

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

SOSYOLOJİ ANABİLİM DALI

YÜKSEK LİSANS PROGRAMI

**DİJİTAL DÜNYADA ETKİLEŞİM FORMLARI VE SİBER SUÇ MAĞDURLARI:
BURSA İLİ ÖRNEĞİ**

YÜKSEK LİSANS

Buket Cansu ULUDAĞ

EYLÜL 2022

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

SOSYOLOJİ ANABİLİM DALI

YÜKSEK LİSANS PROGRAMI

**DİJİTAL DÜNYADA ETKİLEŞİM FORMLARI VE SİBER SUÇ MAĞDURLARI:
BURSA İLİ ÖRNEĞİ**

YÜKSEK LİSANS TEZİ

Buket Cansu ULUDAĞ

Tez Danışmanı: Dr. Öğr. Üyesi Serdal FİDAN

EYLÜL 2022

TRABZON

ONAY SAYFASI

Buket Cansu ULUDAĞ tarafından hazırlanan “Dijital Dünyada Etkileşim Formları ve Siber Suç Mağdurları: Bursa İli Örneği” adlı bu çalışma 25.10.2022 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak jürimiz tarafından Sosyoloji Anabilim Dalı Tezli Yüksek Lisans Programı’nda **yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyesi		Karar		İmza
Adı ve Soyadı	Görevi	Kabul	Ret	
Doç. Dr. Musa Yavuz ALPTEKİN	Başkan	☐	☐	
Dr. Öğr. Üyesi Serdal FİDAN	Üye	☐	☐	
Doç. Dr. Orhan BİNGÖL	Üye	☐	☐	

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduklarını onaylıyorum.

Prof. Dr. Tülay İLHAN NAS
Enstitü Müdürü

BİLDİRİM SAYFASI

Tez içerisindeki tüm bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca Karadeniz Teknik Üniversitesi - Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzu'na uygun olarak hazırlanan bu çalışmada yararlanılan kaynakların tümüne eksiksiz atıf yapıldığını, aksinin ortaya çıkması durumunda yasal sonuçlarını kabul edeceğimi beyan ederim.

Buket Cansu ULUDAĞ

14.09.2022

ÖNSÖZ

Suç olgusu geçmişten günümüze kadar her toplumda ve her çağda var olmuştur. Bireylerin bir araya gelerek oluşturdukları topluluklar daima düzeni sağlamaya çalışmışlardır. Dolayısıyla düzeni sağlamak adına ortaya koydukları toplumsal ve hukuki kurallar her zaman bireylerin düşünce ve davranışları ile uyum sağlayamamış, aykırı davranan bireyler sapkın ve suçlu olarak nitelendirilmiş, gerçekleştirilen eylemler ise sapma ve suç olarak ifade edilmiştir. Gerçekleştirilen aykırı eylemler toplumsal düzene zarar veriyor olsa da öte yandan toplumsal bütünleşmeye de katkı sağlamaktadır. Bu sebeple suçun tamamen olumsuz bir olgu olduğu düşünülmemelidir. Olumlu ya da olumsuz her türlü çatışmanın olduğu ortamlarda suç oluşumu olağandır. Teknolojik gelişmeler ile birlikte suç, her ne kadar yeni bir ortam edinmiş ve birçok çeşidi ortaya çıkmış olsa da; eylem, fail ve mağdur üçlüsü bakımından herhangi bir değişime uğramamıştır. Günümüzde internetin ve dijital olan nesnelerin hayatımızın ayrılmaz bir parçası haline gelmiş olması siber suçları da hayatımızın bir gerçeği haline getirmiştir.

Öncelikle tez çalışması süreci boyunca desteklerini ve tavsiyelerini esirgemeyen, her sorunda mutlaka yardımcı olmaya çalışan danışmanım Dr. Öğr. Üyesi Serdal FİDAN'a ve kendime örnek aldığım hocam Doç. Dr. Bayram SEVİNÇ'e sonsuz teşekkürlerimi sunarım. Bunun yanı sıra her zaman destekçim olan aileme teşekkürü bir borç bilirim. Bu dönemde yanımda olan ve stresimi anlayan tüm arkadaşlarıma ve hocalarıma teşekkürlerimi sunarım.

Eylül, 2022

Buket Cansu ULUDAĞ

İÇİNDEKİLER

ÖNSÖZ.....	IV
İÇİNDEKİLER	V
ÖZET.....	VII
ABSTRACT	VIII
ŞEKİLLER LİSTESİ.....	IIIX
TABLolar LİSTESİ.....	X
GİRİŞ	1

BİRİNCİ BÖLÜM

1. ARAŞTIRMANIN METODOLOJİSİ.....	2-6
1.1. Araştırmanın Konusu	2
1.2. Araştırmanın Amaç ve Önemi.....	2
1.3. Araştırmanın Problematiği	3
1.4. Araştırmanın Sınırlılıkları	3
1.5. Araştırmanın Yöntemi.....	3
1.5.1. Veri Toplama Süreci ve Tekniği	4
1.5.2. Veri Analiz Tekniği.....	4
1.6. Çalışma Grubu	4

İKİNCİ BÖLÜM

2. KAVRAMSAL VE KURAMSAL ÇERÇEVE	6-43
2.1. İnternet Kavramı Ve Tarihsel Gelişimi	6
2.2. Sosyal Medya	10
2.2.1. Facebook	13
2.2.2. Instagram.....	14
2.2.3. Twitter	15
2.2.4. Youtube	16
2.2.5. Diğer Sosyal Medya Ağları.....	17
2.3. Dijital Çağda Gerçeklik Olgusu, Sanal Kimlik Ve İkincil Yaşam (Second Life).....	17
2.4. Dijitalleşme ve Dijital Çağda Kültür.....	24
2.5. Suç.....	27

2.5.1. Suçlu Davranışın Açıklanmasına Dair Yaklaşımlar	29
2.6. Dijital Çağda Suçun Dönüşümü: Siber Suçlar	30
2.6.1. Siber Suç İşleniş Çeşitleri	33
2.6.1.1. Oltalama (Phishing).....	33
2.6.1.2. Truva Atı (Trojan Horse).....	33
2.6.1.3. Çöpe Dalma (Scavenging).....	33
2.6.1.4. Bilgisayar Virüsleri	34
2.6.1.5. Ağ Solucanları (Network Worms)	34
2.6.1.6. Gizli Kapılar (Trap Doors).....	34
2.6.1.7. Salam Tekniği (Salami Techniques)	35
2.6.1.8. Mantık Bombaları (Logic Bombs)	35
2.6.1.9. Tuş Kaydediciler (Keylogger) ve Ekran Kaydediciler (Screenlogger)	35
2.6.1.10. Bukalemun Tekniği (Chameleon Techniques).....	36
2.6.1.11. Zombi Bilgisayar.....	36
2.6.1.12. Botnet Saldırıları	36
2.6.1.13. İstenmeyen Elektronik Postalar (Spam)	36
2.6.1.14. Tavşanlar (Rabbits)	37
2.6.1.15. Diğer Siber Suç Teknikleri.....	37
2.7. Mağdur	37
2.8. Araştırmanın Kuramsal Perspektifi	38
2.8.1. Rutin Aktiviteler Teorisi	38

ÜÇÜNCÜ BÖLÜM

3. ARAŞTIRMANIN BULGULARI.....	43-62
3.1. Katılımcıların Özellikleri ve İnternet Kullanım Alışkanlıkları	43
3.2. Temkinli Olma ve Önlem Alma	46
3.3. Damgalanma Korkusu ve Mücadele Süreci	49
3.4. Olumlama Yaklaşımı ve Kadercilik	55
3.5. Rutin İnternet Kullanım Alışkanlığına Etkiler	57
3.6. Katılımcıların Almış Oldukları Önlemler ve Siber Suç Mağduriyetini Önlemek İçin Önerileri	59
SONUÇ VE ÖNERİLER.....	62
KAYNAKÇA	65
EKLER.....	76
ÖZGEÇMİŞ.....	77

ÖZET

Soğuk Savaş döneminde ortaya çıkan internet ile birlikte dünya çapında büyük bir değişim ve dönüşüm süreci yaşanmaya başlanmıştır. İnternetin keşfinin getirdiği dijitalleşme ile birlikte küreselleşme hız kazanmış ve alışlagelmiş olan kültürel yapıların, rutin aktivitelerin, suç ve benzeri olguların da dijital dönüşümüne yol açmıştır. Suç olgusunun sanal ortama taşınması, mağdurlarını da beraberinde getirmiştir. Bu çalışmada sanal ortama taşınan ve siber suç olarak tanımlanan suçlardan etkilenen mağdurların ortak yönleri araştırılmıştır. Aynı zamanda mağdurların belirli özelliklerinin mağduriyet yaşamalarında etkili olup olmadıkları da araştırılmıştır. Yapılan araştırmanın teorik zeminini Lawrance Cohen ve Marcus Felson'un üzerine çalışmış oldukları Rutin Aktiviteler Teorisi oluşturmaktadır. Araştırmanın mekansal sınırı olarak Bursa ili belirlenmiştir. Çalışma grubu, siber suç mağduriyeti yaşamış olan 20 kişiden oluşmaktadır. Mağdurların yaşadıkları süreci daha iyi anlayabilmek açısından nitel yöntemin tercih edilmiş olduğu bu çalışmada fenomenolojik yaklaşım esas alınmıştır. Araştırma verileri; ölçüt örnekleme tekniği ile belirlenmiş olan 20 katılımcıya yarı yapılandırılmış mülakat yapılarak elde edilmiştir. Elde edilen veriler betimsel analiz tekniği kullanılarak yorumlanmıştır. Bireylerin rutin internet kullanım alışkanlıklarının mağduriyet yaşamalarına sebebiyet vermekte olduğu sonucu elde edilmiştir.

Anahtar Kelimeler: Dijitalleşme, Suç, Siber Suç, Mağdur, Rutin Aktiviteler Teorisi

ABSTRACT

With the internet that emerged during the Cold War period, a great change and transformation process began to be experienced around the world. With the digitalization brought about by the discovery of the Internet, globalization has accelerated and has led to the transformation of conventional cultural structures, routine activities, crime and similar phenomena into digital. The transfer of the crime phenomenon to the virtual environment has brought its victims with it. In this research, the common aspects of the victims who were transferred to the virtual environment and affected by the crimes defined as cybercrime were investigated. At the same time, it was also investigated whether certain characteristics of the victims were effective in experiencing victimization. The theoretical basis of the research is the Routine Activities Theory, which Lawrence Cohen and Marcus Felson have worked on. Bursa province was determined as the spatial limit of the research. The working group consists of 20 people who have been victims of cybercrime. In this research, in which the qualitative method was preferred in order to better understand the process experienced by the victims, the phenomenological approach was taken as the basis. Research data; It was obtained by conducting semi-structured in-depth interviews with 20 participants who were determined by criterion sampling technique. The data obtained were interpreted using the descriptive analysis technique. It has been concluded that the routine internet usage habits of individuals cause them to experience victimization.

Keywords: Digitalization, Crime, Cybercrime, Victim, Routine Activities Theory

ŞEKİLLER LİSTESİ

Şekil Nr.	Şekil Adı	Sayfa Nr.
1	Küresel Ölçekte İnternet Kullanımı	9
2	Küresel Ölçekte Sosyal Medya Kullanımı	12



TABLÖLAR LİSTESİ

Tablo Nr.	Tablo Adı	Sayfa Nr.
1	Siber Suç Mağduru Katılımcı Özellikleri	43



GİRİŞ

İnternetin ortaya çıkışı birçok bilim dalı tarafında merak uyandırmış ve ortaya çıkışından bu yana etkileri sürekli olarak araştırılmıştır. Günümüzde, yaşamın bir parçası haline gelmiştir. Rutin günlük faaliyetlerin birçoğu internet kullanılarak gerçekleştirilmektedir. Alışveriş, fatura ödemeleri, başvuru ücretleri ödemeleri gibi eylemler çok hızlı ve kolay bir şekilde mekan değişimi yapma gereksinimi duymadan gerçekleştirilebilmektedir. Bir sınıf ya da konferans salonu ihtiyacı olmadan çevrimiçi olarak internet yolu ile derslere ve toplantılara katılabilinmektedir. İnternetin hayatı kolaylaştırmasının ve getirdiği bu olumlu etkilerinin yanı sıra olumsuz etkilerinin de olduğu aşikardır. Dijital bir çağ yaşanmaya başlanmış ve içerisinde kültür, suç gibi olgularında bulunduğu alışlagelmiş olan yapıların dönüşümüne yol açmıştır.

Geleneksel suçun sanal ortama taşınması ve yeniden üretilmesi ile birlikte, siber suç eylemlerinden etkilenen mağdurlar ortaya çıkmıştır. Siber suç mağdurlarının internet kullanım sürecindeki rutin aktivitelerinin mağdur olmalarına sebep olduğu konusunda var olan tartışmalar bu araştırmanın yapılmasındaki en büyük amacı oluşturmaktadır. Bu sebeple araştırma rutin aktiviteler teorisi bağlamına dayandırılmıştır. Durumsal suç önleme ile bütünleştirilen rutin aktiviteler teorisi çerçevesinde hangi eylemlerin mağduriyete yol açtığı ve hangi önlemler ile fırsatlar azaltılarak hem suçluların engellenebileceği hem de mağduriyetlerin azalabileceğine ulaşılmaya çalışılmıştır.

Üç bölümden oluşan bu çalışmada; birinci bölüm araştırmanın metodolojisini içermektedir. Araştırmanın konusu, amacı ve önemi, problematiği, yöntemi, sınırlılıklar, çalışma grubu, verileri toplama süreci, verileri toplama ve analiz etme tekniği bu bölüm içerisinde yer almaktadır.

İkinci bölümde araştırmanın temel basamağını oluşturan internet kavramı ve tarihsel gelişimi, internet ile birlikte gerçekleşen dijitalleşme, dijital kültür, sosyal medya, gerçeklik ve dijitalleşmenin etkilediği mahremiyet kavramları detaylandırılmıştır. Aynı zamanda suç olgusunun internetin ortaya çıkışı ile birlikte nasıl bir dönüşüm geçirdiğinden söz edilmiştir. Siber suç olarak adlandırılan, yeniden üretilen suç olgusunun ortaya çıkardığı teknikler detaylandırılmıştır. Suç olgusunun içerisinde yer alan mağdur kavramı açıklanmış ve araştırmanın dayandığı teori hakkında bilgilendirme yapılmıştır.

Üçüncü ve son bölümde ise; Bursa ilinde siber suç mağdurları ile yapılan mülakatlar sonucu elde edilmiş olan verilerin analizi yer almaktadır. Veriler, altı adet tema altında sorular ve verilen cevaplar doğrultusunda yorumlanmıştır.

BİRİNCİ BÖLÜM

1. ARAŞTIRMANIN METODOLOJİSİ

1.1. Araştırmanın Konusu

Küreselleşme ve teknolojik gelişmeler ile birlikte dijitalleşen dünyada, suç olgusu yeni bir anlam kazanmaktadır. Suçun mekan değiştirmesi söz konusu olmakta, fiziksel mekanlarda işlenen geleneksel suçların yanı sıra sanal ortamda işlenen suçlar giderek artmakta ve çeşitlenmektedir. Bu internet tabanlı suçlar, siber suç olarak adlandırılmaktadır. Ortaya çıkan; yer, zaman, mekan sınırlılığı bulunmayan siber suçların ulusalı aşan mağduriyet boyutu bulunmaktadır. Yaşanılan bu dijital mağduriyetler günümüzde, özellikle dijital ortamlarda vakit geçirmenin sıklaştığı salgın sürecinde de artış göstermiş bulunmaktadır. Oluşan mağduriyetlerin nedenlerini ve sonuçlarını da ele alacak olan ve mağdurların ortak noktalarının bulunması amacıyla yapılacak olan bu çalışma, rutin olarak gerçekleşen hangi davranışların ya da durumların siber suç mağduru olmaya zemin hazırladığını, mağdurların ortak özelliklerini ve bu konuda ne gibi önlemler alınabileceğini ortaya koyma amacı taşımaktadır.

1.2. Araştırmanın Amaç ve Önemi

Günümüzde siber suç mağduriyetleri artmakta ve mağduriyet yaşayan bireylerin damgalanma korkusu sebebi ile yaşadıkları durumu paylaşmamaları, sonuç alamayacaklarını düşündükleri için herhangi bir yasal yola başvurmamaları dikkat çekmektedir. Yapılmış olan çalışmanın temel amacı; siber suç mağduru olma nedenlerini süreç hakkında ayrıntılı bilgiler elde ederek ortaya çıkarmak, mağdurların ortak yönlerini bulmak ve hangi davranışların mağduriyet riskini artırdığını saptayarak mağduriyet durumunu önleyebilmek açısından ne gibi önlemler alınabileceği konusunda öneriler sunabilmektir. Mağdurlar ile ilgili bu bilgilere ulaşabilmek amacıyla siber suç mağduriyeti yaşamış bireyler ile görüşmeler gerçekleştirilmiştir. Literatür incelendiğinde mağduriyet alanında, spesifik olarak siber suç mağdurları konusunda yeterli düzeyde kaynak bulunmadığı görülmektedir. Özellikle yeni yaşam koşullarına bağlı olarak gelişen mağduriyet çeşitlenmesi ve dijital araçların kullanımındaki yaygınlıkla beraber alan genişlemesi, bu tür bir literatür kaynağı için eksiklikleri pekiştirmektedir. Bu sebeple yeni çalışmalar yapılarak kaynakların zenginleştirilmesi önem arz etmektedir. Yapılmış olan bu çalışma ile alana katkı sağlanması ve ileride yapılacak yeni çalışmalar için bir kaynak olması amaçlanmıştır.

1.3. Araştırmanın Problematiği

Siber suç mağdurları ile yapılmış olan bu çalışmada öncelikle; mağduriyetlerin eğitim düzeyine göre olasılıklarının artıp azalmasının söz konusu olup olmadığı ve eğitim düzeyi yüksek olan bireylerin internet kullanımında daha dikkatli olup olmadıkları araştırılmıştır. Aynı zamanda eğitim düzeyi arttıkça yaşanan mağduriyetleri çevreleri ile paylaşma eyleminin değişkenlik gösterip göstermediği irdelenmiştir. İkinci olarak; bireylerin rutin internet kullanım alışkanlıklarının; internet kullanım sıklığının ve amaçlarının siber suç mağduriyeti yaşanmasında ne kadar etkili olduğu araştırılmıştır. Bunun yanı sıra; daha önceden siber suç mağduriyetlerine ilişkin bilgi edinmiş olmanın bireylerin internet kullanımında dikkatli olmalarına sebep olup olmadığı ve yaşanan mağduriyet sonrasında internet kullanım alışkanlıklarında herhangi bir değişikliğin söz konusu olup olmadığı incelenmiştir.

1.4. Araştırmanın Sınırlılıkları

Araştırma Bursa ilinde ikamet eden ve siber suç mağduriyeti yaşamış olan bireyleri kapsamaktadır. Bursa ilinde ikamet ediliyor olunması, siber suç mağduriyeti yaşanmış olunması ve salgın dönemi şartları araştırmanın sınırlılıklarını oluşturmaktadır. Araştırma fenomenolojik desen ile tasarlanmış olduğundan görüşme yapılan bireylerin siber suç mağduriyetini deneyimlemiş olmaları gerekmektedir. Araştırmada elde edilmiş olan verilerin geçerliliği ise araştırmaya katılan bireylerin, sorulara doğru yanıtlar verdikleri varsayımına dayanmaktadır.

Bursa ili içerisinde yaşanmış olan toplam siber suç mağduriyeti vaka sayısına ulaşmak istenmiş fakat Bursa Siber Suçlar İle Mücadele Birimi ile yapılan görüşmede herhangi bir veri paylaşımında bulunulamayacağı sonucu ile karşılaşmıştır.

1.5. Araştırmanın Yöntemi

Yapılan çalışma; siber suç mağdurlarının niteliklerini, ortak özelliklerini ve rutin aktivitelerini öğrenme, inceleme ve anlamlandırma amacı taşıdığından dolayı bu kapsamda kullanılmış olan yaklaşım temel nitel araştırma yöntemidir. Görüşmeler, yarı yapılandırılmış mülakat tekniği ile gerçekleştirilmiştir. Çalışma kapsamında veri toplama aracı olarak yarı yapılandırılmış mülakat formu kullanılmıştır. Mülakatlar, görüşmecilerin salgın koşullarından dolayı hür iradeleriyle yapacakları tercihe bağlı olarak yüz yüze (tedbirlere uyulmuş bir şekilde) veya çevrimiçi (online) olarak gerçekleştirilmiştir. Çalışma için gerekli veri doyumu sağlanana kadar toplanmış olan veriler betimsel analiz tekniği kullanılarak çözümlenmiştir.

Uygulanan mülakatlar sırasında katılımcıların tüm kişisel verileri, kendileriyle paylaşılmış olan bilgilendirilmiş onam (rıza) formunun güvencesinde bilimsel veri gizliliğiyle korunacaktır. Katılımcıların araştırma sorularına verdikleri cevaplar gizlilikleri korunarak, rızaları doğrultusunda

kayıt altına alınmış ve araştırmaya katılım için hiç kimse zorlanmamıştır. Araştırma süresince katılımcılar herhangi bir baskı veya yönlendirilmeye maruz bırakılmadan kendi hür iradeleriyle vermek istedikleri cevaplar dikkatle dinlenip, olduğu gibi kabul edilmiştir. Araştırma sonucunda elde edilen tüm veriler bilimsel tarafsızlık ilkesi doğrultusunda incelenip yorumlanarak sonuç raporu hazırlanmıştır. Bulgular bilimsel etik kurallar çerçevesinde değerlendirilmiş ve verilere etik kurallar çerçevesinde bağlı kalınarak herhangi bir etik dışı sonuca asla mahal verilmemiştir.

1.5.1. Veri Toplama Süreci ve Tekniği

Yapılan araştırma; siber suç mağdurlarının niteliklerini, ortak özelliklerini ve rutin aktivitelerini öğrenme, inceleme ve anlamlandırma amacı taşıdığından dolayı bu kapsamda kullanılmış olan yaklaşım temel nitel araştırma yöntemidir. Görüşmeler, yarı yapılandırılmış mülakat tekniği ile gerçekleştirilmiştir. Araştırma kapsamında veri toplama aracı olarak nitel araştırmalarda sıklıkla kullanılan ve mülakat sırasında ortaya çıkan konulara göre yeni soruların da türetilbildiği yarı yapılandırılmış mülakat yöntemi kullanılmıştır. Katılımcılarla 10 sorudan oluşan mülakat formu ile ortalama 15 dakikalık görüşmeler gerçekleştirilmiştir. Mülakatlar, görüşmecilerin salgın dönemi koşullarından dolayı hür iradeleriyle yaptıkları tercihe bağlı olarak yüz yüze (tedbirlere uyulmuş bir şekilde), telefon görüşmesi şeklinde ve çevrimiçi (online) olarak Aralık 2021 ile Mayıs 2022 tarihleri arasında gerçekleştirilmiştir. Çalışma için gerekli veri doyumu sağlanana kadar toplanan veriler fenomenolojik yaklaşım çerçevesinde ele alınarak çözümlenmiştir. Araştırmanın örnekleme oluşturulurken ise siber suç mağduriyeti yaşamış olan bireylere odaklanıldığından, amaçsal örnekleme yöntemi türlerinden biri olan ölçüt örnekleme tekniği kullanılmıştır.

1.5.2. Veri Analiz Tekniği

Araştırmanın mülakat sürecinden elde edilmiş olan tüm veriler öncelikle manuel olarak bilgisayar ortamına aktarılmış ve detaylı şekilde incelenmiştir. İnceleme sonucunda sorulan sorular ve verilen cevaplar baz alınarak 6 farklı tema oluşturulmuş, detaylandırmalar ve analizler bu başlıklar altında yapılmıştır. Elde edilen veriler fenomenolojik yaklaşım çerçevesinde, betimsel analiz tekniği kullanılarak manuel şekilde yorumlanmıştır.

1.6. Çalışma Grubu

Araştırmanın çalışma grubunu Bursa ilinde ikamet eden ve siber suç mağduriyeti yaşamış olan bireyler oluşturmaktadır. Katılımcılara; siber suç mağduriyeti yaşamış olma ve Bursa ilinde ikamet etme gibi belirli ölçütler bulunduğundan, ölçüt örnekleme yöntemi kullanılarak ulaşılmıştır.

Seçilmiş olan araştırma konusu, çalışma grubuna ulaşım sürecinde bireylerin damgalanma korkusu sebebi ile paylaşmak istemeyeceği bilgileri sorgulaması nedeniyle zorluklar çıkarmıştır.

Katılımcılara verecekleri bilgilerin yalnızca araştırma amacı ile kullanılacağı ve bir başkasına aktarılmayacağı iletilmiş olsa da en yakınlarımız dahil olmak üzere birçok kişi tarafından mülakat reddedilmiştir. Bunun yanı sıra 2021 yılının Aralık ayı ile 2022 yılının Mayıs ayı içerisinde gerçekleştirilmiş olan mülakat sürecinde, 2020 yılında başlamış olan Covid-19 salgın dönemi şartlarının hala devam ediyor olması sebebi ile mülakata katılmayı kabul eden birçok kişi tarafından da yüz yüze görüşme onaylanmamış, online (çevrimiçi) olarak ya da telefon görüşmesi ile mülakat tamamlanmıştır.



İKİNCİ BÖLÜM

2. KAVRAMSAL VE KURAMSAL ÇERÇEVE

2.1. İnternet Kavramı ve Tarihsel Gelişimi

Günümüzde her alanda karşılaşılmakta ve kullanılmakta olan internetin ortaya çıkışını, 1969 yılında Arpanet'in icat edilmesine dayandırabilmek mümkündür. Spesifik olarak; Amerika Birleşik Devletleri ve Sovyet Sosyalist Cumhuriyetler Birliği arasında ortaya çıkan Soğuk Savaş Dönemi'nin bir ürünü olduğu söylenebilir. İki ülke arasındaki askeri ve ideolojik bu rekabet; gizli, hızlı ve kesintisiz bir iletişim arayışı içerisine girilmesine sebep olarak internetin ortaya çıkmasına zemin hazırlamıştır. İlk olarak askeri haberleşme amacıyla kullanılmaya başlanmış olsa da zamanla önce bilimsel camia tarafından kullanılarak bilgi alışverişinde kolaylıklar sağlamış, daha sonra kullanımı genele yayılmıştır. Yaygın bir şekilde kullanılmaya başlaması 1991 yılında geliştirilen World Wide Web sayesinde mümkün hale gelmiştir (Akyeşilmen, 2018: 25; Brenner, 2010: 14 - 20). Doğal olarak internet kullanıcısı sayısı da artmıştır. Soğuk Savaş endişelerinin ve gerginliğinin uzaklaşmaya başladığı 1996 yılında, bireyler ya da gruplar tarafından; kişisel, bilimsel vb. her tür amaç ile kullanılan bilgisayar ağ sayısı 20 milyona ulaşmış ve yatay iletişimin temel taşı oluşturmıştır (Castells, 2008a: 8).

İnternet; kısa zaman içerisinde, hızlı bir şekilde yayılmaya devam etmiştir. Matbaanın icadından sonra ilk defa bir teknoloji hızlı ve güçlü bir bilgi değişim ve dönüşümüne sebep olmuştur. Bilgi akışını sağlayan ve birbirleri arasında bağlantılara sahip binlerce bilgisayardan meydana gelen ağ sistemi, internetin omurgasını oluşturmuştur (Akkaş, 2015: 24). Bu şekilde gelişimine devam eden internet sadece teknolojik bir yenilik olarak değil, aynı zamanda teknolojinin özünü de ortaya çıkaran bir güç olarak nitelendirilmiştir. Bireylere sunduğu kullanım imkanlarının ve çeşitliliğinin sınırsızlığı, hiçbir teknolojik yenilik ile karşılaştırılamayacak bir güç olduğunun kanıtı olarak gösterilebilmektedir (Dreyfus, 2016: 13-14).

Hızla ivme kazanan teknolojik gelişmeler ile birlikte bireyler, bilgiye eskisinden daha çok ihtiyaç duyar hale gelmiştir. Bu bilme ihtiyacındaki artışla birlikte iletişim ve bilgisayar teknolojileri alanlarındaki gelişmeler, internetin dünya geneline yayılmasının hızını ve nedenini açıklayabilmektedir. Geçmişte bir şeyi öğrenebilmek günler ve hatta aylar alabiliyorken, öğrenildiği an ise o bilgiye artık ihtiyaç kalmamış olabiliyorken günümüzde saniyeler içerisinde bilmek istenilen her şeye ulaşılabilir. Dolayısıyla keşfi ile bilgi alışverişinde sınırların,

zamanın ve mekanın önemini yitirmesine sebep olan internet; küreselleşmenin en önemli iletişim ve etkileşim aracı olarak görülmektedir (Akkaş, 2015: 57; Fidan, 2011: 25).

Teknolojik gelişmelerin ve internetin getirdiği kitle iletişim araçlarındaki değişim ve dönüşümler medyanın melezeleşmesi olarak ifade edilmektedir. Bu melezeleşme yeni olan sistemin önceki sisteme eklenilerek tamamen ya da kısmen bütünleşmesi olarak tanımlanmaktadır. Öte yandan, yerel olan her şey iletişim ve etkileşimin kolaylaşması sayesinde küresel bir boyut kazanmaya başlamaktadır (McLuhan ve Powers, 2001: 204-205). Örneğin; A kıtasında meydana gelen yerel bir olayı tüm kıtalar öğrenebilmekte ya da B ülkesinin C şehrinde ortaya çıkan herhangi bir ayaklanma, bütün dünya tarafından canlı olarak izlenebilmekte ve etkisini hissettirebilmektedir. Kitle iletişim araçlarının giderek gelişmesi günümüzde birbirlerinden kısmen haberdar olabilen ve nadiren bilgi alışverişinde bulunabilen ülkeler arasındaki kopukluğun artık mümkün olmadığını da göstermektedir. Zaman ve mekandaki farklılıkların önemini yitirmesi ile dünyanın, üzerinde sadece fiziksel sınırlar ile ayrılmış fakat sınırlarının bile anlamlarının muğlaklaştığı ülkelerin var olduğu bir bütün haline almaya başladığı düşünülmektedir. Daha net ifade ile dünyanın küresel bir köy haline gelmeye başladığından söz edilmektedir (Bal, 2013a: 246).

Ülkelerin bir bütün haline gelmesini sağlayan internetin keşfi, her bilim dalında olduğu gibi tarihçiler için de önem arz etmektedir. İnsanlığın gelişim sürecini tanımlayan tarihçilere göre; insanlığı kökten değişime uğratmış iki büyük devrim gerçekleşmiştir. Bunlardan ilki Tarım Devrimi, ikincisi ise Sanayi Devrimi olarak anılmaktadır. Üçüncü bir devrim olarak Dijital Devrimin yaşanıp yaşanmadığı sorusu ise günümüzde çok sık tartışılan bir konu haline gelmiştir (Lokke, 2018: 27). Bazı görüşlere göre; kişisel bilgisayar ve akıllı telefonların yaygınlaşması ile birlikte, internetin ev ya da iş yeri gibi her alanda kullanılabilir olması Dijital Devrimi başlatmıştır (Kaplan, 2017: 37). Gündelik yaşamın her alanına bu şekilde nüfuz etmiş olan internet, her geçen gün yeni bir değişikliğe sebep olmaktadır. Bunun yanı sıra, var olan toplumsal pratiklerin gerçek dünyadan internet tabanlı dijital dünyaya taşınmasına ve yeni pratikler kazanmasına da ortam hazırlamıştır (Yegen, 2014: 118-131). Teknolojik yenilikler, geleneksel ve toplumsal pratiklere üstün gelmektedir. Bu yeniliklerin güçlenerek artmaya devam etmesi ise teknolojik olanın geleneksel olan her şeye karşı üstünlüğünü korumasını sağlamaktadır (Debord, 1996: 140).

Yüz yüze iletişim gibi geleneksel olan iletişim dışında bulunan diğer tüm iletişim araçları elektronikleşmiştir. Öte yandan, internetin kitlesel kullanıma açılmış olması da ona kitle iletişim aracı olarak yeni bir nitelik kazandırmıştır. Eskiden kitle iletişim araçları, bilgisayar sistemleri ve telekomünikasyon birbirinden ayrı iken günümüzde iç içe geçmiş ve yeni bir sistem oluşturmuştur. Ortaya çıkan bu yeni sistemin en önemli özelliğini görüntü, ses ve metni tek bir yapı üzerinden iletebilmesi oluşturmaktadır. İnternetin sahip olduğu bu görsel, işitsel ve yazılı bilgi sağlama potansiyeli diğer iletişim araçlarının sunmakta olduğu birçok imkanı tek elde toplayarak kapsamlı bir medya halini almasını sağlamakta ve geniş kitleler tarafından tercih edilmesini

kolaylaştırmaktadır (Kırcelli, 2011: 12). İnternetin bireylere sınırsız ve çeşitli imkanlar sunuyor olması ve bireylerin de bu imkanlardan faydalanmak istemeleri ise interneti günlük yaşamlarının bir parçası haline getirmelerine sebep olmaktadır. Bu durumun bir sonucu olarak da internet tabanlı birçok farklı uygulama ve sosyal medya platformu geliştirilmekte ve bireylerin kullanımına sunulmaktadır (Aktan ve Çakmak, 2015: 160). İnternet tabanlı uygulamalar veya platformlar ile gündelik yaşam içerisindeki fiziksel olarak gerçekleştirilen; iletişim, alışveriş, eğitim vb. eylemler online olarak yapılabilmektedir. Bireylerin internete bağlanabilen bir aygıta sahip olmaları bu eylemleri gerçekleştirebilmeleri için yeterli olmaktadır.

İnternet teknolojisi ile iletişimin niteliklerinde ve toplumsal pratiklerde meydana gelen dönüşüm, bireysel ve toplumsal yaşamın yeniden yorumlanmasına sebep olmuştur. Bu yeniden yorumlamalar kapitalist anlayış ile benzer bir şekilde, bireyleri sömürme ve kontrol altında tutma ideallerinin güçlenmesine zemin hazırlamıştır. Kapitalizmin içerisinde taşıdığı toplumu metalaştırma eğilimi, internet sayesinde genişlemiş ve iletişim süreci, hiçbir kitle iletişim aracının ortaya çıkışından sonra olmadığı kadar endüstrileşmiştir (Arık, 2018: 130).

İnternet, dünyaya bağlanabilmenin bir aracı olmuştur. Doğal olarak, bilgisayar ve akıllı telefon satışlarında artışlar meydana gelmiştir. Bu sayede elektronik ticaret de aktif olarak işleyen bir sektör haline almıştır (Castells, 2008b: 335-336). Aynı zamanda, Ben Agger'da (2004: 1-10) bireylerin internet sayesinde dünyaya bağlanabildiklerini ve özel olarak interneti karşılıklı iletişime geçmek için kullanarak, birbirlerine ulaşabildiklerini vurgulamaktadır. Hatta gelişen bu internet teknolojisi ile bireylerin işlerini, eğitimlerini ve ailelerini bile internete taşıdıklarından söz etmektedir. Agger internetin gelişiminin etkilerinin toplumu bir bütün olarak etkilemesinin yanı sıra bireyleri de tek tek etkilemiş olduğundan ve bu sürecin yeni tip bir birey yarattığından da söz etmektedir. Bu yeni tip bireyleri, internetin oluşturduğu sanal ortamlarda oluşturulan sanal benlikler olarak ifade etmektedir.

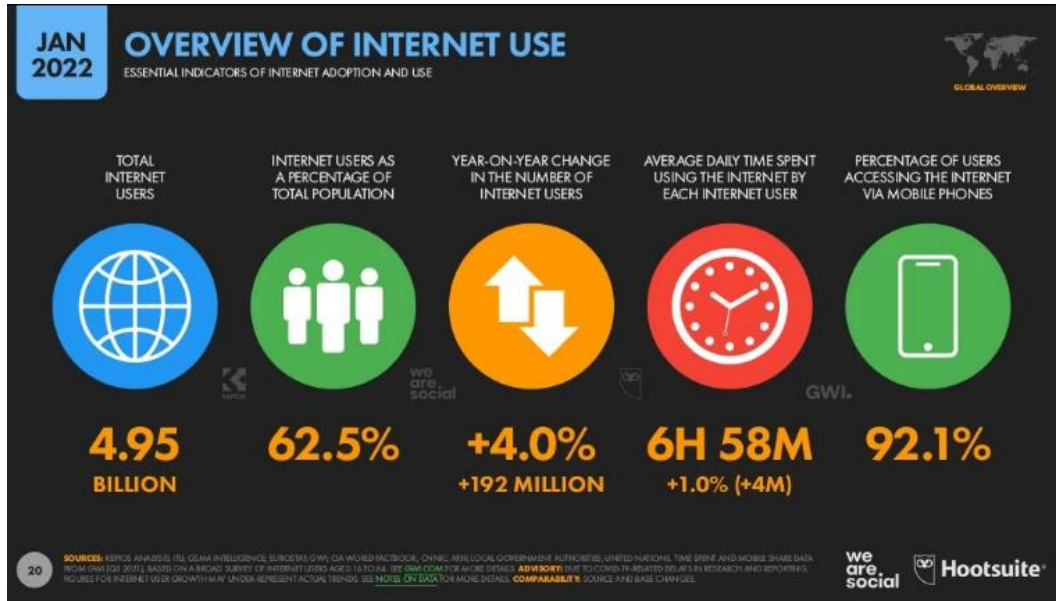
Genel olarak internetin; bilgi edinmek, iletişim kurmak, eğlenceli vakit geçirmek ve ticari faaliyetlerde bulunmak olmak üzere dört amaç doğrultusunda kullanıldığı belirtilmektedir. Bireylerin bilgi edinmelerini kolaylaştırmak amacıyla, bilgi kaynaklarının tümü tek bir çatı altında toplanmakta ve arama motorlarının kullanımı ile istenilen bilgiye kısa sürede ulaşma imkan sağlanmaktadır. Yazılı, sözlü ve görüntülü iletişim seçeneklerinin varlığı bireylerin birbirleri ile iletişim kurabilmelerini hızlı ve pratik hale getirmektedir. Bunun yanı sıra internet, geliştirilmiş online oyunların diğer kullanıcılar ile birlikte oynanabilmesine, Youtube benzeri platformlar aracılığıyla da video, dizi ya da film izlenebilmesine olanak sağlayarak bireylerin eğlenceli vakit geçirmelerine imkan vermektedir. Şirketler zaman, mekan ya da sınır tanımadan satış yapabilmekte, internete bağlanabilen her bireyin sahip olduğu telefona ya da kişisel bilgisayarına bildirimler veya reklamlar göndererek kapitalist düzendeki yerini sağlamlaştırmaya devam etmektedir (Ateş, 2016: 36). Hatta internet ticareti ve tüketimi o denli arttırmış ve hızlandırmıştır

ki; ürünler tüketicilere sunulana dek güncelliğini yitirebilmektedir. Bu süreç içerisinde doğru bilgiye hızlı erişim ve bilginin etkin kullanımı önem arz etmektedir (Ünal, 2015: 7). Bunu gerçekleştirebilen sektörler, satışlarından yüksek kar elde edebilmektedir. Gerçek şu ki; bilgi günümüzde her alanda öneme sahip bulunmaktadır. Kapitalist sistemin çarklarından birini artık bilgi oluşturmaktadır.

Her geçen gün yeni bir elektronik alet ile bağlanılabilen internet Eirik Lokke'ye göre (2018: 30) 'Nesnelerin İnterneti' fenomeniyle ifade edilmektedir. Bu fenomene göre yakın gelecekte, üretilen bütün nesneleri internete bağlamak mümkün olabilecektir. Bunun için ise Lokke; internet üzerinde kendine ait bir kimliğin, bir vericinin ve hareket, ses, tat ya da koku gibi şeyleri kayıt edebilen bir algılayıcının yeterli olacağını savunmaktadır. Dolayısıyla bu ve benzeri ifadeler; internetin gelecekte daha kapsamlı halde kullanılacağına ve yaşamımızın ayrılmaz bir parçası olmaya devam edeceğine dair öngörülerin varlığı şeklinde yorumlanabilmektedir.

İnternet, ortaya çıktığı ilk zamanlarda hızlı veri akışını ve iletişimin pratik yolunu sağlamakta olan bir ortam olarak tanımlanmış olsa da günümüzde bu tanımından farklı olarak sosyal medya kavramı ile tanımlanmaktadır (Arık, 2018: 131). Teknolojik kavramlara atfedilen anlamlar zamanla değişebilmekte, yeniden anlamlandırılabilirler çünkü bireyler teknolojik yeniliklerden sadece pasif olarak etkilenmemekte aynı zamanda bu yeniliklerin kullanımını ve etkisini de aktif olarak şekillendirmektedir (Bargh ve McKenna, 2004: 586). Bireylerin interneti genel olarak sosyal medya hesaplarına erişebilmek amacıyla kullanıyor olması bu duruma sebep olarak gösterilebilmektedir.

Şekil 1: Küresel Ölçekte İnternet Kullanımı



Kaynak: <https://datareportal.com/reports/digital-2022-global-overview-report>

We Are Social web sitesinin yayınlamış olduđu 2022 Ocak ayı verilerine g re, 7 milyar 924 milyon olan d nya n fusunun 4.95 milyarı diğ er bir deyiřle %62,5'i internet kullanmaktadır. İnternet kullanıcı sayısında son bir yılda %4 oranında bir artış s z konusu olduđu ve kullanıcı sayısının 192 milyon artış g sterdiğı g r lmektedir. Bunun yanı sıra g nl k internet kullanımı ortalama olarak 6 saat 58 dakikayı bulmaktadır. İnternete mobil cihazlar ile baėlananlar ise toplam n fusun %92,6'sını oluřturmaktadır. T rkiye'de ise n fusun %82'sinin internet kullanmakta olduđu ve g nl k internet kullanım s resinin ise d nya geneli ortalamasının 1 saat 2 dakika  zerinde, 8 saat olduđu raporlanmaktadır. İnternete eriřim saėlanabilen ara ların artması, kullanımı da artırmaktadır. Bu durum mobil cihaz  retim ve t ketiminin hem nedeni hem de sonucu olarak g r lebilmektedir. McLuhan ve Powers'a g re (2001: 140) de kullanıcılar dijital  aėda hem  retici hem de t ketici konumunda bulunmaktadır.

Sonuc olarak internet; t m d nya da etkilerini hissettiren teknolojik bir yeniliktir. Hızlı bir řekilde i inde bulunduėumuz  aėın doėal bir par ası, bireylerin bir uzvu haline gelmiřtir. Doėal olarak, keřfinden  nce internetsiz yařamak ne kadar m mk n olsa da g n m zde bir o kadar imkansız olduđu s ylenilmektedir (Bargh ve McKenna, 2004: 574; McLuhan ve Powers, 2001: 123). G ndelik yařam i erisindeki eylemlerin bir oėu internet kullanılarak ya da internet sayesinde ger ekleřtirilmektedir. Bunun yanı sıra, bireylerin birbirleri ve d nya ile ilgili algılamalarını, iletiřim řekillerini ve d ř nme bi imlerini deėiřtirmekte, bireylerin davranıř bi imlerinde deėiřimlere sebep olabilmektedir. Aynı zamanda internetin bireyler  zerindeki etkileri arařtırılmıř ve baėımlılık potansiyeli tařıdığı, ger ek hayatta yalnızlařmaya sebep olabildiğı, bireyleri siber zorbalıėa ve maėduriyete a ık hale getirdiğı, siyasi kutuplařmalar yaratabildiğı gibi  eřitli bulgulara rastlanmıřtır (Gosling ve Mason, 2015: 880).

2.2. Sosyal Medya

Sosyal medya; Web 2.0 teknolojisi ile birlikte hayatımıza girmiř ve g n m zde  ok sık kullanılmakta olan bir kavram haline gelmiřtir (řener ve Y cel, 2020: 268). Sosyal medya kavramının, genel kabul g rm ř bir tanımı bulunmamaktadır fakat sosyal medya kavramı ile sosyal i erikli web siteleri kastedilmektedir. Aynı zamanda sosyal medyayı; kullanıcılarının bilgilerini, ilgi alanlarını ve aktivitelerini internet aracılığı ile paylařtıkları, sosyal platformlar olarak tanımlamak da m mk nd r (Aktan ve  akmak, 2015: 160). Bařka bir  alıřmada dar anlamı ile sosyal medya, internetin bireyleri birbirleri ile sanal ortamlarda buluřturduėu web tabanlı hizmetlerden biri olarak tanımlanmaktadır. Geniř anlamıyla ise sınırları belirlenmiř olan bir sistem i erisinde, bireylerin a ık ya da yarı a ık kiřisel profil oluřturmalarına izin veren, i erik paylařımları yapan kiřilerin listesini diğ erlerine g sterebilen web tabanlı hizmetler olarak ifade edilmektedir. Sosyal medya; yazılı, s zl  ve g rsel  eřitliliğı ile kullanıcıları i in enformasyon saėlayan, bireylerin kendi d ř nce ve bilgilerini paylařmalarına imkan tanıyan aynı zamanda

karşılıklı etkileşimi içeren çevrimiçi araçlar ile web sitelerini tanımlamak için ortak kullanılmakta olan bir terimdir (Esen, 2018: 5).

Temelde sosyal medyanın dört genel özelliğinden bahsedilmektedir. İlk olarak; sosyal medya kullanıcılarının, profilleri aracılığıyla kendilerini dijital platformlarda ifade etmelerine imkan vermektedir. İkinci olarak; diğer kullanıcılar ile olan ilişkilerini yani takip veya arkadaş listelerini ortaya koymalarını sağlamaktadır. Üçüncü olarak; kullanıcıların, gerçek dünyada var olan ilişkilerini, sanal ortamda da sürdürmelerine ve yönetmelerine olanak vermektedir. Son olarak ise; kullanıcıların, ilgi alanlarını, bulundukları mekanları ve aktivitelerini temel alarak yeni ilişkilerin oluşması için bir ortam oluşturmaktadır (Zengin vd., 2015: 114-115).

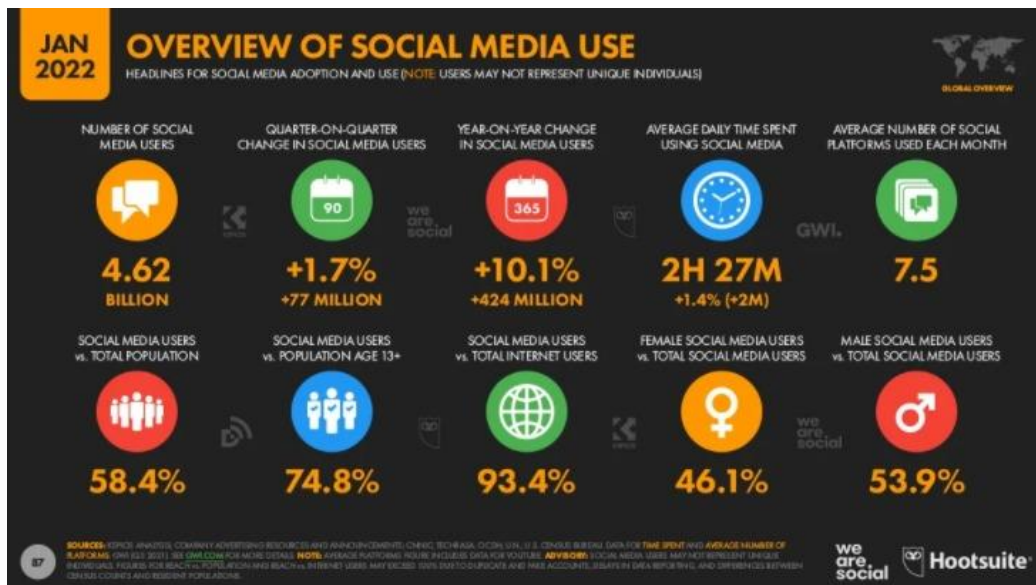
Sosyal medya platformları günümüzde oldukça sık kullanılmalarıyla birlikte günlük bir ihtiyaç halini almışlardır. Farklı kültürden ya da toplumdan birçok kullanıcıyı bünyesinde barındırabilen, zaman ve mekan kavramının öneminin tamamen kaybolduğu bu platformlarda, kullanıcılara istedikleri kadar özgür ve sınırlanmadan davranış sergileme olanağı sunulmaktadır. Aynı zamanda sosyal medya platformları, bireylere gerçek hayatta ihtiyaç duydukları fakat tecrübe edemedikleri beğenilme, takdir edilme ve sosyal çevre edinme gibi unsurları olduğundan daha kolay bir şekilde verebilmektedir (Örs, 2018: 8). Kullanıcılar, sosyal medya üzerinden tanıştıkları kişiler ile yeni bir etkileşim kurabildikleri gibi gerçek hayatlarından tanıdıkları kişiler ile de etkileşimlerini sürdürmek amacıyla sosyal medya platformlarını kullanmaktadır (Çoban, 2019: 38). Öte yandan; kullanıcılar bu platformlar üzerinden iletişim kurmaya başladıkları bireyler ile yeterince güven sağlandıktan sonra geleneksel iletişim yöntemi olan yüz yüze iletişime geçip, onları gerçek hayatlarına dahil edebilmektedir (Bargh ve McKenna, 2004: 586-587). Ayrıca kullanıcılarına kendilerine özel olan gruplar oluşturabilmeleri hususunda kolaylıklar sağlamak ve ortak bir amaç edinmelerine olanak vermektedir (Hekimoğlu, 2019: 9).

Bir başka açıdan bakıldığında sosyal medya platformlarının bu kadar yoğun kullanılması, maliyetinin düşük olması ile açıklanabilmektedir. Kullanıcılar düşük maliyetler ile haberleşme, bilgi edinme vb. birçok eylem gerçekleştirebilmektedir. Sosyal medyanın etkisi oldukça hızlı ve güçlüdür; insanlar cevap aradıkları bir sorun veya politik, ekonomik ya da milli konularda savundukları herhangi bir fikir için kısa bir zaman içerisinde ortak bir başlık ve amaç altında toplanarak gruplar oluşturabilmektedir. Hatta etkilerini birbirleri aracılığıyla, ülke çapına ve uluslararası alana kadar yayabilmektedir (Sepetci, 2017: 23-24).

İnternet ve sosyal medya teknolojileri yeni sosyalleşme mekanları yaratmakta, özgürleştirici ve dönüştürücü etkisinin yanı sıra kullanıcılarının; inanç, kültür, aile ve cinsellik gibi algılarını yenileyerek mahremiyet olgusunda önemli değişim ve dönüşümler oluşturmaktadır. İnternet tabanlı platformların yaygınlaşması toplumlarda; daha kolay gözlemlenebilirlik, kontrol ve manipüle edilebilirlik gibi sorunları meydana getirmektedir. Mark Poster interneti; Jeremy Bentham'ın

Sosyal medya ve internetin sağlamakta olduđu kolaylıkların yanı sıra, dođal olarak bir de veri güvenliđi ve veri mahremiyeti kavramları gündeme gelmeye başlamıştır. Bireylerin kendileri ile ilişkilendirilebilen her türlü bilgi, kişisel veri olarak kabul edilmektedir (Kartal, 2018: 3). Bireyler birbirlerine gönderdikleri ya da paylaştıkları fotoğraf, video ya da mesajların kendi belirledikleri ölçüde, gizlilik içerisinde ulaşmasını istemektedirler fakat bunun ne kadar mümkün olduđu konusunda fikir sahibi olamamakta ve çoğunlukla endişe duymaktadırlar. Dolayısıyla veri mahremiyetinin ve güvenliğinin, özellikle birçok kişi tarafından erişilebilir olan ve gözetlenmenin çok sıkı olduđu sosyal medya platformlarında, tam anlamı ile sağlanamadığı düşünülmektedir (Yılmaz vd., 2016: 27). Buna rağmen günümüzde bireylerin görünür olma istekleri daha baskın gelmekte ve sosyal medya platformlarının kullanıcı sayısı sürekli olarak artmaktadır. We Are Social verileri incelenerek dünya çapında sosyal medya kullanıcılarının ne kadar artmış olduđu görülebilmektedir.

Şekil 2: Küresel Ölçekte Sosyal Medya Kullanımı



Kaynak: <https://datareportal.com/reports/digital-2022-global-overview-report>

Tablodaki verilerden de anlaşılacağı üzere; Dünya nüfusunun %58,4'ü diğer bir deyişle 4.62 milyar kişi sosyal medya kullanmaktadır. Türkiye'de ise nüfusun %80,8'i sosyal medya kullanımı gerçekleştirmektedir. Sosyal medyada geçirilen günlük sürenin dünya ortalaması 2 saat 27 dakika, Türkiye'de ise bu süre 2 saat 59 dakikadır. Özellikle salgın ile birlikte bireyler sosyal medyada daha fazla vakit geçirmeye başlamıştır. Karantina uygulamaları sebebi ile yerine getiremedikleri rutin faaliyetlerini internet ve sosyal medya üzerinden yerine getirmeye çalışmışlardır. Bireylerin amaçlarına yönelik birçok sosyal medya platformu bulunabildiğinden günlük rutin faaliyetlerinin tümüyle aksamamış, aksine yeni bir ortama taşınmış olduğu ifade edilebilmektedir.

Çeşitli özelliklere sahip olan birçok sosyal medya platformu bulunmasına rağmen kullanım yoğunluğuna bakıldığında; Facebook, Instagram, Twitter, Youtube ve Tiktok listede ilk beş sırayı almış bulunan platformlar olarak göze çarpmaktadır. Bu platformların ortak özelliğini yazılı, sözlü ve görsel içeriklere sahip paylaşımlar yapılabilmesi ve genel olarak sosyalleşmek amacıyla kullanılmaları oluşturmaktadır (Öztürk, 2015: 21).

2.2.1. Facebook

Facebook, kullanıcılarının birbirleri ile iletişim kurmasını, bunun yanı sıra bilgi, fotoğraf, video gibi paylaşımlar yapabilmesini sağlayan ve dünyada en fazla kullanıcı kitlesine sahip olan sosyal medya platformudur. 4 Şubat 2004 tarihinde, Harvard öğrencisi Mark Zuckerberg tarafından kurulmuştur (Esen, 2018: 17-18). İlk olarak sadece Harvard Üniversitesi e-posta adresine sahip olan öğrencilerin kullanabileceği, özel bir web sitesi olarak açılmış fakat kullanıcısı olmak isteyen sayısındaki artış sebebiyle özel bir site olmaktan çıkmıştır (Zengin vd., 2015: 115).

Günümüzde 2 milyar 11 milyon kullanıcısı bulunmaktadır ve artış hızı düşmüş olsa da sürekli olarak kullanıcı sayısı artmaktadır. Ücretsiz bir platform olması ve uygulamanın birçok (112) dile çevrilmiş olması kullanıcı sayısındaki sürekli artışın sebeplerini oluşturmaktadır. Aslında bireylerin Facebook'u tercih etmesinin ve kullanmasının birçok sebebi bulunmaktadır. Bu sebepler; bireylerin gözetleme, iletişim kurma, fikir edinme, kendi fikirlerini dile getirme istekleri veya fotoğraf, video paylaşımında buluma, oyun oynama, alışveriş yapma ve etkinlik düzenleme vb. eylemleri şeklinde sıralanabilmektedir (Göçmen, 2018: 73-74; Sepetci, 2017: 38).

Kullanıcılarının paylaşım yapmalarına ve arkadaşlık ilişkileri kurmalarına imkan vermesinin yanı sıra; birbirlerinin paylaşımlarını beğenmelerini, yorum yapmalarını ve kendi profillerinde yeniden paylaşabilmelerini de sağlamaktadır. Ayrıca kullanıcıların kendi aralarında ortak gruplar oluşturarak mesajlaşabilmelerine olanak vermektedir. Aynı zamanda; kullanıcıların kendilerine ait oluşturdukları profillerinin gizliliğini ayarlayabilme ya da rahatsız olduğu kişileri engelleyebilme yetkileri bulunmaktadır (Çoban, 2019: 46-47).

Facebook üzerine yapılan arařtırmalar, herhangi bir konu hakkında yapılmıř olan paylařımların altına bazı kullanıcılar tarafından yazılan yorumlar ve deęerlendirmelerin dięer kullanıcıların fikirlerini büyük ölçüde etkilemekte olduęunu ya da deęişimine yol açabildięini göstermektedir (řener ve Yücel, 2020: 268). Aslında bu durum özellikle alışveriş odaklı platformlarda ürünü satın alma ya da almama kararlarını deęiřtirmede daha belirgin olsa da ideolojik konularda, halihazırda var olan fikirlerin güçlenmesi ya da deęiřimi üzerinde özellikle Facebook gibi platformlar etkili olabilmektedir.

Saęladıęı bunca olanak ve kolaylıęına raęmen, gizlilik konusunda yeterli olmayıřı Facebook'un zayıf yönünü oluřturmaktadır. Kullanıcı profillerinde bireylerin; cinsiyeti, inancı, siyasi görüřü, iliřki durumu, hobileri, ırkı, yařadıęı yer, mesleęi gibi birçok kiřisel bilgisi yer almaktadır. Dięer kullanıcılar profillere tıkladıkları ilk anda bu bilgilerin sahibi olabilmektedir. Kullanıcılar bilgilerini istedikleri kitleye açabiliyor olsalar da Facebook bu bilgileri gerekli gördüęü her yerde kullanma hakkına sahip bulunmaktadır. Paylařılan her řey önce Facebook ile ve daha sonra arkadař olunan dięer kullanıcılar ile paylařılmaktadır (Karagülle, 2015: 92). Sonuç olarak Facebook, kullanıcılarına sunmakta olduęu sosyalleřmenin, eęlencenin ve dięer bütün olanakların bedeli olarak kendi kiřisel bilgilerini paylařmalarını talep etmektedir (Kalaman, 2016: 25).

2.2.2. Instagram

Bir dięer sosyal medya platformu olan Instagram; kullanıcılarının fotoğraf paylařımı yapabilmelerine ve paylařılan fotoęrafları beęenip yorum yapabilmelerine olanak saęlamaktadır. Ayrıca kullanıcılar anlık olarak fotoęraf, yazı ya da video řeklinde durum paylařımında bulunabilmekte, dięer kullanıcılar ile birbirini takip edebilmekte ve mesajlařabilmektedir. 2010 yılında, Kevin Systrom ve Mike Krieger tarafından kurulmuř olan bu platformun asıl amacını fotoęrafların daha profesyonel görünmesini saęlamak oluřturmaktadır. Bu nedenle bünyesinde birçok fotoęraf filtresini barındırmaktadır. Görseellięi ön plana çıkarmıř olması bireylerin ilgisini çekmesine ve kullanıcı sayısının sürekli řekilde artmasına sebep olmaktadır. Dięer fotoęraf paylařım aęlarından farkı ise sadece mobil cihazlarda (ISO ve Android) kullanabiliyor olmasından kaynaklanmaktadır (Esen, 2018: 29-30). Ücretsiz bir sosyal medya platformu olan Instagram'ın yaklařık olarak 1 milyar 48 milyon kiři kullanıcısı bulunmakta ve günde 80 milyonun üzerinde yeni fotoęraf paylařılmaktadır (Sepetci, 2017: 90).

2012 yılında bu platform Facebook tarafından satın alınmıřtır (Olçay, 2018: 95). Bu satıř 1 dolar karřılıęında yapılmıřtır. Instagram aylık 800 milyonun üzerinde aktif kullanıcıya sahiptir ve Facebook'tan sonra en fazla kullanıcıya sahip olan sosyal medya platformu olarak gündeme gelmektedir. Kullanıcıların oluřturdukları profillerinde takipçi sayısının, gönderilerindeki yorum ve beęeni sayısının fazla olması hem kullanıcının daha büyük bir kitleye hitap edebilmesine imkan

vermekte hem de markalar tarafından keşfedilerek pazarlama stratejileri içerisinde yer almasına olanak sağlamaktadır. Aynı zamanda, ünlülerin kendi günlük yaşamlarına dair paylaşımlarda bulunmaları da Instagram'ın kullanıcı sayısındaki sürekli artışa sebep olan faktörlerden birisi olarak görülmektedir (Çoban, 2019: 45).

Instagram, diğer birçok sosyal medya platformu gibi karşılıklı gözetimin kolaylaşmasına fırsat sağlamaktadır. Kullanıcılar profillerini herkese açabildikleri gibi sadece arkadaşlarına gözükecek şekilde de gizleyebilmektedir (Örs, 2018: 20). Fakat yine aynı senaryo bu platform için de geçerlidir. Instagram gerekli gördüğü takdirde kullanıcı bilgilerini paylaşma hakkına sahip bulunmaktadır. Bunun yanı sıra, kullanıcılar profillerini arkadaşı olmayan diğer kullanıcılara karşı gizlemelerine rağmen; Postegro, Lili gibi yasal olmayan versiyonları bulunan bazı uygulamalar tarafından profillerindeki tüm gönderilerine ulaşılabilir. Bu durum gizlilik konusunda Instagram'ın yeterli güvenliğe sahip olmadığını göstermektedir.

Kullanıcıların her hallerini anlık olarak paylaşabilmeleri durumu mahremiyet konusunda tartışmalara sebep olmaktadır. Özellikle Instagram'ın, kamusal alan ve özel alanın birbirine karışmış olmasından ötürü mahremiyeti zedelediğine dair tartışmalar görülmektedir. Örnek olarak; doğum yapmış olan annelerin emzirme görüntülerini, hamile olan anne adaylarının çıplak karınlarını paylaşmaları ya da çiftlerin yatak odalarından kareler paylaşmaları özel ve kamusal olan üzerine birçok tartışmanın meydana gelmesine sebep olmaktadır. Bu tarz görüntülerin özel ile kamusal olan arasındaki ayrımı belirsizleştirmeye başladığı savunulmaktadır. Dolayısıyla mahremiyet kavramının anlamsal içeriği de sürekli bir dönüşüme uğramaktadır (Göçmen, 2018: 80).

2.2.3. Twitter

Twitter, dünya genelinde popülerliğe sahip olan bir diğer sosyal medya platformudur. 2006 yılında yazılımcı olan Jack Dorsey tarafından kurulmuştur. İlk ortaya çıktığı zamanlarda kullanıcıların o anda neler yaptığını yönelik paylaşımlar yapmalarını hedeflemişken bu durum giderek değişime uğramış ve gündemde neler olduğuna odaklanan bir hal almıştır (Sarıyar, 2019: 64).

Popüler bir sosyal medya platformu olmasının en önemli sebeplerini ücretsiz bir platform oluşu ve kullanımının basitliği oluşturmaktadır. Toplam 280 karakterden oluşan iletiler, fotoğraf ve videolar paylaşma ve diğer kullanıcılar ile mesajlaşabilme olanağı sunmaktadır (Kaplan, 2017: 26). Ayrıca, Instagram ve Facebook'da olduğu gibi canlı yayın yapma ve anlık gönderi paylaşma özellikleri de bulunmaktadır. Günümüz itibari ile Twitter'ın 436 milyonun üzerinde aktif kullanıcısı bulunmakta ve günde ortalama 100 bin civarında ileti paylaşılmaktadır (Çoban, 2019: 43; Sepetci, 2017: 39).

Oluşturulan iletilere ‘tweet’ adı verilmekte ve bu tweetler kullanıcının takipçileri tarafından görüntülenebilmektedir. Kullanıcı profilini herkese açık yapabileceği gibi sadece takipçilerinin görebileceği şekilde de ayarlayabilmektedir (Budak, 2016: 78). Twitter kendi misyonunu; herkese fikir ve bilgileri, anında ve hiçbir engel olmaksızın oluşturup paylaşma yetkisi vermek olarak tanımlamaktadır. Ayrıca Twitter, kullanıcılar tarafından haber kaynağı olarak kullanılmaya da uygun bir platformdur ve bu platformda haberler anlık olarak yayınlanmaktadır (Kaplan, 2017: 26).

Diğer sosyal medya platformlarından Twitter’ı ayıran en önemli özelliğinin ‘hashtag’ diğer adıyla ‘etiket’ olduğu söylenebilmektedir. Kullanıcılar diyez işaretini (#) belirledikleri bir konu başlığının önüne getirerek bir etiket oluşturmaktadırlar. Dolayısıyla kullanıcılar tarafından bu etiket kullanarak yapılan her paylaşım, aynı konu hakkında farklı fikirlerden oluşan bir paylaşım kategorisi ortaya çıkarmaktadır. Aynı etiket ile arama yapan bir kullanıcı anında bu kategoriye ulaşabilmektedir. Bu durum örgütlenmeleri de kolaylaştırmakta ve bireylerin kolektif bir güç oluşturarak gündeme getirmek istedikleri konuda seslerinin daha gür çıkmasına fayda sağlamaktadır (Sarıyar, 2019: 66). Örneğin, günümüzde genellikle atama isteyen meslek grupları bir araya gelerek ve belirledikleri bir konu etiketi kullanarak atama sorunlarını gündemde tutmaya çalışmaktadır. Öte yandan; bir bölgede deprem vb. doğal afetler meydana geldiğinde haberlere düşmesi zaman alırken, Twitter’da anında girilip bakıldığında ‘#deprem’, ‘#sel’, ‘#yangın’ gibi etiketlerin oluşturulmuş olduğu görülmekte ve yapılan paylaşımlardan depremin merkez üssünün neresi olduğu ya da yıkım yaratıp yaratmadığı, sel ve yangının nerelerde meydana gelmiş olduğu gibi bilgilere kolaylıkla ulaşılabilir.

Kullanıcılara profillerini gizleme ya da herkese açma yetkisinin verilmiş olması mahremiyet denetimi açısından alternatif sunulduğunu ifade etmektedir. Fakat kullanıcılar anlık ve oldukça kişisel iletiler paylaşabilmektedir. Bu iletilerin başkaları tarafından kolaylıkla tekrar paylaşılması ya da Twitter’ın kamusal niteliğinin oluşu gibi sebeplerle, kullanıcıların mahremiyet beklentisinde olmaları gerekçesiz görülmektedir (Göçmen, 2018: 84).

2.2.4. Youtube

Günümüzde çeşitli sosyal medya platformları bulunmakta fakat sadece birkaç tanesi geniş kitlelere hitap edebilmektedir. Bu platformlardan bir diğerinin de 2 milyarın üzerinde kullanıcıya sahip olan Youtube adlı video platformu olduğu söylenebilmektedir. 2005 yılında Steve Chen, Chad Hurley ve Jawed Karim tarafından ‘Dijital Video Deponuz (Your Digital Video Repository)’ sloganı ile kurulmuş olan Youtube, internet dünyasına yeni bir platform olarak giriş yapmış bulunmaktadır. İlerleyen yıllarda ise bu sloganın ‘Kendini Yayınla (Broadcast Yourself)’ şeklinde değiştirildiği görülmektedir. Üye olmayan kullanıcılar sadece video izleyebilirken üye olan kullanıcılar ise video içeriği yayınlama hakkına da sahip olmaktadır. İzleyiciler videolara yorum yapabilmekte, beğenip beğenmediklerini işaretleyebilmekte ve daha sonra izlemek için

kaydedebilmektedir. Sunduğu çeşitli imkanlar bakımından Youtube dünya üzerinde en çok kullanılan platformlar arasında yer almakta ve hatta birçok kullanıcı yayınladıkları videoların izlenme oranları sayesinde gelir elde edebilmektedir (Çoban, 2019: 48-53).

Düzenli şekilde video yükleyerek, Youtube üzerinden yayın yapıp gelir elde etmekte olan kullanıcıların sayısının artması ile ‘Youtuber’ kavramı ortaya çıkmıştır. Günümüzde neredeyse bir meslek ismi olarak anılmaya başlanmış olan bu kavram genç kuşağın beklentilerini ve arzularını şekillendirmekte büyük rol oynamaktadır. Özellikle örnek aldıkları ünlü Youtube yayıncılarının genç kuşak üzerindeki etkisi göz ardı edilemeyecek düzeydedir.

2.2.5. Diğer Sosyal Medya Ağları

Bireylerin iş hayatlarını ve profesyonel oldukları alanları temel alarak oluşturdukları profiller aracılığıyla diğer kullanıcılar ile etkileşim kurmalarına olanak sağlayan ‘Linkedin’ bir diğer sosyal medya platformudur. Bu platform Reid Hoffman tarafından 2002 yılında oluşturulmuştur. Kullanıcılarının iş hayatları ve profesyonel alanları ile ilgili bilgi alışverişi yapmaları amaçlanmaktadır. Bunun yanı sıra bünyesinde aktif iş ilanları da bulunmakta ve kullanıcıların, oluşturdukları profilleri ile bu ilanlara başvurmalarına olanak sağlamaktadır. Aynı şekilde şirketlerin ya da işverenlerin de aradıkları özelliklere ve donanıma sahip bireyleri bu profiller aracılığıyla bulabilmelerini kolaylaştırmaktadır. Herkesin kullanımına açık olması sebebiyle dünyanın her yerinden kullanıcıları bulunmaktadır (Sepetci, 2017: 46-47).

Günümüzde, her geçen gün yeni bir sosyal medya platformuyla karşılaşabilmek mümkündür. Bu platformların çeşitliliğine ve farklarına dayanarak yapılmış bir sınıflandırma bulunmaktadır. Bu sınıflandırmaya göre; Facebook benzeri işlevleri olan ve kullanıcılarının bilgi paylaşımını kolaylaştıran Myspace, Windowslive, Google vb. platformlar sosyal ağlar olarak adlandırılmaktadır. Blogger, Wordpress vb. platformlar ise bloglar; Twitter ve Tumblr gibi biraz daha kişiselleşmiş profillere sahip olan bloglar ise mikrobloglar olarak sınıflandırılmaktadır. Fotoğraf paylaşım platformları olarak; günümüzde en çok kullanılan sosyal medya platformu olan Instagram, ardından Gravator ve Picasa gibi platformlar sıralanmaktadır (Şener ve Yücel, 2020: 267). Farklı amaçlara hizmet eden çeşitli platformların varlığı, kullanıcıların birden fazla sanal profillerinin oluşmasına sebep olmaktadır.

2.3. Dijital Çağda Gerçeklik Olgusu, Sanal Kimlik Ve İkincil Yaşam (Second Life)

İnternet teknolojisi ile meydana gelen değişim ve dönüşüm sadece zaman ve mekan kavramları ile sınırlı kalmamaktadır. Gerçeklik olgusu da alışlagelmiş olan anlamını yitirmekte, yeni bir anlama bürünmektedir. Kavram olarak gerçeklik; var olan, hakiki olan her şey olarak tanımlanmaktadır. Diğer bir deyişle, bir şeyin gerçekliğinin olması için o şeyin gerçekte var olması gerekmektedir. Günümüzde, gerçeklik her ne kadar varlığını sürdürmekte olsa da temelden bir

değişikliğe uğramış bulunmakta ve ilkesel olarak yok olma yolunda ilerlemektedir. Doğal olarak, ilkesinden mahrum kalmış olan bir gerçekliğin varlığı da eskisi ile kıyaslanamayacak şekilde gücünü kaybetmektedir (Sarıyar, 2019: 40).

Fiziksel dünyada çoğu zaman beş duyu organıyla da algılanabilen gerçeklik, internet teknolojisinin sağladığı güç ile sanal ortama taşınmakta ve sanal gerçekliği oluşturmaktadır. Bir diğer deyişle fiziksel olmayan bir gerçeklik, sanal ortamda yapay olarak üretilmeye çalışılmaktadır. Bu durum ‘simülasyon’ olarak tabir edilmektedir. Simülasyon Kuramını geliştiren Jean Baudrillard’a göre (Baudrillard, 2011: 11-13); gerçeklikten yoksun bir şekilde ve modeller aracılığıyla bir gerçeğin üretilmesine hiper-gerçeklik ya da simülasyon denilmektedir. Simülasyon ile birlikte hayal gücü önemini yitirmekte ve gerçek olanın sentetik bir şekilde üretimi söz konusu olmaktadır. Bunun doğal bir sonucu olarak da gerçeğin sonsuz sayıda yeniden ve yeniden üretilmesi mümkün hale gelmektedir.

Simülasyon, aslında gerçek olan ile sahte olan arasındaki farkı ortadan kaldıracılabilmeyi amaçlamaktadır. Bu sebeple, özellikle teknolojinin de sürekli gelişimi sayesinde simülasyonlar artık daha güçlü gerçeklik algısı yaratabilecek şekillerde oluşturulmaktadır. Bu sayede bireyler gerçek olan ve olmayan arasında fark görememekte ya da görmek istememekte dolayısıyla simülasyon ve gerçek birbirine karışmaktadır. Oluşan bu durum da simülakrları ortaya çıkarmaktadır (Dalaylı, 2018: 13-14). Ortaya çıkan bu simülakrlar, direkt olarak gerçeklik ilkesine saldırmaktadır. Aslında orada hiç var olmayan bir şeyi var olarak göstermekle birlikte bireylerin gerçeklik algıları ile oynanmaktadır. Gerçeği bir simülakr şeklinde sunanlar ise sahtekar olarak görülmektedir (Baudrillard, 2011: 42-54). İnternet teknolojisi günümüzdeki kadar gelişme göstermediği dönemlerde, daha çok minyatür vb. teknikler ile simülakrlar yaratılmaya çalışılmış olsa da günümüzde sanal ortamların gelişimi simülakrları yaratmayı kolaylaştırmaktadır.

Sanal kavramı, kelime olarak ‘gerçek olmayan’ anlamına gelmektedir. Gerçek olmayan bir gerçekliğin yaratılmaya çalışılması da sanal gerçeklik kavramını ortaya çıkarmaktadır (Bostan, 2007: 27). Günümüzde gücü elinde bulunduranın fiziksel gerçeklik değil, sanal gerçeklik olduğu düşünülmektedir. Aynı zamanda teknolojik gelişmeler sayesinde gün geçtikçe sanal olan, gerçek olan her şeyin içerisine nüfuz etmektedir (Baudrillard, 2002; 40-41). Örneğin; 2020 yılında ortaya çıkan yeni tip korona virüsün (Covid 19) yarattığı küresel salgından dolayı yüz yüze eğitime ara verilmiş olması ve öğrencilerin okullarına gidemeyerek sınıf ortamı içerisinde ders işleyememesi, çevrimiçi olarak derslerine devam etmelerine sebep olmaktadır. İnternet tabanlı platformlar kullanılarak öğretmen ve öğrencileri çevrimiçi şekilde, çoklu görüntülü konuşma yaparak ders işlemektedir. Bu durum doğal olarak sanal sınıfların oluşumuna yol açmış bulunmaktadır. Diğer bir deyişle, fiziksel açıdan gerçek olan sınıf kavramı, sanal olarak yeniden üretilmektedir. Aynı şekilde iş toplantıları, tez savunmaları vb. eylemler yine çevrimiçi olarak yapılmakta ve toplantı salonu olmayan, sunum kürsüsü bulunmayan bir gerçeklikte devam etmektedir. Sınavların birçoğu ise

çevrimiçi olarak yapılmakta ve gerçek bir öğretmen gözetiminden yoksun olan öğrenciler, kameralarını açmaları istense dahi, rahatlıkla kopya çekerek sınavlarından yüksek puanlar alabilmektedir. Bu örneklerden de anlaşılabilir olduğu üzere; sanal gerçeklik, tam anlamıyla bir fiziksel gerçeklik ortamı yaratmakta başarılı olamamaktadır.

Fiziksel bir gerçeklik ortamı yaratmakta başarılı olamayan sanal gerçeklik, teknolojik olarak geliştirilmeye çalışılmakta ve gerçekliğinin artırılması hedeflenmektedir. Örneğin; sanal gerçeklik gözlükleri ya da eldivenleri gibi birçok ürün gerçekliği artırması amacıyla kullanılmaktadır. Sanal gerçeklik gözlükleri sayesinde birey evinde ya da ofisinde, yani oturduğu yerde dünyanın herhangi bir yerini gezebilmekte ya da sanal gerçeklikte oluşturduğu bir karakteri bulunuyorsa (özellikle oyunlarda) onun gözleriyle görüyormuş gibi bir algıya kapılabilmektedir. Bu durumda zaman ve mekan içerisindeki fiziksel gerçeklik değişmesi ve beden yerinden kımıldamasa bile algı yolculuk etmektedir. Bu durum, mekanın ve zamanın birey üzerindeki sınırlamalarının işlevini yitirmesine sebep olmaktadır (Medin, 2018: 15).

İnternetin gelişimi ve ortaya çıkan platformlar sayesinde, gerçek hayatta fiziksel olarak yalnız olmak artık sosyal olarak yalnız olmakla aynı anlamı taşımamaktadır. Bireyler gerçek hayatlarında tek bir arkadaşına sahip olmasalar bile internet tabanlı platformlarda birçok arkadaşına sahip olabilmektedir. Hatta aynı zaman dilimi içerisinde, aynı sanal gerçeklik platformlarında bir araya gelen kullanıcıların bir sanal kamusal alan oluşturduğu da söylenebilmektedir. Öte yandan sadece iki kişinin birbiri ile kendilerine has bilgilerini paylaşmasıyla sanal bir özel alan da oluşturulabilmektedir (Akkaş, 2015: 48-49). Kısacası sanal gerçeklik bireylere kolaylıkla kamusal veya özel alan oluşturabilme imkanı vermektedir.

Baudrillard (2011: 45-46), sanal gerçeklik kullanılarak bireylerin aldıkları kararlardan, amaçlarından ve hatta inançlarından vazgeçirilebileceklerini; asıl istenilen fikirlerin ise kolay bir şekilde empoze edilebileceğini ifade etmektedir. O, bu durumu iktidar üzerinden ele alarak açıklamaktadır. Sanal gerçeklik gündelik yaşamın içerisine oldukça güçlü bir şekilde nüfuz etmeye devam etmektedir. Teknolojik gelişmeler, sanal kimlik oluşturmak da dahil her an her şeyi mümkün kılabilir.

Kimlik, bireyin içinde yaşadığı toplumda ya da tüm dünyada kendini başkalarına karşı tanımlamayı amaçlaması ile ortaya çıkan anlamlar bütünü olarak ifade edilmektedir (Sevinç, 2019: 16). Diğer bir deyişle; bireyin kim olduğunu, kişisel niteliklerini ve sahip olduğu yeteneklerini, davranış biçimlerini vb. kapsayan bir kavram olduğu söylenebilmektedir (Seyrek; 2018: 98). Bireyler her zaman başkaları tarafından tanınmak ve bilinmek için kendilerini tanımlama ihtiyacı duymaktadırlar. Teknolojik gelişmelerin henüz hız kazanmamış olduğu modernleşme öncesi dönemlerde bireyler kim olduklarını ait oldukları topluluklar ile ifade etmekten, teknolojik gelişmelerin de payının bulunduğu, modernleşme sonrası meydana gelen toplumsal bağlardaki

öz lmeler ve k reselle menin toplumsal baėların  z lmesine sebep olarak yarattıėı g vensizlik ortamı kimliėin modern d nemde bir kriz haline gelmesine sebep olmuştur. Kim olunduėunun, mensup olunan toplulukların, bireyin kendisini nasıl ve ne ile tanımladıėının yani kimliėin  nemi giderek artış g stermiştir. Dolayısıyla bireyler kendilerini nasıl tanımlayacakları konusunda s rekli bir arayış ierisinde bulunmaktadır. Kimliėi  killendiren fakt rlerden birisini de bireyin ba kaları tarafından nasıl tanımlandıėı oluşturmaktadır (Sevin, 2012: 28-31).

Bireyler kimliklerini in a ettiklerinde, sadece kendileri tarafından iselleştirilmi  olması kimliklerini anlamlı hale getirmemektedir. Bunun yanı sıra toplum tarafından da tanınması ve iselleştirilmesi gerekmektedir. Bireyin kimlik in a s recindeki anlamlandırmaları, bu iselleştirme etrafında  rg tlediėi zaman tam anlamı ile kimlik halini almaktadır. Kimlik in a s recinin ise   farklı  ekilde meydana geldiėi ifade edilmektedir. Toplumların sahip oldukları egemen kurumların kendi egemenliklerini g lendirmek, geni letmek ve ussallaştırmak amacıyla in a ettikleri kimlik ‘me rulaştırıcı kimlik’ olarak tanımlanmaktadır. Egemen olanın mantıksal bakımdan deėersiz g rd ė , etiketlediėi konumlarda ya da ko ullarda bulunan ki iler tarafından kar ıt olarak in a edilen kimlik ise ‘direni  kimliėi’ olarak adlandırılmaktadır. Son olarak, toplumdaki bireyler tarafından, iine doėdukları toplumun onlara sunduėu k lt rel yapıdaki konumlarını yeniden d zenlemek ve toplumsal yapıyı deėi tirmek amacıyla in a edilen kimlik ise ‘proje kimliėi’ olarak ifade edilmektedir (Castells, 2008c: 13-15). Kimlikler, amaları doėrultusunda e itli  ekillerde in a edilebilmektedir.

G n m zde yeni bir kimlik olu turmak iin kullanılan sanal ortamlarda fiziksellik bulunmamaktadır. Bunun doėal bir sonucu olarak da ba kaları ile ileti ime geildiėi sırada stres, gerilme vb. duygular ya anmamakta ya da daha az ya anmakta ve k t  bir ilk izlenim yaratma korkusu ortadan kalkmı  olmaktadır. Bu sayede kullanıcılar kendilerini istedikleri  ekilde ve kendi  rettikleri farklı kimlikler  zerinden tanımlayabilmektedirler. Bireyler genellikle ba kalarına kar ı arzularını, fikirlerini, yaratıcılıklarını, d   kırıklıklarını ya da endi eleri gibi kendilerine has olanı ba kalarına sergileyebilmek amacıyla sanal ortamları kullanmaktadırlar. Bu durumda, sanal ortamlar bir nevi izlenim yaratma araları olarak da tabir edilebilmektedir ( zdemir, 2006: 61-62).

Genellikle sosyal medya platformları  zerinde doldurulan profiller aracılıėıyla bir sanal kimlik olu turularak, benlik in a etme eylemi g r lmektedir. Sanal kimlik; gerek kimlikle birebir aynı olabildiėi gibi, bireylerin gerek hayatlarında sahip olmadıkları  zellikleri taşıyarak tamamen farklı  ekilde de olu turulabilmektedir. Teknoloji, sanal ortamlarda yeniden  retilen kimliklere melez formlar eklenebilmesine olanak vermektedir (Sucu, 2014: 116; G ktepe, 2013: 13-14). Bunun yanı sıra bireyler, tamamen sahte bir kimlik yerine gerek hayatta saklamaları m mk n olmayan kendileri ile ilgili gereklerin bir kısmını gizleyerek de bir kimlik in a edebilmektedir. Bu konular  zerinde yapılan ara tırmalar  zellikle sosyal aėların, kimlikleri ve benlik sunumlarını biimlendirmede etkilerinin olduėunu kanıtlamı  bulunmaktadır. Sanal kimlikler; gerek hayattaki

kimliklerden daha karmaşık bir yapıya sahip bulunabilmekte ve aynı zamanda daha geniş kitlelere sunulabilmektedirler (Tosun ve Akıncı, 2016: 29-30).

Günümüz toplumunda, kimlik inşa sürecinde olduğu gibi görünürlük konusunda da bir değişim yaşanmaktadır. Eskiden görünür olmaktan ve mahremiyetlerinin ifşa edilmesinden rahatsız olan bireyler artık görünür olmamaktan rahatsız olmaktadır. Günlük yaşamın bir parçası haline almış olan sosyal medya platformları sayesinde bireyler kendilerini diğerlerine kolay bir şekilde sunmakta ve diğerleri hakkında da kolayca fikir edinebilmektedir. Bunun sonucunda kendi sanal kimliklerini bu etkileşimler sayesinde istedikleri şekilde biçimlendirebilmektedirler. Sanal ortamlar diğerlerine karşı sorumlulukların, yüz yüze ve gerçek hayatta olduğundan daha az olması durumu ile bireylerin benlik sunumlarını kolaylaştırmaktadır (Kardaş, 2017: 43). Kendilerini günlük yaşam içerisinde kısıtlanmış, sıkışmış ya da yalnız hisseden bireyler, oluşturdukları sanal kimlikleri ile gerçek hayattan uzaklaşmayı amaçlamaktadır (Kırcelli, 2011: 33). Yaşam normalde fiziksel eylemler üzerinden tecrübe edilmekteyken; sanal benlikler yaşamı ve dünyayı ekran üzerinden tecrübe etmektedirler (Agger, 2004: 180).

Sanal ortamda etkileşim ve iletişim bedensiz bir şekilde gerçekleştirilmektedir. Bu bedensiz varoluş, bireylerin istemedikleri fiziksel özelliklerini rahatlıkla gizleyebilmesine olanak sağlamaktadır. Sağladığı anonimlik, bireylerin kendilerine yeni bir yaşam öyküsü yaratmalarına da imkan vermektedir (Çingay, 2015: 110-111). Bunun sebepleri arasında; bedensel eksiklikler veya farklılıklar gösterilebileceği gibi bireylerin toplum tarafından desteklenmeyeceklerini bildikleri seçimlerinden oluşan farklılıklar ve bireyin ailesine atfedilmiş olan, kendisini bir gruba kabul ettirmesi sürecinde zorluk yaratabilecek tanımlamalar ve etiketlemeler de gösterilebilmektedir. Dolayısıyla birey kedisini bu gibi gerçeklerden ve tanımlamalardan soyutlayacak olan bir kimliğe sahip olmak istemektedir (Sevinç, 2019: 62).

Gerçek yaşamda semboller kimliği şekillendiren faktörlerdendir. Belli toplulukların bıraktığı bıyık şekli, bağlanılan fular şekli, selam verme şekli vb. bu sembollere örnek olarak gösterilebilmektedir. Başkaları bu semboller ile karşılaştığında bireyin kimliği hakkında bilgi edinmiş olmakta; bu kişinin hangi topluluğun üyesi, hangi bölgeden geldiği ya da hangi ideolojinin takipçisi olduğu gibi konularda yorumda bulunabilmektedir (Sevinç, 2012: 58). Benzer şekilde, semboller sanal kimliği de şekillendirmektedir. Fakat gerçek yaşamda duyu organları ile algılanabilen somut semboller söz konusu iken, sanal ortamda bireyin hangi sayfaları takip ettiği, hangi gönderileri beğendiği, paylaşımlarını hangi ideolojik çerçeve içerisinde yaptığı vb. sanal faaliyetleri değerlendirilerek bireyin kimliği hakkında yorum yapılabilir.

Yapılan çalışmalara göre genellikle bireyler, sanal ortamlarda oluşturdukları sanal kimlikler aracılığıyla ve anonimliğe de güvenerek kendilerini oldukları kişi değil de olmak istedikleri kişi şeklinde sunmaktadırlar. Bireylerin kendilerini diğerlerine sunuşunu ele alan Erving Goffman

(Goffman, 2018: 108-112), başkalarına karşı yapılan benlik sunumu sürecinde ortaya çıkan ‘vitrin/set’ ve ‘art bölge/sahne arkası’ kavramlarından söz etmektedir. Bireyler kendilerini olmak istedikleri kişi gibi sunarken kusursuz bir vitrin görüntüsü yaratmakta ya da bir setteki kadar dikkatli ve hoş görünümlü olmaktadır fakat vitrinlerin ardında bir art bölge, setlerin ardında bir sahne arkası her zaman bulunmaktadır. Bireylerin gerçek kişilikleri ve kimlikleri buralarda saklı durmaktadır. Örneğin; günlük yaşamında hayvanlara eziyet eden birisi sanal ortamda oluşturduğu profilinde, yani vitrine bakıldığında, hayvanları çok seviyormuş gibi beğeni ve paylaşımlarda bulunarak kendisini hayvan sever bir birey olarak sergileyebilmekte ya da aslında destekçisi olmadığı bir ideolojinin veya projenin sembollerini içeren paylaşımlar yapabilmektedir. Bu noktada, bireyler hakkında fikir edinirken, sanal sembollerin somut semboller kadar belirgin ve güvenilir olamadığı açıktır.

Sosyal medya platformlarında oluşturulan profiller aracılığıyla bireyler, diğer kullanıcıların onayını alabilmek ve kendisini onlara kabul ettirebilmek amacıyla seçici paylaşımlarda bulunabilmektedirler (İşman vd., 2016: 618). Kendilerine dair bilgileri paylaşarak diğerlerine nasıl biri olduklarını, nelerden hoşlandıklarını ya da nerelere gittiklerini göstermeye çalışmaktadırlar. Yaptıkları bu paylaşımları ise oluşturdukları sanal kimliklerini inandırıcılığını yitirmemesi açısından bir çerçeveye oturarak gerçekleştirmektedirler. Bunun sebebi ise kendilerini gözetleyenlerin var olduğunu bilmeleri ve aynı zamanda oluşturdukları sanal kimliklerinin görünür olmasını istemeleridir (Akmeşe ve Deniz, 2017: 28). Oluşturulan profillerin yani sanal kimlikleri ile var olan bireylerin, sanal platformlarda bir araya gelmesi ile birlikte sanal topluluklar meydana gelmektedir. Genel olarak ortak amaç ya da ortak ideolojiye sahip olan bireyler tarafından oluşturulan ortak gruplara dahil olunmaktadır. Bu topluluklara dahil olan bireyler, özellikle de gerçek yaşamda toplumdan dışlanmakta ise sanal kimlikleri sayesinde istemedikleri özelliklerini gizleyerek bir gruba dahil olma ve ait olma duygularını yaşamaktadırlar (Sağtaş, 2013: 43).

David Lyon ile karşılıklı olarak fikirlerini beyan ettikleri bir çalışmada Zygmunt Bauman’ a göre; gündelik yaşam çevrimiçi ve çevrimdışı olmak üzere iki ayrı evrene bölünmüş bulunmaktadır ve bunun geri dönüşü de mümkün gözükmemektedir (Bauman ve Lyon, 2013: 51). Bireyler oluşturdukları sanal kimlikleri ile aslında ikinci bir yaşama dahil olmaktadır. Bu durum ‘Second Life’ kavramı ile ifade edilmektedir. Second Life; Linden Lab isimli bir şirket tarafından, 2003 yılında, üyelerine ikincil bir yaşam olanağı vaat etmeleri sonucunda bir proje olarak ortaya çıkmış bulunmaktadır. Oluşturdukları bu sanal gerçeklik dünyasının ise sadece kullanıcılarının hayalleri ile sınırlı olduğunu, nasıl yaşamayı ya da neler yapmayı tercih ediyorlarsa yapabileceklerini belirtmişlerdir. Zamanla belli bir kitleye özel olan kullanımı da genele yayılmıştır (Sağtaş, 2013: 49).

Sanal gerçeklik platformlarında kullanıcılar ‘avatar’ adı verilen sanal karakter kullanarak kendilerini fiziksel olarak ifade edebilmekte ve farklı bölgelerde ya da zaman diliminde

bulunmalarına rağmen, belirledikleri ortak platformlarda birlikte olma ve sosyalleşme deneyimini gerçekleştirebilmektedirler. Bu platformlar kullanıcılarına, kendilerine ait sanal karakterleri aracılığıyla hem diğer kullanıcılarla hem de nesnelerle ilişki kurma imkanı sunmaktadır (Özonur, 2013: 25-26). Klasik olarak, 2009 yılında ABD yapımı olan “Avatar” adlı film ve günümüzde en yaygın haliyle ikincil yaşam çerçevesinde düzenlenmiş oyun uygulaması olarak “PUBG” adlı oyun örnek gösterilebilmektedir. Bu oyunda kullanıcılar kendilerine bir sanal karakter seçmekte ve fiziksel görünüşlerini istedikleri gibi değiştirebilmektedir. Amaç diğer kullanıcılar ile bir takım olarak ya da bireysel olarak oyunda en son hayatta kalan olabilmektir. Günümüzde sıklıkla sözü edilmeye başlanan ve artırılmış gerçeklik cihazları kullanılarak dahil olunan ‘Metaverse (meta evren)’ bir diğer örnek olarak gösterilebilir. Bireyler bu uygulamalar aracılığıyla günlük yaşamlarında gerçekleştiremeyecekleri iş kurmak, cinayet işlemek, tarla vb. satın alarak çiftlik kurmak gibi bazı aktiviteleri gerçekleştirebilme imkanı bulmaktadırlar. Öte yandan sosyalleşmekte ve gerçek yaşamlarında sosyal bir çevresi bulunmasa dahi bu platformda bir gruba dahil olabilmektedirler.

Sanal gerçeklik içeren platformlarda üye olmadan uygulama kullanımı gerçekleştirilememektedir. Üye olma işleminde ise kişiye özel soruların doldurulması ile birlikte bir profil oluşturularak kişisel bilgilerin paylaşımı istenmektedir. Kullanıcılar bu durumda gerçek yaşamlarına ait bilgilerini paylaşabildikleri gibi tercihlerine göre gerçek yaşamlarından tamamen farklı özellikler içeren bilgiler paylaşarak da sanal bir karakter oluşturabilmektedirler. Aynı zamanda bazı platformlarda kullanıcıların sistem üzerine kaydettikleri boy, kilo, yaş, cinsiyet gibi fiziksel bilgileri kullanılarak kullanıcıların sanal karakterleri oluşturulabilmektedir (Sucu, 2014: 211). Kullanıcılar istekleri doğrultusunda karakterlerine insan görünümünün yanı sıra hayvan görünümü de verebilmektedirler. Öte yandan kullanıcılar bu platformlarda istedikleri şekilde binalar inşa ederek, sınırsız sayıda ve türü fark etmeksizin araçlar tasarlayıp yeni mekanları ziyaret ederek ya da diğer kullanıcılar ile tanışarak gerçek hayatta edinilmesi daha sınırlı ve düşük olasılıklı olan deneyimler edinebilmektedir. Üyelik türlerine göre de toprak satın alabilmekte ve mağazalar kurarak satışlar yapabilmektedirler. Eylemleri tamamen kendi istekleri doğrultusunda şekillenmektedir. Dolayısı ile cazip gelmektedir (Bezir, 2012: 14-15).

Second Life projesi doğrultusunda sanal ortamda her ırktan, toplumdaki ve bölgeden kullanıcıların varlığı ile çok kültürlü bir yapı oluşturulabildiği görülmektedir (Canbek, 2009: 20-23). Bunun yanı sıra, yapılan bir çalışmada; bireylerin gerçek hayattaki mutluluk ve başarıları ile Second Life’da olan mutluluk ve başarıları arasında pozitif yönde bir ilişki olduğu saptanmış olduğu ifade edilmektedir. Kullanıcıların Second Life’ta vakit geçirmelerinin, onlar için terapi özelliği taşımakta olduğu ifade edilmektedir (Uzun ve Aydın, 2011: 270).

2.4. Dijitalleşme ve Dijital Çağda Kültür

Kavram olarak sayısallaştırma (digitization) ve dijitalleşme (digitalization) genel olarak literatürde birbirinin yerine kullanılmaktadır. Fakat aralarında analitik bir ayrım bulunmaktadır. Sayısallaştırma; özellikle bilgisayar aracılığıyla, elde bulunan verileri dijitalleştirmek amacıyla yapılan bir işlem olarak gerçekleşmektedir. Kısacası bir dijitalleştirme süreci ya da eylemi olarak tanımlanabilmektedir. Dijital olmayan veriler 1 ve 0 sembolleri ile temsil edilerek dijitalleştirilmektedir. Bu sebeple hem sembolik hem de somut bir boyuta sahip olan bir süreç olarak görülmektedir. Bu işlem neredeyse her tür veriye uygulanabilmektedir (Brennen ve Kreiss, 2016: 1-2). Başka bir açıdan bakıldığında; dijital teknoloji, kelimelere ya da harflere sayılar kadar ihtiyaç duymamaktadır. Sayılar dijital teknolojinin var olması ve gelişmesinde, özellikle verileri kodlama ve dijitalleştirmede önemli bir rol oynamaktadır (McLuhan, 1994: 80).

Dijitalleştirme süreci sonucunda uzun süre kullanılabilecek olan dijital kopyalar üretilmiş olmakta ve internet aracılığı ile erişime açılmaktadır. Bu dijital kopyalar bilgilerin daha kolay ve kalıcı şekilde depolanabilmesine ve indeks edilebilmesine olanak sağlamaktadır. Herhangi bir zaman ve mekan sınırı olmadan erişim gerçekleştirilebilen bu dijital kaynaklar bilginin gelecek nesillere daha kolay iletilebilmesine imkan vermektedir. Küresel ölçekte paylaşılabilen ve kurumların ya da bireylerin rahatlıkla erişebildiği kaynakların bulunması durumu internetin etkili bir araştırma aracı olarak kullanımını yaygınlaştırmış bulunmaktadır (Acun, 2008: 13-4). Dijital teknolojinin sunmakta olduğu bu tarz yenilikler ve fırsatlar ise yeni taleplerin oluşmasına yol açmaktadır. Talepler etrafında durmaksızın yeniden şekillenen dijitalleştirme eylemi ise dijital dönüşümün gerçekleşmesine sebep olmaktadır. Dijitalleşmek olarak anılan bu dönüşümün de 'dijital çağı' ortaya çıkarmış olduğu öne sürülmektedir (Gobble, 2018: 56-57).

Birçok değişime ve dönüşüme yol açan dijital çağın birkaç özelliğinin bulunduğu ifade edilmektedir. Bu özellikler "... zaman, mekan, seçim, karışıklık, boyut, kimlik, sosyallik, gerçek, açıklık, amaç..." olarak belirtilmektedir (Olca, 2018: 92). Bu özelliklerden yola çıkarak dijital çağı; zaman ve mekandaki sınırlılıkların kalkmış olduğu, seçeneklerin çeşitlendiği, gündelik yaşamdaki fiziksel boyuta bir sanal boyutun eklenmiş olduğu, kimlik inşasının ve sosyalleşmenin yeniden şekillendiği, gerçek kavramının değişime uğradığı ve bir şeylere açıklık getirmenin kolaylaşarak, yeni amaçların oluşturulabildiği ya da var olan amaçlar için daha kolay mücadele edilebildiği bir çağ şeklinde de açıklamak mümkün olmaktadır.

Dijitalleşme, gündelik yaşamı kolaylaştıran birçok yenilik ve kolaylık sağlamış bulunmaktadır. Fakat ortaya çıkardığı bu olumlu etkilerin yanı sıra olumsuz etkilerinin olduğu da bilinmektedir. Özellikle bilgisayar ve internet bağımlılığı ortaya çıkmakta, bazı ülkelerde bu bağımlılık ile mücadele için merkezler bile kurulmaktadır. Bu teknolojik bağımlılık, davranışsal bağımlılık türeri içerisine dahil olmuş bulunmaktadır. Aynı zamanda kendi içerisinde; sanal kumar,

online oyun, sosyal medya, porno ve siber zorbalık gibi alt başlıklara ayrılmakta ve giderek çeşitlenmektedir (Olçay, 2018: 91). Bir başka deyişle dijitalleşmenin yeni nesil hastalıkları ve sorunları da beraberinde getirmiş olduğu söylenebilmektedir. Bağımlılık dışında, uzun süre bilgisayar oyunu oynayan bireyler de fiziksel aktiviteleri ihmal ederek hareketsizlikten kaynaklanan hastalıklara yakalanabilmektedir. Psikolojik olarak telefonlarından ya da internetten yoksun kalma korkusu geliştirmiş olan bireyler bulunmaktadır. Uzun süre ekran başında oturan bireylerde obezite hastası olma riskinin artmış olduğu kaydedilmektedir (İşliyen, 2019: 408-409). Yapılan çalışmalar sonucunda internet ile tanışma yaşının giderek düştüğü gözlemlenmektedir. Güncel çalışmalara göre çocuklar 7 yaşından önce internet ile tanışmakta ve dijital araçların kullanımını öğrenmektedirler. İnternete erişim ve kullanım düzeyinin ise 9 ile 16 yaş aralığında yaklaşık olarak %95 oranında olduğu bildirilmektedir (Bacıoğlu, 2022: 29). Ebeveynlerin çalışma hayatı içerisinde olması, toplumdaki bireyselleşme, yaşanan salgın ile eve kapanma gibi faktörler çocuklar üzerindeki sosyal kontrolün azalmasına sebep olmaktadır. Dolayısı ile çocuklar fiziksel olarak sosyalleşemedikleri için ve teknolojik yeniliklere duydukları merak ile birlikte hızla dijital yaşama atılmakta ve yanlış kullanımları sonucu mağdur olma riski taşımaktadırlar.

Teknolojik gelişmeler bireylerin mahremiyetlerinin sıklıkla ihlal edilmesine yol açmakta ve mahremiyet haklarını korumalarında güçlükler sebep olmaktadır. Özellikle ebeveyn kontrolünün tam olarak sağlanamadığı durumlarda çocukların mağdur edilme olasılıkları yükselmektedir. Aynı zamanda, geliştirilen kötü amaçlı yazılımlar ile kişisel verilere rahatlıkla ulaşılabilme ve bu durum bireylerin özel yaşamları, sağlık kayıtları ya da finansal bilgilerinin güvenliği hakkında kaygılarını doğal olarak arttırmaktadır (Eroğlu, 2018: 132; Kaplan, 2017: 4). Teknolojik gelişmeler ile birlikte mahrem alanın da giderek daralması sorunu kamusal alanın genişlemesine yol açmaktadır. Kamusal alanın genişlemesi ise olumsuz koşulları ortaya çıkarmaktadır (Berkup, 2015: 6). Bugün akla gelen her şey, yapılan her aktivite ya da gidilen her mekan internet üzerinden paylaşılabilmektedir. Sosyal platformlar bu paylaşımlar için imkan sağlayan en popüler paylaşım araçları olarak görülmektedir. Sosyal platformlarda paylaşılan fotoğraflar ya da atılan mesajlar silindiğinde dahi web siteleri, internet servis sağlayıcıları ve arama motorları tarafından arşivlenmektedir. Dijital çağda her bilgi kaydedilmekte ve yok olmamaktadır. Kısacası günümüzdeki dijital iletişim oldukça kalıcı durumdadır, mutlaka iz bırakmaktadır (Zengin vd., 2015: 116-117). İnternet kullanıcıları, tarayıcılar üzerinden herhangi bir web sunucusuna bağlandıkları anda çevrimiçi olarak takip edilme sürecine dahil olmaktadır ve çoğu kullanıcı bundan haberdar değildir. Bu çevrimiçi takiplerin amacı kullanıcının profilini oluşturmak ve kişisel ilgi alanlarını saptayabilmektir. İnternet üzerinden yapılan her alışveriş, okunan her makale ya da haber, takip edilen yayınlar ve siyasi, kültürel vb. alanlarda her tıklayış kullanıcıların arkalarında dijital izler bırakmalarına sebep olmaktadır. Bu izleri sınıflandırarak enformasyon sağlayan şirketler, elde ettikleri verileri diğer şirketlere pazarlayabilmektedir (Arık, 2018: 159). Örneğin birçok uygulama ve internet tarayıcıları ücretsiz olarak kullanıcıların hizmetine sunulmaktadır

çünkü asıl ürün tam anlamıyla kullanıcılardır. Aslında kullanıcıların kişisel verileri, bu ücretsiz olarak sunulan uygulamaların bedelidir (Lokke, 2018: 71). Çok basit bir örnek verecek olursak; herhangi bir arama motoru aracılığı ile bir ayakkabı markasından ürün bakıldığında çevrimiçi olarak yapılan her tıklama ve hangi modellere bakıldığı kaydedilmektedir. Elde edilen bu veriler ise kullanıcıların sosyal medya hesapları var ise (instagram, facebook vb.) bu mecralara pazarlanmakta ve hesaba girildiğinde bakılan markanın modellerinin görüldüğü reklamlar veya indirimler ile karşılaşılmaktadır. Bu reklamlardan faydalanarak yapılacak herhangi bir alışveriş doğrultusunda verileri depolayan ve pazarlayan şirketler amacına ulaşmış olmaktadır. Dolayısıyla kullanıcıların ardında bıraktıkları dijital izler, dijital çağda büyük öneme sahiptir.

Dijital çağ; bilgi çağı olarak da ifade edilmekte olup, toplumların geçmişten günümüze kadar sahip oldukları bilgi birikimlerinin teknoloji aracılığıyla çoğaltılması ve paylaşılması ile karakterize edilmiş olan bir çağ olarak anılmaktadır. Dijital çağda yaşanmakta olan gelişmeler ile birlikte gündelik yaşam pratiklerinde, eğitimde, ekonomide ve hatta toplumların kültürlerinde bile farklılaşmalar meydana gelmiş bulunmaktadır (Sarıyar, 2019: 20; İşliyen, 2019: 408). Tıpkı alfabenin bulunmasıyla birlikte yazılı kültüre geçilmesinin bir devrim olarak kabul edilmesi gibi internet teknolojisi ve onun getirileri aracılığıyla yaşanan değişimler de bir devrim olarak kabul edilmektedir. İnternet teknolojisi yazılı, görsel ve işitsel kültürü aynı sistem içerisinde bütünleştirmesiyle birlikte iletişimin karakterini tümüyle değişime uğratmış bulunmaktadır. İletişimin de kültürü doğrudan doğruya şekillendirebilen bir yapıya sahip olmasından dolayı toplumlarda bir kültürel değişime sebebiyet vermesi kaçınılmaz olmuştur (Castells, 2008a: 440).

Geleneksel kültürün değişime uğrayarak bir dijital kültürün ortaya çıkmış olduğu savunulmaktadır. Kültür geleneksel anlamda; bireylerin bir araya gelerek oluşturdukları toplumdaki norm ve değerleri, ortak davranış kalıplarını, yaşam pratiklerini, maddi ve manevi unsurlarını içeren bir bütün olarak tanımlanabilmektedir. Toplumlarda üretilen bu kültür kalıpları ve bilgi birikimleri nesilden nesile aktararak devamı sağlanmaktadır. Küreselleşme ve teknolojik gelişmeler ile birlikte kültürel temaslar kolaylaşmış ve artmış bulunmakta, tamamen farklı bir kültüre sahip olan bir toplumun kültürel yapısı diğer toplumlara da kolaylıkla yayılabilmektedir (Fidan, 2004: 7-8; Alkan, 2019: 75). İnternet ile birlikte birey, zaman ve mekan arasındaki sınırların aşılmış olmasıyla yeniden üretilen kültür ‘siber kültür’ olarak da adlandırılmaktadır. Aynı zamanda iletişimdeki değişim ve dönüşümler ile birlikte yeniden üretilen kültürün ‘medyatik kültür’ şeklinde tanımlandığı da görülmektedir (Güzel, 2016: 86-87). Teknolojinin gelişmesi, internetin ortaya çıkması ve dijitalleşmenin hayatın bir parçası haline gelmesi, alışlagelmiş geleneksel kültürel davranış kalıplarını, yaşam pratiklerini ve toplumsal değerleri de dönüşüme uğratmış bulunmaktadır. Bireylerin iletişim kurarken artık geleneksel selamlaşma yöntemlerini kullanmak yerine emojiyi kullanmaları örnek olarak gösterilebilmektedir. Dijital çağda kelimelerden daha etkili oldukları düşünülen emoji, bir nevi evrensel dil olarak da kabul

edilebilir. K lt r n oluřumunda, geliřiminde ve tařınmasında en az kelimeler kadar etkili konuma gelmiřlerdir ( nci vd., 2017: 495; řener ve Atar, 2017: 196-198).

Dijital  aęda, bilginin daha hızlı  retimi ve yayılması ile aktarımı kolaylařmıř olan yeni bir k lt r hızla oluřmakta ve yayılmaktadır. Buna  rnek olarak g n m zde sosyal medyalardaki ‘challenge’ řeklinde ifade edilen meydan okumalar da g sterilebilmektedir. Birden fazla kiřinin bir eylemi ger ekleřtirmeye bařlaması ve bunu yayınlaması ile  ok hızlı bir řekilde yeni bir k lt r  retilmekte, tařınmakta ve etkisi zamanla yine  ok hızlı bir řekilde azalmaktadır. Bunun ardından aynı s re  durmaksızın tekrarlanmaktadır. Bařka bir deyiřle g n m zde k lt r  ę t c l ę  diye de tabir edebileceęimiz bir olgu s z konusudur. Bařka bir a ıdan; bireylerin bu hızla deęiřen olguya ayak uydurmaya  alıřırken yaptıkları paylařımlar vb. de onların maęduriyet yařama olasılıklarına temel atmaktadır.

2.5. Su 

D nyanın her yerinde insanlar bir araya gelerek toplumları oluřurmaktadır. Bir arada ve d zen i erisinde yařayabilmek i in ise ortak deęerler temelinde kural ve normlara ihtiya  duyulmaktadır.   nk  toplumsal d zen, bunu bozabilecek her t rl  eylemi yasaklayan kurallar olmadan var olamamaktadır. Bu kural ve normlar; dinsel, hukuksal, geleneksel, ahlaki vb. bir ok formda belirlenebilmektedir (G  l  ve Akbař, 2016: 28-29; Brenner, 2010: 9). Aynı zamanda bu normlar toplumdan topluma ve yařanılan  aęa g re deęiřim g sterebilmektedir. Dolayısıyla d zen i erisinde yařamak isteyen her toplum,  yelerinin bu kurallara uymasını beklemektedir fakat zaman zaman ihlaller s z konusu olabilmektedir. Ortaya  ıkan bu ihlaller ‘sapma’ olarak adlandırılmaktadır. Ger ekleřen sapkın davranıř aynı zamanda toplumda y r rl kte olan ceza yasalarına da aykırı ise ‘su ’ olarak nitelendirilmektedir (Y ksel, 2017: 4-5;   li, 2007: 1). Bařka bir deyiřle; kamusal otoritenin m dahale etmesini gerekli kılan, kanunen a ık a yasaklanmıř olan ve cezai yaptırımı bulunan eylemler su  olarak, toplumsal kural ve normlara aykırı olan fakat hukuki alanda herhangi bir yasaklılıęı ve yaptırımı bulunmayan eylemler ise sapma olarak ifade edilmektedir (Dolu, 2012: 34). Bu durumda; ger ekleřtirilen her sapkın davranıř bir su  olarak nitelendirilememektedir fakat su  teřkil eden bir ok eylem aynı zamanda sapma olarak da deęerlendirilebilmektedir (Bal, 2013b: 14).

Sapma ve su  davranıřları; toplumsal d zeni bozmaları, ortak g veni zedelemeleri ve korkuya sebebiyet vermelerinden dolayı toplumlar i in her zaman bir endiře kaynaęı olarak g r lmektedir (Smith vd., 2015: 1). Ge miřten g n m ze kadar incelendięinde; her toplumun kendi d zenini korumak ve toplumsal ahengi saęlamak i in normları, adetleri, gelenek g renekleri bulunmakta olduęu ortaya  ıkmaktadır. Bunlar toplumdan topluma deęiřkenlik g sterdięi i in bir toplumda ger ekleřtirilen herhangi bir eylem sapma olarak nitelendirilebilirken, dięer toplumda olaęan olarak karřılanabilmektedir. Aynı davranıř bařka bir toplumda ceza yasalarında yer alması

ve hukuki yaptırımı bulunması sebebi ile suç olarak nitelendirilebilmektedir. Bir dönem ceza yasalarında yer almadığı için suç olarak görülmeyen bir eyleme hukuki yaptırımlar getirildiği takdirde de suç olarak sınıflandırılması söz konusu olabilmektedir. Öte yandan hukuken yasaklanmış olduğu ve suç sayıldığı halde toplum içerisinde olağan karşılanan eylemler de bulunabilmektedir. Örneğin; ülkemizde hukuken cinayet işlemek bir suç olmasına rağmen bazı topluluklar tarafından töre cinayetleri olağan karşılanmaktadır. Başka bir örnek olarak; daha önce hayvanlara zarar vermenin ya da öldürmenin, internet aracılığı ile başkasının bilgilerini ele geçirmenin ve kullanmanın (özellikle sosyal medya platformlarında) herhangi bir hukuki yaptırımı bulunmadığı için yalnızca sapma olarak nitelendirebilmek mümkün iken, ceza yasaları içerisinde dahil edilerek hukuki yaptırımlar getirilmiş olması ile birlikte suç kabul edilmeye başlandığı görülmektedir. Bu örnekler de toplumdan topluma farklılıklar göstermektedir. Benzer şekilde hırsızlık da bazı toplumlarda suç iken bazı toplumlarda ‘beğendiğin nesneyi kendin için ödünç almak’ şeklinde olağan karşılanabilmekte, bazı toplumlarda ise eylemi gerçekleştirenin uzvunu kesme vb. şekillerde ciddi toplumsal yaptırımları bulunabilmektedir.

Sosyolojik açıdan suç olgusu değerlendirilecek olduğunda; kendiliğinden ortaya çıkmadığı, tamamıyla toplumsal ve evrensel bir olgu olduğu, toplumsal varoluşun ayrılmaz bir parçası niteliği taşıdığı görülmektedir (Das ve Nayak, 2013: 147; Yavuz, 2019: 31). Bireyin içine doğduğu toplumun kurallarının ihlali sapma ve suçun ortaya çıkmasına temel hazırlamaktadır. Suçun varlığına toplum karar vermektedir. Başka bir deyişle; toplumun var olduğu her yerde ahlaki, hukuki vb. kurallar bulunmakta ve bu kuralların bulunduğu her yerde de suç var olmaktadır (Güçlü ve Akbaş, 2016: 24-25; Dashora, 2011: 242). Çünkü bireyler; kendi doğruları ve arzuları ile toplumsal doğrular ve beklentiler uyuşmadığı takdirde bir çatışma içerisine düşmektedirler. Önce içsel olan bu çatışma, bireyin suç ya da sapma olarak nitelendirilen eylemleri gerçekleştirmesi ile birlikte dışsal bir hal almaktadır. Toplumun bireyi suçlu olarak stigmatize etmesi ise bireyin yaşadığı topluma olan bakış açısında değişimler meydana getirebilmektedir. Dolayısıyla, bireylerin kendi hür iradeleri ile kararlar verebiliyor olması ve toplumların düzenlerini korumak adına, istedikleri zaman bazı davranışları yasaklayabiliyor ya da olağanlaştırebiliyor olması durumu her zaman birey ve toplum arasında bir ayrışmaya ve çatışmaya sebebiyet verebilmektedir. Fiziki ya da fikri çatışmaların ve yasakların olduğu her yerde suç olgusuna rastlamak kaçınılmaz olarak görülmektedir.

Kavram olarak suç, her ne kadar olumsuz bir nitelik taşıyor gibi gözükse de toplum için olumlu fonksiyonları da bulunmaktadır. Gerçekleştirilen eylemin bir suç olarak nitelendirilmesi ve cezalandırılması durumu toplumda var olan normların belirginleşmesine ve istenmedik davranışların gündeme gelerek fark edilmesine imkan vermektedir. Dolayısıyla bireyler bu istenmedik davranışları gerçekleştirmekten kaçınarak, kural ve normları benimsemeye özen göstermektedir. Bunun yanı sıra; toplumsal kurallara uymayan ve suçlu davranışlarda bulunan

bireylere karşı gösterilen ortak tepkiler vb. nedeni ile suçun toplumsal dayanışmayı güçlendirdiği savunulmaktadır. Öte yandan bir toplum içerisinde işlenen suç türleri ve oranları, toplumsal yapı içerisindeki sorunların açığa çıkmasında yardımcı bir rol oynamaktadırlar (Güney, 2008: 12; Kılıç, 2007: 35). Örneğin, bir toplumda hırsızlığın fazla olması durumu ekonomik sorunların göstergesi olarak kabul edilebilirken, toplum içerisindeki azınlıkların birbirine düşmanlığı sonucu işledikleri cinayet vb. suçlar ise sosyolojik sorunların göstergesi olarak ifade edilebilmektedir. Bir bakıma, toplum değişime uğradıkça ve küresel ölçekli gelişmeler söz konusu oldukça suç işleniş şekilleri ve çeşitliliği de değişim ve dönüşüm geçirmektedir. Suç olgusu çağa ayak uydurmaktadır. Bu sebeple iyi bir suç analizi, iyi bir toplum analizi yapabilmeye yardımcı olmaktadır.

2.5.1. Suçlu Davranışın Açıklanmasına Dair Yaklaşımlar

Geçmişten günümüze suç olgusu; bireysel, psikolojik, biyolojik ve sosyolojik ana kategorileri altında birçok farklı yaklaşım ve teori ile açıklanmaya çalışılmıştır. 18. yüzyıla kadar sapkın davranışlar işkence gibi zalimce yöntemler ile engellenmeye çalışılmış, suç ve suçluların doğaüstü kabuller ile açıklanabileceğine inanılmıştır. Bilimden uzak olan bu dönemlerde aykırı davranışlar gerektiren bireylere uygulanan bu yöntemler rüşvetin yaygın olması ve kişiden kişiye göre farklı şiddetlerde uygulanabilmesi sebebi ile adil bulunmamış, suçu engellemede de tam anlamı ile etkin olamamıştır. Klasik Ekol'ün ortaya çıkması ile birlikte suç ve ceza sistemleri ilk defa sorgulanmaya başlanmıştır. Bu yaklaşıma göre bireyler suçu bilerek ve isteyerek işlemektedirler fakat işlemeyen önce bir kar-zarar hesabı yapmaktadırlar. Yaptıkları bu hesaplarda suçu işledikleri takdirde kazançlı çıkacaklar ise bireylerin suç işleyebilecekleri öngörülmektedir. Bunu engelleyebilmenin yolunun ise bireylerin işledikleri suçlar sonucunda elde ettikleri kardan daha yüksek cezalara maruz bırakılmaları olarak savunulmaktadır. Bireysel teorilerin başını çekmekte olan bu yaklaşımın önde gelen temsilcileri Cesare Beccaria ve Jeremy Bentham'dır. Ekolün temel varsayımı cezanın suça uygun olması gerekliliğine dayanmaktadır. Bireyler suçlu davranışı seçmekte ya da seçmemekte özgür ve kanunlar önünde eşit bulunmaktadır. Cezaların amacı da bireylerin toplum ve kanun için yanlış olan davranışları gerçekleştirmelerini engellemek ya da en aza indirebilmektir. Bu sebeple caydırıcılık oluşturması amaçlanan cezalarda; kesinlik, hızlılık ve şiddetlilik önem arz etmektedir (Dolu, 2009b: 91-100).

Klasik Ekol gibi bireysel teoriler suç olgusunun araştırılmasında geliştirilen ilk teoriler olmaları sebebi ile önem arz etmektedirler. Bu teoriler suçu açıklarken bireye odaklanmaktadır. Diğer bireysel teoriler ele alınacak olduğunda; Coğrafi Ekol, bireyin bulunduğu coğrafi bölgelere odaklanmaktadır. Bu yaklaşıma göre bulunan bölgedeki coğrafi şartlar, iklim çeşitliliği vb. faktörler suç oluşumunu etkilemektedir. Buna örnek olarak; güneye gidildikçe cana karşı işlenen suçların fazla olduğu, kuzey bölgelerde ise mala ilişkin suçların ve sarhoşluğun fazla olduğu ifade edilmektedir. Bilime olan inancın ve bilimsel bilginin artmaya başlaması ile 19. yüzyılda ortaya çıkmaya başlayan Pozitif Ekol ise antropolojik araştırmalardan yararlanmakta ve deneyler ile

kanıtlanabilen, metafiziksel varsayımları dikkate almayan bir yapıya sahip bulunmaktadır. Bu yaklaşımın öncüleri antropolog olan Cesar Lombroso ve öğrencileri Ernico Ferri ile Raffaele Garofalo'dur. Bireylerin fiziksel yapılarını incelenerek büyük çene ve güçlü dişler vb. kemik yapısı özelliklerine sahip olanların doğuştan suçlu oldukları savunulmaktadır. Aynı zamanda kalıtsal olarak suçlu davranış gösterme eğiliminin geçişliliğinden söz edilmektedir. Birey, davranışlarını ve fiziksel yapısını kontrol edemediğinden ortaya çıkan suçlar doğal suçlar olarak kabul görmektedir. Suçun toplum tarafından üretildiği, bireylerin her zaman kendi istekleri ile suç işlemedikleri ve toplum tarafından suçlu davranışa itilebildikleri, cezaların da bilimsel metotlar kullanılarak verilmesi gerektiğine de değinmektedir (Özalp, 2020: 80-85; Dolu, 2012: 152-160). Bu yönü ile bireysel teorilerden biraz olsun sıyrılmış olduğu söylenebilmektedir.

Diğer teorilerden Biyolojik Teoriler genel olarak; kalıtsal bozuklukların, beyinde, kromozomlarda ve hormon sistemlerindeki anormalliklerin suçlu davranışa yol açtığını savunarak bu davranışların nedenlerini genetikte aramaktadır. Sosyolojik Teoriler ise toplum ve birey arasındaki etkileşimi başlangıçtan itibaren ele alarak bu etkileşim sürecindeki olumsuzlukların bireyi suçlu davranışa yönelttiğini savunmaktadır. Bu teorilerin temel unsuru suç olgusunun toplum ekseninde açıklanmaya çalışılmasıdır (İçli, 2007: 88-142).

2.6. Dijital Çağda Suçun Dönüşümü: Siber Suçlar

Gelişen ve değişen teknoloji ile birlikte insanlar bilgisayar, akıllı telefon vb. nesneler ve internet aracılığı ile birbirine bağlı ağlar üzerinden yargı sınırlarının olmadığı sanal ortamlarda etkileşimde bulunabilmektedir. Birbirine bağlı olan ve sürekli bilgi akışını sağlayan bu ağlar 'siber uzay' olarak tezahür edilmekte ve siber suçların yolunu açmaktadır (Kundi ve Nawaz, 2014: 3). Günümüzde gerçekleştirilen siber saldırıların birçoğu fiziksel dünyadaki suçların siber uzaya göçünü temsil etmektedir. Siber uzay, suçluların geleneksel suçları yeni yollar ile işlemek için kullanmaya başladıkları bir araç haline gelmiş bulunmaktadır (Brenner, 2010: 10). Günümüzde bilgisayarların boyut olarak küçülmüş olması ve fiyat olarak herkese hitap ediyor olması sebebi ile kullanımı artmış, akıllı telefonların da internete bağlanabiliyor oluşu ile birlikte ağlar üzerindeki trafiğin artışı kötü amaçlı kullanımların kontrolünü zorlaştırmıştır (Akdağ, 2009: 22).

Siber suç; bilgisayarın ve internetin kötüye kullanılması ile birlikte ortaya çıkan, bilgisayara vb. araçlara karşı ya da kullanıcısı olan bireye karşı gerçekleştirilen eylemler olarak ifade edilmektedir. Bilişim suçları olarak da anılmakta fakat bilişim suçları telefon gibi araçlar ile işlenen suçları da içermesi ve daha kapsamlı olması sebebi ile internet ağları kullanılarak siber uzayda işlenen suçlar, siber suçlar olarak tanımlanmaktadır (Budak, 2015: 5-6). Nasıl işleneceklerinin kolay öğrenilebilmesi, neden oldukları potansiyel zarara kıyasla daha az kaynak gerektirmeleri, fiziksel olarak bir ortamda bulunmadan işlenebilir olmaları ve yasalar ile açık ve net şekillerde yasaklanmayarak yasa dışı kabul edilmeyen noktalarının bulunması gibi faktörler ile fiziksel

suçlardan farklılaşmaktadır (Kundi ve Nawaz, 2014: 2; Özudođru, 2010: 9). Bunun yanı sıra siber suçlar; işleniş biçimleri, görülme sıklığı, karşılığında uygulanan yaptırım oranları vb. faktörler açısından farklılık gösterse de ulusal ve uluslararası ortak bir sorun olarak değerlendirilmektedir (Smith vd., 2015: 3). Siber suçlar, herhangi bir demiryolunun durdurulabilmesine, yanlış sinyaller ile uçak ve tren gibi araçların yönlendirilebilmesine, bir ülke için önemli olan politik, askeri, ekonomik vb. verilerin başkalarının eline geçebilmesine sebep olabilmektedir. Aynı zamanda her türlü elektronik medya üzerinde yanlış bilgiler verilebilmesine ya da gizli bilgilerin yayılabilmesine, hedef alınan sistemlerin saniyeler içerisinde çökebilmesine de sebep olabilecekleri için geleneksel suçlara oranla daha büyük zararlara da yol açabilmektedirler (Das ve Nayak, 2013: 142). Örneğin; 20 Eylül 2001 yılında dünyanın en işlek sekizinci limanı olan Teksas'ta ki Houston Limanı'na bir siber saldırı düzenlenmiş ve sistem çökertilerek, gemilerin giriş çıkışından demirlemesine kadar tüm süreci barındıran veritabanlarına erişim engellenmiştir. Saldırıyı başlatan bilgisayarın İnternet Protokolü (IP) adresi belirlenerek saldırganın adresi bulunmuş, hedefinin aslında bir başka ülkedeki bilgisayar sistemi olduğu gerçeğı ortaya çıkmıştır. Saldırı sonucunda çözümsüz problemler ortaya çıkmamış olsa da sistemdeki güvenlik açıklarını kapatmak gerekliliğini göstermiştir (Brenner, 2010: 104-106). Bu sebeple toplumlar siber suçlara karşı önlemler alabilmek ve bilgi güvenliklerini sağlayabilmek için teknoloji alanında gelişmek zorunda kalmışlardır. Bir bakıma siber suçların toplumların siber savunma gelişim sürecine katkı sağlamış olduğu yorumu yapılabilir.

Tüm siber suçlar hem bilgisayar, akıllı telefon vb. araçları hem de kullanan kişiyi mağdur olarak içermektedir. Bu durum hangisinin ana hedef olduğuna bağlı olarak değişmektedir. Hedef birey olduğunda bilgisayar gibi teknolojik aletler hedefe ulaşmak için kullanılan bir araç niteliğı taşımaktadır. Bu tarz siber suçlar genellikle daha az teknik bilgi gerektirmektedir çünkü verilen zarar daha çok psikolojik ve soyut olmaktadır. Suçlu kişi tarafından elde edilen bilgiler doğrultusunda bireylerin zayıflıkları ve veri mahremiyetleri istismar edilmektedir. Öte yandan bilgisayar benzeri aletlerin hedef olarak seçilmesi durumu ise teknik bilgi gerektirmektedir ve bu suçlar bilgisayar ve internetin ortaya çıkması ile birlikte varlık kazandıkları için diğerlerine oranla yeni olarak kabul görmektedir. Günümüzde internetin hayatın bir parçası haline gelmiş olması bu tarz suçların her gün ve sayısızca işlenmesine fırsat vermiş bulunmaktadır (Dashora, 2011: 241). Bu alanda kesin ve belirli bir ceza yasasının bulunmaması durumu, yakın çevre tarafından gözlemlenebilir olmaması gibi nedenler suçluyu vazgeçirici unsurların yetersiz olmasına sebebiyet vermektedir.

Geleneksel suçlarda, işlenecek her suç türü için farklı araçlar ve ortamlar gerekmede olsa da siber suçlarda failin internete bağlı bir bilgisayarının olması yeterli görülmektedir (Brenner, 2010: 170). Bunun yanı sıra geleneksel suçlar ve siber suçlar arasındaki farklılıklar belirtilecek olduğunda; öncelikle siber suçların kapsamını belirlemenin ve bir çerçevesini oluşturabilmenin

teknolojinin sürekli gelişmeye devam etmesi sebebi ile daha güç olduğu ifade edilebilmekte, teknik bilgi gerektirmektedir (Ermeydan, 2018: 11). Anlık, zaman ve mekan kavramlarından bağımsız gerçekleştirilebilmektedirler. Dolayısıyla siber suçlara müdahale edebilmenin geleneksel suçlardan daha zor olduğu sonucuna varılabilmektedir. Geleneksel suç mağdurlarından farklı olarak siber suç mağdurlarında; çevrelerinin tepkisinden çekinmek, damgalanmaktan huzursuzluk duymak, çevresindekilerin güvenini zedelemekten korkmak, güvenlik birimlerine ve ceza sistemine yeterince güvenmemek, kanunları bilmemek gibi nedenlerden ötürü şikayetçi olmaktan kaçınmaları söz konusu olmaktadır. Siber suçların sadece bireyi ya da bir grubu etkiliyor olmasının yanı sıra bir toplumu tehdit edebilme potansiyelinin bulunması sebebi ile bu tarz suçların önlenmesinde kurumlar arası ve hatta uluslar arası işbirliğinin gerekli olduğuna değinilmektedir (Akarslan, 2011: 14-15; Peker, 2010: 33).

Siber suçların ana amacının bilgiye ulaşmak olduğu (Yar, 2005: 419), bilginin günümüzde artan değeri de göz önünde bulundurulduğunda ıskellikten sıyrılmış, modern bir suç türü olduğunu açıkça kanıtlamaktadır. Geleneksel suçlarda iç dürtülerin ön planda olması ve genellikle şiddet içermesine karşın, siber suçlarda bilme isteği ve merak suçun temelini oluşturmaktadır.

Günümüzde her geçen gün siber suçların oluşturduğu riskler ve mağduriyetler artmaktadır. Özellikle salgın sürecinde, çeşitli küresel toplulukların ve ülkelerin gizli tutulan bilgilerini ele geçirmek amacıyla siber saldırıları düzenlendiği ve sürekli bir siber tehdit söz konusu olduğu ifade edilmektedir. Evden çalışmaların yaygınlaşması, karantina sebebi ile bireylerin internet kullanım sıklıklarının artması gibi faktörler ile birlikte, siber suçlular kötü amaçlı yazılımları savunmasız kullanıcılara yayarak salgın döneminden faydalanmış bulunmaktadır (Olofinbiyi, 2022: 40-43). Güncel istatistikler incelendiğinde, teknolojinin sağladığı avantajlar ile birlikte siber suçların sürekli olarak bir artış göstermekte olduğu ve aynı şekilde suç kategorisinde de bir artışın söz konusu olduğu görülmektedir (Akdağ, 2009: 44).

Siber suçlarda delil toplama faaliyetlerinin fiziksel suçlara oranla daha zor olduğu kabul edilmektedir. Fiziksel suçlarda bir olay yeri bulunabiliyor olması delil toplama için bir mekan sunabilirken; siber suçların zaman ve mekandan bağımsız olması, sonuçlarının başka ülkedeki bireyleri ya da toplumu vb. etkileyebiliyor olması sebebi ile delil toplamayı zorlaştırmaktadır. Bunun yanı sıra yasal boşlukların bulunması ve anonimlik oluşturabilmesi sebebi ile de bireyler siber suçlara yönelebilmektedir. Geliştirilen savunma önlemleri her geçen gün teknolojiadaki ilerlemeler sebebi ile ortaya çıkan yeni bir siber suç tekniği ile aşılabileceğinden dolayı, teknolojinin sürekli takibi ve savunmaların da teknik bilgiler ile sürekli güncellenmesi gerekmektedir (Taşçı ve Can, 2015: 231). Geleneksel suçlarda bir suçun oluşması arka sokağa, eve, bahçeye vb. mekanlara kamera sistemi yerleştirilmesi ya da polis kontrol noktası oluşturulması, alarmlar takılması gibi yöntemler ile önlenbilirken; siber suçları önlemek teknik bilgi ve süreklilik arz eden güncel takip gerektirmektedir.

2.6.1. Siber Suç İşleniş Çeşitleri

Geleneksel suçlarda olduğu gibi siber suçlarda da farklı şekillerde işlenme durumu söz konusudur. Dolayısıyla işlenme şekillerine göre siber suçlar da tanımlanmış ve kategorize edilmiştir. Birçok siber suç türü bulunmakla birlikte, temelinde internet ve ağ erişimi gerektirmeleri ortak özelliklerini oluşturmaktadır.

2.6.1.1. Oltalama (Phishing)

Siber suç türleri arasında en sık karşılaşılan tür olan Oltalama tekniği, potansiyel mağdurları tuzığa düşürmek amacıyla hazırlanan sahte elektronik postaların, bilinen bir firmadan, siteden ya da kişiden gönderiliyormuşçasına dizayn edilerek kullanıcılara iletilmesini içermektedir. Gönderilen elektronik posta içerisinde ilgili olduğu belirtilen bağlantılar bulunmakta ve kullanıcı bu bağlantıyı açtığında erişilen sitede istenilen bilgileri girmesi sonucunda bu gizli bilgiler doğrudan elektronik postayı ve siteyi oluşturan suçluların eline geçmektedir (Ermeydan, 2018: 18). Orijinal sitelerin birebir kopyası halinde sahte siteler oluşturularak da oltalama tekniği kullanılabilir. Kullanıcılar şüphelenmeden kredi kartı bilgilerini ya da kullandıkları sosyal medya hesaplarının bilgilerini bu sitelerden giriş yaptıklarında faillerin tuzaklarına düşmektedirler (Bilek, 2012: 40).

2.6.1.2. Truva Atı (Trojan Horse)

Truva atları, tıpkı virüsler gibi zararlı yazılımlar arasında yer almaktadırlar. Hedef bilgisayarda çalıştırılan sunucu ve yazılımcısının bilgisayarında yer alan işlemci olarak iki kısımdan oluşmaktadır. Yerleştikleri bilgisayarlarda yararlı bir dosya olarak görünerek, sistemin arka planında asıl yazılımcı tarafından bilgisayarın yönetilmesine olanak sağlamaktadırlar. Faydalı olarak görülen bir uygulama ile birlikte bilgisayara girebilmekte; kullanıcısı farkında olmadan bilgisayardaki verilerin asıl yazılımcı tarafından değiştirilebilmesine, silinebilmesine ve tüm şifre ve verilerin yazılımcısının bilgisayarına aktarılabilmesine fırsat vermektedirler. Bilgisayardaki tüm aktiviteleri takip etmekte ve kullanıcı tarafından tespit edilmeleri zor olduğundan uzun süre arka planda veri aktarımı gerçekleştirilebilmesine sebep olmaktadır (Budak, 2015: 18; Çekiç, 2006: 65-66). Özellikle günümüzde bireylerin yanlarından hiç ayırmadıkları akıllı telefonlara indirilen ücretsiz ve güvenilir olmayan uygulamalarda istenen erişim izinleri verildiğinde Truva atlarının kolayca telefona yerleşebilmesine ve verilere erişim sağlanabilmesine olanak sağlanmaktadır.

2.6.1.3. Çöpe Dalma (Scavenging)

Atık toplama olarak da adlandırılmakta olan bu teknikte; bilgisayar sisteminden silinmiş verilerin gelişmiş yöntem ve programlar ile tekrar geri getirilmesi ile ele geçirilmesi söz konusu olmaktadır (Çekiç, 2006: 63). Dijital ortamda silinen bilgiler tamamen kaybolmamaktadır. Teknik

bilgi gerektiren bu işlemlerde, hemen hemen silinen her veri yığımına ulaşabilmek mümkündür (Karagöz, 2019: 84). Ticari bilgiler, kişisel veriler ya da askeri özel sırlar bu teknik ile ele geçirilebilmektedir. Örneğin; 1980’li yıllarda Amerika’da birçok askeri ve devlet sırları bu teknik ile ele geçirilmiştir (Alp, 2018: 28).

2.6.1.4. Bilgisayar Virüsleri

Siber suç olarak dünya çapında gerçekleşmiş olan ilk büyük olay; yaklaşık olarak 45 milyon kullanıcıya toplu elektronik posta yolu ile gönderilen bilgisayar virüsünün, kullanıcıların bilgisayarlarını etkilemesi sonucu, 2000 yılında gerçekleşmiştir (Kundi ve Nawaz, 2014: 63-64). Bilgisayar virüsleri; kullanıcının bilgisi ve izni olmaksızın sisteme bulaşarak çalışma şeklini değiştirebilme, fark edilmeyecek değişiklikler ile kendisini kopyalayabilme ve kullanıcıdan gizlenebilme özelliklerini taşıyan zararlı yazılımlardır. Virüs bulaşan dosyalar erişilemez ya da kullanılamaz hale gelebilmektedir. Dosya yapısını değiştirebildiğinden ötürü içerik de hasar alabilmektedir. Bunun yanı sıra virüsler, sisteme aşırı yüklenme yapabilmekte ve sistem hızını yavaşlatabilmektedirler (Karagöz, 2019: 72).

Virüslerin, yayılabilmesi için taşınmaları gerekmektedir. Bu taşınma elektronik postalar, taşınabilir bellekler vb. aracılığı ile gerçekleşmektedir. Taşınmadıkça, ağlar üzerinden yayılamamaktadırlar (Akyeşilmen, 2018: 76-77). Bulaştıkları bilgisayarlar ya da akıllı telefonlar üzerinden izinsiz elektronik posta veya mesajlar gönderebilmeleri sebebi ile de kolay ve hızlı bir şekilde yayılabilirler.

2.6.1.5. Ağ Solucanları (Network Worms)

Ağ solucanları, diğer bir deyişle ‘kurtçuklar’, bulunan ağ bağlantıları sayesinde bilgisayarlara yerleşebilen ve herhangi bir dosya içerisinde gizli kalma gibi bir zorunlulukları bulunmayan, aynı ağ bağlantısına sahip diğer bilgisayarlara da kolaylıkla bulaşarak çoğalabilen zararlı yazılımlardır. Zarar verme şekilleri virüslere benzese de yayılma şekilleri bakımından farklılaşmaktadırlar (Akyeşilmen, 2018: 77). Öncelikle sistemde bilgi aktarımı yapan özelliklerin ele geçirilmesini sağlamak ve sisteme Truva Atı bırakarak, kullanıcının aktifleştirmesini beklemeden kendi kendine ilerleyebilmektedirler. Solucanlar girdikleri ağ sisteminde büyük sayıda kendilerini çoğaltabilmektedirler. Dolayısı ile aynı ağ sistemine bağlı tüm bilgisayarlara ve araçlara kolaylıkla bulaşabilmektedirler. Girdikleri sistemlerde gizli bilgilere rahatlıkla erişebilmekte ve hareket izlerini silmektedirler. Bu sebeple tespit edilmeleri de güç olmaktadır (Güneş, 2015: 19-20).

2.6.1.6. Gizli Kapılar (Trap Doors)

Yazılımcıların, kendi oluşturdukları sisteme müdahale gerektiği durumlarda, güvenlik önlemlerine takılmadan girebilmeleri için bıraktıkları ve sadece kendisi tarafından bilinen bir nevi

açık kapılardır. Arka kapılar olarak da adlandırılmaktadırlar. Kötü niyetli yazılımcıların sisteme sızmak için kullanabilecekleri zayıf noktalardır. Gizli kapıların keşfedilmesi halinde kötü niyetli yazılımcılar sisteme rahatlıkla sızabilmekte ve korunan tüm verilere ulaşabilmektedirler (Budak, 2015: 17).

2.6.1.7. Salam Tekniği (Salami Techniques)

Salam tekniği bankalarda kullanımı yaygın olan bir tekniktir. Failin; banka hesabına sahip olan müşterilerin hesaplarında bulunan paradan, virgülden sonraki miktarını kendisine ait başka bir hesapta toplaması ile gerçekleşmektedir. Hesap sahipleri küçük miktarlardaki bu hareketleri çoğunlukla fark edememektedir. Birçok hesaptan toplanan küçük miktarlardaki para, hukuka aykırı şekilde büyük bir kazanç sağlanmasına yol açmaktadır. Bu tekniği kullanımı için Truva Atı benzeri yazılımlar kullanılmaktadır (Yaycı, 2007: 30-31).

2.6.1.8. Mantık Bombaları (Logic Bombs)

Truva Atı tekniğinin bir türevi olduğu söylenebilmektedir. Zarar verici şekilde sonuçlar elde etmek amacı ile bilgisayar yazılımının içerisine kasten yerleştirilen bir seri komutlar bütünü olarak ifade edilmektedir. Belirlenen özel şartlar meydana geldiğinde zararlı faaliyetler meydana getirmek için tasarlanmış bir tekniktir. Örneğin; mantık bombaları gizlenmiş olan bir bilgisayar sistemi, sadece belirlenen bir tarihte sisteme format atabilir ya da sistemin çökmesine sebep olabilir. Bunun yanı sıra devamsızlığı belli bir günün altına düşen öğrencilerin devamsızlık haklarını yükseltebilmekte, maaşı belli bir miktarın üzerine çıkan ya da altına düşen kişilerin maaşlarının yükselmesine, azalmasına ya da yanlış hesaplanmasına sebep olabilmektedir. Kısacası, belirli bir amaç ile belirli şartlar oluştuğunda çalışması için tasarlanmaktadır. Sistem içerisinde tespit edilmeleri de zor olmaktadır (Pallı, 2008: 56).

2.6.1.9. Tuş Kaydediciler (Keylogger) ve Ekran Kaydediciler (Screenlogger)

İnternet ağı üzerinde herhangi bir dosya içerisine gizlenerek, kullanıcının bilgisi dışında farkında olmadan bilgisayara yüklenebilen yazılımlardır. Bulaştıkları bilgisayarlarda aktif hale gelmelerinden itibaren klavyede kullanılan her harfin bilgisini hatta her tıklamayı kaydederek rapor haline getirmekte ve ağ üzerinden yazılımcısına rapor iletmektedir. Bilgisayar kullanıcısının fare ile yaptığı her tıklama sonucunda, fare simgesinin durduğu ekranda ortalama 100x100 piksel büyüklüğüne sahip ekran görüntüleri de yazılımcıya iletilebilmektedir. Dolayısı ile kötü amaçlı yazılımı tasarlayan kişi tarafından kullanıcının tüm şifre bilgilerine ulaşılabilir (Bilek, 2012: 42).

2.6.1.10. Bukalemun Tekniği (Chameleon Techniques)

Yararlı yazılımlarmış gibi sisteme girerek daha sonra kendilerini iyi şekilde kamufle etmelerinden ve fark edilmelerinin zorlaşmasından dolayı bukalemun adını almışlardır. Bu zararlı yazılımlar bilgisayar sistemine girdikten sonra normal bir program gibi çalışmakta fakat arka planda şifreleri ve kullanıcı adlarını taklit etme özellikleri sebebi ile gizli dosyalara erişebilmekte ve verileri kaydedebilmektedirler. İnternet ağı üzerinden giriş yapılan herhangi bir hesabın bilgisini kaydettikten sonra sistemin geçici olarak bakımda olduğuna yönelik bildirim gönderilmesini sağlamakta ve bilgileri kullanarak hesaplara erişim sağlayabilmektedirler (Güneş, 2015: 26).

2.6.1.11. Zombi Bilgisayar

Bilgisayar kullanıcılarının bilinçsizlikleri, lisanssız yazılım kullanmaları ya da kötü yapılandırılmış bir bilgisayar sistemine sahip olmaları vb. etkenlerden dolayı bilgisayarların uzaktan erişime açık olması durumunda; kötü amaçlı yazılımcıların uzaktan erişim ile bu bilgisayarları kullanarak hukuka aykırı eylemler gerçekleştirmeleri sonucunda bu bilgisayarlar ‘zombi bilgisayar’ ya da ‘köle bilgisayar’ olarak adlandırılmaktadırlar. Orijinalinin kopyası siteler oluşturularak, kullanıcıların hesap bilgilerini bu sitelerde girmeleri ile İnternet Protokol Numarası (IP adresi) ele geçirilerek bilgisayar erişimi gerçekleştirilmektedir. Ele geçirilen bilgisayarlar kullanıcısının bilgisi dışında, hukuka aykırı düzenlenecek her saldırıda kolayca kullanılabilir (Orta, 2015: 43-44).

2.6.1.12. Botnet Saldırıları

Kötü amaçlı yazılımcı tarafından gizlice ele geçirilerek, bot programı bulaştırılan bütün zombi bilgisayarların oluşturduğu ağa ‘botnet’ adı verilmektedir. Tek bir noktadan yönetilen bu bot ağ sistemi ile kötü amaçlı eylemler gerçekleştirilebilmektedir. Kullanıcılarının haberi olmadan zombi bilgisayarlardan herhangi bir internet adresine eş zamanlı saldırılar düzenlenebilmekte, elektronik posta adreslerindeki kullanıcı adları, şifreleri vb. bilgiler ele geçirilebilmekte; bir videonun izlenme oranı, bir reklamın tıklanma sayısı ya da bir sosyal medya hesabının takipçi sayısı artırılabilir. Aynı zamanda, kullanıcıların bilgileri toplanarak şantaj yapılabilir ya da bilgileri satılabilir (Alp, 2018: 46).

2.6.1.13. İstenmeyen Elektronik Postalar (Spam)

Spam olarak alınan elektronik postalar siber suç tekniklerinin bir diğer örneğidir. Kullanıcıların talepleri olmaksızın, aynı iletinin fazlaca kopyasının kişilere gönderilmesi olarak da ifade edilebilmektedir. Postaların birçoğu reklam amaçlı olmasının yanı sıra herhangi bir konuda kamuoyu oluşturma amacı da taşımaktadır. Kullanıcının posta kutusunda gereksiz veri kalabalığı oluşturarak asıl beklediği bilgiyi almasına engel olabilmektedirler. Aynı zamanda bu elektronik

postalar içerisinde zararlı yazılımlar barındırabilmekte ve açılmaları sonucunda bilgisayar sistemine zararlı yazılımları bulaştırabilmektedirler (Güngör, 2007: 72-73).

2.6.1.14. Tavşanlar (Rabbits)

Bilgisayar virüslerinin türevlerinden olan bu virüs çeşidi ise diğerlerine oranla daha hızlı çoğalmaktadırlar. Bu sebepten ötürü tavşan ismini almış bulunmaktadır. Bilgisayar belleğinde veya diskte veri depolama alanı dolana dek çoğalmaya devam etmektedirler. Özellikle birden fazla kullanıcıya sahip olan ağ sistemlerinde ana sistemin veri işleme kapasitesini zorlaştırmaktadırlar. Sistemin yavaşlamasına ve çökmesine sebep olabilmektedirler (Pallı, 2008: 59).

2.6.1.15. Diğer Siber Suç Teknikleri

Detayları belirtilen siber suç teknikleri dışında aynı amaçları taşımakta olan birçok teknik daha bulunmakta ve teknolojik gelişmeler ile birlikte çeşitlenerek artmaya devam etmektedir. Özellikle en basit teknikler arasında yer alan kullanıcının sosyal medya hesaplarını ele geçirme tekniği ile dolandırıcılık faaliyetlerinde bulunma eylemi salgın döneminde en sık karşılaşılan tekniklerden birini oluşturmaktadır. Failler her geçen gün yeni bir teknik geliştirerek kullanıcıları tuzaklarına düşürmeye çalışmaktadırlar. İnternetin varlığı temelinde teknolojik gelişmelerin sağladığı her yeni imkan, yeni bir siber suç çeşidini de beraberinde getirmektedir.

2.7. Mağdur

Mağdur kavramı genel olarak; dolaylı ya da doğrudan olacak şekilde haksızlığa uğramış olan, zarar görmüş ya da acı çekmiş olan kişi şeklinde tanımlanabilmektedir (Katoğlu, 2012: 658-660). Hukuki açıdan ise suçun pasif nesnesi olarak kabul edilmekte ve işlenen suç karşısında zarar gören suç kurbanı olarak ifade edilmektedir (Akcan, 2014: 369). 20. yüzyıla kadar işlenen suçlarda genellikle faile odaklanılmış ve mağdur boyutu yeterince ele alınmamıştır. Suçu açıklamada mağdur kavramına da ilgi duyulmaya başlanması ve “20. yüzyılın son çeyreğinde Avrupa devletlerinde mağdur haklarının gelişmesi ile birlikte 01.06.2005 tarihinde yürürlüğe giren 5271 sayılı Ceza Muhakemesi Kanunu ile mağdur hakları hatırlanmış ve mağdur yönünden birçok yeni düzenleme hayata geçirilmiştir”. Bunun yanı sıra “...aynı tarihte yürürlüğe giren 5237 sayılı Türk Ceza Kanunu’nda onarıcı adalet modelinin en önemli aktörü olan mağdurun haklarına önem verilerek birçok müessese mevzuata dahil edilmiştir”. Böylelikle mağdur ve mağdur haklarına yönelik önemli adımlar atılmış olmaktadır (Aykara ve Özkan, 2017: 145; Seçkin, 2020: 621-622). Ayrıca, mağdur merkezli yaklaşımların ceza sistemleri içerisinde giderek önem arz etmekte ve artış göstermekte olduğu gözlemlenmektedir. Başka bir deyişle; suç olgusu içerisinde unutulmuş ve yeterince önemsenmemiş aktör olan mağdur, eylemlerinin suç oluşumunu ve sonucunu etkilemesi dolayısıyla anahtar aktör niteliği kazanmıştır (Güngör, 2019: 202; Wolhuter vd, 2009; 1-2).

20. yüzyılın sonlarında kriminolojinin alt dalı olan ve mağdurları sosyal, psikolojik, hukuki açılardan incelemekte olan ‘Mağdur Bilim (Victimology)’ in önem kazanmaya başladığı görülmektedir. Viktimoloji; mağduriyetin tekrarlanmaması, mağdur ve fail arasındaki ilişki, mağdurdun suç sonrasındaki problemleri ve hukuki hakları vb. başlıkları konu edinmektedir. Ortaya çıkan suç olgusunda öncelikli olarak mağdur ile fail arasındaki ilişkiyi ve mağdurun suç sonrası davranışlarını araştıran Viktimoloji, özellikle mağdurun suçun meydana gelmesindeki rolüne odaklanmaktadır (Sokullu Akıncı ve Dursun, 2016: 5-6). Mağdurlar suçun ve suçlunun tespit edilmesinde önemli bir rol oynamakta; suç ile ilgili normal şartlarda elde edilmesi güç olan bilgilere ve delillere ulaşmayı kolaylaştırmaktadırlar (Polat ve Gül, 2010: 1293-1294).

Araştırmanın ana konusu olan siber suç mağduriyeti bireyin; şahsi bilgisayarına yetkisiz erişim, izni ve bilgisi dahilinde olmadan bilgisayarına dosya eklenmesi, silinmesi ya da içeriklerin değiştirilmesi, kötü amaçlı yazılımların bulaşması sonucu veri kaybı, mahremiyet ihlali, kişisel verilerin ve kredi kartı vb. gizli bilgilerin sızdırılması sonucu yaşadığı maddi ve manevi kayıplar olarak tanımlanabilmektedir (Ngo, 2011: 777). Gelişen teknolojinin olumlu etkilerinin yanı sıra beraberinde getirdiği; siber dolandırıcılık, siber zorbalık, sexting, nefret söylemi, çocuk pornografisi, mahremiyeti kötüye kullanma vb. siber suçların varlığı hayatın bir parçası olmuş durumdadır. İnternet teknolojisinin getirdiği yeniliklerin denetiminin yetersiz olması durumu mağduriyetler için temel oluşturmaktadır. Bu denetimsizlik, siber suç alanındaki hukuki boşluk ve internetin sağladığı anonimlik siber suç eylemleri gerçekleştirme potansiyeline sahip bireyler için zemin hazırlamaktadır (Karaca vd., 2021: 178-182). Bunun yanı sıra 2009 yılında yapılan bir çalışmaya göre sosyoekonomik statüsü yüksek olan bireylerin ya da ailelerin siber suç mağduriyeti yaşama riskinin yüksek olduğu sonucuna varılmıştır. Gelir seviyesinin artması ile akıllı telefon ve bilgisayarlara ulaşmanın daha kolay hale gelmesi sebep olarak gösterilmektedir (Wang vd., 2009: 369).

2.8. Araştırmanın Kuramsal Perspektifi

2.8.1. Rutin Aktiviteler Teorisi

Suçun kaynağı ve nedenleri her çağda ve her toplumda çeşitli faktörlere odaklanılarak açıklanmaya çalışılmıştır. 1940’lı yıllardan öncesinde suç teorileri suçun kaynağını doğaüstü güçlerde, insan genetiğinde ve bireylerin cezadan kaçabilmek adına yaptıkları rasyonel tercihlerde aramışlardır. Fakat meydana gelen İkinci Dünya Savaşı’ndan sonra suç oranlarında artışların görülmeye başlanması, suçları önleyebilme amacını ortaya çıkarmış bulunmaktadır. Bunun sonucunda suçun kaynağını araştırmaya yönelik bakış açılarında bir farklılaşma meydana gelmiş ve ilk kez suçun işlenme mekanizması ile unsurları üzerinde durularak, suç olgusunun engellenebileceğine dair düşünceler Lawrance Cohen ve Marcus Felson’un yaptıkları bir çalışmada

‘Rutin Aktiviteler Teorisi’ ile savunulmuştur (Birceviz, 2019: 25; Ngo ve Paternoster, 2011: 775-776).

Rutin aktiviteler teorisi bireylerin gündelik yaşamlarındaki rutinlerinin suçun ve mağduriyetin oluşumuna olan etkisini konu edinmektedir (Cohen ve Felson, 1979: 32-33; Yar, 2005: 412). Teorinin; toplulukların bulundukları ortamlarda insan davranışlarının yalnızca mekansal olarak farklılıklar göstermediğini belirterek, zamansal faktörlerin etkisini araştıran Amos Hawley’in İnsan Ekolojisi Teorisi’nden türemiş olduğu bilinmektedir. Ortak toplumsal davranış kalıplarına odaklanan Hawley; bu davranışları ritim, tempo ve zamanlama şeklinde üç temelde açıklamaktadır. Olayların normal, gündelik olarak tekrarlamasını ritim, belirli bir zaman diliminde gerçekleşen olayların sayısını tempo ve çevredeki tüm olayların kesişimi ile eşgüdümlülüğünü ise zamanlama olarak adlandırmaktadır. Cohen ve Felson da bu ilkeleri teorilerine uyarlamışlardır (Branic, 2016: 1). Dolayısıyla bu teorinin diğer kriminolojik teorilerden temelde farklı olmasının sebebinin kökenlerinden kaynaklı olduğu ifade edilmektedir. Çünkü daha önceki teorilerin hiçbirinde zaman faktörünün suça etki eden bir olgu olduğu kabul edilmemiştir. Rutin aktiviteler teorisi ise suçun mekan ile ilişkisinin yanına zaman faktörünü de ekleyerek daha kapsamlı bir açıdan incelenbilmesine olanak sağlamış bulunmaktadır (Clarke ve Felson, 2008: 3). Sonuç olarak suç olgusunu her açıdan ele alabilmek ve açıklayabilmek amacıyla suçun tam olarak nasıl, nerede ve ne zaman meydana geldiğine odaklanmaktadır (Felson ve Eckert, 2018: 17).

Hawley’in teorisine göre insan davranışları; hangi mevsimde, yılın hangi ayında, haftanın hangi gününde ve hatta günün hangi saatinde olunduğuna göre şekillenmekte ve etkilenmektedir. Rutin aktiviteler teorisini büyük ölçüde bu mantıksal çerçeve şekillendirmektedir (Dolu, 2009a: 5). Aynı zamanda; bireylere odaklanan mikro analizlerden ziyade insan popülasyonlarının makro analizini içeren ve insan davranışlarının farklılıkları ile karşılıklı ilişkilerini tanımlamakta olan sistemik düşünme ile bunun yanı sıra bu davranışların zaman içerisinde gerçekleşen değişimlerine dair sunulan bilimsel ve deneysel örnekler, Hawley’in çalışmasından rutin aktiviteler teorisine taşınmış diğer etkenler olarak ifade edilmektedir (Clarke ve Felson, 2008: 3-4).

Suç oluşumunu birçok faktör meydana getirebilmektedir fakat genel olarak bakıldığında suçun ve mağduriyet durumunun oluşumunu tetikleyen beş ana unsur bulunmaktadır. İlk olarak hedefin görünür olması, başka bir deyişle değerli eşyaların korunmasız şekilde bırakılması ya da açık alanda elde yüksek miktarda para ile dolaşılması gibi davranışların suçlu için hedefi görünür kıldığı ve suça davetiye çıkardığı ifade edilmektedir. İkinci olarak hedefin değerli ve arzu edilebilir olması durumu mağdur olma riskini artıran faktörlerden biri olarak görülmektedir. Maddi olarak daha değerli olan bir nesnenin ya da iyi giyimli ve zengin görünen bir kişinin hedef olması olasılığı daha yüksektir. Bunun yanı sıra mağdur bilimi araştırmacıları, bazı insanların tekrarlı olarak suç mağduru olduğunu belirtmektedir. Bu durumun ardında yatan nedenlerin ise suçluların aynı tip bireyleri hedef almalarından ya da hedeflerine atfettikleri değerlerden kaynaklanıyor olabileceği

düşünülmektedir. Üçüncü faktör ise hedefin suça karşı korunmasız olması durumudur. Bu durum suçlunun hedefine yaklaşımını etkilemektedir. Suça ve suçluya karşı koyma ihtimali fazla olan hedeflerin mağdur olma olasılığı daha düşük olarak görülmektedir. Aynı zamanda ve dördüncü unsur olarak; hedefin hareket kabiliyeti de mağdur olup olmama durumunda etkili rol oynamaktadır. Örneğin; hacim olarak büyük ya da ağır olan eşyalar değeri yüksek olsa bile arabalar ya da mücevherler kadar hızlı taşınamadıkları için suçluların öncelikli hedefleri arasına girmemektedirler. Son olarak hedefin erişilebilir olması da suçun meydana gelmesinde diğer faktörler gibi etkili olmaktadır. Suçlular rahatlıkla erişebilecekleri ve sonunda da ortamdan rahatlıkla uzaklaşabilecekleri ya da uzaklaştırabilecekleri hedefler tercih etmektedirler (Dolu, 2009a: 9-11; Felson ve Eckert, 2018: 30-31). Genellikle erişilebilir olmalarının kolaylığından dolayı, suçluların bulundukları muhitlerde ve çevresinde yaşamakta olan ve koruyucusu bulunmayan bireyler suçluların potansiyel mağdurları olarak görülmektedirler (Clevenger vd., 2018: 34).

Rutin aktiviteler teorisine göre; suç oranlarını etkileyebilecek doğrudan ve temaslı bir suçun oluşabilmesi için üç asgari unsur bulunmaktadır. Bunlar; güdülenmiş yani motive olmuş bir suçlunun varlığı, uygun hedeflerin bulunması ve suça karşı yeterli ya da yetenekli koruyucuların bulunmaması olarak ifade edilmektedir (Cohen ve Felson, 1979: 589; Clevenger vd., 2018: 37-38). Aynı zamanda teori, karşısına çıkacak en uygun fırsatları değerlendirmek için bekleyen potansiyel suçlunun varlığını peşinen kabul etmesi yönüyle de diğer teorilerden farklılaşmaktadır (Dolu, 2012: 129). Potansiyel suçlu, herhangi bir nedenle motive olmuş ve suç işleyebilecek herhangi birisidir. Dolayısıyla işlemesi muhtemel suç için kendisine kişi veya nesne olarak bir hedef belirlemektedir. Yeterli koruyucuların bulunmaması durumunda ise suçlu eylemini gerçekleştirebilmekte ve mağduriyet durumu ortaya çıkmaktadır (Clarke ve Felson, 2008: 1-3). Bu üç unsurun bir araya gelmesi ile suçun ortaya çıkması muhtemel olduğu gibi, herhangi birinin eksikliğinin ise suçun oluşumunu engelleyebileceği ifade edilmektedir (Branic, 2016: 1-2). Örneğin; günlük yaşamlarında bireyler çalışmak, alışveriş yapmak, tatil yapmak ya da öğrenim görmek amacıyla çeşitli yerlerde bulunabilmektedir. Dolayısıyla bireylerin ev içerisinde geçirdikleri vakit azalma göstermektedir. Yapılan araştırmalar da bireylerin ev dışında daha çok vakit geçirdiklerini ve bu durumun bazı suçlar için ortam hazırladığını göstermektedir. Yeterli koruyucuların bulunmaması durumunda özellikle hırsızlık vb. suç eylemini gerçekleştirmek amacıyla motive olmuş bir suçlu için boş kalan evler uygun hedef konumunda bulunmaktadır. Aynı zamanda ev dışında geçirilen zamanın artması ile birlikte bireylerin gün içerisinde gerçekleştirdikleri rutin aktivitelerde de artış ve çeşitlilikler meydana gelmektedir (Cohen ve Felson, 1979: 593-594). Böylelikle bir suça maruz kalma ve mağduriyet yaşama olasılıkları artış göstermektedir. İnternet teknolojisinin yaygınlaşmış olması ve salgın nedeni ile evde geçirilen sürenin uzadığı günümüzde ise siber suç mağduriyetleri çoğalmaktadır. Bu durumda suç olgusu ne kadar ortam değiştirmiş olsa da bir suçun meydana gelebilmesi için gerekli olan unsurlar siber suçlar için de geçerli bulunmaktadır. Motive olmuş bir suçlu uygun hedefini seçtikten sonra gerçekleştireceği suç eyleminin tekniğini belirleyebileceği

gibi tekniğini belirledikten sonra da buna uygun hedeflere yönelebilmektedir. Koruyucuların bulunmaması durumunda da suç eylemini gerçekleştirebilmektedir. Koruyucular fiziksel ortamda komşular, akrabalar, kapıcı ya da kameralar olabildiği gibi sanal ortamlarda ise anti virüs programları, güvenlik duvarları, içerik engelleyici yazılımlar, güçlü şifreleme teknikleri kullanma ya da birden çok faktörle doğrulama vb. şeklinde olabilmektedir.

Felson; teorideki suçun oluşumu için gerekli olarak belirtilen üç asgari unsurun suçluları motive eden şeylerin neler olduğunu, suçluların herhangi bir şekilde engelleyebilecek faktörlerin olup olmadığını tam olarak açıklayamadıklarından dolayı yetersiz kaldıklarını düşünmüştür. Bu sebeple suçluların eylemlerini gerçekleştirmelerini önleyebilecek olan koruyucuların olması dışında kalan engelleyici faktörlere odaklanarak ‘tutucular’ adı altında dördüncü bir unsur eklenmesi gerektiğini savunmuştur (Dolu, 2009a: 12). Teoriye eklenen tutucular unsuru aslında suçlunun engellenmesini ifade etmektedir. Başka bir deyişle motive olmuş suçluyu eylemini gerçekleştirmekten alı koyan, vazgeçiren içsel unsurlar olarak ifade edilebilmektedir. Örneğin; aile bağları güçlü ya da çevresi tarafından sürekli gözetim altında olan ve bundan çekinen birey bu tutucu ve engelleyici unsurlar sayesinde suç eyleminden vazgeçebilmekte ya da uzak durmaktadır.

Ortaya çıkışından bir süre sonra rutin aktiviteler teorisinin genellikle sokak suçlarını açıklamada daha başarılı olduğu fakat nicel araştırmalarda kesin bir suç mekanizması ve sonuç ortaya koyamayabileceği düşünülmüş ve diğer suçların da açıklanabilmesi amacıyla ‘Fırsatlar Teorisi’ ile bağdaştırılarak açıklama gücü yüksek bir model geliştirilmeye çalışılmıştır. Bunun yanı sıra, teorisinin kapsamını genişletebilmek bağlamında ‘Rasyonel Tercihler Teorisi’ ile de bütünleştirilmesi amaçlanmıştır. Böylelikle, geliştirilen teori daha geniş alanda suçların açıklanabilmesine imkan vermiş bulunmaktadır (Birceviz, 2019: 25-26).

Felson ve Clarke (1998: 9) suç fırsatları, ortam, suç oluşumu ve suçluyu konu edindikleri ‘*Opportunity Makes The Thief*’ adlı ortak çalışmasında suçun oluşumunun temel nedeninin fırsatlar olduğunu belirtmiş ve suç fırsatlarını on ilke halinde ifade etmişlerdir:

- 1- Fırsatlar, bütün suç türlerinin oluşmasında önemli bir rol oynamaktadır. Bir suçun işlenmesi fırsatlarının bulunması ile ilişkilendirilmektedir.
- 2- Suç fırsatları, suç çeşitlerine özeldir. Her suç farklı bir fırsatlar bütününe bağlı bulunmaktadır.
- 3- Suç oranları, eyleme geçilebilecek fırsatların daha yoğun olduğu günün belirli bir saatine, haftanın günlerine ya da bölgelere göre değişiklik gösterebilmektedir. Dolayısıyla suç fırsatları zaman ve mekanda yoğunlaşabilmektedir.
- 4- Günlük rutin faaliyetler suç fırsatlarını yaratabilmektedir. Başka bir deyişle suç fırsatları günlük faaliyetlere bağlıdır.
- 5- İşlenen bir suç, bir diğeri için fırsat yaratmaktadır. Suçlu yeniden suç eyleminde bulunabilmekte ya da işlenen bir suç beraberinde türevlerine, bir nevi suç silsilesine yol açabilmektedir.
- 6- Bazı nesneler ya da bireyler daha cazip suç fırsatları sunmaktadır. Taşınması kolay ve hızlı olan bir nesne ile yavaş hareket edebilen ve varlıklı görünen bir birey diğerlerine göre daha cazip olabilmektedir.

- 7- Teknoloji ve sosyal alanda meydana gelen deęişim ve gelişimler yeni suç fırsatlarını doğurmaktadır. Siber suçlar bu yeni fırsatlardan doğan suçlar için en iyi örneęi oluşturmaktadır.
- 8- Suç fırsatları azaltılarak suçun önlenmesi muhtemeldir. Durumsal suç önleme yöntemleri her suç türü için uyarlanarak suç eyleminin önlenmesine olanak sağlayabilmektedir.
- 9- Fırsatları azaltmak suçu tamamen ortadan kaldırmamaktadır. Bunun yanı sıra suçun yer deęişimine de neden olmamaktadır.
- 10- Yoęun bir şekilde suç fırsatlarını azaltmaya ya da ortadan kaldırmaya yönelik yapılacak çalışmalarla suç eylemlerinde ve oranlarında düşüşler sağlanabilir.

Maddelerden de anlaşılacağı üzere suç birey ile ortam arasındaki etkileşimin bir ürünü olarak ortaya çıkmaktadır. Ortamda bulunan suç fırsatları suçun ve mağduriyetin oluşumuna temel hazırlamaktadır. Böylelikle fırsatların azaltılmasına ya da ortadan kaldırılmasına odaklanan suç önleme yaklaşımları önem kazanmaktadır.

Durumsal suç önleme yaklaşımı, suçlulardan ziyade suça ve suçun ardındaki temel nedenlerine odaklanmaktadır. Bu yaklaşım ile bireyi suç işlemeye teşvik eden fırsatların azaltılabilmesi veya oluşan mağduriyetlerin, zararların en aza indirilebilmesi hedeflenmektedir. Başka bir deyişle suç oluşumundan önce suça sebebiyet verebilecek ya da suçlulara fırsat yaratabilecek faktörlerin analiz edilerek önlemler alınması ve suçluların kendi rasyonel tercihleri doğrultusunda suç işlemekten vazgeçmeleri amaçlanmaktadır (Bullock vd., 2010; 1-3).

Günümüzde suç önlemede mağdur odaklı bir bakış açısı da getirilerek düzenlemeye gidilmiştir. Daha önceleri suç olgusu içerisindeki mağdurun rolü göz ardı edilmiş olsa da, mağdura yönelik yeni çalışmalar suç önlemede yeni bir bakış açısı kazandırmış bulunmaktadır. Yapılan çalışmalar mağdurların da suç oluşumuna fırsat vermemek için gerekli önlemleri almaması ve dikkatsiz davranmaları sebebi ile en az suç eylemini gerçekleştiren birey kadar suçlu olabileceğini göstermektedir. Dolayısıyla mağdur eksenli bir bakış açısı ile suç ve ceza politikalarında da farklılaşmalar meydana gelmiş bulunmaktadır. Mağdurun tam anlamı ile masum olmama durumu söz konusu olabileceęi gündeme geldięi için suçun ortaya çıkmasına önlem alabilmek adına mağdur davranışlarını deęiştirmeye yönelik çalışmalar geliştirilmesi amaçlanmaktadır. Aslında suçun ortaya çıkardığı toplumsal maliyet bir nevi suçludan mağdura doğru kaydırılmaya başlanmıştır (Akıncı ve Dursun, 2016: 17-19). Yapılan bu çalışma da mağdur eksenli bakış açısından yola çıkarak, rutin aktiviteler teorisinin bütünleyici perspektifi ile birlikte siber suç mağdurlarının, mağduriyetlerine yol açma olasılığı olan davranışlarını ortaya çıkarmaya çalışmıştır.

ÜÇÜNCÜ BÖLÜM

3. ARAŞTIRMANIN BULGULARI

3.1. Katılımcıların Özellikleri ve İnternet Kullanım Alışkanlıkları

Araştırma kapsamında Bursa ilinde ikamet eden 20 siber suç mağduru ile yarı yapılandırılmış mülakat gerçekleştirilmiştir. Katılımcılara ilk olarak kendilerinden bahsetmeleri ve ikinci soru olarak günlük internet kullanım sıklıkları ile amaçları sorulmuştur. Verilen cevaplar çerçevesinde katılımcıların özelliklerinin yer aldığı tablo oluşturulmuştur.

Tablo 1: Siber Suç Mağduru Katılımcı Özellikleri

KATILIMCI	CİNSİYET	YAŞ	EĞİTİM DURUMU	MESLEK	GÜNLÜK İNTERNET KULLANIM SÜRESİ
K1	Erkek	25	Lisans	Yazılım Geliştirme Uzmanı	5 saat ve üzeri
K2	Erkek	40	Ön Lisans	Bilgi İşlem Birimi Müdürü	5 saat ve üzeri
K3	Kadın	38	İlköğretim	Ev Hanımı	2 saatten az
K4	Kadın	32	Lise	İşçi	5 saat ve üzeri
K5	Erkek	28	Lisans	Donanım Uzmanı	5 saat ve üzeri
K6	Kadın	40	Ön Lisans	Muhasebeci	5 saat ve üzeri
K7	Kadın	26	Lisans	Hemşire	2 ile 5 arası
K8	Erkek	30	İlkokul	İşçi	5 saat ve üzeri
K9	Erkek	30	Ön Lisans	Teknisyen	5 saat ve üzeri
K10	Erkek	27	Lisans	Askeri Personel	2 ile 5 arası
K11	Erkek	30	Lisans	Öğretmen	2 ile 5 arası
K12	Kadın	26	Lisans	Hemşire	2 ile 5 arası
K13	Kadın	24	Lisans	Hemşire	5 saat ve üzeri
K14	Kadın	23	Ortaokul	İşçi	5 saat ve üzeri
K15	Kadın	29	Lisans	Yazılım Geliştirme Uzmanı	5 saat ve üzeri
K16	Erkek	37	Lise	İşçi	5 saat ve üzeri
K17	Erkek	33	Lisans	Polis memuru	5 saat ve üzeri
K18	Kadın	27	Lisans	Mimar	5 saat ve üzeri
K19	Erkek	37	Yüksek Lisans	Yönetici	5 saat ve üzeri
K20	Kadın	34	Lisans	Öğretmen	5 saat ve üzeri

Katılımcılar arasında ortaokul, lise, ön lisans, lisans ve yüksek lisans mezunları bulunmaktadır. Katılımcıların eğitim durumları incelendiğinde; siber suç mağduriyeti yaşamamanın eğitim durumu ile bağdaştırılamayacağı söylenebilmektedir. Bu durum siber suç tekniklerinin eğitim düzeyi fark etmeksizin, herkese hitap eden yapılarının olduğunun bir göstergesi olarak

kabul edilebilir. Katılımcıların mesleki farklılıkları incelendiğinde; diğer katılımcılara oranla siber suçların teknikleri hakkında daha fazla bilgi sahibi olan yazılım geliştirme uzmanlarının dahi siber suç mağduriyeti yaşamış oldukları göze çarpmaktadır. Dolayısı ile siber suç mağduriyeti yaşama potansiyelinin meslek ile ilişkilendirilemeyeceği yorumu yapılabilmektedir. Rutin aktiviteler teorisi bu sebepler ile her bireyi potansiyel mağdur olarak kabul etmektedir, çünkü siber suçlar belirli özelliklere sahip olan bireylerde değil toplumun genelinde gözlemlenebilmektedir.

Elde edilen verilerden yola çıkılarak siber suç mağduriyeti yaşamanın cinsiyete dayalı olmadığına kanaat getirilmiştir. Kadın ve erkek katılımcılar arasında internet kullanım süresinde dikkate değer bir farklılık gözlemlenmemiştir. Süre çerçevesinden bakıldığında bir fark gözlemlenmemiş olsa da mülakat süreçleri dikkate alındığında kadın ve erkekler arasında internet kullanım amaçlarının değişkenlik gösterdiği saptanmıştır. Dolayısı ile cinsiyet faktörünün, mağduriyet yaşanan siber suç çeşidi üzerinde etkili olduğu sonucuna varılmıştır. Kısacası günlük internet kullanım süresindeki artışın mağduriyet potansiyelini genel olarak arttırdığı ve internet kullanım amaçlarındaki farklılıkların da mağduriyet çeşidini şekillendirdiği ortaya çıkmıştır.

Cinsiyete bağlı olarak internet kullanım sıklığı detaylı şekilde incelenecek olduğunda; erkek katılımcıların 8'i, kadın katılımcıların ise 7'sinin internet kullanım süresinin 5 saatin üzerinde olduğu görülmektedir. Kadınların erkeklere oranla internet kullanım sürelerinde neredeyse fark olmadığı belirtilebilir. Dolayısı ile katılımcıların %75'inin günün 5 saat ve üzerini internet kullanımı ile geçirdikleri ifade edilebilir. Bu durum internette geçirilen sürenin artmasının siber suç mağduriyeti yaşamada etkili bir faktör olduğu sonucunu içermektedir. Rutin aktiviteler teorisinin ele almış olduğu zaman faktörünün önemi siber suçlarda belirgin roldedir. İnternette geçirilen sürenin artması, dikkatsizce yapılabilecek tıklamalara zemin hazırlamaktadır. Geçirilen sürenin azalması ya da daha dikkatli internet kullanımı sonucunda mağduriyetlerde azalma görülebilir. Öte yandan; kullanım sürelerinde fark olmamasına rağmen kadın ve erkeklerin internet kullanım amaçlarındaki farklılıklar mülakat sorularına verdikleri cevaplardan daha net bir şekilde anlaşılabilir.

Çalışma saatlerinde bilgisayar üzerinden kullanıyorum, çalışma saatleri dışında da ekstra yapmam gereken işlerim var ise yine bilgisayar üzerinden devam ediyorum. Onun dışında sosyal medya, film, dizi o tarz işler için de cep telefonumu kullanıyorum. E-ticaret kullanıyorum sıklıkla, alışveriş olarak kullanıyorum. Bir de geçtiğimiz aylarda bir bitcoin denemem olmuştu. Merak ettim girdim, cüzi bir miktar oynadım hevesimi aldıktan sonra da çıktım. Pek ilgimi çekmedi. Oyun için de kullanıyorum. (K1, 25, Yazılım geliştirme uzmanı)

Yani akşam 6 da işten çıkıyorum, yemeğimi yedikten sonra genelde telefonumu elime alıyorum yatana kadar genelde telefonum elimde oluyor. Sık sık Instagram, Facebook, Twitter gibi sosyal medyayı çok kullanıyorum. 5 saatten fazladır. Sanal yatırım daha çok tabi... Dizi film arada bakıyorum, oyun için de kullanıyorum aynı şekilde. (K8, 30, İşçi)

2 ile 5 saat arası kullanırım. Sosyal medya kullanırım. Alışveriş yapıyorum evet alışveriş de yapıyorum hatta kripto işi de yapıyorum yani sanal para üzerinden şeyler yapıyorum. Oyun da

oynuyorum yani internetin her şeyinden yararlanıyorum. Telefonu daha çok kullanıyorum. (K11, 30, Öğretmen)

İnterneti günlük olarak 5 saatten fazla yani kullandığım oluyor tabi. Yani artık kullanmayan yok zaten sosyal medyayı da biz de kullanıyoruz. Sosyal medyayı kullanıyorum genelde haberleri falan takip ediyorum ne olmuş ne bitmiş onları öğrenmek için takip ediyorum yani günlük olarak. Alışveriş için pek kullanmıyorum. Oyun oynuyorum telefonumda indirdiğim oyunlar var onları oynuyorum. Bitcoin için de kullanıyordum sanal yatırım olarak yani. (K16, 37, İşçi)

Genel olarak tabii ki sosyal medya için kullanıyorum herkes kadar ben de. Oyun pek oynamam aslında ama bazen kafamı dağıtmak için oynadığım oluyor. Günde 5 saatten fazla internet kullandığımı eminim tabi ama hiç ölçmemiştim, ölçeceğim. Sanal yatırım için kullanıyorum, günümüzün dijital parası ben kullanmayan olduğumu da düşünmüyorum var ise de yakın zamanda eminim herkes kullanacak zaten. Alışveriş pek yapmam aslında ama bazen yaptığım oluyor. (K19, 37, Yönetici)

Yukarıda verilen, erkek katılımcıların kullanım amaçlarını içeren yanıtlarının yanı sıra kadın katılımcıların yanıtları da aşağıdaki gibidir. İnternet kullanım amaçlarında farklılıklar bulunduğu kadar ortak amaçların da var olduğu göze çarpmaktadır.

Günlük ortalama 8 saat internet kullanıyorum. Bunun yaklaşık 2.5, 3 saate yakın kısmını iş amaçlı yani işim gereği kullanıyorum. Yaklaşık 1 saatini, bu 1 saatin üzerine hiç çıkmadı, sosyal medya için kullanıyorum. Bunun dışında sadece araştırma amaçlı. Çok alışveriş yapmayı sevmiyorum. Şöyle sevmiyorum; hani günümüz şartları gereği çok fazla dolandırıcılık, o tarz şeyler olduğu için çok fazla sevmiyorum. Ama yine de kullanıyorum. Hemen hemen şu anda vaktimin çoğunu, yani internet bazlı vaktimin çoğunu telefon üzerinden yapıyorum. (K6, 40, Muhasebeci)

Yani, işim gereği interneti aktif olarak kullanıyorum aslında. Bu sebeple günlük 5 saatten fazla kullandığımı söyleyebilirim. Hani genelde araştırma ve sosyal medya, internet alışverişi, youtube için kullanıyorum. Telefon ve bilgisayar ile internet erişimimi sağlıyorum. (K15, 29, Yazılım geliştirme uzmanı)

İnterneti günlük olarak 5 saatin üzerinde kullanıyorumdur. Sosyal medya ve alışveriş için zaten hepimiz kullanıyoruz artık. Dijital çağın getirilerinden biri bu diyebiliriz. Bunun yanında dizi ya da film izlemek için de kullanıyorum fakat genellikle vaktim araştırma ile geçiyor. Makale okumaları ve gündemin takibi gibi şeyler vaktimin çoğunu alıyor diyebilirim. Belki günde 8 saati bile buluyordur internet kullanımım. (K20, 34, Öğretmen)

Erkek katılımcılar interneti; sosyal medya, oyun ve sanal yatırım için daha çok kullandıklarını belirtmişlerdir. Kadın katılımcılar ise sosyal medya, alışveriş ve araştırma için daha çok kullandıklarını belirtmişlerdir. Kullanım amaçları farklılaşmış olsa da sosyal medya kullanımı tüm katılımcılarda ilk sırada yer almaktadır. K20 sosyal medya için “Zaten internet hatta sosyal medya artık resmen günümüzün uyuşturucusu gibi, telefonlarımızda sabah katlığımızda bile sosyal medya hesaplarımızı kontrol ediyoruz.” yorumunda bulunmuştur. Ona göre internet ve sosyal medya günümüzde bağımlılık içeren bir alışkanlığa sebep olmuştur. Tüm katılımcıların sosyal medya kullanımı ve hatta sosyal medya hesapları üzerinden mağduriyet yaşamış olmalarına rağmen kullanmaya devam eden katılımcıların bulunması günümüzde sosyal medyanın vazgeçilmesi zor bir alışkanlığa dönüştüğünün kanıtı olarak da değerlendirilebilir.

Genel olarak bakıldığında; internet kullanım amaçları arasında sosyal medya kullanımının, alışveriş amaçlı kullanımın ve sanal yatırım için kullanımın ilk üç amacı oluşturduğu görülmektedir. Sosyal medya kullanımı tüm katılımcılarda söz konusu iken alışveriş amaçlı kullanımın daha çok kadınlarda, sanal yatırım amaçlı kullanımın ise daha çok erkeklerde olduğu ifade edilebilmektedir. Dolayısı ile sosyal medya kaynaklı mağduriyetlerden sonra; kadınlarda alışveriş temelli mağduriyet, erkeklerde ise sanal yatırım temelli mağduriyetlere daha sık rastlanmaktadır.

3.2. Temkinli Olma ve Önlem Alma

Katılımcılara; internet üzerinden kendilerine ait ne tür bilgileri hakkında paylaşımlar yaptıkları, internet ve uygulama kullanımları sırasında talep edilen bilgileri paylaşırken dikkatli olup olmadıkları sorulmuştur. Katılımcıların tümü sosyal medya kullandığından fotoğraf ve video paylaşımlarında bulunduklarını dile getirmişlerdir. Katılımcıların %50'si herhangi bir web sitesi veya link aracılığı ile kendisinden bilgi talep edildiğinde doldururken dikkatli davrandığını, gerekli görmediği bilgileri paylaşmadıklarını iletmişlerdir. Telefona indirilen uygulamalarda ise talep edilen izinlere onay verirken dikkatli davrandığını katılımcıların sadece %45'i ifade etmiştir.

Tabi sosyal medyada fotoğraf falan paylaşıyoruz. Orda hani çok hani özel bilginiz değil, yarı özel bilgileri paylaşıyoruz. Telefon numaramı paylaşıyorum. Kimlik bilgilerimi sosyal medyada paylaşmam, ona dikkat ediyorum. Son zamanlarda Whatsapp üzerinden bir kişisel bilgileri kullanım olayı çıkmıştı, orada da artık bir Whatsapp'ta da yazmamaya çalışıyoruz ama tabi unutuyoruz arada. Kaçırdığımız oluyor arada. Genelde uygulamayı o an kullanıp hemen faydalanma yönünde eğilim gösterdiğimiz için indirilen uygulamalarda istenen izinlere onlara pek dikkat etmiyoruz. (K2, 40, Bilgi işlem birimi müdürü)

Fotoğraf, video arada paylaşıyorum. Kimlik ve kredi kartı bilgilerimi, adres bilgilerimi paylaşıyorum. Güvenlik önlemi açısından paylaşmıyorum. Bilmediğim uygulamaları kabul etmiyorum, onay vermem ama bildiğim uygulama, hani kullanmış olduğum daha önce güvenilirliğine emin olduğum uygulamalar için izin veriyorum ama onun dışında bilmediğim bir uygulamaya izin vermiyorum. Alışveriş yaptıktan sonra kartı internet alışverişine kapatıyorum. (K4, 32, İşçi)

Yani şöyle söyleyeyim; internet alışverişini yaptığım için bütün kartlarımı kullandığım uygulamalarda neredeyse kayıtlıydı zaten. Kart numaram işte şeyleri direkt otomatik olarak oradan kartımı sürekli yanımda gezdirmediğim için oradan yapıyordum. Onun dışında böyle bazen şeylerde evet izinler çıkıyor işte fotoğraflara, ses kaydına falan izin ver gibisinden. Çok zorunlu kullanacağım bir program değil ise izin vermiyorum. Ama hani kullanmam gereken bir uygulama indirdiysem mecburiyetten veriyorum çünkü bu sefer uygulamayı kullanamıyorum. Düşünce paylaşmıyorum onun dışında fotoğraf ara ara paylaşıyorum. Kişisel ve kimlik bilgilerimi içeren paylaşımlar yapmamaya çalışıyorum. (K7, 26, Hemşire)

Sosyal medya kullandığım için tabi illa ki fotoğraf, video falan paylaşımlarım oluyor. Kimlik bilgilerimi paylaşmıyorum sadece. Onun dışında diğer bilgileri ister istemez paylaşıyoruz yani işte konumdur, kredi kartıdır, iletişimdir vs. paylaştığımız ya da işte kaydettiğimiz oluyor. Uygulamaları da zaten izin vermezsen kullanamıyorsun ki o yüzden hani gerçekten gerekli bir uygulama ise benim için, izinleri veriyorum çok da dikkat ettiğimi söyleyemem o konuda. (K9, 30, Teknisyen)

Katılımcıların sosyal medya kullanımında ve fotoğraf video gibi paylaşımlar yapmakta sorun görmedikleri sonucuna varılmıştır. Bunun yanı sıra kimlik ve kart bilgilerini paylaşma durumu söz konusu olduğunda daha dikkatli davrandıkları ve kendilerince birtakım önlemler almaya çalıştıkları gözlemlenmiştir. Akıllı telefonlara indirilen uygulamaların mikrofon, kamera, galeri, kişiler vb. özelliklere ve dosyalara erişim taleplerinde ise temkinli olmaya çalıştıkları dikkat çekmiş fakat indirilen uygulamalar, talep edilen izinler verilmediği takdirde çalışmadığı için kişisel bilgilerin paylaşımı ve erişimlerine onay vermek durumunda kaldıkları gözlemlenmiştir. Rutin aktiviteler teorisi çerçevesinden bakıldığında bu ve benzeri temkinsizlik içeren internet kullanım davranışları ile birlikte potansiyel mağdurun suçun oluşumuna zemin hazırladığı söylenebilir. Dolayısı ile suçun oluşumunda üçüncü unsur olarak potansiyel bir suçlunun da ortaya çıkması ile suç olgusu gerçekleşmektedir.

Katılımcıların verdikleri cevaplar incelendiğinde; K2 sosyal medya kullandığını ve fotoğraf paylaşımında bulunduğunu belirtmesinin yanı sıra kimlik bilgilerinin paylaşımında ise temkinli davrandığını dile getirmiştir. K4'te sosyal medya konusunda K2 ile benzer düşüncelere sahip olmasına rağmen farklı olarak kredi kartını internet üzerinden kullandığında önlem olarak işlem sonrasında kartını internet harcamalarına kapattığını beyan etmiştir. Aynı zamanda kimlik bilgilerini, adres bilgilerini ve kart bilgilerini paylaşmadığını ifade etmiştir. İndirdiği uygulamalarda ise daha önce kullanmış olup olmadığına, güvenilir olup olmadığına dikkat etmeye çalıştığını söylemiştir. Kart bilgilerini internet alışverişinde pratik olması sebebi ile internet tabanlı uygulamalarda kayıtlı tutmakta olduğunu bildiren K7, indirdiği uygulamalarda ise kullanımını zorunlu görmediğinde talep edilen izinleri onaylamadığını fakat izin vermediği takdirde uygulamaları kullanmadığı için bazı uygulamalarda onay vermek durumunda kaldığını ifade etmiştir. K9'da bu konuda K7 ile aynı fikirde olup, sadece kimlik bilgilerini paylaşmadığını fakat iletişim, adres, kredi kartı gibi bilgilerini paylaşmakta olduğunu iletmiştir. Tam tersi şekilde K15 ise izinler ve bilgi paylaşımı konusunda temkinli davrandığını, internet harcamalarını kendince bir önlem yöntemi olarak gördüğü sanal kart ile yapmakta olduğunu ve hatta günlük harcama limitinin bulunduğunu ifade ederek, akıllı telefonlara indirilen uygulamaların amacı dışında bilgilere ulaşmak istemesinin dikkat edilmesi gereken bir durum olduğunu savunmuştur. Son olarak K17'nin de K9 gibi kişisel bilgilerini ve kart bilgilerini paylaşmaktan çekinmediği göze çarpmaktadır.

Yapılan mülakatlarda katılımcılara dördüncü soru çerçevesinde; siber suç mağduriyeti yaşamadan önce çevrelerinde bu tarz mağduriyetlere şahit olup olmadıkları, siber suç hakkında daha önce herhangi bir bilgilerinin bulunup bulunmadığı ve bunun sonucunda herhangi bir önlem alma eylemleri gerçekleştirip gerçekleştirmedikleri sorulmuştur. Üç katılımcı dışında diğer katılımcıların daha önce siber suçlar hakkında bilgi sahibi oldukları ve çevrelerinden de duydukları ifadelerine rastlanmıştır. Daha önce siber suçlar hakkında herhangi bir şey duymadıklarını belirten

katılımcılar ise eğer duymuş olsalar ve konu hakkında biraz bilgileri olsa daha dikkatli olabileceklerini bildirmişlerdir.

Hayır, açıkçası daha önce iç duymamıştım. Çevremde de yaşanmamıştı bir benim başıma geldi. Ya gerçekten o kadar üzüldüm, çok üzüldüm... Ne yapacağımı ben de bilemedim. Daha önce duysam belki ne yapacağımı bilirdim. Bilgili birisi vardı çevremde bizi de o yönlendirdi yetkililere başvurmamız için yoksa siber suçlar diye bir birim olduğunu da öyle çok bilmiyordum. (K3, 38, Ev hanımı)

Ben yaşadım, ben yaşadığım için yaşamadan önce duymamıştım. Duymamıştım dediğim zaten üniversitedeydim. Üniversitede bundan 5 yıl önce bu kadar yaygın mıydı bilmiyorum ama daha yeni yeni yaygılaştığı dönemdi herhalde bana denk geldi. Benden sonra duyduklarım oldu. Yani çevremden ilk ben tecrübe ettim. Benden sonra duydum yani. Duymadığım için önlem de alamamıştım. (K11, 30, Öğretmen)

Çevresinde siber suç mağduriyeti yaşanmadığını ve kendisinin başına geldiğinde de ne yapacağını bilemediğini ifade eden K3, ne kadar üzüldüğünü ve birileri kendisini yasal başvurular için yönlendirene dek siber suçlar ile ilgilenen ayrı bir birimin bile olduğunu bilmediğini dile getirmiştir. K10 ise 5 yıl önce siber suçların belki de şimdiki kadar yaygın olmadığı için duymamış olabileceğini ve duymuş olsa önlem almış olabileceğini iletmiştir. K14 ise “Ben bu olayı yaşamadan önce etrafımda böyle bir olay yaşayan olmadığı için herhangi bir önlem alma gereği de duymadım açıkçası.” sözleri ile daha önce çevresinde bu tarz bir mağduriyet yaşayan kişiler bulunmadığını ve bu sebeple de önlem alma gereği duymamış olduğunu belirtmiştir. Bu sebeple yaşanan mağduriyetlerin çevredekiler ile paylaşılması, bu ve benzeri durumlarda bireylerin çevrelerini bilinçlendirmesi gerektiği empoze edilmelidir. Durumsal Suç Önleme Yaklaşımı bağlamında değerlendirildiğinde; yaşanan mağduriyetler konusunda çevrenin bilinçlendirilmesi potansiyel mağdur olan diğer internet kullanıcılarının temkinli davranmalarına ve rutin internet kullanım alışkanlıklarına etki edeceğinden, suç olgusunun oluşumunu engelleyebileceğinden ya da olasılığını düşürebileceğinden dolayı önem arz etmektedir. Öte yandan diğer katılımcılar ise daha önce çevrelerinde siber suç mağduriyetleri duymuş olmalarına rağmen önlem almadıklarını ya da kendileri yaşayana kadar önlemin ne kadar gerekli olduğunun farkına varmadıklarını dile getirmişlerdir.

Onunla ilgili şöyle; etrafımda kripto parası ile ilgilenen bir çevre var hemşire grubundan onların aracılığı ile duyduğum şey para kaybına yönelik. Nasıl oluyor bilmiyorum. Bayağı sifra inenler falan olmuş ama nasıl oluyor içeriğini bilmiyorum yani. Ben de kullanmadığım için önlem alma gereği de duymadım herhangi bir şeye karşı. (K12, 26, Hemşire)

Yani duymuştuk işte alışveriş yapmış gelmemiş falan işte arayıp polis gibi rol yapmışlar gibisinden çevremizde duyuyorduk yani parasını kaptıranları. Zaten ben onlar gibi para kaptırmadığım için, benim site, uygulama ile alakalı olduğu için benimki farklı yani o yüzden hiç böyle önlem falan almadık tabi. (K16, 37, İşçi)

Daha önce illa duyuyorduk zaten meslek gereği de mutlaka arkadaşlar söz ederken duyduğumuz oluyordu. Yani önlem, bilmiyorum hani şifreleri güçlü yapınca bir şey olmaz, önlem olur diye düşünüyorsun aslında. Ama tabi bu da tartışılır yani acaba gerçekten koruyucu mu diye. Daha da etkili önlemler almak gerekiyormuş demek ki. (K17, 33, Polis memuru)

Aslında daha önceden de duymuştum, sadece o an yakın çevrende olmadığı için mi desem önemsemediğin için mi desem önlem alma gereksinimi duymuyorsun. Önlem almamıştım ben de açıkçası. Çünkü yani bence önlem alsan da değişmiyor ki zaten. A şeklinde olmazsa B şeklinde mağduriyet yaşayabilirsin yine, bunun garantisi yok. (K18, 27, Mimar)

Bunu şöyle, bile bile lades gibi düşünebiliriz. Çünkü elbette duyuyorsun. Çevrenden duymasan da televizyonda, internette orada burada denk geliyorsun mutlaka yani böyle şeylere. Buna rağmen internet kullanmaya da devam ediyorsun önlem de almıyorsun. Ben almadım yani. Çünkü bana olmaz diye düşünüyorsun. Kaç kere duyduk mesela sanal yatırımlar hakkında tehlikeleri, mağduriyetleri ama kendimiz yaşayana kadar bir şey değiştirmedik önlem konusunda. (K19, 37, Yönetici)

Katılımcıların verdikleri cevaplar incelendiğinde K12'nin kendisinin kullanmamakta olduğu sanal yatırım uygulamalarına istinaden siber suç mağduriyetlerini duyduğu fakat bu alanda herhangi bir işlem yapmamasından kaynaklı olarak önlem alma gereksinimi hissetmemiş olduğu göze çarpmaktadır. Benzer şekilde K16'nın da mağduriyet süreçleri hakkında çevresinden bilgi almış olduğu fakat önlem konusunda herhangi bir eylem gerçekleştirmemiş olduğu görülmektedir. Kullanıcı şifrelerini güçlü olarak oluşturmasının yeterli bir önlem olacağını düşündüğünü ileten K17 ise daha etkili önlemlerin alınması gerektiğine dikkat çekmiştir. Bunun yanı sıra K18 önlem alınsa dahi siber suç tekniklerindeki farklılıklardan dolayı farklı bir şekilde mağduriyet yaşanabileceğini savunmuştur. K19'un beyanı ise kendisinin başına gelmeyeceğini düşünmesi nedeniyle önlem alma gereksinimi duymadığı doğrultusunda olmuştur.

Genel olarak bakıldığında, internetin günlük yaşamı kolaylaştırmasından ötürü, katılımcıların rutin internet kullanım aktiviteleri sırasında temkinli olmadıkları ve dikkatli davranmadıkları sonucu çıkarılmıştır. Dolayısı ile uzun saatler internet kullanımı gerçekleştiren bireylerin temkinli olmaması durumu karşılaşılabilecek siber suçları ve mağduriyet olasılığını yükseltmektedir. Bunun yanı sıra günümüzde sıklıkla kullanılan kamuya açık internet erişim ağları da motive olmuş siber suçlular için fırsatlar doğurmaktadır. Rutin Aktiviteler Teorisi açısından, bu fırsatlar potansiyel suçluları motive etmekte ve diğer unsurların da hazır bulunması sebebi ile siber suç mağduriyeti oluşumuna sebep olmaktadır. Temkinli olunmaması durumunda, kamuya açık olan internet erişim ağları kişisel veriler için tehdit oluşturmaktadır. Birceviz de (2019: 59) yaptığı bir çalışmada kamuya açık internet erişim ağlarının kullanımının günlük rutin haline geldiğini ve bu ağlarda geçirilen vaktin artması ile siber suç mağduru olma riskinin artması arasında doğrudan bir ilişki olduğunu saptamıştır. Kamuya açık olan bu ağlara bağlanıldığında kart bilgileri, kimlik bilgileri gibi önem arz eden bilgilerin kullanılmaması gerektiği iletilmektedir.

3.3. Damgalanma Korkusu ve Mücadele Süreci

Toplumsal hoş görmediği bir davranış sonucu damgalanma olgusu insanlık tarihi boyunca var olagelmıştır. Toplumdan topluma farklı şekillerde tezahürü mümkün olsa da bireylerde bir korku oluşturmıştır. Toplumdan dışlanacaklarını ya da damgalanacaklarını düşünen bireyler toplumun hoş görmediği eylemlerden kaçınmaya çalışmışlardır fakat bu elbette her zaman mümkün

olamamaktadır. Damgalanma çekincesine istinaden katılımcılara yaşadıkları siber suç mağduriyetini çevreleri ile paylaşp paylaşmadıkları, ilgili birimlere başvuruda bulunup bulunmadıkları sorulduğunda çoğunluğun cevabı damgalanmaktan çekindiklerine yönelik olmuştur. Günümüzde bu tarz suçlar ile mağdur olmak halk arasında cahillik, aptallık olarak nitelendirilmekte ve dikkatsizlik sonucu gibi algılanmakta olduğundan, mağduriyet yaşayan bireyler bu durumu çevreleri ile paylaşmakta çekince göstermektedir. Keza mülakatlar sırasında katılımcıların verdiği cevaplardan da damgalanma korkusunun ne kadar baskın olduğu gözlemlenmiştir. Bunun yanı sıra mülakat yapılmasını reddeden mağdurların ise birçoğunun yaşadığı mağduriyetin tekrar duyulmasından ve damgalanmaktan çekindiği için katılımcı olmak istemedikleri sonucuna varılmıştır. Katılımcıların ise verdiği cevaplardan damgalanma korkusunun mağduriyet süreçlerinde ne derece etkin bir faktör olduğu çıkarımı yapılabilir.

Başkalarına anlatmadım çünkü kendime yediremedim çünkü normalde ben böyle şeylerde gözü açık biri görünürüm ama hani böyle bir saflığa mı aptallığa mı nasıl düştüğümü ben bile bilmiyorum yani. Kötü bir dönemdi. Salak, buna inandın mı, bu da salakmış gibi damgalanma korkusu da var aslında insanlarda. (K4, 32, İşçi)

Kimse ile paylaşmadım, sadece ailem biliyor süreci birlikte yaşadığımız ve atlatmaya çalıştığımız için. Çünkü herkes “Sende mi inandın, nasıl dolandırıldın, bu kadar aptal olamazsın” gibi cümleler kuracaklardı eminim. Hiç dinlemek istemedim. Yaşayana kadar ben de böyle değerlendiriyordum. Yaşayınca görüyorsun hiç de öyle olmadığını aslında. Yadırıyacaklardı, eleştireceklerdi o yüzden paylaşmak istemedim. (K9, 30, Teknisyen)

Arkadaşlarım ile konuştum bu durumu ama ailem vs duyar diye bir bildirimde bulunmadım resmi olarak. Ama arkadaşlarımla konuştuk hani nasıl yapabiliriz nasıl kurtarabiliriz kaybımı diye ama bir sonuca varamadık maalesef. Tabi maddi olarak kayıp yaşamak üzdü. Tabi insan kendini aptal yerine konmuş gibi hissediyor böyle bir durumda, nasıl böyle bir şeye inandığımı ben de anlayamadım açıkçası. Ani ve dikkatsizliğime denk gelen bir şey oldu. (K13, 24, Hemşire)

Nasıl tarif edeyim ki yani öyle bir his yok tarif edebileceğim. Bir yandan korkuyorsun paran gitti diye. Bir yandan da üzgünsün, streslisin, endişelisin, çaresizsin de aslında. Kimseye de anlatamıyorsun falan zaten o çok kötü. Kendi kendine yiyip bitiriyorsun kendini ki nasıl çözeceğim bu işi diye. (K17, 33, Polis memuru)

Çevremden kimse ile paylaşmadım. Resmi kurum dışında ilk defa seninle paylaşıyorum diyebilirim. Yani öyle bir şey ki eşimle bile paylaşmadım. Bir damgalanma korkusu söz konusu evet. Çekince diyelim biz ona hatta. Kötü düşünüp, eleştirip kendi kendilerine yargılayacaklarından kimse ile paylaşmamayı seçtim. (K19, 37, Yönetici)

Yaşadıkları mağduriyet sürecini çevreleri ile paylaşmaktan çekinen katılımcılardan K4 karşılaştığı durumun kendisi ile özdeşleşmediğini, normal şartlarda bu tarz eylemlerde bulunmayan ve böyle bir mağduriyet yaşayabileceği düşünülmeyen birisi olması dolayısı ile çevresinin kendisini yargılayacağı düşünmüş olduğunu dile getirmek istemiştir. Yine aynı şekilde K8 de yadırıganacağından koktuğu için çevresi ile paylaşmakta zorlandığını ifade etmiştir. K9 ise mağduriyet yaşamadan önce bu tarz durumları yadırıgadığını fakat kendisi yaşadktan sonra bakış açısının değiştiğini belirtmiştir. K12 yaşadığı mağduriyeti paylaştığı taktirde kendisi ile dalga geçileceğini düşündüğü için paylaşmamış olduğunu söylemiştir. K13, kimse ile paylaşmadığı ve

çevresinden duyulmasından çekindiği için resmi kurumlara da başvuru yapmamış olduğunu belirtmektedir. Resmi kurumda görev yapan K17'nin de yaşadığı durumu kimse ile paylaşmamayı seçtiği dikkat çekmektedir. K19'un ise statüsünden kaynaklı olarak damgalanma çekincesi olduğu gözlemlenmiştir. Sonuç olarak; damgalanma korkusunun mağduriyet sürecindeki mücadelede olumsuz etki eden bir role sahip olduğu görülmektedir. Bireylerin damgalanmaktan korktukları için mücadele girişiminde bulunmamalarının söz konusu olabileceği gözlemlenmiştir.

Öte yandan çevrelerini bilinçlendirmek amacı ile çekinmeden yaşadıkları mağduriyeti paylaşan katılımcılar da bulunmaktadır. Yazılım geliştirme uzmanı olan K1; “Çevremdeki herkes ile paylaştım onların da başına gelirse diye önlemlerini alsınlar diye. Tabi ki haliyle tekrar mağduriyet yaşama endişemiz var ama bu da artık hayatımızın bir parçası olduğunu düşünüyorum ben.” sözleri ile yaşadığı mağduriyet sürecini çevresi ile paylaştığını ifade etmiştir. Bunun yanı sıra siber suçların ve getirdiği mağduriyetin artık günlük yaşamın bir parçası oldukları yorumunda bulunmuştur. Günlük yaşamda, dijitalleşme ile birlikte nasıl ki rutin aktiviteler ve alışlagelmişlikler değişim ve dönüşüme uğradı ise aynı şekilde günlük yaşamın bir parçası olan suç olgusu da dijitalleşme ile yeniden üretilerek dijital çağdaki yeni yaşam pratiklerinin arasında gündelik hayatın bir parçası olmuştur. Benzer şekilde K2'de teknolojik olarak sürekli gelişimlerin söz konusu olduğu günümüzde siber suçların ve mağduriyetlerinin sürekli karşılaşıcağımız bir durum olduğunu ve daha dikkatli olunması gerektiğini belirtmektedir. Siber suçlarda sürekli olarak yeni teknikler geliştirilmeye devam ettiği için bireylerin bilinçlendirilmesi gerektiğini ve önlem almaları gerektiğini ifade etmektedir.

Çevremle tabii ki paylaştım çünkü herkesi bilinçlendirmek lazım bu konuda. Önceden sadece virüs vardı virüs ile uğraşıyorduk, şimdi fidye çıktı. Daha neler çıkacak bilmiyoruz. Daha dikkatli olmaya mecburuz yani, bunu yapmaya mecburuz. Hani bu işte, bu işin nasıl emniyetini alıyorsak nasıl ki sunucularımızı kapalı bir odada tutuyorsak fiziksel olarak bir emniyetini alıyorsak, bu şekilde de almaya mecburuz yani. (K2, 40, Bilgi işlem müdürü)

Katılımcılara mağduriyet sürecinde resmi kurumlar ile mücadele edip etmedikleri, herhangi bir şikayette bulunup bulunmadıkları sorulmuş; şikayette bulunanların herhangi bir sonuç alamadıkları ve şikayette bulunmayanların ise herhangi bir sonuç alamayacaklarını düşündükleri gözlemlenmiştir. Dolayısı ile bu durum akıllarda siber suç mağduriyetinde resmi kurumlara başvurmanın anlamsız olduğunu, resmi kurumların bu alanda yetersiz olduğunu ve başvuru dahi sonuç alınamayacağı düşüncelerini doğurmaktadır. Diğer yandan, yaşadıkları mağduriyet karşısında resmi kurumlara başvuruda bulunan ve buna rağmen sonuç alamamış olan katılımcıların ikinci bir mağduriyet yaşadıkları yorumunda bulunulabilir. Başvuruda bulunmuş olan katılımcıların bu süreç hakkında ‘yıpratıcı’, ‘uzun süren’ şeklinde sıfatlarla tanımlamalarda bulundukları görülmektedir.

Bunun için de siber suçlara gittim, gerekli bütün formları doldurdum, bu bana yazılı mesaj atan kişilerin birebir hepsine ulaşıldı, onların raporu tutuldu. Mahkemeye vermek istediğimi hani

söyledim fakat çok iddialı konuştular konu ile alakalı, işte polisler çok uğraşırsınız dediler bize yani bir seneye öyle sonuçlanamaz kim bilir kaç sene sürer dediler öyle anlamsızlığa kadar götürdüler, ben de çok peşinde durmama kararı aldım... Vazgeçirdiler, destekçi olmadılar, yapabiliriz açabiliriz hakkınızı arayın gibi bir şey söylemediler. Kim bilir ne kadar sürer arkadaşım dedi bir sene de sürer on sene de sürer dedi. Sürse de senin eline hiçbir şey geçmez, bu tarz konuştular. (K3, 38, Ev hanımı)

Çevremdeki insanlardan da bazıları sonuçlandı bazıları sonuçlanmadı o yüzden ben de şu anda hiç bilmiyorum sonuç alabileceğimi. Sadece aşamayı takip edeceğim. Kötü bir durumdayım şu anda. 20 bin liram gitti çünkü. Az bir miktar görünebilir ama gerçekten güzel bir para sonuçta yani harcamadığım bir para elinden gidiyor. İster istemez çok üzücü bir şey. Çaresizlik hissediyorum tabi ki çünkü şu anda yetkililer de devrede ama çözülüp çözülmeceği muallak bir konu.(K7, 26, Hemşire)

Tabii ki hemen gidip ilgili her yere başvuru yaptık. Ama sonuç alamadık. Bulunamadılar yani ve giden bizim 300 bine oldu. Öyle bir yapmış ki adamlar ben yani işlemlerin bilgim dahilinde olmadığını kanıtlamıyorum ki. Kendim resmen adamlara bile isteye göndermiş gibi gözüküyorum paraları. Biraz malımız mülkümüz vardı olmasa ödeyemezdik de... Yani aylarca bekledik ama sonuç alamadık. Bir sürü de masraf çıktı başvuracağız da bir sonuç alacağız diye. Olmadı yani. (K9, 30, Teknisyen)

İşte resmi kuruma başvurduk ama sonuç yok yani daha. Ama eşim sağ olsun çok destek oldu yani yadırgamadı ama bir daha olursa kesin boşarım dedi onun korkusu var işte bizde de şimdi, tabi çocuk da olunca artık hataya yer yok yani. Sonuçlanmasını da hala bekliyoruz. Bu gidişle bir sonuç alabilecek miyiz onu da bilmiyorum. Siber suçlarda çalışan arkadaşım nadiren sonuçlandığını söylüyor. (K17, 34, Polis memuru)

Başvuruda bulundum, arkadaşım ile sürekli irtibat halindeyim takip ediyor davayı. Umudum yok aslında açıkçası sonuç çıkacağına dair de işte meblağ yüksek olduğu için bir umut diye başvuru yapıyorsunuz. (K19, 37, Yönetici)

Katılımcılar içerisinde K3, K7, K9, K17 ve K19 siber suç mağduriyetleri sonucunda resmi kurumlara başvuru yapmış fakat henüz sonuç alamamışlardır. Bu sürecin olumlu şekilde sonuçlanacağına dair inançları gözden geçirildiğinde katılımcıların yaşadıkları mağduriyetin çözüme kavuşacağına inanmadıkları gözlemlenmiştir. K3 başvurusunu yaptıktan ve gerekli incelemeler yapıldıktan sonra dava açmak istediğini ilettiğinde kendisini orada çalışan memurların sonuç alamayacağını ve çok uzun süre uğraşacağını ileterek vazgeçirdiklerini aktarmıştır. K7, çevresinde sonuç alamaya siber suç mağdurlarının bulunduğunu ve kendisinin de sorununun çözüme kavuşacağı konusunda emin olamadığını ifade etmiştir. K9 ise kart bilgilerinin ele geçirilmesinden dolayı yaşadığı siber suç mağduriyeti sonucu 300 bin Türk lirası tutarındaki kaybına yönelik açtığı davadan herhangi bir sonuç alamadığını ve bunun sonucunda ödemek zorunda kalmış olduğunu belirtmiştir. K17, sonuç alıp alamayacağından emin olamadığını iletmekte ve K19'un açıklaması da bunu destekler niteliktedir. Resmi kurumlara başvuruda bulunarak mağduriyetlerini gidermeye yönelik arayışta bulunan katılımcıların bu başvurulardan herhangi bir sonuç alamayacaklarına yönelik inançları olduğu gözlemlenmektedir. Bu durum hem siber suçların yasalarda yeni yer almaya başlaması ile hem de tespit edilmesi güç olan iz ve kanıtlar içermesi ile ilişkilendirilebilir. Fakat gerçek şu ki; siber suç mağduriyeti yaşamış olan bireyler üzerine istatistiksel bir çalışma yapılmak istendiğinde birçok kişi karanlık sayı olarak kalacaktır.

Bu durum öncelikle bireylerin resmi kurumlara başvurmaya yönelik çekincesinden ve ikinci olarak da sonuç alamayacaklarına dair inançlarından kaynaklanmaktadır. Çevrelerinde artan siber suç mağduriyetleri karşısında sonuç alamamış olan bireylerin de artış göstermesi diğerleri için olumsuz birer örnek teşkil etmektedir.

Katılımcılardan bazıları ise yaşadığı mağduriyet sonucu resmi kurumlara başvurmama sebebini çevresindeki bireylerin konu hakkında yaptıkları olumsuz yorumlar ile ilişkilendirmişlerdir. Sonuç alamayacağını söyleyen yakınları dolayısıyla başvuruda bulunmadıklarını iletmışlerdir. Bu durum bireylerin çevrelerinden etkilendiğinin bir göstergesi olarak kabul edilebilir. Katılımcıların, yukarıda çevreleri tarafından damgalanmaktan koktuklarına yönelik verilen söylemleri ile aşağıdaki söylemler bütüncül olarak incelendiğinde çevre etkeninin siber suç mağduriyeti sürecindeki güçlü rolü göze çarpmaktadır.

Şikayet etmedik. Çünkü ben araştırdım bir sonuç çıkmadı. Yani bazı arkadaşlarıma sordum, yurt dışında olduğu için hiçbir şey yapılamaz Türkiye’den. Çünkü verdikleri numara, dekontlar vs. hepsi yurt dışı üzerinden ilerliyor. Hani onlar da şey diyor; biz sizi dolandırmadık, siz şu meblağı yatırsanız biz zaten parayı yollayacağız size. Onlarında o açıklaması olduğu için hiçbir şekilde yasal olarak bir şey yapılmıyor, adamların şirketi yasal gözüküyor. Yaptırımı olacağını düşünmediğim için resmi kurumlarla mücadele etmedim. (K4, 32, İşçi)

Türkiye’de bazı şeyler gerçekten çok çözümsüz. Yani bizim adalet sistemimiz açıkçası çok adil bir ortamda çalışmıyor. Mağdursunuz ve mağduriyetinize hiçbir şekilde çözüm sağlayamıyorsunuz... Yani açıkçası kendinize olan kızgınlık zaten bunları perçinliyor. Birkaç kişiye sordum polis arkadaşlardan da sordum hatta ya abla çözüm sağlayamazsın, koşturduğunla kalırsın boş ver gitsin dediler açıkçası böyle kaldı. (K6, 40, Muhasebeci)

Açıkçası çevremden duyduklarım doğrultusunda herhangi bir sonuç alamayacağımı düşündüm. Hani o sebeple de başvurma gereği duymadım. Yani benim açımdan daha yıpratıcı olacaktı takibi falan. Sonuç da alabileceğin kesin değil, o yüzden başvuru yapmamayı tercih ettim diyebiliriz. (K20, 34, Öğretmen)

Katılımcılardan K4, arkadaşları ile görüşmüş ve mağduriyetinin sonuçlanamayacağı konusunda duyumlar almış olduğu için yasal başvuruda bulunmamıştır. Aynı zamanda yaptırımı olacağını düşünmediğini de dile getirmiştir. K6 yine aynı şekilde resmi kurumlara başvurmama sebebini etrafından herhangi bir çözüm sağlanamayacağı yorumları duymasına bağlarken aynı zamanda sonuç alamayacağına karşı olan düşüncesini de adalet sistemi ile ilişkilendirmiştir. Adalet sistemi içerisinde bu tarz suçların henüz tam olarak yer edinmemesinden kaynaklı bir boşluk olduğunu ifade etmek istemiştir. K20 ise çevresinden duydukları doğrultusunda hem sonuç alamayacağını düşündüğünden hem de sürecin yıpratıcı olmasından endişe ettiğinden başvuruda bulunmadığını ifade etmiştir. Dolayısı ile siber suç mağduriyeti yaşamış olan bireylerin çevresinden yapılan yorumları dikkate aldıkları, herhangi bir yaptırım uygulanmayacağı ve sonuç alamayacaklarına yönelik inançlarının baskın gelmesinden dolayı yasal başvurulardan çekindikleri gözlemlenmektedir. Bu durumda, yaşanan siber suç mağduriyetine karşı sonuç almış olan bireylerin bu süreci çevreleri ile olumlu şekilde paylaşmasının önemi ortaya çıkmış olmaktadır.

Bireylerin bu tarz paylaşımlarda bulunmasına yönelik teşvik edici bilgilendirmeler yapılması gerekmektedir.

Diğer katılımcılar ise direkt olarak herhangi bir sonuç alabileceklerine inanmadıkları için hiçbir yasal başvuruda bulunmadıklarını ve mücadeleye girişmediklerini iletmışlerdir. Siber suçların tespitinin güçlükler içermesi davaların sonuçlanamamasında ya da uzun süre içerisinde sonuçlanmasında en büyük etkeni oluşturmaktadır. Fakat bu durumun katılımcılar üzerinde sanki davalarda çözüm sağlanmasına yönelik çalışmaların yapılmadığı yönünde bir hissiyat doğurduğu gözlemlenmiştir.

Evet, yani kendi şirket içinde çözdük, çözdüğümüz şekil ödemeyi yaptık kendilerine. O zamanlar hani bu konuda ilgilenen bir emniyet birimi de bilmiyorum yoktu herhalde, yeni yeni başlanmıştı siber suç gibi. Çok da bilgimiz yoktu açıkçası varsaydı da, ilk olduğu için. Meblağ çok yüksek olmadığı için kendi içimizde hallettik ama tabi yüksek meblağlarda bir şey olsaydı o zaman daha resmi ya da resmi hani ne kadar faydası olabilir tartışılır ama en azından başvuru yapardık diye düşünüyorum. (K2, 40, Bilgi işlem müdürü)

Yani bu durum beni hem maddi hem manevi açıdan açıkçası yıprattı. Dediğim gibi; site sahte olduğu için benim gibi kandırılan çok kişi olmuş. Hani polise de gitsem, siber suçlara da gitsem yani çok üstüne düşüleceğini zannetmiyorum bu konunun. Bu sebeple gitmedim ben de açıkçası. Arkadaşlarıma anlattım, en azından dedim ben mağdur oldum onlar mağdur olmasın. Çevremi bilinçlendirmeye çalıştım. Yasal süreç izlemedim. Şu an bankaya olan kredi borcumu ödüyorum. (K8, 30, İşçi)

Ya resmi olarak bu şeyden sonra hiçbir başvuru yapmadım resmi olarak, tamamen kendim bireysel olarak işte firmayla görüştüm. Banka üzerinden hiçbir şey yapmadım veya tüketici hakem heyetine falan başvurmadım. (K10, 27, Askeri personel)

Kimseye de başvurmadım yani başvursan ne olacak sonuç alamazsın ki. Başvuranlara sorun bakayım kim sonuç almış parasını geri almış. Peşinde koşulmaz yani zaten hemen sizi suçluyorlar oynamasaydın diye. (K16, 37, İşçi)

Katılımcılardan K2 yaşanan siber suç mağduriyeti döneminde henüz bu suçlara yönelik herhangi bir işlem yapıp yapılmadıklarından emin olmadıkları ve bilmedikleri için resmi kurumlara başvuruda bulunmadıklarını ve sorunu kendi içlerinde çözmeye çalıştıklarını iletmıştır. K5 ise resmi kurumlara başvuruların bu tarz suçlar için sonuçlandırılmasının düşük ihtimalde olduğunu düşündüğünü beyan etmiştir. K8, yaşadığı mağduriyeti resmi kurumlara bildirdiği taktirde ilgilenileceğini düşünmediğinden dolayı başvuruda bulunmadığını aktarmıştır. K10 herhangi bir başvuru yapmadan kendisinin çözmeye çalıştığını ifade ederken, K16 ise sonuç alamayacağından emin olduğu için yasal yollara veya resmi kurumlara başvurmamış olduğunu dile getirmiştir. Dolayısı ile yaşanan mağduriyetler karşısında bireylerin kendilerince çözüm üretmeye çalıştıkları ve resmi yollara tam anlam ile güvenemedikleri saptanmıştır. Bunun en büyük sebebinin ise siber suçlar ile yasal mücadele konusunda katılımcıların bilgi eksikliğinin olduğu gözlemlenmiştir. Aynı zamanda çevreden fazlası ile etkilenme, damgalanma korkusu, yeterince araştırmama gibi faktörlerin de bulunduğu dikkat çekmiştir.

3.4. Olumlama Yaklaşımı ve Kadercilik

Bireyler yaşadıkları kötü deneyimleri olumlama ihtiyacı duymaktadırlar. Yapılan mülakatlarda katılımcılardan yaşadıkları siber suç mağduriyetinden söz etmeleri istendiğinde; daha kötüsü de olabilirdi, yaşanacağı varmış, kader, kısmet gibi kelimelerin sıkça kullanıldığı gözlemlenmiştir. Dolayısı ile katılımcıların yaşamış oldukları mağduriyet sürecini olumlamaya¹ çalıştıklarından söz edilebilir. Olumlama yaklaşımı; olumsuz bir durumu pozitif düşünceler ile olumlu şekilde yeniden kurgulamak olarak tasvir edilebilir. Katılımcıların tümünde bu davranışın hakim olduğu gözlemlenmiştir. Bu davranışa etki eden en büyük faktörün ise damgalanma korkusu olduğu yorumu yapılabilir.

Sonuç aslında alamadık hani bizi memnun eden tarafı şu sonuç kısmı; şifrenin yüzde yetmiş, yüzde seksen oranında çalışması ve şöyle bir durum var hani aldığınız şifre çözücü dosya, şifrelenen dosyaları eski haline getiren dosya yüzde yüz verimde çalışacak diye bir garanti de yok. Hani parayı ödemiş olmak sorunu tamamen çözmüş olduğunuz anlamına da gelmiyor. Geri döndürebildiğimiz yüzde yetmiş oldu. Yüzde yirmilik, yüzde otuzluk bir kayıp oldu mesela. Şifrelendiği zaman bazı dosyalar geri dönüşebiliyor bazısı dönüşmüyor yani yapısı bozuluyor. O sebeple geri döndürülmesi sıkıntı oluyor. Daha kötüsü de olabilirdi. Dosyalar hiç çalışmayabilirdi mesela. (K2, 40, Bilgi işlem müdürü)

Benim için tecrübe oldu bu. Tecrübeyi en azından ben yaşadım, şimdi benden hariç duyuyorum televizyonlarda 50 bin 100 bin kaptıranlar oluyormuş falan. En azından ben 180 tl gibi bir şeyde kurtuldum. Bu şekilde bir tecrübe kazandım. Daha kötüsü de olabilirdi, daha bilinçliyim şu anda... Zararın neresinden dönersek kar mıdır derler yoksa gideceği vardır bu kadar da kafî oldu tarzında yaklaştım yani. (K11, 30, Öğretmen)

Genelde zaaf olarak adlandırabiliriz bilmiyorum o an bir düşünemiyorsunuz sanki yani tutulup kalıyordunuz ve yanlış karar veriyorsunuz. Pişman oldum tabii ki sonradan çok fazla ve üzıldüm çünkü para kaybım vardı fakat ders oldu bu bana. Daha fazla da kaybım olabilirdi ama en azından bununla kurtuldum diye düşünüyorum yani bir nevi tecrübe kazanmak için para ödedim gibi düşünüyorum aslında. (K15, 29, Yazılım geliştirme uzmanı)

Katılımcılardan K2, yaşadığı mağduriyet için daha kötüsünün de olabileceğini dile getirmiştir. K11 de benzer şekilde daha kötüsünün de yaşanabileceğini fakat zararın neresinden dönülürse kar olduğunu belirtmiş ve yaşadığı mağduriyetin kendisi için tecrübe kazandırmış olduğunu, artık daha bilinçli olduğunu ifade etmiştir. Yaşadığı maddi kayıptan daha fazlasının da söz konusu olabileceğini ileten K15, bu durumun kendisini tecrübelendirdiğini ve tecrübe kazanmak için para ödemiş bulunduğunu düşünerek kendisini rahatlattığını bildirmiştir. Anlatılar dikkate alındığında katılımcıların yaşadıkları siber suç mağduriyetini olumlama çabasında oldukları görülmektedir. Bu durumun bir nevi, kendilerine mağduriyet yaşamış olmayı yakıştıramamalarından da kaynaklı olduğu fark edilmiştir. Öte yandan, diğer katılımcıların cevaplarından yaşadıkları mağduriyeti kaderciliğe dayandırdıkları gözlemlenmiştir. Yaşanılan

¹ Olumlama kavramı; halk arasında polyannacılık olarak da bilinen, her kötü durumun iyi tarafına odaklanmayı veya yaşanan olumsuz durumu olumlu gibi aksettirmeyi tasvir edebilmek amacı ile kullanılmaktadır.

durumun ellerinde olmadığını, yaşanacak olduğu için ve kendilerinin kaderlerinde böyle bir mağduriyet yaşamak olduğundan dolayı yaşamış olduklarını beyan etmeye çalışmışlardır. Aslında bu yaklaşımdan yine damgalanmaktan ne kadar korktukları ve suçu kadere attıkları sonucu çıkartılabilmektedir. Kısaca damgalanma korkusunun bireylerin yaşanan mağduriyete karşı olan yaklaşımlarına etki ettiği ifade edilebilir. Bu yaklaşıma istinaden aşağıda, yaşadıkları mağduriyeti kadercilik ile ilişkilendiren katılımcıların verdikleri cevaplardan örnekler paylaşılmıştır.

On beş, yirmi bin liraya kadar bir kaybım oldu maddi olarak. Psikolojik olarak hiç söylemiyorum. Manevi olarak daha kötü etkiledi. Tecrübe oldu diye düşünüyorum. Nasipte bu varmış, olacağı varmış oldu yani. (K4, 32, İşçi)

Valla birçok haber duyduğumuzda zaten televizyonlardan birçok şeyi izliyoruz. Yani bazen şöyle söylüyordum; ya bu insanlar aptal mı niye bunlara müsaade ediyorlar yani artık pes falan diyorduk böyle ama bazen hakikaten insan dumur oluyormuş. Başına gelince anlıyorsun... Basiretiniz mi bağlanıyor yoksa artık hani o nasibinizde mi çıkacak onu tam bilemiyorsunuz ama ben genelde insanları ya bu kadar da aptallık olmaz şeklinde değerlendiriyordum. Birkaç kez başıma gelince bunun aptallık derecesi değil de, yani muhtemelen bir basiret olayı diyorum. Çıkacağı varmış bir şekilde sanırım, ondan dolayı diyorum. Yani kader kismete bağlıyorum açıkçası durumu. (K6, 40, Muhasebeci)

Tabi maddi olarak kayıp yaşamak üzdü. Tabi insan kendini aptal yerine konmuş gibi hissediyor böyle bir durumda, nasıl böyle bir şeye inandığımı ben de anlayamadım açıkçası. Ani ve dikkatsizliğime denk gelen bir şey oldu. Olacağı varmış diyelim. İyi oldu, tecrübe kazandık diyelim. Tecrübe kazanmak için yaşayacağımız varmış demek ki. (K13, 24, Hemşire)

Uzun süre beni zorladı tabi maddi kayıp yaşamış olmak ama biraz da kader aslında, yaşayacağımız varmış. Büyük bir tecrübe oldu mu dersiniz evet tecrübe oldu onu da zaten yaşamadan öğrenemezsiniz ki. Tecrübe gibi düşünüyorum ben bu talihsizliği. Kader, kismet diyorum. (K20, 34, Öğretmen)

Katılımcılardan K4 yaşadığı durumun nasibinde olduğunu, benzer şekilde K6 ise yaşadığı maddi kayıptan dolayı bunun kendisinden zaten çıkacağının var olduğunu ve o sebeple gerçekleşmiş olduğunu beyan etmişlerdir. K9 da diğerleri ile benzer şekilde kader ile ilişkilendirmiş ve yaşadığı bu durumun aynı zamanda kendisine tecrübe kazandırdığını ifade etmiştir. K13 ve K20'de tıpkı K9 gibi yaşadıkları mağduriyetin kendilerine tecrübe kazandırdığını belirterek bu olumsuz durumun kendileri için olumlu olan tarafına işaret etmişlerdir. Kısaca özetlenecek olduğunda; katılımcılar bu ifadeler ile yaşadıkları durumun aslında ellerinde olmadığını, yaşanması gerektiği için yaşanmış olduğunu, yani daha büyük bir güç vesilesi ile meydana geldiğini, iradeleri dışında gerçekleştiğini ve kendi kabahatleri bulunmadığını ifade etmek istemişlerdir. Dolayısı ile şu çıkarımda bulunulabilir; bireyler damgalanmaktan çekindikleri için yaşadıkları siber suç mağduriyetlerini kendi dikkatsizliklerine, rutin internet kullanım alışkanlıklarına ya da bilinçsizliklerine dayandırmak yerine; Rutin Aktiviteler Teorisi'nin savunularının aksine, ellerinde olmayan bir güce dayandırmayı seçerek üzerlerinden sorumluluğu atmaya çalışmaktadırlar. Psikolojik ve bireysel etkenlerin de var olduğu gerçeği söz konusu olsa da daha önce de ifade edildiği gibi bu yaklaşımlara sebep olan en büyük etkenin damgalanma korkusu olduğu göze çarpmıştır. Sonuç olarak bu çalışmada yaşanan mağduriyet durumlarında ve bu

süreçlerin paylaşımında damgalanma korkusunun mağdurlar üzerindeki etkileri belirgin şekilde ortaya çıkmıştır.

3.5. Rutin İnternet Kullanım Alışkanlığına Etkiler

Gündelik yaşam içerisinde rutin eylemlerin birçoğunun gerçekleşmesini sağlayan ve kolaylaştıran internet kullanımından vazgeçebilmek pek de mümkün bir davranış olarak değerlendirilememektedir. Market alışverişinden fatura ödemelerine kadar ve hatta ev temizliğine kadar neredeyse tüm eylemler internet temelinde gerçekleştirilmeye başlanmıştır. Dolayısı ile bu gibi durumlar, internetin gündelik yaşamın vazgeçilmez bir parçası halini almasını sağlamıştır. Yapılan mülakatlarda katılımcılara; yaşadıkları siber suç mağduriyeti sonucunda internet kullanım alışkanlıklarında değişiklikler olup olmadığı sorulmuş, katılımcıların siber suç mağduriyeti yaşamalarına rağmen çoğunlukla internet kullanım sıklıklarında herhangi bir değişim olmadığını ya da sıklık olarak değişmediğini fakat içerik olarak değiştiğini belirttikleri gözlemlenmiştir.

İnternet kullanım alışkanlığında bir değişim olmadı, olaya şöyle bakıyorum yani yolda yürürken cüzdanınız çalındı yine aynı endişeyi duyabilirsiniz ama bu çalınmayacağı anlamına gelmez ama hani kendinizce önlem alırsınız. (K1, 25, Yazılım geliştirme uzmanı)

İnternet kullanımında bir değişiklik yapmadı ama dediğim gibi sayfalardan, şans oyunlarından, bahislerden o tarz sayfaların hepsini hayatımdan çıkardım. Bakmıyorum bile. Diyorum ya devletin bile vermiş olduğu yasal sayısal loto onlara bile yanaşmıyorum. İnternet kullanımında da bir değişiklik yaratmadı yani. Aynı şekilde filmidir, dizidir izlemeye devam ediyoruz. Ama internette alışverişlerimde tabii ki azalma oldu, sıfıra indi diyebiliriz. (K4, 32, İşçi)

İnternet kullanım süremde en fazla 1 saat oynamıştır... çünkü hala sosyal medyayı kullanıyorum. Hayatın bir parçası diyebiliriz gerçekten çünkü herkes orda insanları takip ediyor kim nerede ne yapıyor gibisinden. Bu çağda birbirimizden bu şekilde haberdar oluyoruz aslında yani. (K7, 26, Hemşire)

Ya internet kullanım alışkanlığında hani pek bir kayıp olmadı öyle söyleyeyim. Tekrar aynı vakti ben internet kullanarak geçiriyorum. (K10, 27, Askeri personel)

İnternet kullanımını azaltmanın gereksiz olduğunu düşünen K1, aynı zamanda önlem olarak internet kullanım sıklığını azaltsa bile bu durumun oluşabilecek herhangi bir siber suç mağduriyetini kesin olarak engelleyeceği anlamına gelmediğini savunmaktadır. Kullanım sıklığında bir değişikliğin söz konusu olmadığını belirten K4 ise internet kullanımındaki amaçlar ile içeriğin değiştiğini ve artık tehlikeli olduğunu düşündüğü bazı sanal ortamlarda eskisi kadar vakit geçirmediğini ifade etmiştir. Yaşadığı mağduriyet sonucu internet kullanım süresinde en fazla bir saat kadar oynama olduğunu dile getiren K7 ise hala sosyal medyayı kullanmaya devam ettiğini ve bunun hayatın bir parçası olduğunu dile getirmiştir. Verilen cevaplardan elde edilen verilere göre katılımcılar internet kullanım sıklıkları ile yaşadıkları siber suç mağduriyetlerini ilişkilendirmemiş, dolayısı ile genel olarak internet kullanım sıklıklarında belirgin bir değişim söz konusu olmamıştır. Aşağıda, internet kullanım sıklıklarında değişiklik olmasa bile kullanım

amaçlarında ve kullanım içeriklerindeki değişimleri aktaran diğer katılımcıların cevaplarından örnekler verilmiştir.

Daha çok bu sefer kendimi bilinçlendirmek için daha güzel sitelerde olmaya karar verdim... Belki saat olarak değişmedi ama içerik olarak değişti. (K8, 30, İşçi)

Herhangi bir değişime sebep olmadı, yine aynı sürede internet kullanımım devam ediyor. Sadece alışveriş yapmamaya dikkat ediyorum böyle ortamlardan. Çünkü internet hayatın bir parçası yani. (K13, 24, Hemşire)

Instagram kullanımında bir azalma yaşadım ama hani yine internet kullanımında aynı bir vakit geçirme oluyor. Zaten kısmak mümkün değil ki, her gün kullandığımız bir şey ve neredeyse her işimizi kolaylaştıran bir şey. (K14, 23, Hemşire)

Herhangi bir değişim yaratmadı, farkındalık kattı diyebiliriz. Çünkü yani artık internet her yerde. Yani hayatı kolaylaştıran bir şey yani tehlikeli yönleri var evet ama sonuçta birçok açıdan ve birçok yazılımla da hayatımız hep kolaylaştı. Sosyal medya zaten artık vazgeçilmezimiz çünkü çalışma saatlerimiz o kadar fazla ki ancak sosyal medya ile sosyalleşebilir olduk hani. Bu yüzden internet kullanım alışkanlığım değişmedi doğal olarak yani. (K15, 29, Yazılım geliştirme uzmanı)

Aslında kullanım sürem azalmadı, çünkü o olmasa başka bir şey ile o da yoksa başka bir şey ile hep dolduruyorsunuz ki yani geçirdiğiniz vakti. Zaten kullanmadan ne yapabiliriz ki internet yani bu. Hayatımızın içine işledi artık, mümkün değil ki taş devri gibi bir hayat yaşayalım. Var ki, geliştirilmiş ki kullanıyoruz işte. (K17, 33, Polis memuru)

Günlük internet kullanım sürelerinde herhangi bir değişiklik olmamasına rağmen kullanım amaç ve içeriğinin değiştiğini belirten K8 kendisini bilinçlendirmek için faydalı olduğunu düşündüğü daha farklı sitelerde zaman geçireceğini belirtmiştir. Katılımcılardan K12; yaşadığı mağduriyet sonrası internet üzerinden alışveriş konusunda henüz kendisini güvende hissetmediğini, kredi kartı bilgilerini paylaşmış olduğu site ve uygulamalardan bu bilgileri kaldırdığını dolayısı ile artık interneti alışveriş için eskisi kadar sık kullanmadığını ifade ederek kullanım amacındaki değişikliği dile getirmiştir. K13 de K12'yi destekler nitelikte yorumda bulunmuş ve aynı zamanda internetin hayatın bir parçası olduğu bu sebeple de kullanım sürelerinde değişiklik olmasının pek mümkün olmadığı düşüncesini paylaşmıştır. K14 de benzer şekilde, internet kullanımını sınırlandırmanın mümkün olmadığını ve günlük hayatı kolaylaştırdığını dolayısı ile her halükarda aynı sıklıkta günlük internet kullanımına devam ettiğini dile getirmiştir. K15 internetin tehlikeli yönlerinin bulunmasına rağmen hayatı kolaylaştırmasından ve artık her yerde var oluşundan dolayı bunu kısıtlamayacağını, kullanımında herhangi bir değişiklik söz konusu olmadığını ifade etmiştir. K16 diğer katılımcılardan farklı bir cümle kullanarak interneti bağımlılık olarak tanımlamıştır. K17 ise internetin sınırsız imkanlar sunuyor olmasından dolayı herhangi bir amaç için kullanmayı bıraktığında tamamen farklı bir amaç için tekrar kullanmaya başlayacağından internet kullanım süresinde değişim olmadığını ve hayatın içine işlediğini vurgulamıştır.

Katılımcıların anlatıları incelenecek olduğunda; internetin günlük yaşamın bir parçası olduğunu kabullendikleri ve interneti kullanmadan günlük rutin aktivitelerini yerine

getiremeyeceklerine inandıkları gözlemlenmiştir. İnternetsiz bir yaşamın mümkün olmadığı ana fikrini ortaya çıkaran veriler doğrultusunda siber suçların ve siber suç mağduriyetlerinin bireyler tarafından hayatın içerisinde olağan olarak algılanmaya başlandığının, dijital çağın kabullenilmiş bir olgu olduğunun sonucuna varılmıştır.

3.6. Katılımcıların Almış Oldukları Önlemler ve Siber Suç Mağduriyetini Önlemek İçin Önerileri

Katılımcılara yaşadıkları siber suç mağduriyetinden yola çıkarak diğer kullanıcıların mağduriyet yaşamamaları için ne gibi önlemler almaları gerektiğine yönelik soru yöneltildiğinde cevaplar; kişisel bilgilerin ve kart bilgilerinin paylaşılmamasına, şifrelerin güçlü belirlenmesine ve bilinmedik sitelere girilmeyip bilinmedik mesaj ya da maillere bakılmamasına yönelik olmuştur. Önlem amacı ile internet kullanım süresinin azaltılmasına dair herhangi bir söylemde bulunulmamıştır. Bu durum katılımcıların internet kullanım süresini mağduriyet ile ilişkilendirmediklerini, internette geçirdikleri sürenin mağduriyetlerinin temelini oluşturduğunu kabullenmediklerinin göstergesi olarak kabul edilebilir.

Yani e ticaret için söyleyeyim mesela şey zorunluluğu getirilebilir; her alışverişte bir sms doğrulama kodu hani sms doğrulaması yapılmadan tutarın çekilememesi sağlanabilir. Kart bilgilerinin kesinlikle saklanmaması gerekir mesela trendyol falan bunları yapıyor, kartınızı otomatik kaydediyor. Ufacık bir kutucuk şeklinde, ya bilgi veriyor ama gözünüzden kaçıyor. Küçük bir yazı ile işaretli bir kurucuk ile kartınızı kaydetmenizi sağlıyor. Bunların yasal olarak siber güvenlikçiler tarafından ve bizim devletin belli başlı bürolarından bunların yasal olarak bence çıkartılması doğru olabilir. Bu şekilde bir önlem sağlanabilir. (K1, 25, Yazılım geliştirme uzmanı)

Sürekli şifrelerini güncellemeleri, belli sürelerde değiştirmeleri. Belli bilgilerini paylaşmamaları özellikle şifrelerdeki güvenlik sorularını, her yerde aynı şeyleri kullanmamaları... İşte kendilerince bir güvenlik mekanizması oluşturup farklı sitelerde farklı cevaplar verebilmeleri şekilde bir sistem olması gerekiyor. Ama ne yapılabilir yani yüzde yüz hiçbir şey olmuyor. Mutlaka bir yerden yine bir açık çıkacak, yine bir açık kapı bulacaklar yine girecekler ama ne kadar düşürebilirsek o kadar iyi. (K2, 40, Bilgi işlem müdürü)

Yani resmi olmayan hiçbir sayfa ile kesinlikle bilgilerini, kredi kartı bilgilerini, nüfus bilgilerini kesinlikle paylaşmasınlar. Özellikle bunlardan uzak duruyorum. Hiçbir şekilde kartımı kaydetmiyorum. Hiçbir sitenin resmi bile olsa hiçbir siteye kartımı kaydetmiyorum. Onun dışında hani geçekten ince eleyip sık dokusunlar internet konusunda çünkü siber suç gün geçtikçe daha da çoğalıyor azalma yok. Çünkü bir tuşla insanlar amerikadaki insanların hesabına bile girebiliyor buradan. (K4, 32, İşçi)

Bireylerin günlük rutin internet kullanımında, sitelerde ve uygulamalarda mağduriyetlerine yol açabilecek kötü amaçlı detayların yasal olarak devlet tarafından engellenmesi ve çıkartılması gerektiğini ifade eden K1, internet alışverişlerinde de sms doğrulamanın tamamen zorunlu olması gerektiği düşüncesini paylaşmıştır. Bu şekilde doğrulama ile birtakım mağduriyetlerin önüne geçilebileceğine inanmaktadır. K2 ise kullanılan şifrelerin güçlü seçilmesi ve sürekli olarak da güncellenmesi gerektiğini ifade etmiş fakat hiçbir önlemin siber suçlardan korunmak için yeterli olmadığını, sadece olasılığı düşürdüğünü belirtmiştir. K4’de resmi olmayan hiçbir sitede kişisel,

kimlik ve kredi kartı bilgilerinin paylaşılmaması gerektiğini, başka bir ülkeden bile bilgilerine erişilebileceğini bu sebeple de tüm kullanıcıların daha dikkatli olmaları gerektiğini vurgulamıştır.

Yaşadığı mağduriyet ile ilişkili olarak K5; “Yani şöyle şunu söyleyebilirim; hiç kimse bir başkasına bu kadar kolay para kazandıramaz. Bunun bilincine ulaştım. Bu tarz şeylerden uzak durmaya dikkat ediyorum yani artık. O yüzden herkes uzak durmalı.” yorumu ile siber suç mağduriyetleri ile kolayca para kaybedilebileceğini ifade etmektedir. Dolayısı ile dikkatli olunması gerektiğini vurgulamaktadır.

Dediğim gibi öncelikle bütün kartlarını kesinlikle e ticarete açık bırakmamalılar. Yapacakları alışveriş esnasında kartını zaten online üzerinden kartınızı hemen internete açıp hemen kapatabiliyorsunuz sadece 30 saniyelik bir işlem. Bu otuz saniyede işleme onay verdikten sonra hemen kartlarını kapatabiliyorlar. Bunu yapmalarını öneririm akabinde de çok büyük bir problem yaşayacaklarını zannetmiyorum. Ama ara ara yine kart detaylarını mutlaka kontrol etmeliler. (K6, 40, Muhasebeci)

Kart bilgilerinin kaydedilmemesini savunan K6’ya göre, mobil bankacılık sayesinde internet alışverişlerinde alışveriş yaptığı sırada kart kullanımına izin verildikten sonra tekrar iznin kapatılabileceğini ve bu durumun kredi kartı mağduriyetlerinin önüne geçebileceğini iletmiştir.

Bunun dışında; kendilerine ait kişisel bilgilerini hiçbir yerde paylaşmamalarını tavsiye ederim. İnsanlar artık gerçekten her şeyi her yerde kullanabilir pozisyona geldikleri için her şekilde dolandırıcılık olabilir. Atıyorum bu illa maddi olmak zorunda değil manevi de olabilir. Yani çok moda mesela instagram da şu anda fake hesaplar açılıyor, kişinin fotoğrafları kullanılıyor bu da bir dolandırıcılık ister istemez o yüzden dediğim gibi kişisel bilgilerimizi paylaşmamalıyız. Ama işte yaptık. (K7, 26, Hemşire)

Yani bilinmedik, bilmedik bir yerden link atıldığında tıklamayacaksınız. Direkt onu silip devam edeceksiniz çünkü bilmediğiniz yerden durduk yere niye link gelsin. Yani dolandırılmaya açık bir şey oluyor bir de internet dediğimiz çok büyük bir ağ. Yani ufak bir şey bile yolladıklarında telefonuna sen bilmiyorsan onu tıklama. Seni meraklandıracak bir şey durduk yere gelmez zaten sen kurcalamadıktan sonra. O geldikten sonra zaten bütün bilgilerini alıyor. Çok büyük bir ağ dediğim gibi yani internet, karışık bir ağ, bilmedik yerlerde gezmemek gerekiyor. Bunu söyleyebilirim. Ben de zaten aldığım önlemler bu şekilde, bilmediğim uygulamaları indirmiyorum telefonuma. Dediğim gibi global herkesçe bilinen resmi bir devlet tarafından kabul görmüş şeylerde takılıyorum, sitelerde takılıyorum. Bu şekilde önlemimi alıyorum yani temiz geziyorum böyle gizli saklı sitelerde uğraşmıyorum. (K11, 30, Öğretmen)

İnternet kullanımı sırasında tanımadığı birinden mesaj ile link vb. gelmesi durumunda kesinlikle açılmaması gerektiğini ifade eden K11’e göre resmi olmayan, bilinmedik sitelerden ve uygulamalardan kaçınmak gerekmektedir. Aşağıda verilen K14’ün yorumu da K11’in düşüncelerini destekler niteliktedir. K14 aynı zamanda herhangi bir uygulama vb. kayıt isteyen platformlarda zorunlu olmayan bilgilerin doldurulmaması gerektiğini ifade etmiştir.

Tabii ki bilmediğim, tanımadığım insanlardan gelen mesajları açmadan önce bir düşünüyorum neden böyle bir şey geldi diye. Buna daha çok dikkat ediyorum onun dışında tabii ki sosyal medya uygulamalarının biraz daha güvenliğe dikkat etmek gerektiğini düşünüyorum. Uygulamayı yapan kişilerinde bu knuda kullanıcıları destekleyecek daha güvenli ortamda sosyal medya kullandırabilecek tasarımlar yapmaları gerektiğini düşünüyorum. Kişisel bilgileri

kaydetmemek gerekiyor, bu konuda daha dikkatli olunması gerekiyor. Zaten birçok uygulamanın girişinde , uygulamaya kayıt esnasında her bilgi istenmiyor isteğe bağlı olmayan bilgilerin verilmemesi gerekiyor bence. (K14, 23, İşçi)

Yani aslında bu bir nevi siber güvenlik ve şöyle ki siber güvenlik çok kapsamlı bir konu kendi çapımda aldığım önlemler güvenmediğim şeylerden, sitelerden dosya veya uygulama indirmemek, virüs programları kullanmak, sosyal medya da bilinçli gezmek. Tanımadığım alışveriş sitelerinden alışveriş yapmamak vb. Yani bunlara dikkat etmeye çalışıyorum. Bence herkes bunlara dikkat etmeli de zaten çünkü ancak dikkat edersek kendimizi biraz koruyabiliriz. Zaten gerçi tamamen korunmak mümkün değil ama işte en azından önlemekte bir etken şeyler yani. (K15, 29, Yazılım geliştirme uzmanı)

Çok dikkatli olmak lazım gerçekten oyun moyun kesinlikle inanmamak lazım. Mesajlar linkler falan hiçbirine eğer beklemediğiniz bir şey ise sakın aldanmayın yani. Artık teknik bilgisi olan da olmayan da bu işin içinde... Tespiti de eski suçlar gibi kolay değil ki kim yaptıysa bulabilesin. Bu yüzden gerçekten internet hem güzel bir şey hem de kötü bir şey. Herkesin dikkatli olması öyle her bilgiyi paylaşmaması, her siteye her linke girmemesi gerekiyor. (K17, 33, Polis memuru)

Yazılım geliştirme uzmanı olan K15, güvenilmeyen sitelerden herhangi bir dosya indirilmemesi ve güvenilmeyen uygulamalardan kaçınılması gerektiğini belirtmiştir. Bunun yanı sıra virüs programları kullanılması gerektiğine değinmiştir. Alınacak tüm önlemlerin siber suçlardan tümüyle korumasa bile engelleyebilmesinde öneme sahip olduğunu ifade etmiştir. K17’de siber suçların tespitinin kolay olmamasından söz ederek, internet kullanımında dikkatli olunması gerektiğini vurgulamıştır.

Genel olarak bakıldığında; katılımcılar siber suç mağduriyetlerinden korunmak için kompleks bir yapıya sahip olan internette bilinmeyen herhangi bir siteye girilmemesini, çerezlerin ya da izinlerin kabul edilmemesini, kişisel bilgilerin ya da kart bilgilerinin paylaşılmasından kaçınılması gerektiğini belirtmişlerdir. Özellikle internet alışverişlerinde kart bilgisi paylaşımına dikkat edilmesi gerektiği üzerine yorum yapmışlardır. Öte yandan virüs programı kullanılması gerektiği ve şifrelerin güçlü seçilerek sürekli olarak güncellenmesi gerektiği ifade edilmiştir. Katılımcılardan hiçbiri internet kullanım süresinin azaltılması üzerine bir yorumda bulunmamıştır. İnternetin günlük yaşamın bir parçası olması sebebi ile kullanılması gerektiği fakat daha dikkatli olunması gerektiği ana fikri üzerinde bütüncül yorumlamalarda bulunmuşlardır. Bunun yanı sıra yasal mücadele göz ardı edilmemeli, mutlaka gerekli başvurular gerçekleştirilmelidir. Siber suçlar ile mücadele yöntemlerinin ve sürecinin gelişebilmesi açısından yaşanan mağduriyetler karanlık sayı olarak kalmamalıdır.

SONUÇ VE ÖNERİLER

Soğuk savaş dönemi ile birlikte ortaya çıkan internet, dünya üzerinde birçok değişim ve dönüşüme sebep olmuştur. Her türlü verinin internet ekseninde rakamlar ile kodlanarak işlenebilmesi dijital bir çağı beraberinde getirmiştir. Bu yeni çağ beraberinde; kültür, eğitim, suç gibi olguların yanı sıra günlük rutin aktivitelerin de dijitalleşmesini getirmiştir. Dijitalleşen suç olgusu mağduriyetleri ve dolayısı ile siber suç mağdurlarını ortaya çıkarmıştır.

Nitel tarzda ve fenomenolojik desende yapılmış olan bu araştırmada siber suç mağdurları ile yapılan mülakatlardan elde edilen verilere bakıldığında; yaş, cinsiyet, eğitim seviyesi ve meslek faktörlerinin siber suç mağduriyetleri ile ilişkilendirilemeyeceği ortaya çıkmaktadır. Siber suçlar sürekli olarak kendini yenileyen ve teknolojik gelişmelere ayak uyduran bir niteliğe sahip olduklarından alınan önlemlerin geçerlilikleri yeni bir siber suç tekniği geliştirilene kadar sürmektedir. Dolayısı ile herkesi kapsayabilen bir yapıları bulunmaktadır.

İnternet kullanım sürecinde temkinli olma ve önlem alma açısından elde edilen veriler incelendiğinde, katılımcıların bilgi paylaşımlarında yeterince dikkatli davranmadıkları ve çoğunlukla siber suçlara karşı önlem alma eyleminde bulunmamış oldukları sonucu ortaya çıkmıştır. Katılımcıların dikkatsiz olmasının ve önlem konusunda aksiyon almamalarının siber suç mağduriyeti yaşamalarında etkili bir faktör olduğu sonucuna varılmıştır.

Bunun yanı sıra veriler doğrultusunda; siber suç mağdurlarının damgalanma korkusu olduğu dikkat çekmiştir. Bu durum mülakat sürecinde de katılımcılara ulaşmayı zorlaştırmıştır. Yaşadıkları siber suç mağduriyeti konusunda mülakata katılmak istemeyen bireyler söz konusu olmuştur. Paylaştıklarında yadırganacaklarını düşünmüşlerdir. Katılımcılarda da aynı düşünce söz konusu olmuştur. Mülakat süresi boyunca yadırganacakları ve damgalanacakları konusunda yorumlarda bulunmuşlardır. Bu düşünceler sebebi ile katılımcıların yaşadıkları mağduriyeti çevreleri ile de paylaşmadıkları gözlemlenmiştir. Çevreleri ile paylaşmamalarının psikolojik olarak destek alamamalarına sebep olduğu ve mücadele için ne yapacakları konusunda bilinçlenme durumunda eksik kaldıkları ortaya çıkmıştır. Ailelerinin ve çevrelerinin duymasından çekinen katılımcıların maddi kayıplarına rağmen resmi kurumlara herhangi bir başvuruda bulunmadıkları da gözlemlenmiştir.

Katılımcıların yaşadıkları mağduriyet sonucunda resmi kurumlara başvuruda bulunmama ve mücadele etmeme gibi eylemsizliklerinin bulunduğu dikkat çekmiştir. Damgalanma korkusunun yasal olarak haklarını arayışlarında olumsuz bir etkisinin bulunduğu ortaya çıkmıştır. Aynı

zamanda katılımcıların birçoğu çevrelerinden de duydukları üzere, başvuruda bulunsalar bile sonuç alabileceklerini düşünmemiş ve başvuruda bulunmamışlardır. Başvuruda bulunmuş olan 5 katılımcının ise henüz bir sonuç alamamış oldukları görülmüştür. Bu durumda katılımcıların mücadele sürecinde ikincil bir mağduriyet yaşadıkları söylenebilir. Dolayısı ile katılımcılarda yasal bir sonuç alamayacaklarına yönelik genel bir algı oluşmuştur. Bu ortak bilinç yaşanacak diğer siber suç mağduriyetlerine de işleyeceğinden bu konuda bilinçlendirmeler yapılması gerekmektedir.

Veriler doğrultusunda; katılımcılarda daha kötüsünün de olabileceği ve yaşadıkları ile kurtulmuş oldukları inancının yanı sıra kadercilik eğilimleri gözlemlenmiştir. Yaşanılan mağduriyetleri olacağı varmış şeklinde değerlendirdikleri göze çarpmıştır. Aslında dikkatsizlikleri sonucu meydana gelen mağduriyetleri polyanacılık ve kadercilik eğilimleri ile olumlama çabasında oldukları ortaya çıkmaktadır.

Yaşanılan mağduriyetlere rağmen kullanıcıların internet kullanım alışkanlıklarında belirgin değişimler olmadığı sonucu ortaya çıkmıştır. Dolayısı ile mağduriyet yaşamalarına sebep olan rutin internet kullanım alışkanlıklarının değişmemesi durumu ikinci kez mağduriyetlerin yaşanma olasılığını artırmaktadır. İnternet aracılığı ile gerçekleştirilen günlük rutin aktivitelerin siber suç mağduriyetleri ile birebir ilişkili olduğu sonucu ortaya çıkmıştır. Sonuç olarak katılımcılar bu rutin aktiviteler sonucunda mağduriyet yaşadıklarından, mağdurun suça kendisinin sebebiyet vermekte olduğu çıkarımında bulunulabilir. Siber suçlarda mağdurun rolünün etkili bir faktör olduğu sonucuna varılmıştır.

Elde edilen veriler doğrultusunda katılımcılar çözüm önerisi olarak; kullanıcı hesaplarının şifrelerinin güçlendirilmesi ve sürekli olarak güncellenmesi gerektiğini, bilinmedik site ve uygulamalara karşı temkinli olunması gerektiğini, kişisel bilgilerin ve kart bilgilerinin herhangi bir yerde paylaşılmaması ya da dikkat edilerek paylaşılması gerektiğini iletmışlerdir.

Nihai olarak; siber suç mağduriyetlerinin genel olarak sosyal medya hesapları üzerinden işlendiği görülmektedir ve bu alanda önlemlerin artırılması, kullanıcıların bilinçlendirilmesi gerektiği kanaatine varılmıştır. Günümüzde bireylerin sosyalleşme ve kendileri hakkında bilgi paylaşarak görülme, bilinme arzuları doğrultusunda mağduriyetlerin ortaya çıktığı gözlemlenmiştir. Bunun yanı sıra kolay para kazanma arzusu da sanal yatırımlara ya da şans oyunlarına yönelmesine sebebiyet vermekte ve yüksek miktarda kayıplara yol açmaktadır. Özellikle erkeklerde bu tarz mağduriyetler söz konusu olurken, kadınlarda manevi mağduriyetler ya da alışveriş temelli mağduriyetler söz konusu olmaktadır. Bunun ile ilişkili olarak kadınların yatırım konusunda çekinceleri, temkinli davranışları ve güvensizlikleri sebep gösterilebilirken erkeklerin daha fazlasını kazanma arzularının baskın geldiği görülmektedir. Sanal yatırım dolayısı ile mağduriyet yaşamış olan erkek katılımcılarda, başka siteler aracılığı ile sanal yatırım yapmaya devam etme davranışı gözlemlenmiştir. Bu durumu her sitenin güvenilir olmadığı, güvenilir olan

sitelerde sanal yatırım yapılmasında bir sakınca olmadığı şeklinde olumlamaya çalıştıkları görülmektedir. Kısacası bireylerin rutin internet kullanım alışkanlıklarının mağduriyet yaşamalarına sebebiyet vermekte olduğu sonucu elde edilmiştir.



KAYNAKÇA

- Acun, Fatma (2008), “Küresel Rekabette Dijital Kültür”, **Hacettepe Üniversitesi Türkiyat Araştırmaları Dergisi**, (9), 11-46.
- Agger, Ben (2004), **The Virtual Self: A Contemporary Sociology**, Blackwell Publishing, United Kingdom.
- Akarşlan, Hüseyin (2011), **Bilişim Suçları, Bilişim Yoluyla İşlenen Suçlar ve Adli Bilişim Ayrımı**, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi - Güvenlik Bilimleri Enstitüsü.
- Akcan, Esra Alan (2014), “Ceza Hukukunda Mağdurun Korunmasına Yönelik Düzenlemeler”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, Özel Sayı, 16, 3949-3997.
- Akdağ, Polatkan (2009), **Siber Suçlar ve Türkiye’nin Ulusal Politikası**, Yayınlanmamış Yüksek Lisans Tezi, Polis Akademisi - Güvenlik Bilimleri Enstitüsü.
- Akıncı, Füsün Sokullu ve Dursun, Selman (2016), **Viktimoloji**, 3. Baskı, Beta Yayınları, İstanbul.
- Akkaş, İbrahim (2015), **Sanal Cemaatler**, 1. Baskı, Doğu Kütüphanesi Yayınları, İstanbul.
- Akmeşe, Zuhale ve Deniz, Kemal (2017), “Stalk, Benliğin İzini Sürmek”, **Yeni Düşünceler Dergisi**, (8), 23-32.
- Aktan, Ercan ve Çakmak, Veysel (2015), “Halkla İlişkiler Öğrencilerinin Sosyal Medyadaki Siber Zorbalık duyarlılıklarını Ölçmeye İlişkin Bir Araştırma”, **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, 3(2), 159-176.
- Akyeşilmen, Nezir (2018), **Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik**, 1. Baskı, Orion Kitabevi, Ankara.
- Alkan, Ersoy Özmen (2019), **Tehdit Algısının Toplumsal Değişmeye Etkisi**, Yayınlanmamış Doktora Tezi, İnönü Üniversitesi - Sosyal Bilimler Enstitüsü.

- Alp, Barış Emre (2018), **5237 Sayılı Türk Ceza Kanununda Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme Suçu**, Yayınlanmamış Yüksek Lisans Tezi, Çankaya Üniversitesi - Sosyal Bilimler Enstitüsü.
- Arık, Emel (2018), **Dijital Mahremiyet**, 1. Baskı, Literatürk Academia Yayınları, Konya.
- Ateş, Emre Cihan (2016), **Üniversite Öğrencilerinin Sosyal Ağlara İlişkin Tutumlarının Suç ve Suçla Mücadele Açısından Değerlendirilmesi**, Yayınlanmamış, Yüksek Lisans Tezi, On Dokuz Mayıs Üniversitesi - Fen Bilimleri Enstitüsü.
- Aykara, Aslıhan ve Özkan, Semra (2017), “Mağdur Hakları ve Gereksinimleri Bağlamında Engelli Mağdur Bireyler”, **Trakya Üniversitesi Sosyal Bilimler Dergisi**, 19(1), 143-165.
- Bacıoğlu, Seda Donat (2022), “21. Yüzyılda Çocukları ve Gençleri Bekleyen Siber Riskler”, **Psikiyatride Güncel Yaklaşımlar**, 14(1), 29-37.
- Bal, Hüseyin (2013a), **İletişim Sosyolojisi**, 1. Baskı, Sentez Yayıncılık, Bursa.
- _____ (2013b), **Suç Sosyolojisi**, 1. Baskı, Fakülte Kitabevi Yayınları, Isparta.
- Bargh, John ve McKenna, Katelyn (2004), “The Internet And Social Life”, **Annual Reviews in Psychology**, (55), 573-590.
- Baudrillard, Jean (2002), **Tam Ekran**, (Çev. Bahadır Gülmez), 2. Baskı, Yapı Kredi Yayınları, İstanbul.
- _____ (2011), **Simülakrlar ve Simülasyon**, (Çev. Oğuz Adanır), 6. Baskı, Doğu Batı Yayınları, Ankara.
- Bauman, Zygmunt ve Lyon, David (2013), **Akışkan Gözetim**, (Çev. Elçin Yılmaz), 3. Baskı, Ayrıntı Yayınları, İstanbul.
- Berkup, Sezin Baysal (2015), **Sosyal Ağlarda Bireysel Mahremiyet Paylaşımı: X ve Y Kuşakları Arasında Karşılaştırmalı Bir Analiz**, Yayınlanmamış Doktora Tezi, Ege Üniversitesi - Sosyal Bilimler Enstitüsü.
- Bezir, Çiğdem (2012), **Second Life Ortamında Tasarlanan Yabancı Dil Eğitimi: Öğretmen-Öğrenci ve Ortam Etkileşimi**, Yayınlanmamış Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi - Eğitim Bilimleri Enstitüsü.

- Bilek, Burak Tunç (2012), **Bilişim Suçları ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri**, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi - Bilişim Enstitüsü.
- Birceviz, Ferhat (2019), **Rutin Aktiviteler Teorisi Bağlamında Siber Suç Mağduriyeti**, Yayınlanmamış Yüksek Lisans Tezi, Milli Savunma Üniversitesi - Savunma Bilimleri Enstitüsü.
- Bostan, Barbaros (2007), **Sanal Gerçeklikte Etkileşim**, Yayınlanmamış Doktora Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.
- Branic, Nicholas (2016), "Routine Activities Theory", Wesley G. Jennings (Ed.), **Encyclopedia of Crime and Punishment**, John Wiley & Sons Inc. Publishing, United States, 1-3.
- Brennen, Scott ve Kreiss, Daniel (2016), "Digitalization", Eric W. Rothenbuhler (Ed.), **The International Encyclopedia of Communication Theory and Philosophy II**, John Wiley & Sons Inc. Publishing, United States, 1-12.
- Brenner, Susan (2010), **Cybercrime: Criminal Threats From Cyberspace**, 1. Baskı, Preager, California.
- Budak, Hatice (2016), **Yeni Çağ, Yeni Medya ve Mahremiyetin Yeni Sınırları**, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.
- Budak, Ömer Sıddık (2015), **Bilişim Öğrencilerinin Siber Suç Farkındalığı: Erzurum İli Mesleki ve Teknik Liseler Örneği**, Yüksek Lisans Tezi, Atatürk Üniversitesi - Eğitim Bilimleri Enstitüsü.
- Bullock, Karen vd. (2010), "Introduction", Ronald V. Clarke (Ed.), **Situational Prevention of Organised Crimes**, Willan Publishing, First Publish, United Kingdom, 1-17.
- Canbek, Nil Göksel (2009), **Üniversite-Toplum İşbirliğinde Öğrenen-Ders Yöneticisi Etkileşimi: Second Life (SL) Üzerine Bir Çalışma**, Yüksek Lisans Tezi, Anadolu Üniversitesi - Sosyal Bilimler Enstitüsü.
- Castells, Manuel (2008a), **Enformasyon Çağı: Ekonomi Toplum ve Kültür; Ağ Toplumunun Yükselişi**, (Çev. Ebru Kılıç), 2. Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

- _____(2008b), **Enformasyon Çağı: Ekonomi Toplum ve Kültür; Binyılın Sonu**, (Çev. Ebru Kılıç), 2. Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.
- _____(2008c), **Enformasyon Çağı: Ekonomi Toplum ve Kültür; Kimliğin Gücü**, (Çev. Ebru Kılıç), 2. Baskı, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.
- Clarke, Ronald ve Felson, Marcus (2008), **Routine Activity And Rational Choice**, Second Edition, Transaction Publishers, New Jersey.
- Clevenger, Shelly vd. (2018), **Understanding Victimology**, 1. Baskı, Routledge Publishers, New York.
- Cohen, Lawrence ve Felson, Marcus (1979), “Social Change and Crime Rate Trends: A Routine Activity Approach”, **American Sociological Review**, 44(4), 588-608.
- Çekiç, Burak (2006), **İnternet Aracılığı ile İşlenen Suçlar**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.
- Çingay, Arzu (2015), **Sosyal Medyanın Kiteselleştirici ve Yalnızlaştırıcı Etkisi**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.
- Çoban, Bahşende (2019), **Sosyal Medya Kullanımı İle Değişen Mahremiyet Algısı: Youtube Üzerine Bir İnceleme**, Yayınlanmamış Yüksek Lisans Tezi, Kocaeli Üniversitesi - Sosyal Bilimler Enstitüsü.
- Dalaylı, Feyza Ünlü (2018), **Orta Yaş Üstü Bireylerin Dijital Çağda İletişim Kurma Pratikleri: Sosyal Medya Bağımlılığı ve Sosyal İzolasyon**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.
- Das, Sumanjit ve Nayak, Tapaswini (2013), “Impact of Cyber Crime: Issues and Challenges”, **International Journal of Engineering Sciences & Emerging Technologies**, 6(2), 142-153.
- Dashora, Kamini (2011), “Cyber Crime in The Society: Problems and Preventions”, **Journal of Alternative Perspectives in The Social Sciences**, 3(1), 240-259.
- Debord, Guy (1996), **Gösteri Toplumu** (Çev. Ayşen Ekmekçi ve Okşan Taşkent), 1. Baskı, Ayrıntı Yayınları, İstanbul.
- Dolu, Osman (2009a), “Bir Fırsat Olarak Suç: Suçun Durumsal Belirleyicileri, Suç Fırsatları ve Rutin Faaliyetler Teorisi”, **Polis Bilimleri Dergisi**, 11(2), 1-30.

- _____ (2009b), “Rasyonel Bir Tercih Olarak Suç: Klasik Okul Düşüncelerinin Suçu Açıklama ve Önleme Kapasitesinin Değerlendirilmesi”, **Polis Bilimleri Dergisi**, 11(4), 89-120.
- _____ (2012), **Suç Teorileri: Teori, Araştırma ve Uygulamada Kriminoloji**, 4. Baskı, Seçkin Yayıncılık, Ankara.
- Dreyfus, Hubert (2016), **İnternet Üzerine**, (Çev. Metin Demir), 1. Baskı, Küre Yayınları, İstanbul.
- Ermeydan, Damla (2018), **Türk Ceza Kanununda Bilişim Suçları**, Yayınlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi - Sosyal Bilimler Enstitüsü.
- Eroğlu, Şahika (2018), “Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerinin Mahremiyet ve Kişisel Veri Algılarının Analizi”, **Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi**, 35(2), 130-153.
- Esen, Arzu (2018), **Sosyal Medyada Mahremiyetin İfşası: Namık Kemal Üniversitesi Akademisyenleri Üzerine Yapılan Bir Araştırma**, Yayınlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi - Sosyal Bilimler Enstitüsü.
- Felson, Marcus ve Clarke, Ronald (1998), “Opportunity Makes The Thief: Practical Theory for Crime Prevention”, Barry Webb (Ed.), **Police Research Series**, London.
- Felson, Marcus ve Eckert, Mary A. (2018), **Crime And Everyday Life: A Brief Introduction**, 6. Baskı, SAGE Publications, United States.
- Fidan, Serdal (2004), **Türk Dünyasında Sosyo-Kültürel Bütünleşme**, Yayınlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi - Sosyal Bilimler Enstitüsü.
- _____ (2011), **Küreselleşme Sürecinde Türkiye’de Gençliğin Kimlik Algısı: Üniversite Gençliği Üzerine Bir Araştırma**, Yayınlanmamış Doktora Tezi, Sakarya Üniversitesi - Sosyal Bilimler Enstitüsü.
- Gobble, MaryAnne M. (2018), “Digitalization, Digitization and Innovation”, **Research Technology Management**, 61(4), 56-59.
- Goffman, Erving (2018), **Günlük Yaşamda Benliğin Sunumu** (Çev. Barış Cezar), 2. Baskı, Metis Yayınları, İstanbul.

Gosling, Samuel ve Mason, Winter (2015), “Internet Research in Psychology”, **Annual Reviews in Psychology**, 66, 877-902.

Göçmen, Tuba Livberber (2018), **Toplumsal Yaşamda Bireylerin Mahremiyet Yönelimleri: Sosyal Ağ Kullanıcıları Üzerine Bir Saha Araştırması**, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.

Göktepe, Işıl Bilgehan (2013), **Gerçek Mekan, Sanal Mekan ve Kurumsal Kimlik İlişkisi**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi - Sosyal Bilimler Enstitüsü.

Güçlü, İdris ve Akbaş, Halil (2016), **Suç Sosyolojisi: Kavram, Teori ve Uygulama**, 1. Baskı, Seçkin Yayıncılık, Ankara.

Güneş, Alper (2015), **Bilişim Suçları ve İdarenin Hukuki Sorumluluğu**, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.

Güney, Hami (2008), **Sosyolojik Açından Çocuk Suçluluğu ve Nedenleri**, Yayınlanmamış Yüksek Lisans Tezi, Kırıkkale Üniversitesi - Sosyal Bilimler Enstitüsü.

Güngör, Mümin (2019), “Mağduriyetin Giderilmesi Açısından Uzlaştırma Kurumu İle Mağdur Hakları Tasarısının İncelenmesi”, **Yıldırım Beyazıt Hukuk Dergisi**, (2), 189-230.

Güngör, Necmi Murat (2007), **Yeni Türk Ceza Kanunu Kapsamında Bilişim Suçları ve Emniyet Genel Müdürlüğü Uygulamaları**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Üniversitesi - Sosyal Bilimler Enstitüsü.

Güzel, Ebru (2016), “Dijital Kültür ve Çevrimiçi Sosyal Ağlarda Rekabetin Aktörü: Dijital Habitus”, **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, 1(4), 82-103.

Hekimoğlu, Hande (2019), **Sosyal Ağlarda Mahremiyetin Dönüşümü: Instagram Örneği**, Yayınlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi - Sosyal Bilimler Enstitüsü.

İçli, Tülin Günşen (2007), **Kriminoloji**, 8. Baskı, Seçkin Yayıncılık, İstanbul.

İnci, Mehmet Akif vd., (2017), “Dijital Kültür ve Eğitim”, **Gazi Üniversitesi Gazi Eğitim Fakültesi Dergisi**, 37(2), 493-522.

İşliyen, Mustafa (2019), “Dijital Çağın Yeni Hastalığı: Dijital İstifçilik”, **Akdeniz Üniversitesi İletişim Fakültesi Dergisi**, (31), 404-420.

- İşman, Aytekin vd. (2016), “Sosyalleşmenin Dijitale Dönüşümü ve Dijital Benliğin Sunumu”, **Trt Akademi Dergisi**, 1/2, 608-619.
- Kalaman, Sefer (2016), **Sosyokültürel, Ekonomik ve Siyasi Boyutlarıyla Yeni Medyada Mahremiyetin Dönüşümü: Facebook Örneği**, Yayınlanmamış Doktora Tezi, Ege Üniversitesi - Sosyal Bilimler Enstitüsü.
- Kaplan, İsmail (2017), **Üniversite Öğrencileri Sosyal Medya Kullanıcılarının Mahremiyet Algısı**, Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi - Sosyal Bilimler Enstitüsü.
- Karaca, Mustafa vd. (2021), “Siber Mağduriyet: Kavramsal Bir Çalışma”, **Anadolu Akademi Sosyal Bilimler Dergisi**, 3(1), 177-191.
- Karagöz, Mehmet Can (2019), **Bilişim Sistemini Engelleme, Bozma, Verileri Yok Etme veya Değiştirme Suçu**, Yayınlanmamış Yüksek Lisans Tezi, Akdeniz Üniversitesi - Sosyal Bilimler Enstitüsü.
- Karagülle, Ayşegül Elif (2015), **Günümüzde Değişen Mahremiyet Algısının Sosyal Ağlar Bağlamında İncelenmesi**, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi - Sosyal Bilimler Enstitüsü.
- Kardaş, Selami (2017), **Sanal Kimlik ve Spiritüel İyi Oluşun Üniversite Öğrencilerinin Narsistik Eğilimlerini Yordayıcılığı**, Yayınlanmamış Doktora Tezi, Marmara Üniversitesi - Eğitim Bilimleri Enstitüsü.
- Kartal, Mustafa (2018), “Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme”, **Uluslararası Ekonomi ve Yenilik Dergisi**, 4(1), 1-18.
- Katoğlu, Tuğrul (2012), “Ceza Hukukunda Suçun Mağduru Kavramının Sınırları”, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 61(2), 657-693.
- Kılıç, Yavuz Selim (2007), **Çocuk Suçluluğuna Sebep Olan Sosyo-Ekonomik Faktörler**, Yayınlanmamış Yüksek Lisans Tezi, İnönü Üniversitesi - Sosyal Bilimler Enstitüsü.
- Kırcelli, Seher (2011), **Yeni İletişim Teknolojileri, Sanal Kamusalıklar ve Toplumsal Cinsiyet: Facebook’ta Genç Kadınların Kimlik İnşa Süreçleri**, Yayınlanmamış Yüksek Lisans Tezi - Sosyal Bilimler Enstitüsü.

- Kundi, Ghulam Muhammad ve Nawaz, Allah (2014), “Digital Revolution, Cyber-Crimes and Cyber Legislation: A Challenge To Governments In Developing Countries” **Journal of Information Engineering and Applications**, 4(4), 61-70.
- Lokke, Eirik (2018), **Mahremiyet: Dijital Toplumda Özel Hayat**, (Çev. Dilek Başak), 1. Baskı, Koç Üniversitesi Yayınları, İstanbul.
- McLuhan, Marshall (1994), **Understanding Media**, 1. Baskı, The MIT Press, London.
- McLuhan, Marshall ve Powers, Bruce R. (2001), **Global Köy**, (Çev. Bahar Öcal Düzgören), 1. Baskı, Scala Yayıncılık, İstanbul.
- Medin, Burak (2018), “Dijital Kültür, Dijital Yerliler ve Günümüzdeki Yeni Film Seyir Deneyimleri”, **Erciyes İletişim Dergisi**, 5(3), 142-158.
- Ngo, Fawn ve Paternoster, Ray (2011), “Cybercrime Victimization: An Examination of Individual and Situational Level Factors”, **International Journal of Cyber Criminology**, 5(1), 773-793.
- Olçay, Sümeyya (2018), “Sosyalleşmenin Dijitalleşmesi Olarak Sosyal Medya ve Resimler Arasında Kaybolma Bozukluğu: Photolurking”, **Yeni Medya Elektronik Dergisi**, 2(2), 90-104.
- Olofinbiyi, Sogo Angel (2022), “Cyber Insecurity in The Wake of Covid-19: A Reappraisal of Impacts and Global Experience Within The Context of Routine Activity Theory”, **Science Rise: Juridical Science**, 1(19), 37-45.
- Orta, Mesut (2015), **Bilişim Suçlarında Adli Analiz**, Yayınlanmamış Doktora Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.
- Örs, Özlem Dalkıç (2018), **Mahremiyet ve Instagram Mahremiyetinin İnsanın Yaşam Olgusuna Etkileri**, Yayınlanmamış Yüksek Lisans Tezi, Fırat Üniversitesi - Sosyal Bilimler Enstitüsü.
- Özalp, Ahmet (2020), **Suçlu Çocuk Algısı**, 1. Baskı, Çimke Yayınevi, Konya.
- Özdemir, Nihan Gümrükçü (2006), **Sanal Topluluklarda İzlenimi Yönetme**, Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi - Sosyal Bilimler Enstitüsü.

Özonur, Mesut (2013), **Sanal Gerçeklik Ortamı Olarak İkincil Yaşam (Second Life) Uygulamalarının Tasarlanması ve Bu Uygulamaların İnternet Tabanlı Uzaktan Eğitim Öğrencilerinin Öğrenmeleri Üzerindeki Etkilerinin Farklı Değişkenler Açısından İncelenmesi**, Yayınlanmamış Doktora Tezi, Mersin Üniversitesi - Eğitim Bilimleri Enstitüsü.

Öztürk, Ali (2015), **Yeni Medya Araçlarının Mahremiyet Algısındaki Dönüşüme Etkisi**, Yayınlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi - Sosyal Bilimler Enstitüsü.

Özüdoğru, Uğur (2010), **Siber Suçlar ve Mücadele Yöntemleri: Dünya Uygulamaları ve Türkiye İçin Çözüm Önerileri**, 1. Baskı, Bilgi Teknolojileri ve İletişim Kurumu, Ankara.

Pallı, Hayati (2008), **Türk Hukukunda ve Mukayeseli Hukukta Bilişim Suçları**, Yayınlanmamış Yüksek Lisans Tezi, Erciyes Üniversitesi - Sosyal Bilimler Enstitüsü.

Peker, Bekir (2010), **Bilişim Suçları ve Bilişim Güvenliğinin Ulusal ve Uluslararası Boyutu**, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.

Polat, Ahmet ve Gül, Serdar Kenan (2010), “Kriminoloji Araştırmalarında Mağdur Anketlerinin Yeri ve Önemi”, **Uluslararası İnsan Bilimleri Dergisi**, 7(1), 1290-1310.

Sağtaş, Saadet (2013), **Second Life Sanal Yaşam Dünyasında Girişimcilik: Avapreneurship (Avatar Girişimcilik)**, Yayınlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi - Sosyal Bilimler Enstitüsü.

Sarıyar, Hatice (2019), **Dijital Çağda Kimliğin Kavramsallaştırması ve Gerçeklik: Twitter Parodi Hesapları**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.

Seçkin, Mehmet Beyhan (2020), “Ceza Muhakemesinde Mağdur ve Şikayetçinin Hakları”, **Uyuşmazlık Mahkemesi Dergisi**, (15), 621-664.

Sepetci, Nurten (2017), **Sosyal Medyada Mahremiyet Algısının Çöküşü: Instagram Örneği**, Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi - Sosyal Bilimler Enstitüsü.

Sevinç, Bayram (2012), **Diyalog ve Korku**, 1. Baskı, İz Yayıncılık, İstanbul.

_____ (2019), **Terör Endüstrisi, Din ve Şiddet**, 1. Baskı, Ankara Okulu Yayınları, Ankara.

Seyrek, Ahmet Murat (2018), **Sosyoloji Sözlüğü**, 1. Baskı, Yediveren Yayınları, İstanbul.

- Smith, Russell vd. (2015), “Introduction: Cybercrime Risks and Responses-Eastern and Western Perspectives”, Russell G. Smith (Ed.), **Cybercrime Risks And Responses**, Palgrave Macmillan, New York.
- Sokullu Akıncı, Füsun ve Dursun, Selman (2016), **Viktimoloji**, 3. Baskı, Beta Yayıncılık, İstanbul.
- Sucu, İpek (2014), **Kullanımlar ve Doyumlar Yaklaşımı Açısından Sosyal Medya Sanal Dünya Oyunu Olarak Second Life Örneği**, Yayınlanmamış Doktora Tezi, Maltepe Üniversitesi - Sosyal Bilimler Enstitüsü.
- Şener, Arzu ve Yücel, Sevde (2020), “Sosyal Medyanın Y Kuşağı Satın Alma Davranışları Üzerindeki Etkisi: Bir Literatür İncelemesi”, **Dumlupınar Üniversitesi Sosyal Bilimler Dergisi**, (65), 265-284.
- Şener, Gülcan ve Atar G. Motif (2017), “Türkiye’ye Özgü Kültürel sembollerin Emojilere Dönüşümü: Dijital İletişimde Kültürel Sembollere Yönelik Bir Araştırma”, **İstanbul Üniversitesi İletişim Fakültesi Dergisi**, 53, 189-209.
- Taşçı, Ufuk ve Can, Ali (2015), “Türkiye’de Polisin Siber Suçlarla Mücadele Politikası: 1997-2014”, **Fırat Üniversitesi Sosyal Bilimler Dergisi**, 25(2), 229-248.
- Tosun, Ülkü ve Akıncı, Funda Nur (2016), “Sosyal Ağ Kullanan Bireylerin Benlik Sunumu Stratejilerinin İncelenmesi”, **İstanbul Aydın Üniversitesi Dergisi**, (32), 27-60.
- Uzun, Kadriye ve Aydın, Hakan (2011), “Kullanıcı Profilinin ve Bireylerarası İlişkilerin Gerçek Yaşamla Karşılaştırılması: Second Life Örneği”, **Eskişehir Osmangazi Üniversitesi İİBF Dergisi**, 7(2), 263-290.
- Ünal, Ahmet Naci (2015), **Siber Güvenlik ve Elektronik Bileşenleri**, 1. Baskı, Nobel Akademik Yayıncılık, Ankara.
- Wang, Jing vd. (2009), “School Bullying Among Adolescents in The United States: Physical, Verbal, Relational and Cyber”, **Journal of Adolescent Health**, 45, 368-375.
- Wolhuter, Lorraine vd. (2009), **Victimology: Victimisation and Victims’ Rights**, 1. Baskı, Routledge Cavendish, New York.
- Yar, Majid (2005), “The Novelty of ‘Cybercrime’: An Assessment in Light of Routine Activity Theory”, **European Journal of Criminology**, 2(4), 407-427.

- Yavuz, Yıldız (2019), “Suç Mağduru Olma Korkusuna Sosyolojik Bir Bakış”, **Toplum ve Kültür Araştırmaları Dergisi**, 4, 28-52.
- Yaycı, Esra (2007), **Bilişim Suçları**, Yayınlanmamış Yüksek Lisans Tezi, Gazi Üniversitesi - Sosyal Bilimler Enstitüsü.
- Yegen, Ceren (2014), “Dijital Aktivizmin Bir Türü Olarak Hacktivizm ve RedHack”, **Intermedia International E-journal**, 1(1), 118-132.
- Yılmaz, Eren vd. (2016), “Öğretmenlerin Dijital Veri Güvenliği Farkındalığı”, **Sakarya Üniversitesi Eğitim Bilimleri Enstitüsü Dergisi**, 6(2), 26-45.
- Yüksel, Mezher (2017), “Klasik Suç Kuramları”, Fuat Güllüpnar (Ed.), **Suç Sosyolojisi**, Anadolu Üniversitesi Yayını, Eskişehir.
- Zengin, Mücahid vd. (2015), “Sosyal Medya ve Değişen Mahremiyet: Facebook Mahremiyeti”, **Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi**, 3(2), 112-136.

EKLER

Ek 1: Mülakat Formu

MÜLAKAT SORULARI

- 1) **Kendinizden bahseder misiniz? (Sizi tanıyabilir miyiz?)**
- 2) **Günlük internet kullanım alışkanlığınızı, kullanım amaç, alan ve araçlarını aktaracak şekilde anlatır mısınız?**
- 3) **İnternet kullanım sürecinde kendinize ait ve korunması gerektiğini düşündüğünüz ve bazen sizden talep edilen bilgilerin (fotoğraf, video, düşünce, cinsiyet, yaş, medeni durum, meslek, adres, uygulama izinleri, kredi kartı bilgileri, kimlik bilgileri vb.) paylaşımına dair olası sorunlar için güvenlik açısından ne tür önlemler alıyorsunuz, anlatır mısınız?**
- 4) **Siber suç olgusunun ne olduğuna dair bildiklerinizi ve daha önce çevrenizde siber suç mağduriyeti yaşayan kişiler vb. haberdar olduğunuz olayları, sizi nasıl etkilediğini de aktaracak şekilde anlatır mısınız?**
- 5) **Yaşadığınız siber suç mağduriyetinden (nasıl, nerede, ne zaman, hangi sanal ortam üzerinden, sonucunda ne kaybedildiği vb.) söz eder misiniz?**
- 6) **Yaşadığınız bu durumu nasıl değerlendirdiğinizi (hisler, yorumlar vb.) ve bu mağduriyetle nasıl ve kimlerle birlikte (çevre, resmi görevliler, kurumlar vb.) mücadele ettiğinizi anlatır mısınız?**
- 7) **Mağduriyetinizle mücadelede sonuç aldığınız ve aksaklıklar yaşadığınız kısımları anlatır mısınız?**
- 8) **Maruz kaldığınız bu mağduriyet, sizin (sanal ve gerçek) sosyal etkileşiminize nasıl ve ne yönde etkilerde bulundu, anlatır mısınız?**
- 9) **Sizin gündelik hayatınızı sürdürmeniz açısından baktığımızda; tekrar mağduriyet yaşama ve damgalanma korkusu gibi faktörlerin internet kullanım alışkanlığınızda ne tür değişimlere sebep olduğundan söz eder misiniz?**
- 10) **Tekrar benzer bir siber suç mağduru olmamak için ne tür önlemlerin gerekli olduğunu düşünüyorsunuz ve aldığınız önlemler varsa anlatır mısınız?**

ÖZGEÇMİŞ

Buket Cansu ULUDAĞ, 2007 yılında Yenice 19 Mayıs İlköğretim Okulu'nu; 2013 yılında Turgut Alp Anadolu Lisesi'ni; 2017 yılında da Karadeniz Teknik Üniversitesi – Edebiyat Fakültesi, Sosyoloji Bölümü'nü bitirdi. 2017 yılında Karadeniz Teknik Üniversitesi – Sosyal Bilimler Enstitüsü, Sosyoloji Anabilim Dalında yüksek lisans programına başladı. Bekar olan ULUDAĞ, 2021 yılından beri özel bir firmada sorumlu pozisyonunda görev almaktadır.

