ACADEMIC SOCIAL RESOURCES Journal
Open Access Refereed E-Journal & Refereed & Indexed
Year 2022, Vol: 7, Issue: 33, pp: 36-53

e-ISSN: 2630-6417

International Academic Social Resources Journal

ARTICLE TYPE
Review Article
SUBJECT AREAS
Social Sciences, Sociology

Article ID
57292
Article Serial Number
05

Received
15 December 2021
Published
31 January 2022

How to Cite This Article:
Şenol, D. & Karataşoğlu, E.B. (2022). "Siber Suçlara Sosyolojik Bakış ", International Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:7, Issue:33; pp:36-53.

Siber Suçlara Sosyolojik Bakış

Sociological Perspective On Cyber Crime

Prof. Dr. Dolunay ŞENOL[1] Elif Buket KARATAŞOĞLU[2]

[1] Kırıkkale Üniversitesi, Fen ve Edebiyat Fakültesi, Sosyoloji Bölümü, Kırıkkale/Türkiye
[2] Yüksek Lisans Öğrencisi, Sosyal Bilimler Enstitüsü, Sosyoloji Anabilim Dalı, Kırıkkale/Türkiye (Corresponding Author)

ÖZET

Geçmişten günümüze insanın olduğu her yerde var olan suç olgusu, teknolojik gelişmeler ile birlikte farklılaşmıştır. Özellikle bilişim teknolojilerinin hızlı ilerleyişi suç işleme şeklini değiştirmiş ve siber suç kavramının ortaya çıkmasında etkin bir rol oynamıştır. Günümüzde siber suçlar diğer suç türlerine göre önemli ve hızlı bir artış göstermektedir. Siber suçların gelişimini ve bu gelişimde etkili olan toplumsal faktörleri ortaya koymak amacıyla hazırlanan bu çalışmada, öncelikle suç ve siber suçlarla ilgili teorik bilgiler ortaya konulmaya çalışılmıştır. Siber suçlar, ortaya çıkışları ve nitelikleri açısından diğer suç türlerinden önemli farklılıklar ortaya koymaktadırlar. Şahsa ve mala karşı suçlar, tarihin en erken dönemlerinden itibaren var olmalarına rağmen siber suçların ortaya çıkabilmesi için öncelikle teknolojinin gelişmesi ve yaygınlaşmış olması gerekmiştir. Bu sebeple, siber suçlar çağdaş dönemin ve teknolojinin suçları olarak değerlendirilmektedir. Ayrıca suç ve eğitim seviyesi arasında ters orantının var olduğu kabul edilirken, bilişim suçları bu kabulü de tersine çevirmiştir. Siber suç işleyenlerin siber suç işleyebilecek kadar eğitim seviyelerinin yüksek, bilişim teknolojilerini kullanıp istismar edebilecek kadar bu alana hakim olmaları gerekmektedir. Her geçen gün hızlı artış gösteren bu suç türünün, çağdaş dünyada ortadan kaldırılabilmesi mümkün olmamakla birlikte en aza indirilebilmesi için bu suç türünü ortaya çıkaran sebep ve toplumsal şartların ortaya konulması önemli bir rol oynamaktadır. Suçu önleme çalışmalarının, cezai müeyyidelerden daha etkili ve ekonomik olduğu gerçeğinden hareket edildiğinde, bu yönde yapılan çalışmaların yetkililere ışık tutmada önemli olduğu dikkatlerden kaçırılmamalıdır. Siber suçların Türkiye'de ve dünyadaki seyrini ortaya koyan bu çalışmaların sayılarının arttırılmasının, her gün kendilerini güncelleyen bilişimcilerle yarışan bilişim suçu işleyenlerin önünü bir ölçüde de olsa kesmede dolayısı ile siber suçlarla mücadelede önemli bir rol oynayacağını hatırlatmakta yarar bulunmaktadır.

Anahtar Kelimeler: Suç, Sapma, Siber Suç, Siber Güvenlik, Toplum 5.0

ABSTRACT

The phenomenon of crime, which has existed everywhere from the past to the present, has differentiated with technological developments. Especially the rapid progress of information technologies has changed the way of committing crimes and has played an active role in the emergence of the concept of cyber crime. Today, cybercrime shows a significant and rapid increase compared to other types of crime. In this study, which was prepared to reveal the development of cybercrime and the social factors that are effective in this development, firstly, theoretical information about crime and cybercrime was tried to be revealed. Cyber crimes show significant differences from other types of crimes in terms of their emergence and characteristics. Although crimes against persons and property have existed since the earliest periods of history, technology had to develop and become widespread in order for cybercrime to emerge. For this reason, cyber crimes are considered as crimes of the modern era and technology. In addition, while it is accepted that there is an inverse ratio between crime and education level, computer crimes have reversed this acceptance. Those who commit cybercrime should have a high level of education to commit cybercrime, and have a command of this field enough to use and abuse information technologies. Although it is not possible to eliminate this type of crime, which is increasing day by day, in the modern world, it is important to reveal the reasons and social conditions that lead to this type of crime in order to minimize it. Considering the fact that crime prevention activities are more effective and economical than penal sanctions, it should not be overlooked that the studies carried out in this direction are important in shedding light on the authorities. It is worth remembering that increasing the number of these studies, which reveal the course of cybercrime in Turkey and in the world, will play an important role in the fight against cybercrime, in order to cut the way of cybercrime perpetrators who compete with informatics who update themselves every day.

Keywords: Crime, Deviance, Cybercrime, Cybersecurity, Society 5.0

1. GİRİŞ

Geçmişten günümüze birçok araştırmaya konu olan suç ve sapma olguları toplumsal hayatta önemli bir yere sahiptir. Çoğunlukla birbirleri ile ilişkili olarak anılan suç ve sapma kavramları insanın olduğu her yerde varlığını korumak ve sürdürmektedir. Özellikle toplumsal hayatın varlığı suç ve sapma olgularını kaçınılmaz kılmaktadır. Suç kavramından çok daha tanımlanması güç olan sapma kavramı, suçtan çok daha geniş bir yelpazeye sahiptir. Suç kavramını dahi içinde barından sapma kavramı yine aynı şekilde toplumlara, kültürlere göre farklılıklar ortaya koymaktadır. Genel olarak toplumsal hayatın norm ve kurallarının ihlali olarak tanımlanan sapma kavramı esasen her suçu içinde barındırmaktadır. Kısaca söylemek gerekir ise yasalarla sınırlanmış olan eylem ve tutumlar olduğu kadar yazılı olamayan normların ya da kuralların çiğnenmesi de sapma olarak algılanmaktadır.

Öte yandan insanlığın gelişimi de suç ve sapma kavramlarının niteliğini değiştirmiş özellikle suç ve işleme biçimleri farklı bir boyut kazanmıştır. Günümüzde *Toplum 5.0* olarak nitelendirilen 21. yüzyılda bilgiye ulaşmak saliseler almaktadır. Teknolojik gelişmelerin hızlı bir şekilde ilerlemesi ile ağ sistemlerinin, internetin kullanımının evlerin içine kadar girmesi ve yaygınlaşması da bir o kadar hızlı olmuştur. Günlük yaşamlarında internet ve ağların kullanımına bağımlı hale gelen günümüz insanı için Bilgi ve İletişim teknolojileri (BİT) çok daha önemli hale gelmiş bulunmaktadır. Tüm dünyaya yayılan bilgi iletişim teknolojileri özelde olduğu gibi kamuda da kendisini göstermeye başlamasıyla birlikte ülkelerin ve uluslararası kuruluşların büyük bir tehditle karşı karşıya kalmasını ve herhangi bir suçun elektronik ortamda işlenebilmesini mümkün hale getirmiştir.

Bilgi, iletişim ve telekomünikasyon sistemleriyle birlikte iyice yaygınlaşan internet kullanımı, birden fazla elektronik cihazın iletişim ağları aracılığı ile karşılıklı olarak bağlantı sağlaması yeni saldırılara, suçlara ve tehditlere neden olmuş, böylece yeni bir suç türünün ortaya çıkmasında etken olmuştur. Dünyada genellikle *siber suçlar* olarak tanımlanan bu yeni suç türü, Türkiye'de *bilişim suçu* olarak adlandırılırken, dünya üzerinde *bilgisayar suçu, dijital suç, elektronik suç* gibi çeşitli şekillerde tanımlanabilmektedir. Siber suç terimi farklı şekillerde karşımıza çıksa da bu kavramların ortak noktaları bilişim sistemleriyle ve elektronik ağlar ile işlenen suçlar olmalarıdır. Bahsedilen bu suç türünde silah olarak bilgisayarlar, zararlı yazılımlar, virüsler kullanılmaya başlanmıştır. Bütün bu gelişmeler, suç algısının değişmesinde etken olduğu gibi dünya devletlerinin güvenlik anlayışlarının ve önlemlerinin de değişmesinde önemli rol oynamıştır. Fakat siber suçların hızla değişen bir yapıya sahip olması önlemleri yetersiz kılabilmektedir.

Artan bir olgu olarak siber suçların ele alındığı bu çalışmada ilk olarak suç, sapma ve siber suç kavramları tanımlanmıştır. İkinci kısımda nelerin siber suç olduğu ve siber suçların farklı tasniflerinden örnekler verilmiştir. Daha sonra siber suçların dünyada ve Türkiye'de nasıl başladığı ve nasıl devam ettiği ele alınarak siber suçun kısaca tarihi seyri ortaya konulmaya çalışılmıştır. Sonraki kısımda siber suçların, dünyada yaşanan beş büyük devrime bağlı olarak geçirmiş oldukları süreç içerisinde neden ve nasıl arttığı üzerinde durulmuştur. Son kısımda ise siber güvenlik kavramı ele alınarak siber suçlarla mücadele noktasında, öneri niteliğinde alınması gereken, önlemlere dikkat çekilmiştir.

2. SUÇ, SAPMA VE SİBER SUÇ

2.1. Suç

Sosyal birer varlık olarak insanlar, tarih boyunca ihtiyaçlarını karşılayabilmek için farklı şekillerde de olsa birbirleri ile etkileşim içinde bulunmak durumunda kalmışlardır. İnsani ihtiyaçlar hasebiyle bir araya gelerek topluluklar halinde yaşamaya başlayan insanlar, beraberinde suç olgusunu da getirmiştir. Bu bağlamda Hobbes (2007) tarafından ortaya konulan doğa durumu, suç olgusunu açıklayan önemli perspektiflerden biri olarak görülmektedir. Hobbes (2007: 92-94), doğa durumunda insanların dünyaya eşit olarak geldiklerini ileri sürmektedir. Ona göre, doğa insanları o kadar eşit yaratmıştır ki aralarındaki herhangi bir fark bu eşitliği bozacak kadar üstün değildir. Bu eşitlik düşüncesi, insanlar arasında güvensizliği doğurmaktadır. Çünkü güç ve yeterlilik bakımından eşit olan insanlar arzuladıkları şeylere ulaşmakta da eşit olduklarını düşünmeye başlamaktadırlar. Böylece insanların aynı şeyi arzulamaları ve bu arzularını yerine getirebilmek için eşit olduklarını düşündükleri tüm haklarını kullanma isteklerini doğurmaktadır. Bu durum, bireylerin çatışmasını ve insanların birbirlerinin varlıklarını sonlandırmaları isteğini de kaçınılmaz kılabilmektedir. Birbirlerine karşı üstünlük kazanma istekleri, birbirlerine karşı güvensizlik geliştirmelerinde de etkili olmaktadır. Bu güvensizlik, beraberinde suçu ve savaşı getirmektedir. Hobbes'un doğa durumunda bahsettiği güvenlik, korku, endişe ve arzular doğrultusunda insanlar, kendi varlıklarını korumak ve idame ettirmek adına suça yönelmektedir. Yani insanlık tarihi boyunca varlığını koruyan suç olgusunun, doğası gereği insanın olduğu her alanda görülmesi mümkün olmaktadır.

Marshall (1999: 702) suçu, "kişisel alanı aşıp, kamusal alana giren ve yasak olan kural ya da yasaları çiğneyen, buna bağlı olarak meşru cezaların ya da yaptırımların uygulandığı ve kamusal bir otoritenin müdahalesini gerektiren fiiller" şeklinde nitelendirirken, Güçlü ve Akbaş (2019: 2) suçu, yasalar tarafından net bir biçimde belirtilen kuralların dışına çıkılması durumunda, buna mukabil cezai bir yaptırımın öngörüldüğü her türlü fiil olarak tanımlamaktadırlar.

Sutherland'a (1974: 4) göre suç, ceza kanununca yasaklanan her türlü eylemdir ve ahlaksızlık ya da kınama düzeyi ne derece olursa olsun, bir fiil kanunlarca yasaklanmadıysa suç sayılmamaktadır. Aynı şekilde Schmalleger (2014: 2), belirli bir davranış biçimini tanımlayan bir ceza yasası olmadığı müddetçe söz konusu davranışın her nasıl olursa olsun suç olmayacağını ileri sürmektedir.

Buna göre suç olgusunun zamana ve mekana göre farklılık gösterdiğini söyleyebilmek doğru olacaktır (Alpman ve Yarcı, 2018: 146). Bazı toplumlarda suç olarak algılanan, kabul gören bir eylem yahut söylem, bazı toplumlarda suç olarak algılanmamaktadır. Ya da bugün suç olarak görülmeyen davranışın ileri bir zaman diliminde suç olarak görülme ihtimali bulunmaktadır. Bu durumda suç durağan bir olgu değildir (Bal, 2003: 180-181). Öte yandan suç; sosyoloji, kriminoloji, antropoloji, psikoloji, hukuk ve din gibi birçok disiplinin ilgilendiği ve bu alanlarda üzerine birçok çalışma yapılan bir konu olduğu görülmektedir. Farklı disiplinlerin de inceleme alanına girmesine bağlı olarak suç, farklı bakış açıları ile tanımlanmaya çalışılmaktadır (Güçlü ve Akbaş, 2019: 2). Buna bağlı olarak suç tanımında ortak bir noktada buluşmak oldukça güç olabilmektedir. Dönmezer'e (1984: 57) göre suç, çeşitli biçimlerde tanımlansa dahi tüm tanımlardaki ortak husus, bir eylemin suç olarak kabul edilebilmesi içi kanun koyucu tarafından cezalandırılmış olmasının gerekliliğidir.

Toplumsal yapı ve işleyiş içerisinde farklı düzey yahut çeşitlilikte meydana gelen ve kompleks bir yapıya sahip bir olgu olan suç; aile, din, kültür, siyaset, ekonomi, statü ve hatta insan hisleri de dahil olmak üzere toplumsal yaşamda var olan birçok alanda yinelenen bir olgu olarak karşımıza çıkmaktadır. Bu bağlamda suçun sadece hukuksal olarak

tanımlanması eksik kalmasına sebep olmaktadır. Çünkü bir toplumda suç olarak görülen eylemler toplumsal kurgulara bağlıdır ve göreceli bir yapıya sahiptir. Sosyolojik olarak bakıldığında suçun tanımını etkileyen bazı faktörler bulunmaktadır ve bu faktörlerin başında toplumun ahlak ile ilgili görüşleri ve dinsel inançları yer almaktadır (Bahar, 2009: 120). Bununla birlikte suç, bazı bireylerin eylem ve tavırları ile üyesi oldukları topluluğun model davranışları arasındaki bir tenakuzdan ibaret olabilmekte ve bu tenakuzun yer ve zaman fark etmeden zorunlu olarak var olmasından kaynaklı, evrensel bir olgu olma niteliğine sahiptir. Tarih boyunca suçun olmadığı hiçbir toplum ve bu suça karşılık yaptırımların, yasakların, cezaların uygulanmadığı bir devlet bulunmamaktadır. Ayrıca, belirtmek gerekir ki suçlar, toplumsal yapı ve koşullara göre şekillenmektedir (Dönmezer 1994: 64-72).

Macionis (2013: 230) tarafından yerel otorite, bir devlet yahut federal hükümetlerce konulan kanunların ihlali olarak nitelendiren suç, birkaç yüzyıl önce bazı düşünürler tarafından yalnızca biyolojik olarak algılanmıştır. Örneğin 1870'lerde suçlu tiplerinin belirli anatomik özellikler ile saptanabileceğini düşünen İtalyan kriminolog Cesare Lambroso tarafından suçlu olarak nitelendirilen kişiler, fiziksel yahut anatomik olarak incelenmiş ve bu özelliklerin insan evriminin önceki aşamalarından kalan özellikler olduğu ileri sürülmüştür. Bunun üzerine beden tipiyle suç arasında umumi bir korelasyon kurulmasını yadırgayan ve hatta gülünç bulan Giddens (2008: 842), kalıtımla devralınan özelliklerin de suçluluk ile bir ilişkisinin olmadığını ileri sürmüştür. Ona göre, suçun doğası ile ilgili olarak tatmin edici herhangi bir yaklaşım sosyolojik olmak zorundadır. Çünkü suç toplumsal kurumlara bağlı olarak nitelik kazanmaktadır. Bu kurumlardaki ceza hukukunun dayattığı davranış biçimleri ile ilgilenen ve suç ölçüm teknikleri, suçluluk oranlarındaki eğilimler, topluluk içindeki suçların azalmasına yönelik politikalar gibi konularla ilgilenen disiplin de Kriminolojidir.

Suçu normal bir olgu olarak gören Durkheim'a (2004: 15-16) göre, bir toplumda cezalandırmanın normal karşılandığı oranda suç da normal karşılanmalıdır. Çünkü suçun önüne geçmeye yönelik mekanizmaların var oluşu, en az suçun var oluşu kadar genel geçer bir olgu olarak görülür ve toplumun huzuru için her ikisi de hayati önem taşımaktadır. Ona göre suçu cezalandıran bir sistemin olmayışı, toplumun ahlaki değerlerindeki homojenliğin ortadan kalkmasını gerektirir. Bu durumda toplumun var olması hakikati, kendisiyle örtüşmeyen bir olgu olarak kabul edilmektedir. Durkheim, suçun direk ortadan kaldırılması düşüncesini yanlış bulur. Suç, her ne kadar nefret edilen bir unsur olsa dahi toplumda var olması gereken önemli bir olgudur. Öte yandan Durkheim'a göre, ilkel toplumlarda suç olarak nitelendirilen, kınanan fakat artık öyle görülmeyen eylemler, ilkel toplumlarla ilişkili olarak en az bugün bizlerin kabul ettiği suç kadar kriminaldir. O, değişmeye yüz tutan suçların oluşturduğu grubun, toplumsal hayatın değişen şartları içinde ve değişmeden kalanların ise toplumsal hayatın sabit şartları içinde değerlendirilmesi gerektiğini öne sürmektedir. Buna göre suçlar birbirlerinden ayrılmayarak patolojik ve normatif biçimler çerçevesinde değerlendirilmedir (Durkheim, 2004: 109-110).

2.2. Sapma

Suç sosyolojisinin çıkış noktası olarak da görülen sapma kavramının tanımı, suç kavramına nazaran daha zor yapılabilmektedir. Suç tanımları az çok benzer ve farklılıklarla genel bir tanımda kendine yer edinebilirken sapma kavramı için net ve ortak bir tanım söz konusu olmayabilmektedir. Bununla birlikte sapmanın suç kavramından çok daha geniş olduğunu hatta suç kavramını kapsadığını söylemek yanlış bir ifade olmayacaktır.

Sosyolojik olarak sapma kavramı ele alındığında görülmektedir ki birçok farklı tanım ve niteliği bulunmaktadır. Kültürel normların gözle görülür bir biçimde ihlalini sapma olarak tanımlayan Macionis (2013: 216) suçu, sapmanın bir kategorisi olarak nitelendirmektedir. Çünkü suç, toplum tarafından onaylanan, egemen tarafından resmileştirilen yasalarının ihlali iken cezai sapma; küçük bir trafik cezası, seks işçiliği yahut cinayet gibi suçlara kadar uzanan bir yelpazedir. Uyumsuzluk olarak da nitelendiren sapma ona göre olumlu yahut olumsuz da olabilmektedir. Macionis, tüm sapkınlıkların eylem ya da seçim içermediğini ileri sürmektedir. Çünkü bazı insanların varlığı dahi diğerleri için sorun teşkil edebilmektedir.

Toplumların belli bir düzen ve süreklilik içinde varlıklarını sürdürebilmeleri için normları olduğu bilinmektedir. Bu normlar, toplumdan topluma, kültürden kültüre farklılık gösterebildiği gibi aynı toplum ve kültür içerisinde de farklılıklar gösterebilmektedir. Bu normların ötesine geçmeyi anormal bir davranış olarak nitelendiren Arıkan'a (1986: 123) göre, bilinçli yahut bilinçsiz toplumda kabul edilen normal davranışların ötesine geçmeyi alışkanlık haline getirmiş kişi sapkındır. Ona göre suç ve suçluluk bir sapma davranışı olarak nitelendirilir ve toplumsal normların ihlali olarak değerlendirilen bu kapsamdaki her türlü eylem ve davranış sapma olarak kabul edilir.

Sapma, sosyal beklentilerin ihlalini içeren herhangi bir davranış olarak, suçtan daha kapsamlı biçimde değerlendirilmektedir. Çünkü sapma organizasyonun ve hatta organizasyonsuzluğun aynı anda bir ürünü olabilmektedir (İçli, 1991: 14). Hem sosyal yapının zayıflığını hem de alternatif kalıpların yaratılış ve yürütülüşünü göstermektedir. Selçuk (2014: 86) hukukçu olmayan bir kimsenin, suç kavramını teknik anlamda kullanamayacağını ileri sürmektedir. Ona göre suç kavramı geniş anlamda kullanır; yalnızca ahlaka, töreye, hukuka aykırılıklar değil, toplumdaki bütün sapmalar suç olarak kabul edilmelidir.

Merton, toplumun çok fazla sapkınlığı teşvik edecek şekilde kurulabileceğini ileri sürmektedir. Merton'a (1938: 674) göre, "sapkın davranış, kültürel olarak tanımlanmış arzular ile sosyal olarak yapılandırılmış araçlar arasındaki ayrışmanın bir belirtisi olarak görülebilir". Kişilerin içinde bulunduğu sapkınlık türü, kültürel hedeflere ulaşmak maksadı ile toplumun onlara sağladığı araçlara bağlıdır (Macionis, 2013: 220). Anomi kavramını, onaylanmış normların sosyal gerçeklik ile çatışma yaşadığında bireylerin eylemleri üzerindeki gerginliğe atıfta bulunacak şekilde değiştiren Merton (1938: 676), toplumsal olarak öne çıkarılan değerler ile toplumsal amaçlara ulaşmak için kullanılacak araçların sınırlı olması arasındaki gerilimlerle gösterilen beş olası tepki ileri sürmektedir. Bunlar; uyum gösterenler, yenilikçiler, törenciler, geri çekilenler ve başkaldıranlar şeklindedir. Öte yandan Giddens'a (2008: 445-446) göre, Merton, göreli yoksullaşmaya dikkat çekerek, sapkın eylemlerin öne çıkan bileşenlerini ortaya koymaktadır.

Fisher ve Strauss'a (1997: 480-481) göre, yukarıda bahsi geçen yapısal işlevselci yaklaşımların aslında insan eylemini açıklamak için gerekli olduğunu yahut yeterli olmadığını dile getiren Goffman, etkileşimci yaklaşımlarla dikkat çekmektedir. Etkileşim kurallarının nasıl sürdürüldüğüne, ihlal edildiğine, nasıl düzensizliğe dönüştüğüne dikkat çeken Goffman, kuralların, normların ya da rollerin yahut herhangi yapısal öğenin, davranışı kesinlikle etkilediği düşüncesine karşı tutum sergiler. Sapkınlık yahut olağan dışı davranış olarak nitelendirdiği eylemler üzerinde duran Goffman (1963), normal olamayan eylemleri psikolojik yaklaşımlar ile açıklamaya karşı gelmektedir. Çünkü Goffman'a (1963: 54) göre, sapma bir hastalık değildir. Ona göre toplumsal normlar kendiliğinden değil, topluluk üyelerinin sürekli eylemleri ile benimsenmektedir ve toplumsal kuralların varlığı, bu normlardan sapabileceğimiz, suçlanabileceğimiz, damgalanabileceğimiz böylece de topluluktan dışlanabileceğimiz anlamına gelmektedir. Goffman'a (1963: 130-133) göre, hepimiz etiketlenebilir, damgalanabiliriz. Bu durumda damgalanan bir birey sapkın olarak adlandırılıyorsa insan olarak hepimiz "normal sapkınlarız".

Sapkınlık üzerine çalışmaları ile dikkat çeken bir diğer isim olan Howard S. Becker (1963), sapma görüşü ile ilgili bilimsel teorilerin, yasaları ihlal eden bireylerin eylemlerini doğal bir sapma olarak gördüğü müddetçe ve yargı süreçleri içinde verili olduğunu varsaydıkça önemli olan bir değişkeni dışarıda bırakabileceklerini ileri sürmektedir. Becker'a (1963: 4) göre, en basit hali ile sapkınlık, istatistiklere dayanmaktadır. Dolayısıyla ortalamadan çok geniş ölçüde farklılaşan şey sapkın olmaktadır. Bu durumda en yaygın olandan farklı olan her şey sapkın olarak nitelendirilebilir. Örneğin, kızıl saçlı insanların ortalamaya göre daha az olması, sol elini kullanan bireylerin sağ elini kullanan bireylere oranla çok daha az olması gibi durumlarda kızıl saçlılar ve sol elini kullanan bireyler sapkın olarak değerlendirilmektedir. Ona göre herhangi bir vaka değerlendirilirken ortalamaya olan uzaklığı göz önüne alınarak değerlendirilmedir. Bir kural ihlaline bağlı olarak davranışı sapkın biçiminde nitelendirmek çok doğru olmayabilmektedir. Çünkü görüldüğü gibi herhangi bir kural ihlali olmadan da bazı şeyler sapkın olarak düşünülebilmektedir.

Sapkınlığın istatiksel bir tanımını yapan Becker (1963: 9), grup kurallarına uyulmaması biçimiyle de sapmayı açıklamaktadır. Sosyal bir grubun kurallar koyması bozulma ve sapmayı meydana getirmektedir. Çünkü grup kurallarına uymayan ya da kural ihlali yapan bireyler sapkın olarak görülmektedir. Bu bağlamda sapkınlıkla ilgili temel gerçek, sapkınlığın "toplum tarafından yaratılmasıdır". Ayrıca sapmayı bir birey eylemine, diğerleri tarafından verilen tepki olarak ifade eden Becker, sapkın olarak etiketlenmiş bireylerin üzerinde inceleme yapanların, homojen bir kategori oluşturduklarını ve onlarla uğraştıklarının farkına varamayacaklarını ileri sürmektedir. Belirtmek gerekir ki sapkın olarak görülen bireylerin oluşturduğu homojen grup toplumdaki diğer gruplar ile çatışma yaşayabilmektedir. Buna göre genel olarak bakıldığında sapkının, sosyal süreçler ile ilgili olduğunu söyleyebilmek mümkündür.

2.3. Siber suç

Bilgi ya da Bilişim Çağında birden fazla yeni kavramın insan hayatına girdiği bilinmektedir. Çoğunlukla yabancı kaynaklardan Türkçeye intibak eden birçok bilişim suçu kavramı mevcuttur. Bu kavramlardan en yaygın olan siber (*cyber*) kelimesi, bilgi ve iletişim teknolojilerine yönelik birçok şeyi betimlemek için kullanılmaktadır. Modern suçluların, suç işleme alanı olan bilgisayarlar ve internet vasıtasıyla gerçekleştirdikleri suç eylemlerine ise siber suç adı verilmektedir (Gray, 2014: 4-6). Genellikle bilgisayarlar, akıllı telefonlar veya internet kullanılarak işlenen her türlü suç için siber suç kavramını kullanılmaktadır.

Siber suç (*cybercrime*) "yasadışı olan ya da belirli taraflarca yasa dışı sayılan ve küresel elektronik ağlar aracılığıyla yürütülebilen faaliyetler" (Küçükvardar, 2018: 4) olarak tanımlanmaktadır. Ayrıca bu suç türünün yasalar tarafından sınırları çizilmemiş, toplumsal normları içine alan ve istenmeyen, onaylanmayan eylemleri de içinde barındıran bir yapıya da sahip olduğu bilinmektedir.

Bilişim kavramı, belgeleme tekniği adı verilen bir yöntemin disiplin olarak kabul edilmesi ile doğmuş, günümüze kadar gelişmiş ve günümüzde de hızla gelişmeye devam eden bir kavramdır. İlk olarak bilginin saklanması ve erişimi gibi çalışmalar için kullanılan bu kavram, yaşanan teknolojik gelişmeler ile birlikte bir bilim haline gelmiştir. Kalay (2019: 133), bilişim kavramının Fransızca da *informatique* ve Türkçede *enformatik* biçiminde kullanılan bir kavramdan türetildiğini ifade etmektedir. İngilizce olarak da *information* sözcüğünden gelen bilişim kavramı

Türkçeye *enformasyon* biçiminde geçmiştir (Akbulut, 2017: 13; Dülger, 2020: 66). Daha sonra yabancı kökenli sözcük yerine bilişim kavramı tercih edilmeye başlanmıştır.

Türk Dil Kurumunda (TDK) [1] enformatik, "İnsanoğlunun teknik, ekonomik ve toplumsal alanlardaki iletişiminde kullandığı ve bilimin dayanağı olan bilginin özellikle elektronik makineler aracılığıyla düzenli ve akla uygun bir biçimde işlenmesi bilimi." olarak tanımlanmaktadır.

Türk Ceza Kanunu'nda (TCK) 1991'de değişikliğe gidilerek *bilgisayar kullanarak işlenen özel suçlar* yani *bilişim suçları* düzenlenmiştir. Ceza kanunda bahsi geçen suçlar tasnif edilirken "bilgileri otomatik işleme tutulmuş bir sistem" ibaresi kullanılarak, bir sistemden bahsedilmektedir. Bu sisteme ise bilgisayar ve veri kullanımı şekli ile ilgili olarak bütün bilişim cihazları dahil edilmektedir (Gökrem, 2000: 10-45).

Bilişim sistemine girme suçunun oluşması ve bir eylemin bilişim suçu olarak kabul edilmesi için sisteme girmenin hukuka aykırı olarak gerçekleşen bir eylem olması gerekmektedir (Kalay, 2009: 134). Öte yandan bilişim sisteminin sahibi izin vermediği durumda ya da başlangıçta rıza gösterse dahi sisteme giriş yapıldıktan sonra kişisel bilgiler veya kişisel sebeplerden dolayı kişinin sistemden çıkmasını istemesi durumunda sistem içerisinde kalmaya devam etmesiyle de suç gerçekleşmektedir.

3. NELER SİBER SUÇ?

Bir şeyin suç olup olmadığı yasalarca belirlenen bir husus olduğu ve yasalar tarafından yapılmaması gereken ya da yasal olarak belirlenmeyen eylemlerin, suç olarak kabul edilmediğinden daha önce bahsedilmişti. Bu bağlamda nelerin siber suç olduğu önemli bir soru olmaktadır. Siber suçların neler olduğunu açıklamak için esasen yasal düzenlemelere bakmak gerekmektedir. Bu bağlamda insanoğlunun sürekli olarak değişim ve gelişim içinde olması insan unsuru olan suçları da oldukça etkilemektedir. Özellikle siber suç, geçmişten günümüze oldukça değişmiş çeşitlenmiş ve değişmeye de devam etmektedir. Durağan olmayan bu süreç içerisinde toplulukların kendilerine özgü ya da evrensel birtakım kural yahut yasaları bulunmaktadır. Bu kural ya da yasalar çerçevesinde nelerin suç olduğu belirlenmektedir. Fakat toplumdan topluma yasaların, normların değişmesi hem suçların hem de cezaların farklı tasniflerine sebebiyet vermektedir. Hem bu duruma bağlı olarak hem de sınırlarını henüz net bir şekilde bilinemeyen sanal dünya değişimleri ile birlikte siber suç tasnifleri de farklılık göstermektedir. Çalışmanın bu bölümünde, siber suçların neler olduğu hususunda birkaç farklı sınıflandırma örneği verilerek TCK'ye göre siber suç üzerinde durulacaktır.

Erken dönem siber suçlar ile ilgili olarak yasal düzenlemeler araştırıldığında siber suç vakalarının belirleyici alt kümesini kanıtlayan iki önemli tüzüğün olduğu dikkati çekmektedir. Bu tüzükler; değerli bir şeyden belirgin biçimde yoksun bırakılan davranış ve mülkiyet suçu tüzüğü uyarınca hazırlanan iddianamelerdir. Bununla birlikte siber suç yasalarının mülkiyet hukukuna sık sık atıfta bulunarak geliştiği görülmektedir. Mülkiyet hukuku bağlamında siber suç yasalarına Bilgisayar Sahtekarlığı ve Kötüye Kullanımı Yasası (CFAA) ve Dijital Binyıl Telif Hakkı Yasası (DMCA) gibi tüzükler bulunmaktadır. Fakat mülkiyet temelli siber suç tüzükleri, çoğu elektronik iletişim yasal korumasında sınırlamalara yol açmaktadır. Telefon sahtekarlığı, posta sahtekarlığı, hırsızlık ve izinsiz girişler gibi eylemler içeren suç tüzüklerinin erken siber suç kovuşturmalarına kısmen karşılık geldiği görülmektedir. Bunların geneli ilk olarak mülkiyet suçları altındaki kavuşturmalarda yer almaktadır. Öte yandan 1900'lü yıllarda bu hususta bazı kanunlar öne çıkmıştır. Örneğin; 1973 yılında İsveç'in, Veri Koruma Kanununu çıkardığı, 1974 yılında Amerika Birleşik Devletleri (ABD)'nin Özel Hayatın Korunması Kanuna yer verdiği, 1977 yılında Almanya tarafından Federal Veri Koruma Kanununun çıkarıldığı, 1978 yılında Fransa'nın, Bilişim, Fişyeler ve Özgürlükler Kanununu kabul ettiği ve 1979 yılında ise Lüksemburg'un bilgisayar uygulamalarına ilişkin bir kanun çıkardığı bilinmektedir.

Birçok ülke benzer yasalar ile hukuki yaptırımlarını genişletmiştir. Öte yandan suçların süregelmesi ve sürekli olarak değişiklik göstermesi durumunda yasal belirsizlikler dikkati çektiği için yasalarda da buna bağlı olarak değişime gitmek durumunda kalındığı bilinmektedir. Örneğin, yeni tüzükler ışığında bilgisayarlara yetkisiz giriş net bir şekilde suç olarak kabul edilmiştir. Artık suç kapsamı fiziki mülkiyet hakkından fikri mülkiyet hakkına da geçiş yapmıştır. Esasen Dijital Binyıl Telif Hakkı Yasası (DMCA) tüzüğü, fikri mülkiyete dayandırılmaktadır ve telif hakkı gündeme gelmiştir. Bu süreç içerisinde Amerika Birleşik Devletleri (ABD), Elektronik Hırsızlık Yasası'nı (NETA) kabul ederek siber suça yeni bir nitelik kazandırmıştır (Burstein, 2003: 313-338; Akbulut, 2017: 30-37). Daha sonra 1984 tarihli Sahte Erişim Aygıtı ve Bilgisayar Sahtekarlığı ve Kötüye Kullanımı Yasası (CFAA) doğmuştur. Bu yasa erişimden kaynaklanan çeşitli cezai ihlalleri içermiştir ve kapsamında "virüs", "solucan", "Truva atı" zarar verici yazılımlar suç kategorisine alınmıştır. 1996 yılında Elektronik Casusluk Yasası (EEA) çıkarılmıştır ve ticari sırların ihlali suç sayılmıştır. O dönemler lisanssız programların kullanımı, kopya programlara erişim ve bu programların dağılımı ticari sırların ihlali altında suç olarak görülmüştür ve cezai uygulama örnekleri bulunmaktadır. Bu yıllardan sonra artan teknoloji kullanımı ve teknolojik gelişmelerin etkisiyle birlikte birçok ülkede siber suçlar ile ilgili düzenlemeye gidildiği bilinmektedir.

[1] https://sozluk.gov.tr/, E.T. 09.11.2021.

Yukarıda bahsi geçen süreç zaman içerisinde bireylerin diğer birey ya da topluluklara karşı rahatsız edici eylemlerine bağlı olarak geliştirilmiş, genişletilmiştir. Günümüzde hala eylemlerin ve vakaların seyrinde değişikliklere gidilmektedir. Bunların çok çeşitli örnekleri bulunmaktadır. Aynı şekilde mevcut siber suçun sınırlarının ayrı bir bölüm olarak çizildiği örnekler de mevcuttur. Bu örneklerden birkaçı fikir vermesi açısından aşağıda verilmiştir.

S.M. Furnell'ın (2001: 36), gözden geçirdiği *(UK) Birleşik Krallık Denetim Komisyonu (1998)* sınıflandırması:

- ✓ *Dolandırıcılık:* kişisel kazanç ya da menfaat için yetkisiz bilgisayara giriş, verilerin değiştirilmesi, yok edilmesi, kötüye kullanımı.
- ✓ *Çalmak*: veri ya da yazılımları çalmak.
- ✓ *Lisanssız yazılım kullanmak*: yasa dışı yazılım kopyaları kullanmak.
- ✓ *Kişisel verilerin kötüye kullanımı*: bilgisayar kayıtları ve veri ihlalleri arasında resmi olmayan *tarama* koruma mevzuatı.
- ✓ *Özel iş ihlali*: kuruluşun bilgi işlem olanaklarının özel kazanç için yetkisiz kullanımı veya yarar.
- ✓ *Hackleme*: Bilgisayar sistemlerine kasıtlı olarak yetkisiz giriş.
- ✓ *Pornografik materyal tanıtımı*: internetten pornografik materyal indirme tanıtımı vermek.
- ✓ *Virüs*: Bilgisayar sürecini bozmak maksadı ile programı dağıtan bir virüs.

Ngafeeson (2010), tarafından gösterilen Fraser'ın(1996) düzenlediği FBI'ın *Ulusal Suç Birimi* siber suç sınıflandırması şu şekildedir:

- ✓ Genel Anahtarlamalı Ağın İzinsiz Girişleri (telefon şirketi),
- ✓ Büyük bilgisayar ağı izinsiz girişleri,
- ✓ Ağ Bütünlüğü ihlalleri,
- ✓ Endüstriyel casusluk,
- ✓ Korsan bilgisayar yazılımı,
- ✓ Suçun işlenmesinde bilgisayarın önemli bir faktör olduğu diğer suçlar.

Bir farklı sınıflandırma da *Bilgisayar Güvenliği Enstitüsü (CSI)* (CSI/FBI, 2001)'nün sınıflandırmasıdır:

- ✓ Hırsızlık ve özel bilgiler,
- ✓ Veri veya ağların sabote edilmesi,
- ✓ Telekom dinleme,
- ✓ Dışarıdan gelen sistem sızması,
- ✓ Net erişimin içeriden suistimal edilmesi,
- ✓ Finansal dolandırıcılık,
- ✓ Hizmet Reddi,
- ✓ Sahtekarlık,
- ✓ Virüs,
- ✓ Yetkisiz içeriden erişim,
- ✓ Telekom dolandırıcılığı,
- ✓ Aktif telefon dinleme,
- ✓ Dizüstü bilgisayar hırsızlığı.

TCK'ye göre siber suç olarak kabul edilen fiiller, ilk olarak 765 sayılı TCK'da kendine yer edinmektedir (Açıkgöz, 2020: 45-59). 1 Haziran 2015 tarihinde siber suçlar, 5237 sayılı kanunla, topluma karşı suçlar bölümü düzenlenerek "bilişim alanında suçlar" olarak tasnif edilmiştir. Bunlar kısaca şu şekildedir:

- ✓ Bilişim sistemine girmek veya orada kalmak (m.243).
- ✓ Veri nakillerini teknik araçlar ile izlemek (m.244).
- ✓ Bilişim sistemini engellemek, bozmak, verileri yok etmek veya değiştirmek (m.245)

- ✓ Bankaya veya kredi kartlarının kötüye kullanılması (m.245).
- ✓ Yasak program veya cihazların üretilmesi ve ticareti.

TCK'de "bilişim alanında suçlar" dışında "diğer suçlar" olarak geniş anlamda bilişim suçuna dahil olarak görülen "özel hayata ve hayatın gizli alanına karşı suçlar" da bulunmaktadır (Dülger, 2020: 236-237). Burada suç olarak kabul edilen verilerin ihlali, verilerin kötüye kullanımı, haberleşme ve özel hayatın gizliliğinin ihlalidir. Ayrıca TCK'nin çeşitli bölümlerinde siber suçlar ile ilgili olarak bilişim sistemleri vasıtasıyla olanaklı suç tipleri de yer almaktadır. Bu suçlar şunlardır:

- ✓ Haberleşmenin gizliliğinin ihlal edilmesi,
- ✓ Haberleşmenin engellenmesi,
- ✓ Hakaret etmek,
- ✓ Bilişim sistemi yolu ile hırsızlık,
- ✓ Bilişim sistemi yolu ile dolandırıcılık,
- ✓ Müstehcenlik,
- ✓ Kumar oynanması için yer ve imkan sağlamak.

Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK, 2019) siber suç tasnifi:

- ✓ Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim,
- ✓ Bilgisayar Sabotajı,
- ✓ Bilgisayar Yoluyla Dolandırıcılık,
- ✓ Bilgisayar Yoluyla Sahtecilik,
- ✓ Bir Bilgisayar Yazılımının İzinsiz Kullanımı,
- ✓ Kişisel Verilerin Kötüye Kullanılması,
- ✓ Sahte Kişilik Oluşturma ve Kişilik Taklidi,
- ✓ Yasadışı Yayınlar,
- ✓ Ticari Sırların Çalınması,
- ✓ Terörist Faaliyetler,
- ✓ Çocuk Pornografisi,
- ✓ Hacking,
- ✓ Diğer Suçlar (Organ, fuhuş, tehdit, uyuşturucu, vb.).

Yukarıdaki sınıflamalardan da anlaşılacağı gibi sosyo-kültürel yapılanmaların şartlarına, dönemin özelliklerine ve bu suçları işleyenlere göre konu ile ilgili sınıflandırmaların yapıldığı, zaman içinde ekleme ve çıkarmalarda bulunulduğu dikkati çekmektedir.

4. SİBER SUÇLAR DÜNYADA NASIL BAŞLADI VE NASIL DEVAM ETTİ?

Ross'a (2010: 11) göre, David S. Wall isimli İngiliz uzman siber suç tarihinin üç farklı aşamaya bölünebileceğini savunmaktadır. Bunlar; (1) geleneksel ya da sıradan suçlar, (2) hibrit siber suçlar, (3) gerçek siber suçlar şeklindedir. Wall'ın (2007: 44-48) tasnif ettiği birinci nesil suçlar, ilk nesil siber suçlar olarak geçmektedir ki bu suçlar ayrık bilgi sistemleri içinde gerçekleşen suçlar yani iletişim ve bilgi sistemlerini kullanarak suç tasarlama, suça hazırlık aşaması gibi düşük uçlu siber suçlardır. İkinci nesil suçlar ya da hibrit suçlar, ücretsiz telefon görüşmeleri yapmak için telefon sistemlerini kırmak gibi bilgi işlem sistemlerine erişim sağlanarak işlenen suçlar yani ağlar arasında işlenen suçlar olarak kabul edilmektedir. Üçüncü nesil suçlar, ilk olarak 21. yy'da çevirmeli modem erişiminin geniş bant ile toptan değiştirilmesiyle gerçekleşmeye başlayan, gerçek siber suçlar olarak geçen, tamamen teknolojinin aracılık ettiği suçlardır. Bu suçlar spamlar, virüsler, vb. gibi yollar ile tamamen ağ teknolojileri vasıtasıyla gerçekleşmektedir.

Dünyada kayıtlara geçen ilk bilişim suçunun 1958 yılında Amerika'da gerçekleştiği bilinmektedir. Siber suçların tarihi 1960'lı yıllarda meydana gelen birtakım olaylar nedeniyle "bilgisayar suçları" ya da "bilgisayar ile ilgili suçlar" şeklinde basında yer alan ve bilimsel çalışmalarda çıkan yazılara dayanmaktadır. Savcılık tarafından takibe alınan ilk siber suçun Amerika'da 18 Ekim 1966 tarihli *Minneapolis Tribune* gazetesinde yayınlanan hesaba para aktarma ile ilgili bir haberle kamuoyuna duyurulduğu bilinmektedir (Dülger, 2012: 97).

Tarihte işlenen ilk bilişim suçları günümüzdeki şeklinden farklı olarak meydana gelmiş bulunmaktadır. Örneğin, bilişim suçu olarak bilinen suç ABD'de Bell telefon sisteminden bir kısım gencin telefon görüşmelerini ücretsiz bir şekilde yapmak için yeni yöntem arayışlarıyla başlamıştır (Kurt, 2005: 54). "*Phreakers*" adı verilen bu gençler işin eğlencesinde yer alırken yaptıkları eylemin suça meylettiklerinin farkında değillerdi. Bu gençler, aramalar arasındaki boşluklardan yararlanan yetenekli ve bilgili gençlerdi. Bu en eski Pekarslar'ın çoğu kısmen kör çocuklardı. "*Phreaking*" yani dolandırıcılık onlar için üstün olabilecekleri bir şeydi. Bu çocukların konuşmak için görmeye ihtiyaçları yoktu, duymaya ve elektronik bir yeteneğe ihtiyaçları vardı. Bu da zaman içinde onlar için doğal bir hobiye dönüştü. Amaçları teknolojiyi özgürleştirmekti (Mungo ve Clough, 1992: 3). Gençlerin eylemleri sadece kendi arkadaş çevreleri ile sınırlı kalırken bu süreçte telefon şirketlerini dolandırıyorlardı. Bu onlar için teknolojiyi özgürleştirmek iken suç işlediklerinin farkında değillerdi.

Phearker'lar, uzun yıllar faaliyetlerini sürdürdü. Fakat Ekim 1971'de *Esquire* dergisi, onların habercisi olmuş ve Amerikan kamuoyuna bu durumu duyurmuştur. Ron Rosenbaum tarafından yazılan *The Secrets of the Little Blue Box* isimli makale ile kitlesel dolaşımda korsanlığın ilk açıklaması yapılmıştır. Rosenbaum, makalesi ile dolandırıcılık hareketinin popülerleştiricisi olarak görülmektedir (Mungo ve Clough, 1992: 4-6). Bu ilk nesil dolandırıcıların ilham kaynağı Mark Bernay'dır. Aslen gerçek isminin bu olmadığı ve takma isim kullandığı düşünülen Bernay, telefon kullanıcılarının ücretsiz arama yapmasını sağlayan mekanizması ile tanınmaktadır. Bu durum insanların sadece ücretsiz konuşma yapmasına fayda sağlamamış ayrıca *Ma Bell* isimli ünlü telefon şirketinin sistemi içerisinde elektronik geçit ve bölümler olduğunu da keşfederek sistemin açığını bulmuştur.

Geçmiş dönemlerde siber suçların yayılışında çok etkili olan *Captan Crunch* lakaplı Draper'in, bir makalesinde Phreaking ve Hacking taktiklerini uyuşturucu satıcılarının dünyasına ve yer altı dünyasına duyurduğu ileri sürülmektedir (Kurt, 2005: 55). Hapse giren Draper bilgilerini hapishanede de yaymaya devam ederek suçlulara telefonları dinlemeyi, güvenli devre kurmayı öğretmiştir. Sonraki yıllarda YIPL (Uluslararası Gençlik Parti Hattı) kurucularından olan A.Hoffman 1973 yılında Draper ile bağlantıya geçerek suç sayısının günden güne artışına sebep olan, TAP'yi (Teknolojik Yardım Programı) kurmuş ve telefon dinleme, phreaking teknikleri üzerine okuyucularıyla bilgi paylaşımında bulunmuştur.

Bir bilgisayar programcısı olan ve ilerleyen yıllarda sosyal bir fenomen haline gelen Bernay, zaman içinde merakını başka yönlere çevirmeye başlamış ve yazdığı programlarla başka sistemlere girmeyi başarmıştır. Yaptığı şeyler ile yakalanmak istemeyen fakat başkalarını etkilemek isteyen Bernay hususi olarak arkasında ipuçları bırakmakta bunu da "*The Midnight Skulker*" imzası ile yapmaktadır (Mungo ve Clough, 1992: 18). Burada suçun evrimi gün yüzüne çıkmaya başlamıştır.1979 yılında yine Ron Rosenbaum yayınladığı bir makalesinde bilgisayara girme işini tarif etmiş ve bunu net bir şekilde adlandırmamıştır. Daha sonra Kurt (2005: 53) bu tarifi "hacking'den başka bir şey değil" şeklinde belirtmiştir.

Hacking, yani hacklemek olarak bilinen yeni nesil suç, fikri bir mülkiyet hırsızlığı ya da müseccel bilgilerin çalınmasıdır. Yetkisiz başka birinin bilgisayarına bağlanarak kişisel ya da ticari sırlar gibi özel bilgilere erişim sağlamak süratiyle gerçekleşmektedir. İlk *hack* olarak tanımlanan şey ilk nesil filmler olarak bilinmektedir. İlk nesil filimler de erkek hackerlar tanıtılmıştır. İkinci nesil filmlerde, bilgisayar korsanları tasnif edilmiş ve üçüncü nesil filimler de ise sanal ortamlar, hack ve hackerlar tanımlanmıştır (Ross, 2010: 27-28).

Öte yandan 1960 ve 1970 yılları arasında *Massachusetts Institute of Technology* (MIT) isimli enstitüde *Tech Model Railroad Club* (TMRC) akademik keşifler sayesinde, bilgisayar donanımı ve yazılımı icat edilme fırsatı yakalanmıştır. MIT öğrencileri bilgi ve becerileri ile ilk hackerlar olarak kabul edilmektedirler (Schell ve Martin, 2004: 4-5). O dönemde hack kavramı teknik odaklı bireyi temsil eden bir kavram olarak kullanılmıştır. Daha sonra bir grup haline gelen hackerlar, ilk olarak suç işlemek ya da suçlu olarak ortaya çıkmadıkları görülmektedir. Onlar sadece karşılaştıkları sorunları gidermeye çalışırken bir yandan da yeni yazılım türleri geliştirmeye çalışmışlardır. Serbestçe erişilebilir bir bilgi birikimi oluşturulmaya çalışırken bilgisayar kodlarını paylaşmaya başlamışlar ve böylece bir hacker grubu oluşturulmuştur. Bu grup amaçları ve ilkeleri doğrultusunda "beyaz şapkalı hackerlar" olarak adlandırılmıştır. Yukarıda daha önce bahsedilen Rosenbaum'un yazılarında yer verdiği hackerlar için ise siyah şapkalı hackerlar ifadesi kullanılmıştır.

1970'li yıllardan sonra Avrupa'da bahse konu suçların sayısı hızla artmaya başlamıştır. 1970'li yılların ortalarına gelindiğinde ise kriminolojik çalışmalar başlamış ve bilgisayar ile işlenen suçların artıyor olduğu tespit edilmiştir. Esas olarak bilişim suçlarının bilimsel ve genel öngörüleri 1980'li yıllara dayanmaktadır (Akbulut, 2017: 52-54). Kişisel bilgisayarların üretime ve kullanıma sunulmasıyla birlikte bilişim suçlarının da değişime uğradığı dikkati çekmektedir. Bilgisayarların sadece hukuka aykırı çıkar sağlama amaçları için kullanımı dışında kişilik haklarının ihlali gibi maksatlar ile de kullanılmaya başlanması bu duruma bir örnek olarak gösterilebilir. Bu yıllarda bankamatiklerin, iletişim ağlarının kötüye kullanımı gibi birçok siber suç da yaygınlaşmıştır. 1988'e gelindiğinde siber suçların işlenmesinde kurtçuk ve virüslerin önemli bir tehlike oluğunun farkına varılmıştır.

1989 yılında büyük çaptaki ilk hack olayını Almanlar gerçekleştirmiştir. Yapılan araştırmalara göre ABD Savunma Bakanlığı dosyalarına erişmek için Alman hackerlar kullanılmıştır. 2002-2003 verilerine göre Almanya'daki

şirketlerin %50'sinden fazlası küçük çaplı siber saldırılara maruz kalmıştır (Karagülmez, 2005: 118). Fakat Almanya'da bu duruma rağmen, siber güvenlik kapsamında, bilişim suçları ayrı bir yasa olarak çıkarılmamış sadece Ceza Kanunu içerisinde düzenlemelere gidilmiştir.

1990'lı yıllarda hayatımıza giren bilgisayarlar ve bilgisayar ağları ile birlikte kullanımı yaygınlaşan "siber uzay" kavramı ve "siber ortam" denilen sanal bir dünyanın kapılarının açılmasıyla temelde sistemlerle ilgili çok daha fazla bilgi edinmeye yönelik saldılar yapan bilgisayar korsanları(hacker) da hayatımıza girmiş oldu. O yıllarda bu tür saldırılar ego üzerine kurulu olurken büyük bir hızla gelişen teknoloji ile saldırıların hedefi de yön değiştirmiş ve günümüzde ekonomik getiriye dönüşmüştür (Parlak, 2016). Bu durum fail ile mağdur arasındaki fiziksel sınırları da ortadan kaldırmış ve suçu kolay işlenebilir bir hale getirmiştir. Artık bilgisayar korsanlığı boyutunu, amacını aşmış ve sınır tanımayan, illegal amaçlar için kullanılan bir suça dönüşmüştür.

Bu tip suçlara, *siber suç, dijital suç, bilgisayar suçu* gibi adlandırmalar yapılması, suç olan şeyin ne olduğu yahut ne olmadığı hususunda net tanımlamalar olmamasına rağmen suçun hedefi, işleniş biçimi vb. faktörlerle bilişim suçlarının çeşitlilik gösterdiğini ortaya koymaktadır. İçerisinde bulunulan ve bilgi çağı olarak adlandırılan bu dönemdeki hızlı gelişmeler *bilişim suçları* kapsamında birçok farklı şekillerde nitelik kazanan suçlarla karşı karşıya kalınmasına sebep olmuş ve olmaya da devam edecek gibi görünmektedir.

1990'ların ortalarında, internetin tam teşekküllü bir kamu ağı haline gelmesiyle birlikte bir siber alan oluştuğu fikri ortaya çıkmıştır. Bu fikir bizim karşımıza yukarıda bahsi geçen siber uzay kavramını çıkartmıştır. Siber uzay kavramını ilk kullanan kişinin William Gibson olduğu bilinmektedir (Agre, 2002: 149). Ünlü bilim kurgu yazarı olan Gibson'ın, *Neuromancer* isimli romanından gelen siber uzay kavramı, süreç içerisinden onun tanımından yola çıkarak akademik söylem ve kültürel alanlara konu olmuştur. Gibson'nın (1994: 51), "İnsan sistemindeki her bilgisayarın bankalarından soyutlanan verilerin grafik bir temsili" şeklinde nitelendirdiği "siber uzay" kavramı onun anlatımına göre rızaya dayalı bir halüsinasyon, tıpkı şehrin ışıkları gibi veri kümelerinden takım yıldızlara kadar uzanan ışık çizgileridir.

2000'li yıllara gelindiğinde bilişim suçları artmaya devam etmektedir. Artık bilişim suçlarının büyük bir kısmı ağlar aracılığı ile işlenmeye başlamıştır. Kredi kartlarının kötüye kullanımı, kişi verilerinin ihlali, özel verilere erişim, verilerin yayılması, tahribi, izinsiz dağıtımı gibi birçok suç eylemi gerçekleştirilmiştir (Akbulut, 2017: 53). Bu süreç içerisinde giderek hukuk, penoloji, kriminoloji, sosyoloji alanlarında siber suçlara yer verilmeye başlanmış ve günümüze kadar bu süreç devam etmiştir. Günümüzde siber suçun farklı boyutları, türleri kendini göstermektedir ve gelişen teknoloji ile birlikte bu husus sürmeye devam edecek gibi görünmektedir.

5. SİBER SUÇLARIN TÜRKİYE'DEKİ SEYRİ

Türkiye, ilk olarak 1987 yılında internet ile tanışmıştır. Bu gelişme, Ege Üniversitesi tarafından öncülük edilen, Türkiye Üniversite ve Araştırma Kurumları Ağı vasıtası ile gerçekleştiği bilinmektedir (Gökrem, 2000: 32). Ancak esas olarak Türkiye, 12 Nisan 1993 tarihinde Ankara-Washington arası kiralanan bir hat aracılığı ile kurulan bağlantı sayesinde interneti bünyesine almış ve Nisan 1993 tarihinden bu yana Türkiye internet ile bağlantılı bir duruma gelmiştir. Türkiye'nin internete ilk bağlantısı ODTÜ'den gerçekleştirilmiştir. 1996 yılına kadar internet bağlantısını sağlayan ODTÜ görevini Turnet'e bırakmıştır. 1999 yılında ise Turnet kapanmış ve TTNet tüm Türkiye'ye internet hizmeti vermeye başlamıştır.

Türkiye'de 2000 yılına gelindiğinde internet kullanıcı sayısı iki milyon olduğu tahmin edilmektedir ve kullanıcı sayılarının büyük bir hızla arttığı öne sürülmektedir. Dünyada ise milyonlarca insan bilişim bağlantılı olan bu sistemin içerisinde paylaşımlarda bulunmaya, bilgi edinmeye ve alışverişlerini dahi bu sistem ile yapmaya başlamıştır (Akdağ, 2009: 36). Ülkemizde de seyir benzer şekilde gerçekleşmiş hatta internet kullanımı pek çok ülkeye göre çok daha hızlı yaygınlaşmıştır.

İnternet kullanımının küresel olarak istatistikleri incelendiğinde, en yüksek kitlenin Amerika Birleşik Devletleri'nde olduğu görülmektedir. Verilerden elde edilen bilgilere göre uzak doğu ülkelerinin de 2007 yılından itibaren internet ile yakından ilişkili oldukları görülmektedir. Türkiye'de de aynı şekilde internet kullanımı, yıllara göre hızlı bir artış göstermiş ve 2007 yılından sonra 16 milyon kullanıcı ile küresel olarak en fazla internet kullanıma sahip ülkeler arasında 17. ülke olarak sıralamadaki yerini almıştır (Akdağ, 2009: 37-39). 30 Haziran 2007 yılında *Miniwatts Marketing Group*[2] tarafından hazırlanan rapor, *Nielsen/NetRatings, International Telecommunications Union,* resmi ülke raporları ile birlikte bunun yanında diğer güvenilir araştırma kaynaklarına dayanarak, ülkemizde yıllara göre internet kullanımının hızlı bir yükseliş içinde olduğunu söylemek mümkündür. Sunulan istatistik ve verilere göre 2000 yılında internet kullanıcısı sayısı 2 milyon iken 2004 yılına gelindiğinde 3,5 milyon arttığı, 2008 yılında 26 milyon 5 yüz bin kişiye ulaştığı bilinmektedir. Öte yandan 2008 yılından itibaren dünya genelinde internet kullanıcısı

[2] 2007, Miniwatts Marketing Group, http://www.internetworldstats.com/stats.htm E.t. 20.11.2021

sayısı ile Türkiye 13. sırada yer almaktadır. 2019 yılına gelindiğinde ise *M.Group Raporu*'na göre[3], Avrupa ülkeleri arasında Türkiye, internet kullanıcısı oranında 3. sırada yer almaktadır.

İnternet kullanımının çok hızlı artıyor olması sanal alemde meydana gelen suç türleri ile ilgili yasal düzenlemelerin gözden geçirilmesini zorunlu hale getirmiştir. O güne kadar suç kapsamında olan eylemlerin ihbar kapsamında birçok farklı kuruma çeşitli yollar ile iletilmesi, istatistiki verilerin tekdüze olması açısından sorun yaratmakta olduğu görülmüştür. Bu bağlamda siber suçlar, ilk olarak TCK literatürüne 2756 sayılı Kanunla *Bilişim Suçu* kavramı şeklinde girmiştir. Akademik kayıtlara bakıldığında bilişim suçu, bilgisayar suçları, siber suç gibi daha birçok kavram birbirinin yerine kullanılmaktadır. Bu kavramlar, bilişim alanındaki gelişmelere ve zaman içerisindeki işlenen suçlara göre değişiklik göstermektedir.

Bilgisayar suçları ile ilgili ilk düzenlemeler yapıldığı dönemde internet ve iletişim günümüzde olduğu kadar yaygın olmadığı için bu iki kavram bazen birbirinin yerine kullanılmıştır. Bilişimin bir parçası olan internette işlenen ve siber suç tanımlarının içine girmeyen suçlar da bulunmaktadır. Bu suçlar verilerin işlenmesi ile ilgili değil iletimi ile ilgilidir ve bu suçların tamamının siber suç kavramı ile açıklanması mümkün değildir. Bilişim teknolojileri ile bilgisayar suçlarının dışında başka suçların da işlenebiliyor olması, farklı suç saha ve kategorilerinin ortaya çıkmasında etkili olmuştur.

Tıpkı dünyada olduğu gibi Türkiye'de de internet kullanımının artması ile birlikte siber suçlar da ortaya çıkmaya başlamıştır. Türkiye'de siber suçun ilk örneği, rehber öğretmeni olan Özgen İmamoğlu'nun çocukların pornografik görüntülerini çekip internet vasıtası ile satmak iddiasıyla yakalandığı olay olarak gösterilmektedir (Kurt, 2005: 54). Ancak o dönem TCK'deki bilişim suçlarının çerçevesi net değildir. Türkiye'nin tescilli ilk hackerı Tamer Şahin olarak tarihe geçmiştir. Şahin, 2002 yılında Bill Gates ile Steve Ballmer'in e-postaları ve dokümanları gibi belgeler Microsoft Bilgisayar sistemlerine giriş yaparak internette yayınlamıştır. Ayrıca Şahin, Türkiye'nin ilk yerli bilgi güvenliği yazılımının (Mind-wall IDS) geliştiricisi olarak da bilinmektedir (Yazıcı, 2012: 14).

Sanal alemdeki suç işleme oranları yıllar içerisinde git gide artış göstermiştir. Geçmiş yıllara bakıldığında eldeki ilk verilere göre 1998 yılında Türkiye'de işlenmiş olan siber suç dosya sayısı sadece 5 iken 2001 yılında bu sayının 136'ya yükseldiği görülmektedir. Türkiye'de siber suçların, sahtecilik, yasadışı yayınlar (müstehcen yayınlar), dolandırıcılık, bilgisayar sabotajı gibi suçlar üzerinden geliştiği görülmektedir (Tanyeri ve Civelioğlu, 2007: 98).

Bilgi Teknolojileri ve İletişim Kurumu (BTK), Telekomünikasyon İletişim Başkanlığı (TİB), İnternet Daire Başkanlığının [4](İDB, 2008: 33) 23.11.2007 ve 01.11.2008 arasında gelen ihbarlar olarak hazırladığı rapora göre, internet ağında kanun dışı olan içeriklere ilişkin 28 bin 595 ihbar yapıldığı görülmektedir. Ancak, ihbarların sadece 14 bin 503'ü için işlem başlatıldığı ve ihbarların birçoğunun müstehcenlik üzerine yapıldığı ve sayısının 8 bin 498 olduğu bilinmektedir. Öte yandan en az yapılan ihbarların, sağlığa zarar veren tehlikeli madde teminiyle ilgili olduğu ve sayısının 67 olduğu görülmektedir.

Kaçakçılık ve organze suçlarla Mücadele Daire Başkanlığı (KOM) 2008 raporuna [5]göre, Türkiye' de siber suçlar ile ilgili yapılan çalışmalarda karşılaşılan suç türleri şu şekildedir:

- ✓ İnteraktif banka dolandırıcılığı,
- ✓ Banka veya kredi kartı dolandırıcılığı veya sahteciliği,
- ✓ Hesap bilgileri ve kart bilgilerinin bilişim sistemleri ile elde edilmesi,
- ✓ ATM ve diğer sistemler üzerinden finans, şifre bilgilerinin elde edilmesi amacıyla bilişim sistemlerine sızılması,
- ✓ Bilişim sistemlerine girme, sistemi engelleme, bozma, verileri yok etme veya değiştirme,
- ✓ Zararlı programlar ile bilişim sistemlerinde kullanılan yazılımların kırılması veya çalınması olaylarıdır.

Çığır İlbaş ve Mehmet Ali Köksal (2011) tarafından hazırlanan *Türkiye Bilişim Suçları Raporu, 1990- 2011 Temmuz* isimli raporda 1990 yılından 2011 yılına kadar Türkiye'de işlenen siber suçlar incelenmiştir. Bu raporda Türkiye'nin ilk siber suç haritası çıkartılmış (TBD, 2011: 14) olup hazırlanan rapora göre, Türkiye'de mahkeme kayıtlarında geçen ilk siber suç 1990 yılında işlenmiştir. Türkiye'nin bilişim suçu profiline katkı sağlayan bu çalışmada kullanılan dava dosyalarının kanunları aşağıdaki gibi verilmiştir:

- ✓ Kişisel veriler ile ilgili suçlar (TCK m. 135,136,137,138).
- ✓ Nitelikli Hırsızlık (TCK m.142/2.e).
- ✓ Nitelikli Dolandırıcılık (TCK m.158/1.f).
- ✓ Müstehcenlik (TCK m.226).

[3] 2019, Miniwatts Marketing Group https://www.internetworldstats.com/stats4.htm#europe E.t. 20.11.2021
[4] Günümüzde İDB ve TİB, BTK altında birleştirilmiştir. İDB ve TİB tarafından hazırlanan güncel raporlar BTK'nın resmi sitesinde verilmektedir. tib.gov.tr
[5] https://www.egm.gov.tr/kurumlar/egm.gov.tr/IcSite/kom/YAYINLARIMIZ/T%C3%9CRK%C3%87E/2008%20RAPORU%20T%C3%9CRK%C3%87E.pdf

- ✓ Yetkisiz Erişi (TCK m.243).
- ✓ Sisteme ve veriye müdahale (TCK m.244).
- ✓ Banka ve kredi kartlarının kötüye kullanılması (TCK m.245).
- ✓ Manevi mali haklar, koruyucu programları etkisiz kılma (FSEK m.71,72,73).
- ✓ 5651 Sayıl kanuna muhalefet.

Bu kanunlar ve kanun maddelerince incelenen dava dosyaları ışığında hazırlanan raporda, en çok dosya %57 oranında "banka ve kart" daha sonra %17 oranında bilişim sistemi dosyaları olmuştur. Bu sırayı telif hakları, müstehcenlik, çocuk istismarı, kişisel veriler takip etmiştir. Yıllara göre ayrılan suçlar baz alındığında toplam davalardaki en büyük oranı "banka ve kredi kartı" suçlarının oluşturduğu tespit edilmiştir. Eldeki verilere göre 1990 ve 2003 yılları arasında toplam 389 adet bilişim suçu davası varken bu sayının 2004 yılında 429'a yükseldiği görülmektedir. İlbaş ve Köksal (2011: 170) bu artışın sebebini internet kullanımının artışına bağlamaktadır. 2003 yılından sonra siber suçlarla ilişkili dava dosyalarının arttığı gözlemlenmiştir. Bu artışta TCK'nin 12.10.2004 tarihinde siber suçlara özel ilk yasal düzenlemeyi yapmış olması etkili olmuştur.

Jandarma Genel Komutanlığı'nın 2020 Yılı Faaliyet Raporuna göre son yıllarda siber suçlarda önemli oranda artış olduğu görülmektedir. Rapora göre 2020 yılında 2019 yılına oranla siber suçlarda %229, siber suç şüpheli sayısında ise %304 artış olduğu tespit edilmiştir.

6. SİBER SUÇLAR NEDEN ARTTI?

Geçmişten günümüze insanlık, farklı farklı dönemlerden geçmiştir. Bazı dönemler insanlık tarihinin büyük değişim ve gelişim noktaları olarak kabul edilmiştir. Fukuyama (2018: 47), insanlık tarihini beş döneme ayırmaktadır. Doğada yaşayan ilk insan grupları avcı- toplayıcı toplum olarak bilinmektedir. Avcı ve toplayıcı olan toplum "*Toplum 1.0*" şeklinde nitelendirilmektedir. İnsan topluluklarının yerleşik hayata geçmesi ile birlikte tarıma dayalı bir ulus inşası gerçekleşmeye başlamış ve tarıma dayalı toplumlar "*Toplum 2.0*" olarak nitelendirilmektedir. Sanayi Devrimi ile birlikte toplumlar sanayi toplumuna geçmiş ve teşvik eden bir toplum olarak "*Toplum 3.0*" şeklinde adlandırılmıştır. Daha sonra yaşanan bilgi toplumu "*Toplum 4.0*" şeklinde adlandırılmıştır. Son dönemde ise merkeze insanı koyan bir toplumu hedef edinen ve "*Toplum 4.0*" üzerine kurulan toplum ise "*Toplum 5.0*" olarak kabul edilmektedir. Toplum 5.0'ın asıl amacı ekonomik kalkınma ve sosyal sorunların üstesinden gelerek insanlığın rahat ve aktif bir yaşam sürmesi olmuştur. Yeni bir bakış açısı olan "*Toplum 5.0*" Japonya kaynaklıdır. Japonya insan merkezli bir toplum olarak "Toplum 5.0" biçiminde adlandırdığı toplum için "*Süper Akıllı Toplum (Super Smart Society)*" adını da kullanmaktadır.

Süper akıllı toplum, Endüstri Devrimi ile yakından ilişkili olan bir toplumdur. 18. yüzyılın ortalarında başlayan ve hala devam etmekte olan endüstriyel gelişmeler, dört evrede ele alınmaktadır (Saracel, 2020: 27- 29). Bunlar; ilk olarak toplumların tarım toplumundan sanayi toplumuna geçiş yaptığı, ilk önemli teknolojik alet olarak buhar motorunun icat edildiği, makine ve fabrikalarda büyük değişimlerin yaşandığı *Endüstri 1.0*; elektrik gücü otomatik operasyonların gelişmesi ile birlikte ilk otomobil üzerinde çalışılması, telefon ve telgrafın icadı gibi gelişmelerin olduğu *Endüstri 2.0*; ilk bilgisayarların icadı, seri üretime geçiş ile birlikte *Dijital Devrim* olarak adlandırılan *Endüstri 3.0* ve 2011 yılında *Industrie 4.0* isimli girişimin fikri ile yaygınlaşan, Siber-Fiziksel Sistemlerin (CPS), Nesnelerin İnterneti'nin (IOT), Bulut Bilişiminin (Cloud), akıllı teknolojik ürünlerin ve birçok ileri düzey teknolojik gelişmelerin içinde barındığı ve kullanıldığı, *Endüstri 4.0*'dır. Bu üç önemli devrimden en farklı olanı *Endüstri 4.0* olarak görülmektedir.

Endüstri 4.0, Almanya'da tartışma konusu olmuş ve ilk kez 2011'de gerçekleştirilen Hannovver Fuarı esnasında gündem olmuştur. Dördüncü Sanayi Devrimi olarak görülen devrim, sanal ve fiziksel imalat sistemlerinin bir araya geldiği ve kişiye özel üretimlerin gerçekleştiği bir devrim olarak tasnif edilmektedir. Fiziksel, dijital, biyolojik ve birçok alanın etkileşim içinde olduğu bu devrim diğer devrimlere nispeten çok daha geniş ölçekli ve hızlı bir şekilde gerçekleşmiştir (Schwab, 2018).

Endüstri 4.0 ile yaşanan gelişmeler beraberinde, insansız teknolojiler olarak tanımlanan *Endüstri 5.0*'i getirmiştir. Endüstri 5.0 ise *Toplum 5.0*'ı ortaya çıkartmıştır. İlk kez 2017 yılında Almanya'da gerçekleşen CeBIT fuarında ortaya atılan Toplum 5.0 felsefesi, 2016'da Japonya Bakanlar Kurulu tarafından onaylanmıştır (BTK, Toplum 5.0, t.y.). Bu toplum bilgi toplumunun birikimine dayanmaktadır. Merkeze insanı alan bu toplumda kullanılan; Nesnelerin İnterneti (IoT), Büyük Veri (Big Data), Kablosuz Ağ Sensörü, Bulut bilişimi (Cloud), makinalar arası iletişim (M2M) gibi birçok teknolojik gelişme bir arada bulunmaktadır.

Süper Akıllı İnsan olarak adlandırılan dönemde, yukarıda bahsi geçtiği gibi teknolojik alanda büyük gelişmeler yaşanmıştır. Günümüze kadar olan süreçte sürekli olarak yenilik ve ilerleme içinde olan insanlık, çağa uyum sağlamak ve gelişmelerden faydalanmak amacıyla giderek teknoloji ve bilişimle iç içe olmuştur. Teknolojinin siber

dünyanın kapılarını aralaması, bireyleri de bu dünyanın içine almaya başlaması sadece ekonomik, sosyal, politik alanları etkilemekte ayrıca suç ve suç eylemlerinin de değişimine neden olmaktadır.

Endüstri 2.0 ile birlikte hayatımıza giren bilgisayarlar ve devamında zaman ve mekan kavramını ortadan kaldıran internet, suçun şeklini de değiştirmiştir. Günümüzde diğer suçlardan faklı olarak karşımıza çıkan siber suç, gün geçtikçe artış göstermiştir. Bu artışın sebebi ise oldukça önemli bir soru olarak kaşımıza çıkmaktadır. Öncelikle siber suçların ortaya çıkmasına zemin hazırlayan yukarıda bahsettiğimiz toplumsal dönemler, sanayi devrimi dönemleri sadece siber suçların oluşumuna kapı açmamış giderek artmasında da önemli roller oynamıştır.

Bilişim teknolojileri ile birlikte internete erişim gün geçtikçe kolaylaşmış ve yaygınlaşmıştır. Özellikle *Toplum 5.0* olarak adlandırılan günümüzde mevcut kullanıcıların yeni teknolojik aletlere uyum sağlama çabası ve Covid-19 salgının küresel çapta yarattığı etkiyle birçok kişinin ilk kez internete bağlanması ve sanal dünya ile tanışması gerçekleşmiştir. Bu durum doğal olarak internet kullanımını ve birçok bilişim sistemli araçların kullanımını arttırmıştır. We Are Social ve Hoousuite tarafından yayınlanan *Digital 2021: Global Overview Report*[6] isimli rapora göre, dünyanın %59,5'i internet kullanırken %66,6'sı mobil kullanmaktadır. Dünyanın %92,6 'sı mobil cihazlar ile internete erişmektedir (Kemp, 2021; We Are Social ve Hoousuite, 2021a: 8-46). Dünya üzerinde internet kullanımı yıllık olarak %7,3 oranında artmaktadır. Türkiye'de ise *Digital 2021: Turkey* raporuna göre 2020 ve 2021 arasında internet kullanımı %6 artmıştır. Ocak 2021 de Türkiye'de toplam 65,80 milyon internet kullanıcı bulunmaktadır. Türkiye'nin nüfusunun bu dönemde 84,60 milyon nüfusa sahip olduğu düşünüldüğünde internet kullanıcılarının oranı oldukça yüksek seviyelerde olduğu görülmektedir. Türkiye'de mobil ile internet erişimi ise 2020 ve 2021 arasında %2,7 artış göstermiştir. Esasen mobil bağlantıların aynı kişi tarafından birçok kez farklı cihazlar ile sağlanması düşünüldüğünde mobil bağlantılar tahmini olarak nüfusun %100'ünü aşabilir. Öte yandan Türkiye'de 16 ve 65 yaş arası internet kullanıcıların günlük internet kullanımları ortalama 7 saat 57 dakika olduğu belirlenmiştir (We Are Social ve Hoousuite, 2021b).

Yukarıdaki veriler son dönemde internet kullanımının ne derece arttığını ortaya koyarken bilişim suçlarının artmasını da tahmin edilebilir hale getirmektedir. Özellikle Toplum 5.0'da yaygınlaşan, Nesnelerin İnterneti (IoT), Büyük Veri (Big Data), Kablosuz Ağ Sensörü, Bulut bilişimi (Cloud), gibi teknolojik gelişimlerin kullanılması siber suçların yaygınlaşmasında oldukça etkili olmuştur. Örneğin, tüm izleme cihazları, sensörler, biochipler veya erişim sistemleri, bilgisayarlar ya da akıllı cihazları birbirine bağlayan ya da veri paylaşımını sağlayan Nesnelerin İnterneti (IoT) teknolojisi, uzaktan birçok erişime kapı açmıştır (Oral ve Çakır, 2017: 173). Bu da verilerin gizliliğini ihlal etme niyetinde olanlar için esasen bir fırsattır. Ayrıca birbirine bu sayede bağlı olan cihazların herhangi birinin sadece tek bir sistemine erişim sağlamak diğer cihazlara da erişim sağlamak anlamına gelmektedir. Kullanıcılara büyük bir kolaylık sağlayan bu teknoloji, aynı şekilde bu teknolojiyi kullanan birey ya da şirketlere yönelik siber saldırılar için de büyük bir kolaylık sağlamaktadır.

Holst'a (2021) göre, tüketici sektöründe IOT ile bağlantılı cihaz sayısı 2030 yılında 3 kat daha fazla olacaktır. Bu gelişimeler insanların hayatlarını kolaylaştırdığı gibi siber suçları ya da saldırıları da daha kolay hale getirmekte ve bireyleri ya da şirketleri bu saldırılara açık hale getirmektedir. Siber suçun artışında erişim kolaylığı ve sanal dünyada yakalanmama olasılığının daha az olması suç eğilimli bireyler için çekici bir faktör olmuştur. Sanal dünya içinde fiziki varlığın öneminin olmaması, zaman ve mekan kavramının ortadan kalkmış olması, suç işleyecek birey ya da suçlu birey için riski diğer geleneksel suçlara ilgiyi nispeten oldukça aza indirgemiştir. Bu da bireylerin eski ya da geleneksel suçlar olarak nitelendirilen suçları terk ederek siber suçlara yönelmesinde önemli bir rol oynamaktadır.

IOT tarafından toplanan verilerin ya da birçok özel yahut kişisel verilerin Bulut bilişimi depolanmasını sağlamaktadır. Son yıllarda birçok alanın online platformlara taşınması, veri kullanımında artışa neden olmuştur. Dolayısıyla verilerin artışı Bulut Bilişime ihtiyacı arttırmıştır (BTK, Bulut Bilişim, 2013). Sistem güncellemeleri ve sistem açıklarına bağlı olarak siber suçlara ortam hazırlayan bu teknolojin kullanımı yaygınlaştığı sürece siber suçlarda da artış yaşanabilecektir. Son veriler göz önünde bulundurulduğunda yetkisiz erişim siber suçlar arasında genellikle ilk beşte yer almaktadır. Bu tür teknolojilerin varlığı sistemlere, verilere ve birçok şeye erişime fırsat sağlarken siber riskleri de oldukça arttırmaktadır.

Öte yandan STM Teknolojik Düşünce Merkezi tarafından hazırlanan *Ocak- Mart 2020 Siber Tehdit Durum Raporu*[7]'nda koronavirüs hastalığı (Covid-19) ile birlikte siber saldırılarda artış olduğu belirlenmiştir. Bu bağlamda koronavirüs hastalığı ile oltalama adı verilen siber saldırılarda artış olduğu gözlemlenmektedir. Virüsün yayılması hususunda ortaya çıkan siber tehditleri; uzaktan çalışma, internet dolandırıcılıkları ve casusluk saldırıları şeklinde sıralayan STM 'ye (2020: 31) göre, virüs ile birlikte paralel bilişim kanallarının sıklıkla kullanılması, online satış sitelerine yönelerek dolandırıcılığa maruz kalınması, koronavirüs hastalığı temalı sahte linklerin, ilintilerin yahut uygulamaların ortaya çıkması gibi durumlar değerlendirilerek siber saldırılarda artış olduğu tespit edilmiştir.

[6] https://datareportal.com/reports/digital-2021-turkey E.t. 12.11.2021
[7] https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2021

Avrupa Birliği Polis Teşakilatı'nın (Europol, 2021) *Internet Organised Crime Threat Assessment*[8] raporuna göre, siber suçlar en çok internet alt yapısı iyi olan ve online ödeme sistemlerinin olduğu, AB Üye Devletleri gibi büyük ülkelerde sorun oluşturmaktadır. Bu bağlamda internet alt yapısının iyileştirilmesi ve her türlü ödeme işleminin online sistemler ile gerçekleştirilebilmesi siber suçların artmasına neden olmaktadır. Öyle ki Covid-19 hem iş dünyasını hem toplumsal yaşamı dijital bir dönüşüme zorunlu kılmıştır. 2020 yılının ilk çeyreğinde dünya çapındaki temassız ödemeler %40 oranında artış göstermiştir. Bunun yanı sıra Türkiye'de de online alışverişler salgın öncesi döneme kıyasla yaklaşık %70 oranlarında artış göstermiştir[9] (EY Türkiye, 2021). Bilişim sistemleri ve internet kullanımı, bu süreçte bilinçli veya bilinçsiz birçok insanı kendine çekmiştir. Bu durum da yine siber suçların artmasına zemin hazırlamıştır.

Ayrıca belirtmek gerekir ki teknoloji kullanımındaki bilgi güvenliği ile ilgili kısıtlamalar, bilişim suçları ile mücadelede kuruluş ve kolluklarının kapasite olarak yetersiz kalması, bu alanda profesyonel ve uzmanlaşmış personellerin çok fazla olmaması, suç analizleri ile ilgili olarak yeterli düzeyde akademik çalışmaların üzerinde durulmaması siber suçların artışına neden olduğu *Jandarma Genel Komutanlığının 2018 Raporu'*nda [10]da belirtilmektedir.

7. SİBER SUÇLAR NASIL ÖNLENEBİLİR?

Sürekli olarak değişen ve gelişen dünyamızda yaşanan birçok problemin önüne geçilmeye çalışmaktadır. Günümüzde bu problemlerden en çok karşılaşılan ve ilerleyen süreçte daha fazla yaygınlaşması muhtemel olan siber suçların önüne geçmek de bu süreçte daha fazla önem arz etmeye başlamıştır. Her geçen gün farklı biçimleri ile karşılaşılan siber suçlarla mücadele, sanal dünyada gizlenmenin daha kolay olmasından dolayı diğer suçlara nispeten çok daha zordur.

Siber suçların önlenmesi söz konusu olduğunda karşılaşılan ilk kavram siber güvenliktir ya da dijital güvenlik olmaktadır. Siber güvenlik alanında ülkemizde ve birçok devlette çok çeşitli politikalar, uygulayıcı kurumlar, siber suçlarla mücadele çalışmaları ve sözleşmeler bulunmaktadır. Bu çalışmada siber suçların önlenmesi konusu politikalar, uygulayıcı kurumlar, siber suçlarla mücadele çalışmaları ve sözleşmeler kapsamında değil öneriler niteliğinde ele alınmaktadır.

Siber güvenliğin birçok boyutunun olmasına karşın yedi prensipten bahsedilse de bilgi güvenliğinin ana unsurları *gizlilik, erişebilirlik* ve *bütünlük* şeklinde özetlenebilir. Bahsedilen bu temel prensip kısaca CIA şeklinde tanımlanmaktadır. Bilginin gizliliği (*confidentiality*), sadece bilgisayara erişim izni olan kişiler tarafından kullanılmasıdır. Erişebilirlik (*availability*), bilişim sistemlerinde bulunan bilginin sadece yetkisi olan kişiler tarafından görüntülenebilmesidir. Bilginin bütünlüğü (*intergrity*) var olan bilginin değiştirilmemiş, bir kısmının veya bilginin tamamının silinmemiş olmasıdır. Bunların yasa dışı olması durumunda ise siber suç meydana gelmektedir. Siber suç, sadece bunların aşılması durumunda meydana gelen sistemlerden bilgi çalma, silme, izinsiz erişim gibi eylemlerle sınırlı değildir. Gün geçtikçe gelişen teknolojinin sunmuş olduğu birçok kolaylıkla siber suç da farklı farklı nitelikler kazanmıştır. Günümüzde geniş bir nitelik kazanan siber suça karşı alınan önlemler de yani siber güvenlik sistemleri de gelişme göstermiştir (Yıldız, 2014: 59; Aslay, 2017: 24-28; Başaranoğlu, 2019). Yıllar içerisinde bu durumun büyük bir tehdit olacağı dünya tarafından kabul görmeye başlanmıştır. Daha etkin savunma sistemlerinin kurulması, saldırıların gerçekleştiği anlarda tespit edilebilmesi gibi çeşitli çalışmalar gündeme gelmeye başlamış ve siber güvenlik politikalarının geliştirilmesi önemli hatta zorunlu bir hal almaya başlamıştır. Bu politikalar gün geçtikçe geliştirilmiş olmakla birlikte her geçen gün daha da hızlı geliştirilmeye devam etmek zorunda kalmaktadır.

Siber güvenlik, bilişim sistemlerine kötü amaçlı saldırı risklerini azaltmayı içermektedir. Fakat siber güvenlik her ne kadar gelişmiş olsa da siber suç verilerine bakıldığında yeterli olmadığı görülmektedir. Hatta siber saldırıların riskleri siber güvenlikler ile ilişkili olarak artış gösterdiği için siber güvenliğin son zamanlarda siber suçların problem olması kadar büyük bir sorun haline geldiği de dikkatleri çekmeye başlamıştır. (Amoroso, 2007: 2-3). Buna göre siber saldırılar çeşitlendikçe, siber güvenlik probleminin de büyüyeceği göz önüne alınarak tedbirlerin bilimsel çalışmaların ışığı altında arttırılması gerekecektir.

Güvenlik alt yapılarının güçlendirilmesi adına CIA (gizlilik, bütünlük, erişebilirlik) üçlüsünün önemli bir bileşen olarak ele alınması gerekmektedir. Bu alanların dışında kalarak siber güvenliği sağlamak amacıyla sadece bilişim teknolojilerini devreye sokmak yeterli değildir (Yıldız, 2014: 62). Bu noktada siber suçların nasıl önlenebileceği sorusu önem arz etmektedir.

İlk olarak siber suçları önlemek için siber suçluları tutmak, yaptırım yahut cezalar ile caydırmak mümkün ama düşük bir ihtimaldir. Siber suçları engellemenin yolu suçlulardan değil güvenlikten geçmektedir. Siber suçlar ancak siber güvenlik arttırıldıkça ve gereken önlemler alındıkça azaltılabilir. Çünkü herhangi bir suçu, suç eylemini tamamen

[8] https://www.europol.europa.eu/publications-events/main-reports/iocta-report
[9]https://www.ey.com/tr_tr/ey-turkiye-yayinlar-raporlar/covid-19-sonrasi-bilgi-teknolojilerinin-dijital-dunyada-yeni-rolu E.T. 11.11. 2021
[10] https://www.jandarma.gov.tr/indirilebilir-icerikler E.t. 11.11.2021

ortadan kaldırmak neredeyse imkansızdır. Siber suçları önlemek, siber suçlara meyli azaltmak, yetkililerin alacakları önlemlerle daha kolay gerçekleşecektir. Siber güvenliği arttırmak ve mümkün önlemleri almak kadar kullanıcıların bu tehditlere karşı bilgilendirilmeleri, farkındalıklarının arttırılmaları da önem arz etmektedir.

Siber suçları önlemek için sadece devlet tarafından alınan önlemler ya da yasal cezaların yeterli olmadığı fark edildiğinde birey ve kurumların kendi güvenliklerine önem vermeleri ve kendileri için önlemler almaları gerektiği de fark edilmiş olacaktır. Bu noktada atılması gereken ilk adımlardan birisinin, bireylerin kurumların bilişim sistemlerinde *fire Wall* ismindeki güvenlik duvarı yazılımları kullanmasının gerekliliğidir. Birey ya da kurumların güvenlik açısından kurdukları her yazılımın güncelliğine önem vermeleri gerekmekle birlikte her yazılımın açığı ve eksiğinin bulunduğu da dikkatlerden kaçırılmadan hareket edilmelidir.

Bu noktada en büyük görev uzmanlara düşmektedir. Program ya da bilişim mühendislerinin en az istismar edenler kadar hatta onların çok ötesinde yaygın olarak kullanılan ya da kullanılabilir programların açıkları üzerinde çalışmalar yapmaları, devletin de bu alandaki uzman kadrolarını genişletmesi gerekmektedir. Bilişimde dünyası çok hızlı geliştiği için kesin çözüme ulaşılamasa da "en iyi güvenlik" amaçlanmalıdır (Dülger, 2012: 681-684). Öte yandan test edilen sistemlerin açıkları en aza indirildiği için öngörülen saldırılara karşı daha güvenilir olacaklarından birey ve kurumlar test edilen bilişim sistemlerine yöneltilmelidir. Her birey gerçekleştiremese dahi her şirket ve kurum mutlaka güvenlik uzmanı ile yazılı bir sözleşme çerçevesinde anlaşmalıdır. Test süreçleri ile ilgili olarak da devletin yasal düzenlemeler yapması gerekmektedir. Dülger'e (2012: 685) göre, bu yasal düzenlemeler bilişim suçlarına yönelik cezalarda yapılmak yerine "bilişim sistemleri güvenliği konusunda bir yönetmelik" çıkarılmadır.

Daha önce de bahsedildiği gibi siber suçları önlemek, alınan önlemlerden geçmektedir. Bu noktada dikkat edilmesi ve alınması gereken çok sayıda unsur bulunmaktadır. Bunların her birine değinmek bu çalışma için mümkün olmamakla birlikte birkaç önemli nokta üzerinde durulabilir. Bir önceki bölümde bahsedildiği gibi günümüzde farklı cihazlar üzerinden internet kullanımının hızlı artış göstermiş olması, internet kullanımına olan ihtiyacın da artış göstermiş olduğunu ortaya koymaktadır. Dijital dünyanın getirisi olarak bireyler bulundukları her alanda internete erişmek istemektedirler. Çoğu kez kişisel veri bağlantıları olmayan bireyler halka açık, ücretsiz WiFi bağlantı noktalarını kullanmaktadırlar (Altun, 2016: 96- 102). İnternet erişimi için kamuya açık, ücretsiz WiFi noktalarına bağlanmak siber saldırılar için açık bir kapı olmaktadır. Kişisel verilerin gizliliğini korumak ve ekonomik kaybın önüne geçmek için bu tür güvensiz WiFi noktalarına bağlanmaktan kaçınmak siber güvenlik için son derece önemli bir husustur.

WiFi ile ilgili olarak bir diğer husus ise pos cihazlarıdır. Günümüzde seyyar pos cihazları oldukça popüler kullanım alanlarına sahiptir. Bu cihazların hepsi WiFi ile bağlantılı olup cihazların kullanımı kartlar açısından son derece risklidir. Okutulan her kartın bilgilerinin aktarımı günümüz şartlarında mümkün olup siber saldırılar için bir fırsat yaratmaktadır. Covid-19 nedeni ile kredi kartlarının kullanımının da artması ile banka/kart suçlarının da arttığından yukarıda bahsedilmişti. Bu bağlamda kartların kullanımına ve özellikle kart bilgilerinin cihazlarda kayıtlı olmamasına dikkat edilmesi gerekmektedir. Hiçbir sistemin tam olarak güvenli olmadığı, teknolojinin hayatımızı kolaylaştırdığı kadar riskleri de beraberinde getirdiği hafızalardan uzak tutulmamalıdır.

Öte yandan internette en çok kadınların ve çocukların mağdur olduğu bilinmektedir. Maalesef çocuklar genellikle internette güvenlik kavramını ve nelere dikkat etmesi gerektiğini yeteri kadar bilmemektedirler. Öte yandan günümüzde çocukların mobil cihazlara ve internete ulaşım oranlarının yüksek seviyelerde olduğu, bu durumun onların sosyal hayatlarını ve sağlıklarını son derece olumsuz yönde etkilediği bilinmektedir. Çocukların teknolojiyle iç içe olmalarının sadece çocukları değil ailelerini ve aileleri ile olan ilişkilerini de etkilediği görülmektedir. Çocukların bilişim teknolojilerini bilinçsiz bir şekilde kullanmaları, ebeveynlerin gerekli önlemleri almaması/alamaması çocukları siber suçlar maruz kalmaya açık hale getirmektedir. Bu yüzden bilişim teknolojilerinde çocuklar için hazırlanan güvenli program ve yazılımlar kullanılmalı çocukların kullandıkları alanların ebeveynlerden farklı olması önemli bir önlem olacaktır. Anne babaların kişisel verilerinin çocuklar tarafından bilinçsizce paylaşımı siber suça ortam hazırlayabildiği gibi çocukların ne olduğunu bilmedikleri görsel yerlere tıklamaları sonucu bilişim sistemlerine yönelik saldırılara kapı açabilmektedirler (Altun, 2016). Devlet tarafından çocuklar için sağlanan güvenli internet siteleri ve yazılımların olması, bunların çocukların kullandığı her türlü bilişim sisteminde kullanılması bu açıdan son derece önem arz etmektedir.

Bilişim teknolojileri vasıtasıyla işlenen suçlar, yapısına bağlı olarak tüm toplumları etkilemektedir. Bu suç tipinin sınır ve zaman tanımaksızın bilişim teknolojilerinin ve ağ sistemlerinin var olduğu global bir dünyada siber suçlarla etkili bir biçimde mücadele edebilmek için devletlerin birlikte hareket etmelerinin en az devletlerin kendi içlerindeki mücadele kadar önemli olduğunun gözlerden uzak tutulmaması gerekmektedir.

Siber suçluluğun getirdiği çeşitlilikten dolayı bazen ülkeler ortak hareket edememektedirler. Devletlerin siber suçlar konusunda ortak hareket edememelerinin nedenlerini Turhan (2016: 74) şu şekilde özetlemektedir:

- ✓ Yapısal düzenlemeler konusunda uzlaşım sağlanamaması,
- ✓ Siber suçların hukuki tasniflerinde bütünlük sağlanamaması,

- ✓ Siber suçlar alanındaki çalışma yürüten kurum ve kuruluşların tecrübe eksikliği,
- ✓ Ulusal düzeydeki farklılıklara bağlı olarak siber suçların takibatında uyum sağlanamaması,
- ✓ Siber suçların birçoğunun uluslararası yapı arz etmesi,
- ✓ Suçluların iadesi ve karşılıklı yardım tekliflerindeki eksikliklere bağlı olarak uluslararası iş birliği hususunda mekanizmalarının uyumlu bir şekilde çalıştırılamaması.

Siber suçlar bu derece yaygınsa siber suçların nasıl önlenebileceği ile ilgili önerilerin de o derece fazla olması gerekir. Alınabilecek birçok önlem ve dikkat edilecek birçok husus bulunmakla birlikte öncelikle devletin ve kolluk kuvvetlerinin aldığı önlemlerin yanı sıra toplumsal bir iş birliğinin rolü gözden uzak tutulmamalıdır. Sadece cezai yaptırımların yeterli olamayacağı açıkça görülmektedir. Siber suçlar ve siber güvenlik konusunda toplum bilinçlendirilmeli, bu hususta özel eğitimler verilmeli, dijitalleşen dünya göz önüne alınarak, temel müfredatta siber güvenliğe de yer verilmelidir. Öte yandan siber suçlar ile ilgili olarak kriminoloji, sosyoloji, penoloji ve bilişim alanlarında daha fazla akademik çalışma ve analiz yapılmasının önemi fark edilmeli ve bu yöndeki çalışmalar desteklenmelidir.

8. SONUÇ

Suç ve sapma insanlık tarihiyle birlikte başlayarak günümüze kadar uzanan önemli bir toplumsal olgu haline gelmiştir. Kompleks bir yapıya sahip olan her iki kavram da pek çok durumda örtüşse dahi birbirlerinden farklı kavramlardır. Ortak bir tanım ve açıklamada bulunmanın zor olduğu bu kavramlar toplumsal koşul ve şartlara göre farklı şekillerde karşımıza çıkmaktadır. Sapmanın bir alt kategorisi olarak görülen suç kavramı daha çok yasalar ile belirlenmiş ve hukuksal tanımlamalara konu olmuştur. Bunun yanı sıra toplumsal hayatı büyük ölçüde etkileyen ve insan ürünü olma hasebi ile sosyolojik çalışmaların ilgi odağı olmuştur.

Toplumsallaşmanın sonucu olarak bireylerin izlediği toplumsal norm ve kurallar, toplumsal hayatın düzeni ve devamlılığı için gerekli olarak görülmektedir. İnsanların doğası gereği toplumsal alanda var olan bu norm ve kurallardan sapma normal olarak görülmekte fakat bazı durumlarda bireyler bilinçli yahut bilinçsiz sergiledikleri eylem ve tutumlar karşısında etiketlenmelere maruz kalmaktadırlar. Bunun en büyük sebebi sapma kavramının kompleks ve dinamik bir yapıya sahip olmasıdır. Daha çok toplumların yaşam biçimine, kültürüne, ahlak algısına ve dini görüşlerine bağlı olarak şekillenen sapma kavramı evrensel bir tanıma tabi tutulamamaktadır. Sonuç olarak evrensel olarak suç kabul edilen tutum ve davranışlar da birer sapma olarak nitelendirilmektedir. Fakat bu niteliğin her suç için geçerli olup olmadığı tartışmalı bir konudur.

Birçok farklı türü olan suç olgusunun değişen dünya ile birlikte çok farklı şekli ortaya çıkmıştır. Bir suç çeşidi olarak karşımıza çıkan kavramlardan biri de siber suç olmuştur. Sapma ve suç kavramları gibi ortak bir tanımı olmayan siber suçlar, geleneksel suçlardan farklılıklar ortaya koymaktadırlar. Siber suçlardaki farklılıklar kavramların tanımlarından ziyade eylemlerde açığa çıkmış olup farklılıklar kültür, inanç, ahlak algısı gibi unsurlara bağlı olarak değil insanlığın teknolojik gelişimine bağlı olarak ortaya çıkmıştır.

Teknolojik alanda yaşanan gelişmelere bağlı olarak gündelik hayat çok büyük farklılıklar ortaya koymaya başlamıştır. Özellikle Endüstri 1.0 ile birlikte başlayan büyük gelişmeler suçların ilk evrildiği dönem olmuştur. Daha sonra teknolojik alanda yaşanan büyük gelişmeler her süreçte suçu farklı bir boyuta taşımıştır. Bilişim teknolojileri alanında gerçekleşen hızlı gelişmeler, yalnızca insan hayatını kolaylaştırarak fertlerin hayat kalitesini arttırmakla kalmamakta öte yandan aygıtların kötüye kullanımını da beraberinde getirmektedir. Özellikle Endüstri 3.0 ile birlikte klasik olarak işlenen suçlar sanal dünyaya geçmeye başlamıştır. Bu suçların gerçek olmadığı anlamını taşımamaktadır. Suçlar tamamen gerçektir ve bireylere, kurumlara ya da toplumlara fiziksel, ekonomik, siyasal, sosyal her türlü alanda gerçek bir zarar verebilmektedirler. Sadece suçun işlenme şekli sanal bir dünya olan siber uzayda gerçekleşmektedir. Siber uzayın, yaşanan teknolojik gelişmelere bağlı olarak genişlemesi ve insanların gelişmelere uyum sağlama süreçleri ve adapte olmaları siber suçların oranlarını attırmaktadır.

Bilişim teknolojilerinin süreklilik arz etmesi ve doğası gereği durağan olmamasına bağlı olarak hukuki düzenlemeler, sürekli değişen ve yenilikler ile dolu olan bu sahada bir süre sonra yetersiz kalmaya başlamıştır. Hükümetler artık reel dünyada yer almayan suçlara aşina olmak adına mücadele etmektedirler. Fakat dünyaya yayılan siber uzay alanında suçlular durmaksızın yeni eylemler hedeflemektedirler. Toplumların sanal dünyaya gün geçtikçe artan bağımlılığı bireyleri, sistem hatalarına ve tehditlere karşı daha savunmasız hale getirmektedir. Dünyayı saran bu durumla beraber, siber suçun ortaya çıkışı sosyologlar, penologlar, kriminologlar, iletişimciler ve daha birçok ilişkili disiplinler için de ilgi alanı olmaya başlamış ve bünyesinde zor soruları bandırır hale gelmiştir. Bunlardan en önemlisi siber suçların neden arttığıdır ve bu artışın önüne nasıl geçilebileceği sorusudur. Çalışmada siber suçların bilişim teknolojilerinin ve bu teknolojilerin kullanımının yaygınlaşmasına bağlı olarak arttığı, gösterilen veriler ışığında tespit edilmiştir.

Siber suçların, Toplum 3.0 düzeyinde olan ve özellikle Toplum 5.0 düzeyine ulaşmış toplumlarda ortadan kaldırılması mümkün görünmemektedir. Fakat siber suçların en aza indirgenmesi olanaklıdır. Siber suçlar ile

mücadele hususunda günümüze kadar gerçekleştirilmiş olan politikaların, uygulayıcı kurumların, siber suçlarla mücadele çalışmalarının ve sözleşmelerinin siber suçların artışına engel olmadığı veriler ile ortaya konulmuştur. Bu bağlamda siber suçlar ile mücadelenin toplumsal iş birliği ile yürütülmesinin daha faydalı olacağı sonucuna ulaşılmıştır. Siber suçlulara ya da suçlu olma potansiyeli taşıyanlara yönelik girişimlerin siber suç oranlarını düşürmediği, suçluları caydırmadığı açıkça görülmektedir. Bu sebeple siber suçları önlemeye yönelik çalışmalarda yaptırım ve caydırma politikaları yerine, bilişim teknolojilerinin geliştirilmesi ve kontrol altında tutulması önemsenmelidir. Bu noktada her bilinçsiz bilişim teknolojisi kullanımının ya da kullanıcısının siber suç için bir fırsat olduğu unutulmamalıdır.

KAYNAKÇA

Açıkgöz, E. İ. (2020). *Bilişim Sistemi Aracılığıyla Haksız Yarar Sağlama Suçu (TCK m. 244/4).* Ankara: Adalet yayınevi.

Agre, P. E. (2002). Introduction: The Limits Of Cyberspace. *Science as Culture*, 11(2), 149-153 . doi:https://doi.org/10.1080/09505430220137216

Akbulut, B. (2017). Bilişim Alanında Suçlar. İstanbul: Adalet yayınevi.

Akdağ, P. (2009). Siber Suçlar ve Türkiye'nin Ulusal Politikası. *Yüksek Lisans Tezi*. Ankara.

Alpman, S. P., & Yarcı, S. (2018). Göç Ve Kimlik: Suç Teorilerinde Göç Olgusu. *Turkish Studies(13/18)*,143-152. doi:http://dx.doi.org/10.7827/TurkishStudies.14098

Altun, İ. (2016). *Ortam Sanal Suç Gerçek*. İstanbul: İskenderiye Kitap.

Amoroso, E. G. (2007). *Cyber Security*. AT&T Inc, Silicon Press.

Arıkan, Ç. (1986). Psiko-sosyal Yönleriyle Sapma. *Hacettepe Üniversitesi Sosyal Hizmetler Yüksekokulu Dergisi (4(2-3))*, 123-140.

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *International Journal Of Multidisciplinary Studies And Innovative Technologies*, 1(1), 24-28.

Bahar, H. İ. (2009). *Sosyoloji*. Ankara: Uşak Yayınları.

Bal, H. (2003). *Hukuk- Hukuk Sosyolojisi*. Isparta: Süleyman Demirel Üniversitesi.

Başaranoğlu, E. (2016). *Bilgi Güvenliği Unsurları (CIA ve Diğerleri).* 11 20, 2018 tarihinde https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/ adresinden alındı

Becker, S. H. (1963). *Outsiders; Studies in The Sociology of Deviance*. London: Free Press of Glencoe.

BTK. (2013). *Bulut Bilişim.* Bilgi Teknolojileri ve İletişim Kurumu. Ankara: Bilgi Teknolojileri ve İletişim Kurumu. 11 13, 2021 tarihinde https://www.btk.gov.tr/uploads/pages/slug/bulut-bilisim.pdf adresinden alındı

BTK. (2019). *2019 yılı Faaliyet raporu.* Bilgi Teknolojileri ve İletişim Kurumu. 11, 2021 tarihinde https://internet.btk.gov.tr/bilisim-hukuku-ve-bilisim-sucu adresinden alındı

BTK. (t.y.). *Toplum 5.0*. Bilgi Teknolojileri ve İletişim Kurumu. Sektörel Araştırma ve Strateji Geliştirme Dairesi Yayını. 11 10, 2021 tarihinde https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/toplum-5-0-arastirma-raporu.pdf adresinden alındı

Burstein, A. (2003). A Survey of Cybercrime in the United State. *Annual Review of Law and Technology*, 18(1), s. 313-338.

CSI/FBI. (2001). *CSI/FBI Computer Crime and Security Survey Computer Security Issues & Trends.* VII. Computer Security Institute.

Dönmezer, S. (1994). Kriminoloji. İstanbul: Beta Basım Yayın.

Durkheim, E. (2004). *Sosyolojik Yöntemin Kuralları*. (C. Saraçoğlu, Çev.). İstanbul: Bordo Siyah Yayınları.: Bordo Siyah Yayınları.

Dülger, M. V. (2012). *Bilişim Suçları ve İnternet İletişim Hukuku.* Ankara: Seçkin Hukuk.

Dülger, M. V. (2020). *Bilişim suçları ve İnternet İletişim Hukuku*. Ankara: Seçkin Hukuk.

Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA).* Europol. Luxembourg: Publications Office of the European Union, https://www.europol.europa.eu/publications-events/main-reports/iocta-report adresinden alındı

EY Turkey. (2020). COVID-19 Sonrası Bilgi Teknolojilerinin Dijital Dünyada Yeni Rolü. *Ey Turkey*. 11 11, 2021 tarihinde https://www.ey.com/tr_tr/ey-turkiye-yayinlar-raporlar/covid-19-sonrasi-bilgi-teknolojilerinin-dijital-dunyada-yeni-rolu adresinden alındı.

Fisher, M. B. ve Strauss, A. L. (1997). Etkileşimcilik. (Kurtuluş Dinçer, Çev.). Bottomore, T. Nısbet R. (Mete Tunçay, Aydın Uğur, Yay. Haz.). içinde, *Sosyolojik Çözümlemenin Tarihi* (s. 459-497). Ankara: Ayraç Yayın evi.

Fraser, B. T. (1996). Computer Crime Research Resources. *School of Library and Information Studies, School of Library and Information Studies*. Florida State University. http://mailer.fsu.edu/~btf1553/ccrr/search1.htm adresinden alındı

Fukuyama, M. (2018, Temmuz/Ağustos). Society 5.0: Aiming for a New Human. *Centered Society*. 11 10, 2021 tarihinde https://www.jef.or.jp/journal/ adresinden alındı

Furnell, S. M. (2001). Categorising cybercrime and cybercriminals: The problem and potential approaches. *Journal of Information Warfare*, 1(2), 35-44. 11 13, 2021 tarihinde https://www.jstor.org/stable/10.2307/26486092 adresinden alındı

Gibson, W. (1984). *Neuromancer*. Londra: HarperCollins.

Giddens, A. (2008). Sapkınlık ve Suç. C. Güzel (Çev. ed.) içinde, *Sosyoloji* (H. Özel, Çev.). İstanbul: Kırmızı Yayınları.

Goffman, E. (1963). *Stigma; Notes on the Management of Spoiled İdentity*. Englewood Cliffs, N.J.: Prentice-Hall.

Gökrem, B. (2000, Ekim). İnternet Aracılığıyla İşlenen Sermaye Piyasası Suçlarının Gözetimi ve Denetimi. *Kurul Yeterlik Etütleri*, 10-45. Anakara: Sermaye Piyasası Kurulu Denetleme Dairesi. https://www.spk.gov.tr/SiteApps/Yayin/YeterlikEtutleri adresinden alındı

Gray, L. (2014). *Cybercrime*. New York, NY: Gareth Stevens.

Güçlü, İ., & Akbaş, H. (2019). *Suç sosyolojisi: kavram, teori, uygulama*. Ankara: Gazi Kitabevi.

Hobbes, T. (2007). *Leviathan: Bir Din ve Dünya Devletinin İçeriği, Biçimi ve Kudreti*. (S. Lim, Çev.) İstanbul: Yapı kredi Yayınları.

Holst, A. (2021, Ekim 19). Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030, by vertical. 11 13, 2021 tarihinde *Statista*: https://www.statista.com/statistics/1194682/iot-connected-devices-vertically/#statisticContainer adresinden alındı

İçli, T. G. (1991, Aralık). Sosyal Problemlerin Bir Göstergesi Olarak Bireysel Sapmalar. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi,* 8(1-2), 13-18.

İDB. (2008). *"İhbar İstatistikleri" 23 Kasım 2007 – 23 Kasım 2008 Faaliyet Raporu*. Bilgi Teknolojileri ve İletişim Kurumu. Bilgi Teknolojileri ve İletişim Kurumu-Telekomünikasyon İletişim Başkanlığı. 11 12, 2015 tarihinde tib.gov.tr adresinden alındı

İlbaş, Ç., & Köksal, M. A. (2011). Türkiye Bilişim Suçları Raporu: 1990-2011 arasında. T. Memiş, A. Koltuksuz, & M. Akkan (Ed.) içinde, *2.Uluslararası Bilişim Hukuku Kurultayı 17-19 Kasım Bildiriler Kitabı*. İzmir: Uluslararası Bilişim Hukuku Kurultayı.

JKG. (2018). *Jandarma Genel Komutanlığı, 2018 Yılı Faaliyet Raporu*. Jandarma Genel Komutanlığı. Jandarma Genel Komutanlığı. 11 11, 2021 tarihinde https://www.jandarma.gov.tr/indirilebilir-icerikler adresinden alındı

JKG. (2020). *Jandarma Genel Komutanlığı 2020 Yılı Faaliyet Raporu*. Jandarma Genel Komutanlığı. 11 11, 2021 tarihinde https://www.Jandarma.Gov.Tr/Jandarma-Genel-Komutanligi-2020-Yili-Faaliyet-Raporu adresinden alındı

Kalay, M. (2009). TCK'da Bilişim Suçları. M. Balcı (Ed.) içinde, Genç Hukukçular Hukuk Okumaları Birikimler 3 (s. 133-141). İstanbul: Step Matbaacılık.

Karagülmez, A. (2005). *Bilişim Suçları ve Soruşturma-Kavuşturma Evreleri*. Ankara: Seçkin Yayıncılık.

Kemp, S. (2021, Ocak 27). Digital 2021: Global Overvıew Report. *Digital In 2021: Business As Unusual*. We Are Social ve Hootsuite. 11 12, 2021 tarihinde https://hootsuite.widen.net/s/zcdrtxwczn/digital2021_globalreport_en adresinden alındı

KOM. (2009). *Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı 2008 Raporu.* Ankara: EGM-KOMDB Yayınları.

KOM. (2013). *Kaçakçılık ve Organize Suçlarla Mücadele 2012 Faaliyet Raporu*. Ankara: EGM/KOM. 12 12, 2021 tarihinde https://www.egm.gov.tr/kom/raporlarimiz adresinden alındı

KOM. (2015). *Kaçakçılık ve Organize Suçlarla Mücadele 2014 Faaliyet Raporu*. Emniyet Genel Müdürlüğü. Ankara: KOM; EGM. 12 11, 2021 tarihinde https://www.egm.gov.tr/kom/raporlarimiz adresinden alındı

Kurt, L. (2005). *İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması.* Ankara: Seçkin yayıncılık.

Küçükvardar, M. (2018). Suç Olgusunun Değişen Yüzü: Siber Suçlar. *Isophos: Uluslararası Bilişim, Teknoloji ve Felsefe Dergisi (1),* 1-17. https://www.isophos.org/is-cont/uploads/pdf/01/suc-olgusunun-degisen-yuzu-siber-suclar.pdf adresinden alındı

Macionis, J. J. (2013). Sapma. J. J. Macionis, & V. Akan (Çev. Ed.) içinde, *Sosyoloji* (H. Çavuşoğlu, Çev.). Ankara: Nobel Akademik Yayıncılık.

Marschall, G. (1999). *Sosyoloji Sözlüğü*. (O. Akınhay, & D. Kömürcü, Çev.) Ankara: Bilim ve Sanatı Yayınları.

Merton, K. R. (1938). *Social Structure and Anomie (Vol. 3).* American Sociological Review.

Moore, W. E. (1997). İşlevselcilik. T. N. Bottomore, & M. U. Tunçay. içinde, *Sosyolojik Çözümlemenin Tarihi* (Ş. Tekeli, Çev., s. 327-369). Anakara: Araç Yayınevi.

Mungo, P., & Clough, B. (1992). *Approaching Zero: The Extraordinary Underworld Of Hackers, Phreakers, Virus Writers, And Keyboard Criminals*. New York: Random House.

Ngafeeson, M. (2010). Cybercrime Classification: A Motivational Model. *The Southwest Decision Sciences Institute Conference*. Texas. 11 12, 2021 tarihinde www.swdsi.org/swdsi2010/sw2010_preceedings/papers/pa168.pdf adresinden alındı

Oral, O., & Çakır, M. (2017). Nesnelerin İnterneti Kavramı ve Örnek Bir Prototipin Oluşturulması. *Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitü Dergisi (Özel Sayı 1),* 172-177. 11 12, 2021 tarihinde http://dergi parkı.gov.tr/makuateşli adresinden alındı

Parlak, Ö. (2016). *Suçun Evrimi: Siber Suçlar*. 11 03, 2018 https://tr.linkedin.com/pulse/su%C3%A7un-evrimi-siber-su%C3%A7lar-%C3%B6zhan-parlak adresinden alındı

Ross, J. İ. (2010). *Cybercrime.* New York: Chelsea House.

Saracel, n. a. (2020). Toplum 5.0: Süper Akıllı Toplum. *Social Sciences Research Journal*, 9(2), 26-34. 11 13, 2021 tarihinde http://socialsciencesresearchjournal.com/ adresinden alındı

Schell, B. H., & Martin, C. (2014). *Cybercrime: A Reference Handbook*. California: abc Clio.

Schmalleger, F. (2014). Criminology. Boston: Pearson.

Schwab, K. (2018, Kasım). *Dördüncü Sanayi Devrimi*. (T. U. Bulsun, Çev.) Optimist Yayın.

Selçuk, S. (2014). Suç, Suçun Öz Nitelikleri ve Tanımı. A. Nuhoğlu (Ed.) içinde, *Prof. Dr. Feridun Yenisey'e Armağan* (Cilt 1, s. 85-106). Beta Yayınevi.

STM. (2020). *Siber Tehdit Durum Raporu Ocak- Mart 2020*. Savunma Teknolojileri ve Mühendislik Ticaret A.Ş. Mühendislik Teknoloji Danışmanlık. 13 12, 2021 tarihinde https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-ocak-mart-2020 adresinden alındı.

Sutherland, E. H., & Cressey, D. R. (1974). *Criminology*. Philadelphia and London: J. B. Lippincott Company.

Tanyeri, G., & Civelioğlu, A. S. (2007, Bahar). Hukuk Gündemi, Bilişim Suçları ve Çocuk Pornografisi. *Ankara Barosu Dergisi* (7), 98.

TBD. (2011). *Aylık Bilişim Kültürü Dergisi*, 39(137).

Turhan, O. (2016). *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar).* Planlama Uzmanlığı Tezi, Ankara.

We are Social & Hoousuite. (2021a). *Digital 2021: Global Overview Report*. We Are Social; Hoousuite. 12 11, 2021 tarihinde https://hootsuite.widen.net/s/zcdrtxwczn/digital2021_globalreport_en adresinden alındı

We are Social & Hoousuite. (2021b). *Digital 2021: Turkey Report*. We Are Social; Hoousuite. 12 11, 2021 tarihinde https://datareportal.com/reports/digital-2021-turkey adresinden alındı

Wall, D. S. (2017). *Cybercrime: The Transformation of Crime in the İnformation Age*. Cambridge; Malden, MA: Polity.

Yazıcı, D. (2012, Ekim Cuma). Türkiye'nin İlk Bilgisayar Korsanı Tamer Şahin Anlattı. *Aydınlık Kitap Dergi*, 1(35).

Yıldız, M. (2014). *Siber Suçlar ve Kurum Güvenliği*. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı.