşimdir. Bilişim çağında sınırların çok da önemsenmediği ve bilginin hızlı, özgür şekilde paylaşıldığı sanal ortamlardaki araçlar, günümüzde birbirleriyle sıkça etkileşim içerisinde olan farklı ırkların, dillerin, kültürlerin ve çeşitli isteklerin ortaya çıkmasına yol açmıştır. Siber toplum olarak adlandırdığımız şey aslında reel bireylerin arasında ancak reel olmayan, adeta bir gölge gibi dolaşan siber suçları kapsamaktadır. Bunlar her geçen gün etkinlik ve değişkenliğini arttırmaktadır (Yazıcıoğlu, 1997, s. 76).

Bilişim teknolojilerin büyük bir ivmeyle gelişim göstermesi, boyutlarının ufalması ve ücretlerin düşmesiyle birlikte kullanıcı sayısında görülen artış önemli dinamiklerdir. Bu dinamiklere ek olarak bilgi saklama, işleme ve dağıtma üzerine yoğunlaşan bilişim teknolojileri eski tekniklerin ikinci plana atılmasına yol açmıştır. 90'lı yıllarından ilk çeyreğinden itibaren internet mecrasında görülen gelişme dünyadaki çok sayıda bilgisayarın birbirine bağlanmasıyla sonuçlanmıştır. Bu bağlantı suç işlemeye meyilli kişi ve grupların bu alanlara doluşmasına, farklı suçların ortaya çıkmasına yol açmıştır (Durmaz, 2005, s. 76). Sanal ağların resmi kurumlar için olmazsa olmaz bir hale gelmesi bu sistemlerin her an saldırılara maruz kalma riskini arttırmaktadır. Özellikle yakın dönemlerde NASA, NATO ve

benzeri örgütlere yapılan saldırılar sonucu sistemler ciddi zarar uğramıştır. Bazı büyük bilişim kuruluşlarına ait siteler ise kullanılmaz hale gelmiştir.

7. Elektronik Ağdaki En Yaygın Suçlar

Siber suç, hızla büyüyen bir suç alanıdır. Her geçen gün daha fazla suçlu, fiziksel ve sanal olarak sınır tanımayan, ciddi zararlara neden olan ve dünya çapındaki potansiyel kurbanları barındıran İnternet'in hızını, rahatlığını ve gizliliğini kullanmaktadır. Bu nedenle bilgisayar korsanlığı popüler tanımlar olarak, teknolojinin farklı tarzda içeriğe müdahale edici olarak kullanılması *(hack)* ve bunu yapan kişi *(hacker)* üzerinden tanımlamaktadır (Tim Jordan, 2004, s. 6). Yaygın kullanılan şekliyle *bilgisayar korsanlığı* yetkisiz erişim sağlamak amacıyla bir sistemin güvenlik tedbirlerini etkisiz hale getirmeye çalışmak olarak tanımlanmaktadır (Hekim & Başıbüyük, 2013, s. 142).

Siber suçlardaki yeni eğilimler çoğu zaman oldukça yıkıcıdır ve küresel ekonomiye tahmini maliyeti milyarlarca doları bulmaktadır. Geçmişte siber suçlar çoğunlukla bireyler veya küçük gruplar tarafından işlenmiştir. Bugün, son derece karmaşık siber suçların ve suçluların yer aldığı ağlarda, şimdiye kadar görülmemiş bir oranda suç işlemek için gerçek zamanlı olarak bireylerin bir araya geldiği görülmektedir. Suç örgütleri, faaliyetlerini kolaylaştırmak ve kârlarını en kısa sürede maksimize etmek için giderek internete yönelmektedir. Suçların kendileri, hırsızlık, dolandırıcılık, yasadışı kumar, sahte ilaçların satışı gibi çeşitlidir. Ancak suçlar, çevrimiçi sunulan fırsatlara göre çok değişkendir ve bu nedenle hedef aldığı kitleye daha zarar verici niteliktedir.

Günümüzde çoğu adli vakada bilişim araçlarına rastlamak mümkündür. Durum böyle olunca adli bilişim alanında karşılaşılan konu çeşitliliği de artmaktadır. Adli bilişim alanında olayın konusuna göre değişik metotlar uygulanabilmektedir (Ekim, 2013, s. 15). Siber suç işlemeye yönelik farklı isimlerle adlandırılan birçok sayıda teknik bulunmaktadır. En sık şekilde kullanılan belli başlı siber suç yöntemleri mevcuttur. Bilişim dünyasında en çok karşılaşılan suç teknikleri özetlemek mümkündür:

"Çöpe dalma (Scavenging)" veya "*Atık toplama*" olarak adlandırılan bu yöntem, bilişim sistemlerinde yapılan bir veri girişi ve çıkışı sonrası ortaya çıkan bilgilerin depolanması durumudur. İki tür teknik mevcuttur. Bu kimi zaman çıktı alınan ve daha sonra çöplüğe atılan kâğıt ve benzeri malzemelerin toplanmasıyla elde edilebileceği gibi aynı zamanda bilişim sistemlerinin ha-

fızasında kalan ve silinmiş bilgilerin geri getirilmesi şeklinde de olabilir (Yazıcıoğlu, 1997, s. 159). Özellikle şirketlerde, içeriden ya da dışarıdan her türlü tehditkâr müdahaleyle bu bilgilerin elde edilmesi söz konusu olabilir. Ayrıca ATM cihazlarından yapılan bir işlem sonucu verilen kâğıtların orada bırakılması ve gelişigüzel atılması da gizli bilgilerin elde edilmesine ve daha sonra saldırı amaçlı kullanılabilmesine olanak sağlamaktadır.

Şirketlerde veri döngüsünün mevcut olduğu alt yapı sistemlerine dışarıdan yapılan müdahaleler de söz konusu olabilir. Bu durum verinin dağılım sürecinin takip edilmesi, görsel öğelerin elde edilmesi gibi çeşitli şekillerde ortaya çıkabilir. Ayrıca merkeze yönelik yerleştirilen çeşitli cihazlarla iletişim sinyallerine sızılma durumu da görülebilmektedir. (Diffie & Landau, 2008, s. 3).

Bir başka siber suç çeşidi de mitolojideki "Truva atı" hikâyesine benzer niteliktedir. İsmini bu meşhur hikâyeden alan suç çeşidi, bilgisayarlara yararlı bir yazılım izlenimi altında sızarak kişisel güvenliği tehdit etmekte ve sistemde bulunan mevcut programların, dosyaların çalışamaz hale gelmesine yol açmaktadır. Ayrıca dışarıdan takılan diğer sistemlerinden bu zararlı yazılımdan etkilenmesine neden olmaktadır. Özellikle son dönemlerde e-mail yoluyla farklı sistemlere yaygınlık göstermektedir (Diffie & Landau, 2008, s. 4).

Elektronik ağlar vasıtasıyla işlenen diğer bir suç türü de sahteciliktir. Sahtecilik bir şeyin kopyasını gerçekmiş süsü vererek değiştirmek olarak tanımlanabilmektedir (Mobbs, 2003). Bilişim sistemleri aracılığıyla özellikle de basılı materyallerin sahtesini oluşturmak oldukça basit hale gelmiştir. Basılı materyaller üzerindeki sahtecilik, dijital ortama da sıçramıştır. Kimliklerin kopyalanması, başkasına ait kimlik bilgilerinin elde edilmesi ve farklı alanlarda kullanılması sahteciliğin en temel örnekleridir (Chuck Easttom, 2011, s. 11). Bilgisayarda bulunan içeriğin değiştirilmesine yönelik bir müdahale ayrıca *"Veri Dolandırıcılığı"* olarak değerlendirilebilir.

Son dönemin en popüler siber suçu ise *"Phishing" (Oltalama)* olarak bilinen yöntemdir. Kavram İngilizce tanımıyla balık tutma anlamına gelen "fishing" den türetilmiştir. Siber suçların bir çeşidi olan oltalama da hedeflenen kurbana belirli bilgi kırıntıları bırakılır ve hedefin bu yemi yutması beklenir. En bilinen örneği sahte e-mail gönderilmesi sonucu çeşitli bilgilerin elde edilmesidir. Gmail ve benzeri e-posta hizmetlerinin sayfaları oldukça titiz bir şekilde yeniden tasarlanarak kurbana gönderilir, kurbanda sahip olduğu mail bilgilerini bu sahte sayfaya girer ve tüm bilgileri siber suçluların eline geçer (Dülger M. , 2014, s. 212).

Siber suçlar oldukça çeşitlidir ve ebeveynlerin internetin güvenliğine yönelik çekinceleri boş değildir. Özellikle sohbet odaları ve kurbanlarını arayan sosyal paylaşım sitelerini kullananlar çoğu kez virüsler ve diğer kötü amaçlı yazılımların saldırılarına maruz kalmaktadır. Örneğin, Mayıs 2000'de "*love bug*" isimli bir virüsün internette yayılması sonucu, İngiltere ve ABD devlet kurumları da dâhil olmak üzere milyonlarca bilgisayar etkilenmiştir. Bahsi geçen virüsün neden olduğu hasar 7 milyar dolar ile 10 milyar dolar arasında olmuştur.

8. Sonuç

19. yüzyılda sanayi devrimini, 20. yüzyılda bilgisayar devrimini gerçekleştiren medeniyetler, 21.yüzyılda bilgiyi temel alan bilişim devrimini gerçekleştirmektedirler. Suç olgusu ise teknoloji eliyle bir kabuk değişimi yaşamıştır. Bilişim devrimi, çok çeşitli suçların ortaya çıkmasına yol açmış ve geleneksel olarak işlenen suçlar siber alana geçmeye başlamıştır. Bilişim teknolojilerinde son yirmi yılda yaşanan gelişmeler dünyayı birçok yönden etkilemiştir. Bilgi eskiden klasik yöntemlerle elde edilip saklanırken artık bilgisayarlarda hızlı ve yüksek kapasitelerde saklanır hale gelmiştir. Bilişim teknolojilerinin hızlı ilerlemesi sadece insan hayatını kolaylaştırıp insanın yaşam kalitesini yükseltmekle kalmamış aynı zamanda araçların kötüye kullanımını da arttırmıştır. Herkesçe bilinen klasik suçlar, bilgisayarlar marifetiyle daha tehlikeli boyutlarda işlenir hale gelmiştir. Ulusal ve uluslararası alanda yeni suç tipleriyle mücadele edebilmek sadece rutin düzenlemelerle başa çıkılamayacak kadar büyük boyutlara ulaşmıştır. Bilişim teknolojilerinin sürekli değişen ve gelişen doğası gereği yapılan hukuki düzenlemeler bir süre sonra demode olmaya başlamıştır. İnternet ise günden güne hayatımızın önemli bir parçası olmaya devam etmektedir. Devasa çevrimiçi toplulukların oluşması, ekonomik alışverişlerin yaygınlığı, ibadet biçimlerinin bile sanal alana taşınması siber suçların ulaşabileceği alanları arttırmaktadır. Kamuoyu çoğu zaman siber saldırıların yarattığı sorunlardan haberdar olmasına rağmen, çevrimiçi suçlular farklı yöntemlerle ve yazılımlarla insanlara, sistemlere zarar vermeye devam etmektedir. Siber suçlular, finans alanlarını hedef almaya, siber casusluk yapmaya, virüsleri yaymaya ve sistemleri istila etmeyi sürdürdükçe, siber suçlarla mücadele her daim önemini koruyacaktır.

Hükümetler artık karasal dünyada yer almayan suçlara uyum sağlamak için

mücadele etmekte ancak dünyaya yayılan siber uzay ortamında suçlular her daim yeni olanaklar peşindedir. Toplumun sanal ağlara artan bağımlılığı insanları sistemlerin başarısızlığına ve sömürülmesine karşı daha savunmasız hale getirmektedir. Aynı şekilde, siber suçun ortaya çıkışı kriminologlar, iletişimciler, sosyologlar ve daha çok sayıda bağlantılı disiplinler için zor soruları içerisinde barındırmaktadır. Karasal dünyadaki suçlamalardan elde edilen varsayımlar temelinde (kim, ne, nerede, ne şekilde vs.) suç teorilerini ve açıklamalarını oluşturan araştırmacılar çoğu zaman başarısız olabilmektedir. Uygar medeniyetlerin amacı artık bilişimin nimetlerinden hayatın her alanında sonuna kadar faydalanmaktır. Ve Türkiye asla bu yarıştan geri kalmamalıdır. Çünkü geleceğin en güçlü ülkeleri, en son teknoloji silahlara sahip olan devletler veya sanayileşmiş devletler değil, en yüksek oranda bilgi toplumu olabilmiş ülkeler olacaktır.

Sonuç olarak, siber suçların tüm dünyada bir panik havası oluşturduğu ve bu durumun uluslararası karar mercilerini hızlı bir seçim yapmaya zorladığı bir düzende bilişim hukuku, adli bilişim, siber suçlar ve siber suç tekniklerine yönelik literatür taraması yapılmış, konu Dünya'da ve Türkiye'de yer alan hukuksal düzenlemeler ve çeşitli kavramların da yardımıyla aydınlatılmaya çalışılmıştır. Siber suçlar her geçen gün kendisini yenileyen ve daha fazla araştırılmayı hak eden bir alandır. Bu konuda derinlemesine araştırılma yapılmaması ve gerekli hukuki düzenlemelerin atılmadığı bir ortamda birçok kişi ve kurumun zarar görmesi olasıdır. Özellikle ülkemizde konuya ilişkin atılan adımlara bakıldığında belirli bir hukuki düzlemin tam olarak oturtulamadığı görülmektedir. Her ne kadar Türkiye, AB standartlarını takip etse de özellikle yasalarda siber suçlara yönelik bazı eksiklikler mevcuttur. Temel eksiklikler siber suç çeşitlerinin her gün farklı biçimde ve farklı isimlerle kendini ortaya çıkarmasından kaynaklanmaktadır. Dolayısıyla gelecekte bu alana yönelik yapılması gereken çalışmalar, seneler içerisinde görülen vaka olaylarının incelenmesi ve farklı kavramlarla ortaya çıkan siber suçlara karşı ne gibi önlemler alınması gerektiğinin ortaya koyulması gibi önemli görevleri üstlenecektir.

9. Kaynakça

Artun, E. (2005). *Türk Halkbilimi.* Ankara: Kitapevi.

Bilişim Suçları ve Yeni Türk Ceza Kanunu. (2014). Ankara: TBMM.

Ceyhun, Y. v. (1997). *Bilgi Teknolojileri Türkiye İçin Nasıl Bir Gelecek Hazırlamakta.* Ankara: Türkiye İş Bankası Kültür Yayınları.

Chuck Easttom, J. T. (2011). *Computer Crime, Investigation, and the Law.* Cambride: Course Technology Publishing.

Demirbaş, T. (2005). *Kriminoloji.* Ankara: Seçkin Yayınları.

Diffie, W., & Landau, S. (2008). Internet Eavesdropping: A Brave New World of Wiretapping. *Scientific American Magazine*.

Durmaz, Ş. (2005). *Bilişim Suçlarının Sosyolojik Analizi.* Ankara: Gazi Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetim Ana Bilim Dalı Yayımlanmamış Yüksek Lisans Tezi.

Dülger, M. (2014). *Bilişim Suçları ve İnternet İletişim Hukuku.* İstanbul: Seçkin Yayıncılık.

Ekim, A. (2013). *Bilişim Suçlarında Sayısal Delillerin Toplanması, Muhafaza Edilmesi, İncelenmesi ve Raporlanması.* İstanbul: Marmara Üniversitesi Sosyal Bilimler Enstitüsü Gazetecilik Anabilim Dalı Yayınlanmış Yüksek Lisans Tezi.

Güven, S. K. (2008). Yeni Dünya Düzeni İçinde Enformasyon Teknolojilerinin Vaatleri ve Tehditleri. *Boğaziçin Üniversitesi İletişim Fakültesi Dergisi*, 69-85.

Hafner, K. (1996). *CYBERPUNK: Outlaws and Hackers on the Computer Frontier, Revised.* Pennsylvania: Simon & Schuster.

Hekim, H., & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*(4 (2)), 135-158.

Kara, M. (2013). *Siber Saldırılar ve Siber Savaşlar.* İstanbul: İstanbul Bilgi Üniversitesi, Bilişim Teknoloji ve Hukuku Yayınlanmış Yüksek Lisans Tezi.

Keskin, İ. (2012). *Medya ve İletişim.* Eskişehir: Anadolu Üniversitesi Yayınları No: 2548.

Klimburg, A. (2012). *National Cyber Security Framework Manual.* ATO Cooper-

ative Cyber Defense Center of Excellence Publisher.

Mobbs, B. (2003). *Computer Crime The Law On The Misuse Of Computers and Networks.* http://www.internetrights.org.uk/briefings/irtb08-rev1-draft.pdf adresinden alındı

Naisbitt, J. (2004). İnsan ve Teknoloji. CSA Yayın Ajansı.

Tim Jordan, P. T. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* London & Newyork: Taylor & Francis Group.

Yazıcıoğlu, Y. (1997). *Bilgisayar Suçları: Kriminolojik, Sosyolojik ve Hukuksal Boyutları ile.* İstanbul: Alfa Yayınları.

Yücel, M. (1992). *Bilişim Suçları.* Ankara: Ankara Barosu Dergisi (Y.49).