

# YAPISAL FONKSİYONALİST BAĞLAMDA SİBER SUÇLARIN SOSYOLOJİK ANALİZİ<sup>1</sup>

## SOCIOLOGICAL ANALYSIS OF CYBERCRIMES IN A STRUCTURAL FUNCTIONALIST CONTEXT

**Doç.Dr. Melda Medine SUNAY**

Bursa Teknik Üniversitesi, İnsan ve Toplum Bilimleri Fakültesi, [sosyologmelda@gmail.com](mailto:sosyologmelda@gmail.com),  
Bursa/Türkiye, 0000-0003-3210-5942

**Ebru BİREL**

Bursa Teknik Üniversitesi, Lisansüstü Eğitim Enstitüsü, [Ebru.birel21@outlook.com](mailto:Ebru.birel21@outlook.com),  
Bursa/Türkiye, 0000-0002-5987-9297

### ÖZET

Tarih boyunca toplumlar farklı toplumsal yaşam evrelerinden geçerek yaşamlarını sürdürmektedirler. Sabanın icat edilmesiyle beraber avcı ve toplayıcı toplumlardan tarım toplumlarına, buhar makinesinin icat edilmesiyle sanayi toplumlarına ve son olarak gelişen bilgi ve internet kullanımına bağlı olarak Daniel Bell'in post-endüstri toplumları olarak isimlendirdiği evreye geçilmiştir. Toplumlar değişen toplumsal yaşamlarına bağlı olarak ortaya çıkan suç türlerine yönelik farklı önlemler almıştır. Özellikle günümüzde ortaya çıkan siber suç türleri toplumların (uyrukların), dijital ortamda korunmasına yönelik çalışmaları gerekli kılmıştır. Zira günümüzde teknoloji ve internetin gelişimine bağlı olarak ortaya çıkan siber suçlar güvenlik konusunda önemli bir tehdit olarak görülmektedir. Bu bağlamda çalışmanın temel amacı yapısal fonksiyonalistlerin suça karşı yaklaşımlarını inceleyerek siber suçları sosyolojik bağlamda irdelemektir. Siber suçların seçilmesinin temel nedeni günümüzde ortaya çıkan bir tehdit olarak önlenmesi konusunda güvenlik önlemlerin eksik olmasının yanı sıra sosyal bilimler literatüründe toplumsal etkileri konusunda yeterli çalışmalara yer verilmemiş olmasıdır. Yapılan çalışmada yöntem olarak nitel araştırma yöntemleri ile ulaşılan veriler kullanılarak siber suçların yapısı ve toplumsal etkileri hakkında bilgi verilmektedir. Sonuç olarak siber suçların; devletlerarası işbirliğini zorunlu kılmasıyla bağımlılığı ve dayanışmayı artıran, teknolojik alanda mücadeleye yönelik geliştirilen yazılım ve araçlarla ilerlemeyi tetikleyen ve son olarak hukuksal anlamda yeni kanunların eklenmesiyle değişimi ve toplumsal sınırları belirleyen toplumsal bir fenomen olduğu sonucuna ulaşılmıştır.

**Anahtar Kelimeler:** Suç, Siber Suç, Yapısal Fonksiyonalizm.

### ABSTRACT

Throughout history, societies have lived through different social life stages. With the invention of the plow, it has passed from hunter and gatherer societies to agricultural societies, to industrial societies with the invention of the steam engine, and finally to the stage that Daniel Bell called post-industrial societies depending on the developing information and internet use. Societies have taken different measures against the types of crimes that arise depending on their changing social life. Especially the types of cybercrime emerging today have necessitated studies for the protection of societies (nationalities) in the digital environment. Cybercrime, which has emerged due to the development of technology and the internet, is seen as an important threat to security today. In this context, the main purpose of the study is to examine cybercrime in a sociological context by examining the approaches of structural functionalists to crime. The main reason for choosing cybercrime is the lack of security measures to prevent it as an emerging threat, as well as the lack of sufficient studies on its social effects in the social sciences literature. In the study, information about the structure and social effects

---

<sup>1</sup> Bu çalışma 13-17 Aralık 2022 tarihinde düzenlenen Socrates 6. Uluslararası Eğitim, İşletme, İktisat ve Sosyal Bilimler Kongresinde sunulan tebliğin geliştirilmiş / genişletilmiş halidir.

of cybercrime is given by using the data obtained by qualitative research methods. As a result, cyber crimes; It has been concluded that it is a social phenomenon that increases dependency and solidarity by necessitating interstate cooperation, triggers progress with software and tools developed for the struggle in the technological field, and finally determines change and social boundaries with the addition of new laws in the legal sense.

**Keywords:** Crime, Cybercrime, Structural Functionalism.

## 1.GİRİŞ

Tarihsel süreçte tüm toplumlarda suç ve ceza yöntemleri çeşitli şekillerde ortaya çıkmakla beraber toplumların değer, inanç, gelenek, görenek gibi toplumsal yaşam biçimlerinden etkilenmektedir. Bu bakımdan suç teşkil eden davranışlar ve ceza yöntemleri toplumsal ve dönemsel açıdan farklılık göstermektedir. Örnek vermek gerekirse suç, avcı ve toplayıcı toplumlarda yazının kullanılmaması dolayısıyla töreye (yazısız kurallara) dayanması şeklinde tanımlanırken, bu toplumların sürekli hareket halinde olmaları ceza yönteminin günümüz modern cezaevi uygulamalarından ziyade sürgün, öldürme veya kırbaç şeklinde yaptırımların uygulanmasıyla sonuçlanmaktadır. Sanayi öncesi toplumlarda suçun meşru dayanak noktası olarak inançlar, gelenek ve görenekler etkili olmakta iken günümüz modern toplumlarında bu unsurların etkisi olmakla beraber rasyonel temellere dayanan evrensel hukuk kurallarının hâkim olduğu görülmektedir. Bu bakımdan ele alacak olursak suç ve ceza tanımlamalarının geçmiş, şimdi ve gelecek arasında farklı ölçütler içerisinde yer aldığı/alacağı görülmektedir.

Günümüzde en genel anlamda suça ilişkin tüm tanımlamalar ve yaklaşımların ortak temelinde herhangi bir toplumda toplumsal düzen ve sürekliliğin devamı amacıyla oluşturulan yazılı kanunların kasten ihlal edilmesiyle ortaya çıkan davranışlar yargısı bulunmaktadır. Suçun meşruluğunun dayanmış olduğu dayanak noktasının farklılaşmasına bağlı olarak değişen suç türleri ve suça yönelik tanımlamalar olmakla beraber Marshall ve Sutherland tanımlamaları suçu anlamaya yönelik geniş bir perspektif sunmaktadır.

*“Marshall suçu, “kişisel alanı aşır, 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; Sutherland’a göre suç, ceza kanununca yasaklanan her türlü eylemdir ve ahlaksızlık ya da kınama düzeyi ne derece olursa olsun, bir fiil kanunlarca yasaklanmadıysa suç sayılmamaktadır (Mashall,1999: 702, Sutherland, 1997: 4, akt. Karataşoğlu, 2022: 37)”.*

Dinamik bir yapıya sahip suç olgusunu incelemek, açıklamak ve önlemek amacıyla çeşitli teorik yaklaşımlar ortaya çıkmaktadır. Bu anlamda 1885’lerden bu yana bir bilim olarak gelişmeye başlayan Kriminoloji suç olgusunun incelenmesi ve önlemesine yönelik bir bilim olarak gelişmiştir (Bal, 2016: 29). Suçun ortaya çıkış noktasında farklı ayrıntılara dikkat etmek kriminolojide farklı kuramların ortaya çıkmasıyla sonuçlanmıştır. Kriminolojide ilk 1985’lerde ortaya çıkan klasik biyolojik kuramların (Lomroso, Garofalo) yanı sıra 1920/30’larda Freud’un çalışmalarıyla beraber modern kuramların ortaya çıktığı görülmektedir. Bu kuramlar arasında Neoklasik okul; davranışın ortaya çıkmasına neden olan etmenlerin ortadan kaldırılmasıyla suçlu davranışın ortadan kalkacağını savunan görüş, biyolojik kuram; kişilerin doğuştan fiziksel ve ruhsal bozukluklara bağlı olarak suçlu doğduğunu ileri süren bakış açısı ve Freud’un psikoanalitik yaklaşımı yer almaktadır (Özcan, 2022: 91). Bu kuramların ortak amacı suçlu davranışı anlamaya çalışarak faydacı bir bakış açısıyla bu davranışı önlemeye çalışmaktır.

## 2. SİBER SUÇ

Günümüzde teknoloji ve internet altyapısında meydana gelen ilerlemelerle beraber gündelik yaşamda kullanılan internet, bilgisayar, internete bağlanabilen telefonlar, gündelik işleri kolaylaştıran mobil bankacılıkla alışveriş ve faturaların ödenmesi, kamu hizmetlerin internet aracılığıyla verilmesi gibi uygulamalar insan yaşamını kolaylaştırıcı imkânlar yaratmaktadır. İnsan yaşamını kolaylaştırıcı etkiye sahip olan bu uygulamalarla beraber insanlar artık toplumsal yaşamlarının hemen hemen her anını siber ortamlara aktarmaktadır. Günümüzde gündelik yaşamdaki işlerin yapıldığı alan olan siber sistemler kişisel bilgilerin yanı sıra devletlere ait verilerin yer aldığı ortamlardır. Dijital ortamlarda yer alan bu bilgiler güvenlik konusunda devletlerin farklı tedbirler almalarını gerekli kılmaktadır.

Özellikle Soğuk Savaş döneminden sonra daha geniş ölçekte güvenlik problemlerinin ortaya çıkmasıyla beraber (siber güvenlik, çevre güvenliği vs.) güvenliğe yönelik tanımlamalar değişmekte olup güvenlik; devlet uyruklarını sadece askeri anlamda koruması değil aynı zamanda dijital ortamlarda yer alan kişisel bilgilerin korunması gibi sorumlulukları da üstlenmektedir (Doğrul ve Erğurum, 2021: 178). Sanayi Devrimi'nin birikimsel bir ürünü olarak gelişen bu ilerlemeler günümüzde toplumsal hayatın yaşamını kolaylaştıran ve kişilere özgürlük vaat eden bileşenler olarak görülmektedir. Lakin Manuel Castells'in "Ağ Toplumu", Ulrich Beck'in "Risk Toplumu" olarak isimlendirdiği günümüz toplumlarında birtakım tehdit, belirsizlik ve güvensizlik ortamları oluşturulduğuna dair görüşler bu gelişmeler karşısında temkinli olmamız gerektiğini öğütler niteliktedir. Aynı şekilde Bauman'ın da (2013:119-120) Modernite, Kapitalizm, Sosyalizm, Küresel Çağda Sosyal Eşitsizlik kitabında aktardığı şekilde internet topluluklarının (daha sonra ağlar diyecektir) uzun dönemli bağlılık, sadakat ya da katı disiplin gerektirmemeleri gibi çekici yönleriyle bireyin özgürleşmesi olarak görülmüş ve coşkuyla karşılanmış; fakat ağları çekici kılan yine bir başka bedel olarak güvensizlik problemini beraberinde getirmektedir. 1990'lı yıllarda bilgisayar mühendisleri tarafından kullanılan siber güvenlik, "ağa bağlı olan sistemlerin erişilebilir, çalışılabilir ve sürekliliği ile muhafazasını sağlamaktır" (T.C. Kültür ve Turizm Bakanlığı, 2017: 45). Bu bakımdan günümüzde gerek ulusal gerekse uluslararası düzeyde geniş siber güvenlik tedbirleri alınması zorunlu bir hal almaktadır.

Her toplumda değişen yaşam koşulları ve olanaklarına bağlı olarak yeni kavramlar kullanılmaya başlamıştır. Bu doğrultuda siber suç kavramı dijitalleşen endüstri toplumları sonrasında ağlar aracılığıyla yasadışı gerçekleştirilen suç davranışlarını ifade etmek amacıyla kullanılmaktadır. En geniş anlamıyla siber suç; bilişim sistemleri kullanılarak herhangi bir bilişim sisteminin güvenliğini, verilerini veya kullanıcılarını hedef alan hukuka aykırı yapılan eylemlerin tümünü ifade etmektedir (Suveren, 2019: 164-165). Marcum ve Higgins (2019; 460) 'Cybercrime' isimli yazısında melez (karışım) suçlar olarak tanımladıkları siber suçların daha önce fiziksel dünyada var olan suç davranışlarının çevrimiçi bir şekilde işlenmeye başlaması olarak isimlendirmiştir. Bu bakımdan yeni suç türlerin ortaya çıkması söz konusu olabileceği gibi eski suç davranışların esnek teknolojilerin kullanılmasıyla yeniden biçimlenmesi ve sanal ortamda daha kolay bir şekilde gerçekleştirilmesi söz konusu olmaktadır. Bu suçlar kişinin özel yaşam gizliliğini ihlal etme (gizli dinleme, gözetleme, hesap veya bilgisayarları hacklemek), taciz, yalan haber yayma ve propaganda yapmak gibi manevi boyutları olabileceği gibi kişilerin malvarlığına yönelik kredi kartlarından para çekme, dolandırıcılık faaliyetleri şeklinde görülebilmektedir. Siber saldırılar kişilerin yani sıra kurumsal şirketler, bankalar, kamu daireleri karşısında da tehdit oluşturabilmektedir. Günümüzde bu tehditler karşısında önlemlerin alınmasına yönelik çalışmalar yapılmış olsa dahi siber saldırıların tam olarak önlenmesi henüz mümkün görülmemektedir. Zira siber suçlar söz konusu olduğu zaman mekânsal açıdan bir yere bağlı olmaması ve suçu işleyen kişinin kim olduğunun saptanamaması konusunda kriminolojik güçlükler ortaya çıkmaktadır (Wall, 2001: akt. Suveren, 2019: 168).

## 2.1. Siber Suç Çeşitleri ve İstatistikleri

Uluslararası Telekomünikasyon Birliği (ITU) siber suçları 4 ana başlık içinde sınıflandırmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2022: 24):

- Bilgisayarlarda yer alan veri ve sistemlerin kullanılabilirliği, gizliliği ve bütünlüğüne yönelik işlenen suçlar (yasadışı veri hırsızlığı, değiştirilmesi ve müdahale edilmesi),
- Bilgisayar ile ilgili suçlar (kimlik hırsızlığı, dolandırıcılık, virüs yayma, online kumar),
- Telif hakkı ile ilgili suçlar,
- İçerikle ilgili suçlar (yalan haber, ırkçılık, müstehcen yayın satmak, nefret ve şiddet söylemleri).

Furnell ise siber suçları 2 ayrı kategori içerisinde değerlendirme yapmaktadır (Furnell, 2001, s. 35-37; akt. Kolukırık ve Gün, 2020: 328).

*Bilgisayar odaklı suçlar:* Bilgisayar ve internet sistemleri olmadan önce var olan fakat daha sonra bilgisayar/internet sistemlerinin geliştirilmesiyle bu olanaklardan faydalanarak daha rahat bir şekilde işlenen suçlar. Dolandırıcılık, online kumar, hırsızlık vs.

*Bilgisayar Destekli Suçlar:* Bilgisayarın ortaya çıkmasıyla beraber ortaya çıkan yeni suçlardır. Yazılım destekli olan bu suçlar virüs yayma, bilgisayar korsancılığı vb. şekilde görülmektedir.

5237 Türk Ceza Kanunu'nun Toplumla Karşı Suçlar başlıklı 3. Kısmında 10. Bölüm "Bilişim alanında suçlar" konusuna ayrılan maddeler şu şekildedir (Url, 1);

Madde 243 – Bilişim sistemine girme

Madde 244 – Sistemi engelleme, bozma, verileri yok etme veya değiştirme

Madde 245 – Banka veya kredi kartlarının kötüye kullanılması

Madde 245/A – Yasak cihaz veya programlar

Madde 246 – Tüzel kişiler hakkında güvenlik tedbiri uygulanması

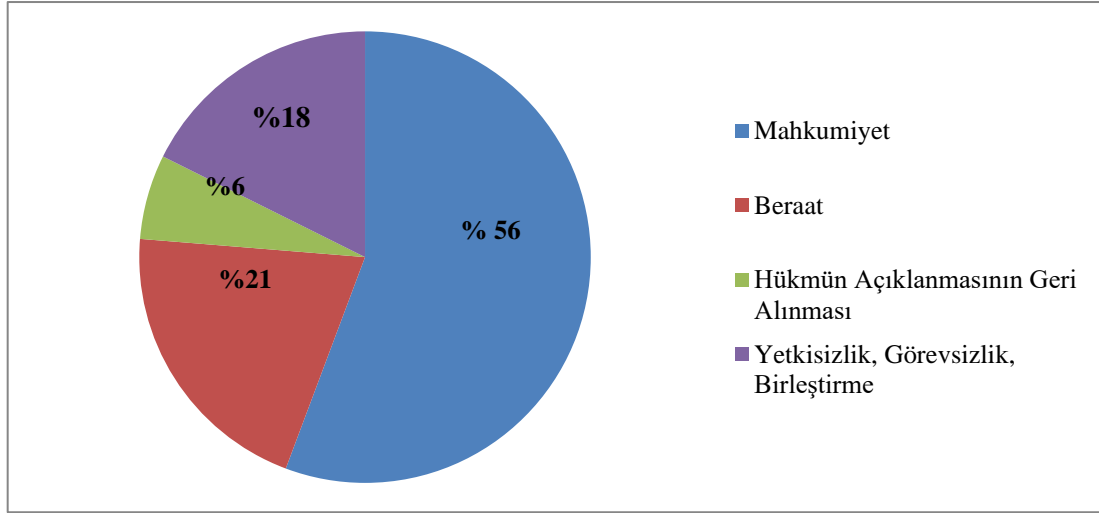
Adli Sicil ve İstatistik Genel Müdürlüğü tarafından hizmete özel olarak yayınlanan raporda bilişim suçları yıllara göre dağılımı aşağıdaki gibidir;

	TCK. Madde no.	2017 ve öncesi	%	2018	%	2019	%	2020	%	2021	%	Toplam	%
Bilişim Alanındaki Suçlar	243-246	7168	23,1	2242	7,2	7251	23,4	6093	19,7	8239	26,6	30993	1,0

**Kaynak: (Url, 1)**

Tabloda da görüleceği üzere Türkiye’de siber suç sayılarında artış-azalış şeklinde düzensiz dalgalanmalar görülmekle beraber son yıllarda özellikle 2021 yılında ciddi bir artış olduğu görülmektedir. Tablonun tamamının yer almış olduğu kaynakta siber suçlar 28 çeşitli suç kategorisi içerisinde 14. Sırada yer almaktadır. Günümüzde yaygın bir şekilde kullanılan iletişim teknolojileri alanında meydana gelen ilerlemeler beraberinde siber suçların artması tehdidini de getirecektir. Bilişim suçlarıyla ilgili 2021 yılında açılan 19.947 kamu davasından 71.131 kovuşturmayaya yer olmadığına dair karar verilirken önceki yıla- 2020 yılında 17.790 davadan 38.659 kovuşturmayaya yer yoktur- kovuşturmayaya yer olmadığına dair verilen karar sayısında bir artış olduğu ve yapılan suç duyurularından yalnızca %16,2’i kamu davasına dönüştüğü görülmektedir.

2021 yılında siber suçlara yönelik açılan toplam 47.352 davanın verilen kararların türüne göre sayısı



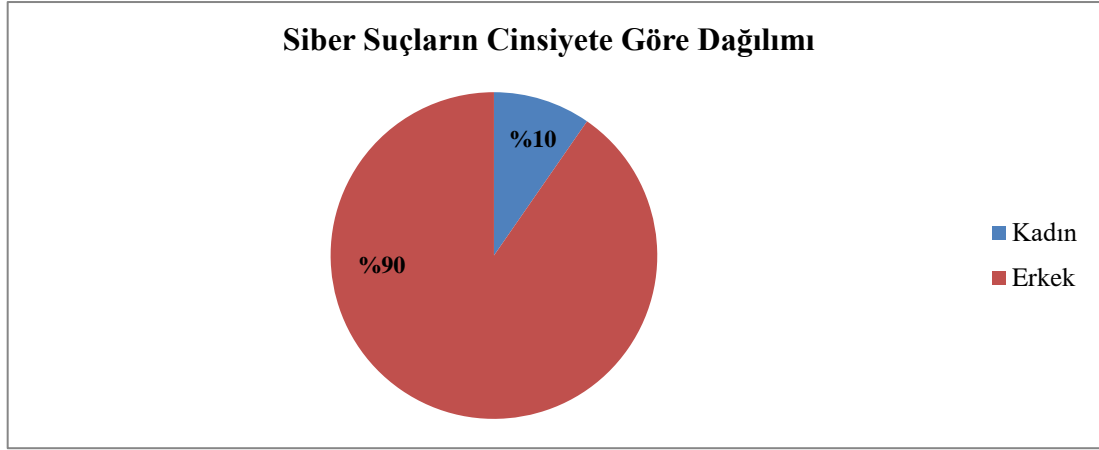
Mahkûmiyet	Beraat	Hükümün Açıklanmasının Geri Alınması	Yetkisizlik, Görevsizlik, Birleştirme	Diğer
24 336	8 990	2 650	7 708	3 668

Tabloda görüldüğü üzere 2021 yılında siber suçlara yönelik toplam 47,352 davanın 24,336'sı mahkûmiyetle sonuçlanmıştır. Mahkûmiyet kararları, sanıklar hakkında verilen hürriyeti bağlayıcı ceza, adli para cezası, erteleme, güvenlik tedbirleri ve diğer mahkûmiyet kararlarını içermektedir. Bir sanık hakkında bir suçtan dolayı aynı mahkûmiyet kararı içerisinde hürriyeti bağlayıcı ceza, para cezası ve güvenlik tedbirine hükmedilmesi halinde UYAP yazılımı nedeniyle mahkûmiyet karar sayısı üç olarak sayılmaktadır. 3,3668 dava ise davanın düşmesi, ceza verilmesine yer olmadığı, hüküm verilmesine yer olmadığı, davanın reddi, özel yasalar gereğince erteleme, TCK madde 32 gereğince verilen kararlar ile sonuçlanmıştır.

2021 yılında sanıkların işledikleri bilişim suçlarına yönelik yaş, cinsiyet ve uyruğa yönelik tablosu şu şekildedir;

	12-15	15-18	18 ve üzeri	Yabancı uyruklu
Erkek	611	977	19815	452
Kadın	28	99	2160	78
<b>Toplam</b>	<b>639</b>	<b>1076</b>	<b>21975</b>	<b>530</b>

(Kaynak: Url 1 )



Genel olarak yıllara göre erkeklerin kadınlardan daha fazla siber suçlar konusunda suça karıştığı görülse de, suç türü bakımından diğer suç türlerine göre kadın suçluluğunun arttığı görülmektedir. Ayrıca dikkat çeken bir diğer unsur ise siber suça karışan kişilerin 18 yaş ve üzeri olmasına rağmen yaş alt sınırın 12'ye kadar düşmesidir. Yine diğer suç türlerine göre siber suça karışan nüfusun yaş bakımından diğer yaşlara göre daha genç olduğu bir suç türü olduğu görülmektedir. Günümüzde küçük yaşta telefon, bilgisayar ve internet erişimi imkânlarına sahip olan kişilerin siber suçların yaş sınırının düşmesi konusundaki temel etken olarak görülebilmektedir. Ayrıca çocuklar günümüzde sosyal medya ve internet (çevrimiçi oyun gibi) aktif bir şekilde kullanan çocuklar siber suçlular tarafından seçilen kurbanlar olma riski arasında da yer almaktadır.

1953 yılından itibaren yaygın bir şekilde üretilen bilgisayarlar Türkiye'ye ilk 1960 yılında gelirken internet ise 1993 yılında Ortadoğu Teknik Üniversitesi Laboratuvarlarında kullanılmaya başlamıştır. Yakın geçmişte kullanılmaya başlanana internet ve bilgisayar sistemlerine bağlı olarak Türkiye'de siber suçlarla ilgili suç ve ceza kapsamında davaların açılmasına yol açmaktadır.

Türkiye Bilişim Suçları Araştırmasına (Url, 2) göre 1990-2011 yılları arasında Türkiye'de siber suçlar kapsamında açılan dava dosya sayısı tablosu aşağıdaki gibidir;

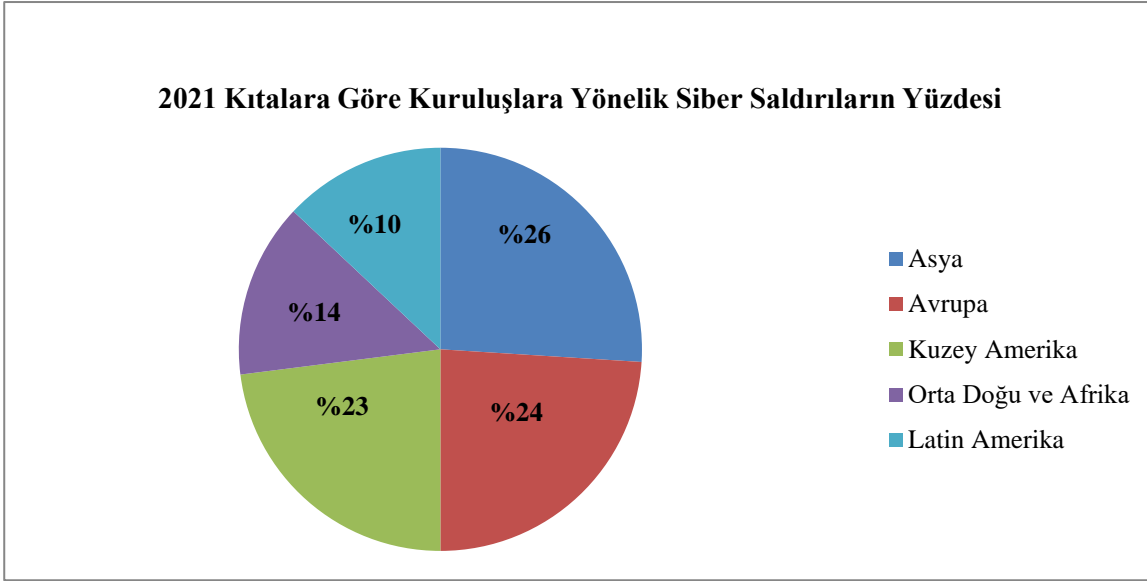
SIRA	SUÇ TANIMI	DOSYA SAYISI
1	Bilişim sistemleri banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık	24254
2	Başkasına ait banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlama	14166
3	Manevi haklara tecavüz	6029
4	Bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama	4258
5	Bilişim sistemlerinin kullanılması suretiyle hırsızlık	3517
6	Şiddet kullanarak hayvanlarla ölmüş insan bedeni ile ilgili müstehcen yayın üretmek ve satmak	2538
7	Sahte banka veya kredi kartı kullanmak suretiyle yarar sağlama	2044

8	Bilişim sistemindeki verileri bozma yok etme erişilmez kılma, sisteme veri yerleştirme vb.	1898
9	Bilişim sistemine hukuka aykırı olarak girme ve orada kalma	1706
10	Müstehcen yayınlara alışveriş merkezleri dışında satmaya arz etmek, satmak veya kiraya vermek	1578
11	Alenen müstehcen yayın satmak veya kiralamak	1110
12	Kişisel verileri hukuka aykırı olarak ele geçirmek veya yaymak	1093
13	Kanuna aykırı çoğaltılan nüshayı ticari amaçla elde bulundurmak	1075
14	Bilişim sisteminin işleyişini engelleme veya bozma	1074
15	Mali hakların ihlali suçları	1049
16	Çocukların kullanıldığı müstehcen yayınları ülkeye sokmak, çoğaltmak, satmak, nakletmek, ihraç etmek vs.	879
17	Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üretme, satma, vb.	764
18	Müstehcen yayınların yayınlanmasına aracılık etmek	686
19	Çocuğun görebileceği yerlerde müstehcenlik	521
20	Müstehcen yayınların üretiminde çocukları kullanmak	494

**Kaynak: (Url, 2)**

Tablodan da anlaşılacağı üzere siber suçlar genelde haksız para kazanma amaçlı işlenen suçlardır. Ki tabloda da görüldüğü üzere ilk iki sırada banka ve kredi kartlarına yönelik işlenen suçlar yer almaktadır. Yine aynı şekilde toplam dava dosya sayısı da siber suç aracılığıyla mala yönelik, dolandırıcılık ve hırsızlık gibi suçları kapsamaktadır. Toplumsal anlamda büyük bir çöküşün işareti anlamına gelen çocuğa yönelik şiddet, taciz, istismar vakalarının siber suçlar aracılığıyla da işlendiği görülmektedir. Zira 521 adet dosya çocuğun görebileceği yerlerde müstehcenlik, 494 adet dosya ise müstehcen yayınların üretiminde çocukları kullanmaya yönelik açılmış dava dosyalarıdır.

2021 yılında kıtalar bazında gerçekleştirilen siber saldırılara ilişkin veriler aşağıdaki grafikte verilmiştir.



**Kaynak:** (Url, 3)

Türkiye’de olduğu gibi dünyada da siber suçlar ciddi bir tehdit olarak görülmekle birlikte siber saldırılardan korunmak amacıyla çok sayıda yatırım yapılmaktadır. 2021 yılında kıtalar bazında gerçekleştirilen siber saldırılara en fazla Asya kıtasının maruz kaldığı görülmektedir. Verilere bakarak, kıta nüfusu ve kıtanın sosyo ekonomik koşulları dolayısıyla bilişim imkânlarından yararlanma durumunun siber saldırı yüzdesini etkilediğini söylemek mümkündür.

## 2.2 Siber Suçlara Yönelik Mücadeleler

Küreselleşmenin arttığı günümüz toplumlarında teknolojik gelişmelerle beraber uzak sınırlar arasındaki mesafe ortadan kalkmaktadır. Bu durum dünyanın herhangi bir yerinden başka bir yerine iletişim ve ulaşımı kolaylaştırdığı gibi herhangi bir yerden gelebilecek tehlikelere açık hale gelmeyi de beraberinde getirmektedir. Bu tehlikelerden en önemlisi şüphesiz siber suçlar olarak görülmektedir. Mekândan bağımsız bir şekilde gerçekleştirilen siber suçların önlenmesi beraberinde güçlükleri de getirmektedir. Kullanılan yazılım sistemleriyle devlet bilgilerinin, sırlarının, güvenlik tedbirlerinin, iletişim kanallarının dinlenmesi ve daha birçok bilginin ele geçirilmesi tehditiyle karşı karşıya kalan devletler bu anlamda küresel düzeyde güvenlik tedbirleri almaya çalışmaktadırlar. Yakın zamanda Euronews haber sitesinde yayınlanan bir haberde Meksika devleti tarafından yabancı bir grubun devletin suç rakamları, silahlı kuvvetler hakkındaki gizli bilgiler, iletişim kayıtları ve ABD’nin Meksika Büyükelçisi Ken Salazar’ın izlenmesi de dâhil olmak üzere Meksika Savunma Bakanlığından altı terabayt veriyi hacklediğini bildirdi (Url, 4). Bu tür siber saldırılar ülkelerin siber güvenlik önlemlerini gözden geçirmeleri ve uluslararası çalışmalara katkı sağlamalarına ilişkin beklentileri getirmektedir. Sonuç itibariyle günümüzde siber saldırıları engellemeye yönelik uluslararası önlemlerin alınmasına yönelik kurum ve kuruluşlar -Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA), Siber Tehditlere Karşı Uluslararası Çok Taraflı İşbirliği (IMPACT), Uluslararası Telekomünikasyon Birliği (ITU), Avrupa Siber Güvenlik Kurumu (ECSSO), G-8 Topluluğu- kurulmuştur.

Türkiye’de siber suçlara yönelik alınan siber tedbirler hukuki boyut ve dijital suçlarla ilgili yapılan düzenlemeler, polisiye yöntemler ve teknik yöntemler olmak üzere 3 ana başlık altında toplanabilmektedir. Kısaca bunlar (Bilgi Teknolojileri ve İletişim Kurumu, 2022: 62-88);

- 26.09.2004 tarihinde 5237 numaralı kanunla siber suçlar farklı bir başlık altında toplanarak ayrıntılı bir şekilde hukuki düzenlemeler yapılmıştır.



- Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde kurulan Bilişim Suçları ve Sistemleri Şube Müdürlüğü 2010 yılında ikiye bölünmüştür. Bilişim Suçları Şube Müdürlüğü tek başına ayrı bir müdürlük olarak devam etmektedir.
- Adli bilişim ve siber güvenlik süreçleri olarak ikiye ayrılan teknik yöntemler suçun işlenmiş olduğu siber uzay ortamda teknik yöntemlerle (geriye dönük kayıt ve veri toplama, silinen kaybolan verileri geri getirme, veri analizi vb. süreçler) suçu aydınlatmaya yönelik delilleri toplamaktır.

### 2.3. Teknolojik Gelişmeler (Sanayi Gelişimi) ve Siber Suçlar

Tarihsel bağlamda toplumlar çeşitli aşamalardan geçerek varlığını sürdürmektedir. Bu aşamalar daha ilkel yaşamın hâkim olduğu; avcı ve toplayıcı toplumlar, bahçıvan ve tarım toplumlarının yanı sıra teknolojik gelişmelere bağlı olarak gelişen endüstri toplumları ve internet ve otomasyon işlemlerinin kullanılmaya başlamasıyla gelişen endüstri sonrası toplumlar şeklinde ilerlemektedir. Avcı ve toplayıcı toplumlardan, endüstri/endüstri sonrası toplumlara gelinceye kadar suç ve ceza yöntemleri çeşitli biçimlerde var olmaktadır.

Suçun olmadığı bir toplumun varlığını hayal etmek imkânsızdır. Yalnız neyin suç olarak görülebileceği? Hangi suç türlerinin ortaya çıkabileceği? Bu suçların ne şekilde cezalandırılacağı? Toplumların değer, inanç, gelenek, görenek, yaşayış biçimleri, teknolojik gelişmeler gibi unsurlara bağlı olarak belirlenmektedir. Bu bakımdan suç ve ceza türleri toplumlara göre farklılık gösterebileceği gibi aynı toplumlarda dönemsel açıdan farklılıklar gösterebilmektedir. Bu bakımdan günümüzde var olan suç çeşitlerinin geçmiş toplumlarda var olmadığı görülebilmektedir. Bunun en açık örneği siber suçlardır. Gelişen teknolojik gelişmeler ve internetin kullanılmasıyla beraber birbirlerine bağlanan ağlar aracılığıyla, suçlu-mağdur yüz yüze, yakın temas veya mekân paylaşımı olmaksızın gerçekleşen siber suçlar günümüzün en temel sorunlarından biri olarak görülmektedir. Bu bağlamda toplumların geçirmiş oldukları değişimleri, sanayi devrimini ve sanayi sonrası yaşanan teknolojik gelişmeleri açıklamak siber suçların ortaya çıkışını ve yapısını anlamak açısından yararlı olacaktır.

Alvin Toffler (2008: 16-17) Üçüncü Dalga adlı eserinde toplumların ileri doğru bir sıçrama hareketinde olduğunu söyleyerek bu gelişim evrelerini; *Birinci Dalga; tarımsal devrim, İkinci Dalga; endüstri devrimi* ve son olarak içinde yaşadığımız çağ olarak görülen *Üçüncü Dalga; bilgi artışı ve teknoloji çağı* olarak adlandırmaktadır. Bunun yanı sıra günümüzde sanayi devrimin ortaya çıkmasıyla başlayan aşamalar endüstri 1.0, endüstri 2.0, endüstri 3.0 ve son olarak günümüz toplumlarını ifade eden endüstri 4.0 olarak dönemsel ayrımlar yapılmaktadır. Sanayi devrimi ilk olarak İngiltere’de 1760 yılında James Watt’ın buhar makinesini icat etmesiyle başlamış ve bu dönem endüstri 1.0 olarak ifade edilmektedir. Bu dönemde yaşanan teknolojik ve toplumsal gelişmeler; buhar gücünün kullanılmasıyla beraber makineleşmenin artması ve artan fabrika sayılarıyla kentsel yapıların artması şeklinde görülmektedir.

Bir diğer adı Elektrik Çağı olan Endüstri 2.0 dönemi ise enerji kaynağı olarak elektriğin kullanılmasıyla telefon, telgraf (ucuz gazete kağıdıyla), radyo gibi yenilikler iletişim teknolojisinin gelişimini sağlamıştır (Siemens, 2016: 6; akt. Çavdar, 2019: 11). Bu dönemde (1957) Sovyetler Birliği tarafından uzaya gönderilen Sputnik uydusu sonrasında dünyanın farklı yerlerine yerleştirilen savaş sistemlerini bir bilgisayar ağı ile yönetme düşüncesi 1970’lerde ABD mühendisleri tarafından geliştirilmesiyle günümüz bilgisayar ağlarının temelleri atılmıştır (Altunok ve Vural, 2011: 75).

Dijital Devrim olarak da isimlendirilen Endüstri 3.0 aşamasında (1970-1990) günümüzde kullanılan yazılımların üretiminin başlaması, internet kullanımı, otomasyon sistemlerinin kullanımı, bilgi işlem teknikleri, dijital haberleşme gibi yeniliklerin yanı sıra siber-fiziksel sistemler ve nesnelerin internetine geçmeye başlanması gibi önemli gelişmeler dördüncü sanayi devriminin sinyalleri olarak görülmektedir (Koca, 2020: 4539-4541). *“İlk olarak 1960’lı yıllarda askeri*

*teknolojiler geliştirme amacıyla kurulan internet 1970'li yıllarda akademisyenler ve üniversiteler tarafından kullanılması ile sivilleşme sürecine girmesi (Gönenç, 2014: 148; akt. Birel, 2022; 21)" sivil hayatta internetin kullanılmaya başlamasının ilk adımlarını oluşturmaktadır. "1990'larda İsviçre CERN araştırma merkezinde geliştirilen küresel ağ adlı iletişim kuralları, e-posta gibi uygulamalar ve Ethernet gibi ucuz donanımsal çözümler ile bilgisayar ağları yaygınlık kazanmıştır" (Altunok ve Vural, 2011: 75). 1960 yılında kablo/radyoya bağlı telefonların yerine Echo 1 isimli uyduya bağlı bir şekilde ABD'nin doğu ve batı yakası arasında haberleşme yapılmıştır. Bunu izleyen süreçte 1985 yılında Discovery'nin yörünge koyduğu uydulardan biriyle aynı anda 20.000 konuşma yapabilme imkânı sağlanmış ve günümüzde uydular aracılığıyla iletişim sağlanan mobil telefon sistemlerin oluşmasına zemin hazırlamıştır (Url, 5).*

Günümüz bilgi toplumlarını ifade eden Endüstri 4.0 kavramı ilk olarak 2011 yılında Almanya'nın Hannover kentindeki bir fuarda kullanılmış ve temel bileşenleri olarak; mobil internetin yaygın bir şekilde kullanımı, gelişmiş bilgisayarlar, yapay zeka, nesnelerin interneti, gelişmiş yazılım kullanımları, siber-fiziksel sistemler, robotların üretimi gibi gelişmeler görülmektedir (Batal ve Tuğlu, 2018: 218). Sanayi alanında meydana gelen bu değişimler şüphesiz üretimin artışı ve daha fazla kar elde etme güdüsüyle gerçekleştirilmektedir. Fakat sadece üretim alanıyla sınırlanmayan bu gelişmeler toplumsal yaşamımızın her alanında etkili olmaktadır.

Bilgisayar ve internet sistemlerinin gelişmesi, ucuzlaşması ve yaygınlaşmasıyla beraber sanal bir dünyayı temsil eden siber ortamlarda kişisel bilgi ve sistemlerle ilgili bilgileri elde etmeye yönelik saldırılar yapan hacker (bilgisayar korsanları) ortaya çıkmıştır. Mağdur-suçlu arasındaki mekânsal bağımlılığı ortadan kaldıran bu suç türü suçun işlenilebilirliği açısından kolaylık sağlamaktadır. Fakat bilgisayar ve yazılımlar hakkında bilgi sahibi olma gerekliliği siber saldırılarda bulunan kişilerin belirli bir eğitim seviyesinde olma zorunluluğunu getirmektedir. Öncelikli olarak bilgisayar kullanımı aracılığıyla yapılan siber saldırılara ek olarak herkesin internete kolayca erişebilen mobil telefonlar, telefon dolandırıcılığı, mobil bankacılığa erişimle kredi kartı izinsiz ve kötüye kullanımı, kişi verilerine ulaşma ve izinsiz dinleme, müstehcen yayın yapma, yalan haber yayma gibi birçok suç eylemi gerçekleştirilmesi geniş alana yayılmıştır. Bu bakımdan günümüzde bilginin üretilmesi, depolanması ve yayılması ve birey özerkliğinin sağlanması açısından önemli adımlar olarak görülen bilişim teknolojisindeki bu gelişmelerle oluşan dijital dünya içerisinde yeni güvenlik tehditleri oluşmaktadır.

## **2.4. Suçun Tarihsel Gelişimi /Siber Suça Dönüşmesi**

Toplumsal anlamda gerçekleştirilen her suç türü içindeki yaşamış olduğu ortamın olanakları doğrultusunda gerçekleştirilmektedir. Suç tarihsel süreçte değişen toplumsal koşullara bağlı olarak bir gelişim seyri izlemektedir. Var olan suçların organize edilmesine bağlı olarak işlenen suçların yanı sıra kullanılan aletlere (teknoloji) bağlı olarak yeni suç türleri ortaya çıkabilmektedir. Günümüzün temel sorunlarından biri olan siber suçların incelenmesi için geçmişten günümüze gelişim seyri içinde olan suç davranışlarını ve bu davranışların siber suçlara dönüşme aşamalarını incelemek faydalı olacaktır.

H. Oppenheimer, Steinmetz'in ilkel ırkların yapmış oldukları suç davranışlarının sıralamasında birtakım değişiklikler yaparak şu şekilde sıralamaktadır (Oppenheimer, 2016: 274-275);

1. Vatana ihanet (düşman kabileye askeri ve ordu sırlarını açıklayarak yardım etme gibi),
2. Cadılık (doğüstü güçleri kullanarak devlete ve halka zarar verme),
3. Kutsala saygısızlık ve diğer dini suçlar,
4. Encest veya diğer cinsel suçlar,
5. Zehirlenme ve bağlı suçlar,
6. Av kurallarının ihlali (amaç, köyün gıda kaynaklarını korumak),

İlkel toplumlarda ortaya çıkan suç türleri buldukları kabileyle sınırlı olması açısından dar kapsamlı ve fiziksel ortamda yüz yüze iletişim sonucu gerçekleştirilmesi sayesinde suçlu kişinin

kolay tespit edilip yakalanabildiği türlerde olmaktadır. Bu dönemde suç ve ceza temelde dini inançlara göre şekillenmekteydi. Aydınlanma ve Sanayi Devrimiyle beraber din ve hukuk alanında ayrıştırmalar yaşanmakta olup, töre yerine yazılı hukuk kurallarının laik ve akılcı bir çerçevede toplandığı, yeni suç türlerinin ortaya çıktığı bir döneme adım atılmaktadır. Özellikle 2. Dünya Savaşı'ndan sonra hayatımıza giren siber suçlar günümüzün temel sorunu olarak görülmektedir. Günümüzde ilk 1970'lerde ortaya çıkan siber suçların ortaya çıktığı ortamların (telefon, bilgisayar vs.) çok daha eski dönemlere dayandığı görülmektedir. Lakin endüstrinin ilk aşamalarında bulunan teknolojik aletlerin kullanımı sınırlı ve devlet denetiminde genel bir merkez tarafından yönetildiğinden dolayı siber saldırılara maruz kalma ihtimali daha düşüktü. Bu durumu Alex Blau (2020: 16-17) *Şimdi Hepimiz İçindeyiz* adlı yazısında şu şekilde anlatmaktadır;

*Eskiden sanayi kuruluşlarında mekanik pompa, kompresör, valf, röle ve tahrik düzenekleri kullanılırdı. Durum kontrolü; beceri sahibi güvenilir mühendislerin analog ölçümleri aletleriyle elde ettiği bilgileri sabit telefonla genel merkeze ilemesiyle sağlanırdı. Bir sabotajcının tedarik zincirini sekteye uğratmasının tek yolu tesise gidip kapı veya bekçiden oluşan fiziksel güvenlik ayağını aşmasıydı. Bugün ABD İç Güvenlik Bakanlığı'nın kritik kabul ettiği 16 altyapı sektöründen 12'sinde operasyonlar kısmen ya da tamamen dijital kontrol ve güvenlik sistemine dayalı olarak yürütülüyor. Dijital teknolojiler harika yeni beceri ve etkinlikler kazandırdı ama aynı zamanda siber saldırı riskine son derece açıktırlar.*

Günümüzde yaygın olarak gerçekleştirilen siber suçlar dönemselsel açıdan farklı amaçlarla ve şekillerde ortaya çıkmaktadır. 1970'lerde yaygın bir şekilde ortaya çıkan telefon hatlarına sızma suçunu ele alacak olursak ilkin temel amaç ücretsiz telefon konuşması yapmaktır. Dönemin ünlü siber suçlularından John Drape, ücretsiz telefon konuşması yapmayı sağlayan geliştirmiş olduğu sistemle ve minibüsüyle Amerika'yı gezerek bilişim sistemlerine müdahale olan ilk suçu gerçekleştirmiştir (Url, 6). Tamamen farklı amaçlarla ortaya çıkan bu suçlar günümüzde artık şarj aletleriyle telefonlara zararlı kodların yüklenmesiyle hackerler tarafından verilerin çalınması, gizlice konuşmaların dinlenmesi boyutuna kadar ulaşmış, ancak Apple firması iOS 7'nin beta sürümünde bu sorunu ortadan kaldırmaya yönelik düzenleme yaptığını duyurmuştur (Altun, 2016: 41). Toplum güvenliğini tehdit edecek boyutlara varan siber suçlara yönelik yapılan mücadeleler gerçekleştirilmektedir. Fakat gelişen bilimsel araştırmalar yeni siber suçların oluşumuna zemin hazırlayabilecek ölçüde paralel ilerlemektedir.

1960/70'li yıllarda kullanılmaya başlanan hacker unvanı bilgisayar teknolojisinde yekin, hızlı ve yazılım alanında üretim yapma kabiliyetine sahip olan uzman kişiler için kullanılırken günümüzde bilgisayar sistemine izinsiz girerek zarar veren kişiler için kullanılan kötü bir üne sahiptir (T.C. Kültür ve Turizm Bakanlığı, 2017: 38-39). Günümüzde siber suçlardan biri olan *hacking* ilk olarak 1981'de *Texas A&M Üniversitesi* öğrencisi *Joe Dellinger'in Apple II* bilgisayarları için kendisini geometrik olarak kopyalayabilen ve bu yolla da bilgisayar sistemlerine zarar verebileceğini keşfetmesiyle ortaya çıkmıştır (Kurt, 55; akt. Ermeydan, 2018: 10). 1982'de ABD'de lise öğrencisi Richard "Rich" Skrenta'nın bilgisayara takılan her diske yayılabilen "ELK CLONER" virüsünün yanı sıra 1986'da Pakistanlı Basit Alvi ve Amjad Farooq Alvi tarafından korsan program satışını engellemek ve telif mesajı yayınlamak amacıyla yazılan 'Brain' adlı bilgisayar virüsü zamanla amacından saparak bilgisayarlara zarar vermeye başlamıştır (Url, 6). Başlangıçta tamamen masum amaçlarla geliştirilen bazı yenilikler zamanla zararlı bir duruma dönüşebilmektedir.

Bu yeni suç türlerinin yanı sıra geçmişte var olan suçların dönüşüm geçirdiği görülmektedir. Bunların başında şüphesiz hırsızlık veya dolandırıcılık gelmektedir. Zira hırsızlar artık kapıdan girip insanları fiziksel ortamda soymak yerine siber fiziksel sistemler aracılığıyla telefon ve bilgisayar pençelerinden hayatımıza girmektedir. Hatta biz yokken değil tam da bize ulaşarak (konuşma, mesajlaşma vb.) dolandırıcılık faaliyetlerini sürdürmektedirler. Telefonlar aracılığıyla dolandırıcılık,

banka hesaplarına erişim ve bilgisayar hackleme bu temel suçlar arasında görülmektedir. Ayrıca hırsızlık, fiziksel anlamda (mala yönelik) maddi kazanç sağlamanın ötesinde intihal (kişilerin görüş ve bilgisini çalmak), sosyal medya hesaplarını çalmak, fotoğraf ve videolarını çalmak ve izinsiz kullanmak şeklinde de gerçekleşir bir hale bürünmektedir.

İlkel zamanlarda büyü, günah ve büyük bir suç olarak görülmektedir. Medyum ve büyü dolandırıcılığı günümüzde sosyal ağlar aracılığıyla kendisine geniş bir alan bulmaktadır. Herhangi bir bilimsel yönü olmayan, asılsız sözlerle haksız maddi kazanç sağlamaya yönelik olan bu dolandırıcılık türleri internet siteleri aracılığıyla yüz yüze iletişimin olmasına gerek kalmadan insanları kandırmaktadırlar.

## 2.5. Yapısal Fonksiyonalizm ve Siber Suçlar

Suçta yönelik kuramsal yaklaşımlardan biri olan Yapısal Fonksiyonalist kuram içinde Durkheim önemli bir yer edinmektedir. Sosyolojik Yöntemin Kuralları isimli eserinde normal ve anormali birbirinden ayırt etmeye çalışan Durkheim suçta normal ve yaralı bir toplumsal olgu olarak görmektedir. Suçta ancak belirli istatistiksel artış olduğu durumlarda anormal bir durum olup suçun yararlarını şu şekilde açıklamaktadır (Durkheim, 2019: 95);

*“Suç yalnızca gerekli değişimlere giden yolun açık kalmasına yardımcı olmakla kalmaz aynı zamanda bazı durumlarda bu değişimleri bizzat hazırlar. Suçun var olduğu yerde, bir yandan kolektif duygular yeni biçimler almak için gerekli esnekliği kazandırır; diğer yandan suçun kendisi, duyguların alacağı yeni biçimlerin belirlenmesinde katkıda bulunur kimi zaman. Gerçekten de, birçok durumda, suç gelecekteki ahlak anlayışının oluşumunu hızlandıran bir faktördür; olacak olan şeylere doğru bir ilerlemedir.*

Suçun yararlı, değişim ve dayanışmayı sağlayan, ahlaki normları tamamlayıcı ve oluşabilecek yeni ahlaki normların sınırlarını belirleyen toplumsal bir olgu olarak gören Durkheim, Sokrates’in Atina hukukundaki suçluluk durumunu örnek vererek günümüz modern toplumlarda oluşan düşünce özgürlüğün oluşumunda, bu özgürlüğü kısıtlayan kuralların çığnenmesiyle oluşan suç davranışının etkili olduğunu ileri sürer.

Günümüzde Durkheim’in suçta yönelik görüşleri çerçevesinde ele alınan siber suçların birçok gelişme ve bütünleşmeye yönelik olumlu işlevleri görülmektedir. Toplumsal bütünleşme, uyum ve denge açısından suçun yararlı olduğuna yönelik iddia edilen bu görüşler çerçevesinde siber suçlara baktığımız zaman bu suçların ortaya çıkmasıyla beraber ülkeler arası dayanışma, bağlılık ve bütünleşmeyi artıran uluslararası örgütlerin (ENISA, IMPACT, ITU vs.) ortaya çıkmasını sağlamaktadır. Bunun yanı sıra siber güvenlik uzmanları ve siber suçlarla mücadele emniyet kollukları siber suçların önlenmesine yönelik ortaya çıkan modern toplumlara özgü gelişmiş meslekler kategorisi içerisinde yer almaktadır. Buna paralel bir şekilde günümüzde birçok ülke hukukunda siber suçlarla ilgili ayrı bir başlık altında yasal düzenlemeler yapılmaya başlanmıştır.

Ayrıca her ne kadar etik kurallara aykırı olarak da görülse de bazen devletler arasında askeri savunma ve harekât tarzında oluşabilecek saldırıların önceden bilinmesine yönelik yapılan siber saldırılar devletlerin bu doğrultuda gerekli savunma önlemleri almasını sağlayan yararlı işlev sağlamaktadır.

Rousseau (2021: 26) *Toplum Sözleşmesi* adlı eserinde insanın her zaman kendi iyiliğini istediğini fakat bunun ne olabileceğini bilemeyeceğini ve çoğu kez aldatılabileceğini ileri sürmektedir. Özellikle günümüzde temsili demokrasinin çoğunlukta olduğu ülkelerde halk, suçlu kişiler kendilerini gizleyerek siyasi yönetimde önemli olarak görülen görevlere gelebilmektedir. Aldatıcı davranışta bulunan bu kişilerin siber saldırılar (telefon kayıtlarının dinlenmesi, telefon veya bilgisayarların hacklenmesiyle bilgilerinin ele geçirilmesi gibi) sonucunda ortaya çıkan kişisel

çıkarlara dayalı suçlarının ortaya çıkarılması devlet ve halk açısından yararlı bir işleve sahiptir. Siber saldırı bir suç olarak karşımıza çıkarken aynı zamanda herhangi bir vatandaş tarafından ihlal edilen bu davranış (izinsiz hesaplarına erişimi gibi) başka bir suçun ortaya çıkarılması konusunda fayda sağlayabilmektedir.

İnternet ve yazılım sistemleriyle siber fiziksel ortamlarda gerçekleştirilen siber suçların önlenmesine yönelik geliştirilen yazılım ve programlarla beraber yazılım anlamında gerekli ilerlemelerin sağlanması ve güvenliği tehdit eden açıkların tespit edilmesi mümkün olmaktadır. Kişilerin rahat bir şekilde erişebileceği Türkiye’de de kullanılan başlıca bu program ve yazılımlar; antivirüs, veri kaçağı önleme sistemi, güvenlik duvarı, saldırı tespit / önleme sistemi, şifreleme, elektronik/sayısal imza vs. bulunmaktadır. Siber suçların önlenmesine yönelik geliştirilen bu program ve yazılımlar toplumsal değişimin sağlanmasında rol oynamaktadır.

Suç analizi ederken Durkheim’in üzerinde durmuş olduğu temel kavramlardan biri anomidir. Durkheim anomiyi, sosyal bir yaşam alanında bireylerin ya da grupların davranışlarına öncülük edecek etkili sosyal kurum ve kuralların olmadığı durumlarda ortaya çıkan normsuzluk veya kuralsızlık durumunu ifade etmek için kullanır (Giddens ve Sutton, 2018: 325-326). Bu durumda kişiler ne yapacaklarını ve amaçlarını bilemedikleri bir çaresizlik içine düşmektedirler. Günümüzde siber suçlar arasında bulunan kişiler yazılım programlarını kullanabilmek için gerekli eğitime ve maddi güce sahip olması gereken kişiler olduğu görülmektedir. Bu bakımdan siber suçlar yoksul ve sadece maddi kazançlar peşinde koşan kişiler tarafından yapılmamaktadır.

Toplumu bir arada tutan bir güç olarak dayanışma kavramı üzerinde duran Durkheim, sanayi öncesi toplumlarında benzerliğe dayalı mekanik dayanışma içinde olduğunu ve buna karşın sanayi sonrası toplumların çeşitli alanlardaki uzmanlıklara bağlı olarak farklılığa dayalı organik dayanışmanın hâkim olduğunu ileri sürmektedir. Farklı şekillerde ortaya çıkan suç davranışlarının yanı sıra bu toplumlarda ceza sistemleri de farklılaşmaktadır. Mekanik dayanışmanın hâkim olduğu toplumlarda cezalandırıcı hukuk kuralları hüküm sürmekteyken organik dayanışmalı toplumlarda iyileştirici hukuk kuralları uygulanmaktadır. Artık ölüm, sürgün, kırbaç cezasının yerini günümüz toplumlarında cezaevi, kontrollü serbestlik, zorunlu hizmet gibi politikalar almaktadır.

Durkheim’den almış olduğu Anomi kavramını genişleterek kullanan Merton’a göre anomi, kültürel amaçlar ve bu amaçlara ulaşmak amacıyla oluşturulan meşru yollar arasında var olan kopukluktur (Bal, 2018: 14). İnsanlar kültürel amaçlar ile bu amaçlara ulaşmak amacıyla kullanmış oldukları araçlara ulaşmada bir eksiklik yaşadıkları durumlarda sosyal bir gerilim yaşamakta ve dolayısıyla suç düzeylerinde artış meydana gelmektedir. Bu bakımdan suç toplumsal anlamda var olan koşullara bağlı olarak oluşmuş dışsal kaynaklı bir sorundur. Bu bakış açısı Yapısal Fonksiyonalist bakış açısı içerisinde değerlendirilmektedir.

### 3. SONUÇ VE DEĞERLENDİRME

Suç ve ceza tarihsel süreç içerisinde çeşitli şekillerde var olarak günümüze kadar gelmiş önemli bir sorun olarak görülmektedir. Değişen toplumsal koşullara bağlı olarak çeşitli dönemlerde farklı suç türlerinin ortaya çıktığı görülmektedir. Günümüz modern veya Daniel Bell’in tanımladığı şekliyle ‘postmodern toplumlar’da da siber suç önemli bir suç çeşidi olarak görünürlük kazanmıştır. Günümüzde teknolojik ürünlerin ya da araçların üretiminde meydana gelen gelişmeler ve sivilleşme sürecine giren internetin geniş kitleler tarafından kullanılması gibi eş öneme sahip olan itici faktörler sonucunda siber suçların arttığı görülmektedir. Yapılan bilimsel çalışmalarda siber suçların kültürel, toplumsal, ekonomik gibi birçok etkilerine değinilmekte olup gerekli müdahalelerin alınmasına yönelik faaliyetler sürdürülmektedir.

Siber suçlar geçmişte var olan suçların siber fiziksel sistemler ortamında gerçekleştirilmesi şeklinde olabileceği gibi yeni suç türlerinin meydana gelmesi şeklinde de meydana gelmektedir. Bu

anlamda var olan yeni suç türlerinin cezalandırılmasına yönelik devletler hukuksal, teknolojik ve askeri alanda birtakım faaliyetler yürütmektedir. Mekândan bağımsız olması ve (uzak mesafe) mağdurlardan kilometrelerce uzak yerlerden sanal ortamda gerçekleştirilmesi dolayısıyla siber suçluların tespit edilmesi konusunda yaşanan zorluklar, ülkelerin siber saldırılar karşısında işbirliği içerisinde mücadele etmesini gerekli kılmaktadır.

Durkheim, yapısal işlevselci teori kapsamında önemli öncüllerden biridir. Özellikle suç olgusu üzerinde yapmış olduğu tespitlerle suçun faydaları ve dayanışmayı, kolektif bilinci arttırıcı bir unsur olarak görmesi onu diğer teorisyenlerden ayıran önemli bir bakış açısıdır. Durkheim, yaşadığı dönem itibarıyla siber suçların olmaması bakımından doğrudan siber suçlara yönelik bir değerlendirmesi bulunmamaktadır. Ancak suç türleri içinde yer alan siber suçlar bu genel değerlendirmeleri içinde barındırmaktadır. Yapılan çalışmada siber suçların, faydalı, dayanışmayı arttırıcı, değişim ve gelişmelerin önünü açan toplumsal bir olgu olarak ele alınmaktadır. Bu kapsamda siber suçların; devletlerarası işbirliğini zorunlu kılmasıyla bağımlılığı ve dayanışmayı arttıran, teknolojik alanda mücadeleye yönelik geliştirilen yazılım ve araçlarla ilerlemeyi tetikleyen ve son olarak hukuksal anlamda yeni kanunların eklenmesiyle değişimi ve toplumsal sınırları belirleyen toplumsal bir fenomen olduğu görülmektedir.

Siber suçluların ve mağdurların verilerine yönelik gizlilik dolayısıyla eğitim durumu, coğrafi konum, yaş, cinsiyet, meslek, medeni durum gibi temel değişkenler incelenememektedir. Bu nedenle yapılan çalışma hizmete dayalı yayınlanan siber suç verileriyle sınırlı kalmaktadır. İleride yapılacak bilimsel çalışmalarda bu gibi değişkenlerin değerlendirilmesi alınacak müdahaleler konusundaki boşlukların neler olduğu konusunda ipuçları vermesi açısından faydalı olacaktır.

## KAYNAKÇA

- Altun, İ. (2016). *Ortam Sanal Suç Gerçek*. İstanbul: İskenderiye.
- Altunok, E. ve Vural, A. F. (2016). Bilişim Suçları, *Kamu Denetçileri Derneği Denetim Dergisi*, (8), 74-84.
- Bal, H. (2016). *Suç Sosyolojisi*, Bursa: Sentez.
- Batal, S. ve Tuğlu, K. (2018). Endüstri 4.0 Ve Yeni Teknolojiler Karşısında Yerel Yönetimlerde Yaşanan Değişimler. *Avrasya Uluslararası Araştırmalar Dergisi*, 14(6), 216-232.
- Bauman, Z. (2013). *Modernite, Kapitalizm, Sosyalizm Küresel Çağda Sosyal Eşitsizlik*, (Çev. F. Doruk Ergun), İstanbul: Say.
- Birel, E. (2022). *Sosyolojik Açından Televizyonda Değişen Hegemonik Kodlar Üzerine Bir Tahlil; Hercai Dizisi*. Yüksek Lisans Tezi, Adıyaman Üniversitesi Lisansüstü Eğitim Enstitüsü Sosyoloji Anabilim Dalı, Adıyaman.
- Blau, A. (2020). Şimdi Hepimiz İçindeyiz. *Siber Güvenlik Dijital Dönüşüm*, (Çev. Ümit Şensoy), İstanbul: Optimist.
- Çavdar, S. S. (2019). *Endüstri 4.0 Ve İşgücü Piyasası'na Yansımaları*. Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Çalışma Ekonomisi ve Endüstri İlişkileri Anabilim Dalı, Trabzon.
- Doğrul, M. ve Ergürüm, A. (2021). Blok Zincirinin (Blockchain) Literatür Büyümesi Işığında Yeni Siber Güvenlik Arayışları, *Güvenlik Bilimleri Dergisi*, 10(3), 175-194.
- Durkheim, E. (2019). *Sosyolojik Yöntemin Kuralları*. (Çev. Özcan Doğan), Ankara: Doğubatı.
- Ermeydan, D. (2018) *Türk Ceza Kanunu'nda Bilişim Suçları*. Yüksek Lisans Tezi, Çağ Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı, Mersin.
- Giddens, A. ve Sutton, P.W. (2018). *Sosyolojide Temel Kavramlar*. (Çev. Ali Esgin), Ankara: Phoenix.
- Karataşoğlu, E. B. (2022). Siber Suçlara Sosyolojik Bakış. *Academic Social Resources Journal*, 33(7), 36-53.

- Koca, D. (2020). Sanayi Devrimlerinin Tarihsel Arka Planı ve İşgücü Becerileri Üzerindeki Yansımaları, *OPUS Uluslararası Toplum Araştırma Dergisi*, 31(16), 2528-9527.
- Marcum, C.D. ve Higgins, G.E. (2019). Cybercrime, *Handbook on Crime and Deviance* iç. (Editör: John DeLamater), Switzerland: Springer, 459-478,.
- Oppenheimer, H. (2016). İlk Suçlar. (Çev. Devrim Aydın), *Ankara Barosu Dergisi*, (4), 271-288.
- ÖZCAN, Ö. Ö. (2022). Sosyoloji, Kriminoloji ve Fotoğraf. *Sosyolojik Bağlam Dergisi*, 3(1), 90-103.
- Rousseau, J.J. (2021). *Toplum Sözleşmesi*. (Çev. Vedat Günyol), İstanbul: Türkiye İş Bankası Kültür Yayınları.
- Suveren, Y. (2019). Küreselleşme, İnternet ve Yeni Suçlar: Siber Dünya ve Siber Suçlar, *Suç Sosyolojisi* iç. (Editör: Fuat Güllüpnar), Eskişehir: Açıköğretim Fakültesi.
- T.C. Turizm ve Kültür Bakanlığı. (2017). *Siber Mücadeleye Giriş*. İstanbul: Kutlu.
- Toffler, A. (2008). *Üçüncü Dalga: Bir Fütürist Ekonomi Analizi Klasığı*. İstanbul: Koridor.
- Url 1: <https://adlisicil.adalet.gov.tr/Home/SayfaDetay/adl-istatistikler-yayin-arsivi> (Erişim Tarihi: 08.11.2022)
- Url 2: <https://www.bilisimdergisi.org.tr/s137/pdf/14-19.pdf> (Erişim Tarihi: 19.11.2022).
- Url 3: <https://aag-it.com/the-latest-2022-cyber-crime-statistics/> (Erişim Tarihi: 5.12.2022).
- Url 4: <https://tr.euronews.com/2022/09/30/meksikali-lider-ulkesine-duzenlenen-siber-saldirilari-ve-hakkindaki-saglik-kayitlarini-dog> (Erişim Tarihi: 12.11.2022).
- Url 5: <https://www.btk.gov.tr/uploads/pages/arastirma-raporlari/dijitallesen-dunyada-bilisim-suclari-ve-mucadele-yontemleri-6218e2417eaea.pdf> (Erişim Tarihi: 15.11.2022).
- Url 6: <https://tr.wikipedia.org/wiki/Telefon> (Erişim Tarihi: 13.11.2022).
- Url 7: <https://www.muhammedbalci.com/hukukdunyasi/makaleler/birikimlerVI/1372.pdf> (Erişim Tarihi: 20.11.2022).