

**T.C.**  
**MİLLÎ SAVUNMA ÜNİVERSİTESİ**  
**ALPARSLAN SAVUNMA BİLİMLERİ ENSTİTÜSÜ**  
**GÜVENLİK BİLİMLERİ ANA BİLİM DALI**  
**SUÇ ARAŞTIRMASI PROGRAMI**

**RUTİN AKTİVİTELER TEORİSİ BAĞLAMINDA**  
**SİBER SUÇ MAĞDURİYETİ**

**YÜKSEK LİSANS TEZİ**

**HAZIRLAYAN FERHAT BİRCEVİZ, 158593**  
**TEZ DANIŞMANI PROF. DR. ALPTEKİN ERKOLLAR**  
**EŞ DANIŞMAN DR. MÜH. ALB. RECEP BENZER**

**ANKARA**

**2019**

**T.C.**  
**MİLLÎ SAVUNMA ÜNİVERSİTESİ**  
**ALPARSLAN SAVUNMA BİLİMLERİ ENSTİTÜSÜ**  
**GÜVENLİK BİLİMLERİ ANA BİLİM DALI**  
**SUÇ ARAŞTIRMASI PROGRAMI**

**RUTİN AKTİVİTELER TEORİSİ BAĞLAMINDA**  
**SİBER SUÇ MAĞDURİYETİ**

**YÜKSEK LİSANS TEZİ**

**HAZIRLAYAN FERHAT BİRCEVİZ, 158593**  
**TEZ DANIŞMANI PROF. DR. ALPTEKİN ERKOLLAR**  
**EŞ DANIŞMAN DR. MÜH. ALB. RECEP BENZER**

**ANKARA**

**2019**

## **ETİK BEYAN**

Milli Savunma Üniversitesi Alparslan Savunma Bilimleri Enstitüsü Müdürlüğü Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallara uygun olarak hazırladığım bu tez çalışmada; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmada yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Ferhat BİRCEVİZ

18.01.2019

**T.C.**  
**MİLLÎ SAVUNMA ÜNİVERSİTESİ**  
**ALPARSLAN SAVUNMA BİLİMLERİ ENSTİTÜSÜ**  
**GÜVENLİK BİLİMLERİ ANA BİLİM DALI**  
**ANKARA 2019**  
**RUTİN AKTİVİTELER TEORİSİ BAĞLAMINDA SİBER SUÇ**  
**MAĞDURİYETİ**  
**YÜKSEK LİSANS TEZİ**  
**Ferhat BİRCEVİZ**

**ÖZET**

Günümüzde internetin yoğun olarak kullanılması ve sosyal ilişkilerin sanal ortamlara taşınması ile birlikte sosyal bir olgu olan suç da sanal ortama taşınmaya başlamış, bu gelişme sonucunda siber suç kavramı ortaya çıkmıştır. Her geçen gün artan siber suç sayısı ile birlikte bu suçlardan mağdur olanların sayıları da artmaktadır. Bu bağlamda çalışmanın kavramsal çerçevesinde öncelikle siber suç kavramı üzerinde durulmuş, bu suçların kanunlarda bulunduğu karşılıklar araştırılmış. Kuramsal çerçevesinde klasik okulun suçu açıklamada kendisinden önceki teorilere göre farklı bir bakış açısı getiren rutin aktiviteler teorisi incelenmiş. Uygulama kısmında ise Amerika Birleşik Devletleri vatandaşları arasında suç mağduriyetinin incelenmesi için, Pew Research Center isimli bir kuruluşa ait verilerin analizi SPSS programı ile çözümlenmiştir. Yapılan incelemelerde siber suç mağduriyeti ile demografik değişkenler arasında (cinsiyet hariç) anlamlı ilişkiler tespit edilmiştir. İnternet kullanıcılarının çoğunluğunun kendilerini suçtan koruyacak tedbirler aldığı, bununla birlikte yoğun bir şekilde rutin aktivitelerde bulunduğu görülmüştür. Rutin aktiviteler ile siber suç mağduru olma arasında anlamlı ve pozitif yönde bir ilişki tespit edilmiş olup rutin aktiviteler teorisinin siber suçları açıklamakta başka çalışmalarla desteklenmesi gerektiği kabul edilmekle birlikte kısmen yeterli olduğu görülmüştür.

**Anahtar Kelimeler:** Siber Suç, Avrupa Konseyi Siber Suçlar Sözleşmesi, Rutin Aktiviteler Teorisi, Mağduriyet.

**NATIONAL DEFENCE UNIVERSITY**  
**ALPARSLAN DEFENCE SCIENCES INSTITUTE**  
**DEPARTMENT OF SECURITY SCIENCES**  
**VICTIMIZATION OF CYBER CRIME IN THE CONTEXT OF**  
**ROUTINE ACTIVITIES THEORY**  
**MASTER THESIS**  
**Ferhat BİRCEVİZ**  
**ABSTRACT**

Nowadays, with the intense use of the Internet and the transfer of social relations to the virtual platforms, a social phenomenon what is crime has begun to be moved to the virtual environment and the concept of cyber crime has emerged as a result of this development. With the increasing number of cyber crime, the number of victims of these crimes is increasing too. In this context, first of all, the concept of cyber crime has been emphasized in the conceptual framework of the study and the responses to these crimes in the laws have been investigated. In the theoretical framework, the classical school's theory of routine activities, which brought a different perspective to the previous theories, was examined in explaining the crime. In the application part, for analyzing crime victimization among the citizens of the United States, the analysis of data belonging to an organization named Pew Research Center was analyzed by SPSS program. Significant relationships between cybercrime and demographic variables (except gender) were determined. It was seen that the majority of the Internet users took measures to protect themselves from crime, but were engaged in routine activities. A significant and positive relationship was found between routine activities and victimization of cybercrime, and it was found that the theory of routine activities was partially sufficient, but it should be supported by other studies to explain cybercrime.

**Key Words:** Cyber Crime, Cyber Crimes Treaty Of European Council, Routine Activities Theory, Victimization

## **ÖNSÖZ VE TEŞEKKÜR**

Bu çalışmada siber ortamın bireyler tarafından her geçen gün daha fazla kullanılmaya başlaması ile toplumsal bir olgu olan suçun da siber ortama taşındığı bu günlerde bireylerin her gün rutin bir şekilde yaptıkları faaliyetlerinin ve siber ortamı kullanma alışkanlıklarının suç mağduru olmaları üzerine etkileri incelenmiştir.

Çalışmanın konusunun belirlenmesinde ve zorlu tez yazım sürecinde her zaman yanımda olan ve engin tecrübelerini benimle paylaşan tez danışmanlarıma, desteklerinden, yardımlarından ve çözüm odaklı yaklaşımlarından dolayı Alparslan Savunma Bilimleri Enstitüsü personeline, benden desteklerini esirgemeyen iş arkadaşlarıma teşekkürlerimi sunarım.

Ayrıca her zaman ve her konuda olduğu gibi tez yazım sürecinde de desteklerini her zaman hissettiğim ve hep yanımda olan, bu hayattaki en büyük şansım; sevgili eşim Sengül ve kızım İdil'e sonsuz teşekkürler. İyi ki varsınız.

**Ferhat BİRCEVİZ**

**Ankara, Ocak 2019**

## İÇİNDEKİLER

TEZ ONAY SAYFASI.....	iii
TEZ İNTİHAL RAPORU.....	iv
ETİK BEYANI.....	v
TÜRKÇE ÖZET.....	vi
İNGİLİZCE ÖZET (ABSTRACT).....	vii
ÖNSÖZ VE TEŞEKKÜR.....	viii
İÇİNDEKİLER.....	ix
TABLO LİSTESİ.....	xiii
ŞEKİL LİSTESİ.....	xv
KISALTMALAR.....	xvi
1. GİRİŞ.....	1
2. ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ.....	3
2.1. Temel Kavramlar.....	3
2.1.1. Suç.....	3
2.1.2. Sapma.....	3
2.1.3. Suç ve Sapma Arasındaki İlişki.....	3
2.1.4. Siber.....	5
2.1.5. Siber Suç.....	5
2.1.6. Siber Suçun Tarihsel Gelişimi.....	5
2.1.7. Siber Suçların Sınıflandırılması.....	6
2.2. Siber Suçların Sınıflandırılması.....	6
2.2.1. Bilgisayar Verilerinin ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Yönelik Suçlar.....	7
2.2.1.1. Yasadışı Erişim.....	7
2.2.1.2. Yasadışı Araya Girme.....	8
2.2.1.3. Verilere Müdahale.....	9
2.2.1.4. Sisteme Müdahale.....	9
2.2.1.5. Cihazların Kötüye Kullanımı.....	10
2.2.2. Bilgisayarla Bağlantılı Suçlar.....	11
2.2.2.1. Bilgisayarla Bağlı Sahtecilik.....	11
2.2.2.2. Bilgisayarla Bağlantılı Dolandırıcılık.....	12
2.2.3. İçerikle Bağlantılı Suçlar.....	14
2.2.3.1. Çocuk Pornografisi.....	14
2.2.4. Telif Hakkı ve Bununla Bağlantılı Hakların İhlaline İlişkin Suçlar.....	15
2.3. Siber Suçların İşlenme Biçimleri.....	16
2.3.1. Bilgi ve Veri Aldatmacası.....	16
2.3.2. Salam Tekniği.....	17
2.3.3. Süper Darbe.....	17
2.3.4. Eş Zamansız Saldırıları.....	17
2.3.5. Truva Atı.....	18
2.3.6. Zararlı Yazılımlar.....	18
2.3.7. Mantık Bombaları.....	18

2.3.8. Oltalama.....	19
2.3.9. Tarama.....	19
2.3.10. Bukelamun.....	19
2.3.11. İstem Dışı Alınan Elektronik Postalar.....	20
2.3.12. Çöpe Dalma.....	20
2.3.13. Gizli Kapılar.....	20
2.3.14. Sırtlama.....	21
2.3.15. Yerine Geçme.....	21
2.3.16. Sistem Güvenliğinin Kırılıp Sisteme Sızılması.....	21
2.3.17. Hukuka Aykırı İçerik Sunulması.....	22
2.3.18. Web Sayfası Hırsızlığı ve Yönlendirme.....	22
2.3.19. Sosyal Mühendislik.....	23
<b>3. ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ.....</b>	<b>25</b>
3.1. Rutin Aktiviteler Teorisi.....	25
3.1.1. Rutin Aktiviteler Teorisinin Oluştugu Ortam.....	25
3.1.2. Rutin Aktiviteler Teorisine Göre Suçun Unsurları.....	26
3.1.2.1. Motive Olmuş Suçlu.....	28
3.1.2.2. Koruyucuların Yokluğu.....	29
3.1.2.3. Uygun Hedef.....	30
3.1.2.3.1. Hedefin Görünür Olması.....	31
3.1.2.3.2. Hedefin Değerli Veya Arzu Edilebilir Olması.....	31
3.1.2.3.3. Hedefin Suça Karşı Korumasız Olması.....	31
3.1.2.3.4. Hareket Kabiliyeti.....	32
3.1.2.3.5. Hedefin Müsait ve Erişilebilir Olması.....	32
3.1.3. Diğer Bir Faktör Olarak Tutucular.....	32
3.1.4. Suç Fırsatları.....	33
3.1.5. Rutin Aktiviteler Teorisi Bağlamında Durumsal Suç Önleme.....	34
3.1.6. Teori Kapsamında Yapılan Bilimsel Çalışmalar.....	37
<b>4. ARAŞTIRMANIN KAPSAMI VE ÖNEMİ.....</b>	<b>41</b>
4.1. Araştırmanın Amacı ve Önemi.....	41
4.1.1. Araştırmanın Amacı.....	41
4.1.2. Araştırmanın Önemi.....	41
4.2. Araştırmanın Yöntemi.....	41
4.2.1. Araştırmanın Evren ve Örneklemi.....	41
4.2.1.1. Araştırmanın Evreni.....	41
4.2.1.2. Araştırmanın Örneklemi.....	41
4.2.2. Araştırmanın Veri Toplama Teknikleri.....	41
4.2.3. Araştırmada Kullanılan Verilerin Analizi.....	42
4.2.4. Araştırmanın Sınırlılıkları.....	42
<b>5. ARAŞTIRMANIN BULGULARI.....</b>	<b>43</b>
5.1. Tanımlayıcı İstatistiklerin Analizi.....	43
5.1.1. Katılımcıların Demografik Özellikleri.....	43
5.1.1.1. Katılımcıların Cinsiyete Göre Dağılımı.....	43



5.1.1.2. Katılımcıların Yaşa Göre Dağılımı.....	43
5.1.1.3. Katılımcıların Eğitim Durumu.....	44
5.1.1.4. Katılımcıların Medeni Hali.....	44
5.1.1.5. Katılımcıların Çocuk Sahibi Olma Durumları.....	45
5.1.1.6. Katılımcıların Çalışma Durumları.....	45
5.1.1.7. Katılımcıların Gelir Durumları.....	46
5.1.1.8. Katılımcıların Hane Halkı Mevcudu.....	47
5.1.1.9. Katılımcıların Yerleşim Yeri.....	47
5.1.2. Katılımcıların İnternet Kullanım Alışkanlıklarının İncelenmesi.....	47
5.1.2.1. Katılımcıların İnternet Kullanma Durumları.....	47
5.1.2.2. Katılımcıların İnternete Erişim Sıklıkları.....	48
5.1.2.3. Katılımcıların Sosyal Medya Kullanım Durumları.....	49
5.1.2.4. Katılımcıların İnternet Üzerinden Finansal İşlem Yapma Eğilimleri.....	49
5.1.2.5. Katılımcıların Kişisel Verilerinin Korunması Konusundaki Endişe Seviyeleri.....	50
5.1.2.6. Katılımcıların Halka Açık İnternet Erişiminde Yaptığı İşlemlerin İncelenmesi.....	51
5.1.3. Katılımcıların Siber Suç Mağduru Olma Durumlarının İncelenmesi.....	52
5.1.4. Katılımcıların Siber Suçun Hedefi Olarak Yaptığı Rutin Aktivitelerin İncelenmesi.....	54
5.1.4.1. Katılımcıların Şifre Yönetim Davranışları.....	54
5.1.4.2. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumları.....	56
5.1.4.3. Katılımcıların Şifrelerini Paylaşma Alışkanlıkları.....	57
5.1.4.4. Katılımcıların Sosyal Medya Hesaplarını Farklı Sitelere Erişirken Kullanma Eğilimleri.....	58
5.1.4.5. Katılımcıların Kamuya Açık Modemler Üzerinden İnternete Erişme Eğilimleri.....	59
5.1.5. Katılımcıların Suçtan Koruyabilecek Koruyucular Kullanma Alışkanlıklarının İncelenmesi.....	60
5.1.5.1. Katılımcıların İki Faktörlü Koruma Sistemi Kullanma Alışkanlıkları.....	60
5.1.5.2. Katılımcıların Cihazlarına Ulaşırken Şifre Kullanma Alışkanlıkları.....	61
5.1.5.3. Katılımcıların Kullandıkları Uygulamaları ve İşletim Sistemlerini Güncelleme Alışkanlıkları.....	62
5.1.5.4. Katılımcıların Anti Virüs Programı Kullanma Alışkanlıkları.....	64
5.2. Ölçüm.....	65
5.2.1. Siber Suç Mağduriyeti Değişkeninin Ölçülmesi.....	65
5.2.2. Koruyucular Değişkeninin Ölçülmesi.....	66
5.2.3. Rutin Aktiviteler Değişkeninin Ölçülmesi.....	66
5.3. Siber Suç Mağduriyeti İle Demografik Değişkenler Arasında ki İlişkinin İncelenmesi.....	67

5.3.1. Cinsiyet İle Siber Suç Mağduriyeti Arasındaki İlişki.....	67
5.3.2. Yaş İle Siber Suç Mağduriyeti Arasındaki İlişki.....	67
5.3.3. Eğitim Düzeyi İle Siber Suç Mağduriyeti Arasındaki İlişki.....	68
5.3.4. Medeni Hal İle Siber Suç Mağduriyeti Arasındaki İlişki.....	69
5.3.5. Çalışma İle Siber Suç Mağduriyeti Arasındaki İlişki.....	71
5.3.6. Yıllık gelir İle Siber Suç Mağduriyeti Arasındaki İlişki.....	72
5.4. Suç Mağduriyeti, Rutin Aktiviteler ve Koruyucular Arasındaki İlişkinin Analizi.....	73
<b>6. SONUÇ VE DEĞERLENDİRME.....</b>	<b>75</b>
6.1. Tanımlayıcı İstatistikler ve Hipotezlerin Değerlendirilmesi.....	76
6.2. Öneriler.....	78
6.3. Sonuç.....	79
<b>KAYNAKÇA.....</b>	<b>81</b>
<b>EKLER.....</b>	<b>85</b>
Ek 1. ANKET FORMU (Orijinal Dilinde).....	85
Ek 2. ANKET VERİLERİNİ KULLANIM İZİN BELGESİ.....	112
<b>ÖZGEÇMİŞ.....</b>	<b>113</b>

## TABLÖLAR LİSTESİ

	Sayfa No.
<b>Tablo 1:</b>	Katılımcıların Cinsiyete Göre Dağılımı.....43
<b>Tablo 2:</b>	Katılımcıların Yaşa Göre Dağılımı.....43
<b>Tablo 3:</b>	Katılımcıların Eğitim Durumuna Göre Dağılımı.....44
<b>Tablo 4:</b>	Katılımcıların Medeni Hali.....44
<b>Tablo 5:</b>	Katılımcıların Çocuk Sahibi Olma Durumları.....45
<b>Tablo 6:</b>	Katılımcıların Çalışma Durumu.....45
<b>Tablo 7:</b>	Katılımcıların Gelir Durumu.....46
<b>Tablo 8:</b>	Katılımcıların Hane Halkı Mevcudu.....46
<b>Tablo 9:</b>	Katılımcıların Yerleşim Yeri.....47
<b>Tablo 10:</b>	Katılımcıların İnternet Kullanma Durumları.....47
<b>Tablo 11:</b>	Katılımcıların İnternete Erişim Sıklığı.....48
<b>Tablo 12:</b>	Katılımcıların Sosyal Medya Kullanım Oranları.....48
<b>Tablo 13:</b>	Katılımcıların İnternet Üzerinden Finansal İşlem Yapma Eğilimleri..49
<b>Tablo 14:</b>	Katılımcıların Kişisel Verilerinin Korunması Konusundaki Endişe Seviyeleri.....50
<b>Tablo 15:</b>	Katılımcıların Halka Açık İnternet Erişiminde Yaptığı İşlemler.....51
<b>Tablo 16:</b>	Katılımcıların Siber Suç Mağduriyeti Durumları.....52
<b>Tablo 17:</b>	Katılımcıların Şifre Yönetim Alışkanlıkları.....54
<b>Tablo 18:</b>	Katılımcıların Kullandığı Şifrelerin Benzerlik Durumu.....56
<b>Tablo 19:</b>	Katılımcıların Şifrelerini Paylaşma Alışkanlıkları.....57
<b>Tablo 20:</b>	Katılımcıların Sosyal Medya Hesaplarını Farklı Sitelere Erişirken Kullanma Eğilimleri.....57
<b>Tablo 21:</b>	Kamusal Alanda Bulunan Ağlara Erişim Durumu.....58
<b>Tablo 22:</b>	Katılımcıların İki Faktörlü Koruma Sisteminin Kullanma Durumu....60
<b>Tablo 23:</b>	Katılımcıların Cihazlarına Ulaşırken Şifre Kullanma Alışkanlıkları...60
<b>Tablo 24:</b>	Katılımcıların Cihazlarına Erişimde Kullandığı Güvenlik Tedbirleri..61
<b>Tablo 25:</b>	Katılımcıların Akıllı Cihazlardaki Uygulamaların Güncelleme Durumu.....62
<b>Tablo 26:</b>	Katılımcıların Akıllı Cihazlarının İşletim Sistemlerini Güncelleme Durumu.....63

<b>Tablo 27:</b>	Katılımcıların Anti Virüs Programı Kullanma Aışkanlıkları.....63
<b>Tablo 28:</b>	Mağduriyet, Rutin Aktiviteler ve Koruyucular Arasındaki İlişki.....72

## ŞEKİLLER LİSTESİ

### Sayfa No.

<b>Şekil 1:</b> Siber Suçların Sınıflandırılması.....	6
<b>Şekil 2:</b> Suçun Yapısı.....	25
<b>Şekil 3:</b> Durumsal Suç Önleme Yöntemleri.....	35
<b>Şekil 4:</b> Siber Suç Mağduriyeti İle Yaş Arasında ki İlişki.....	67
<b>Şekil 5:</b> Siber Suç Mağduriyeti İle Eğitim Düzeyi Arasında ki İlişki.....	68
<b>Şekil 6:</b> Siber Suç Mağduriyeti İle Medeni Hal Arasında ki İlişki.....	69
<b>Şekil 7:</b> Siber Suç Mağduriyeti İle Çalışma Durumu Arasında ki İlişki.....	70
<b>Şekil 8:</b> Siber Suç Mağduriyeti İle Yıllık Gelir Arasında ki İlişki.....	71

## KISALTMALAR LİSTESİ

<b>ABD</b>	.....Amerika Birleşik Devletleri.
<b>DNS</b>	.....Domain Name System.
<b>IBAN</b>	.....International Bank Account Number.
<b>IP</b>	.....Internet Protocol.
<b>TBMM</b>	.....Türkiye Büyük MilletMeclisi.
<b>TCK</b>	.....Türk Ceza Kanunu.

## GİRİŞ

İnsanlığın başladığı günden bu yana toplumsal bir olgu olarak karşımıza çıkan suç olgusu toplumsal yaşamın her döneminde değişime uğrayarak günümüze kadar gelmiştir. Özellikle 1990'lı yıllardan sonra insanlar arasındaki ilişkilerin boyutlarının sanal ortamlara kaymaya başlaması ile birlikte suç olgusunun da bu ortamda belirmeye başlaması son derece hızlı bir şekilde gerçekleşmiştir.

Suç olgusunun sanal ortama da yayılması ile birlikte günümüzde internete erişen herkes her an siber suç mağduru olma durumu ile karşı karşıya kalmıştır. Siber suçlular, suç işleme yöntemleri kullanılarak, mağdurların birtakım şahsi bilgilerini ele geçirmeye çalışılmakta ve bunun sonucunda haksız kazanç sağlamayı amaçlamaktadırlar.

Sanal ortamda bulunan potansiyel siber suçlular her gün suç mağduru olabilecek insanlar ile karşılaşmakta ve kendilerine uygun hedefler aramaktadırlar. Uygun hedefleri buldukları anda saldırıya geçerek siber suç olayını meydana getirmektedirler. Suçun oluşmasının önüne geçebilmek için bu buluşma engellenmelidir. Bu engellemede asıl görev, suç mağduru olabilecek şahsa düşmektedir. Zira potansiyel siber suçlu suç işlemek amacıyla sanal ortamda bulunmaktadır ve onu bu kararından vazgeçirmek oldukça zordur.

Potansiyel suç mağduru bu buluşmanın engellenmesi için bir takım tedbirler almalıdır. Bunlar anti virüs programları vb. birtakım koruyucu tedbirler olabilir. Bununla birlikte varsa her çevrimiçi hesapta aynı parolayı kullanmak gibi yaptığı rutin faaliyetlerinden vazgeçmelidir.

Kriminoloji alan yazını bu kapsamda incelendiğinde klasik okul teorilerinden rutin aktiviteler teorisi\* siber suçların yapısına uygun bir açıklama ortaya koymaktadır.

Bu açıklamalardan sonra öncelikle araştırmanın kavramsal çerçevesi incelenecek, çeşitli tanımlara yer verilecek ve kanunlarda tanımlı siber suçlar irdelenecektir.

---

\* Teorinin kapsam ve varsayımları üçüncü bölümde detaylı olarak açıklanmıştır.





## ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ

### 2.1. Temel Kavramlar

#### 2.1.1. Suç

Suçun tanımı çoğu kaynakta “kanunlarla yasaklanan eylemler” olarak geçmektedir. Fakat suç gibi karmaşık bir toplumsal olgunun bu kadar basit bir tanıma indirgenmesinde pekçok aşamadan geçtiği aşîkârdır. Öncelikle suçu anlayabilmek için diğerk bir toplumsal olgu olan sapma üzerinde durmamız gerekmektedir.

#### 2.1.2. Sapma

Sapmanın tanımı da pekçok kaynakta “toplumca hoş karşılanmayan fakat kanunlarda yer almayan eylemler” olarak karşımıza çıkmaktadır.

#### 2.1.3. Suç ve Sapma Arasındaki İlişki

Sapma ve suç tanımlarına yukarıda kısaca değindikten sonra bu iki kavram arasındaki ilişkiden bahsetmek gerekir. Dolu’ya göre söz konusu suç olduğunda hukuki bir tanım algılanırken, sapmadan bahsedildiğinde toplum tarafından kabul gören yargıların ihlali durumunun anlaşıldığı ortaya çıkmaktadır.<sup>1</sup> Bu açıdan bakıldığında her iki kavram da farklı normlar sistemini esas almaktadır. Bu sistemlerin dışına çıkıldığında oluşan durumlar ise suç veya sapma olarak adlandırılmaktadır.

Bahse konu kavramların dayandığı normlar sisteminin birbirleri ile ortak olduğu veya çatışma içinde olduğu durumlar var olabilir. Toplum tarafından hoş karşılanmayan bir davranış kanunlarda suç olarak tanımlanmış veya tanımlanmamış olabilir. Ya da tam aksine; kanunlarda suç olarak tanımlanmış bir davranış toplumda olumlu veya olumsuz karşılanıyor olabilir.<sup>2</sup> Mevcut kaynakların pek çoğunda bu duruma zina örnek verilmektedir. Fakat ülkemiz özelinde düşündüğümüzde, daha çok Güneydoğu Anadolu Bölgesi’nde görülen töre cinayetleri ve kan davaları bu hususa çok güzel örnek teşkil etmektedir. Türk Ceza Kanunu’na göre adam öldürmek suç teşkil etmektedir ve bu suçu işleyen failin bir cezai sorumluluğu vardır. Fakat bölgede

---

<sup>1</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.5

<sup>2</sup> Emile Durkheim *Toplumsal İşbölümü*, çev. Özer OZANKAYA (İstanbul: Cem Yayınevi, 2014), s.107

yaşayan insanlar için töre cinayetleri işlemek veya kan davası güderek bir insanın hayatına son vermek, onurlandırıcı bir davranış olarak görülmektedir. Bu suçu işleyen insanlar, işledikleri suçun karşılığında ağır cezalar alacaklarını bilerek hareket etmektedirler. Fakat toplum tarafından üzerlerinde kurulan baskının kaldırılması uzun yıllar ceza evinde yaşamaktan daha önemli görülmektedir. Bu örnekten anlaşılacağı üzere, töre cinayetleri ve kan davaları bölgesel temelde düşündüğümüzde bir sapma olmamasına karşın kanunlarda suç olarak tanımlanmıştır.

Bu örnekten sonra suçu devletin hoş görmediği, sapmayı ise toplumun hoş görmediği davranışlar şeklinde özetleyebiliriz. Yani suç yazılı kurallara aykırı hareketlerdir. Sapma ise toplumun içinde var olan herkes tarafından bilinen fakat herhangi bir yerde yazılı olmayan kurallara aykırı hareketlerdir. Bu noktada sorulması gereken soru şudur; sapma ile suç arasında bir geçişkenlik var mıdır?

Durkheim'e göre toplumsal yaşamın bulunduğu her yerde o toplumun üyeleri sürekli bir etkileşim halindedir.\* Bununla birlikte toplumsal yaşam var olduğu her yerde örgütlenmeye başlamakta ve etkileşimleri belli bir kalıba sokmaya çalışmaktadır. Bu etkileşimler zamanla toplum içinde herkes tarafından bilinen kurallar haline gelmektedirler. İşte bu kurallar yasa koyucuların yasaları hazırlarken faydalandığı kaynaklardır.<sup>3</sup>

Buradan da anlaşılacağı üzere toplumda var olan yazılı olmayan kurallar zamanla yazılı hale gelmektedirler. Yani geçmişte sapma olarak tanımlanan bir davranış günümüzde suç olarak tanımlanabilir ya da toplumsal dinamiklerin değişmesiyle birlikte bu durumun tam tersi de yaşanabilir.

İşte siber suçlar da ortaya çıkmaya başladığı ilk zamanlarda bu şekilde birer sapmadan ibaretti çünkü kanunlarda yazılı bir karşılıkları yoktu. Zaman içinde mağduriyetlerin ve işlenen suç miktarının artması ile yavaş yavaş kanunlarda suç olarak tanımlanmaya başlandı.

---

\* Bu etkileşiminden bahsederken sadece toplumun üyeleri arasında olan yüz yüze etkileşimden değil aynı zamanda toplumun içinde bulunan kuruluşlarla (esnaflar, tüccarlar, devlet kurumları vb.) süregelen bir etkileşim anlaşılmalıdır.

<sup>3</sup> Emile Durkheim *Toplumsal İşbölümü*, çev. Özer OZANKAYA (İstanbul: Cem Yayınevi, 2014), s.92

Bu çalışmada siber suçlar mer'î mevzuata göre incelenmiş olup Türk Ceza Kanunu kapsamında tanımlanan suçların araştırması yapılmıştır.

Suç ve sapmayı yukarıda gibi tanımladıktan sonra çalışma kapsamında suçun birleştirileceği siber kavramı üzerinde durulacaktır.

#### **2.1.4. Siber**

Siber sözcüğünün ingilizce karşılığı cyber olup Longman sözlüğünde araştırıldığında “relating to computers, especially to messages and information on the Internet”.<sup>4</sup> Bilgisayarla ilgili (özellikle internet üzerindeki bilgi ve mesajlarla) cümlesi karşımıza çıkmaktadır. Bu tanımdan “siber” tabirinin bilgisayarla ilgili hemen hemen her şeyi kapsadığına ulaşabiliriz. Bu noktada bilgisayar tabirinden sadece masaüstü veya dizüstü bilgisayarlar değil bunları da kapsamakla birlikte bilişim sistemleri anlaşılmalıdır.

#### **2.1.5. Siber Suç**

Yukarıda “siber” tabirinin ve suç olgusunun tanımlarını yaptıktan sonra artık siber suçu bilişim sistemleri üzerinden işlenen her türlü suç olarak tanımlayabiliriz. Ancak bir eylemin suç olgusunu oluşturabilmesi için onun kanunlarla tanımlanmış olması gerekmektedir. Türkiye Cumhuriyeti kanunlarında siber suçlar 5237 sayılı Türk Ceza Kanunu’nun 243, 244 ve 245’inci maddelerinde tanımlanmıştır.\*

#### **2.1.6. Siber Suçun Tarihsel Gelişimi**

1960’ların ortalarına kadar siber suçlar bilinmeyen bir olguydu. Siber Suçların yer aldığı bilinen ilk çalışma 1966 tarihinde Minneapolis Tribune adlı bir dergide yer alan “bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor.” isimli bir makaleydi.<sup>5</sup>

Siber suç olgusu, ortaya çıktığı ilk zamanlarda siber suçların yapısı bugünkü kadar karmaşık değildi. Siber suçlar günümüze nazaran daha basit bir şekilde sistemlerin yasadışı kullanılması, farklı yollarla sabote edilmesi gibi basit yollarla

---

<sup>4</sup> <https://www.ldocecevrیمیچی.com/dictionary/cyber> [Erişim Tarihi: 26.11.2018]

\* Söz konusu maddelerin açıklaması ilerleyen bölümlerde yapılacaktır.

<sup>5</sup> Emin Doğan AYDIN “Bilişim Suçları ve Hukukuna Giriş.” den aktaran Hüseyin ÇAKIR ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara: Seçkin Yayınları, 2014), s.21

gerçekleştiriliyordu. Fakat internetin özellikle ABD’de hızlı bir şekilde gelişmesi ile birlikte siber suçların işlenme şekilleri farklılaşmış, siber suçların yapıları değişmeye ve siber suçluların sayıları hızlı bir şekilde artmaya başlamıştır. <sup>6</sup>

Siber suç olgusu üzerine 1970’li yıllarda daha fazla çalışma yapılmaya başlanmıştır. Özellikle 1980’li yıllara gelindiğinde sanal ortamda işlenen suçların cezai bir yaptırımını olmadığı tespit edilerek siber suçların hukuki bir şekilde düzenlenmesi gereksinimi doğmuştur. Ayrıca, bu tür suçların sadece ekonomik etkilerinin değil, çok daha önemli hatta küresel boyutta sonuçlarının olabileceği anlaşılmış ve siber suçlar farklı bir disiplin olarak kabul edilmeye başlanmıştır.<sup>7</sup>

Siber suçların tarihsel gelişiminden bahsederken onları içinde barındıran “siber uzay” teriminden de bahsetmeliyiz. Siber uzay terimi ilk defa “Neuromancer” isimli kitabında William GIBSON tarafından kullanılmıştır. Gibson bilim kurgu tarzındaki romanında dünya üzerinde giderek bilginin paradan daha önemli hale geldiğini, hükümetlerin yerine geçen büyük şirketlerle, güvenli olduğu düşünülen verilere savaş açan ve onları ele geçirerek büyük şirketleri çeşitli zararlara uğratmaya çalışan bilgisayar korsanlarının mücadelesini anlatmaktadır. Söz konusu kitapta anlatılan bu ortam, bilginin elektronik ortamlarda oluşturulup herhangi bir yerden ona ulaşılmasını sağlayan her türlü vasıtayı\* da içinde bulundurmaktadır.<sup>8</sup>

## 2.2. Siber Suçların Sınıflandırılması

Alan yazınında çeşitli sınıflandırmalar\* olmakla birlikte, Türkiye Cumhuriyeti Devleti, Avrupa Konseyi bünyesinde hazırlanarak, 23 Kasım 2001 tarihinde

---

<sup>6</sup> Oğuz TURHAN *Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)* (Planlama Uzmanlığı Tezi) 2006 s.28.

<sup>7</sup> age, s. 29.

\* Birbirine bağlı ağ sistemleri, uydular, yazılımlar, bilgisayarlar, telefon hatları, kurumların kendi iç ağları vb.

<sup>8</sup> A.Emin DOĞAN “Bilişim Suçları ve Hukukuna Giriş.” den aktaran Hüseyin ÇAKIR ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara: Seçkin Yayınları, 2014), s.21

\* Karagüllemez’in sınıflandırması; Bilişim sistemleri aracılığıyla işlenen suçlar, bilişim sistemlerine yönelik suçlar olmak üzere ikili ayrım şeklinde, Easttom ve Taylor’un sınıflandırması; kimlik hırsızlığı, yetkisiz erişim, erişim gerektirmeyen siber suçlar, çevrim içi taciz ve dolandırıcılık şeklindedir. Birleşmiş Milletlerin sınıflandırması ise bilgisayar ve bileşenlerine zarar vermek, yetkisiz erişim, veri trafiğini durdurma veya ele geçirme, bilişim sisteminin işleyişini engellemek amacıyla sabotaj ve veri trafiğini durdurma veya ele geçirme şeklindedir. (M.Alper SÖZER ve diğ. *Kriminoloji* (Ankara: Nobel yayınları, 2016) s.265.

Budapeşte’de imzaya açılan ve 1 Temmuz 2004 tarihinde yürürlüğe giren Sanal Ortamda İşlenen Suçlar Sözleşmesi’ni, 10 Kasım 2010 tarihinde bir kısım çekinceler ile birlikte Strazburg’da imzaladığı ve sözkonusu Sözleşme 26 Aralık 2012 tarihinde TBMM’de kabul edildiği için Şekil 1 de özetlenen ve çalışmada kullanılacak sınıflandırma bu Sözleşme esaslarına göre yapılacaktır.

<b>Bilgisayar Verilerinin ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Yönelik Suçlar.</b>
Yasadışı Erişim.
Yasadışı Araya Girme.
Verilere Müdahale.
Sisteme Müdahale.
Cihazların Kötüye Kullanımı.
<b>Bilgisayarlarla Bağlantılı Suçlar.</b>
Bilgisayarla Bağlı Sahtecilik.
Bilgisayarla Bağlı Dolandırıcılık.
<b>İçerikle Bağlantılı Suçlar.</b>
Çocuk Pornografisi.
<b>Telif Hakkı ve Bununla Bağlantılı Hakların İhlaline İlişkin Suçlar.</b>

**Şekil 1: Siber Suçların Sınıflandırılması.**

## **2.2.1. Bilgisayar Verilerinin ve Sistemlerinin Gizliliğine, Bütünlüğüne ve Erişilebilirliğine Yönelik Suçlar**

### **2.2.1.1. Yasadışı Erişim**

Bu suç günümüzde bilişim sistemleri üzerinden en çok işlenen suç türüdür. Nasıl ki kişilerin ve/veya kurumların özel mülklerine izinsiz olarak girmek bir suç teşkil ediyorsa kişilere ve/veya kurumlara ait bilişim sistemlerine kişinin rızası olmadan herhangi bir şekilde erişmek de suç teşkil etmektedir.<sup>9</sup>

Yasadışı erişimde suçun hedefinde bilişim sistemleri bulunmaktadır. Erişim sisteme herhangi bir şekilde müdahil olmayı ifade etmektedir. Bu erişim fiziki olarak sistemin bulunduğu yerde veya uzaktan mesela internet üzerinden ya da diğer bilişim sistemleri üzerinden gerçekleşebilir.<sup>10</sup>

<sup>9</sup> Yavuz ERDOĞAN, “Bilişim Sistemine Girme ve Kalma Suçu” *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, c.12 özel sayı (2010): s.1363-1433

<sup>10</sup> Hüseyin ÇAKIR ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara: Seçkin Yayınları, 2014), s.22

Bu suç türü Türk Ceza Kanunu'nun üçüncü kısmının\* onuncu bölümünde yer alan Bilişim Alanında İşlenen Suçlar başlığı altında, “bilişim sistemlerine girme” şeklinde belirtilmiştir ve 243. Maddenin birinci fıkrasında şu şekilde tanımlanmıştır.<sup>11</sup>

*“Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.”*

Bu fıkra ile bilişim sistemlerine yetkisiz olarak yapılan her türlü giriş suç olarak tanımlanmıştır. Sistemlere girip herhangi bir çıkar sağlanamasa ve yahut herhangi bir zarar verilemese bile yapılan eylem suç olarak kabul edilmektedir.

### 2.2.1.2. Yasadışı Araya Girme

Avrupa Konseyi sözleşmesinin ilgili maddesi şu şekildedir;

*“Taraflardan her biri verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dâhil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanabilmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.”<sup>12</sup>*

Bu maddeden anlaşılacağı üzere yasadışı araya girme; suçun, elektronik ortamdaki verilere müdahale etmek suretiyle işlenmesini ele almaktadır. Burada asıl korunmak istenen iletişimin gizliliği ve kişisel verilerdir. Bu madde, genellikle telefon konuşmalarının ve içinde bulunan ortamların dinlenmesi ile son zamanlarda hemen hemen her ülkenin gündeminde bulunmaktadır. Hatta ülkeler arası krizlere bile yol açan bir konuyu ele almaktadır.\*

---

\* “Topluma Karşı İşlenen Suçlar.”

<sup>11</sup> “Türk Ceza Kanunu (5237 S.K.)”

<sup>12</sup> Dışişleri Bakanlığı, “Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu” (1/676, Yasama Dönemi:24, Yasama Yılı:3, ss.:380; Tarih 20 Aralık 2012): s.14

\* “Münih merkezli Focus dergisinin haberine göre, Alman Dış İstihbarat Servisi (BND), dönemin başbakanı Helmut Schmidt'in 'kesin talimatıyla' 1976'da Türkiye'yi dinlemeye aldı. Bugünkü dinlemelere meclis komisyonunca karar verildiğini belirten Focus, dinleme iznini veren komisyonun Başbakanlık, Savunma Bakanlığı, Dışişleri Bakanlığı ve Ekonomi Bakanlığı uzmanlarından oluştuğunu belirtti. İki Almanya birleşmeden önce Batı Almanya'da 1974-1982 yılları arasında başbakanlık yapan sosyal demokrat Helmut Schmidt, Türkiye karşıtı açıklamalarıyla bilinen bir siyasetçi.” (<http://www.aljazeera.com.tr/haber/almanya-turkiyeyi-1976dan-beri-dinliyor>)

Bu suç iletişimin içeriğinin ve/veya içinde bulunulan ortamın teknik cihazlar veya farklı yöntemler kullanılarak dolaylı veya doğrudan olarak dinlenmesi, kaydedilmesi, izlenmesi, içeriğinin denetlenmesi veya izlenmesi ile ilgilidir.<sup>13</sup>

### 2.2.1.3. Verilere Müdahale

Avrupa Konseyi sözleşmesinin ilgili maddesi şu şekildedir;

*“Taraflardan her biri, bilgisayar verilerine haksız yere zarar verilmesi, verilerin silinmesi, tahrip edilmesi, değiştirilmesi veya engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanabilmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.”<sup>14</sup>*

Sanal ortamda işlenen suçlar sözleşmesinin yukarıda yazılan maddesi Türk Ceza Kanunu’nda 244. Maddenin 2. Fıkrasında;

*“Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.”<sup>15</sup>*

Maddesi ile karşılık bulmuştur. Bu madde ile siber uzay ortamında bulunan verilere yetkisiz olarak erişip o veriler üzerinde haksız bir işlem gerçekleştiren şahıslar ile ilgili olarak tanımlama yapılmıştır. Bu suçun oluşabilmesi için verilere müdahale eyleminin bilinçli olarak yapılmış olması gerekmektedir.<sup>16</sup>

### 2.2.1.4. Sisteme Müdahale

Avrupa Konseyi Siber Suçlar Sözleşmesinin ilgili Maddesi şu şekildedir;

*“Taraflardan her biri, bilgisayar sistemlerine veri girişi yaparak, bu verileri ileterek, bilgisayar verilerine zarar vererek, bunları silerek, tahrip ederek, değiştirerek veya engelleyerek bir bilgisayar sisteminin işleyişinin haksız yere engellenmesinin, kasten gerçekleştirildiği zaman, kendi iç hukuku kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.”<sup>17</sup>*

---

<sup>13</sup> Sevil Yıldız, *Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi* (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, 2006), s.177.

<sup>14</sup> Dışişleri Bakanlığı, “Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu” (1/676, Yasama Dönemi:24, Yasama Yılı:3, ss.:380; Tarih (20 Aralık 2012): s.14

<sup>15</sup> “Türk Ceza Kanunu (5237 S.K.)”

<sup>16</sup> Berrin AKBULUT, “Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, c.24, S.2, (2016): ss.7-55

<sup>17</sup> Dışişleri Bakanlığı, “Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu” (1/676, Yasama Dönemi:24, Yasama Yılı:3, ss.:380; Tarih 20 Aralık 2012): s.14

Bu maddenin TCK'daki karşılığı ise 244. Maddenin 1. Fıkrasında şu şekilde ifade edilmiştir;

*“Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.”*<sup>18</sup>

Bu noktada bilişim sistemi üzerindeki verilere yetkili kişilerin erişiminin engellenmesi de bu suçun kapsamına girmektedir. Bu bağlamda, suçlunun sisteme yapmış olduğu müdahale fiziki olarak değerlendirilmemeli aynı zamanda uzaktan yapılan saldırılar da bu kapsama dâhil edilmelidir. Yetkili kişilerin ilgili verilere erişmesinin ve verileri yönetmesinin bir şekilde engellenmesi (mevcut şifrenin değiştirilmesi, kullanıcının bilmediği yeni bir şifre tanımlanması veya daha önce şifre bulunmayan bir veri üzerine yeni şifre tanımlanması vb.) gibi eylemler suç kapsamında tanımlanmaktadır.<sup>19</sup>

#### **2.2.1.5. Cihazların Kötüye Kullanımı**

Avrupa Konseyi Siber Suçlar Sözleşmesinin bu maddesi ile yukarıda sayılan suçların işlenebilmesi maksadıyla tasarlanmış bir cihaz, bir bilgisayar programı, sahte erişim şifreleri ve benzerlerinin üretimi, pazarlaması, kullanım amacıyla tedarik edilmesi ve bulundurulması yasaklanmıştır.

Sözleşmenin bu maddesi TCK'nin 245/A\* maddesinde karşılık bulmuştur. Kanunda suçun unsurları tek tek sayılmıştır fakat sözleşmede benzer hareketlerinde suç olacağı tanımlanarak ileride gelişebilecek çeşitli durumlar için açık kapı bırakılmıştır.<sup>20</sup>

---

<sup>18</sup> “Türk Ceza Kanunu (5237 S.K.)”

<sup>19</sup> Berrin AKBULUT, “Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme”, Selçuk Üniversitesi Hukuk Fakültesi Dergisi, c.24, S.2, (2016): ss.7-55

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

<sup>20</sup> İbrahim Korkmaz, “Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu” *Terazi Hukuk Dergisi*, c.13.s.142, (2018): s.45-55



## 2.2.2. Bilgisayarla Bağlantılı Suçlar

### 2.2.2.1. Bilgisayarla Bağlı Sahtecilik

Bilişim sistemleri kullanılarak işlenen diğer bir suç ise bir bilgi ya da belgenin aslına benzetilerek uydurma olarak elektronik ortamlarda üretilmesidir. Eski TCK'nin 52'inci Maddesinin c fıkrasında bu suç aşağıdaki şekilde tanımlanmaktaydı; fakat 1 Haziran 2005 tarihinde yeni TCK'nin yürürlüğe girmesi ile bu veya buna benzer bir maddeye yer verilmemiştir.

*“Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme, verileri veya diğer unsurları yerleştiren veya var olan verileri, diğer unsurları tahrif eden kimseye bir yıldan üç yıla kadar, tahrif edilmiş olanları bilerek kullananlara altı aydan iki yıla kadar hapis cezası verilir.”*

Kanunda bu suç ile ilgili bir boşluk bulunmaktadır. Bu boşluk Adalet Bakanlığı tarafından hazırlanan ve başbakanlığa sunulan “Bilişim Ağı Hizmetlerinin Düzenlenmesi ve Bilişim Suçları Hakkında Kanun Tasarısı”nın 18'inci maddesinde;

*“Sahte belge düzenlemek amacıyla, bilişim sisteminde bulunan verileri silen, değiştiren, yok eden veya yeni veri giren kişi hakkında 16. maddenin birinci fıkrasına (Bir bilişim sisteminde bulunan verileri veya programları hukuka aykırı olarak bozan, silen, değiştiren, yok eden, erişilmez kılan, sisteme veri veya program yerleştiren veya ekleyen, veri veya programlara zarar veren kişi iki yıldan beş yıla kadar hapis cezası ile cezalandırılır.) göre verilecek ceza yarı oranda artırılır. Şeklinde tanımlanmıştır.” Aynı maddenin 2'nci fıkrasında ise; Birinci fıkra belirtilen fiillerin işlenmesi suretiyle oluşturulan verilere dayalı olarak sahte belge düzenlenmesi halinde, ayrıca 26.9.2004 tarihli ve 5237 sayılı Türk Ceza Kanununun belgede sahtecilik suçuna ilişkin hükümlerine göre cezaya hükmolunur.*

Maddesi getirilerek TCK'da bulunan eksiklik doldurulmaya çalışılmıştır ancak söz konusu teklif halen onaylanmış değildir.

Kısaca bu suç; kendisine veya bir başkasına menfaat sağlayacak şekilde bilişim sistemlerine girme, oradaki verileri manipüle etme ve bu yolla hukuken delil niteliği taşıyabilecek yeni bilgi ve belgeler oluşturmak şeklinde tanımlanabilir.<sup>21</sup>

Avrupa Konseyi Siber Suçlar Sözleşmesinde ise bu suç aşağıda belirtildiği şekilde tanımlanmıştır.

*“Taraflardan her biri özgün olmayan verilerle sonuçlanan yeni veri girme, verileri değiştirme, silme veya engelleme eylemlerinin, söz konusu verilerin yasal açıdan özgün veriler gibi kabul edilmesi veya işlem görmesi niyetiyle, kasten ve haksız yere gerçekleştirildiği zaman, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına*

---

<sup>21</sup> Tanrıkulu ve diğ., "Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu." **Kamu Bilişim Platformu 9** Mayıs (2007) s.41

*bakılmaksızın, bu eylemlerin kendi iç hukukunda cezai suç olarak tanımlanabilmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.”*

Bu tür suçlarda bilişim sistemleri kullanılmak vasıtasıyla hukuki bir delil niteliği taşıyabilecek bir evrak üzerinde değişiklik yapılabilir, olmayan bir bilgi veya belge varmış gibi gösterilebilir, var olan gerçek bir belge silinebilir veya yerine yanlış içerik barındıran bir belge koyulabilir.<sup>22</sup>

Evrakta sahtecilik suçuyla bilgisayarla bağlı sahtecilik suçunda korunmak istenen hukuksal değer aslında aynıdır. Burada korunan asıl şey devletin hukuksal değer yüklediği bir bilgidir. Yapılan sahtecilik eylemi zaman zaman şahısları doğrudan ilgilendirebilecek olsa da bu konuda suçun mağduru her zaman devlettir. Eylemden zarar gören şahıs ise “suçtan zarar gören kimse” konumundadır.<sup>23</sup>

Bu suç incelenirken dikkat edilmesi gereken diğer bir nokta da evraklarda tahrifatın bilişim sistemleri üzerinden yapılmış olması gerektiğidir. Yani tahrif edilmiş olan, bilişim sistemi üzerinde bulunan bir veri olmalıdır. Örneğin; bilişim sistemleri üzerinde iken tahrifata uğramış bir sözleşmenin yazıcıdan çıktısının alınarak tahrif edilmiş şekilde uygulamaya sokulması, evrakta sahtecilik suçunu oluşturacaktır.<sup>24</sup>

#### **2.2.2.2. Bilgisayarla Bağlantılı Dolandırıcılık**

Dolandırıcı sözcüğünün Türkçe sözlükte açıklaması; “Birini aldatarak mal veya parasını alan kimse”<sup>25</sup> olarak belirtilmiştir. Dolandırıcılık ise; “Dolandırıcı olma durumu”<sup>26</sup> olarak tanımlanmıştır. Bu tanımlardan yola çıkarak dolandırıcılığı; hileli davranışları bir kişiyi kandırıp kendisine veya bir başkasına fayda sağlamaya çalışmak olarak tanımlayabiliriz.

Bilgisayarla bağlantılı dolandırıcılığı ise “dolandırıcılık eyleminin bilişim sistemleri üzerinden yapılması yolu ile, failin kendisine veya bir başkasına haksız fayda sağlaması” olarak tanımlayabiliriz.

---

<sup>22</sup> Tanrıku ve diğ., "Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu." **"Kamu Bilişim Platformu 9"** Mayıs (2007) s.41

<sup>23</sup> age, s. 42.

<sup>24</sup> age, s. 43.

<sup>25</sup> [http://www.tdk.gov.tr/index.php?option=com\\_gts&arama=gts&guid=TDK.GTS.5acdedbe05cb02.27771390](http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5acdedbe05cb02.27771390) [Erişim tarihi: 20.10.2018]

<sup>26</sup> [http://www.tdk.gov.tr/index.php?option=com\\_gts&arama=gts&guid=TDK.GTS.5acdedcbdd5266.96043506](http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5acdedcbdd5266.96043506) [Erişim tarihi: 20.10.2018]

Avrupa Konseyi Siber Suçlar Sözleşmesinde bu suçu şu şekilde yer verilmiştir;

*“Taraflardan her biri, aşağıda belirtilenler, kasten veya haksız yere gerçekleştirildiği zaman, bir başka şahsın mal kaybına sebebiyet verdiğinde, bunların kendi iç hukukunda cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.*

*Şahısların kendilerine veya bir başkasına haksız yere maddi menfaat sağlamak için hile veya sahtekârlık yapmak niyetiyle;*

*Bilgisayar Sistemlerine Veri Girişi Yapmak, Verileri Değiştirmek, silmek veya engellemek.*

*Bir Bilgisayar Sisteminin İşleyişine Herhangi Bir Müdahalede bulunmak.”*

Bu maddeye bakıldığı zaman suçun gerçekleşebilmesi için öncelikle kastın varlığından söz edilmesi gerektiği görülmektedir. Eğer ortada kasıt yoksa suç da gerçekleşmiş olmayacaktır. Yani bilgisayar sistemleri üzerinden yanlışlıkla veya bilinçsizce yapılan bir hareket sonucu, diğer bir kişi maddi olarak zarara uğramış ve fail bu durumdan maddi bir kazanım elde etmiş olsa bile, suç oluşmayacaktır. Diğer bir durum ise; dolandırıcılık eyleminin mağdur üzerinde mal kaybına sebebiyet vermesi gerektiridir.

Avrupa Konseyi Siber Suçlar Sözleşmesinin TCK’ya yansımaları ise farklı maddelerde karşımıza çıkmaktadır. Bunlarda ilki nitelikli dolandırıcılığın tanımlandığı 158. Maddenin 1. Fıkrasının f bendinde, “Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle” şeklinde belirtilmiştir ve bu şekilde gerçekleştirilen dolandırıcılık suçu da cezayı arttıran bir unsur olarak belirlenmiştir.

İkincisi ise banka veya kredi kartlarının kötüye kullanılması başlığı altında, 245’nci maddenin ilk üç fıkrasında belirtilmiştir. Bu üç fıkra aşağıdaki gibidir.

Birincisi fıkra;

*“Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.”*

İkinci fıkra;

*“Başkalarına ait banka hesaplarıyla ilişkilendirilerek sahte banka veya kredi kartı üreten, satan, devreden, satın alan veya kabul eden kişi üç yıldan yedi yıla kadar hapis ve on bin güne kadar adli para cezası ile cezalandırılır.”*

Üçüncü fıkra;

*Üçüncü fıkrası; “Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır*

*cezaı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan sekiz yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.”*

Bu madde incelendiğinde maddenin, bilişim sistemleri vasıtasıyla dolandırıcılık eyleminin genelde kredi kartları ve banka hesapları üzerinden olan kısımları ile ilgili olduğu görülmektedir. İlk fıkrada başkasına ait bir kartın kullanılması, ikinci fıkrada sahte kartın üretilmesi vb. eylemler, üçüncü fıkrada ise sahte kartların kullanılması üzerinde durulmuştur.

Dikkat edilmesi gereken bir diğer nokta ise günümüzde bu suçun sosyal medya üzerinden işlenen halinin giderek artmakta olduğudur. Sosyal medya üzerinden işlenen dolandırıcılık eylemleri de suç oluşturmaktadır. Buna örnek olarak sosyal ağlar üzerinden satış yapan ve çok sayıda takipçisi bulunan bir satıcının yapılan antlaşma sonucunda parayı alması fakat satışa konu malı teslim etmemesi gösterilebilir.<sup>27</sup>

### **2.2.3. İçerikle Bağlantılı Suçlar**

#### **2.2.3.1. Çocuk Pornografisi**

Çocuk pornografisinin tanımı, kamu bilişim platformunun Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu konulu çalışmasında; *“Bir çocuğun gerçek veya kurgulanmış herhangi bir cinsel aktivite içinde gösterilmesi veya vücudunun belli yerlerinin cinsel amaçla gösterilmesidir.”*<sup>28</sup> şeklinde yapılmıştır.

Günümüzde dünya genelinde internet kullanımının aşırı derecede artması ile birlikte bu tür içeriklere erişim de daha kolay hale gelmeye başlamıştır. Bu tür içeriklerin daha çok evden kaçmış, terkedilmiş veya ilgisiz kalmış çocukların sömürülmesi ile üretilmesinin bilindiği gibi bilişim teknolojileri kullanılarak oluşturulan sanal çocuklar üzerinden de üretildiği bilinmektedir.

Avrupa Konseyi Siber Suçlar Sözleşmesinin dokuzuncu maddesine göre; taraf devletler, bir bilgisayar sistemi üzerinden dağıtımını yapmak amacıyla çocuk pornografisi üretmek, sunmak veya erişilebilir hale getirmek, dağıtımını veya iletimini yapmak, kendisi veya bir başkası için bilgisayar sistemi üzerinden çocuk pornografisi temin etmek, bir bilgisayar sisteminde veya bilgisayar verileri depolama aygıtında

---

<sup>27</sup> <http://www.yurtgazetesi.com.tr/gundem/aman-dikkat-dolandiricilarin-yeni-mekani-instagram-h86713.html> [Erişim Tarihi: 15.10.2018]

<sup>28</sup> Tanrıku ve diğ., "Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu." *Kamu Bilişim Platformu 9* Mayıs (2007) s.65

çocuk pornografisi bulundurmak eylemlerini suç olarak kendi hukuk sistemlerine dâhil etmek durumundadır.

Yine aynı sözleşmeye göre çocuk pornografisinin tanımı; reşit olmayan şahsın ve/veya bu görünümdeki bir şahsın cinsel içerikli eylemlerde bulunması ve bunları betimleyen gerçekçi görüntüler olarak tanımlanmıştır. Aynı maddenin üçüncü fıkrasında da “reşit olmayan” teriminin tanımı; 18 yaş altındaki tüm şahıslar olarak tanımlanmış olup taraf devletlere 16’dan küçük olmamak kaydıyla kendi sınırlarını belirleyebilme imkânı tanınmıştır.

5237 sayılı TCK’da bu suçlar her ne kadar çocuk pornografisi başlığı altında olmasa da genel ahlaka karşı işlenen suçlar başlığının müstehcenlik kısmında aşağıdaki şekilde düzenlenmiştir;

*“Müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanan kişi, beş yıldan on yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır, bu ürünleri ülkeye sokan, çoğaltan, satışa arz eden, satan, nakleden, depolayan, ihraç eden, bulunduran ya da başkalarının kullanımına sunan kişi, iki yıldan beş yıla kadar hapis ve beş bin güne kadar adli para cezası ile cezalandırılır.”*

Adalet Bakanlığı tarafından hazırlanan bilişim suçları ile ilgili tasarının yirmi altıncı maddesinin birinci fıkrasında bu suçun bilişim sistemleri üzerinden işlenmesi halinde düzenlemenin nasıl olacağı aşağıdaki şekilde belirtilmiştir.

*“Bir çocuğa veya çocuk gibi görünen veya çocuk olduğu izlenimi veren bir kişiye ait gerçek ya da temsili görüntü, yazı veya sesleri içeren pornografik ürünleri bilişim ortamında dağıtmak amacıyla üreten kişiye sekiz yıldan on iki yıla kadar hapis ve beş bin güne kadar adli para cezası verilir.”*

Tüm bu düzenlemelerin yanında, bilişim sistemleri veya photoshop vb. gibi bir takım yazılımların kullanılarak montaj ile oluşturulan sanal çocukların kullanıldığı pornografik görüntülerin üretilmesi, yayınlanması, bulundurulması gibi konuların da yasal düzenlemelere eklenmesi gerektiği unutulmamalıdır.

#### **2.2.4. Telif Hakkı ve Bununla Bağlantılı Hakların İhlaline İlişkin Suçlar**

Kültür ve Turizm Bakanlığının Telif Hakları Genel Müdürlüğünün tanımına göre telif hakkı; “ Kişinin her türlü fikri emeği ile meydana getirdiği ürünler üzerinde hukuken sağlanan haklardır.” şeklinde tanımlanmıştır.

Ülkemizde telif haklarının korunmasına ilişkin süreç Osmanlı İmparatorluğu dönemlerine rastlamaktadır. Bu süreç matbaanın daha geç kurulmuş olması sebebiyle Avrupa’dakinden yaklaşık 300 yıl daha geç başlamıştır. 1857 yılında Osmanlı

Devletinde “Telif Nizamnamesi” adı ile bir düzenleme yapılmıştır fakat bu düzenleme çağın gereklerini karşılayamamıştır. Kanun niteliğinde ilk düzenleme “Hakkı Telif Kanun” adıyla ilk defa 8 Mayıs 1910 tarihinde yapılmıştır ve bu kanun 1 Ocak 1952 tarihine kadar yürürlükte kalmıştır. 1 Ocak 1952 tarihinde 5846 sayılı “Fikir ve Sanat Eserleri Kanunu” yürürlüğe girmiştir. Bu kanun çeşitli yıllarda değişikliğe uğrayarak bugünkü halini almıştır ve halen yürürlüktedir.

Avrupa’da ise telif haklarını düzenleyen 2 temel antlaşma söz konusudur. Bunlarda birincisi; Yazın ve Sanat Ürünlerinin Korunmasına ilişkin Bern Anlaşması diğeri ise; Roma’da yapılan Uluslararası Fonogram üreticilerini, kullanıcılarını ve yayıncı kurumları koruma anlaşmasıdır.\*

Avrupa Konseyi Siber Suçlar Sözleşmesinde telif haklarının siber ortamda korunmasına değinirken özel bir tanımlama yapılmayarak bu iki antlaşmanın kapsam alanına giren suçların kasıtlı olarak ve ticari boyutta bilgisayar sistemle vasıtasıyla işlendiğinde suç olarak tanımlanması ile ilgili taraf devletlere sorumluluk yüklenmiştir. Keza Türk Ceza Kanununda da siber ortamda telif haklarının korunması ile ilgili bir düzenleme bulunmamakla birlikte bu suçlar 5846 numaralı “Fikir ve Sanat Eserleri Kanunu” nda tanımlanmıştır. Bu kanunda tanımlı suçların siber ortamda işlenmesi ile de aynı cezai hükümlerin uygulanacağı açıktır.

### **2.3. Siber Suçların İşlenme Biçimleri**

#### **2.3.1. Bilgi ve Veri Aldatmacası (Data Didling)**

Bilgi ve veri aldatmacası bilişim sistemine işlenmiş verilerin sahte verilerle değiştirilmesi veya verilerin manipüle edilerek girilmesi ile oluşmaktadır. Bu suç işleme biçimi bilişim alanında tercih edilen basit ve yaygın bir suç işleme biçimidir. Zira bu suçun işlenebilmesi için ileri seviyede bilgisayar bilgisine ihtiyaç yoktur. Bilgisayar kullanmasını basit seviyede bilen bir şahıs bu suçun faili olabilmektedir. Diğer taraftan bu suç bilişim sistemlerine uzaktan erişim sağlanıp sistemin mevcut güvenlik duvarları aşılarda ta işlenebilir. Her iki durumda da asıl olan doğru bilginin manipüle edilip failin kendisine maddi veya manevi haksız bir kazanç sağlamasıdır.

---

\* Roma Antlaşması.

Bu suçun işlenmesine örnek olarak bir banka şubesinde bulunan veznedarın uzun süreden beri işlem görmeyen hareketsiz hesapları takip etmesi ve beraber çalıştığı iş arkadaşının kısa süreli olarak bilgisayarının başından ayrılırken ekranı kilitlememesini fırsat bilerek söz konusu hesaplardan ödeme talimatı vermesi ve vezneden ödemeyi alarak paraları kendi zimmetine geçirmesi verilebilir.

### 2.3.2 Salam Tekniği (Salami Techniques)

Salam tekniği çok fazla sayıdaki değerden az miktarda belirlenen varlığın belirli bir havuza aktarılmasıdır.<sup>29</sup> Bu bilişim suçu metodu genellikle bankalarda veya çok sayıda çalışanı olan iş yerlerinin muhasebe bölümlerinde gerçekleşmektedir. Bu yöntemde banka hesaplarının veya çalışanların maaşlarının küsuratlarının belirlenen kısımları failin hesabına aktarılmaktadır. Böylelikle hak sahipleri varlıklarında küçük değişikliği fark edememekte fakat failin hesabında çok fazla hesaptan alınan küçük değerler toplanıp fail adına haksız bir kazanç sağlamaktadır.

Küçük bir hesapla; örneğin, 1.000.000 müşterisi olan bir bankada failin hesaplardan 10'ar kuruşu kendi hesabına aktardığını farz edersek, fail toplamda bu tekniğin uygulayarak kendi hesabına 100.000 TL aktaracaktır.

Bu tekniğin gerçekleştirilebilmesi için fail genellikle kötücül yazılımlar\* kullanmaktadır.<sup>30</sup>

### 2.3.3. Süper Darbe (Super Zapping)

Süper darbe çeşitli sebeplerle işlemez hale gelen bilişim sistemlerine, güvenlik tedbirlerini aşarak kısa sürede müdahale edilmesini sağlayan programlardır.<sup>31</sup>

### 2.3.4. Eş Zamansız Saldırıları (Asynchronous Attack)

Eş zamanlı çalışma bilişim sistemlerinin birden çok işlemi aynı anda yürütmesine verilen isimdir. Bazı durumlarda ise bilişim sistemleri işlemleri belirlenmiş bir sırada yürütmektedirler buna da eş zamansız çalışma denilmektedir. Bu durumlarda bir işlemin başlatılması için başka bir işlemin bitmesi beklenmektedir. Eş

---

<sup>29</sup> Zakir Avşar, Gürsel Öngören. *Bilişim hukuku*, yayın no:270 (İstanbul, Türkiye Bankalar Birliği, 2010), s.51

\*Trojanlar , truva atları ve virüsler gibi istenmeyen kötü niyetli yazılımlara verilen genel bir isim.

<sup>30</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.27

<sup>31</sup> Ebru ALTUNOK, Ali Fatih VURAL, “Bilişim Suçları”, *Denetim*, s.8 (2011): S.74.

zamansız saldırılarda suçlunun hedefinde bellekte işlem yapılması için bekleyen veriler bulunmaktadır. Sisteme herhangi bir şekilde girilerek işlem bekleyen veriler üzerine değişiklik yapılması, eş zamansız saldırı olarak adlandırılmaktadır. Bu saldırı türünün en bariz örneği yazıcıda işlem bekleyen belgeler üzerinde değişiklik yapılması olarak belirtilmektedir.<sup>32</sup>

### 2.3.5. Truva Atı

Truva atları yasal veya yasal gibi görünen bir programın içine yerleştirilmiş, belirlenen yerlerden belirlenen bilgileri toplayıp belli bir yere gönderen programlardır. Virüslerden farklı olarak kendilerini kopyalayamazlar ve yayılma amaçları yoktur. Genel olarak indirilen programlar içinde veya e-posta üzerinden sisteme yerleşmektedirler.<sup>33</sup>

Truva atları istemci ve sunucu olmak üzere iki bölümden oluşurlar, istemci hedef bilişim sistemi üzerindeki verilerin gönderildiği ve söz konusu sisteme müdahale edebilen bölüm, sunucu ise hedef bilgisayar üzerine yüklenmiş ve amacı topladığı bilgileri istemciye göndermek olan programdır.<sup>34</sup>

### 2.3.6. Zararlı Yazılımlar

Genel olarak truva atı mantığı ile çalışırlar fakat truva atlarından farklı olarak, yayılma amacı güderler. Başka bilgisayar veya bilişim sistemlerine geçerek bu sistemlerde (yavaşlama, kendini kopyalayarak sistemi çalışamaz hale getirme, bilgileri başka sistemlere gönderme vb.) çeşitli etkiler meydana getirirler.

### 2.3.7. Mantık Bombaları (Logic Bombs)

Önceden belirlenmiş durumlar oluşuncaya kadar, kendini sistemin içerisinde gizleyip belirlenen durum gerçekleştiğinde harekete geçerek sisteme yıkıcı zararlar vermek üzerine tasarlanmış bilgisayar programlarıdır. Belirlenen şartlar gerçekleşinceye kadar truva atları gibi kendilerini saklarlar fakat şartlar gerçekleştiğinde harekete geçme özellikleri ile onlardan ayrılırlar.

Mantık bombalarına verilecek en güzel örneklerden bir tanesi; 1982'de (soğuk savaş döneminde) Sovyet ajanların Kanada'dan çaldıkları ve Sibiry'a'dan geçen

---

<sup>32</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.28

<sup>33</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.28

<sup>34</sup> Burak Tunç BİLEK, *Bilişim Suçları Ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri* (Ankara: Gazi Üni. Bilişim Enstitüsü Yüksek Lisans Tezi, 2012), s.37



doğalgaz boru hattının yönetilmesinde kullanılan bir yazılımın, CIA ajanları tarafından fark edilerek programın içine yerleştirilen bir mantık bombası ile belirlenen tarih ve saatte sisteme aşırı yükleme yaptırılarak boru hattının patlatılmasıdır.<sup>35</sup>

#### **2.3.8. Oltalama (Phishing)**

Mağdurun, yüksek güvenlik seviyesindeki bilgilerini (şifre vb.) ele geçirmek amacıyla sosyal mühendisliğin kullanılması olarak tanımlanmaktadır.

Genellikle mevcut resmi internet sitesi veya uygulamanın bir benzeri yapılarak kurbanın buralara girdiği bilgiler art niyetli bilgisayar korsanlarınca çalınır.

Oltalama da diğer bir yöntem ise e-mail üzerinden bir kısım bilgilerin güncellemesinin talep edilmesidir. Eğer kurban bunu fark etmez ve istenen bilgileri gönderilen forma girerse bilgiler direkt olarak bilgisayar korsanına gönderilmiş olur.<sup>36</sup>

#### **2.3.9. Tarama (Scanning)**

Bilişim sisteminin olumlu cevap vereceği durumların tespit edilebilmesi için belirli bir algoritma ile bir kısım değerlerin sisteme hızlı bir şekilde girilmesi ve sistemin kabul ettiği değer veya değerlerin tespit edilmeye çalışılmasıdır. Olabilecek tüm seçeneklerin denenerek cep telefonu şifrenizin tespit edilebilmesi bu duruma örnek olarak gösterilebilir. Bu işlemi yapabilen programlar internet üzerinden bulunabileceği gibi aynı zamanda bilgisayar korsanlarınca da geliştirilebilmektedir.

#### **2.3.10. Bukelamun (Chalemon)**

Bu programlar bilişim sistemlerinde diğer normal programlar gibi çalışırlar fakat aynı zamanda gizli dosyalar oluşturarak bir takım aldatmalar ile kullanıcının şifrelerini açtıkları bu gizli dosyalara kaydederler. İlerleyen bir zamanda sistemin kapatılacağını kullanıcıya bildirip bu arada daha önceden kaydettikleri bilgileri istemciye gönderirler.<sup>37</sup>

---

<sup>35</sup> Uğur TADOĞAN “Savaşa hazır mıyız?”, <https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527> [Erişim Tarihi: 20.11.2018]

<sup>36</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.30

<sup>37</sup> Fulya ASLAY, *Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi* (International Journal of Multidisciplinary Studies and Innovative Technologies) c.1,s.1 (2017) s.24-28

### 2.3.11. İstem Dışı Alınan Elektronik Postalar (Spam)

Spamlar internet kullanıcılarına istekleri dışında gönderilen aynı veya benzer içerikli genelde reklam amaçlı e-postalardır. Reklam amacı gütmeyen diğer bir spam türü de bulunmaktadır. Bunlar eşzamanlı olarak on binlerce e-posta hesabına gönderilen kamuoyu oluşturmak veya siyasi propaganda yapmak amacı ile gönderilen e-postalar da olabilir.<sup>38</sup>

Spam gönderen şahıslara veya kuruluşlara spammer denilmektedir. Spammerların sizin e-posta hesaplarınızı ele geçirmek için kullandığı pekçok yöntem bulunmaktadır. Örneğin herhangi bir internet sitesine üye olmak için e-posta hesabınızı belirtmek zorundasınız. Bu hesaplar bilgisayar korsanları tarafından toplanır ve spam göndermek için kullanılır. Bunun dışında posta listeleri, tartışma grupları, forumlar vb. ortamlar spammerlar tarafından e-posta adresi temin etmek maksadıyla sıkça kullanılan alanlardır.<sup>39</sup>

2007 yılında dünya genelinde 1 milyardan fazla e-posta üzerinde yapılan bir incelemede gönderilen e-postaların %95'inin spam içerikli olduğu tespit edilmiştir.<sup>40</sup>

### 2.3.12. Çöpe Dalma (Scavenging)

Bu suç işleme türünde bilişim sistemleri üzerinde gerçekleştirilen bir işlem sonrasında geride kalan veriler toplanmaktadır. Bu yöntemde genellikle bilişim sistemlerinin belleğinde kalan fakat kullanıcılar tarafından önemsiz addedilen bilgiler toplanır veya silinmiş fakat halen bellekte yer tutan bilgiler çeşitli programlarla geri getirilmeye çalışılır.<sup>41</sup>

### 2.3.13. Gizli Kapılar (Trap Doors)

Gizli kapılar, bir bilgisayar programı yapılırken geliştirici tarafından programın içine yerleştirilmiş virüs yazılımıdır. Program yasal olarak çalışırken arka planda çalışan virüs yazılımı tespit edilen bilgileri yasal programı hazırlayan istemciye göndermektedir.

---

<sup>38</sup> “Spam Nedir?”, <http://web.deu.edu.tr/ssss/spam.html> [Erişim Tarihi: 20.11.2018]

<sup>39</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.30

<sup>40</sup> Özen, Ü. ve Sarı A. *Gazi Üniversitesi Bilişim Teknolojileri Dergisi*, Cilt:1, Sayı: 3’ten aktaran M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.30

<sup>41</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.32

#### 2.3.14. Sırtlama (Piggybacking)

Bilişim sistemlerine elektronik veya fiziki yollarla yetkisiz olarak erişimin sağlanmasıdır.

Elektronik sırtlamada yasal kullanıcıların kullandıkları hatlar üzerinden bilişim sisteme yetkisiz olarak erişim sağlanır. Fiziki sırtlamada ise söz konusu bilişim sistemine girme yetkisi bulunan kullanıcının bilgilerinin ele geçirilmesi ile yetkisiz erişim sağlanır.<sup>42</sup>

#### 2.3.15. Yerine Geçme (Masquerading)

Bilişim sistemleri genellikle kendi içlerinde farklı yetki seviyelerine sahiptir. Kullanıcıların yetkileri dâhilindeki bilgilere erişilmesine izin verilmektedir. Kullanıcıların ilgili verilere erişebilmesi öncelerde sadece kullanıcı adı ve parola ile sağlanırken teknolojinin gelişmesi ile birlikte artık parmak izi, retina taraması, yüz tanıma sistemleri vb. güvenlik seviyesi daha yüksek tedbirler ile erişimler mümkün olmaya başlamıştır. İşte yetkili kullanıcıların sahip olduğu bilgilerin bir şekilde ele geçirilmesi veya sahip olduğu fiziksel özelliklerin taklit edilmesi yolu ile sisteme erişim sağlanmasına, yerine geçme denilmektedir.<sup>43</sup>

#### 2.3.16. Sistem Güvenliğinin Kırılıp Sisteme Sızılması (Hacking)

Hacking sözcüğü ilk kullanılmaya başlanıldığı zamanlarda, alışılmışın dışında yenilikçi ve yaratıcı bir biçimde bilgisayar kullanmak anlamını taşıyordu. Zamanla bu anlamdan çıkarak aktivist faaliyetlerin hacking eylemleri ile uygulanması anlamında kullanılmaya başlandı.<sup>44</sup>

Hacking eylemleri 5 safha da gerçekleşir. İlk safhada hedef hakkında bilgi toplanır, ikinci safhada hedef sistem taranır ve sistemin ağ haritası oluşturulur, üçüncü safha hedef sisteme erişim safhasıdır, dördüncü safha ele geçirilen hedef sistemden

---

<sup>42</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.32

<sup>43</sup> Kurma, E. (1999) Approaching Zero Data Crime and the Computer Underworld, çeviri (Mungo,P. Ve Bryan Clough) den aktaran M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.33

<sup>44</sup> Ceren Yeğren, "Dijital aktivizmin bir türü olarak Hacktivism ve "Redhack". *E-Journal of Intermedia* c.1, s.1 (2014): s.118-132

bilgi elde etme safhasıdır. Son safha ise hedef sistemde iz bırakmadan ve tespit edilmeden sistemden çıkma safhasıdır.<sup>45</sup>

### 2.3.17. Hukuka Aykırı İçerik Sunulması

Hukuka aykırı içerik ülkelerin yasalarına göre değişkenli arz etmektedir. Ülkemizde bu düzenleme “İnternet Ortamında Yapılan Yayınların ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun” ile düzenlenmiştir. Bu kanuna göre genel olarak intihara yönlendirme, çocukların cinsel istismarı, uyuşturucu madde kullanılmasını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, fuhuş ve kumar internet üzerinden yapılan yasadışı yayınlar olarak kabul edilmektedir.<sup>46</sup>

Yasadışı içerikle mücadele genelde yasadışı yayın yapan web sitesine erişimin engellenmesi ve eğer tespit edilebilirse söz konusu sitenin sahiplerine yasal yaptırımların uygulanması yoluyla yapılmaktadır. Ancak erişim yasağı getirilen sitelere bazı tekniklerle girilebilmesi bakımından bu tedbirin işe yaradığı pek söylenemez.<sup>47</sup>

### 2.3.18. Web Sayfası Hırsızlığı ve Yönlendirme

Bir kişi veya firma eğer bir internet sitesi üzerinden yayın yapmak istiyor ise öncelikle bir internet sitesi açmalıdır ve siteye bir ad belirlemelidir (Alan adı almalıdır). Şayet istenilen alan adı daha önce başka bir kullanıcı tarafından alındıysa aynı adın ikinci kere alınması mümkün olmadığından, alan adını önce tescil ettiren şahıslar genelde bu alan adlarını olması gerekenden çok daha yüksek fiyatlara satmaktadırlar. Bu suç genelde internet servis sağlayıcılarının başvuru içeriklerini kötü niyetli üçüncü kişilere ulaştırması şeklinde işlenmektedir.<sup>48</sup>

Diğer bir yöntem ise DNS sunucularında hukuka aykırı şekilde değişiklikler yaparak web sitesinin başka bir IP adresine yönlendirilmesi sonucunda istenilen site yerine tamamen farklı bir siteye erişilmesi şeklinde olmaktadır.<sup>49</sup>

---

<sup>45</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.33

<sup>46</sup> M.Alper SÖZER ve Diğ. *Kriminoloji* (Ankara Nobel Yayıncılık 2016), s.272

<sup>47</sup> M.Alper SÖZER ve Diğ. *Kriminoloji* (Ankara Nobel Yayıncılık 2016), s.273

<sup>48</sup> M.Akif OCAK ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara 2014) s.34

<sup>49</sup> age, s. 34.

Başka bir yöntem ise kötü niyetli kişilerin genel olarak yapılan yazım yanlışlarından yararlanması ile ortaya çıkmaktadır.<sup>50</sup> Örneğin Türkiye’de vatandaşlık işlemlerinin yapılabildiği internet sitesi www.turkiye.gov.tr iken kötü niyetli kullanıcılar tarafından www.turkiye.com.tr adresi yasadışı yayın yapmak amacıyla kurulursa her gün yanlışlıkla yüzbinlerce ziyaretçi alabilir.

### **2.3.19. Sosyal Mühendislik\***

Sosyal mühendislik; bilgisayar korsanının, ilgilendiği sistemin kullanıcılarını hedef alarak onlar üzerinden sisteme erişim sağlamak için uyguladığı her türlü sosyal ve psikolojik aldatmacalar olarak tanımlanmaktadır.<sup>51</sup>

Sosyal mühendislik genelde suçlunun kişisel becerilerine dayanan ve mağdurun zayıf yanlarından faydalanan bir siber suç işleme tekniğidir. Sosyal mühendisliği etkin bir şekilde uygulayan suçlu, çok kısa bir zamanda mağdurdan istediği bilgileri toplayabilir ve bu şekilde sisteme giremse bile sistem içinde bulunan istediği bilgiyi rahatça ele geçirebilir. Sosyal mühendislik saldırılarının önlenmesi için bilişim sistemine girmeye yetkili şahıslar çok iyi seviyede eğitilmelidirler.

---

<sup>50</sup> age, s. 35.

\* Sosyal mühendisliğin sadece siber suç işleme yöntemi olarak değerlendirilmesi uygun değildir. Sosyal mühendislik dolandırıcılık vb. diğer pek çok konuda uygulanabilir, psikolojinin ve diğer bilimlerin ilgi alanına girebilir. Çalışma konusu kapsamında değerlendirildiğinde burada sadece siber suç işleme yöntemi olarak ele alınmıştır.

<sup>51</sup> Barwinski, M. A., Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads, Thesis, Naval Postgraduate School, Monterey, California, 37, September 2005. Den aktaran G.CANBEK, Ş.SAĞIROĞLU *Bilgisayar Sistemlerine Yapılan Saldırılar Ve Türleri: Bir İnceleme* Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi S.23, 2007, s. 1-12



## ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

### 3.1. Rutin Aktiviteler Teorisi

#### 3.1.1. Rutin Aktiviteler Teorisinin Oluştığı Ortam

İkinci Dünya Savaşı sonrasında ve devam eden süreçte, başta ABD olmak üzere, dünya üzerindeki devletlerde gerek kamusal alanda gerekse şahısların özel yaşantılarında ve yaşam tarzlarında önceden tahmin edilemeyen ve geri dönüşü olmayan değişimler hızlı bir biçimde yaşanmaya başlamıştır. Özellikle toplumsal alanda, dünyada o zamana kadar alışılmış toplumsal yaşamın dışında, kadınlar da iş yaşamına girerek topluma daha fazla adapte olmaya başlamışlardır. Toplumsal yaşamda meydana gelen bu hızlı değişiklik beraberinde çeşitli çalkantılar da meydana getirmiştir. Toplumsal yaşamın değişmesi ile birlikte güven ortamı ve asayiş bozulmuş, bunun sonucunda da suç oranlarında bir artış meydana gelmiştir.<sup>52</sup>

İkinci Dünya Savaşı'ndan önceki suç teorileri (Klasik okul) suçun kaynağını genetikte, doğaüstü güçlerde, insanların acıdan kaçmasını sağlayacak şekilde yaptığı rasyonel tercihlerde aramıştır. İkinci Dünya Savaşı sonrasında artan suç oranlarının önüne geçilebilmesi maksadıyla rutin aktiviteler teorisi ile suçun kaynağı araştırılırken ilk defa suç mekanizması üzerinden durulmuş, bu mekanizmanın incelenerek suç olayının engellenebileceği Lawrance COHEN ve Marcus FELSON'un "Social Changes And Crime Rate Trends: A Routine Activity Approach" isimli makalelerinde savunulmuştur.

Bu yeni yaklaşım, sosyal hayatın değişmesi ile birlikte aşırı derecede artan suç olaylarının açıklamasını tartışmış, mağdurların ve suçluların hayatın olağan akışı içinde yaşadığı günlük rutinlerin suç sayısındaki artışın sebebi olduğunu savunmuştur.<sup>53</sup>

Teoride başlangıçta suçun unsurları araştırılmış ve bu unsurlar uygun hedef, motive olmuş suçlu ve koruyucuların yokluğu olarak belirlenmiştir. Sonraki dönemlerde teoriye bunlardan motive olmuş suçlunun engellenmesini sağlayan "tutucular" eklenmiştir. İlerleyen zamanlarda teorinin sokak suçlarını açıklamada daha etkin bir teori olduğu düşünülerek diğer suçların açıklanabilmesi maksadıyla suç

---

<sup>52</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.116

<sup>53</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.116

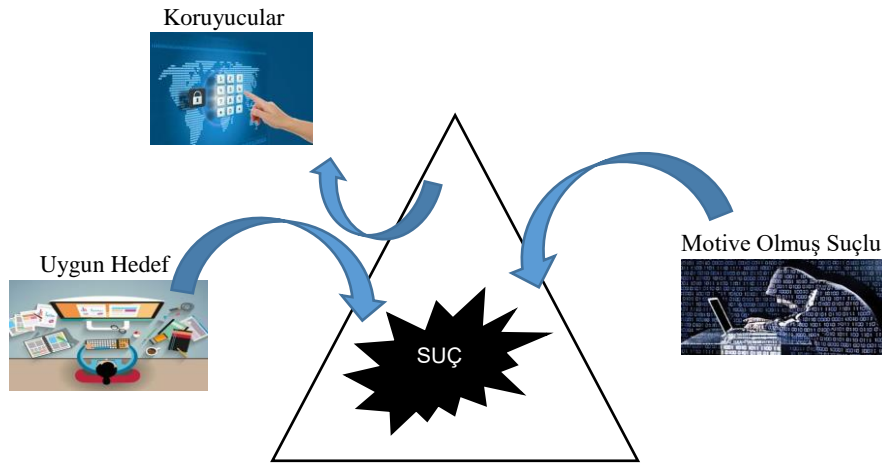
fırsatları yaklaşımı da eklenerek teori geliştirilmiş, rasyonel tercih teorisi\* ile birleştirilmeye çalışılmıştır. Bu bağlamda, sadece sokak suçlarında değil daha geniş bir alanda suçların açıklanabilmesine imkân sağlanmıştır.

Bu bölümde önce Rutin Aktiviteler Teorisi bağlamında sırasıyla suçun unsurları, sonradan eklenen unsur olan tutucular, suç fırsatları, teori bağlamında suç önleme stratejileri ve yapılan bilimsel çalışmalar incelenecektir.

### 3.1.2. Rutin Aktiviteler Teorisine Göre Suçun Unsurları

1979 yılına kadar olan yaklaşımlar suçu anlamada oldukça etkili olmuştu fakat bu yaklaşımlar genelde suçu mekânsal olarak analiz etmiş, suçun oluşmasında insan davranışlarının ve yapılan rutin faaliyetlerin etkilerini çok fazla dikkate almamıştır. Dolayısıyla ne kadar tedbir alınmış olursa olsun suçun önlenmesinde başarılı olunamamıştır.

Bu başarısızlık neticesinde suçun incelenmesi ve önlenmesi için yeni bir yaklaşıma ihtiyaç duyulmuştur. Bu bağlamda Cohen ve Felson tarafından suç mekanizmasının motive olmuş suçlu, uygun hedef ve hedefi koruyacak koruyucuların yokluğu olmak üzere Şekil 2 de gösterilen üç sacayağından oluştuğu iddiası ortaya atılmıştır.<sup>54</sup>



Şekil 2: Suçun Yapısı.

\* Şuçluların, suç işlerken en az çaba ile en çok getiriye sağlayacakları ve bununla birlikte en çok haz ile en az elemi birlikte yaşayacakları suç türlerini seçeceklerini savunan bir klasik okul teorisi.

<sup>54</sup> Lawrence E.COHEN, Marcus FELSON “Social Change And Crime Rate Trends: A Routine Activity Approach” *American Sociological Review* s.44 (Ağustos 1979): s.588-608



Bu durumda suçun oluşabilmesi için üç temel unsur vardır. Bunlardan ilki elbette, suç işlemeye niyetli olan, olumsuz motive olmuş kişi veya kişilerin varlığı, ikincisi (verilen emeğin karşılığını verebilecek değerde) suça uygun bir hedeftir. Son unsur ise ortamda bahsi geçen hedefi motive olmuş suçludan koruyabilecek bir koruma mekanizmasının (bekçi, ışık, ses vs.) bulunmaması gerekliliğidir.. Sayılan üç unsurun herhangi bir zamanda bir araya gelmesi suçu oluşturacaktır. Suç oluşmadan önleyici tedbirler ile bu üç unsurun aynı zaman ve mekânda bir araya gelmesi engellenebilirse suç oranları da zamanla azalacaktır.<sup>55</sup>

Şekil- 2 incelendiğinde motive olmuş suçlu ile uygun hedefin bir araya geldiği ortamlarda eğer hedefi koruyabilecek nitelikte bir koruyucu yoksa suç olayının gerçekleştiği, ortamda nitelikli koruyucu mevcut değilse suç olayının gerçekleşmediği görülecektir.

Bu bağlamda düşünüldüğünde içinde bulunulan zamanın önemli olduğu anlaşılır. Bu durumu bir örnekle açıklamak gerekirse saat 17:50 de nitelikli koruyucunun bulunduğu bir anda iş yerinden evine giden bir birey (uygun hedef ) yol üzerinde motive olmuş suçlu ile karşılaştığında suç olayı gerçekleşmeyecektir. Fakat nitelikli koruyucunun sadece 17:50 de ortamda bulunduğu kabul edilirse evine giden birey 17:55 te aynı yerden geçtiğinde ve motive olmuş suçlu ile karşılaştığında bu sefer suç olayı gerçekleşecektir.

Daha önceki suç teorilerinin hiçbirinde zaman, suç olayına etki eden bir kavram olarak düşünülmüyordu. İlk defa rutin aktiviteler teorisi ile suç ve mekân faktörünün yanına zaman faktörü de eklenerek suç daha geniş kapsamlı açıdan incelenmeye başlandı. <sup>56</sup>

Rutin aktiviteler teorisindeki zaman faktörünün temelinde Amos HAWLEY'in 1950 yılında yayımladığı "İnsan Ekolojisi Teorisi" (Human Ecology Theory) adlı meşhur teorisi yatmaktadır. Hawley bu teorisinde toplum yaşamının zamansal boyutlarını incelemiştir ve bu incelemeyi 3 farklı boyutta yapmıştır. Bu 3 boyut ritim, tempo ve zamanlamadır.<sup>57</sup> Ritim; bir yerden başka bir yer gidiş gelişleri ve sosyal hadisenin ne zaman meydana geldiğini, tempo; birim zamanda meydana gelen olay

---

<sup>55</sup> Lawrence E.COHEN, Marcus FELSON "Social Change And Crime Rate Trends: A Routine Activity Approach" *American Sociological Review* s.44 (Ağustos 1979): s.588-608

<sup>56</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.119

<sup>57</sup> age, s. 119.

sayısını ve zamanlama ise; aslında birbirinden bağımsız olan faaliyetlerin ne kadar koordinasyon ve benzerlik içinde meydana geldiklerini ifade etmektedir.<sup>58</sup>

Bu teori ile suç tanımının içine, suçlu ve mağdurların günlük yaşantı akışının benzerlikler barındırması ve neredeyse eşzamanlı hale gelmesi ile diğer teorilerin öngöremediği zamansal ve mekânsal bir bağlantı suçun oluşum mekanizması içine eklenmiştir.<sup>59</sup>

Bu teoride suçlu ve mağdurlar birbirlerinden ayrı olarak düşünülmemiş aksine suç olayının ortaya çıkabilmesi için bu iki unsur arasında dikkate değer bir ilişki olduğu ileri sürülmüştür.<sup>60</sup>

İnsanların rutin faaliyetleri genel olarak üç yerde devam etmektedir; evde, işyerinde ve bunlardan uzak mekânlarda. İşte bu üç mekânda özellikle insanların kendilerini koruyabilecekleri koruyuculardan uzakta olduğu mekânlarda (genelde bunlar ev ve işyerinden uzakta olan mekânlar olarak düşünülebilir.) suçlularla karşılaşma ihtimali daha fazladır. Buna istinaden insanların gerçekleştirdikleri rutin faaliyetlerle bağlantılı olarak genelde sokak suçları (Kapkaç, yankesicilik vb.) biçiminde tabir edilen suçların mağduru olma ihtimali daha da artmaktadır.<sup>61</sup>

Şimdi yukarıda anlatılan motive olmuş suçlu, suçun hedefi ve o hedefi motive olmuş suçlulardan koruyacak koruyucu unsurların yokluğunun incelemesi yapılacaktır.

### **3.1.2.1. Motive Olmuş Suçlu**

Bu teori, motive olmuş suçluların varlığını peşinen kabul ederek yine diğer teorilerden farklılaşmaktadır.<sup>62</sup> Bu durumda motive olmuş suçlular suçun oluşması için gerçekleşecek fırsatları takip edecek, hatta bu şartların yapay olarak oluşturulabilmesi için istedikleri önlemleri alabilecektir.<sup>63</sup>

---

<sup>58</sup> Hawley AMOS “Human Ecology: A Theory Of Community Structure.” (1950)’den aktaran Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.119

<sup>59</sup> Lawrence E.COHEN, Marcus FELSON “Social Change And Crime Rate Trends: A Routine Activity Approach” *American Sociological Review* s.44 (Ağustos 1979): s.588-608

<sup>60</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.120

<sup>61</sup> Lawrence E.COHEN, Marcus FELSON “Social Change And Crime Rate Trends: A Routine Activity Approach” *American Sociological Review* s.44 (Ağustos 1979): s.588-608

<sup>62</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.120

<sup>63</sup> age, s. 120.

Bu yaklaşımda pekçok insan potansiyel suçlu olarak kabul edilir. Şimdiye kadar suç işlememiş olmalarının nedeni, henüz önlerine suç işleyebilmek için gerekli fırsatların çıkmamış olması olabilir. Potansiyel suçlular uygun fırsatlarla birlikte gerçek suçlulara dönüşürler. Bu yüzden bu yaklaşımın temelinde insanlar potansiyel suçlu olarak görülüp suçun önlenmesi için diğer iki unsura odaklanılmıştır.<sup>64</sup>

Bu bağlamda Zipf'in en az çaba prensibine yüzeysel olarak değinmekte fayda vardır. Bu prensibe göre insanlar, elde etmek istedikleri şeyleri en az emek ve çaba ile elde etmeyi isterler. Bu bağlamda suçlular, suç işlemek için gidebilecekleri en yakın yerleri veya yollarının üzerindeki hedefleri seçerler.<sup>65</sup> Bu durumda suçluların yoğun bulunduğu bir mahalden veya oraya yakın bir yerden geçiyorsanız ve eğer koruyucularınız yoksa suç mağduru olma ihtimaliniz daha yüksektir.

Zipf'in ikinci prensibi ise; insanların konu üzerine fazla düşünmeden mevcut bilgilere göre hareket ettiklerini savunmaktadır.<sup>66</sup> Buna göre; nasıl ki daha ucuza alınabilecek bir ürün için genelde gerekli araştırmayı yapmayıp aynı üründen önümüze ilk çıkanı alıyorsak, motive olmuş suçlular da yollarının kesiştiği ve koruyuculardan yoksun ilk hedef üzerinde suç fiilini gerçekleştirmektedirler.

Bu durumda rutin aktiviteler teorisinin Zipf'in prensiplerinden etkilendiğini söylemek yanlış olmaz ama, Zipf'in bu prensipleri uzun zaman tasarlanarak ve gerekli çalışmaların yapılması suretiyle emek harcanarak işlenen suç fiillerini açıklamakta yetersiz kalmaktadır. Örneğin bir bankanın bütün güvenlik sistemlerini aşip banka müşterilerinin hesaplarından çok küçük miktarlarda paralar transfer ederek kendisine bir getiri sağlayan ve arkasında iz bırakmadan sistemden çıkarak yakalanmayan bir bilgisayar korsanının işlediği suç şüphesiz ki uzun süre planlanıp üzerinde çalışılmadan gerçekleştirilmiş olamaz.

### 3.1.2.2. Koruyucuların Yokluğu

Felson'a göre koruyucular denildiğinde akla ilk olarak polis ve diğer güvenlik kuvvetleri gelmektedir. Evet, bu unsurlar bir koruyucudur fakat çoğu zaman suç fiili gerçekleştirildiğinde olay mahallinde dahi olmamaktadır. Koruyuculardan asıl kasıt,

---

<sup>64</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.121

<sup>65</sup> George Kinsley Zipf, "*human behavior*" *principle of least effort* ( Newton, Massachusetts, 1948)

<sup>66</sup> age.

sokak suçları düşünüldüğünde, bir arkadaş, etraftaki diğer insan/insanlar, bir evcil hayvan veya başboş bir sokak köpeği ve benzeri şeylerdir.<sup>67</sup> Evden hırsızlık suçu düşünüldüğünde kapıda güçlü bir kilit, çalışan hatta sahte bir kamera sistemi vb. siber suçlar düşünüldüğünde bir anti virüs yazılımı, üzeri mat bantla kapatılmış bir bilgisayar kamerası, bir erişim şifresi vb., olabilir. Koruyucular denilince illa ki güvenlik güçlerinin düşünülmesi yanlıştır.

Suç mağduru olma ihtimalinin en az olduğu yer koruyucuların bulunduğu ortamlardır. İnsanların günlük rutinlerine dalıp etrafındakileri dışarıdan gelebilecek saldırılara karşı koruma ihtimalleri azaldığı için suçun önlenmesinde koruyucuların varlığı en önemli husustur.<sup>68</sup>

### 3.1.2.3. Uygun Hedef. (Suçun Hedefi

İnsanların ekonomik durumları iyileştikçe suçlular tarafından çalınacak daha fazla şeyin ortaya çıktığı, şahıslar üzerinde kıymetli pekçok şey taşıdıkları için gerek şahısların kendisine gerekse de mallarına yönelik olarak saldırı ihtimalinin gittikçe arttığı görülmektedir.<sup>69</sup> Yani bu teori kapsamında artan uygun hedeflerin suç sayısını arttırmakta etkili bir faktör olduğunu söyleyebiliriz. Bir başka deyişle motive olmuş suçluların yolu ne kadar çok uygun hedefler ile birleşirse ve hedefler koruyuculardan yoksunlarsa suç oranlarının da artacağı anlaşılmaktadır.

Bu durumda bir hedefi uygun yapan şeylerin araştırılması gerekmektedir. Aslında bir hedefi uygun yapan şey suçlular için o hedefi çekici yapan unsurlardır. Felson ve Cohen'e göre uygun hedef tanımı ile değerli, erişilebilir, görünür, durağan (rutin faaliyetlerde bulunan olarak anlaşılmalıdır.), koruyuculardan yoksunluk gibi özelliklere sahip olması gerektiği anlaşılmalıdır.<sup>70</sup> Günümüzde sıkça kullanılan dizüstü bilgisayarlar, cep telefonları ve benzeri ürünler özellikle hırsızlık bağlamında düşünüldüğünde taşınması kolay ve aynı zamanda maddi değerleri yüksek olduğundan uygun hedefler olarak düşünülebilir. Siber suçlar bağlamında düşünüldüğünde ise,

---

<sup>67</sup> Marcus FELSON, Rachel L.BOBA *Crime And Evreyday Life* (Washington D.C.: Sage Yayıncılık, 2010), s.110

<sup>68</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theroy* (Boston, Northeastern University Press, 1996), s.22

<sup>69</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.122

<sup>70</sup> Lawrence E.COHEN, Marcus FELSON "Social Change And Crime Rate Trends: A Routine Activity Approach" *American Sociological Review* s.44 (Ağustos 1979): s.588-608

zayıf güvenlik sistemlerine sahip fakat değerli bilgiler barındıran bilişim sistemleri uygun hedef olarak değerlendirilebilir.

Alan yazınına bakıldığında suç mağduru olmayı etkileyen beş temel unsurdan bahsedildiği görülmektedir. Bunlar; hedefin görünür olması, değerli veya arzu edilebilir olması, suça karşı korunmasız olması, hareket kabiliyeti ve erişilebilir olmasıdır. Şimdi bunların açıklamaları üzerinde durulacaktır.

#### **3.1.2.3.1. Hedefin Görünür Olması**

Motive olmuş suçlu tarafından sürekli bir hedef aranmaktadır. Bu durumda suça konu olabilecek unsurların dikkatsiz bir şekilde ortada bulundurulması suça davetiye çıkartmak gibi değerlendirilebilir. Örneğin kalabalık bir yerde bir deste para sayılması, Aracın içinde görülebilecek bir şekilde kıymetli bir eşya bırakılması ya da kıymetli veriler içerdiği bilinen bir bilişim sisteminin insanların göreceği bir yerde parola ile korunmaksızın terk edilmesi motive olmuş suçluları harekete geçirmek için çok güzel fırsatlardır.

#### **3.1.2.3.2. Hedefin Değerli Veya Arzu Edilebilir Olması**

Bir şeyin suç hedefi olmasını belirleyen en önemli faktör onun değerli ve arzu edilebilir olmasıdır.<sup>71</sup> Örneğin bir bilgisayar korsanının koruma seviyeleri aynı olan saldırılabileceği 10 tane bilgisayar olduğunu ve korsanın sadece bir bilgisayara saldıracağını farz ettiğimizde bilgisayar korsanı kendisine göre rasyonel bir tercih yapacak ve kendisi için daha değerli olana veya sızmayı daha fazla istediği bilgisayara saldıracaktır.

#### **3.1.2.3.3. Hedefin Suça Karşı Korunmasız Olması**

Korunmasızlık ile suçlunun hedefe ne kadar kolay ulaşılabilirdiği, ona ne kadar kolay saldırılabildiği ve hedefin saldırgandan ne kadar zor kaçabilirdiği kast edilmektedir. Bu durumda yaşlılar, çocuklar ve engellilerin diğer insanlara göre daha çok suç mağduru olacakları aşîkârdır.<sup>72</sup> Ya da anti virüs sistemleri ile korunmayan bir bilişim sistemi korunana nazaran daha korunmasız bir hedef olarak düşünülebilir.

---

<sup>71</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.123

<sup>72</sup> George E.ANTUNES ve diğ. “Patterns of Personel Crime Against The Elderly” *The Gerontologist* c.17. s.4 (1977) s.321-327

#### 3.1.2.3.4. Hareket Kabiliyeti

Bir hedefin suça konu olmasını etkileyen başka bir faktör de hedefin hareket kabiliyetidir. Hiçbir suçlu kendi kas gücüyle taşıyamayacağı ağırlıkta bir altın kütesini destek donanımları olmadan çalmaya teşebbüs etmez. Aksine arabalar suçluların taşıyamayacağı kadar ağır olmasına rağmen hareket kabiliyetleri yüksek olduğundan hırsızların hedefi haline gelebilir.<sup>73</sup>

#### 3.1.2.3.5. Hedefin Müsait ve Erişilebilir Olması

Hedefin müsait ve erişilebilir olmasından kasıt motive olmuş suçlunun rahatlıkla hedefe ulaşabilmesini ve oradan rahatça uzaklaşabilmesini ifade eder. Suçluların kullandığı güzergâh üzerinde bulunan değerli ve arzu edilebilir her şey potansiyel bir hedefdir. Dolayısıyla da suçluların daha çok bulunduğu yerlerde yaşayanlar daha fazla mağdur ve onların kullandıkları eşyalar diğer yerlerdekilere göre daha fazla suç konusu olurlar.<sup>74</sup>

Günümüzde insanların rutin faaliyetleri içinde evde geçirilen zamanın azalması ile birlikte evlerin gündüz vakitlerinde daha boş kalması evlerin müsait ve erişilebilir bir hedef olmasına neden olmuş, dolayısıyla evden hırsızlık olayları artmıştır.<sup>75</sup>

Siber ortam bu bağlamda düşünüldüğünde; insanların internette gezinti alışkanlıkları onların daha çok suç mağduru olmasına, ya da benzer internet kullanım alışkanlıklarına sahip olanların benzer suçların mağdurları olmasına sebep olabilir.

Yine güvenlik katmanları kolayca aşılabilecek ve geride iz bırakmadan kolayca çıkılabilecek müsait ve erişilebilir bilişim sistemleri her zaman bilgisayar korsanlarının hedefi olacaktır.

#### 3.1.3. Diğer Bir Faktör Olarak Tutucular

Felson, bu teoride suçu oluşturan faktörler olarak tanımlanan 3 faktörün dışında suçluların motive olmasını sağlayan şeyin ne olduğunun, motive olmuş suçlunun

---

<sup>73</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theory* (Boston, Northeastern University Press, 1996), s.22

<sup>74</sup> George E.ANTUNES ve diğ. “Patterns of Personel Crime Against The Elderly” *The Gerontologist* c.17. s.4 (1977) s.321-327

<sup>75</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theory* (Boston, Northeastern University Press, 1996), s.24

sergileyeceği suçlu davranışların nasıl engellenebileceğinin veya onları engelleyebilecek faktörler olup olmadığına dair araştırmaların eksik kaldığını düşünmüş ve teoriye bu işlevi yerine getirecek dördüncü bir unsur olarak tutucuların eklenmesi gerektiği<sup>76</sup> tezini ortaya atmıştır.

Felson “engellenmiş suçlu” yaklaşımında suçlu davranışlar gösterecek kişilerin çevre, aile ve toplum gibi tutucular tarafından engellenebileceğini düşünmüştür. Bunlardan en önemli tutucuların, kişiyi yakından tanıyan ve otoritesi suçlu tarafından kabul edilen bireyler olacağını savunmuştur.<sup>77</sup>

Rutin aktiviteler teorisi ilk olarak geliştirildiğine hedefin kontrol altında tutulmasının yani koruyucuların önemi üzerinde durulurken, Felson’un bu yaklaşımı ile birlikte suçluların engellenmesi gibi bir düşünce gelişmeye başlamıştır. Bu değişiklik ile birlikte suçlular “motive olmuş suçlu” durumundan çıkarak “suç işlemesi muhtemel” durumuna getirilmiştir ve insanları potansiyel suçlu olarak görmekten yavaş yavaş vazgeçilmeye başlanmıştır.<sup>78</sup>

#### 3.1.4. Suç Fırsatları

Rutin aktiviteler teorisinin bütün suç türleri için bir açıklama getirmeye zorlandığını yukarıda belirtmiştik. 1998 yılında Felson ve Clarke bir araya gelerek “Opportunity makes the thief...” (“Fırsat hırsız yapar...”) isimli ünlü makalelerinde suçun asıl sebebinin fırsatlar olduğunu ortaya atarak rutin aktiviteler teorisinin kapsama alanın biraz daha geliştirmekle kalmamışlar aynı zaman da onu rasyonel tercih teorisi ile birleştirerek suç olayına yeni bir bakış açısı getirmişlerdir.<sup>79</sup> Onlara göre fırsat-suç ilişkisinin aşağıda belirtilen 10 esas prensibi vardır:<sup>80</sup>

1. Bütün suçların nedeni olarak fırsatlar yadsınamaz bir rol oynar.
2. Her suç tipine göre suç fırsatları değişiklik gösterir. (Suçlu açısından bakıldığında nasıl ki araçtan hırsızlıkta aracın camının açık bırakılması bir fırsatken,

---

<sup>76</sup> Marcus Felson, “Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes” *The Reasoning Criminal: Rational Choice Perspectives On Offending* (1986) s.119-128.

<sup>77</sup> Marcus Felson, “Those Who Discourage Crime” *Crime And Place* c.4 (1995) s.53-66.

<sup>78</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.126

<sup>79</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.128

<sup>80</sup> Marcus FELSON, R.V.Clarke. “Opportunity Makes the Thief.” *Police Research Series Paper 98, Policing and Reducing Crime Unit. Research, Development and Statistics Directorate. London: Home Office* (1998).

“123456” gibi kolay tahmin edilebilecek şifreleri kullanmak da bilişim suçlarında bir fırsattır.)

3. Fırsatlar belli mekân ve zamanlarda yoğunlaşmıştır. (İnternet üzerinden yayılan virüslerin büyük bir çoğunluğu müstehcen içerikli siteler yoluyla başka bilgisayarlara geçmektedir.)

4. Fırsatlar insanların rutin olarak her gün yaptıkları faaliyetlerin sonucu olarak ortaya çıkarlar.

5. Önce işlenmiş bir suç sonra işlenecek bir suç için fırsat doğurur.

6. Bazı durumlar veya ürünler karşı konulamaz suç fırsatları açığa çıkarır.

7. Teknoloji ve sosyal alanda olan değişiklikler yeni suç fırsatları ortaya çıkarır.

8. Suçun önlenmesi suç fırsatlarının azaltılması ile mümkündür.

9. Suç fırsatlarının azaltılması genelde suçun yer değiştirmesine sebep olmaz.

10. Fırsatların yoğun olarak azaltılması suç oranlarında büyük bir düşüş sağlar.

Bu düşüncelerin ispatlanabilmesi için birtakım deneyler yapılması çok zordur. Çünkü bir fırsat yaratıp o fırsat karşısında insanların suçlu davranış sergileyip sergilemeyeceklerini takip etmek etik değildir. Ama buna rağmen geçmişte bu konu ile ilgili olarak pek çok deney yapılmıştır. Deneylerden birinde kopya çekme fırsatı yaratılan bir sınavda öğrencilerin büyük çoğunluğunun kopya çektiği tespit edilmiştir. Bunun gibi daha pekçok deney yapılmıştır.<sup>81</sup> Yapılan bu deneylerde gözlemlenen durumlar sonucunda etkileyici bir suç fırsatı ortaya çıktığı zaman bireylerin genelde rasyonel bir tercih yaparak suç işledikleri tespit edilmiştir.<sup>82</sup>

### 3.1.5. Rutin Aktiviteler Teorisi Bağlamında Durumsal Suç Önleme

“Durumsal suç önleme” suçluların suç önlemek için aradığı fırsatların ortadan kaldırılarak suçların azaltılmasından başka bir şey değildir.<sup>83</sup> Bu yaklaşımda

---

<sup>81</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.129

<sup>82</sup> Marcus FELSON, R.V.Clarke. “Opportunity Makes the Thief.” *Police Research Series Paper 98, Policing and Reducing Crime Unit. Research, Development and Statistics Directorate. London: Home Office* (1998).

<sup>83</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theory* (Boston, Northeastern University Press, 1996), s.23-25.



suçluların peşinden koşup onları yakalamaya çalışmak gibi bir durum söz konusu olmamaktadır. Sadece onların suç fırsatları olarak değerlendirdiği şeyleri önceden analiz edip bu durumların üzerine gidilerek, suçluların kendiliğinden suç işleme iradesinden vazgeçmesi beklenir. Mesela internet bankacılığına giriş yaparken kullandığımız şifreler bankalar tarafında belirlenen bir takım şartları (örneğin; “şifreniz en az bir büyük harf ve en az bir simge içermelidir”) taşımak zorundadır. Görünürde bir güvenlik tedbiri olarak algılansa da bu uygulama aslında, durumsal suç önleme yaklaşımına çok güzel bir örnek teşkil etmektedir. Şifrelerin güvenlik seviyeleri arttıkça suçlular tarafından kırılabilme ihtimali azalmaktadır. Belki bir suçlu onlarca kere deneyip kıramadığı şifreyle uğraşmayı bırakacak ve “nasıl olsa o bankanın sistemine ne kadar uğraşsam da giremiyorum” şeklinde bir düşünceye kapılacak, dolayısıyla suç işlemekten vazgeçebilecektir. Bunun sonucunda da bilgisayarla bağlantılı dolandırıcılık suçlarının oranında bir azalma görülecektir.

Yukarıda verilen örnekten de anlaşılacağı üzere durumsal suç önleme yaklaşımlarında motive olmuş suçlu ile değil, suçu meydana getiren durumlarla ilgilenilmektedir. Bu durum durumsal suç önleme yaklaşımının en temel ve belirgin özelliğidir.<sup>84</sup>

Durumsal suç önleme, sıklıkla, işlenen suçlarla ilgili olan suç fırsatlarının azaltılması şeklinde ortaya konulmaktadır. Bunun için yapılacak çevre düzenlemeleri, mevzuat düzenlemeleri, bilgilendirme faaliyetleri vb. her türlü yönetsel işlemler bu kapsamda değerlendirilebilir. Böyle bir suç önleme stratejisi farklı suç türleri üzerine derinlemesine analiz yapılarak geliştirilebilir.<sup>85</sup> Bu yaklaşımın temelinde yatan asıl düşünce suçun rasyonel bir tercih olmaktan çıkarılmasıdır.<sup>86</sup>

Suçun bu yöntemle engellenmesi üzerine yapılan en ünlü çalışma Oscar NEWMAN’ın “Savunulabilir Alan, Suçun Şehir Dizaynı Yoluyla Engellenmesi” (Defenceble Spaca, Crime Prevention Through Urban Design) isimli kitabıdır.<sup>87</sup>

---

<sup>84</sup> David D.HERBERT, Stephen W.Hyde “Enviromental Criminology: Testing Some Area Hypotesis.” *Transactions of the Institute of British Geographers* c.10, s.3 (1985), s.259-274.

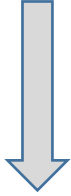
<sup>85</sup> Clarke, Ronald V. “Situational Crime Prevention: Its Theoretical Basis and Practical Scope.” *Crime and Justice*, c.4, (1983) s. 225–256.

<sup>86</sup> Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.130

<sup>87</sup> age, s. 130.

Newman bu kitabında temel olarak kişilerin birbirlerini tanımalarına daha fazla imkân verecek şekilde düzenlenen şehirlerde suçun kendiliğinden azalacağını belirtmektedir.

Durumsal suç önleme yöntemleri Şekil 3 te gösterildiği gibi hedeflerle ve mekânlarla ilgili olmak üzere iki ana başlık altında toplanmaktadır. Her iki tedbir şekli de, doğrudan önleme metotlarından dolayı biçimde önleme metotlarına doğru giden bir mantığı barındırmaktadır.

<b>DOĞRUDAN ÖNLEME</b>	<b>HEDEFLERLE İLGİLİ TEDBİRLER.</b>	<b>MEKÂNLARLA İLGİLİ TEDBİRLER.</b>
	<b>1.</b> Hedefler yok edilmeli ya da hedef olmaktan çıkartılmalı.	<b>6.</b> Erişim ve giriş çıkışlar yasaklanmalı
	<b>2.</b> Hedefler değiştirilmeli.	<b>7.</b> Giriş çıkışlar azaltılmalı ve giriş çıkış kuralları değiştirilmeli
	<b>3.</b> Hedefler güçlendirilmeli.	<b>8.</b> Çalışanlar gözetim altında tutulmalı
	<b>4.</b> Hedefler işaretlenmeli.	<b>9.</b> Doğal gözetim uygulanmalı
<b>DOLAYLI ÖNLEME</b>	<b>5.</b> Alternatifler oluşturulmalı.	<b>10.</b> Giriş çıkışlar değiştirilmeli

**Şekil 3: Durumsal Suç Önleme Yöntemleri.**

---

Osman DOLU, *Suç Teorileri* (Ankara: Global Yayıncılık, 2015), s.132

Hedeflerle ilgili tedbirleri birer örnekle açıklamak gerekirse her bir tedbir için şu örnekler verilebilir. Birinci tedbir olarak, genel ağ üzerinden yapılan alışverişlerde gerçek kredi kartı yerine sanal kart kullanılarak gerçek kart bilgilerinin çalınmasının önüne geçilebilir. İkinci tedbir kapsamında, mağazaların kullandığı teşhir ürünlerinin maket olanlarla değiştirilmesi söylenebilir. Üçüncü tedbir için, teşhir ürünlerinin tezgâha sabitlenmesi düşünülebilir. Dördüncü tedbir çerçevesinde, satılan ürünlerin üzerine manyetik işaretleyiciler koyarak kasadan geçmeden mağazadan çıkarılmaya çalışılan ürünlerin tespit edilmesi sağlanabilir. Beşinci tedbir olarak ise suçluların ilgisini çekecek sportif veya sosyal faaliyet girişimlerinde bulunularak dikkatin dağıtılması ve dolayısıyla ilgilerinin yönünün değiştirilmesi sağlanabilir.<sup>88</sup>

---

<sup>88</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theory* (Boston, Northeastern University Press, 1996), s.23-25.

Mekânlarla ilgili alınabilecek tedbirlerin açıklamak için ise şu örneklerden yararlanılabilir. Altıncı tedbir kapsamında kapı ve pencerelerin girişi engelleyecek şekilde demir parmaklarla kapatılması. Yedinci tedbir olarak, kartlı giriş çıkış sistemleri getirilip suç mekânı olabilecek yere olan girişlerin seyreltilmesi. Sekizinci tedbir çerçevesinde suçun oluşabileceği mekânlarda bulunan görevlilerin ve söz konusu mekânın kamera sistemleri ile gözlemlenmesi. Dokuzuncu tedbir demek için, suçun oluşabileceği mekânların herkesin birbirini kontrol edecek şekilde düzenlenmesi ve son tedbir kapsamında ise suç oluşabilecek mekânlara giriş çıkış yapılan yerlerin belirli bir plan dâhilinde değiştirilmesi sağlanabilir.<sup>89</sup>

### 3.1.6. Teori Kapsamında Yapılan Bilimsel Çalışmalar

Stahura ve Sloan, kayıtlı suç istatistiklerinden faydalanarak, 1972 ile 1980 yılları arasında 8 yıl boyunca 676 Amerikan varoşundaki suçları, 1998 yılında incelemiştir. Çalışmalarının sonucunda bu teorinin mala karşı işlenen suçlar ve şiddet suçlarında geçerli olduğunu tespit etmişlerdir. Ayrıca suçun 3 unsurunun bir arada bulunmasının mala karşı işlenen suçları tetikleyici bir sebep olduğunu özellikle vurgulamışlardır.<sup>90</sup>

Miether, Stafford ve Long 1987 yılında ABD'nin 13 şehrinde ikamet eden 107678 kişilik bir örnekleme şahısların rutin aktivitelerinin ve yaşam tarzlarının mala karşı işlenen suçlardaki değişiklikleri doğru bir şekilde değerlendirdiğini tespit etmişlerdir.<sup>91</sup>

Mustaine ve Tewbusky 1998 yılında üniversite öğrencileri arasında yaptığı çalışmalarında, teorinin basit suçları ve daha karmaşık olan özellikle hırsızlık gibi mala karşı suçları açıklamada geçerli olduğunu, ancak suçun unsurları olan koruyucuların yokluğunun basite indirgenmiş şekilde değil de bireyin zamanını nasıl geçirdiği,

---

<sup>89</sup> Cordella PETER, Siegel LARRY, *Readings in Contemporary Criminological Theory* (Boston, Northeastern University Press, 1996), s.23-25.

<sup>90</sup> John M.STAURA, John J.SALOAN “Urban Stratification of Places, Routine Activities and Suburban Crime Rates” *Social Forces* c.4 (1988), s.1102-1118

<sup>91</sup> Terance D.Miethe, Mark C.Stafford, Long J.Scott. “Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories.” *American Sociological Review*” c.52, s. 2, (1987), s.184–194.

dışarıda bulunduğu zamanlarda nerelere gittiği gibi unsurların daha derin şekilde analiz edilerek incelenmesi gerektiğini tespit etmişlerdir.<sup>92</sup>

Schwartz, DeKeseredy, Tait ve Alvi 2001 yılında yaptıkları çalışmalarında koruyucunun etkisinin suçun oluşması üzerine olan etkilerini araştırmışlardır. Çalışmada Kanada’da ulusal düzeyde yapılan bir anket sonuçları değerlendirilmiş ve çalışma sonucunda alkol kullanan bir erkek arkadaşına sahip üniversiteli kız öğrencilerin tecavüze uğrama ihtimalinin arttığını tespit etmişlerdir.<sup>93</sup> Bu da koruyucunun etkili olmasını suç oranlarını azaltacağı manasına gelmektedir.

Cohn ve Rotton 2000 yılında mala karşı işlenen suçlardan gasp, evden hırsızlık ve adi hırsızlık üzerine yoğunlaşarak bu teoriyi test etmişlerdir. Çalışmalarında ABD’nin Minneapolis şehrinde polise gelen ihbarlar üzerinden veriler toplanmıştır. Araştırmanın sonucunda, suç olaylarının haftanın belli günlerinde ve belli zamanlarında meydana geldiğini, ayrıca sıcak havalarda belirtilen suçların daha fazla işlendiğini tespit etmişlerdir.<sup>94</sup>

Yine Cohn ve Rotton 2003 yılında yaptıkları başka bir çalışmada uzun tatiller sırasında şiddet suçlarının arttığını, mala karşı işlenen suçların azaldığını fakat bu ilişkinin kısa tatillerde geçerli olmadığını tespit etmişlerdir.<sup>95</sup>

Sherman, Gartin ve Buerger 1998 yılında yaptıkları çalışmada suçun mekânla olan ilişkisini test etmişlerdir. Çalışmada ABD’nin Minneapolis şehrinde bir yıl içinde 115000 farklı adresten gelen 323979 telefon görüşmesini incelemişler ve çalışmanın sonucunda gelen aramaların yüzde ellisinden fazlasının sadece şehrin %3’lük bir bölümünden geldiğini tespit etmişlerdir. Bunun dağılımına baktıklarında tecavüz olaylarının şehrin sadece %1,2’lik, oto hırsızlıklarının %2,7’lik, gasp olaylarının ise

---

<sup>92</sup> Elizabeth Ehrhardt Mustaine, Richard Tewksbury. "Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures." *Criminology* c.36 s.4 (1998) s.829-858.

<sup>93</sup> Martin D. Schwartz ve diğ. "Male peer support and a feminist routing activities theory: Understanding sexual assault on the college campus." *Justice Quarterly* c.18. s.3 (2001) s.623-649.

<sup>94</sup> Ellen G. Cohn, James Rotton. "Weather, seasonal trends and property crimes in Minneapolis, 1987–1988. A moderator-variable time-series analysis of routine activities." *Journal of Environmental Psychology* c.20 s.3 (2000) s.257-272.

<sup>95</sup> Ellen G. Cohn, James Rotton. "Even criminals take a holiday: Instrumental and expressive crimes on major and minor holidays." *Journal of Criminal Justice* c.31 s.4 (2003) s.351-360.

%2,2'lik bir bölümünde meydana geldiğini tespit etmişler ve suç ile mekân arasında çok büyük bir ilişki olduğunu belirtmişlerdir.<sup>96</sup>

Roncek ve Maier 1991 yılında yaptıkları çalışmalarında içkili mekânlar ile suç arasındaki bağlantıyı incelemişlerdir. Çalışmalarında ABD'nin Cleveland şehrinde bulunan bir içkili mekânın çevresindeki mekân açılmadan önceki ve açıldıktan sonraki suç oranları karşılaştırılmış ve içkili mekân açıldıktan sonra bölgedeki suç oranlarının arttığı tespit edilmiştir.<sup>97</sup>

Bennet 1991 yılında 52 ülkeyi kapsayan 25 yıllık bir veri seti ile yaptığı çalışmada bu teorinin geçerliliğini test etmiştir. Araştırmanın sonucunda söz konusu teorinin genel bir suç teorisi olmaktan ziyade suça özel bir yaklaşım olabileceği sonucuna varmıştır. Teorinin mala karşı işlenen suçlarda güçlü olduğunu fakat şahsa karşı işlenen suçlarda o kadar güçlü olmadığını tespit etmiş ve sonraki çalışmaların suç özelinde yapılması gerektiğini açıklamıştır.<sup>98</sup>

Ünal, Orçan ve Sezer 2014 yılında yaptıkları çalışmalarında mağdur bakış açısıyla mekân ile suç arasındaki ilişkiyi araştırmışlardır. Araştırma Ankara'dan 476, Muğla'dan 173 katılımcı ile yapılmıştır. Çalışma sonucunda Ankara ilinde parkların, Muğla ilinde ise mahalle içinde belli alanların katılımcılar tarafından tehlikeli olarak belirtildiği tespit edilmiştir.<sup>99</sup> Yani suç ile mekân ilişkisi mağdur (suçun hedefi de denebilir) gözünden bakıldığında önem arz etmektedir.

Duru, 2013 yılında yaptığı çalışmada Bursa ilinde 2003-2007 yılları arasında polise ulaşan suç sayılarından faydalanarak içkili yerlerin, kahvehanelerin ve lise seviyesindeki okulların suç sayısını arttırdığını tespit etmiştir.<sup>100</sup> Bu da rutin aktiviteler teorisinin doğrulandığı mânâsına gelmektedir.

---

<sup>96</sup> Lawrence W. Sherman, Patrick R. Gartin, and Michael E. Buerger. "Hot spots of predatory crime: Routine activities and the criminology of place." *Criminology* c.27 s.1 (1989) s.27-56.

<sup>97</sup> Dennis W. Roncek, Pamela A. Maier. "Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of "hot spots"." *Criminology* c.29 s.4 (1991) s.725-753.

<sup>98</sup> Richard R. Bennett, "Routine activities: A cross-national assessment of a criminological perspective." *Social Forces* c.70 s.1 (1991) s.147-163.

<sup>99</sup> Halime Ünal, Mustafa Orçan, Serdenger SEZER "Kentlerde Tehlikeli Alanlar: Ankara ve Muğla Örneği" *Geleceğin Şehri Sempozyumu Bildiriler, 24-25 Aralık 2014* (İstanbul: Yıldız Teknik Üniversitesi, 2014) s.325-340.

<sup>100</sup> Hacı Duru, "Liselerin, İçkili Yerlerin Ve Kahvehanelerin Sokak Üzerinde Oluşan Suça Etkisi Bursa Örneği", *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* c.3, s.2, (2013) s.1-105.

Madenüs 2016 yılında yaptığı çalışmasında 2010-2014 yılları arasında Türkiye genelinde kırsalda gerçekleşen hırsızlık olaylarını Jandarma Genel Komutanlığı verilerinden faydalanarak incelemiş, suç fırsatlarının kırsalda meydana gelen hırsızlık olaylarının büyük bir bölümünü açıkladığını fakat hırsızlık olaylarının oluşmasında etkili sosyolojik nedenlerin göz ardı edilmemesi gerektiğini tespit etmiştir.<sup>101</sup>

Bossler ve Holt bir lisede topladıkları 650 örneklem ile 2009 yılında rutin aktiviteler teorisinin siber suçları açıklama seviyesini ölçmek üzere yaptıkları çalışmalarında; rutin aktiviteler arttıkça suç mağduriyetin de arttığını, koruyucuların da suç mağduriyeti üzerine bir etkisi olmadığını tespit etmiştir.<sup>102</sup>

---

101 Murat MADENÜS, “Değişen Kırsal Yaşam Alışkanlıklarının Hırsızlık Suçuna Etkisi.”, *Güvenlik Bilimleri Dergisi* c.5 s.2, (2016) s.85

102 Adam M.Bossler, Thomas J. Holt. “On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory.” *International Journal of Cyber Criminology* . c.3 s.1 (2009) s.415

## ARAŞTIRMANIN KAPSAMI VE ÖNEMİ

### 4.1. Araştırmanın Amacı ve Önemi

#### 4.1.1. Araştırmanın Amacı

Araştırmanın amacı geçmişte daha çok hırsızlık gibi mala karşı olan suçlarda geçerliliğinin yüksek olduğu<sup>103</sup> fakat diğer suç türlerini açıklamakta zorluk çektiği anlaşılan rutin aktiviteler teorisinin siber suçları açıklama düzeyini tespit etmektir.

#### 4.1.2. Araştırmanın Önemi

Türk alan yazınında siber suçlar ve kriminoloji ekseninde yapılan çalışmalar genelde siber suç algısı üzerine durmuştur Bunun sonucu olarak, siber suç mağduriyetini rutin aktiviteler teorisi bakış açısından inceleyen araştırma sayısı yok denebilecek kadar az sayıda kalmıştır. Bu çalışma alan yazınındaki bu boşluğu az da olsa dolduracaktır.

### 4.2. Araştırmanın Yöntemi

#### 4.2.1. Araştırmanın Evren ve Örneklemi

##### 4.2.1.1. Araştırmanın Evreni

Bu araştırmanın evreni olarak ABD’de bulunan tüm sabit ve mobil telefon hattı sahipleri belirlenmiştir.

##### 4.2.1.2. Araştırmanın Örneklemi

Araştırmanın evreni içinden eyaletlerin nüfusları ile orantılı olarak rastgele seçilen 35930 telefon numarasına yapılan aramaya cevap veren 18 yaş üstü 1040 katılımcı araştırmanın örneklemi oluşturmaktadır.

#### 4.2.2. Araştırmanın Veri Toplama Teknikleri

Araştırma ABD’de bulunan sabit hat ve cep telefonu hattı sahiplerinin tamamını temsil edecek şekilde yine ABD’de bulunan “Pew Research Center” adlı kuruluş adına “Survey Sampling International” isimli kuruluş tarafında sağlanan örneklem ile

---

<sup>103</sup> John M.STAURA, John J.SALOAN “Urban Stratification of Places, Routine Activities and Suburban Crime Rates” *Social Forces* c.4 (1988), s.1102-1118

yapılmıştır. Anketin uygulaması ise Princeton Survey Research Associates International adlı kuruluş tarafından EK-1’de orijinali sunulan görüşme formuna göre yapılmıştır.

Anket kapsamında görüşmeler 30 Mart-3 Mayıs 2016 tarihleri arasında gerçekleştirilmiştir. Anket kapsamında potansiyel katılımcılara ulaşma şansını maksimuma çıkartmak için aramalar tekrarlı olarak yapılmış, bir potansiyel katılımcıya bir gün ulaşılamadıysa aynı gün değil farklı günlerde aramalar tekrarlanmıştır.

Sabit hatlar için yapılan aramalarda anketörler aradıkları telefon numarasında karşısına çıkan şahıstan, reşit olmak şartı ile o anki sosyal ortamda bulunan en genç, mobil hatlar için yapılan aramalarda ise en yaşlı kişi ile görüşmek talebinde bulunup bu şart sağlandıktan sonra görüşmeye başlamışlardır.

#### **4.2.3. Araştırmada Kullanılan Verilerin Analizi**

Yukarıda bahsedilen kuruluşlar tarafından uygulanan anket verileri SPSS programına aktarılmış, verilerin çözümlenmesinde SPSS 20.0 paket programı kullanılmıştır. Öncelikle katılımcıların belirli durumlara ait tanımlayıcı istatistikleri çıkarılmış, sonrasında değişkenlerin birbirleri ile olan ilişkilerini belirlemek üzere korelasyon analizi yapılmıştır.

#### **4.2.4. Araştırmanın Sınırlılıkları**

Bu çalışmanın kavramsal çerçevesinin incelendiği 2’nci bölümde siber suçlar mer’i mevzuata göre incelenmiş olup Türk Ceza Kanunu ve Avrupa Birliği Konseyi tarafından geliştirilen “Sanal Ortamda İşlenen Suçlar Sözleşmesi” kapsamında olan siber suçların araştırılması yapılmıştır.

Zaman kısıtı dolayısıyla saha çalışması yapılamayıp EK-2’ de sunulan gerekli izinler alınıp ABD’de yapılan bir anket üzerinden inceleme gerçekleştirilmiştir.

Anket formu üzerinde katılımcılar tarafından cevap verilmeyen soruların sayısı yüksek olup bu eksik, verilerin analizi esnasında SPSS programı ile doldurulmuştur.

Katılımcıların siber suç mağduriyetleri sınırlı sayıda suç ile ölçülmüştür. Oysa bu çalışma kapsamında incelenmeyen başka siber suçlar da vardır.

Bu çalışmada siber suçlar sadece kriminolojik boyutu ile işlenmiştir. Oysa siber suçların bir de siber güvenlik boyutu bulunmaktadır. Bu çalışmada siber güvenlik boyutuna değinilmemiş olması çalışmanın bir diğer kısıtlılığıdır.



## ARAŞTIRMANIN BULGULARI

Çalışmanın bu bölümünde örneklemin tanımlayıcı istatistik verileri, katılanlara yöneltilen soruların değerlendirmeleri ve belirlenen hipotezlerin testleri yapılacaktır.

### 5.1. Tanımlayıcı İstatistiklerin Analizi

#### 5.1.1. Katılımcıların Demografik Özellikleri

##### 5.1.1.1. Katılımcıların Cinsiyete Göre Dağılımı.

Katılımcıların cinsiyetleri tablo 1’ de gösterilmiştir. Buna göre katılımcıların %48,9’u erkek, %51,1’i erkeklerden oluşmaktadır.

**Tablo 1: Katılımcıların Cinsiyete Göre Dağılımı.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	Erkek	509	48,9	48,9	48,9
	Kadın	531	51,1	51,1	100,0
	Toplam	1040	100,0	100,0	

##### 5.1.1.2. Katılımcıların Yaşa Göre Dağılımı

En genç katılımcı 18, en yaşlı katılımcı 93 yaşında olup katılımcıların yaş ortalaması 51,49’ dur. Yaşlara göre dağılımlar Tablo 2’ de gösterilmiştir.

**Tablo 2: Katılımcıların Yaşa Göre Dağılımı.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	18-24	96	9,2	9,2	9,2
	25-34	146	14,0	14,0	23,3
	35-44	143	13,8	13,8	37,0
	45-54	170	16,3	16,3	53,4
	55-64	223	21,4	21,4	74,8
	65+	234	22,5	22,5	97,3
	Cevap vermeyen	28	2,7	2,7	100,0
	Toplam	1040	100,0	100,0	

### 5.1.1.3 Katılımcıların Eğitim Durumu

Veri setinde bu değişkenin ölçülebilmesi maksadıyla “What is the highest level of school you have completed or the highest degree you have received?” (Mezun olduğunuz en son okul veya en üst eğitim dereceniz nedir?) sorusu katılımcılara sorulmuş ve cevaplar Tablo 3’ te gösterilmiştir.

**Tablo 3: Katılımcıların Eğitim Durumuna Göre Dağılımı.**

	Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
İlköğretim mezunu	27	2,6	2,6	2,6
Lise terk	53	5,1	5,1	7,7
Lise mezunu	223	21,4	21,4	29,1
Kolej mezunu	159	15,3	15,3	44,4
2 yıllık yüksekokul	106	10,2	10,2	54,6
4 yıllık yüksekokul	238	22,9	22,9	77,5
Yüksek lisans öğrencisi	16	1,5	1,5	79
Yüksek lisans veya doktora mezunu	208	20	20	99
Bilmiyorum	1	0,1	0,1	99,1
Cevap vermek istemiyorum	9	0,9	0,9	100
Toplam	1040	100	100	

### 5.1.1.4. Katılımcıların Medeni Halleri

Bu değişkenin ölçülebilmesi maksadıyla katılımcılara “Are you currently married, living with a partner, divorced, separated, widowed, or have you never been married?” (Evli misiniz? Partneriniz ile birlikte mi yaşıyorsunuz? Dul musunuz? Boşandınız mı?, Ayrı mı yaşıyorsunuz?, ya da hiç evlenmediniz mi?) sorusu yöneltilmiş ve cevaplar tablo 4’ te gösterilmiştir.

**Tablo 4: Katılımcıların Medeni Hali.**

	Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Evli	524	50,4	50,4	50,4
Birlikte yaşayan	59	5,7	5,7	56,1
Boşanmış	131	12,6	12,6	68,7
Ayrı	23	2,2	2,2	70,9
Dul	89	8,6	8,6	79,4
Hiç evlenmemiş	196	18,8	18,8	98,3
Bilmiyorum	4	0,4	0,4	98,7
Cevap vermek istemiyorum	14	1,3	1,3	100
Toplam	1040	100	100	

#### 5.1.1.5. Katılımcıların Çocuk Sahibi Olma Durumları

Bu değişkenin ölçülebilmesi maksadıyla veri setinde kullanılan soru: “Are you the parent or guardian of any children under age 18 now living in your household?” (Çocuğunuz var mı veya bir çocuğun bakımından sorumlu musunuz?) Sorusu yöneltilmiş ve tablo 5’ ten de anlaşılacağı üzere katılımcıların %26,7’sinin çocuk sahibi olduğu, %71,9’unun ise çocuk sahibi olmadığı tespit edilmiştir.

**Tablo 5: Katılımcıların Çocuk Sahibi Olma Durumları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	Evet	278	26,7	26,7	26,7
	Hayır	748	71,9	71,9	98,7
	Cevap vermek istemiyorum	14	1,3	1,3	100,0
	Total	1040	100,0	100,0	

#### 5.1.1.6. Katılımcıların Çalışma Durumları

Katılımcıların çalışma durumunun tespit edilebilmesi maksadıyla onlara “Are you now employed full-time, part-time, or are you not employed for pay?” (Tam zamanlı mı, yarı zamanlı mı çalışıyorsunuz ya da çalışmıyor musunuz?) sorusu yöneltilmiş ve verilen cevapların sonuçları tablo 6’ da gösterilmiştir.

**Tablo 6: Katılımcıların Çalışma Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	Tam zamanlı çalışan	473	45,5	45,5	45,5
	Yarı zamanlı çalışan	159	15,3	15,3	60,8
	Çalışmayan (işsiz)	391	37,6	37,6	98,4
	Bilmeyen	4	0,4	0,4	98,8
	Cevap vermeyen	13	1,3	1,3	100,0
	Toplam	1040	100,0	100,0	

#### 5.1.1.7. Katılımcıların Gelir Durumları

Bu değişken veri setinde “Last year - that is in 2015 - what was your total family income from all sources, before taxes?” (Geçen yıl tüm vergiler çıktıktan sonra yıllık geliriniz ne kadardı?) sorusu ile ölçülmüş ve sonuçlar tablo 7’ de gösterilmiştir.

**Tablo 7: Katılımcıların Gelir Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	10,000 Dolardan az	83	8,0	8,0	8,0
	10000 ile 20000 Dolar arasında	94	9,0	9,0	17,0
	20000 ile 30000 Dolar arasında	104	10,0	10,0	27,0
	30000 ile 40000 Dolar arasında	83	8,0	8,0	35,0
	40000 ile 50000 Dolar arasında	71	6,8	6,8	41,8
	50000 ile 75000 Dolar arasında	122	11,7	11,7	53,6
	75000 ile 100000 Dolar arasında	125	12,0	12,0	65,6
	100000 ile 150000 Dolar arasında	133	12,8	12,8	78,4
	150000 Dolardan fazla	108	10,4	10,4	88,8
	Bilmeyen	35	3,4	3,4	92,1
	Cevap vermeyen	82	7,9	7,9	100,0
	Toplam	1040	100,0	100,0	

#### 5.1.1.8. Katılımcıların Hane Halkı Mevcudu

Bu değişkenin ölçülebilmesi maksadıyla katılımcılara “How many people, including yourself, live in your household?” (Aynı evde kaç kişi yaşıyorsunuz?) sorusu yöneltilmiştir. Verilen cevaplar tablo 8’ de gösterilmiştir.

**Tablo 8: Katılımcıların Hane Halkı Mevcudu.**

	Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
1	221	21,3	21,3	21,3
2	352	33,8	33,8	55,1
3	187	18,0	18,0	73,1
4	127	12,2	12,2	85,3
5	79	7,6	7,6	92,9
6	32	3,1	3,1	96,0
7	8	,8	,8	96,7
8’den fazla	12	1,2	1,2	97,9
Cevap vermeyen	22	2,1	2,1	100,0
Toplam	1040	100,0	100,0	

#### 5.1.1.9. Katılımcıların Yerleşim Yeri

Katılımcılara yerleşim yerleri sorulmuş ve cevaplar tablo 9’ da gösterilmiştir. Buna göre katılımcıların genelinin banliyölerde yaşadığı görülmektedir.

**Tablo 9: Katılımcıların Yerleşim Yeri.**

	Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Kırsal	202	19,4	19,4	19,4
Banliyö	513	49,3	49,3	68,8
Kentsel	325	31,3	31,3	100,0
Toplam	1040	100,0	100,0	

#### 5.1.2. Katılımcıların İnternet Kullanma Alışkanlıklarının İncelenmesi

##### 5.1.2.1. Katılımcıların İnternet Kullanma Durumları

Katılımcıların genellikle İnternet veya e-posta kullanıp kullanmadığının tespiti maksadıyla veri setinde “Do you use the internet or email, at least occasionally?” (Genelde internet veya e-posta kullanır mısınız? Sorusu kullanılmış ve sonuçlar tablo 10’ da gösterilmiştir. Buna göre katılımcıların %86,3’ü internet kullanıcısı olduğunu beyan etmiştir.

**Tablo 10: Katılımcıların İnternet Kullanma Durumları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
	Evet	897	86,3	86,3	86,3
	Hayır	141	13,6	13,6	99,8
	Cevap vermeyen	2	,2	,2	100,0
	Toplam	1040	100,0	100,0	

**5.1.2.2. Katılımcıların İnternete Erişim Sıklıkları**

Veri setinde bu değişkenin değerlendirilebilmesi için katılımcılara “About how often do you use the internet?” (İnterneti genellikle hangi sıklıkla kullanırsınız?) sorusu yöneltilmiş ve katılımcıların “neredeyse her zaman, gün içinde pekçok kez, günde bir kere, haftada pekçok kez, bunlardan daha az” seçeneklerinden birisini seçmeleri istenmiştir. Aşağıda tabloda gösterildiği gibi katılımcıların 221 tanesi neredeyse her zaman, 467 tanesi gün içinde pek çok kez, 120 tanesi günde bir kere, 63 tanesi haftada pekçok kez, 50 tanesi ise belirtilen değerlerden daha az internete eriştiğini belirtmiş, 114 katılımcının cevabı geçersiz sayılmıştır. Cevaplar tablo 11’ de gösterilmiştir.

**Tablo 11: Katılımcıların İnternete Erişim Sıklığı.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Neredeyse her zaman	221	21,3	23,9	23,9
	Gün içinde pek çok kez	467	44,9	50,4	74,3
	Günde bir kere	120	11,5	13,0	87,3
	Haftada pek çok kez	63	6,1	6,8	94,1
	Bunlardan daha az	50	4,8	5,4	99,5
	Bilmiyorum	1	0,1	0,1	99,6
	Cevap vermek istemiyorum	4	0,4	0,4	100,0
	Toplam	926	89,0	100,0	
Geçersiz Cevaplar		114	11,0		
Toplam		1040	100,0		

### 5.1.2.3. Katılımcıların Sosyal Medya Kullanım Durumları

Veri setinde bu değişkenin ölçülebilmesi maksadıyla kullanılan soru “Do you ever use a social media site or app like Facebook, Twitter or LinkedIn?” (Hiç Facebook, Twitter ya da linkedin gibi sosyal medya uygulamalarını kullandınız mı?) sorusudur. Tablo 12’ de gösterildiği üzere katılımcıların çoğunluğu bu tür sosyal medya uygulamalarını kullandığını belirtmişlerdir.

**Tablo 12: Katılımcıların Sosyal Medya Kullanım Oranları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli cevaplar	Kullanan	665	63,9	71,8	71,8
	Kullanmayan	259	24,9	28,0	99,8
	Cevap vermeyen	2	0,2	0,2	100,0
	Toplam	926	89,0	100,0	
Geçersiz cevaplar		114	11,0		
Toplam		1040	100,0		

### 5.1.2.4. Katılımcıların İnternet Üzerinden Finansal İşlem Yapma Eğilimleri

Katılımcıların internet üzerinden finansal işlem yapma eğilimlerini ölçmek için veri setinde 4 farklı soru kullanmıştır. Bu sorular Do you have any online accounts with your bank or financial services provider? With your healthcare provider, with a household utility provider? Any online accounts that involves bill payment? (İnternet bankacılığı hesabınız var mı? Sağlık servisi sağlayıcınızın çevrimiçi hesabını kullanıyor musunuz? Ev hizmetleri sağlayıcınıza ait internet hesabınız var mı? Veya bunların dışında finansal faaliyetler içeren başka bir hesabınız var mı?) sorularıdır. Katılımcıların sorulara verdiği cevapların içerikleri tablo 13’ te gösterilmiştir.

**Tablo 13: Katılımcıların İnternet Üzerinden Finansal İşlem Yapma Eğilimleri.**

			Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
İnternet Bankacılığı Hesabı	Geçerli Cevaplar	Kullanan	665	63,9	71,8	71,8
		Kullanmayan	229	24,9	28	99,8
		Cevap Vermeyen	2	0,2	0,2	100
		Toplam	926	89	100	
	Geçersiz Cevaplar		114	11		
	Toplam		1040	100		
Sağlık Servisi Sağlayıcısı Hesabı	Geçerli Cevaplar	Kullanan	373	35,9	40,3	40,3
		Kullanmayan	531	54,1	57,3	97,6
		Cevap Vermeyen	22	2	2,7	100
		Toplam	926	89	100	
	Geçersiz Cevaplar		114	11		
	Toplam		1040	100		
Ev Hizmetleri Servisi Sağlayıcısı Hesabı	Geçerli Cevaplar	Kullanan	406	39	43,8	43,8
		Kullanmayan	501	48,2	54,1	97,9
		Cevap Vermeyen	19	2,1	2,1	100
		Toplam	926	89	100	
	Geçersiz Cevaplar		114	11		
	Toplam		1040	100		
Başka Türlü Finansal İşlemler	Geçerli Cevaplar	Kullanan	434	41,7	46,9	46,9
		Kullanmayan	481	46,3	51,9	98,8
		Cevap Vermeyen	11	1,2	1,2	100
		Toplam	926	89	100	
	Geçersiz Cevaplar		114	11		
	Toplam		1040	100		

#### 5.1.2.5. Katılımcıların Kişisel Verilerinin Korunması Konusundaki Endişe Seviyeleri

Veri setinde bu değişkenin değerlendirilebilmesi için katılımcılara “Have you ever chosen to not use or not create an account with an online service because you were worried about how your personal information would be handled?” (Şahsi verilerinizin güvenliğinden şüphelendiğiniz için çevrimiçi bir hesap oluşturmayı reddettiniz mi?) sorusu yöneltilmiş ve katılımcıların “evet, hayır, bilmiyorum, cevap vermek istemiyorum” seçeneklerinden birisini seçmeleri istenmiştir. Aşağıda tablo 14’te gösterildiği gibi, katılımcıların 657 tanesi şahsi verilerinin güvenliğinden endişe duyduğunu, 261 tanesinin böyle bir endişesi bulunmadığını, 5 tanesi bilmediğini



belirtmiş 3 kişi cevap vermeyi reddetmiştir. 114 katılımcının cevabı geçersiz sayılmıştır.

**Tablo 14: Katılımcıların Kişisel Verilerinin Korunması Konusundaki Endişe Seviyeleri.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Evet	657	63,2	71,0	71,0
	Hayır	261	25,1	28,2	99,1
	Bilmiyorum	5	0,5	0,5	99,7
	Cevap Vermeyi Reddeden	3	0,3	0,3	100,0
	Toplam	926	89,0	100,0	
Geçersiz Cevaplar		114	11,0		
Toplam		1040	100,0		

#### **5.1.2.6. Katılımcıların Halka Açık İnternet Erişiminde Yaptığı İşlemlerin İncelenmesi**

Katılımcıların kamusal alanlarda herkesçe ulaşılabilen kablosuz hatları kullanıp kullanmadığının tespit edilebilmesi maksadıyla yapılan incelemeye ileride değinilecektir. Burada katılımcıların genel internet kullanım alışkanlıklarının incelenmesi bağlamında kamusal alandan internete eriştiklerinde yaptıkları işlemler tespit edilmeye çalışılmış ve sonuçlar tablo 15’te gösterilmiştir. Buna göre katılımcıların kamusal alanda internete eriştiklerinde yapmaktan çekindiği işlemlerin başında %18,1 oranı ile internet bankacılığı işlemleri gelmektedir. Onu, yine aynı kapsamda değerlendirilebilecek, çevrimiçi alışveriş yapma işlemleri %19,9 ile takip etmektedir. Çekinmedikleri işlemler ise %76,7 ile sosyal medya kullanımı, %72,7 ile e-posta kullanımı olarak görülmektedir. Burada soruların kamusal alanda internete erişenlere evet yanıtı verenlere sorulduğu dikkate alınmalıdır. Tabloda “geçersiz cevaplar” olarak belirtilenler zaten en başta kamusal alanda internete girmediklerini beyan ederek bu soruların değerlendirilmesine katılmamışlardır.

**Tablo 15: Katılımcıların Halka Açık İnternet Erişiminde Yaptığı İşlemler.**

			Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Çevrimiçi Alışveriş	Geçerli cevaplar	Yapan	100	9,6	19,9	19,9
		Yapmayan	396	38,1	78,9	98,8
		Cevap vermeyen	6	0,6	1,2	100
		Toplam	502	48,3	100,0	
	Geçersiz cevaplar		538	51,7		
	Toplam		1040	100		
İnternet Bankacılığı İşlemleri	Geçerli cevaplar	Yapan	91	8,8	18,1	18,1
		Yapmayan	407	39,1	81,1	99,2
		Cevap vermeyen	4	0,4	0,8	100
		Toplam	502	48,3	100,0	
	Geçersiz cevaplar		538	51,7		
	Toplam		1040	100		
Sosyal Medya Kullanımı	Geçerli cevaplar	Kullanan	316	30,4	76,7	76,7
		Kullanmayan	92	8,8	22,3	99,0
		Cevap vermeyen	4	0,5	1	100
		Toplam	412	39,6	100,0	
	Geçersiz cevaplar		628	60,4		
	Toplam		1040	100,0		
E-posta Kullanımı	Geçerli cevaplar	Kullanan	365	35,1	72,7	72,7
		Kullanmayan	136	13,1	27,1	99,8
		Cevap vermeyen	1	0,1	0,2	100
		Toplam	502	48,3	100,0	
	Geçersiz cevaplar		538	51,7		
	Toplam		1040	100		

### 5.1.3. Katılımcıların Siber Suç Mağduru Olma Durumlarının İncelenmesi

Katılımcıların siber suç mağduriyetleri “Have you ever received a notice that your social security number had been compromised?” (Hiç sosyal güvenlik numaranızın ele geçirildiğine dair bir bildirim aldınız mı? ), “Have you received a notice that other sensitive personal information, such as your account number, had been compromised?” (Hesap numaranız gibi diğer hassas kişisel bilgilerinizin ele geçirildiğine dair bir bildirim aldınız mı?), Have you noticed fraudulent charges on your debit or credit card, (Banka veya kredi kartınızda şüpheli işlem fark ettiniz mi?), “Had someone take over your e-mail account without your permission,” (Hiç e-posta hesabınız çalındı mı?), “Had someone take over your social media account without

your permission,” (Hiç sosyal medya hesabınız çalındı mı?), “Had someone attempt to open a line of credit or apply for a loan using your name?” (Birisi haberiniz olmadan sizin adınıza kredi kartı ya da kredi başvurusu yaptı mı?) soruları ile ölçülmeye çalışılmıştır. Katılımcıların yaşadığı mağduriyet durumları tablo 16’ da gösterilmiştir. Tablo incelendiğinde en çok mağduru olunan siber suç türünün %45,7 ile kredi veya banka kartında şüpheli işlemler fark edilmesi, en az mağduru olunan siber suç türünün ise %14,7 ile mağdurun bilgilerinin çalınarak adına kart açılması veya farklı şekilde borçlandırılması olarak tespit edilmiştir. Burada dikkat edilmesi gereken bir diğer nokta da siber suçluların maddi getirisi olan suçlara daha fazla ağırlık vermesidir. E-posta veya sosyal medya hesaplarının çalınması gibi suçlar tabloda da görüldüğü üzere daha seyrek görülmektedir. Bu da rutin aktiviteler teorisi bağlamında uygun hedefte bulunması gereken unsurlardan erişilebilirlik ve arzu edilebilirliği açıklar bir durum olarak karşımıza çıkmaktadır.

**Tablo 16: Katılımcıların Siber Suç Mağduriyeti Durumları.**

			Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Sosyal Güvenlik Numarasının Ele Geçirilmesi	Geçerli cevaplar	Geçirilen	167	16,1	16,1	16,1
		Geçirilmeyen	867	83,4	83,4	99,4
		Bilmeyen	6	0,6	0,6	100,0
		Toplam	1040	100,0	100,0	
	Geçersiz cevaplar		-	-		
	Toplam		1040	100		
Hesap Numarasının Ele Geçirilmesi	Geçerli cevaplar	Geçirilen	402	38,7	38,7	38,7
		Geçirilmeyen	628	60,3	60,3	99,0
		Bilmeyen	10	1	1	100
		Toplam	1040	100,0	100,0	
	Geçersiz cevaplar		-	-		
	Toplam		1040	100		
Kartta Şüpheli İşlem Fark Edilmesi	Geçerli cevaplar	Fark eden	475	45,7	45,7	45,7
		Fark etmeyen	561	53,9	53,9	99,6
		Cevap vermeyen	4	0,4	0,4	100
		Toplam	1040	100,0	100,0	
	Geçersiz cevaplar		-	-		
	Toplam		1040	100,0		

Tablo 16 – devam						
E-posta Hesabının Çalınması	Geçerli cevaplar	Çalınan	175	16,8	18,9	18,9
		Çalınmayan	741	71,3	80,0	98,9
		Cevap vermeyen	10	0,9	1,2	100
		Toplam	926	89,0	100,0	
	Geçersiz cevaplar		114	11		
	Toplam		1040	100		
Sosyal Medya Hesabının Çalınması	Geçerli cevaplar	Çalınan	123	11,8	18,5	18,5
		Çalınmayan	539	51,8	81,1	99,6
		Cevap vermeyen	3	0,3	0,4	100
		Toplam	665	63,9	100,0	
	Geçersiz cevaplar		375	36,1		
	Toplam		1040	100,0		
Bilgileri Çalınarak Adına Kart veya Kredi Açılması	Geçerli cevaplar	Açılan	153	14,7	14,7	14,7
		Açılmayan	871	83,8	83,8	98,5
		Cevap vermeyen	16	1,5	1,5	100
		Toplam	1040	100,0	100,0	
	Geçersiz cevaplar		-	-		
	Toplam		1040	100,0	100,0	

#### 5.1.4. Katılımcıların Siber Suçun Hedefi Olarak Yaptığı Rutin Aktivitelerin İncelenmesi

##### 5.1.4.1. Katılımcıların Şifre Yönetim Davranışları

İnternet üzerinde güvenliğimizi belki de en çok sağlayan unsurun şifre olduğu düşünüldüğünde, onların suçluların hedefinde olduğunu anlamak pek de zor olmayacaktır. İnternet kullanıcılarına düşen de şifrelerini motive olmuş suçlulara karşı korumaktır. Kullanıcıların günümüzde onlarca web sitesine abone oldukları göz önüne alındığında, bir zaman sonra bütün şifrelerin akılda tutulmasının neredeyse imkânsız hale geleceği aşikârdır. Bu durumda birtakım şifre yönetim davranışları gündeme gelmektedir. Veri setinde, söz konusu davranışlardan en genel 5 tanesi için anket uygulaması yapılmış, diğer davranışlar için ise katılımcılara “bunların dışında” biçiminde ayrı bir soru yöneltilmiştir.

Katılımcılara bu davranışlar arasında “ezberleme” için “do you ever keep track of your passwords by memorizing them in your head? (Şifrelerinizi ezberleyerek mi takip edersiniz?) sorusu, “bir kâğıtta yazılı olarak saklamak” için “do

you ever keep track of your passwords by writing them down on a piece of paper” (Şifrelerinizi bir kâğıda yazarak mı takip edersiniz?) sorusu, “Şifre yönetim programı kullanmak” için “do you ever keep track of your passwords by using a password management program such as Dashlane, Lastpass, or Apple Keychain” (Şifrelerinizi Dashlane, Lastpass ya da Apple Keychain gibi bir şifre yönetim programı kullanarak mı takip edersiniz?) sorusu, “bilgisayarda bir doküman olarak kaydetmek” için “do you ever keep track of your passwords by saving them in a note or document on your computer or mobile device?” (Şifrelerinizi mobil cihazınızda ya da bilgisayarınızda bir dokümanda mı takip edersiniz?) sorusu, “İnternet Browser üzerinden takip etmek” için “do you ever keep track of your passwords by saving them in your internet browser?” (Şifrelerinizi internet browser üzerinden mi takip edersiniz?) sorusu ve “diğer yöntemler” için ise “do you ever keep track of your passwords by some other way that I haven't already mentioned” (Şifrelerinizi başka bir şekilde mi takip ederseniz?) sorusu yöneltilmiş ve alınan sonuçlar tablo 17’de gösterilmiştir.

**Tablo 17: Katılımcıların Şifre Yönetim Alışkanlıkları.**

			Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Şifreleri Ezberlemek	Geçerli cevaplar	Ezberleyen	776	74,6	83,8	83,8
		Ezberlemeyen	148	14,2	16,0	99,8
		Bilmeyen	2	0,2	0,2	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11,0		
	Toplam		1040	100,0		
Bir Kâğıtta Saklamak	Geçerli cevaplar	Saklayan	481	46,3	51,9	51,9
		Saklamayan	442	42,5	47,8	99,7
		Bilmeyen	3	0,2	0,3	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11,0		
	Toplam		1040	100,0		
Şifre Yönetim Programı Kullanmak	Geçerli cevaplar	Kullanan	112	10,8	12,1	12,1
		Kullanmayan	806	77,5	87,0	99,1
		Cevap vermeyen	8	0,7	0,9	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11,0		
	Toplam		1040	100,0		

Tablo 17 - devam						
Bilgisayarda Bir Doküman Olarak Kaydetmek	Geçerli cevaplar	Kaydeden	215	20,7	23,2	23,2
		Kaydetmeyen	707	68,0	76,2	99,6
		Cevap vermeyen	4	0,3	0,4	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11,0		
	Toplam		1040	100,0		
İnternet Browserda Saklamak	Geçerli cevaplar	Saklayan	163	15,7	17,6	17,6
		Saklamayan	758	72,9	81,9	99,5
		Cevap vermeyen	5	0,5	0,5	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11,0		
	Toplam		1040	100,0		
Bunların Dışında Bir Yöntem Kullanmak	Geçerli cevaplar	Kullanan	30	2,9	3,2	3,2
		Kullanmayan	876	84,2	94,6	97,8
		Cevap vermeyen	20	2	2,2	100
		Toplam	926	89	100	
	Geçersiz cevaplar		114	11		
	Toplam		1040	100		

Tablo 17’ deki veriler incelendiğinde şifrelerin yönetilmesinde en sık kullanılan iki yöntemin şifreleri ezberlemek ve şifreleri bir kâğıda not etmek olduğu; en az kullanılan yöntemin ise şifre yönetim programı kullanmak olduğu görülmektedir.

#### 5.1.4.2. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumları

Benzer veya aynı şifrelerin kullanılması internet kullanıcısının rutin bir faaliyeti olarak kabul edilebilir ve bu davranış söz konusu kullanıcıyı suçun hedefi haline getirecektir. Rutin aktiviteler teorisi bağlamında motive olmuş suçlu sanal ortamda gezerken müsait ve erişilebilir bir hedef olan bu tipteki kullanıcıları hedef olarak belirleyecektir. İnternet kullanıcısının benzer veya aynı şifreleri kullandığı bir sitedeki hesabının ele geçirilmesi sonucunda diğer bütün sitelerdeki hesapları da risk altında olacaktır.

Kullanıcıların bu yöndeki eğilimleri veri setinde, “Thinking about all of the passwords you use to access your various online accounts, would you say that Most of your passwords are the same or very similar to each other or Most of your passwords are very different from each other?” (Kullandığınız tüm şifreler düşünüldüğünde, çoğu

birbirinin benzeri mi yoksa tamamen farklı mı?) sorusu ile ölçülmeye çalışılmış ve sonuçlar tablo 18’ de gösterilmiştir.

**Tablo 18: Katılımcıların Kullandığı Şifrelerin Benzerlik Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Şifrelerim Çoğu Aynı veya Benzer	348	33,5	37,6	37,6
	Şifrelerimin Pek Çoğu Birbirinden Farklı	544	52,3	58,7	96,3
	Bilmiyorum	11	1,1	1,2	97,5
	Cevap Vermek İstemiyorum	23	2,2	2,5	100,0
	Toplam	926	89,0	100,0	
Geçersiz Cevaplar		114	11,0		
Toplam		1040	100,0		

Tablo 18 incelendiğinde katılımcıların %58,7 sinin farklı şifreler kullandığı, % 37,6 sının ise benzer veya aynı şifreler kullandığı görülmektedir. Bu sonuçlara göre katılımcıların büyük kısmının benzer şifrelerin kullanılmaması konusunda farkındalıkların iyi seviyede olduğu görülmektedir.

#### **5.1.4.3. Katılımcıların Şifrelerini Paylaşma Alışkanlıkları**

Veri setinde bu değişkenin değerlendirilebilmesi için katılımcılara “Have you ever shared a password to one of your online accounts with a friend or family member? (Kullandığınız şifreyi hiç arkadaşlarınızla veya akrabalarınızla paylaştığınız oldu mu?) sorusu yöneltilmiş ve katılımcıların “evet, hayır, bilmiyorum” ve “cevap vermek istemiyorum” seçeneklerinden birisini seçmeleri istenmiştir.

Aşağıda, tablo 19’ da gösterildiği gibi; katılımcıların 368 tanesi şifresini tanıdıkları ile paylaştığını, 555 tanesi paylaşmadığını, 1 tanesi bilmediğini ve 2 tanesi de cevap vermek istemediğini belirtmiştir. 114 katılımcının cevabı da geçersiz sayılmıştır.

**Tablo 19: Katılımcıların Şifrelerini Paylaşma Alışkanlıkları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Evet	368	35,4	39,7	39,7
	Hayır	555	53,4	59,9	99,7
	Bilmiyorum	1	0,1	0,1	99,8
	Cevap Vermek İstemiyorum	2	0,2	0,2	100,0
	Toplam	926	89,0	100,0	
Geçersiz Cevaplar		114	11,0		
Toplam		1040	100,0		

Benzer şifreleri kullananların oranı (Tablo 18’e göre %37,6) ile katılımcıların şifrelerini paylaşma oranlarının (Tablo 19’a göre %39,7) birbirine yakınlığı görülmektedir.

#### **5.1.4.4. Katılımcıların Sosyal Medya Hesaplarını Farklı Sitelere Erişirken Kullanma Eğilimleri**

Veri setinde bu değişkenin değerlendirilebilmesi için katılımcılara “Have you ever used your social media account information to log into another website, or have you never done this?” (Sosyal medya hesap bilgilerinizi diğer sitelere erişim sağlamak için hiç kullandınız mı?) sorusu yöneltilmiş ve katılımcıların evet, hayır, bilmiyorum ve cevap vermek istemiyorum seçeneklerinden birisini seçmeleri istenmiştir.

Aşağıda, tablo 20’ de gösterildiği gib katılımcıların 237 tanesi bunu yaptığını, 420 tanesi yapmadığını, 6 tanesi bilmediğini ve 2 tanesi de cevap vermek istemediğini belirtmiştir. 375 katılımcının cevabı da geçersiz sayılmıştır.

**Tablo 20: Katılımcıların Sosyal Medya Hesaplarını Farklı Sitelere Erişirken Kullanma Eğilimleri.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Evet	237	22,8	35,6	35,6
	Hayır	420	40,4	63,2	98,8
	Bilmiyorum	6	0,6	0,9	99,7
	Cevap Vermek İstemiyorum	2	0,2	0,3	100,0
	Toplam	665	63,9	100,0	
Geçersiz Cevaplar		375	36,1		
Toplam		1040	100,0		



#### 5.1.4.5. Katılımcıların Kamuya Açık Modemler Üzerinden İnternete Erişme Eğilimleri

Siber suçların yoğun olarak işlendiği yerlerden biri de kamuya açık ağlar olduğu bilinmektedir. Dolayısıyla bu ağları daha çok kullananların daha fazla mağduriyet yaşama olasılıkları bulunmaktadır. Şahısların kamusal alanda herkese açık olan ağlara erişimleri onların rutin aktivitelerinden birisi haline geldiği kabul edilebilir. Teori bağlamında kullanıcıların kamuya açık ağlar üzerinde ne kadar çok vakit geçirilirse aynı ağ içinde bulunan motive olmuş suçlu ile karşılaşmaları ve bu bağlamda suçun mağduru olma olasılıkları yükseleceği beklenmektedir.

Veri setinde katılımcıların bu eğilimlerinin ölçülebilmesi maksadıyla “Do you ever access public WiFi in places such as airports, cafes, hotels or libraries?” (Havaalanı, kafe, otel gibi yerlerde bulunan kamuya açık ağlara erişim sağlar mısınız? Bunu hiç yaptınız mı?) sorusu kullanılmış ve tablo 21’ de gösterildiği üzere; katılımcıların %54,2 sinin bu şekilde olan ağlara erişim sağladığı tespit edilmiştir. Aynı zaman da tablo 15’te de gösterildiği üzere; bu ağlara erişim yapan katılımcıların finansal işlemler yapmakta dikkatli olduğu, daha çok bu ağlar üzerinden e-posta ve sosyal medya hesaplarına eriştikleri görülmüştür. Bu da katılımcıların kamuya açık ağlarda daha fazla siber mağdur olabileceklerinin farkında olduklarını işaret etmektedir.

**Tablo 21: Kamusal Alanda Bulunan Ağlara Erişim Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Erişen	502	48,3	54,2	54,2
	Erişmeyen	422	40,6	45,6	99,8
	Cevap vermeyen	2	0,2	0,2	100,0
	Toplam	926	89,0	100,0	
Geçersiz cevaplar		114	11,0		
Toplam		1040	100,0		

### 5.1.5. Katılımcıların Suçtan Koruyabilecek Koruyucular Kullanma Alışkanlıklarının İncelenmesi

#### 5.1.5.1. Katılımcıların İki Faktörlü Koruma Sistemi Kullanma Alışkanlıkları.

İki faktörlü koruma sistemleri (Two factor authentication)’nde güvenlik sadece bir şifre ile sağlanmaz sizin bildiğiniz ya da sadece sizin bildiğinizi düşündüğünüz şifre sisteme giriş sağlayabilmenin ilk faktörüdür. Bu ilk faktör alan yazınında “bilinen” olarak geçmektedir. Bilinen şifreniz yetkisiz kişilerin eline de geçmiş olabilir. Bu tür yetkisiz kişilerin eline geçmiş şifreler ile sisteme girişin önlenebilmesi için ikinci faktör olarak “sahip olunan” kavramı geliştirilmiştir. Sahip olunan kavramı ile sizin şifreniz ile sisteme erişim yapılmaya çalışıldığında elinizde mevcut “sahip olunan” ile bu girişi onaylamazsanız sisteme giriş engellenmektedir.<sup>104</sup> Böylece yetkisiz kişiler şifrelerinizi ele geçirse bile sisteme erişim sağlayamamaktadır.\* Bu bağlamda bakıldığında rutin aktiviteler teorisi kapsamında bu sistemin kullanılması hedefin korunması açısından çok etkili bir tedbirdir ve bu sistemin kullanılması bir “koruyucu” olarak değerlendirilebilir.

Katılımcıların bu sistemi kullanıp kullanmadıkları veri setinde “Do you use two-factor or two-step authentication for any of your online accounts?” (Çevrimiçi hesaplarınız için iki faktörlü koruma sistemini kullanıyor musunuz?) sorusu ile ölçülmüştür. Soruya verilen yanıtlar tablo 22’ de gösterilmiştir. Buna göre katılımcıların %54’ü bu sistemi kullandığını belirtmişlerdir.

---

<sup>104</sup> Ertem Esiner, Anwitaman Datta “Two-factor authentication for trusted third party free dispersed storage” **Future Generation Computer Systems** s. 90 (2019): s. 291–306

\* İki faktörlü korumayı en güzel örneklerinden bir tanesi günümüzde internet bankacılığı işlemlerinde genellikle kullanılmaktadır. İnternet bankacılığı uygulamalarında ilk önce kullanıcıdan şifrenin girilmesi istenir bu “bilinen” dir. Kullanıcı şifreyi girdikten sonra elinde mevcut bir cihaza ikinci bir kod gelmektedir. Bu da “sahip olunan” faktörüdür. Sisteme erişim her iki bu iki faktörün birleşmesi ile olabilmektedir ve böylece yetkisiz kişilerin sisteme erişimi engellenmiş olmaktadır.

**Tablo 22: Katılımcıların İki Faktörlü Koruma Sisteminin Kullanma Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli cevaplar	Kullanan	500	48,1	54,0	54,0
	Kullanmayan	408	39,2	44,1	98,1
	Bilmeyen	11	1,1	1,2	99,2
	Cevap vermeyen	7	0,7	0,8	100,0
	Toplam	926	89,0	100,0	
Geçersiz cevaplar		114	11,0		
Toplam		1040	100,0		

**5.1.5.2. Katılımcıların Cihazlarına Ulaşırken Şifre Kullanma Alışkanlıkları**

Veri setinde bu değişkenin ölçülebilmesi için iki farklı soru kullanılmıştır. Birinci soru “Do you have to use a code, password, or other security feature in order to access your phone?” (Telefonunuza erişim sağlamak için kod, şifre veya farklı özellikte bir güvenlik özelliği kullanıyor musunuz?) şeklindedir. Bu soru ile katılımcıların mobil cihazlarına erişimde güvenlik tedbiri kullanıp kullanmadığı tespit edilmek istenmiştir bu kapsamda; katılımcılardan “evet, hayır, bilmiyorum” ve “cevap vermek istemiyorum” seçeneklerinden birisini seçmeleri istenmiştir. Tablo 23’ de gösterildiği üzere katılımcıların 529 tanesi bir güvenlik özelliği kullandığını (%70,9), 212 tanesi kullanmadığını (%28,4), 5 tanesi cevap vermek istemediğini belirtmiş, 294 katılımcının cevabı ise geçersiz sayılmıştır.

**Tablo 23: Katılımcıların Cihazlarına Ulaşırken Şifre Kullanma Alışkanlıkları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Evet	529	50,9	70,9	70,9
	Hayır	212	20,4	28,4	99,3
	Cevap Vermek İstemiyorum	5	0,5	0,7	100,0
	Toplam	746	71,7	100,0	
Geçersiz Cevaplar		294	28,3		
Toplam		1040	100,0		

İkinci Soru “What kind of security feature do you use to access your phone?” (Mobil cihazına erişimde kullandığınız güvenlik özelliği nedir?) şeklinde sorulmuş ve katılımcılardan “sadece numaralardan oluşan bir pin kodu, harf, rakam ve sembollerini içeren bir şifre, parmakla çizilen bir model, parmak izi, başka bir çeşit ekran kilidi” seçeneklerinden birisini seçmeleri istenmiştir. Tablo 24’ te gösterildiği üzere katılımcıların 190 tanesi numaralardan oluşan bir pin kodu kullandığını, 72 tanesi harf, sembol ve rakam içeren bir şifre kullandığını, 55 tanesi parmakla çizilen bir model kullandığını, 162 tanesi parmak izi kullandığını, 16 tanesi daha farklı bir ekran kilidi kullandığını, 6 tanesi bilmediğini, 28 tanesi de cevap vermek istemediğini belirtmiş. 511 katılımcının cevabı geçersiz sayılmıştır.

**Tablo 24: Katılımcıların Cihazlarına Erişimde Kullandığı Güvenlik Tedbirleri.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Numaralardan Oluşan Pin Kodu	190	18,3	35,9	35,9
	Harf, sembol ve numaralardan oluşan bir şifre	72	6,9	13,6	49,5
	Parmakla çizilen bir model	55	5,3	10,4	59,9
	Parmak İzi	162	15,6	30,6	90,5
	Daha Farklı Bir Ekran Kilidi	16	1,5	3,0	93,6
	Bilmiyorum	6	,6	1,1	94,7
	Cevap Vermek İstemiyorum	28	2,7	5,3	100,0
	Toplam	529	50,9	100,0	
Geçersiz Cevaplar		511	49,1		
Toplam		1040	100,0		

#### 5.1.5.3. Katılımcıların Kullandıkları Uygulamaları ve İşletim Sistemlerini Güncelleme Alışkanlıkları

Uygulamaların ve işletim sistemlerinin siber ortamda gelişen tehditlerin sürekli olarak hedefi olduğu düşünüldüğünde bu kuruluşların tehditlere karşı sürekli olarak kendilerini geliştirdiklerini ve bunun sonucu olarak da kendilerini güncelledikleri bilinen bir durumdur. Yeni gelişen bir tehdide karşılık olarak güncellenen işletim sistemi veya uygulama tehdidi bertaraf edebilirken güncellenmeyenler koruyucusuz

kalarak siber suçluların hedefleri olmaya devam edebilir. Çünkü motive olmuş siber suçlu güncellenen sistemlere giremeyecek ve güncellenmeyen sistemlere yönelecektir.

Kullanıcıların bu alışkanlıklarının tespit edilebilmesi maksadıyla veri setinde iki adet soru kullanılmıştır. Bu sorularla katılımcıların uygulamaları ve işletim sistemlerini güncelleme durumları ayrı olarak ölçülmüştür. Kullanılan ilk soru “Thinking about the APPS on your smartphone, how frequently do you update them?” (Akıllı telefonunuzdaki uygulamalar incelendiğinde onları hangi sıklıkla güncellersiniz?) şeklindedir ve cevaplar tablo 25’ te gösterilmiştir. Buna göre katılımcıların çok büyük bir çoğunluğu geç de olsa güncellemeleri yapmaktadır.

**Tablo 25: Katılımcıların Akıllı Cihazlardaki Uygulamaların Güncelleme Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli Cevaplar	Otomatik Olarak	213	20,5	28,6	28,6
	Yeni sürüm olduğun dair uyarı geldiğinde	135	13,0	18,1	46,6
	Uygun olduğum zamanlarda kendim güncellerim	286	27,5	38,3	85,0
	Güncellemem	84	8,1	11,3	96,2
	Farklı uygulamalar için farklı ayarlarım var	13	1,3	1,7	98,0
	Bilmiyorum	7	,07	0,9	98,9
	Cevap vermek istemiyorum	8	0,8	1,1	100,0
	Toplam	746	71,7	100,0	
Geçersiz Cevaplar		294	28,3		
Toplam		1040	100,0		

İkinci soru ise; “Thinking about the OPERATING SYSTEM on your smartphone, how frequently do you update it?” (Mobil cihazınızın işletim sistemini hangi sıklıkta güncellerseniz?) şeklinde olup katılımcıların akıllı cihazlarını güncelleme durumları tespit edilmek istenmiştir. Soruya verilen yanıtlar tablo 26’ da gösterilmiştir. Geçerli cevaplara bakıldığında katılımcıların %84,2’si İşletim sistemlerini güncellediğini, %13,7’si güncellemediğini belirtmiştir. Bu durum tablo 25’ teki veriler ile karşılaştırıldığında işletim sistemi ve uygulamaların güncelleme oranlarının birbirine çok yakın olduğu görülmektedir.

**Tablo 26: Katılımcıların Akıllı Cihazlarının İşletim Sistemlerini Güncelleme Durumu.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli cevaplar	Yeni sürüm olduğuna dair uyarı geldiğinde	318	30,6	42,6	42,6
	Müsait olduğumda	310	29,8	41,6	84,2
	Güncellemem	102	9,8	13,7	97,9
	Bilmiyorum	8	,8	1,1	98,9
	Cevap vermek istemiyorum	8	,8	1,1	100,0
	Toplam	746	71,7	100,0	
Geçersiz cevaplar		294	28,3		
Toplam		1040	100,0		

#### 5.1.5.4. Katılımcıların Anti Virüs Programı Kullanma Alışkanlıkları

Bilindiği üzere anti virüs programları kendi veri tabanlarını sürekli gelişen tehditlere karşı güncel tutarak bilişim sistemlerine zararlı yazılımların girişini engelleyebilirler. Bu kapsamda düşünüldüğünde bir teori bağlamında bir “koruyucu” olarak değerlendirilebilirler.

Bu tür uygulamaların kullanılma oranlarının tespit edilebilmesi maksadıyla veri setinde “Have you installed any virus protection apps on your smartphone, or not?” (Akıllı telefonunuza herhangi bir anti virüs yazılımı yüklediniz mi?) sorusu yöneltilmiştir. Katılımcıların bu soruya verdiği cevap tablo 27’ de gösterilmiştir. Geçerli cevaplara göre katılımcıların %31,8’i anti virüs programı kullandığını, %65,7’si ise kullanmadığını belirtmiştir. Anti virüs programı kullanmayanların siber suç mağduru olma ihtimallerinin daha fazla olacağı değerlendirilmektedir.

**Tablo 27: Katılımcıların Anti Virüs Programı Kullanma Alışkanlıkları.**

		Sayı	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli cevaplar	Evet	237	22,8	31,8	31,8
	Hayır	490	47,1	65,7	97,5
	Bilmiyorum	18	1,7	2,4	99,9
	Cevap vermek istemiyorum	1	0,1	0,1	100,0
	Toplam	746	71,7	100,0	
Geçersiz Cevaplar		294	28,3		
Toplam		1040	100,0		

## 5.2. Ölçüm

Verilerin tanımlayıcı istatistiklerinin değerlendirilmesinden sonra yapılacak analizlerin daha anlamlı sonuç verebilmesi ve değişkenler arasındaki bağı daha sağlıklı değerlendirilebilmesi amacıyla boş veriler SPSS programı vasıtası ile tamamlanmış ve uç değerler de bulunan veriler yine aynı program vasıtası ile tespit edilerek veri setinden çıkarılmıştır. Bütün bu işlemlerin yapılmasından sonra başlangıçta 1040 olan örneklem sayısı 795 e düşmüştür ve bundan sonraki analizler 795 sayısı üzerinden yapılmıştır.

Çalışmada asıl aralarındaki ilişkilerin ölçülmesinin amaçlandığı suç mağduriyeti, koruyucular ve rutin aktiviteler değişkenlerinin nasıl ölçümlenmesi gerektiği alan yazını ve kullanılan anket soruları birlikte değerlendirilerek araştırılmış ve bu değişkenler aşağıda belirtilen şekilde ölçülmüştür.

### 5.2.1. Siber Suç Mağduriyeti Değişkeninin Ölçülmesi

Anket metninde suç mağduriyetinin ölçülebilmesi amacıyla altı farklı soru kullanılmıştır. Bu sorular aşağıda verilmiştir.

1. Sosyal güvenlik numaranız başkası tarafından ele geçirildi mi?
2. Banka hesap numarası gibi daha başka şahsi numaralarınız başkaları tarafından ele geçirildi mi?
3. Banka kartlarınızdan bilginiz dışında para çıkışı oldu mu?
4. E-mail hesabınız başkaları tarafından ele geçirildi mi?
5. Sosyal medya hesabınız başkaları tarafından ele geçirildi mi?
6. Bilginiz dışında adınıza borçlandırıcı işlem (Kredi çekilmesi vb.) yapıldı mı?

Siber suç mağduriyeti değişkeninin ölçülmesinde ilk başta bu soruların hepsinde bir mağduriyet ölçeği oluşturulmak istenmiş olsa da yapılan güvenilirlik analizi neticesinde soruların kendi içlerinde tutarlılık göstermediği tespit edildiğinden ölçek oluşturulmaktan vazgeçilmiş ve suç mağduriyeti ankette belirtilen her suç için ayrı olarak ölçülmüştür.

### 5.2.2. Koruyucular Değişkeninin Ölçülmesi

Koruyucular değişkeninin ölçülebilmesi maksadıyla yapılan alan yazını çalışması ile ankette kullanılan sorular birlikte değerlendirildiğine aşağıda belirtilen beş soru belirlenmiştir.

1. Sanal ortamdaki hesaplarınıza erişirken “İki Faktörlü Koruma Sistemi” kullanıyor musunuz?
2. Telefonunuza erişmek için herhangi bir kod, şifre ya da başka bir güvenlik tedbiri kullanıyor musunuz?
3. Telefonunuzda bulunan uygulamaları günceller misiniz?
4. Cihazlarınızın işletim sistemini günceller misiniz?
5. Anti virüs programı kullanıyor musunuz?

Koruyucular değişkeninin ölçülebilmesi maksadıyla bu beş soru kullanılarak “Koruyucular” ölçeği oluşturulmuştur. Bu ölçekte yer alan soruların kendi aralarında iç tutarlılığının ölçülebilmesi maksadıyla güvenilirlik analizi yapılmıştır.<sup>105</sup> Yapılan güvenilirlik analizi sonucunda Cronbach Alpha sayısı 0,831 olarak tespit edilmiştir. Elde edilen bu değer “koruyucular” ölçeğinin yüksek güvenilirliğe sahip olduğunu belirtmektedir.

### 5.2.3. Rutin Aktiviteler Değişkeninin Ölçülmesi

Bu değişkenin ölçülebilmesi maksadıyla ankette kullanılan sorular alan yazını araştırması ile karşılaştırılmış ve aşağıda belirtilen dört adet sorunun bu değişkeni ölçmek için yeterli olduğu tespit edilmiştir.

1. Kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlıyor musunuz?
2. Kullandığınız şifreler birbirinin benzeri mi yoksa birbirinden farklı mı?
3. Şifrelerinizi başkaları ile paylaşıyor mısınız?

---

<sup>105</sup> Nuran BAYRAM, *Sosyal bilimlerde SPSS ile veri analizi* (Bursa: Ezgi Kitapevi, 2004), s.127



4. Sosyal medya hesaplarınızı başka sitelere erişim için de kullanırmısınız?

Belirtilen dört soru kullanılarak “Rutin aktiviteler” ölçeği oluşturulmuş ve ölçeğe güvenirlik analizi uygulanmıştır. Uygulanan analiz sonucunda Cronbach Alpha sayısı 0,708 olarak tespit edilmiştir. Elde edilen bu değer “Rutin aktiviteler” ölçeğinin yeterli güvenirliğe sahip olduğunu belirtmektedir.

### **5.3. Siber Suç Mağduriyeti İle Demografik Değişkenler Arasındaki İlişkinin İncelenmesi**

Siber suç mağduriyetinin ölçülmesinde anket uygulamasında mağdur olanlar 1, olmayanlar 2 olarak değerlendirilmiştir. Çalışmada gösterilecek şekillerin daha anlaşılabilir olması maksadıyla bu ölçümler SPSS programında mağdur olanlar 2, olmayanlar 1 olacak şekilde düzenlenmiş, 363 kişinin siber suç mağduru olduğu, 432 kişinin ise olmadığı tespit edilmiş, suç mağduriyeti ortalaması 1,45 olarak belirlenmiştir. Siber suç mağduriyetinin demografik değişkenlerle ilişkisinin incelenmesi maksadıyla yapılacak olan aşağıdaki analizlerde bu hususun dikkate alınması gerekmektedir.

#### **5.3.1. Cinsiyet İle Siber Suç Mağduriyeti Arasındaki İlişki**

Bu ilişkinin var olup olmadığının tespit edebilmek için aşağıda belirtilen hipotez kullanılmıştır.

H0: Cinsiyet ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Cinsiyet ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla T-Testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi kabul edilmiştir. Diğer bir ifade ile Siber suç mağduriyeti ile cinsiyet arasında anlamlı bir ilişki yoktur. ( $T=-1,143$ ,  $P>0,05$ )

#### **5.3.2. Yaş İle Siber Suç Mağduriyeti Arasındaki İlişki**

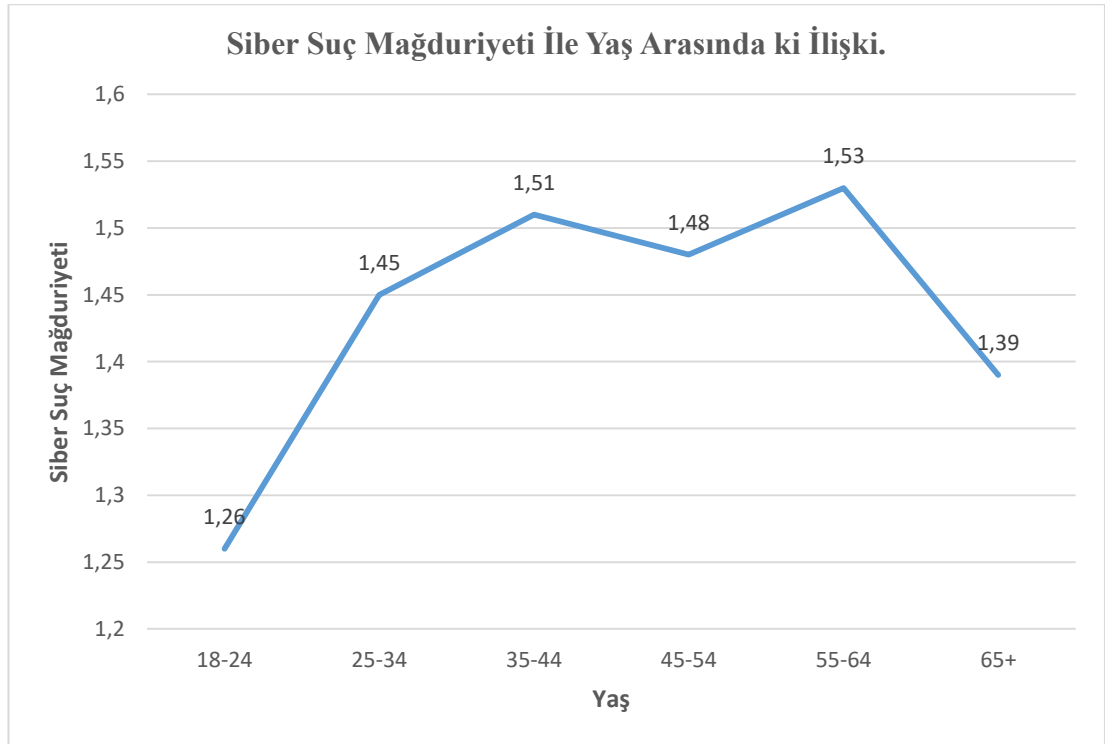
Yaş değişkeni analize katılmadan önce 18-24, 25-34, 35-44, 45-54, 55-64, 65+ olacak şekilde yeniden kodlanmış siber suç mağduriyeti ile belirtilen yaş grupları arasında anlamlı bir ilişkinin var olup olmadığının tespit edebilmek için aşağıda belirtilen hipotez kullanılmıştır.

H0: Yaş ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Yaş ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla tek yönlü ANOVA testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi reddedilmiştir. Diğer bir ifade ile yaş ile siber suç mağduriyeti arasında bir ilişki vardır. (f:4,221,  $P<0,05$ )

Kişilerin siber suç mağduru olma durumları yaş gruplarına göre farklılık göstermektedir buna göre Şekil 4’ te gösterildiği üzere siber suç mağduriyeti yaşama durumu 25-64 yaş arasında yoğunlaşmıştır. Yani bu yaş aralığında bulunanlar diğerlerine göre daha fazla siber suç mağduru olmaktadır.



**Şekil 4: Siber Suç Mağduriyeti İle Yaş Arasında ki İlişki.**

### 5.3.3. Eğitim Düzeyi İle Siber Suç Mağduriyeti Arasında ki İlişki

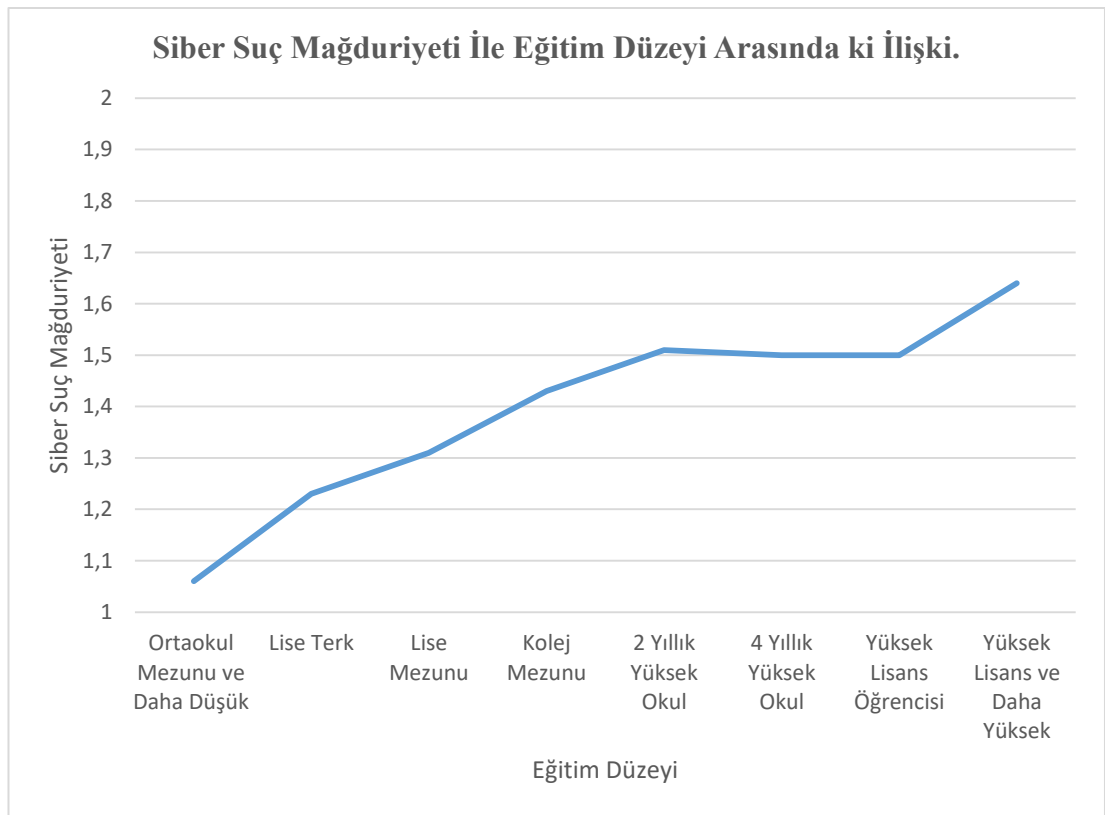
Bu ilişkinin var olup olmadığının tespit edebilmek için aşağıda belirtilen iki adet hipotez oluşturulmuştur.

H0: Eğitim düzeyi ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Eğitim düzeyi ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla tek yönlü ANOVA testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi reddedilmiştir. Diğer bir ifade ile eğitim düzeyi ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır. ( $f=8,758$ ,  $P<0,05$ )

Kişilerin siber suç mağduriyetleri eğitim düzeylerine göre farklılık göstermektedir. Buna göre Şekil 5’ te gösterildiği üzere kişilerin eğitim düzeyi arttıkça siber suç mağduru olma ihtimalleri de artmaktadır.



**Şekil 5: Siber Suç Mağduriyeti İle Eğitim Düzeyi Arasında ki İlişki.**

#### **5.3.4. Medeni Hal İle Siber Suç Mağduriyeti Arasında ki İlişki**

Medeni hal değişkeninin ölçümü için katılımcılardan “evli, birlikte yaşayan, boşanmış, ayrı yaşayan, dul, hiç evlenmemiş” seçeneklerinden birisini seçmeleri istenmiştir.

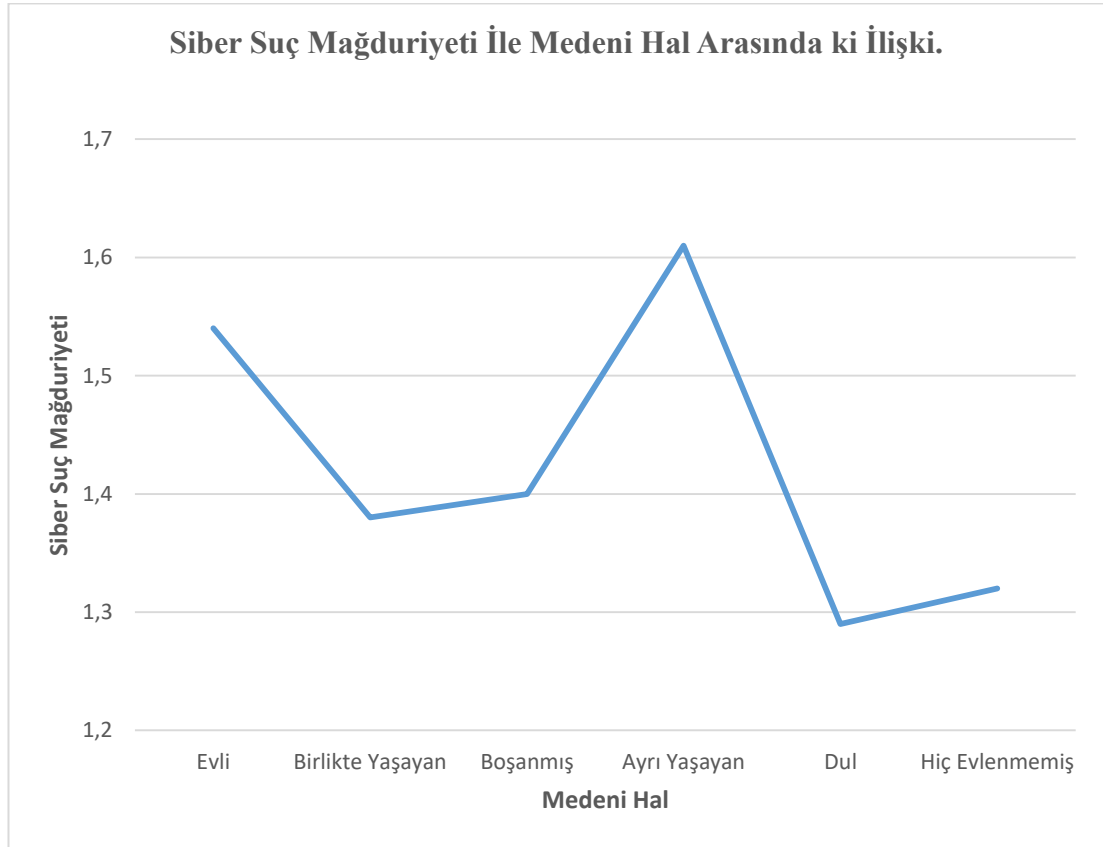
Bu ilişkinin var olup olmadığının tespit edebilmek için aşağıda belirtilen iki adet hipotez oluşturulmuştur.

H0: Medeni hal ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Medeni Hal ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla tek yönlü ANOVA testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi reddedilmiştir. Diğer bir ifade ile medeni hal ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır. ( $f=7.388$ ,  $P<0,05$ )

Kişilerin siber suç mağduriyetleri medeni durumlarına göre farklılık göstermektedir. Buna göre Şekil 6’ da gösterildiği üzere ayrı yaşansa bile evli olanlar diğerlerine göre daha fazla siber suç mağduru olmaktadır.



**Şekil 6: Siber Suç Mağduriyeti İle Medeni Hal Arasında ki İlişki.**

### 5.3.5. Çalışma ile Siber Suç Mağduriyeti Arasında ki İlişki

Katılımcıların çalışma durumları “tam zamanlı çalışan, yarı zamanlı çalışan ve çalışmayan” olmak üzere üç farklı grup altında ölçülmüştür.

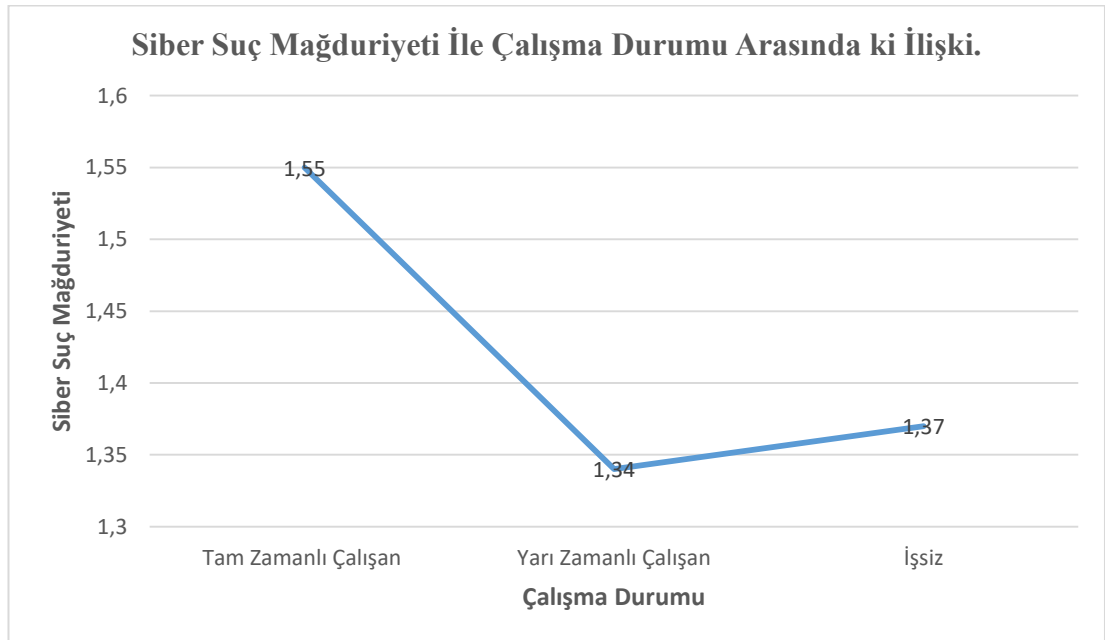
Bu ilişkinin var olup olmadığının tespit edebilmek için aşağıda belirtilen iki adet hipotez oluşturulmuştur.

H0: Çalışma durumu ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Çalışma durumu ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla tek yönlü ANOVA testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi reddedilmiştir. Diğer bir ifade ile çalışma durumu ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır. ( $f=14.620$ ,  $P<0,05$ )

Kişilerin siber suç mağduru olma durumları çalışma durumlarına göre farklılık göstermektedir. Şekil 7’ de gösterildiği üzere tam zamanlı çalışanlar diğerlerine göre daha fazla siber suç mağduru olmaktadır.



**Şekil 7: Siber Suç Mağduriyeti İle Çalışma Durumu Arasındaki İlişki.**

### 5.3.6. Yıllık Gelir ile Siber Suç Mağduriyeti Arasındaki İlişki

Katılımcıların yıllık gelirlerinin ölçülebilmesi maksadıyla yıllık gelirlerini belirtmeleri istenmiş ve tespit edilen veriler “10000 Doların altında, 10000-20000 Dolar arasında, 20000-30000 Dolar arasında, 30000-40000 Dolar arasında, 40000-50000 Dolar arasında, 50000-75000 Dolar arasında, 75000-100000 Dolar arasında, 100000-150000 Dolar arasında ve 150000 Doların üzerinde” olacak şekilde gruplandırılmıştır.

Bu ilişkinin var olup olmadığının belirlenebilmesi maksadıyla aşağıdaki hipotez oluşturulmuştur.

H0: Yıllık gelir ile siber suç mağduriyeti arasında anlamlı bir ilişki yoktur.

H1: Yıllık gelir ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır.

H0 hipotezinin test edilebilmesi maksadıyla tek yönlü ANOVA testi uygulanmıştır. Yapılan analiz sonucunda H0 hipotezi reddedilmiştir. Diğer bir ifade ile yıllık gelir ile siber suç mağduriyeti arasında anlamlı bir ilişki vardır. ( $f=12.763$ ,  $P<0,05$ )

Kişilerin siber suç mağduriyeti yaşama durumları yıllık gelirlerine göre farklılık göstermektedir. Şekil 8’ de de görüleceği üzere yıllık gelir arttıkça siber suç mağduriyeti yaşama durumu da artmaktadır.



Şekil 8: Siber Suç Mağduriyeti ile Yıllık Gelir Arasında ki İlişki.

#### 5.4. Suç Mağduriyeti, Rutin Aktiviteler ve Koruyucular Arasındaki İlişkinin Analizi

Rutin aktiviteler teorisinin 3 ana ögesi olan bu değişkenlerin arasında ki ilişkinin analiz edilebilmesi maksadıyla Pearson Korelasyon katsayılarının hesaplanması yoluna gidilerek değişkenler arasındaki ilişki belirlenmeye çalışılmıştır. Hesaplamalara koruyucular, rutin aktiviteler ve ankette ölçülen 6 farklı suç tipi sokulmuştur. Tablo 28’ de rutin aktiviteler ve koruyucular değişkeni ile arasında hiçbir ilişki tespit edilemeyen kimlik numarasının çalınması ve adına borçlandırıcı işlem yapılması (Kredi çekilmesi vb.) gösterilmemiştir. Analiz sonuçları yorumlanırken dikkat edilmesi gereken en önemli nokta; siber suç mağduru olanların mağduriyet sonrasında koruyucuları kullanmaya başlayacaklarıdır. Ankette kullanılan soru şeklinde bu ayrıma gidilmemiş, dolayısıyla koruyucu kullananların daha fazla suç mağduru olduğu gibi sonuçlar ortaya çıkmıştır. Bundan sonra yapılacak olan çalışmalarda bu hususun üzerinde durulması önem arz etmektedir. Bu durumu ölçmek için kullanılacak sorular “Anti virüs programı kullanıyor musunuz?” şeklinde değil, suç mağduriyeti yaşamış olanlara; “Mağdur olmadan önce anti virüs programı kullanıyor muydunuz?” şeklinde belirlenmelidir.

Yapılan korelasyon analizi sonucunda;

1. Katılımcıların kimlik numaraları dışında diğer hassas bilgilerinin çalınması yoluyla suç mağduru olmaları ile rutin aktiviteleri arasında negatif yönlü zayıf bir ilişki tespit edilmiştir. ( $r=-0,075$ ,  $P<0,005$ ) bununla birlikte aynı suçtan mağduriyet yaşamak ile koruyucular arasında herhangi bir ilişki tespit edilememiştir.

2. Katılımcıların banka hesaplarında şüpheli hareketler gözlemlenmesi sonucu siber suç mağduru olmaları ile koruyucular arasında negatif yönlü zayıf bir ilişki ( $r=-0,099$ ,  $P<0,001$ ), rutin aktiviteler arasında yine negatif yönlü zayıf bir ilişki ( $r=-0,096$ ,  $P<0,001$ ) tespit edilmiştir.

3. Katılımcıların E-posta hesaplarının çalınması sonucunda siber suç mağduru olmaları ile koruyucular arasında pozitif yönlü orta seviyede bir ilişki ( $r=0,469$ ,  $P<0,001$ ), rutin aktiviteler arasında yine pozitif ve orta seviyede bir ilişki ( $r=0,680$ ,  $P<0,001$ ) tespit edilmiştir.

4. Katılımcıların Sosyal medya hesaplarının çalınması sonucunda siber suç mağduru olmaları ile koruyucular arasında pozitif yönlü orta seviyede bir ilişki

( $r=0,348$ ,  $P<0,001$ ) rutin aktiviteler arasında yine pozitif ve orta seviyede bir ilişki ( $r=0,532$ ,  $P<0,001$ ) tespit edilmiştir.

**Tablo 28: Mağduriyet, Rutin Aktiviteler ve Koruyucular Arasındaki İlişki.**

	Koruyucular	Rutin Aktiviteler	Diğer Hassas Şahsi Bilgilerin Çalınması	Banka Hesaplarında Şüpheli Hareketler Tespit Edilmesi	E-Posta Hesabının Çalınması	Sosyal Medya Hesabının Çalınması
Koruyucular	1					
Rutin aktiviteler	,432**	1				
Diğer Hassas Şahsi Bilgiler (Kimlik numarası dışında) in Çalınması	-,067	-,075*	1			
Banka Hesaplarında Şüpheli Hareketler Tespit Edilmesi	-,099**	-,096**	,349**	1		
E-Posta Hesabının Çalınması	,469**	,680**	,007	-,028	1	
Sosyal Medya Hesabının Çalınması	,348**	,532**	-,121**	-,076*	,348**	1

\*İlişki %95 oranında önemlidir.

\*\*İlişki %99 oranında önemlidir.



## SONUÇ VE DEĞERLENDİRME

2'nci Dünya Savaşı sonrası değişen yeni sosyal düzen içinde, gittikçe artan suç olaylarına bir açıklama getirmeye çalışan Rutin Aktiviteler Teorisi ilk ortaya çıktığı zamanda, kendisinden önceki teorilerden sıyrılarak bir çığır açmıştı. Önceki teoriler sadece suçlu üzerinden suçu tanımlamaya çalışırken, Rutin Aktiviteler Teorisi suçu bir fırsatlar ürünü olarak görmeye başlamış ve suçun oluşabilmesi için motive olmuş suçlu, koruyucuların yokluğu, uygun hedef üçlüsünün belli bir zaman ve mekânda bir araya gelmesi gerektiğini savunmuştu. Bunun sonucu olarak da suç önleme stratejilerini, bu bir araya gelmenin önlenmesi üzerine kurmuştu. Teori'nin, ilk ortaya atıldığı zamanlar, özellikle, mala karşı işlenen suçları çok iyi açıklayabildiği<sup>106</sup> test edildi.

İnsanlar arasında var olan sosyal düzen ve sosyal ilişkiler, Rutin Aktiviteler Teorisi'nin ortaya çıktığı zamandan farklı olarak, günümüzde hızlı bir şekilde sanal ortama taşınmaya başladı. Bunula birlikte, toplumun her döneminde var olan suç kavramı da sanal ortama kayma yoluna girdi. Önceleri sadece sapma olarak tanımlanan; siber ortamda işlenen hoş görülmeyen davranışlar, zamanla kendilerine kanunda yer bularak suç haline gelmeye başladı.

Sosyal ilişkilerin siber ortamlara kayması ile birlikte insanların rutin faaliyetleri de siber ortamlara doğru kaymaya başladı. Eskiden insanlar bir ürün almak için sokağa çıkmak ve mecburen bir rutin faaliyette bulunmak zorundaydılar. Ama günümüzde aynı ürün evden çıkmadan, sanal ortam üzerinden satın alınabilmekte buna karşın faaliyet hâlâ bir rutin aktivite içermektedir. Sokakta bizi suçtan koruyabilecek bir köpekken, rutin aktivitenin bulunduğu sanal ortamda koruyabilecek belki de bir anti virüs programı veya alacağımız basit bir tedbirdir. Bu bağlamda Rutin Aktiviteler Teorisi araştırmanın kuramsal çerçevesini oluşturmuştur.

---

<sup>106</sup> John M.STAURA, John J.SALOAN "Urban Stratification of Places, Routine Activities and Suburban Crime Rates" *Social Forces* c.4 (1988), s.1102-1118

## 6.1. Tanımlayıcı İstatistikler ve Hipotezlerin Değerlendirilmesi

Kuramsal çerçeve bu şekilde belirlendikten sonra ABD’de bir araştırma şirketi tarafından uygulanan anket verileri SPSS 20.0 programı üzerinden analiz edilmiştir. Bu analizin sonuçları aşağıda sıralanmıştır.

Katılımcıların demografik özellikleri ile ilgili olarak;

%51,1’inin kadın, %48,9’unun erkek olduğu,

Çoğunluğunun 25-65 yaş arasında olduğu,

%53,6’sının eğitim düzeyinin yüksekokul ve daha üstünde olduğu,

%50,4’ünün evli olduğu,

%60,8’inin tam veya yarı zamanlı çalıştığı,

%49,3’ünün banliyölerde, %31,3’ünün şehirde, %19,4’ünün ise kırsal da yaşadığı, görülmüştür.

Katılımcıların İnternet kullanım alışkanlıkları ile ilgili olarak;

%86,3’ünün internet kullanıcısı olduğu,

%50,4’ünün her gün pek çok kez internete eriştiği,

%63,9’unun sosyal medya kullandığı

%71,8’inin internet bankacılığı kullandığı,

%71’inin şahsi verilerinin güvenliğinden şüphe duyduğu,

%49,7’sinin kamuya açık alanlardan internete erişim sağladığı görülmüştür.

Katılımcıların siber suç mağduriyeti ile ilgili olarak;

%13,1’inin sosyal güvenlik numarasının ele geçirildiği,

%38,7’sinin banka hesap numarasının ele geçirildiği,

%45,7’sinin kartında şüpheli işlemler tespit edildiği,

%16,8’inin e-posta hesabının,

%11,8’inin ise sosyal medya hesabının çalındığı,

%14,7'sinin şahsi bilgileri çalınarak adına borçlandırıcı işlem yapılmış olduğu görülmüştür.

Katılımcıların rutin aktiviteleri ile ilgili olarak;

%74,6 sınıfın şifrelerini ezberleyerek aklında tutmaya çalıştığı,

%46,3' ünün şifrelerini bir kâğıda yazılı olarak saklamaya çalıştığı,

%10,8' inin bir şifre yönetim programı kullandığı,

%20,7' sinin bilgisayarda bir doküman üzerine kaydettiği,

%15,7'sinin browser üzerinde sakladığı,

%37,6' sınıfın benzer veya tamamen aynı şifreleri kullandığı,

%39,7' sinin şifrelerini başkaları ile paylaştığı,

%35,6'sının sosyal medya hesapları üzerinden başka sitelere bağlandığı ve

%54,2' sinin kamuya açık alanlardan internete eriştiği görülmüştür.

Katılımcıların koruyucu kullanma durumları incelendiğinde;

%54' ünün iki faktörlü koruma sistemleri kullandığı,

%70,9' unun cihazlarına erişirken şifre veya güvenlik kodu gibi önlemleri kullandığı,

%28,6' sınıfın uygulamalarını ve işletim sistemlerini otomatik olarak güncellediği,

%31,8' inin anti virüs programları kullandığı görülmüştür.

Demografik değişkenler ile suç mağduriyeti arasındaki ilişkinin incelenmesi neticesinde;

Siber suç mağduriyeti ile cinsiyet arasında anlamlı bir ilişki olmadığı ( $T=-1,143$ ,  $P>0,05$ ),

Siber suç mağduriyetinin 24-65 yaş arasında yoğunlaştığı, ( $f=4,221$ ,  $P<0,05$ ),

Eğitim seviyesi arttıkça siber suç mağduriyetinin arttığı ( $f=8,758$ ,  $P<0,05$ ),

Ayrı yaşıyor olsa bile evli olmanın mağduriyeti arttırdığı, ( $f=7.388$ ,  $P<0,05$ ),

Tam zamanlı çalışanların diğerlerine göre daha fazla mağduriyet yaşadığı ( $f=14.620$ ,  $P<0,05$ ),

Yıllık gelir arttıkça mağduriyetin de arttığı ( $f=12.763$ ,  $P<0,05$ ) görülmüştür.

Siber suç mağduriyeti, koruyucular ve rutin aktiviteler arasındaki ilişkinin incelenmesi neticesinde;

Katılımcıların kimlik numaraları dışında diğer hassas bilgilerinin çalınması yoluyla suç mağduru olmaları ile rutin aktiviteleri arasında negatif yönlü zayıf bir ilişki tespit edilmiştir. ( $r=-0,075$ ,  $P<0,005$ ) bununla birlikte aynı suçtan mağduriyet yaşamak ile koruyucular arasında herhangi bir ilişki tespit edilememiştir.

Katılımcıların banka hesaplarında şüpheli hareketler gözlemlenmesi sonucu siber suç mağduru olmaları ile koruyucular arasında negatif yönlü zayıf bir ilişki ( $r=-0,099$ ,  $P<0,001$ ), rutin aktiviteler arasında yine negatif yönlü zayıf bir ilişki ( $r=-0,096$ ,  $P<0,001$ ) tespit edilmiştir.

Katılımcıların e-posta hesaplarının çalınması sonucunda siber suç mağduru olmaları ile koruyucular arasında pozitif yönlü orta seviyede bir ilişki ( $r=0,469$ ,  $P<0,001$ ), rutin aktiviteler arasında yine pozitif ve orta seviyede bir ilişki ( $r=0,680$ ,  $P<0,001$ ) tespit edilmiştir.

Katılımcıların sosyal medya hesaplarının çalınması sonucunda siber suç mağduru olmaları ile koruyucular arasında pozitif yönlü orta seviyede bir ilişki ( $r=0,348$ ,  $P<0,001$ ) rutin aktiviteler arasında yine pozitif ve orta seviyede bir ilişki ( $r=0,532$ ,  $P<0,001$ ) tespit edilmiştir.

## 6.2. Öneriler

Sonraki çalışmalar esnasında, siber suç mağduru olanların mağduriyet sonrası koruyucuları kullanmaya başlayabileceği düşünülerek, koruyucular değişkeninin ölçülmesi hususunda dikkatli olunmalıdır. Bu değişkenin ölçülebilmesi maksadıyla sorulabilecek bir soru “Anti virüs programı kullanıyor musunuz?” şeklinde değil de, suç mağduriyeti yaşamış şahıslara “Mağduriyet yaşamadan önce anti virüs programı kullanıyor muydunuz?” şeklinde olmalıdır.

Siber suçlar incelenirken sadece mevzuatta bulunan suçlar üzerinden inceleme yapmak çoğu zaman günceli yakalayamamak ile sonuçlanacaktır. Çünkü siber dünya

ve onun çok küçük bir parçası olan siber suçların her geçen gün işlenme yöntemleri değişmekte dolayısıyla siber suçlular kendilerini sürekli yenilemektedir. Bunun sonucu olarak da günümüzde suç olarak tanımlanması akla bile gelmemiş birtakım eylemler, yakın bir gelecekte suç olarak karşımıza çıkabilecektir. Sonraki çalışmalarda bu husus da göz önünde bulundurulmalıdır.

İncelenen teori bağlamında, siber suçların önlenmesi için; kamuoyunun bilgilendirilmesi ve kamuoyunda bir farkındalık oluşturulması maksadıyla kamu spotları ve/veya ilan afişler oluşturulmalıdır.

- Bunların içeriğinde özellikle, tanınan kişilerle dâhi şifre ve kişisel bilgilerin paylaşılması gerektiği,
- Kullanılan şifrelerin aynı veya benzer olmaması gerektiği,
- Kullanılan uygulama ve işletim sistemlerinin güncel bulundurulması gerektiği gibi hususlar yer almalıdır.

Siber suç mağduru olmak açısından yüksek risk grubunda yer alanlardan, özellikle eğitim düzeyi ve gelir durumu yüksek olanların, 25-64 yaş arasında olanların, evli olanların, tam zamanlı bir işte çalışanların yüksek risk grubunda olduklarına dair e-posta veya mektup ile bilgilendirilmeleri ve bu bilgilendirme metinlerinin içerisinde alınması gereken tedbirlere de mutlaka yer verilmesi gerektiği unutulmamalıdır.

Kanunlar, hâli hazırda kendilerinde var olmayan fakat her an gelişebilecek/geliştirilebilecek siber suç işleme yöntemlerini de içine alacak şekilde geliştirilmelidir.

### **6.3. Sonuç**

Yapılan araştırmada farklı siber suç türleri farklı ilişkiler gözlemlenmiştir. Bu bağlamda Rutin Aktiviteler Teorisi her suç türü için farklı özellik göstermektedir. Bu yüzden geliştirilecek suç önleme stratejileri de her suç için ayrı düşünülerek ortaya konulmalıdır. Rutin Aktiviteler Teorisi penceresinden bakıldığında, koruyucular ve suç mağduriyetinin arasında negatif yönlü bir ilişki beklenirken çalışmada bunun aksi yönünde bir ilişki tespit edilmiştir. Bunun sebebi olarak siber suç mağduriyeti yaşayanların hemen sonrasında koruyucuları kullanmaya başlamaları ve ankette sorulan sorulara buna göre cevap vermeleri görülebilir. Bundan sonraki çalışmalarda

bu konu üzerinde hassasiyetle durulmalı, koruyucular değişkeni ölçülürken dikkatli davranılmalı, çok yönlü düşünülmelidir.

Teori bağlamında rutin aktiviteler ile suç mağduriyeti arasında pozitif yönlü bir ilişki öngörülmektedir. Yapılan analiz sonuçlarında öngörüldüğü üzere, bu iki değişken arasında anlamlı ve pozitif yönde bir ilişki gözlemlenmiştir.

Tüm analizler birlikte değerlendirildiğinde Rutin Aktiviteler Teorisi'nin bilişim suçlarını açıklamakta yeterli olduğu, fakat bu yeterliliğin tespiti için özellikle teorinin koruyucular temeli üzerinde daha farklı, daha detaylı ve farklı kültürler üzerinde çalışılması, nicel verilerin nitel yöntemlerle de desteklenmesi gerekmektedir.

## KAYNAKÇA

- Akbulut, Berrin. “Sistemi Engelleme, Bozma, Verileri Yok Etme Veya Değiştirme”. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi*, c.24. s.2 (2016): ss.7-55.
- Altunok, Ebru, Ali Fatih Vural. “Bilişim Suçları”. *Denetim*. s.8 (2011): ss.74-84.
- Antunes, George E., Fay Lomax Cook, Thomas D.Cook, Wesley G. Skogan. “Patterns of Personal Crime Against The Elderly” *The Gerontologist* c.17. s.4 (1977) ss:321-327
- Aslay, Fulya. “Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi” *International Journal of Multidisciplinary Studies and Innovative Technologies*, c.1. s.1 (2017) ss.24-28
- Avşar Zakir, Öngören Gürsel. *Bilişim hukuku*. yayın no:270 (İstanbul, Türkiye Bankalar Birliği, 2010).
- Aydın, Emin Doğan. *Bilişim Suçları ve Hukukuna Giriş*, 1. bs. Ankara, Doruk Yayınları, 1992 den (aktaran Hüseyin Çakır ve diğ., *Güncel Tehdit: Siber Suçlar* (Ankara: Seçkin Yayınları, 2014).
- Bademci, Vahit. “Kuder-Richardson 20, Cronbach’ın Alfası, Hoyt’un Varyans Analizi, Genellenirlik Kuramı Ve Ölçüm Güvenirliği Üzerine Bir Çalışma”. *Dicle Üniversitesi Ziya Gökalp Eğitim Fakültesi Dergisi*, s.17. (2011) ss.173-193
- Barwinski, M. A., “Taxonomy of Spyware and Empirical Study of Network Drive-By-Downloads, Thesis,” *Naval Postgraduate School, Monterey, California*, 2005 den aktaran G.CANBEK, Ş.SAĞIROĞLU Bilgisayar Sistemlerine Yapılan Saldırıları Ve Türleri: Bir İnceleme *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi* s.23, (2007) ss. 1-12
- Bayram, Nuran. *Sosyal bilimlerde SPSS ile veri analizi* 1.bs. Bursa: Ezgi Kitapevi, 2004.
- Bennert Richard R., "Routine activities: A cross-national assessment of a criminological perspective." *Social Forces* c.70. s.1. (1991) ss.147-163.
- Bilek, Burak Tunç. *Bilişim Suçları Ve Üniversite Lisans Öğrencilerinin Bilişim Suçlarına Yönelik Görüşleri*. Ankara: Gazi Üniversitesi Bilişim Enstitüsü Yüksek Lisans Tezi, 2012).
- Bossler, Adam M., Thomas J. Holt. “On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory.” *International Journal of Cyber Criminology*. c.3 s.1 (2009) s.400-420
- Büyüköztürk, Şener. *Sosyal Bilimler İçin Veri Analizi El Kitabı İstatistik, Araştırma Deseni, SPSS Uygulamaları ve Yorum*. bs.24, Ankara, Pegem Akademi, 2018.
- Clarke, Ronald V. “Situational Crime Prevention: Its Theoretical Basis and Practical Scope.” *Crime and Justice* c.4. (1983) ss. 225–256.

- Cohen Lawrence E., Marcus Felson "Social Change And Crime Rate Trends: A Routine Activity Approach" *American Sociological Review* s.44. (Ağustos 1979): ss.588-608
- Cohn Ellen G., James Rotton. "Weather, seasonal trends and property crimes in Minneapolis, 1987–1988. A moderator-variable time-series analysis of routine activities." *Journal of Environmental Psychology* c.20. s.3. (2000) ss: 257-272.
- \_\_\_\_\_. "Even criminals take a holiday: Instrumental and expressive crimes on major and minor holidays." *Journal of Criminal Justice* c.31. s.4. (2003) ss.351-360.
- Cordella PETER, LARRY J. Siegel, *Readings in Contemporary Criminological Theory*, Boston, Northeastern University Press, 1996.
- Çakır, Hüseyin, Mehmet Serkan KILIÇ, M. Akif Ocak, Yıldırım Yalman, Nursel Yalçın, Çelebi Uluyol, Erinc Karataş, Recep Benzer, Şahin Gökçearslan, Ahmet Çubukcu, Akın Aytekin, Ömer Özer, Tarık Doğan *Güncel Tehdit: Siber Suçlar* 1. bs. Ankara: Seçkin Yayıncılık, 2014.
- Dışişleri Bakanlığı. "Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu" 1/676, Yasama Dönemi:24, Yasama Yılı:3, ss.:380, 20 Aralık 2012.
- Dolu, Osman. *Suç Teorileri*, 5. bs. Ankara, Global Politika ve Strateji Yayınları, 2015.
- Durkheim, Emile. *Toplumsal İşbölümü*, çev. Özer Ozankaya İstanbul: Cem Yayınevi, 2014.
- Duru, Hacı. "Liselerin, İçkili Yerlerin Ve Kahvehanelerin Sokak Üzerinde Oluşan Suça Etkisi Bursa Örneği", *Süleyman Demirel Üniversitesi Hukuk Fakültesi Dergisi* c.3. s.2. (2013) ss.1-105.
- Erdoğan, YAVUZ. "Bilişim Sistemine Girme ve Kalma Suçu" *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, c.12. özel sayı (2010) ss.1363-1433.
- Esiner, Ertem, Anwitaman Datta "Two-factor authentication for trusted third party free dispersed storage" *Future Generation Computer Systems* s.90. (2019) ss.291–306
- Felson, Marcus. *Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes The Reasoning Criminal: Rational Choice Perspectives On Offending* 1.bs. New Jersey, Transaction Publishers, 1986.
- \_\_\_\_\_. "Those Who Discourage Crime" *Crime And Place* c.4. (1995) ss.53-66.
- Felson, Marcus, Rachel L. BOBA. *Crime And Evreyday Life* Washington D.C., Sage Yayıncılık, 2010.
- Felson, Marcus, R.V. Clarke. "*Opportunity Makes the Thief.*" Police Research Series Paper 98, Policing and Reducing Crime Unit. Research, Development and Statistics Directorate. London: Home Office 1998..



- Hawley AMOS "Human Ecology: A Theory Of Community Structure." Newyork Ranold Yayıncılık (1950)'den aktaran Dolu, Osman. **Suç Teorileri**, 5. bs. Ankara, Global Politika ve Strateji Yayınları, 2015.
- Herbert David D., Stephen W. Hyde "Enviromental Criminology: Testing Some Area Hypotesis." **Transactions of the Institute of British Geographers** c.10. s.3. (1985) ss.259-274.
- İçli, Tülin Günşen. **Kriminoloji**. 9. bs. Ankara: Seçkin Yayıncılık, 2016.
- Kanayama, Taisuke. "Impact of Cybercrime in Japan Findings of Cybercrime Victimization Survey" **Sociology Study**. c.7. s.6. (2017) ss.331-340
- Korkmaz, İbrahim. "Cihaz, Program, Şifre ve Güvenlik Kodlarının Bilişim Suçlarının İşlenmesi Amacıyla İmal ve Ticareti Suçu" **Terazi Hukuk Dergisi**, c.13. s.142. (2018) ss.45-55.
- Kurma, E. "Approaching Zero Data Crime and the Computer Underworld," çeviri Mungo,P. Ve Bryan Clough, 1999. (Aktaran: Çakır, Hüseyin, Mehmet Serkan KILIÇ, M. Akif Ocak, Yıldıray Yalman, Nursel Yalçın, Çelebi Uluyol, Erinç Karataş, Recep Benzer, Şahin Gökçearsan, Ahmet Çubukcu, Akın Aytekin, Ömer Özer, Tarık Doğan **Güncel Tehdit: Siber Suçlar** 1. bs. Ankara: Seçkin Yayıncılık, 2014.
- Madenüs, Murat. "Değişen Kırsal Yaşam Alışkanlıklarının Hırsızlık Suçuna Etkisi.", **Güvenlik Bilimleri Dergisi** c.5 s.2, (2016) ss.61-91.
- Miethe Terance D., Mark C.Stafford, J.Scott Long. "Social Differentiation in Criminal Victimization: A Test of Routine Activities/Lifestyle Theories." **American Sociological Review** c.52. s.2. (1987) ss.184-194.
- Mustaine, E. Ehrhardt, Richard Tewksbury. "Predicting risks of larceny theft victimization: A routine activity analysis using refined lifestyle measures." **Criminology** c.36. s.4. (1998) ss.829-858.
- Roncek Dennis W., Pamela A. Maier. "Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of hot spots." **Criminology** c.29. s.4. (1991) ss.725-753.
- Schwartz Martin D., Walter S. Dekeserdy, David Tait, Shadid Alvi. "Male peer support and a feminist routing activities theory: Understanding sexual assault on the college campus." **Justice Quarterly** c.18. s.3. (2001) ss.623-649.
- Sherman, Lawrence W., Patrick R. Gartin, Michael E. Buerger. "Hot spots of predatory crime: Routine activities and the criminology of place." **Criminology** c.27. s.1. (1989) ss.27-56
- Sözer, M. Alper, Ercan Balcıoğlu, Hüseyin Akdoğan, Fatih Tombul, Kazım Seyhan, Murat Özkan, Mehmet Kul, Arif Akgül, Fatih Irmak, Kübra Gültekin, Ekrem Muş, Ahmet Eker, Oğuzhan Ömer Demir, Yaşar Erjem, Hakan Hekim, Nurullah Altun, İsmail Dinçer Güneş, Nadir Koçak, İbrahim Meşe, Mehmet

- Arıcan, Ercan Sünger, Halil İbrahim Bahar, Mustafa Bülent Halıcıoğlu, Sevgi Güney, Salih Elmas, **Kriminoloji**. 1. bs. Ankara: Nobel Yayıncılık, 2016.
- Sözlük, Longman, <https://www.ldoceonline.com/dictionary/cyber> [Erişim Tarihi: 26.11.2018].
- Sözlük, Türkçe. <http://www.tdk.gov.tr/index.php> [Erişim tarihi: 20.10.2018].
- “Spam Nedir?”. <http://web.deu.edu.tr/sss/spam.html> [Erişim Tarihi: 20.11.2018].
- STAURA, John M., SALOAN John J. “Urban Stratification of Places, Routine Activities and Suburban Crime Rates” **Social Forces** c.4. (1988) ss.1102-1118
- Tadoğan, Uğur. “Savaşa hazır mıyız?”. <https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527> [Erişim Tarihi: 20.11.2018]
- Tanrıkulu, Cengiz, Eyüp Ayar, Leyla Ersun, Özgür Eralp, Servet Yetim, Cemal Gemci, Emrullah Aycı, Osman Günaydın, Çağatay Cengiz, Mehmet Ali Uzun, Neziha Çarkıt, Derya Orman, Mesut Budak, Nuran Görgün, Ayşen Merih Acar, Murat Turan, Özgür Sayar, Tekin Memiş, Osman Nihat Şen, Metin Özderin, Ersin Tufan Yalvaç, Çiğdem Çamurdan, Murat Soysal, Kemal Akgül. Türkiye Bilişim Derneği **"Bilişim Teknolojilerinin Kullanılmasının Hukuksal Boyutu."** Kamu Bilişim Platformu 9” Mayıs (2007).
- Turhan, Oğuz. **Bilgisayar Ağları İle İlgili Suçlar (Siber Suçlar)**, Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği Planlama Uzmanlığı Tezi, 2006.
- “Türk Ceza Kanunu (5237 S.K.)”. **Resmi Gazete**, 25611, Ekim 2004.
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. Ulusal Siber Güvenlik Stratejisi 2016-2019. Ankara, 2015.
- Ünal, Halime, Mustafa Orçan, Serdenger SEZER. “Kentlerde Tehlikeli Alanlar: Ankara ve Muğla Örneği” **Geleceğin Şehri Sempozyumu Bildiriler**, 24-25 Aralık 2014. İstanbul: Yıldız Teknik Üniversitesi, 2014: ss.325-340.
- Yeğren, Ceren. "Dijital aktivizmin bir türü olarak Hactivizm ve Redhack" **E-Journal of Intermedia** c.1. s.1 (2014) ss.118-132.
- Yıldız, SEVİL. **Suçta Araç Olarak İnternetin Teknik Ve Hukuki Yönden İncelenmesi**. (Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Anabilim Dalı Doktora Tezi, 2006).
- Yılmaz, Yunus. **"Siber Suç Korkusu ve Önlem Alma Stratejileri: Ankara'daki Teknokentler Örneği"**. Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı Yüksek Lisans Tezi. Ankara, 2018.
- Zipf, George Kinsley. **human behavior principle of least effort**, Massachusetts, 1948.

## **Ek 1. Anket Formu**

Princeton Survey Research Associates International for  
Pew Research Center's Internet, Science & Technology Project "Cybersecurity"  
Survey 2016  
Final Questionnaire  
3/30/2016

### **START TIMING MODULE**

#### **LANDLINE INTRO:**

Hello, I am \_\_\_\_\_ calling on behalf of the Pew Research Center. We are conducting a telephone opinion survey about some important issues facing this country today. I'd like to ask a few questions of the YOUNGEST **[RANDOMIZE: MALE / FEMALE]**, 18 years of age or older, who is now at home. **[IF NO MALE/FEMALE, ASK: May I please speak with the YOUNGEST (FEMALE/MALE), 18 years of age or older, who is now at home?]**

#### **GO TO MAIN INTERVIEW**

#### **CELL PHONE INTRO:**

Hello, I am \_\_\_\_\_ calling on behalf of the Pew Research Center. We are conducting a telephone opinion survey about some important issues facing this country today. I know I am calling you on a cell phone. If you would like to be reimbursed for your cell phone minutes, we will pay all eligible respondents \$5 for participating in this survey. This is NOT a sales call.

**[IF R SAYS DRIVING/UNABLE TO TAKE CALL:** Thank you. We will try you another time...]

**VOICEMAIL MESSAGE [LEAVE ONLY ONCE -- THE FIRST TIME A CALL GOES TO VOICEMAIL:]** I am calling on behalf of the Pew Research Center. We are conducting a national survey of cell phone users. This is NOT a sales call. We will try to reach you again.

**CELL PHONE SCREENING INTERVIEW:**

S1 Are you under 18 years old, OR are you 18 or older?

- 1 Under 18
- 2 18 or older
- 9 Don't know/Refused

**IF S1=2, CONTINUE WITH MAIN INTERVIEW**

**IF S1=1, THANK AND TERMINATE – RECORD AS AGE INELIGIBLE:**

This survey is limited to adults age 18 and over. I won't take any more of your time...

**IF S1=9, THANK AND TERMINATE – RECORD AS SCREENING**

**REFUSAL:** This survey is limited to adults age 18 and over. I won't take any more of your time...

**READ TO ALL CELL PHONE RESPONDENTS**

**INTRODUCTION TO MAIN INTERVIEW:** If you are now driving a car or doing any activity requiring your full attention, I need to call you back later. The first question is...

**INTERVIEWER:** If R says it is not a good time, try to arrange a time to call back. Offer the toll-free call-in number they can use to complete the survey before ending the conversation.

**[PROGRAMMER NOTE: PLEASE INCLUDE THE INTRODUCTION RANDOMIZATION VARIABLES IN THE ALL CONTACTS FILES. WE WOULD LIKE TO BE ABLE TO RUN RESPONSE RATES SEPARATELY FOR EACH VERSION OF THE INTRODUCTION FOR THE LANDLINE AND CELL FRAMES SEPARATELY. PLEASE RANDOMIZE INTRO LANGUAGE WITH ONE TREATMENT PER PHONE NUMBER NOT PER CALL.]**

**END TIMING MODULE**

## START TIMING MODULE

### ASK ALL:

Q1 Generally speaking, would you say that most people can be trusted or that you can't be too careful in dealing with people?

- 1 Most people can be trusted
- 2 You can't be too careful
- 3 (VOL.) It depends
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

[READ TO ALL:] On a different subject...

### ASK ALL:

EMINUSE Do you use the internet or email, at least occasionally? {PIAL Trend}

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

### ASK ALL:

INTMOB Do you access the internet on a cell phone, tablet or other mobile handheld device, at least occasionally? {PIAL Trend}

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

### ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):

INTFREQ About how often do you use the internet? [READ] {Libraries 2016}

- 1 Almost constantly

- 2 Several times a day
- 3 About once a day
- 4 Several times a week, OR
- 5 Less often?
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF LANDLINE SAMPLE (SAMPLE=1):**

DEVICE1a Next, do you have a cell phone, or not? {PIAL Trend}

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF HAVE CELL PHONE (DEVICE1a=1 or SAMPLE=2):**

SMART1 Some cell phones are called “smartphones” because of certain features they have. Is your cell phone a smartphone such as an iPhone, Android, Blackberry or Windows phone, or are you not sure? {PIAL Trend}

- 1 Yes, smartphone
- 2 No, not a smartphone
- 8 Not sure/Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

SNSINT2 Do you ever use a social media site or app like Facebook, Twitter or LinkedIn? {modified Educational Ecosystem 2015}

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**END TIMING MODULE**



## START TIMING MODULE

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

- ACCT1        Do you have **[INSERT ITEMS; RANDOMIZE; 'ANY OTHER ONLINE ACCOUNT' ALWAYS LAST]**, or not?
- a.        Any ONLINE accounts with your bank or financial services provider
  - b.        Any ONLINE accounts with your health care provider
  - c.        Any ONLINE accounts with a household utility provider, such as your gas, water, or electric company
  - d.        Any other online account that involves bill payments or transactions

### **CATEGORIES**

- 1        Yes
- 2        No
- 3        **(VOL.)** Does not apply/Don't have this account at all
- 8        **(VOL.)** Don't know
- 9        **(VOL.)** Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

- ACCT2        Have you ever chosen to NOT use or NOT create an account with an online service because you were worried about how your personal information would be handled?
- 1        Yes, have done this
  - 2        No, have not done this
  - 8        **(VOL.)** Don't know
  - 9        **(VOL.)** Refused

**ASK ALL:**

- ACCT3        Thinking about some of the companies and organizations that you interact with, how confident are you that they will keep your personal records safe from hackers or unauthorized users? **[FOR FIRST TWO RANDOMIZED ITEMS: Thinking about [INSERT ITEMS; RANDOMIZE; ALWAYS ASK**



**ITEMS a AND b TOGETHER AND IN ORDER]**, how confident are you that these records will be safe from hackers and unauthorized users?

How about...**[INSERT NEXT ITEM]**? **[READ FOR FIRST ITEM THEN AS NECESSARY:** Would you say you are very confident, somewhat confident, not too confident, or not at all confident that these records will be safe from hackers and unauthorized users?]

**ASK ITEM a AND b IF CELL PHONE USER (DEVICE1a=1 or SAMPLE=2):**

- a. The telephone company that provides your cell phone service
- b. The company that manufactured your cell phone

**ASK ITEM c IF INTERNET USER (EMINUSE=1 OR INTMOB=1):**

- c. Your email provider

**ASK ITEM d IF SOCIAL MEDIA USER (SNSINT2=1)**

- d. The social media sites you use
- e. The federal government
- f. Your credit card company
- g. The companies or retailers you do business with

#### **CATEGORIES**

- 1 Very confident
- 2 Somewhat confident
- 3 Not too confident
- 4 Not at all confident
- 5 **(VOL.)** Does not apply
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**END TIMING MODULE**

## GENERAL ATTITUDES/BEHAVIORS AND ONLINE ACCOUNTS

### START TIMING MODULE

#### ASK ALL:

SECUR1      In general, how secure do you feel your personal information is compared with five years ago? Do you think it is [READ] [RANDOMIZE 1-2]

- 1      More secure
- 2      Less secure
- 3      Or about as secure as it was five years ago?
- 8      (VOL.) Don't know
- 9      (VOL.) Refused

#### ASK ALL:

SECUR2      (To the best of your knowledge...) Have you ever...[INSERT ITEMS; RANDOMIZE; ASK ITEMS a AND b TOGETHER IN ORDER]?

- a.      Received a notice that your social security number had been compromised
- b.      Received a notice that other sensitive personal information, such as your account number, had been compromised
- c.      Noticed fraudulent charges on your debit or credit card

**ASK ITEM d IF INTERNET USER (EMINUSE=1 OR INTMOB=1):**

- d.      Had someone take over your email account without your permission

**ASK ITEM e IF SOCIAL MEDIA USER (SNSINT2=1):**

- e.      Had someone take over your social media account without your permission
- f.      Had someone attempt to open a line of credit or apply for a loan using your name
- g.      Had someone attempt to receive a tax refund using your name

### **CATEGORIES**

- 1 Yes
- 2 No
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

### **END TIMING MODULE**

### **PASSWORDS AND CYBER HABITS**

### **START TIMING MODULE**

**[READ TO ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):]** On a different subject...

### **ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS1 Thinking about your online activities, do you ever keep track of your passwords by...**[INSERT ITEMS; RANDOMIZE; ASK ITEMS c AND d TOGETHER IN ORDER; ‘SOME OTHER WAY’ ALWAYS LAST]?**  
How about by...**[INSERT NEXT ITEM]?** **[READ AS NECESSARY:** Do you ever keep track of your passwords in this way?]

- a. Memorizing them in your head
- b. Writing them down on a piece of paper
- c. Using a password management program such as Dashlane, Lastpass, or Apple Keychain
- d. Saving them in a note or document on your computer or mobile device
- e. Saving them in your internet browser
- f. Some other way that I haven't already mentioned (**SPECIFY**)

### **CATEGORIES**

- 1 Yes
- 2 No
- 8 **(VOL.)** Don't know

9 (VOL.) Refused

**ASK IF ANSWERED YES TO MORE THAN ONE ITEM IN HABITS1 LIST:**

HABITS2 Thinking about the different ways you keep track of your online passwords, which one do you use the MOST? Is it **[READ; ONLY INCLUDE “YES” RESPONSES FROM HABITS1; LIST RESPONSES IN SAME ORDER AS HABITS1]**?

- 1 Memorizing them in your head
- 2 Writing them down on a piece of paper
- 3 Using a password management program such as Dashlane, Lastpass, or Apple Keychain
- 4 Saving them in a note or document on your computer or mobile device
- 5 Saving them in your internet browser
- 6 Some other way
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS3 Thinking about all of the passwords you use to access your various online accounts, would you say that **[RANDOMIZE: (most of your passwords are the same or very similar to each other) or that (most of your passwords are very different from each other)]**?

- 1 Most passwords are the same or very similar
- 2 Most passwords are very different
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**[RANDOMIZE HABITS4A THRU HABITS4C]**

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS4A Do you ever have a hard time keeping track of your passwords, or is this not something that happens to you?

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS4B Do you ever worry about how secure your passwords are, or is this not something you worry about?

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS4C Do you ever use passwords that are less secure than you'd like because complicated passwords are too hard to remember, or is this not something you do?

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS5 Have you ever shared a password to one of your online accounts with a friend or family member?

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

HABITS6 Do you use two-factor or two-step authentication for any of your online accounts? **[IF RESPONDENT ASKS FOR DEFINITION OF “TWO FACTOR”:** Two-factor authentication is a feature where you are sent a one-time code via email, text message, or some other method that you would enter after first entering your username and password, and only works for a single login and for a limited amount of time.]

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF SOCIAL MEDIA USER (SNSINT2=1):**

HABITS7 Have you ever used your social media account information to log into another website, or have you never done this?

- 1 Yes, have done this
- 2 No, have never done this
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**END TIMING MODULE**

**START TIMING MODULE**

**[READ TO SMARTPHONE OWNER (SMART1=1):]** Now thinking specifically about your smartphone...

**ASK IF SMARTPHONE OWNER (SMART1=1):**

HABITS8 Do you have to use a code, password, or other security feature in order to access your phone?

- 1 Yes
- 2 No

- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF PHONE REQUIRES BYPASS CODE (HABITS8=1):**

HABITS9 What kind of security feature do you use to access your phone? Is it

**[READ]**

- 1 A PIN CODE containing only numbers
- 2 A PASSWORD containing numbers, letters, or symbols
- 3 A pattern of dots you connect with your finger
- 4 A thumbprint, OR
- 5 Some other kind of screen lock I haven't mentioned yet? (**SPECIFY**)
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF SMARTPHONE OWNER (SMART1=1):**

HABITS10 Thinking about the APPS on your smartphone, how frequently do you update them? Do you set them to update automatically, do you update them yourself as soon as you are notified that there is a new version available, do you update them yourself whenever it's convenient, or do you never update your apps?

- 1 Set them to update automatically
- 2 Update them yourself as soon as a new version is available
- 3 Update them yourself whenever it is convenient
- 4 Never install app updates
- 5 (VOL.) Different settings for different apps
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF SMARTPHONE OWNER (SMART1=1):**

HABITS11 And thinking about the OPERATING SYSTEM on your smartphone, how frequently do you update it? Do you usually update it as soon as you are

notified that a new version is available, do you update it whenever it's convenient, or do you never update your smartphone operating system?

- 1 Update as soon as new version is available
- 2 Wait until it is convenient
- 3 Never update operating system
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**ASK IF SMARTPHONE OWNER (SMART1=1):**

HABITS12 Have you installed any virus protection apps on your smartphone, or not?

- 1 Yes
- 2 No
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**END TIMING MODULE**

**START TIMING MODULE**

**[READ TO ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):]** On a different subject...

**ASK ALL INTERNET USERS (EMINUSE=1 OR INTMOB=1):**

WIFI1 Do you ever access public WiFi in places such as airports, cafes, hotels or libraries?

- 1 Yes
- 2 No
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**ASK IF EVER ACCESS PUBLIC WIFI (WIFI1=1):**

WIFI2 Do you ever **[INSERT ITEMS; RANDOMIZE]** while connected to public WiFi, or not?

- a. Make online purchases



- b. Do online banking or conduct other financial transactions

**ASK ITEM c IF SOCIAL MEDIA USER (SNSINT2=1):**

- c. Use social media
- d. Use email

**CATEGORIES**

- 1 Yes
- 2 No
- 3 **(VOL.)** Not applicable
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**END TIMING MODULE**

**CYBER POLICY**

**START TIMING MODULE**

**[READ TO ALL:]** Next...

**ASK ALL:**

**POLICY1** Many technology services use encryption of their customers' data and communications. Encryption prevents other people from accessing users' data without their permission, but can also prevent government law enforcement agencies from accessing that data during criminal investigations. Which one of the following statements comes closer to your view, even if neither is exactly right? **[READ AND RANDOMIZE]**

- 1 Technology companies should be able to use encryption technology that is unbreakable, even to law enforcement, OR
- 2 The government should be able to access encrypted communications when investigating crimes?
- 3 **(VOL.)** It depends
- 8 **(VOL.)** Don't know

9 (VOL.) Refused

**ASK ALL:**

POLICY2a How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on our public infrastructure, such as our air traffic control system or power grid? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

- 1 Definitely happen
- 2 Probably happen
- 3 Probably NOT happen
- 4 Definitely NOT happen
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL:**

POLICY2b How likely do you think it is that in the next five years, the United States will experience a significant cyberattack on the banking and financial system? Do you think this will definitely happen, probably happen, probably NOT happen, or definitely NOT happen in the next five years?

- 1 Definitely happen
- 2 Probably happen
- 3 Probably NOT happen
- 4 Definitely NOT happen
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL:**

POLICY3      How well-prepared do you think the U.S. government is to prevent  
cyberattacks on our public infrastructure? Is it **[READ]**

- 1      Very prepared
- 2      Somewhat prepared
- 3      Not too prepared, OR
- 4      Not at all prepared?
- 8      **(VOL.)** Don't know
- 9      **(VOL.)** Refused

**ASK ALL:**

POLICY4      How well-prepared do you think the U.S. government is to prevent  
cyberattacks on government agencies? Is it **[READ]**

- 1      Very prepared
- 2      Somewhat prepared
- 3      Not too prepared, OR
- 4      Not at all prepared?
- 8      **(VOL.)** Don't know
- 9      **(VOL.)** Refused

**ASK ALL:**

POLICY5      How well-prepared do you think U.S. BUSINESSES are to prevent  
cyberattacks on their own systems? Are they **[READ]**

- 1      Very prepared
- 2      Somewhat prepared
- 3      Not too prepared, OR
- 4      Not at all prepared?
- 8      **(VOL.)** Don't know
- 9      **(VOL.)** Refused

**ASK ALL:**

POLICY6      Thinking about some recent instances of cyberattacks, have you heard anything about **[INSERT ITEMS; RANDOMIZE]**, or is this not something you have heard of? **[IF YES, ASK:** Have you heard a lot about this, or a little about it?]

Next, have you heard anything about...**[INSERT NEXT ITEM]**? **[IF YES, ASK:** Have you heard a lot about this, or a little about it?]

- a.      The publication of company emails at the Sony Corporation
- b.      The exposure of government security clearance information at the Office of Personnel Management
- c.      The exposure of credit card data of customers who shopped at Target stores
- d.      The disruption of the power grid in Ukraine
- e.      The publishing of the identities of AshleyMadison.com customers

**CATEGORIES**

- 1      Yes, have heard a lot
- 2      Yes, have heard a little
- 3      No, have not heard of this
- 8      **(VOL.)** Don't know
- 9      **(VOL.)** Refused

**END TIMING MODULE**

**START TIMING MODULE**

**[READ TO ALL:]** Now, just a few questions for statistical purposes only.

**ASK ALL:**

**SEX    RECORD RESPONDENT SEX [DO NOT ASK]**

- 1      Male
- 2      Female

**ASK ALL:**

**AGE    What is your age?**

\_\_\_\_\_ years **[RECORD EXACT AGE 18-96]**

97 97 or older

98 Don't know

99 Refused

**ASK ALL:**

EDUC2 What is the highest level of school you have completed or the highest degree you have received? **[DO NOT READ] [INTERVIEWER NOTE: Enter code 3-HS grad if R completed training that did NOT count toward a degree]**

- 1 Less than high school (Grades 1-8 or no formal schooling)
- 2 High school incomplete (Grades 9-11 or Grade 12 with NO diploma)
- 3 High school graduate (Grade 12 with diploma or GED certificate)
- 4 Some college, no degree (includes some community college)
- 5 Two year associate degree from a college or university
- 6 Four year college or university degree/Bachelor's degree (e.g., BS, BA, AB)
- 7 Some postgraduate or professional schooling, no postgraduate degree (e.g. some graduate school)
- 8 Postgraduate or professional degree, including master's, doctorate, medical or law degree (e.g., MA, MS, PhD, MD, JD)
- 98 Don't know
- 99 Refused

**[MAKE FULL NOTE AVAILABLE FOR INTERVIEWERS: Enter code 3-HS graduate if R completed vocational, business, technical, or training courses after high school that did NOT count toward an associate degree from a college, community college or university (e.g., training for a certificate or an apprenticeship)]**

**ASK ALL:**

HISP Are you of Hispanic, Latino, or Spanish origin, such as Mexican, Puerto Rican or Cuban? {QID:hisp4} {first asked in Educational Ecosystem 2015}

- 1 Yes
- 2 No
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL:**

RACE Which of the following describes your race? You can select as many as apply.  
White, Black or African American, Asian or Asian American or some other race.  
**[RECORD UP TO FOUR IN ORDER MENTIONED BUT DO NOT PROBE FOR ADDITIONAL] [IF R VOLS MIXED BIRACIAL, PROBE ONCE: What race or races is that?]** {QID:race3} {first asked in Educational Ecosystem 2015}

- 1 White (e.g., Caucasian, European, Irish, Italian, Arab, Middle Eastern)
- 2 Black or African-American (e.g., Negro, Kenyan, Nigerian, Haitian)
- 3 Asian or Asian-American (e.g., Asian Indian, Chinese, Filipino, Vietnamese or other Asian origin groups)
- 4 Some other race (**SPECIFY**) [**IF NEEDED: What race or races is that?**]
- 5 (VOL.) Native American/American Indian/Alaska Native
- 6 (VOL.) Pacific Islander/Native Hawaiian
- 7 (VOL.) Hispanic/Latino (e.g., Mexican, Puerto Rican, Cuban)
- 8 (VOL.) Don't know
- 9 (VOL.) Refused (e.g., non-race answers like American, Human, purple)

**ASK IF HISPANIC (HISP=1 OR RACE=7):**

BIRTH\_HISP Were you born in the United States, on the island of Puerto Rico, or in another country? {QID:birth\_hisp2} {first asked with this modified filter in Educational Ecosystem 2015}

- 1 U.S.

- 2 Puerto Rico
- 3 Another country
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**ASK ALL:**

**MARITAL** Are you currently married, living with a partner, divorced, separated, widowed, or have you never been married? **[IF R SAYS “SINGLE” PROBE TO DETERMINE APPROPRIATE CATEGORY]**

- 1 Married
- 2 Living with a partner
- 3 Divorced
- 4 Separated
- 5 Widowed
- 6 Never been married
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**ASK ALL:**

**PAR** Are you the parent or guardian of any children under age 18 now living in your household?

- 1 Yes
- 2 No
- 8 **(VOL.)** Don't know
- 9 **(VOL.)** Refused

**ASK ALL:**

**EMPLNW3** Are you now employed full-time, part-time, or are you not employed for pay? {Educational Ecosystem 2015}

- 1 Employed full-time
- 2 Employed part-time

- 3 Not employed for pay
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL**

PARTY In politics TODAY, do you consider yourself a Republican, Democrat, or independent?

- 1 Republican
- 2 Democrat
- 3 Independent
- 4 (VOL.) No preference
- 5 (VOL.) Other party
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK IF INDEP/NO PREF/OTHER/DK/REF (PARTY=3,4,5,8,9):**

PARTYLN As of today, do you lean more to the Republican Party or more to the Democratic Party?

- 1 Republican
- 2 Democrat
- 8 (VOL.) Don't know
- 9 (VOL.) Refused

**ASK ALL**

IDEO In general, would you describe your political views as... **[READ]**

- 1 Very conservative
- 2 Conservative
- 3 Moderate
- 4 Liberal, OR
- 5 Very liberal?
- 8 (VOL.) Don't know



9 (VOL.) Refused

**ASK ALL:**

INC Last year -- that is in 2015 -- what was your total family income from all sources, before taxes? Just stop me when I get to the right category... **[READ]** {Master INC2}

- 1 Less than \$10,000
- 2 10 to under \$20,000
- 3 20 to under \$30,000
- 4 30 to under \$40,000
- 5 40 to under \$50,000
- 6 50 to under \$75,000
- 7 75 to under \$100,000
- 8 100 to under \$150,000, OR
- 9 \$150,000 or more?
- 98 (VOL.) Don't know
- 99 (VOL.) Refused

**ASK ALL:**

HH1 How many people, including yourself, live in your household?

**INTERVIEWER NOTE: HOUSEHOLD MEMBERS INCLUDE PEOPLE WHO THINK OF THIS HOUSEHOLD AS THEIR PRIMARY PLACE OF RESIDENCE, INCLUDING THOSE WHO ARE TEMPORARILY AWAY ON BUSINESS, VACATION, IN A HOSPITAL, OR AWAY AT SCHOOL. THIS INCLUDES INFANTS, CHILDREN AND ADULTS.** {QID:hh1} {first asked in Educational Ecosystem 2015}

— **[ENTER EXACT NUMBER 1-7]**

- 8 8 or more
- 98 (VOL.) Don't know
- 99 (VOL.) Refused

**ASK IF MORE THAN ONE PERSON IN HH (HH1>1):**

HH3 How many, including yourself, are adults, age 18 and older? {QID:hh3} {first asked in Educational Ecosystem 2015}

\_\_\_ [ENTER EXACT NUMBER 1-7]

8 8 or more

98 (VOL.) Don't know

99 (VOL.) Refused

[PROGRAMMER: HH3 SHOULD NOT EXCEED HH1 RESPONSE]

**END TIMING MODULE**

**START TIMING MODULE**

[READ IF (DEVICE1a=2,8,9 AND HH1>1) OR SAMPLE=2:] Thinking about your telephone use...

**ASK IF NO CELL PHONE AND MULTI-PERSON HOUSEHOLD**

(DEVICE1a=2,8,9 AND HH1>1)

QL1a Does anyone in your household have a working cell phone? {PIAL trend; QL1HH}

1 Yes

2 No

8 (VOL.) Don't know

9 (VOL.) Refused

**ASK ALL CELL PHONE SAMPLE (SAMPLE=2):**

QC1 Is there at least one telephone INSIDE your home that is currently working and is not a cell phone?

1 Yes, home telephone

2 No home telephone

8 (VOL.) Don't know

9 (VOL.) Refused

## END TIMING MODULE

## START TIMING MODULE

### ASK ALL:

RZIPCODE What is your zip code? [INTERVIEWER NOTE: Must **VERIFY** the zip code given before moving on]

[IF DK/REFUSED, PROBE ONCE: This question helps us to accurately determine what part of the country people who complete the survey live in and is used only for classification purposes. You cannot be contacted based on this information. Can you please tell me your ZIP code?]

\_\_\_\_\_ [ENTER 5-DIGIT ZIPCODE – **VERIFY**] [PROGRAMMER: **HIGHLIGHT THE WORD “VERIFY”**]

99999 Don't know/Refused

## END TIMING MODULE

## START TIMING MODULE

### ASK CELL PHONE SAMPLE ONLY:

MONEY5 That's the end of the interview. If you would like to be reimbursed for your cell phone minutes, we can send you \$5. I will need your full name and a mailing address where we can send you the money.

[INTERVIEWER NOTE: If R does not want to give full name, explain we only need it to send the \$5 out to them personally.]

1 [ENTER FULL NAME] – INTERVIEWER: PLEASE **VERIFY** SPELLING

2 [ENTER MAILING ADDRESS]

3 [CITY] – INTERVIEWER: PLEASE **VERIFY** SPELLING

4 [STATE]

5 [CONFIRM ZIP CODE]

9 Respondent does not want the money (VOL.)

## END TIMING MODULE

## START TIMING MODULE

**THANK RESPONDENT:** Thank you very much for your time. This survey is being conducted by the Pew Research Center, which will be issuing a report on the results of this survey on their website, pewresearch dot ORG, in the coming weeks.

**THANK YOU** again for your help! Have a nice (day/evening).

**END TIMING MODULE**

**INTERVIEWER: I HEREBY ATTEST THAT THIS IS A TRUE AND HONEST INTERVIEW.**

**INTERVIEWER GENDER:**

ISEX {QID:isex}

- 1 Male
- 2 Female

**INTERVIEWER RACE/ETHNICITY:**

IHISP1 Are you, yourself, of Hispanic origin or descent, such as Mexican, Puerto Rican, Cuban, or some other Spanish background? {QID:ihisp1}

- 1 Yes
- 2 No
- 9 Don't know/Refused (**VOL.**)

IRACE1 Which of the following describes your race? You can select as many as apply. [**READ LIST; RECORD UP TO FOUR RESPONSES IN ORDER MENTIONED**] {QID:irace1}

- 1 White
- 2 Black or African-American
- 3 Asian or Asian-American
- 4 Or some other race
- 9 Don't know/Refused (**VOL.**)

**[PLEASE MAKE THE FOLLOWING TEXT AVAILABLE TO INTERVIEWERS  
ANYTIME A RESPONDENT ASKS ABOUT THE NATURE OF THE PEW  
RESEARCH CENTER:]**

The Pew Research Center is an independent nonpartisan public opinion research organization that studies attitudes toward politics, the press and issues facing the nation. The Center has no connection to the government, political parties, or any campaigns. Reports about its surveys are made available free of charge on their website [pewresearch dot ORG](http://pewresearch.org).

## Ek 2. Anket Verilerinin Kullanılabilmesi İçin İzin Belgesi.

Çalışmada siber suçların incelenebilmesi maksadıyla kullanılan veriler ABD merkezli Pew Research Center isimli şirkete aittir söz konusu verilerin kullanılabilmesi için aşağıda gösterilen elektronik posta yazar tarafından Pew Research Center’a gönderilmiştir.

*“Hi. If possible I want to make a research about cyber crimes by using your "March 30- May 3, - cybersucurity" data set so I need a permission for this research. Thanks.”*  
(Merhaba, mümkünse şirketinize ait 30 Mart-3 Mayıs- Cybersecurity isimli veri setini kullanarak siber suçlarla ilgili bir çalışma yapmak istiyorum bunun için izninize ihtiyacım var.)

Yazarın elektronik postasına Pew Research Center tarafından verilen yanıt ise aşağıdaki gibidir.

*“Hi Ferhat, Thank you for reaching out. You do not need express permission for this, so feel free to use our datasets.”* (Merhaba Ferhat. Bize ulaştığınız için teşekkür ederiz. Çalışman için bizden izin almana gerek yok verilerimizi istediğin gibi kullanabilirsin.)

Söz konusu elektronik postalara ait ekran resimleri aşağıda gösterilmiştir.



Ferhat Birceviz <ferhat.birceviz@gmail.com>

### Permission request for research.

2 ileti

Ferhat Birceviz <ferhat.birceviz@gmail.com>  
Alıcı: info@pewresearch.org

23 Aralık 2018 22:27

Hi. If possible I want to make a research about cyber crimes by using your "March 30-May 3, - cybersucurity" data set so I need a permission for this research. Thanks.



Virüs bulunmuyor. [www.avast.com](http://www.avast.com)

Pew Research Center <info@pewresearch.org>  
Alıcı: Ferhat Birceviz <ferhat.birceviz@gmail.com>

27 Aralık 2018 02:53

Hi Ferhat,

Thank you for reaching out. You do not need express permission for this, so feel free to use our datasets. Our use policy is available here: <http://www.pewresearch.org/terms-and-conditions/>.

Best,  
Hannah Tiner  
Pew Research Center

From: Ferhat Birceviz <ferhat.birceviz@gmail.com>  
Sent: Sunday, December 23, 2018 2:27:02 PM  
To: Pew Research Center  
Subject: Permission request for research.

## ÖZGEÇMİŞ

Ferhat BİRCEVİZ 1 Temmuz 1984'te Mersin' de doğmuş, ilk ve orta öğrenimini Silifke ilçesinde tamamlamış, 2002 yılında Bursa Işıklar Askeri Lisesi'nden, 2006 yılında, Ankara Kara Harp Okulun'dan, 2013 yılında Eskişehir Üniversitesi adalet meslek yüksekokulundan mezun olmuştur. Halen Maltepe Üniversitesi Hukuk Fakültesi öğrencisidir. Kara Harp Okulu Mezuniyetine müteakip Türk silahlı kuvvetlerinin çeşitli birliklerinde takım ve batarya komutanlığı görevlerinde bulunmuş olup yüzbaşı rütbesi ile Kara Kuvvetleri Komutanlığı Personel Başkanlığında görevine devam etmektedir. Okumayı, üretmeyi, yeni yerler keşfetmeyi seven ve iyi seviyede İngilizce bilen yazar, Sengül BİRCEVİZ ile evli ve bir çocuk babasıdır.

