Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Sosyoloji Anabilim Dalı

SİBER SUÇ KORKUSU VE ÖNLEM ALMA STRATEJİLERİ: ANKARA'DAKİ TEKNOKENTLER ÖRNEĞİ

Yunus YILMAZ

Yüksek Lisans Tezi

Ankara, 2018

SİBER SUÇ KORKUSU VE ÖNLEM ALMA STRATEJİLERİ:

ANKARA'DAKİ TEKNOKENTLER ÖRNEĞİ

Yunus YILMAZ

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Sosyoloji Anabilim Dalı

Yüksek Lisans Tezi

Ankara, 2018

KABUL VE ONAY

Yunus YILMAZ tarafından hazırlanan "Siber Suç Korkusu ve Önlem Alma Stratejileri: Ankara'daki Teknokentler Örneği" başlıklı bu çalışma, 12.06.2018 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Yüksek Lisans Tezi olarak kabul edilmiştir.

Doç. Dr. Rahşan BALAMİR BEKTAŞ (Başkan)

Doç. Dr. Birsen ŞAHİN KÜTÜK

Doç. Dr. Ayça GELGEÇ BAKACAK (Danışman)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Musa Yaşar SAĞLAM

Enstitü Müdürü

BİLDİRİM

Hazırladığım tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kağıt ve elektronik kopyalarının Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım:

☐ Tezimin/Raporumun tamamı her yerden erişime açılabilir.

☐ Tezim/Raporum sadece Hacettepe Üniversitesi yerleşkelerinden erişime açılabilir.

☒ Tezimin/Raporumun …3… yıl süreyle erişime açılmasını istemiyorum. Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir.

12.06.2018

Yunus YILMAZ

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinlerin yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

o**Tezimin/Raporumun tamamı dünya çapında erişime açılabilir ve bir kısmı veya tamamının fotokopisi alınabilir.**
(Bu seçenekle teziniz arama motorlarında indekslenebilecek, daha sonra tezinizin erişim statüsünün değiştirilmesini talep etseniz ve kütüphane bu talebinizi yerine getirse bile, teziniz arama motorlarının önbelleklerinde kalmaya devam edebilecektir)

●**Tezimin/Raporumun .....12/06/2021.....tarihine kadar erişime açılmasını ve fotokopi alınmasını (İç Kapak, Özet, İçindekiler ve Kaynakça hariç) istemiyorum.**
(Bu sürenin sonunda uzatma için başvuruda bulunmadığım takdirde, tezimin/raporumun tamamı her yerden erişime açılabilir, kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisi alınabilir)

o**Tezimin/Raporumun.....tarihine kadar erişime açılmasını istemiyorum ancak kaynak gösterilmek şartıyla bir kısmı veya tamamının fotokopisinin alınmasını onaylıyorum.**

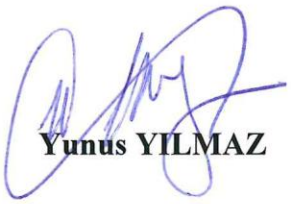
o **Serbest Seçenek/Yazarın Seçimi**

12/06/2018

Yunus YILMAZ

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, Doç. Dr. Ayça GELGEÇ BAKACAK danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.



Yunus YILMAZ

Sevgili eşim Öznurum’a…

TEŞEKKÜR

Öncelikle bu çalışmayla ilgili her türlü konuda her zaman kendisine rahatlıkla danışabildiğim ve kendisinden yardım alabildiğim değerli danışmanım Doç. Dr. Ayça GELGEÇ BAKACAK'a, çalışmamın özellikle veri analizi kısmında önemli destekleri olan ve jürimde bulunan Doç. Dr. Birsen ŞAHİN KÜTÜK'e, jürimdeki yapıcı eleştirileri ile çalışmama katkıda bulunan Doç. Dr. Rahşan BALAMİR BEKTAŞ'a ve yüksek lisans öğrenimim süresince kendilerinden çokça istifade ettiğim Prof. Dr. Esra BURCU SAĞLAM, Doç. Dr. Abdülkerim SÖNMEZ, Doç. Dr. Tuğça POYRAZ TACOĞLU ve Hacettepe Üniversitesi Sosyoloji Bölümünün çok değerli hocalarına teşekkürü bir borç bilirim.

Bu çalışmanın başından sonuna her anında sabrıyla, özverisiyle, güler yüzüyle ve tüm içtenliğiyle bana destek olan ve çalışmamı kolaylaştıran sevgili eşim Öznur AKCALI YILMAZ'a minnettarım. Hayatıma kattığı neşe, mutluluk ve renk için ne kadar teşekkür etsem azdır.

Yine maddi ve manevi desteklerini hiçbir zaman üzerimden eksik etmeyen anneme, babama, kardeşime ve ablama müteşekkirim. İyi ki varsınız.

Özellikle Sosyoloji alanına yönelmeye beraber karar verdiğimiz, her türlü konuya birlikte kafa yorduğumuz, en zor zamanlarında bile bana destek olmaya devam eden ve bu tezi tamamlayabilmem konusunda beni teşvik eden çok kıymetli dostum İsmail SİZER'e ve değerli eşi Merve'ye şükranlarımı sunarım.

Son olarak ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark'ta çalışan ve çok değerli zamanlarını ayırarak bu çalışmada yer alan tüm katılımcıları bilimsel bilginin gelişimine olan inançlarından dolayı tebrik eder ve kendilerine teşekkürlerimi sunarım.

ÖZET

YILMAZ, Yunus. *Siber Suç Korkusu ve Önlem Alma Stratejileri: Ankara'daki Teknokentler Örneği*, Yüksek Lisans Tezi, Ankara, 2018.

Siber suçlar günümüzün gelişen bilim ve teknoloji dünyasında giderek daha da yaygınlaşmakta ve yalnızca bireyler için değil topluluklar, kuruluşlar ve devletler için dahi ciddi tehditler oluşturabilecek en önemli konulardan biri haline gelmektedir. Bireylerden gruplara, örgütlerden devletlere kadar toplumun hemen her kesimini etkileyen bu denli ciddi bir tehdit karşısında bireylerin korku duymaları ve önlem alabilmek için belirli stratejiler geliştirmeleri de son derece doğal ve olasıdır. Bu bağlamda bu çalışmada siber suç korkusu ve önlem alma stratejileri ele alınmaktadır. Çalışmada Ankara'da bulunan 4 adet Teknokent'in (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışanları ile anket uygulaması gerçekleştirilmiştir. Yapılan anket sonucunda ulaşılan nicel veriler SPSS paket programı kullanılarak analiz edilmiş ve hipotezler test edilmiştir. Çalışma sonucunda Ankara'daki Teknokent çalışanları üzerinde siber suç korkusu bulunduğu ve katılımcıların çoğunluğunun orta ve üst düzeyde önlem alma stratejileri geliştirdikleri görülmüştür. Çalışmada ayrıca belirli siber suç türleri açısından korku ile katılımcıların cinsiyetleri, eğitim durumları, geçmiş siber suç mağduriyetleri, aldıkları önlemleri yeterli bulmaları ve siber suçlara ilişkin yasal düzenlemeler, kolluk ve yargı birimlerine ilişkin algıları arasında anlamlı bir ilişki bulunduğu görülmüştür. Yine çalışmada katılımcıların iş yerlerinde ve dışında kullandıkları elektronik cihazlarındaki bazı önlem alma stratejileri arasında da anlamlı bir ilişki bulunduğu sonucuna ulaşılmıştır.

Anahtar Sözcükler

Siber Suç Korkusu, Siber Suçlar, Suç Korkusu, Teknokentler, Siber Güvenlik

ABSTRACT

YILMAZ, Yunus. *Fear of Cybercrime and Precaution Taking Strategies: The Sample of Technoparks in Ankara*, Masters Thesis, Ankara, 2018.

Cybercrimes are becoming increasingly widespread in today's emerging science and technology world and are becoming one of the most important issues that may pose serious threats not only to individuals but also to communities, organizations and states. In the face of such a serious threat affecting almost every segment of society, from individuals to groups and from organizations to governments, it is also natural and possible for individuals to be afraid and develop certain strategies to take precautions. In this context, this study focuses on fear of cybercrime and precaution taking strategies. At the study, a survey was conducted with the employees of four Teknoparks (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent and Gazi Technopark) located in Ankara, Turkey. Quantitative data obtained at the survey were analyzed using SPSS package program and hypotheses were tested. At the end of the study, it is reached that there is a fear of cybercrime on Teknopark employees in Ankara and majority of the participants developed middle and upper level precaution taking strategies. At the study a significant relationship is found between fear of certain types of cybercrime and the participants' gender, educational status, previous cybercrime victimization, finding the precautions taken enough and perceptions about legal regulations, law enforcement and judicial units related to cybercrimes. It is also concluded at the study that there is a significant relationship between the participants' some precaution taking strategies in the electronic devices they used at work and out of work.

Keywords

Fear of Cybercrime, Cybercrimes, Fear of Crime, Technoparks, Cyber Security

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

GRAFİKLER DİZİNİ

GİRİŞ

Her ne kadar teknolojinin ve internetin bireylerin günlük yaşantılarına dahil olması insanlık tarihiyle kıyaslandığında çok yeni sayılabilecek bir zamana denk gelse de teknolojik gelişmeler baş döndürücü bir hızla ilerlemiş ve günümüzde geldiğimiz noktada teknolojinin nimetleri bireylerin hayatlarının hemen her alanında vazgeçilmez bir yer edinmeyi başarmıştır. Bilgisayarlar, cep telefonları, tabletler, akıllı eşyalar vb. pek çok bilişim sisteminin günümüzde bireylerin günlük hayatlarını ciddi anlamda kolaylaştırması, onları günlük hayatın ayrılmaz bir parçası haline getirmiştir. Bireylerin sabahleyin kendilerini uyandıran cep telefonu alarmlarından gün içerisinde kullandıkları akıllı eşyalara, bilgisayarlarından gece yatarken kitap okudukları tabletlerine kadar hemen her şeyin bilişim ve internet tabanlı olması bireylerin çepeçevre teknolojiyle sarılmalarına neden olmuştur.

Teknolojik gelişmelerin bireylerin günlük hayatlarının bu denli içerisine girmesi bireylerin geleneksel sosyalleşme alanlarını da önemli ölçüde değiştirmiştir. Daha önceleri evlerde, işyerlerinde, okullarda, sokaklarda, caddelerde, toplu taşıma araçlarında, kafelerde vb. yerlerde yüz yüze etkileşim şeklinde gerçekleşen sosyalleşmeler, özellikle internetin ve Facebook, Twitter, Instagram vb. sosyal medya ortamlarının yaygınlaşmasıyla birlikte yerini siber dünyada gerçekleşen ve geleneksel anlamda yüz yüze olmayan sosyalleşmelere bırakmıştır. Siber dünyanın bireylerin ve toplumların etkileşimi için gerçek dünyadan ayrı bir alan olarak ortaya çıkması bireyleri artık yalnızca gerçek dünyanın değil siber dünyanın da birer aktörü haline getirmiştir.

Siber dünya insan hayatını kolaylaştıran pek çok olanağı içinde barındırmakla birlikte bireylerin zarar görmelerine neden olabilecek bir ortam olma özelliğini de bünyesinde taşımaktadır. Bireylerin siber dünyada zarar görmelerine neden olabilecek en önemli konulardan birini de siber suçlar oluşturmaktadır. Bireylerin günlük hayatlarında karşılaşmış oldukları birçok suç türü teknolojinin ve internetin bireylerin hayatlarına girmesiyle birlikte siber dünyaya taşınmış, bunun yanında siber dünyanın olanaklarından faydalanan pek çok yeni suç türü de gelişerek siber dünyada işlenen suçlar çeşitlenmiş ve karmaşıklaşmıştır. Günümüzde artık sadece gerçek dünyanın değil, siber dünyanın da birer aktörü haline gelen bireyler gerçek dünyada karşılaştıkları suçlara paralel olarak,

siber dünyada da çok daha ciddi ve tehlikeli olabilen siber suçlarla karşı karşıya bulunmaktadırlar. Siber dünyada kendisini geliştirmiş ve uzmanlaşmış olan suçlular arkalarında neredeyse hiçbir iz bırakmadan bireyler, gruplar, topluluklar ve devletler için geleneksel suçlulardan daha büyük çaplı mağduriyetler oluşturabilmektedirler. Dolayısıyla günlük yaşamlarında bütün bu sayılan siber suçlar ve tehditlerle bir arada ve iç içe yaşayan bireylerin de en az herhangi bir suçtan mağdur olma korkusu yaşamaları kadar siber suçlardan mağdur olma korkusu yaşamaları da muhtemeldir. Nitekim ABD'de IBM tarafından yapılan bir araştırmada katılımcılar siber suçlardan mağdur olma olasılıklarını fiziksel suçlardan mağdur olmaya göre üç kat daha fazla görmüşlerdir (IBM, 2006). Ayrıca ABD'de yapılan diğer bir araştırmada Amerikalıların en fazla korku duymakta oldukları suçun hackerlar tarafından kredi kartı bilgilerinin çalınması olduğu ortaya çıkmıştır (Stuart, 2014). Yine ABD'de yapılan başka bir araştırmada ise katılımcıların %66'sı geçen yıla göre siber suçlardan daha fazla korkmakta olduklarını belirtmişlerdir (GFI, 2015).

Uluslararası alandaki bu örneklerle birlikte Türkiye'de ise bireyler üzerindeki siber suç korkusuna ilişkin literatürde önemli bir eksiklik olduğu görülmektedir. Bu bağlamda bu çalışma Ankara'daki teknokentler örneği üzerinden siber suç korkusunu ve önlem alma stratejilerini incelemekte olup, toplamda beş bölümden oluşmaktadır. İlk bölümde araştırmanın konusu, amacı, önemi, yöntemi ve sınırlılıklarına yer verilmekte olup, ikinci bölüm araştırmanın kavramsal çerçevesinin ele alındığı bölüm, üçüncü bölüm araştırmanın kuramsal çerçevesinin ele alındığı bölüm, dördüncü bölüm araştırmada toplanan verilerin analizine yer verilen bölüm ve beşinci bölüm ise tüm bu analizler kavramsal ve kuramsal çerçeve ışığında araştırma konusunun ele alındığı sonuç ve değerlendirme bölümüdür.

1. BÖLÜM ARAŞTIRMANIN KAPSAMI VE YÖNTEMİ

1.1. ARAŞTIRMANIN KONUSU, AMACI VE ÖNEMİ

1.1.1. Araştırmanın Konusu

Siber suç korkusu konusu ile ilgili olarak ulusal ve uluslararası literatür incelendiğinde öncelikle ulusal literatürde bu konuda yapılmış olan çalışma sayısının yok denecek kadar az olduğu belirtilmelidir. Bununla birlikte bu araştırmanın konusu ile de bağlantılı olabilecek türdeki birkaç çalışmaya burada değinilmiştir.

Literatüre bakıldığında Türkiye'de genel olarak suç korkusu üzerine yapılmış bazı çalışmalar bulunduğu görülmektedir (Çardak, 2011; Çetin, 2010; Gaziarifoğlu, 2009; Gökulu, 2011; Karakaya, 2015; Kosukoğlu, 2011; Kul, 2009; Öztürk, 2015). Bu çalışmalarda genel olarak kentlerde yaşayan kadınların suç mağduru olma korkusu (Çardak, 2011), suç mağduriyeti korkusu ve algılanan suç mağduriyeti riski ilişkisi (Gaziarifoğlu, 2009; Gökulu, 2011), orta sınıfa mensup bireylerde suç korkusu (Kosukoğlu, 2011), liseli gençlerde suç mağduru olma korkusu (Karakaya, 2015) ve suç korkusu ile yaşam memnuniyeti ilişkisi (Öztürk, 2015) gibi konular araştırılmıştır.

Aynı şekilde siber gözetim konusu da Türkiye'de suç korkusuna nazaran daha az olmakla birlikte literatürde kendisine yer bulabilmiştir (Akgüç, 2004; Aslanyürek, 2015; Karslıoğlu, 2014). Bu çalışmalar arasında Akgüç (2004) elektronik gözetim ve denetimi bireylerin mahremiyeti açısından ele almış, Karslıoğlu (2014) hukuksal bir perspektifle siber gözetim ve bir toplumsal denetim aracı olarak internetin dönüşümünü incelemiş ve Aslanyürek (2015) ise internet güvenliği ve çevrimiçi gizlilik alanlarında yaşanan sorunları araştırmıştır.

Bununla birlikte her ne kadar suç korkusu üzerine yapılmış olan çalışmalar ile siber suç korkusu arasında belirli oranda bir ilişki kurulabilecek olsa da, Türkiye'de yapılmış olan suç korkusu ve siber gözetim konulu çalışmaların neredeyse hiçbirisinin siber suç korkusu konusuna odaklanmadıkları belirtilmelidir.

Bu çalışmada rastlanılan ve ulusal literatür içerisinde siber suç korkusu konulu olduğu söylenebilecek tek çalışma Erdal Servet YURTSAL tarafından yapılmış olan ve 2016 yılı Kasım ayında Güvenlik Bilimleri Dergisinde yayınlanan "Fear of Crime in Social Networks: Facebook Example (Sosyal Ağlarda Suç Korkusu: Facebook Örneği)" başlıklı makaledir. Yurtsal (2016) yapmış olduğu çalışmada 141 kişi üzerinde uygulamış olduğu anket çalışması ile sosyal paylaşım sitesi Facebook örneği üzerinden suç korkusunu ölçmeyi amaçlamıştır. Yurtsal (2016) çalışmasının sonucunda geçmişte bilişim suçlarından mağdur olmuş kişilerin daha fazla suç korkusuna sahip olduklarını; daha önceki çalışmaların aksine, cinsiyet ve suç korkusu arasında anlamlı bir ilişki görülemediğini ve Facebook üyelik süresi ve günlük Facebook kullanım sıklığı arasında da anlamlı bir ilişki bulunamadığını belirtmektedir. Dolayısıyla bu çalışmanın oldukça spesifik bir konu üzerinden siber suç korkusuna odaklanmakta olduğu görülmektedir.

Siber suç korkusu konusuna ilişkin uluslararası literatür incelendiğinde ise öncelikle literatürün Türkiye'dekine nazaran oldukça gelişmiş olduğu ve çok sayıda çalışma içerdiği belirtilmelidir (Abdulai, 2016; Alshalan, 2006; Bernik, Dobovšek, & Markelj, 2013; Boss, Kirsch, Angermeier, & Boss, 2009; Furedi, 2006; Henson, 2011; Higgins, Ricketts, & Vegh, 2008; Meško & Bernik, 2011; Ohm, 2007; Radda & Ndubueze, 2013; Roberts, Indermaur, & Spiranovic, 2013; Wall, 2008a, 2008b; Yu, 2014). Bu çalışmalar özellikle Amerika Birleşik Devletleri (ABD) ve Avrupa merkezli olarak yoğunlaşmakta olup, büyük bir bölümü itibarıyla doğrudan siber suç korkusu konusuna odaklanmakla birlikte kendi içlerinde bir sınıflandırmaya tabi tutulabileceklerdir. Bu anlamda bu çalışmaların bir kısmı çeşitli spesifik ya da genel siber suçlar üzerinden siber suç korkusu ve mağduriyet gibi konulara yoğunlaşmakta (Alshalan, 2006; Roberts vd., 2013), bir kısmı üniversite öğrencileri üzerinde yapılan çalışmalardan hareketle siber suç korkusunu, belirleyicilerini vb. incelemekte (Abdulai, 2016; Henson, 2011; Higgins vd., 2008; Radda & Ndubueze, 2013; Yu, 2014), bir kısmı özellikle farkındalık ve bilgi düzeyi ile siber suç korkusu arasındaki ilişkiye odaklanmakta (Bernik vd., 2013; Meško & Bernik, 2011), bir kısmı çeşitli mitolojik yaklaşımlar ve toplumdaki yaygın endişeler üzerinden korkunun oluşum sürecine odaklanmakta (Furedi, 2006; Ohm, 2007; Wall, 2008a), bir kısmı da medyanın siber suçlara ilişkin toplumsal algıları nasıl şekillendirdiğine değinmektedir (Wall, 2008b).

Siber suç korkusu ve mağduriyeti konularına odaklanan ve alandaki ilk çalışmalardan olan Alshalan (2006)'ın çalışması ABD'de internet kullanıcıları arasındaki siber suç mağduriyetini bilgisayar virüsü ile siber suç mağduriyetini etkileyen faktörlerin değerlendirilmesi ve siber suç korkusunun tahmin edilmesi üzerinden araştırmaktadır. Alshalan (2006) yapmış olduğu çalışma neticesinde, Rutin Aktiviteler Teorisi'nin bilgisayar virüsü mağduriyeti ve siber suç mağduriyetinin tahmin edilmesinde güçlü bir teori olduğunu saptamış, bunun yanında araştırmaya konu olan internet kullanıcılarının %80'inin siber suçlar konusunda "oldukça endişeli" oldukları ve en yüksek korku oranlarına sahip olanların ise daha önce mağdur olanlar, siber suçları ciddi olarak görenler ve kadınlar olduklarını belirtmiştir.

Siber suç korkusunu spesifik bir suç üzerinden inceleyen bir çalışmayı ise Lynne D. Roberts vd. (2013) tarafından yapılan çalışma oluşturur. Roberts vd. (2013) çalışmalarında siber kimlik hırsızlığı ve bağlantılı hileli faaliyetlerin batı toplumlarında her yıl yaklaşık her 25 gençten birini etkilemesinden hareketle çalışmalarında bu suç türlerine odaklanmışlar, diğer yandan da internetin kimlik hırsızlığının etki boyutunu artırdığını savunmuşlardır.

Üniversite öğrencileri üzerinde gerçekleştirilen siber suç korkusu çalışmalarına bakıldığında ise Higgins vd. (2008) tarafından yapılan çalışmada Facebook'ta mağduriyet konusunda daha yüksek risk algısına sahip olan öğrencilerin daha çok korkuya sahip oldukları ortaya konmuştur. Henson (2011) ise Cincinnati Üniversitesi öğrencileri üzerinde yaptığı çalışmasında çok sayıda öğrencinin siber taciz mağduriyeti yaşamaktan korkmakta olduğunu ve bunun yanında cinsiyet, ilişki durumu, suçlu tipi ve takip davranışları sıklığının ise siber taciz mağduriyeti korkusunda önemli bir etkiye sahip olduğunu belirlemiştir. Henson (2011) ayrıca siber taciz mağduriyeti ile siber taciz mağduriyeti risk algısının da siber taciz mağduriyeti korkusunda anahtar belirleyiciler olduğu sonucuna ulaşmıştır. Yine üniversite öğrencileri üzerine yapılan bir diğer çalışmada Radda ve Ndubueze (2013, s. 35) Nijerya'da yer alan iki üniversiteyi incelemişler ve bu iki üniversitenin verilerini karşılaştırdıklarında her iki üniversite öğrencilerinde de online mağduriyet korkusunun yaygın olduğu sonucuna ulaşmışlardır. Araştırmada, iki üniversite öğrencileri arasında karşılaştırmalı olarak değerlendirilen beş korku türü içerisinde dolandırıcılık mailleri korkusunun en çok ifade edilen korku olduğu

bulunmuştur (Radda & Ndubueze, 2013, s. 42). Araştırmada son olarak, online mağduriyet korkusunun Nijerya'da Merkez Bankası tarafından teşvik edilen "nakitsiz Nijerya" hedefini, bu hedefin ana bileşenlerinden birisi online bankacılık olduğu için olumsuz etkileyebileceği ifade edilmiş, bilgi ve iletişim teknolojilerinin duyarlı kullanımı ve bu kullanım sırasında da kendini korumaya yönelik önleme stratejileri geliştirilmesi önerilmiştir (Radda & Ndubueze, 2013, s. 35). Üniversite öğrencileri üzerine yapılan başka bir çalışmada Yu (2014) suç korkusunun üç ana belirleyicisi olan suç ciddiyeti algısı, mağduriyet riski algısı ve mağduriyet deneyimini 4 siber suç (online dolandırıcılık, siber zorbalık, dijital korsanlık, bilgisayar virüsleri) üzerinden incelemiş ve bu 4 siber suç korkusunun, suça bağlı olarak, her zaman aynı belirleyicilerinin bulunmadığı sonucuna ulaşmıştır. Yu (2014) ayrıca internet kullanımının da siber suç korkusunda rol oynamakta olduğunu ifade etmektedir. Saskatchewan Üniversitesi öğrencileri arasında spesifik bir suç olarak kredi/banka kartı dolandırıcılığı üzerine yapılan bir çalışmada ise Abdulai (2016) Ulrich Beck'in risk toplumu teorisinin kuramsal çerçevesinden faydalanarak geçmiş mağduriyet tecrübesi ve internet kullanımı davranışının öğrencilerin kredi/banka kartı dolandırıcılığı mağduriyeti korkusu ve riski ile pozitif ilişki içerisinde bulunduğu sonucuna ulaşmaktadır. Abdulai (2016) ayrıca çalışmasındaki bulguların, risk toplumu teorisinin günümüz teknoloji çağında riskleri anlamamızı kolaylaştıran ve açıklayıcı güce sahip bir teori olduğunu gösterdiğini belirtmektedir.

Farkındalık ve bilgi düzeyi ile siber suç korkusu arasındaki ilişkiye odaklanan çalışmalara bakıldığında ise Meško ve Bernik (2011) Slovenya perspektifi üzerinden siber suçlarda farkındalık ve korku arasındaki ilişkiyi araştırmışlar, belirledikleri örneklemdeki siber suç mağdurlarının en çok bilgisayar virüslerinden mağdur oldukları, bunu sırasıyla e-mail yoluyla taciz, online sosyal ağlar yoluyla taciz, çocuk pornografisi, uygunsuz materyallere maruz kalma, sahte beyan, nefret söylemi ve kimlik hırsızlığının takip ettiği sonucuna ulaşmışlardır. Meško ve Bernik (2011) çalışmalarında siber suç korkusunun azaltılmasının ancak siber alanı kullanan bireylerin eğitilmesiyle, siber tehditler hakkında daha fazla bilgiye sahip olmalarıyla ve farkındalıklarının artırılmasıyla mümkün olacağını savunmuşlardır. Yine Bernik vd. (2013) ise bireylerin genellikle teknolojik cihazları yalnızca kullanmak istediklerini fakat kullanırken başta güvenlik olmak üzere diğer konuları unutmakta olduklarını ifade etmekte ve siber alanın kullanıcılar için daha güvenli bir çevre haline gelmesini sağlamak için bireylerin kendi kişisel ve/veya

kurumsal verilerini daha iyi koruyabilmek konusunda daha bilgili, eğitimli ve farkında olması ve siber suçların mağduru olmaktan kaçınması gerektiğini savunmaktadırlar.

Çeşitli mitolojik yaklaşımlar ve toplumdaki yaygın endişeler üzerinden korkunun oluşum sürecine odaklanan çalışmalardan Wall (2008a, s. 862) siber alanla ilgili olarak bireylerin ne söylediği ve gerçekte ne olduğu arasındaki çelişkinin siber alan ve siber suçlarla ilgili olarak bir mitolojiyi ortaya koymakta olduğunu ve bu mitolojinin bir gerçek olarak sunulmasının da halihazırda var olan toplumsal endişe ve kaygıları güçlendirdiğini savunmaktadır. Wall (2008a)'un bahsetmiş olduğu ve toplumda siber suçlara ilişkin korku kültürünün oluşmasına zemin hazırlayan bu mitlerin bazıları şunlardır;

- Siber suçlar dramatik, fütüristik ve distopiktir.
- Siber alan patolojik olarak güvensiz ve suç üretici yapıdadır.
- Her şeye kadir süper-hackerlar bulunur.
- Hackerlar organize suçların parçası olmuşlardır.
- Suçlular anonimdir ve takip edilemezler.
- Suçlular cezasız kalır ve işledikleri suç yanlarına kar kalır.
- Kullanıcılar zayıftır ve bu yüzden kendilerinden korunmalıdırlar.

Toplumda siber suç korkusunu oluşturduğu öne sürülen bu mitolojilere ilişkin bir başka çalışmada Ohm (2007, s. 1327) benzer şekilde "süper kullanıcı" figürünün bulunması zor, teknolojik sınırlamalardan bağımsız ve yasal boşlukların bilincinde bir mitik (efsanevi) figür olduğunu ve bu güçlü bilgisayar kullanıcısından duyulan korkunun online çalışmalarla ilgili tartışmalarda baskın geldiğini ifade etmektedir. Ohm (2007, ss. 1327-1328) bununla birlikte bilgisayar güvenliği ve internet hukuku uzmanlarının bizi korkudan kurtarmakta başarısız olduğunu, bunun da aşırı yasaklamalar, temel haklara yönelik zararlar, kolluk hizmetleri kaynaklarının boşa kullanılması ve ekonomik yatırımların yanlış tahsisine neden olduğunu belirtmektedir. Ohm (2007, s. 1401) çalışmasının sonunda teknoloji ve internet ortamlarında bilgi farklılıklarının bazıları tarafından güç kazanarak diğerlerine zarar vermek amacıyla sömürüldüğünü ve bunun da belirsizlik ve korku oluşturduğunu, fırsatçıların ise bu korkudan kişisel ve kurumsal kazanç elde ettiğini vurgulamaktadır. Yine toplumdaki suç korkusu ve endişesi algısına ilişkin olarak Furedi ise (2006) surveylerin bireylerin mağduriyetleri ile suça ilişkin

endişeleri arasında önemli bir farklılık bulunduğunu ortaya koyduğunu belirtmiştir. Örneğin medyanın risk raporlaması üzerine bir çalışmada, genç siyah erkekler en çok mağduriyet bildiren ancak en düşük korkuya sahip grup iken, daha yaşlı kadınlar (hem siyah hem beyaz) en yüksek korkuya sahip olan ancak en az mağduriyet sayısına sahip grup olarak karşımıza çıkmaktadır (Singer ve Endreny 1993, s. 62'den akt. Furedi, 2006, s. 16). Dolayısıyla gerçek suç tehdidi ile algı arasındaki ilişki yukarıda mitolojiye değinen çalışmalarda da görüleceği üzere belirgin olmaktan uzaktır (Furedi, 2006, s. 16). Bununla birlikte Furedi (2006, s. 23) suçların amansız artışına ilişkin algıların sağlık ve çevrede panik benzeri reaksiyonlarla paralel seyrettiğini ifade etmektedir. Furedi (2006, s. 24) çoğu çalışmanın kişisel güvenlikle ilgili toplumda yaygın bir endişe bulunduğunu ortaya koyduğunu belirterek suç hakkındaki bu yüksek seviyedeki endişenin dünyayı ancak daha güvensiz kıldığını savunmaktadır.

Medyanın siber suçlara ilişkin toplumsal algıları nasıl şekillendirdiğine değinen çalışmalara bakıldığında ise Wall (2008b, s. 58) düşük sayıdaki adli davaların kesinlikle siber suçların olmadığının bir delili olamayacağını, siber suçların kesinlikle bulunduğu ancak onlara yanlış objektiflerden bakıldığı, siber suçların dijital gerçekliklerinin paradoksal olarak siber suç mitolojisinin öngördüğünden farklı olduğu sonucuna ulaşıldığına dikkat çekmektedir. Wall (2008b, s. 58) siber suçların medyanın da yardımıyla insanların korkmasına neden olduğu ve bu korkunun da beklendiğini ve bu korkunun insanların siber suç beklentileri ile internet güvenliği beklentileri arasındaki boşlukta büyüdüğünü ifade etmektedir.

Siber suç korkusu konusunda uluslararası alanda yapılmış olan çalışmalardan bu çalışmaya yakın olan bir çalışma ise Boss vd. (2009) tarafından yapılmış ve Bilgi Sistemleri Güvenlik Araştırmaları Uluslararası Çalıştayı'nda sunulmuş olan "Familiarity Breeds Content: How Fear of Cybercrime Influences Individual Precaution-Taking Behavior (Aşinalık Rıza Doğurur: Siber Suç Korkusu Bireysel Önlem Alma Davranışlarını Nasıl Etkiler)" başlıklı çalışmadır. Boss vd. (2009) çalışmalarında bireylerin sistemlerini siber suçlardan korumak adına neden önlem almadıklarını/aldıklarını araştırmaktadırlar. Boss vd. (2009, s. 25)'nin araştırma sonuçları siber suçlara ilişkin geçmiş tecrübelerin bireylerin siber suç mağduru olma olasılıklarına ve siber suçun etkilerine ilişkin algılarını etkilediğini göstermiştir (Boss vd., 2009, s. 25).

Diğer yandan bireylerdeki bu algıların, her ne kadar her zaman beklenen yönde olmasa da, bireylerin önlem alma davranışlarını etkilemekte olduğu sonucuna ulaşılmıştır (Boss vd., 2009, s. 25).

Sonuç olarak siber suç korkusu konusundaki tüm bu ulusal ve uluslararası literatür taraması ışığında aşağıdaki hususlar göz önüne çıkmaktadır:

- Özellikle Türkiye'de Yurtsal (2016) tarafından yapılan ve siber suç korkusuna spesifik bir konu üzerinden yaklaşan çalışmanın dışında bu alanda hiçbir çalışmaya rastlanılmamıştır,
- Avrupa ve özellikle de ABD merkezli olarak yoğunlaşmakta olan uluslararası literatürde ise önlem alma stratejileri çok fazla ele alınmamıştır. Bu çalışmalar arasında örneğin Boss vd. (2009)'nin çalışması bireylerin kişisel konulardaki davranışlarının iş yerindeki davranışlarına da yansıyacağı kabulünden hareketle özellikle evdeki bilgisayar kullanımına odaklanmış, ancak bireylerin iş yerlerindeki ile iş yerleri dışındaki bilgi sistemleri kullanımları ve önlem alma davranışları arasında bir farklılık bulunup bulunmadığı konusuna ise değinmemiştir,
- Siber suçlara ilişkin yasal düzenlemeler, kolluk ve yargı birimlerine ilişkin algılar ile siber suç korkusu ilişkisine değinen araştırmaya rastlanılmamıştır,
- Siber suç korkusu ile ilgili çalışmalarda üniversite öğrencileri üzerinde yapılan çalışmalar ve ulusal survey verilerinden faydalanıldığı görülmekle birlikte, siber alanın en merkezi olarak kullanılmakta olduğu bölgelerden olan teknokentlerde bu konu ile ilgili bir çalışmaya rastlanılmamıştır.

Dolayısıyla temelde Türkiye'de oldukça eksik olduğu gözlenen siber suç korkusu literatürüne bir katkı sağlamak, yine literatürde eksik olduğu gözlenen önlem alma stratejileri konusunda bir katkı sağlamak, iş yeri ve dışındaki önlem alma stratejilerini incelemek, siber suçlara ilişkin yasal düzenlemeler, kolluk ve yargı birimlerine ilişkin algılar ile siber suç korkusu ilişkisine değinmek ve siber alanın en merkezi olarak kullanılmakta olduğu bölgelerden olan teknokentlere odaklanmak gibi gerekçelerle bu çalışmanın konusunu Ankara'daki teknokentler örneği üzerinden siber suç korkusu ve önlem alma stratejileri oluşturmuştur.

1.1.2. Araştırmanın Amacı

Bu çalışmanın temel amacını Ankara'da bulunan toplam 4 adet teknokentin (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışanları üzerindeki siber suç korkusunun ve önlem alma stratejilerinin araştırılması oluşturmaktadır. Çalışmada Ankara'daki teknokent çalışanları üzerinde siber suç korkusu bulunup bulunmadığı; siber suç korkusuna ilişkin önlem alma stratejilerinin neler olduğu; siber suç korkusu ile yaş, cinsiyet, eğitim durumu ve gelir durumu, geçmiş siber suç mağduriyeti, siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulma ve siber suçlara ilişkin yasal düzenlemeler, kolluk ve yargı birimlerine ilişkin algı arasında anlamlı bir ilişki bulunup bulunmadığının ortaya konulması amaçlanmaktadır. Araştırmada ayrıca teknokent çalışanlarının iş yerlerinde ve iş yerleri dışında kullandıkları elektronik cihazlardaki önlem alma stratejileri arasındaki ilişkinin de incelenmesi amaçlanmaktadır.

1.1.3. Araştırmanın Önemi

Siber suç korkusu konusunda yapılan bu çalışmanın birçok yönden önem arz etmekte olduğu söylenebilir. İlk olarak bu çalışma Ankara'daki teknokentlerde çalışan bireylerin siber dünyadaki güvenlik algılarının ve kendilerini ne kadar güvende hissettiklerinin ortaya konulması açısından oldukça önemlidir. Zira siber suç korkusu bireylerin günlük yaşamlarında ve siber aktivitelerinde herhangi bir korku, endişe, kaygı vb. hissetmeksizin ya da kendilerine karşı bir tehdit algılaması görmeksizin rahat bir biçimde davranabilmelerini engelleyen bir konudur. Her an bir siber suçun mağduru olma ihtimali ile yaşayan bireylerin sosyal ya da siber aktivitelerinde yeterince özgür olabileceklerini söylemek çok da mümkün değildir. Bu bağlamda bu çalışma Ankara'daki teknokentlerde çalışan bireylerin siber suç korkularının düzeyinin ortaya konulması açısından önemlidir.

İkinci olarak teknoloji ve internetin en üst düzeyde kullanıldığı alanlardan birisi olarak görülebilecek teknokentlerde çalışan bireylerin siber suç korkusuna ilişkin önlem alma stratejilerinin neler olduğunun ortaya konulması da bu çalışmanın önemini artırmaktadır. Zira çoğunluk itibariyle iyi bir eğitim seviyesine sahip olan ve günlük hayatlarının önemli bir bölümünde teknoloji ve internetle iç içe olarak çalışan teknokent çalışanlarının siber

suç korkusuna ilişkin geliştirmiş oldukları önlem alma stratejileri toplumun bu korku ile yaşayan diğer bireyleri için de önemli bir veri teşkil edebilecektir.

Üçüncü olarak bu çalışmada siber suç korkusu ve önlem alma stratejileri, bireylerin siber suçlara ilişkin yasal düzenlemeler ve işlemlere ilişkin algıları ve geçmiş siber suç mağduriyeti konularını da içeren kapsamlı bir anket hazırlanmıştır. Hazırlanmış olan bu anketin ve anket sorularının siber suçlar konusunda daha sonra yapılacak olan çalışmalarda faydalanılabilecek olması açısından önemli olduğu söylenebilir.

Dördüncü olarak bu çalışma Türkiye'de siber suç korkusu konusunda oldukça eksik olduğu gözlemlenen literatüre bir katkı sağlaması açısından önem arz etmektedir.

Bu bağlamda son olarak bu çalışmanın siber suç korkusu konusunda yeni yapılacak olan çalışmaların da önünü açması hedeflenmektedir.

1.2. ARAŞTIRMANIN YÖNTEMİ

Bu çalışmanın ana amacını Ankara'daki 4 teknokentin (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışanları üzerindeki siber suç korkusunun ve önlem alma stratejilerinin araştırılması oluşturmaktadır. Bu bağlamda bu çalışma nicel bir araştırma olarak tasarlanmıştır. Araştırmanın nicel bir araştırma olarak tasarlanmasının arka planında, Türkiye'de siber suç korkusu konusuna spesifik olarak yaklaşan bir çalışma dışında hiçbir çalışmaya rastlanılmamış olması ve dolayısıyla istatistiksel olarak tanımlayıcı bir çalışma yapılmasının bu konuda Ankara'daki teknokentlerdeki genel görünümü kapsayıcı bir şekilde tasvir etmek ve betimlemek açısından yararlı olacağı ve bundan sonra yapılacak olan nicel ya da nitel çalışmalar açısından yol gösterici bir işleve sahip olması düşüncesi etkili olmuştur.

Araştırma yöntemsel açıdan teorik ve uygulamalı olmak üzere iki kısımdan oluşmuştur. Araştırmanın teorik olan ilk kısmında çalışmanın amacı doğrultusunda öncelikle suç korkusu ve siber suç korkusu ile ilgili literatür incelenmiş ve değerlendirilmiştir. Yapılan bu literatür incelemesi sırasında, Türkiye'de özellikle siber suç korkusu konusunda henüz bir literatürün oluşmamış olduğu görüldüğünden ABD ve Avrupa ağırlıklı olmak üzere uluslararası literatürden faydalanılmıştır.

Araştırmanın kavramsal çerçevesi ile ilgili olarak özellikle Türkiye'deki bilişim suçları ile ilgili yasal mevzuat ve kavramsallaştırmalar incelenmiş, bunun yanında siber suçlara ilişkin uluslararası yaklaşımlar da değerlendirilmiştir. Yapılan değerlendirmeler neticesinde siber suçlara ilişkin bu çalışma açısından kapsayıcı olacağı düşünülen bir tanımlama oluşturulmuş ve benimsenmiştir.

Araştırmanın temel konusunu siber suçlardan mağdur olma korkusu oluşturduğundan, araştırmanın kuramsal çerçevesi ile ilgili olarak ise sosyoloji, kriminoloji ve viktimoloji teorileri incelenmiştir. Yapılan bu incelemeler neticesinde siber suçları ve siber suçlardan mağdur olma korkusunu en iyi şekilde açıklayabileceği düşünülen teori ve yaklaşımlara çalışmada yer verilmiştir.

Yapılan tüm bu literatür taramaları ve çalışmanın teorileri doğrultusunda bu araştırmanın konusunu oluşturan siber suç korkusu ve önlem alma stratejilerine ilişkin hipotezler geliştirilmiştir. Geliştirilen bu hipotezlerin test edilebilmesi amacıyla araştırma evrenini temsil etmek üzere seçilen örnekleme yöneltilmek amacıyla 49 sorudan oluşan bir anket formu oluşturulmuştur. Anket sorularının oluşturulması sırasında daha önce suç korkusu ve siber suç korkusunun ölçümü için literatürde yer alan farklı çalışmalarda geliştirilmiş ve kullanılmış olan ölçekler ve sorular incelenmiştir. Oluşturulmuş olan anket formu için öncelikle pilot bir çalışma gerçekleştirilmiş ve bu pilot çalışmadan elde edilen yorum ve değerlendirmeler neticesinde anket soruları yeniden düzenlenmiştir. Pilot çalışma neticesinde son hali verilen anket formu resmi onay için Hacettepe Üniversitesi Etik Komisyonu'na sunulmuş ve bu komisyonun 20 Haziran 2017 tarihinde yapmış olduğu toplantıda incelenerek etik açıdan uygun bulunmuştur.

Araştırmanın uygulamalı olan ikinci kısmının başında ise daha önce Etik Komisyon onayı alınmış olan anket formu ile birlikte Ankara'da bulunan 4 adet teknokentin (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) yönetimlerine anketin bu teknokentlerde yer alan firmaların çalışanlarına uygulanabilmesi için dilekçe ile izin başvurusunda bulunulmuştur. Bahse konu teknokent yönetimlerinin tamamından gerekli izinlerin alınması neticesinde anket formu yukarıda belirtilen 4 adet teknokentin firma çalışanlarına araştırmacı tarafından birebir yüz yüze görüşme yoluyla uygulanmıştır.

1.2.1. Araştırmanın Hipotezleri

Bu araştırmanın hipotezleri aşağıda sıralanmaktadır:

1- Bireylerin yaş, cinsiyet, eğitim durumu ve gelir düzeyleri ile siber suç korkuları arasında anlamlı bir ilişki bulunmaktadır.
2- Geçmiş siber suç mağduriyeti ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır.
3- Siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır.
4- Siber suçlara ilişkin yasal düzenlemeleri, kolluk ve yargı birimlerini siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır.
5- Teknokent çalışanlarının iş yerlerinde ve iş yerleri dışında kullandıkları elektronik cihazlarda önlem alma stratejileri arasında anlamlı bir ilişki bulunmaktadır.

1.2.2. Araştırmanın Evren ve Örneklemi

Bu çalışmanın evrenini Ankara'da bulunan 4 adet teknokent (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) oluşturmaktadır. Araştırmanın evren sayısı toplam **13095 kişi** olup araştırma evrenine ait sayısal veriler aşağıdaki tabloda gösterilmektedir.

Tablo 1. Evren Sayıları

ANKARA'DAKİ TEKNOKENTLER	ÇALIŞAN SAYISI*
ODTÜ Teknokent	5751
Bilkent Cyberpark	3614
Hacettepe Teknokent	2844
Gazi Teknopark	886
Ankara Üniversitesi Teknokent (Yeniden yapılanmakta oldukları gerekçe gösterilerek bilgilerini tarafımızla paylaşmadığı için araştırma dışında bırakılmıştır.)	512

Ankara Sanayi Odası Teknopark (Bu araştırmanın yapıldığı dönemde henüz tam olarak faaliyete geçmediği için araştırma dışında bırakılmıştır.)	-
Ankara Teknopark (Bu araştırmanın yapıldığı dönemde henüz tam olarak faaliyete geçmediği için araştırma dışında bırakılmıştır.)	-

*Bu çalışmadaki çalışan sayılarına ilişkin veriler 2017 yılı Mayıs-Haziran aylarına aittir.

Araştırma örneklemi yukarıdaki tabloda çalışan sayıları gösterilen ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark'ın çalışan sayıları ile orantılı olarak tabakalı örneklem metodu kullanılarak belirlenmiştir. Bu bağlamda araştırmanın örneklem sayısı 0.05 hoşgörü miktarı ve 0.01 hata payı ile toplam **266 kişi** olarak belirlenmiş olup, aşağıdaki tabloda ayrı ayrı gösterilmektedir.

Tablo 2. Örneklem Sayıları

ANKARA'DAKİ TEKNOKENTLER	ÖRNEKLEM SAYILARI
ODTÜ Teknokent	117
Bilkent Cyberpark	73
Hacettepe Teknokent	58
Gazi Teknopark	18
TOPLAM	266

Burada bu araştırma açısından seçilen örneklemle ilgili olarak değinilmesi gereken bazı hususlar bulunmaktadır. Bu araştırmanın evren ve örnekleminin belirlenmesi aşamasında ilk olarak evreni oluşturan teknokentlere gidilerek bu teknokentlerde çalışan personel sayıları bu sayıları vermeyi kabul eden teknokentlerden sektörel olarak elde edilmiştir. Çalışan sayılarını paylaşmayı yeniden yapılanma durumunda olmalarını gerekçe göstererek reddeden Ankara Üniversitesi Teknokent bu aşamada araştırma dışı bırakılmış ve geriye kalan ve Ankara'da faal durumda bulunan 4 adet teknokent (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Tekopark) üzerinden çalışmaya devam

edilmiştir. Araştırmanın anket formunun oluşturulmasının ve Hacettepe Üniversitesi Etik Komisyonu Onayının alınmasının ardından ise bu 4 teknokentin her birinin yönetimlerine ayrı ayrı dilekçe ile başvurularak araştırmanın yapılabilmesi ve anketin uygulanabilmesi için izin istenilmiştir. Bu aşamada bu 4 teknokentin tamamı araştırmanın yapılabilmesi için gerekli izni vermişlerdir. Sonrasında bu 4 teknokent üzerinden örneklem belirlenmesi aşamasına geçilmiş ve her bir teknokentten teknokentlerde çalışan toplam çalışan sayısıyla oransal olarak seçilecek şekilde tabakalı örneklem metodu kullanılarak örneklem sayısı belirlenmiştir. Fakat tam da bu aşamada teknokentlerdeki sektörel çalışan listeleri üzerinden seçim yapmaya imkan tanıyacak olan çalışan isim listelerinin elde edilememesi üzerine çalışmada olasılıklı olmayan örnekleme tekniklerinden tesadüfi örnekleme tekniği kullanılmıştır.

1.2.3. Araştırmanın Veri Toplama Teknikleri

Bu araştırmanın veri toplama tekniğini araştırmacı tarafından yüz yüze olarak gerçekleştirilen anket çalışması ve inter-survey olarak da adlandırılan web tabanlı anket çalışması oluşturmuştur. Web tabanlı anket uygulaması teknokentlerde katılımcılarla birebir yapılan görüşmelerde katılımcıların web tabanlı anket çalışmasını doldurmayı tercih etmeleri neticesinde kendilerine bu anketin adresinin verilerek doldurmalarının sağlanması suretiyle gerçekleşmiştir. Araştırmada yer alan anket çalışmasını web tabanlı olarak dolduran katılımcı sayısı toplam 266 katılımcı içerisinden 36'dır (%13,53).

Araştırmada uygulanan anket formu toplam 6 bölümden oluşmaktadır. Anket formunun ilk bölümü "Demografik ve Genel Sorular" başlığı altında yer alan 5 kapalı uçlu ve 1 açık uçlu olmak üzere toplam 6 sorudan oluşmaktadır. Bu sorular katılımcının "yaşı, cinsiyeti, eğitim durumu, aylık gelir düzeyi, çalıştığı kurumdaki pozisyonu ve çalıştığı kurumun hangi sektörde faaliyet gösterdiği" sorularından oluşmaktadır.

Anket formunun ikinci bölümü "Siber Suç Korkusu ile İlgili Sorular" başlığı altında yer alan toplam 16 adet kapalı uçlu sorudan oluşmaktadır. Anketin bu ikinci bölümünde katılımcılara toplam 16 adet siber suç türü üzerinden bu suçlardan mağdur olma konusundaki korkularının düzeyi sorulmuştur. Katılımcılar her bir suç türü için "mağdur olmak konusunda hiç korku yaşamıyorum – mağdur olmak konusunda zaman zaman

korku yaşıyorum – mağdur olmak konusunda genellikle korku yaşıyorum" olmak üzere 3 seçenekten birini seçmişlerdir. Araştırmanın bu bölümündeki sorular özellikle siber suçlardan mağdur olmak konusunda "korku yaşıyorum – korku yaşamıyorum" şeklinde ikili bir seçenekle sorulmayarak mağdur olmaktan duyulan korkunun derecesine ulaşılmaya çalışılmıştır. Zira literatürde bu konuda yapılmış olan çalışmalara bakıldığında siber suç korkusu ile ilgili yapılan ilk çalışmaların korku yaşıyorum – korku yaşamıyorum şeklinde iki seçenekli sorularla gerçekleştirildiği ancak ilerleyen çalışmalarda yaşanılan korkunun sıklığı ve yoğunluğunun da yapılan çalışmalar için önemli olacağının farkına varıldığı anlaşılmıştır (Henson & Reyns, 2015, s. 93).

Anket formunun üçüncü bölümü "Geçmiş Siber Suç Mağduriyeti ile İlgili Sorular" başlıklı 2 adet sorudan oluşmaktadır. Bu bölümde katılımcılara ilk olarak son 12 ay içerisinde herhangi bir siber suç türünden mağdur olup olmadıkları sorulmuştur. Son 12 ay içerisinde herhangi bir siber suçtan mağdur olanlara ise ikinci olarak geçmişte yaşamış oldukları siber suç mağduriyetinin siber suçlardan mağdur olmamak adına almış oldukları önlemlerde bir değişiklik meydana getirip getirmediği sorulmuştur.

Anket formunun dördüncü bölümü "Yasal Düzenlemeler ve İşlemlere İlişkin Algı" başlıklı 4 adet sorudan oluşmaktadır. Bu 4 sorunun ilk üçü kapalı uçlu olup, dördüncüsü ise açık uçlu olarak sorulmuştur. Kapalı uçlu olarak sorulan sorularda katılımcılara Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri, kolluk (polis, jandarma vb.) ve yargı birimlerini siber suçlarla mücadele, siber suç faillerinin yakalanması ve cezalandırılması noktasında yeterli bulup bulmadıkları sorulmuştur. Bu üç sorunun ardından gelen açık uçlu soruda ise bu konuya ilişkin eklemek istedikleri bir görüşlerinin olup olmadığı sorusu katılımcılara yöneltilmiştir.

Anket formunun beşinci bölümü "Başa Çıkma/Önlem Alma Stratejilerine İlişkin Sorular" başlıklıdır. Bu bölüm 19'u kapalı 1'i açık uçlu olmak üzere toplam 20 sorudan oluşmakta olup bu bölümde katılımcılara siber suç korkusu ile başa çıkma ve önlem alma stratejilerine ilişkin sorular yöneltilmiştir. Bu bölümde yer alan sorulardan 12'si katılımcıların iş yerleri ve iş yerleri dışında kullanmış oldukları elektronik cihazlardaki siber suç korkusu ile başa çıkma ve önlem alma stratejilerini ayrı ayrı değerlendirebilmek amacıyla ayrı ayrı sorulmuştur. Bu bölümün son sorusunu oluşturan açık uçlu soruda ise katılımcılara bu bölümdeki sorularda belirtilen stratejilerden farklı olarak kendilerinin

kullanmış olduğu herhangi bir siber suç korkusu ile başa çıkma ve önlem alma stratejisi bulunuyor ise bunları belirtmeleri istenmiştir. Böylelikle teknokent çalışanlarının kendi kullanmış oldukları stratejilerin de bu çalışma kapsamında ortaya konulabilmesi amaçlanmıştır.

Anket formunun altıncı ve son bölümünü oluşturan "Alınan Önlemlerin Yeterli Bulunup Bulunmadığı" başlıklı bölümde ise katılımcılara siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulup bulmadıklarına dair bir adet soru yöneltilmiştir.

1.2.4. Araştırmanın Veri Analizi

Araştırmada gerçekleştirilen anket uygulaması neticesinde elde edilmiş olan verilerin tamamı araştırmacı tarafından SPSS 25.0 paket programına aktarılarak analiz edilmiş ve yorumlanmıştır.

Araştırma sonucunda anket formunun ilk bölümünde yer alan "Demografik ve Genel Sorular" başlığı altında yer alan sorular vasıtasıyla ilk olarak araştırma örnekleminin sosyo-demografik yapısı ve genel özellikleri "frekans" ve "yüzde" değerleriyle birlikte ortaya konulmuştur.

Ardından anket formunun diğer bölümlerinde yer alan sorular da katılımcıların vermiş olduğu cevaplar üzerinden "frekans" ve "yüzde" değerleriyle birlikte analiz edilmiş ve değerlendirilmiştir.

Sonraki aşamada anketin bölümleri arasındaki karşılıklı ilişkilerin analizi yapılmıştır. Bu kısımda katılımcıların siber suç korkusu ile demografik özellikler, geçmiş siber suç mağduriyeti, yasal düzenlemeler ve işlemlere ilişkin algı ve alınan önlemlerin yeterli bulunup bulunmadığı çapraz tablolar ve ki kare analizleri vasıtasıyla incelenmişlerdir. Yine bu kısımda katılımcıların işyerlerinde ve dışında kullandıkları elektronik cihazlardaki önlem alma/başa çıkma stratejileri arasındaki ilişki de ki kare analizleri ile incelenmiştir.

Son olarak araştırma hipotezlerinin durumu yapılan tüm bu analizler neticesinde incelenmiş ve yorumlanmıştır.

1.2.5. Operasyonel Tanımlar

Suç: Türk Ceza Kanunu ve Türk mevzuatında yer alan diğer ilgili kanunlar uyarınca karşılığında bir ceza öngörülmüş olan fiillerin tamamı bu çalışma açısından suç olarak kabul edilmiştir.

Siber Suç: Bilişim sistemleri aracılığıyla veya bilişim sitemleri hedef alınarak işlenmiş olan suçların tamamı bu çalışma açısından siber suç olarak ele alınmaktadır. Esasında bilişim suçları, siber suçlar, internet suçları gibi kavramlar birbirlerinden farklı anlamlar içermekte olsalar da bu çalışma açısından hepsi bir arada değerlendirilmiş ve siber suç adı altında ele alınmıştır. Bu bağlamda her ne kadar literatürde siber suç tanımı internet vasıtasıyla işlenen suçlar olarak değerlendirilmekte olsa da bu çalışma açısından internet olmadan işlenen bilişim suçları da siber suçlar tanımına dahil edilmiştir.

Siber Suç Korkusu: Siber suçlardan mağdur olmaktan duyulan korku, endişe, telaş vb. durumlardır. Korku, endişe, telaş gibi duygusal durumlar esasında birbirleriyle birebir aynı olmayan durumlarda ortaya çıkan farklı duygusal tepkiler olmakla birlikte bu çalışma açısından bir arada değerlendirilmişlerdir. Söz gelimi korku boyutuna ulaşmamakla birlikte endişe boyutunda kalan siber suçlardan mağdur olma endişesi de bu çalışma kapsamında korkuya dahil edilmiştir.

Siber Suç Korkusuna İlişkin Önlem Alma/Başa Çıkma Stratejileri: Bireylerin siber suçlardan mağdur olmak konusunda yaşamış oldukları korkunun öncesinde veya sonrasında bu korkuyu henüz oluşmadan ortadan kaldırmak adına almış oldukları önlemler ile korkunun oluşmasının ardından korkuyu ortadan kaldırmak adına geliştirdikleri başa çıkma stratejilerinin tamamını ifade etmektedir. Siber suç korkusuna ilişkin önlem alma ve başa çıkma stratejileri her ne kadar başlangıç itibariyle farklı stratejilermiş gibi gözükseler de esasında aynı stratejileri içermekte ve bu çalışmada da birbirleriyle aynı stratejileri ifade etmektedirler.

1.3. ARAŞTIRMANIN SINIRLILIKLARI

Bu araştırma Ankara'da yer alan 4 adet teknokent (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknopark ve Gazi Teknopark) ile ve bu teknokentlerden bu araştırmaya katılmış olan bireyler ile sınırlıdır. Araştırmanın bu sınırlılıklara sahip olmasının arkasında iki temel zorluk yatmaktadır.

Bu zorluklardan ilki araştırmanın örneklem sayısının belirlenmesi esnasında Ankara Üniversitesi Teknokent'ten sektörel olarak çalışan sayılarının talep edilmesi sırasında meydana gelmiştir. ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknopark ve Gazi Teknopark gibi her biri Ankara Üniversitesi Teknokentten daha fazla çalışan sayılarına sahip olan teknokentlerin sektörel olarak çalışan sayılarına nispeten rahat bir şekilde ulaşılmakla birlikte Ankara Üniversitesi Teknokent yönetimi ilk önce sektörel olarak personel sayılarını paylaşabileceklerini belirtmiş ancak daha sonra yeniden yapılanma durumunda olmalarını gerekçe göstererek istenilen veriyi araştırmacı ile paylaşmamışlardır. Sonuç olarak bürokratik olarak da oldukça ağır işleyen bir yapıya sahip olduğu gözlenen Ankara Üniversitesi Teknokent, Ankara'da faaliyet gösteren teknokentler içerisinde bu araştırmanın kapsamından çıkarılan tek teknokent olmuştur.

Araştırmada karşılaşılan ikinci zorluk araştırmanın evrenini oluşturan teknokentlerden, evreni temsil kabiliyetine sahip olan bir örneklemin belirlenebilmesi açısından, bu teknokentlerde yer alan sektörel çalışan listelerine erişim izni verilmemesi olmuştur. Bu durum teknokentlerde çalışan ve özellikle de savunma sanayi, havacılık gibi oldukça hassas birimlerin yanında yazılım geliştirme, ar-ge vb. belli oranda gizliliğe sahip olabilecek birimlerde çalışan personele ait listelerin paylaşıma kapalı bulundurulması noktasında kabul edilebilir gerekçelere sahip olabilir. Bu nedenle bu araştırma tabakalı örnekleme metodu ile belirlenmiş örneklem sayısına herhangi bir kriter gözetmeksizin tesadüfi olarak ulaşılması yoluyla gerçekleştirilmiştir.

2. BÖLÜM ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ

2.1. SİBER SUÇLAR

2.1.1. Geleneksel Suçlar ve Siber Suçlar

Teknolojinin giderek daha fazla gelişmesi ve bireylerin hayatlarına her zamankinden daha fazla dahil olmasıyla birlikte bireyler teknolojinin kendilerine sağladığı geniş imkanlar ve kolaylıkların yanında teknolojik gelişmenin neden olduğu tehlike ve risklerle de karşı karşıya bulunmaktadırlar. Teknolojiyle bağlantılı bu tehlike ve risklerden birisi de şüphesiz siber suçlardır. Daha önceleri geleneksel yöntemlerle işlenmekte olan suçlar teknolojinin gelişmesiyle birlikte yerini dijital ortamda meydana gelen ya da dijital ortamdan faydalanılarak işlenen siber suçlara bırakmıştır. Nitekim İngiltere'de 2016 yılında Ulusal Suç Ajansı (National Crime Agency)'nin Ulusal İstatistikler Ofisi (Office for National Statistics) verilerine dayanarak hazırladığı Cyber Crime Assessment 2016 raporuna göre, 2015 yılında İngiltere'de işlenen siber suçlar tüm suçların yarısından daha fazlasını oluşturarak geleneksel suçları geçmeyi başarmıştır (National Crime Agency, 2016). Bu konudaki bir diğer örnekte ise İngiltere ve Galler'de suç araştırmasının 2017 yılı haziran ayında tamamlanan survey verilerine göre İngiltere'de işlenen dolandırıcılık suçlarının yarısından daha fazlasını (%57) siber ilişkili dolandırıcılık suçları oluşturmuştur (CSEW, 2017). Dolayısıyla siber alanın sağladığı geniş olanaklardan faydalanan siber suçlular artık geleneksel suçların zaman, mekan vb. herhangi bir kısıtlaması altında olmaksızın dünyanın herhangi bir yerindeki bireyler için rahatlıkla bir tehdit unsuru olabilmektedirler.

Bu yönüyle günümüzde suçlar arasında bir sınıflandırma yapılmak istendiğinde bu sınıflandırmayı genel anlamda iki başlık altında yapabilmek mümkündür. Bu başlıklardan ilkini geleneksel suçlar oluşturur. Geleneksel suçlar en basit tanımıyla gerçek dünyada işlenen suçlar olarak tanımlanabilir. Bu bağlamda kasten öldürme (TCK m. 81), kasten yaralama (TCK m. 86), cinsel saldırı (TCK m. 102) vb. gerçek dünyada işlenen suçlar geleneksel suçlara örnek olarak gösterilebilir. Bu sınıflandırmadaki ikinci başlığı ise sanal suçlar ya da bu çalışmadaki ifadesiyle siber suçlar oluşturur. Siber suçlar ise gerçek

dünyada işlenen suçlara zıt olarak sanal dünyada ya da siber alanda işlenen suçlar olarak karşımıza çıkmaktadır. Bilişim sistemine girme (TCK m. 243) ve sistemi engelleme, bozma, verileri yok etme veya değiştirme (TCK m. 244) vb. siber alanda işlenen suçlar siber suçlara örnek olarak gösterilebilir. Bununla birlikte geleneksel suçlar ve siber suçları birbirinden tümüyle bağımsız iki ayrı küme şeklinde tanımlamak doğru olmayıp, Şekil 1'deki gibi birbirleriyle kesişen iki küme şeklinde tanımlamak daha doğru olacaktır. Geleneksel suçlar ve siber suçların kesişiminde yer alan bölgeyi siber alanın yardımıyla işlenen geleneksel suçlar oluşturmaktadır. Bu bölgeyi P. N. Grabosky (2001) ve Brenner (2006)'nın tabirleriyle "old wine in new bottles (yeni kaplardaki eski şaraplar)" şeklinde de tanımlamak mümkündür. Bu suçlara örnek olarak bilişim sistemleri aracılığıyla dolandırıcılık (TCK m. 158/1-f) suçu gösterilebilir. Zira örneğin bir internet adresi üzerinden satılmakta olduğu gözüken ancak gerçekte bulunmayan bir ürünün bir müşteriye satılması işlemi bu suç türü içerisinde değerlendirilecek ve dolayısıyla gerçek dünyadaki dolandırıcılık suçunun siber alanın yardımıyla işlenmesine bir örnek teşkil edecektir.

Yine Burden ve Palmer (2003, s. 222) ise siber suçlara ilişkin olarak "true (gerçek)" siber suçlar ve "e-enabled (internet destekli)" suçlar şeklinde bir ayrıma gitmektedirler. Burada gerçek siber suçlar online ortam dışında bulunmayan sahtekar veya kötü niyetli fiiller olarak tanımlanırken, internet destekli suçlar ise dünya çapında ağ (world wide web)'ın bulunmasından önce bilinen fakat şu anda giderek internet üzerinde işlenmeye başlanan suç fiilleri olarak tanımlanmaktadır (Burden & Palmer, 2003, s. 222). Dolayısıyla aşağıdaki Şekil 1.'de siber suçlar olarak adlandırılan ve siber alanın yardımıyla işlenen suçlar dışında kalan alanın Burden ve Palmer (2003, s. 222)'in "true (gerçek)" siber suçlar olarak adlandırdıkları suçları içermekte olduğu, geleneksel suçlar ve siber suçlar kesişiminde yer alan siber alanın yardımıyla işlenen geleneksel suçlar'ın ise "e-enabled (internet destekli)" suçlar olarak adlandırılan suçları içermekte olduğu da söylenebilecektir.

Aynı şekilde Lilley (2002, s. 24) de bilgisayarla ilgili suçlar (computer related crime - CRC) ve bilgisayar destekli suçlar (computer assisted crime - CAC) şeklinde ikili bir sınıflandırmadan söz etmektedir ki bu sınıflandırmada CRC bilgisayar ya da içeriğinin suç saldırısının konusu olduğu suçları ifade ederken, CAC ise bilgisayarların suçun

işlenmesini sağlamada yalnızca bir araç olarak kullanıldıkları suçları ifade etmektedir. Benzer şekilde Furnell (2001, ss. 30-31) UK Audit Commission'un (1998) bilgisayar suçları ve kötüye kullanım sınıflandırmasının dolandırıcılık, hırsızlık, lisanssız yazılım kullanımı, korsan işler, kişisel verilerin kötüye kullanımı, hacking, sabotaj, pornografik materyal, virüs şeklinde olduğunu ve bunların da genel olarak bilgisayar destekli suçlar (computer assisted crimes) ve bilgisayar odaklı suçlar (computer focused crimes) şeklinde iki başlık altında sınıflandırılabileceğini belirtmektedir. Dolayısıyla hem Furnell (2001), hem de Lilley (2002)'nin bahsetmiş oldukları bilgisayar destekli suçlar sınıflandırmasının da Şekil 1.'de yer alan siber alanın yardımıyla işlenen geleneksel suçlara, bilgisayar odaklı suçlar sınıflandırmasının ise siber alanın yardımıyla işlenen geleneksel suçlar dışında kalan siber suçlara karşılık gelmekte olduğu söylenebilir.

Sonuç olarak Furnell (2001) ve Lilley (2002)'nin bilgisayar odaklı suçlar tanımlamaları ile Burden ve Palmer (2003)'in "true (gerçek)" siber suçlar tanımlaması ve Karagülmez (2009)'in bilişim sistemine yönelik suçlar tanımlamaları birbirleriyle aşağı yukarı aynı noktalara atıfta bulunmakta olup Şekil 1.'de yer alan siber suçlar alanına karşılık gelmektedirler. Aynı şekilde Furnell (2001) ve Lilley (2002)'nin bilgisayar destekli suçlar tanımlamaları ile Burden ve Palmer (2003)'in "e-enabled (internet destekli)" suçlar tanımlaması ve Karagülmez (2009)'in bilişim sisteminin kullanıldığı suçlar tanımlamaları ise yine benzer noktalara atıfta bulunmakta olup Şekil 1'de yer alan Siber Alanın Yardımıyla İşlenen geleneksel suçlara karşılık gelmektedirler.

Şekil 1. Geleneksel Suçlar ve Siber Suçlar

Bununla birlikte siber suçlar yalnızca bireyler için değil, aynı zamanda örgütler, kuruluşlar ve devletler için de önemli bir tehdit unsurudur. Örneğin iş dünyasında faaliyet gösteren herhangi bir kuruluş, bir siber saldırı neticesinde bünyesindeki siber güvenlik zafiyetleri nedeniyle önemli veri kayıpları yaşayabilirken, devletler de siber suçluların siber terörizm, siber casusluk vb. faaliyetleri sonucunda maddi ve manevi geniş çaplı zararlarla karşı karşıya kalabilmektedirler.

Bu bağlamda bu çalışmada gerçekleştirilmiş olan anket çalışmasında da katılımcıların korku düzeylerinin ölçülmesi adına toplam 16 adet siber suç belirlenmiş olup, bu siber suçlar aşağıda sıralanmıştır:

- Bilişim Sisteminize Hukuka Aykırı Olarak Girilmesi ve Sistemde Kalınmaya Devam Edilmesi (TCK m. 243) olarak adlandırılan "Bilgisayar Korsanlığı (Hacking),
- Bilişim sistemlerinin erişilebilirliğine yönelik hizmeti engelleme saldırıları olarak adlandırılan "Denial of Service (DoS) Saldırıları" TCK m. 244/1,
- Virüsler, Truva Atları ve Zararlı Yazılımlar (TCK m. 244/2),
- Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız (TCK m. 245),
- Kişisel Verilerinizin Rızanız Dışında Hukuka Aykırı Olarak Kaydedilmesi (TCK m. 135) suçunu oluşturan Casus Yazılımlar,
- Kişisel Verilerinizin Rızanız Dışında Hukuka Aykırı Olarak Üçüncü Kişilere Verilmesi, Yayılması ya da Bu Verilerin Üçüncü Kişiler Tarafından Ele Geçirilmesi (TCK m. 136) olarak adlandırılabilecek olan Kimlik Hırsızlığı,
- Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi (TCK m. 138),
- Siber Zorbalık (Bilgisayar, cep telefonu, vb. elektronik cihazlar vasıtasıyla ısrarcı, tekrar eden ve zarar verici nitelikteki davranışlar – TCK m. 81, 84, 96, 106, 122, 123, 125, 132, 133, 134, 135, vb.,)
- Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü – TCK m. 125),

- Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi (TCK m. 132),
- Bilişim Sistemleri Aracılığıyla Hırsızlık (TCK m. 142/2-e) olarak adlandırılabilecek olan Siber Hırsızlık,
- Bilişim Sistemleri Aracılığıyla Dolandırıcılık (TCK m. 158/1-f) olarak adlandırılabilecek olan Siber Dolandırıcılık,
- Siber Taciz (TCK m. 105/2-d),
- Siber Tehdit ve Şantaj (TCK m. 106, 107),
- Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu (TCK m. 122),
- Siber Terörizm (Terörle Mücadele Kanunu).

2.1.2. Akıllanan Eşyalar, Nesnelerin İnterneti, Kripto Paralar, Robotik Teknolojiler ve Yapay Zeka

Günümüzde bireylerin artık siber alanda da birbirleriyle oldukça yoğun şekilde etkileşime girmeye başladıkları ve her geçen gün zamanlarının daha fazlasını siber alanda harcamaya başladıkları görülmeye başlanmıştır. Daha önceleri evde, okulda, iş yerinde, kahvehanelerde, çay bahçelerinde, toplu taşıma araçlarında vb. yerlerde yüz yüze etkileşimler şeklinde gerçekleşen sosyalleşmeler, artık yerini siber dünyada gerçekleşen sanal etkileşimlere ve sosyalleşmelere bırakmıştır. Teknolojinin ve internetin gelişmesiyle birlikte siber dünyaya dahil olan bireylerin sayısı her geçen gün daha fazla artmakta ve halihazırda siber dünyaya dahil olmuş olan bireyler ise her geçen gün günlük zamanlarının daha fazlasını burada geçirmeye başlamaktadırlar. Nitekim Cybersecurity Ventures tarafından yayınlanan 2017 Siber Güvenlik Raporu'na göre dünyada internet kullanıcılarının sayısının 2022 yılına kadar 6 milyarı, 2030 yılına kadar ise 7.5 milyarı bulması beklenmektedir (Morgan, 2017, s. 4).

Bununla birlikte bireylerin giderek siber dünyaya daha fazla dahil olmaya başlamaları yalnızca bireylerin interneti kullanması yoluyla olmamaktadır. Son yıllarda meydana gelen pek çok teknolojik gelişmenin insan hayatının her alanında önemli ve ciddi değişiklikler meydana getirdiğini ve bireyleri giderek siber alanın içerisine doğru çektiğini söylemek mümkündür. Son yıllarda meydana gelen bu teknolojik gelişmelerden bazıları aşağıda sıralanmıştır.

İlk olarak bireylerin günlük hayatlarında iç içe oldukları pek çok eşyanın ve nesnenin özellikle son yıllarda giderek "akıllanmakta" olduğunu söylemek mümkündür. İnternetin ve teknolojinin eşyaların bünyelerinde kullanılmaya başlamasıyla birlikte artık eşyalar geleneksel eşyalar olmaktan çıkıp akıllı eşyalar sınıfına geçiş yapmaktadırlar. İlk olarak 1999 yılında Kevin Ashton tarafından kullanılan bir kavram olarak "nesnelerin interneti" ile birlikte artık insan yapımı olan eşyaların da akıllanmaya başladıkları görülmektedir (Ashton, 2009). Daha önceleri ancak bireylerin aktiviteleri sonucu harekete geçen ve belirli faaliyetleri gerçekleştiren televizyon, cep telefonu, çamaşır makinesi, bulaşık makinesi vb. eşyalar artık internete bağlı olarak belirli faaliyetleri kendi kendilerine gerçekleştirebilmekte, birbirleriyle etkileşim içerisinde çalışabilmekte, ihtiyaç duyabilecekleri bilgiye internet üzerinden ulaşıp kullanabilmekte ve bireyler ile iletişim içerisinde olabilmektedirler.

İkinci olarak son yıllarda meydana gelen önemli teknolojik gelişmelerden bir diğeri günlük hayattaki alışverişlerde kullanılan gerçek paraların ya da kredi/banka kartlarının yerini internet ortamında şifreyle korunan ortamlarda saklanan sanal paralara ya da başka bir tabirle kripto paralara bırakmasıdır. Günümüzde piyasada kripto paralar sınıfında değerlendirilebilecek olan binden fazla para türü bulunmakta olup (Bitcoin, Ethereum, Ripple, Litecoin, Dash, Monero, Neo, Nem vb.), bu paraların sanal olmaları fiziksel olarak basılı halde bulunmayıp, bilgisayar sisteminde kayıtlı olmalarından kaynaklanmaktadır (Eğilmez, 2017). Her ne kadar henüz sınırlı sayıda birey tarafından kullanılmakta olsalar da bu kripto paraların giderek yaygınlaşmakta olduğunu ve gelecekte gerçek paraların yerini almalarının son derece muhtemel olabileceğini öngörmek mümkündür.

Son yıllarda meydana gelen önemli teknolojik gelişmelerden üçüncüsünü ise robotik teknolojilerde meydana gelen gelişmeler oluşturmaktadır. Günümüzde robotik teknolojiler özellikle Amerika, Almanya, Japonya, Çin ve Güney Kore gibi ülkelerin liderliğinde giderek artan bir hızla gelişmekte ve her geçen gün yeni eklenen özelliklerle birlikte kabiliyetleri çeşitlenmektedir. Robotik teknolojilerin kullanım alanları endüstriyel alandan, askeri alana, tıp sektöründen, inşaat sektörüne, gıda sektöründen, tekstil sektörüne ve daha pek çok alana doğru hızla genişlemektedir. Robotik teknolojilerdeki gelişmeler ile birlikte giderek insana yaklaşan ve hatta bazı noktalarda

insandan çok daha üstün özelliklere sahip olarak kusursuz şekilde çalışan robotların insan hayatına nüfuzunun giderek artması, günlük hayatı pek çok anlamda kolaylaştırmanın yanında robotların insanlara bir alternatif olarak işgücü ve istihdam piyasalarına olan etkilerinin giderek artması da işsizlik oranlarının yükselmesine neden olabilecektir. Aynı şekilde günlük hayatta robotların sayısındaki artışla birlikte bunlara yapılacak siber saldırıların sayılarında da bir artış riskinin meydana gelmesi söz konusu olabilecektir.

Son yılların teknolojik gelişmelerinden dördüncüsünü ise yapay zeka oluşturmaktadır. En sade şekliyle makine ve/veya yazılımlar tarafından sergilenen zihinsel süreç işletebilme yeteneği olarak tanımlanabilecek olan yapay zekanın odağında makine ve/veya yazılımların neden-sonuç ilişkisi kurma, öğrenme, planlama, algılama ve tahmin yürütme yeteneklerinin geliştirilmesi yer almaktadır (Mevlütoğlu, 2016, ss. 4-5). Bilim kurgu edebiyatı ve sinemasında yoğun şekilde işlenen yapay zeka, günümüzde kişisel uygulamalar, ekonomi, savunma sistemleri, otomasyon ve üretim araçları gibi çok geniş bir alanda kullanılmaktadır (Mevlütoğlu, 2016, s. 5). Robotik teknolojilerle de bir arada kullanılabilen yapay zeka uygulamalarıyla ilgili 2017 yılı temmuz ayında çıkan bir haber ise yapay zekanın risklerini ortaya koyar niteliktedir. İngiliz haber sitesi Independent'da yayınlanan habere göre Facebook tarafından geliştirilen iki yapay zeka programı kendi aralarında yalnızca birbirlerinin anlayabileceği bir dilde konuşmaya başlayınca Facebook tarafından program sonlandırılmıştır (Griffin, 2017).

Sonuç olarak bireyler artık günlük yaşamlarında teknolojiyle ve internetle iç içe yaşamaktadırlar ve bireylerin içinde yaşamakta oldukları gerçek dünya yerini giderek sanal dünyaya bırakmaktadır. Teknolojik gelişimin sonucu olarak ortaya çıkan akıllı eşyalar, robotik teknolojiler, yapay zeka, nesnelerin interneti ve sanal para birimlerinin yaygınlaşması gibi konular da insanlığa sunmuş oldukları imkanların ve kolaylıkların yanında siber saldırılara açık olma ve bireyleri siber zafiyetlerle daha çok karşı karşıya bırakma gibi riskleri de bünyelerinde taşımaktadırlar. Nitekim yine Cybersecurity Ventures tarafından yayınlanan 2017 Siber Güvenlik Raporu'na göre siber suçların dünyaya verdiği zararın miktarının 2021 yılına kadar yılda 6 trilyon doları bulacağı tahmin edilmektedir (Morgan, 2017, s. 3).

2.1.3. Kavram Sorunu – Siber Suçlar mı? Bilişim Suçları mı? İnternet Suçları mı?...

Siber suçlar ve siber saldırılar bu denli önemli olan ve gelişen teknolojilerle de birlikte önemi giderek artan konular olmakla birlikte siber suçlar konusunda henüz uluslararası alanda uzlaşılmış bir tanım bulunmamaktadır. Dijital ortamda ya da dijital ortamın sağladığı kolaylıklardan faydalanmak suretiyle işlenen suçlar için günümüzde siber suçlar kavramının yanında bilişim suçları, bilgisayar suçları, internet suçları, online suçlar, bilgisayarla ilişkili suçlar, teknoloji suçları, yüksek teknoloji suçları, elektronik suçlar ve bilgi çağı suçları gibi pek çok tanımlama kullanılmaktadır (Ngo & Jaishankar, 2017, s. 2). Esasında tüm bu tanımlamaların kesişmekte olduğu bazı alanlar bulunmakla birlikte, birbirlerinden ayrılmakta oldukları alanlar da söz konusudur. Sözgelimi Türkiye'de literatürde daha yoğun bir şekilde kullanılmakta olduğu görülen "bilişim suçları" tanımlaması internet suçlarının (ya da online suçların) atıfta bulunduğu alana da atıfta bulunmakla birlikte internetin bulunmadığı ortamlarda işlenmekte olan suçları da içine alarak daha kapsayıcı bir tanımlama oluşturmaktadır. Örneğin online hırsızlık suçu hem internet suçları tanımlamasının hem de bilişim suçları tanımlamasının sınırları içerisinde yer alan bir suç türü iken, internete bağlı olmayan bir bilgisayarda yer alan verilerin ele geçirilmesi suçu için internet suçları tanımlaması yeterli olmayacak ve daha kapsayıcı bir tanımlama olarak örneğin bilişim suçları tanımlamasını kullanmak gerekecektir. Clough (2015, s. 9) bu noktada kelimesi kelimesine kullanılacak her tanımlamanın bir veya birden fazla eksikliğinin bulunduğunu belirtmektedir. Örneğin "bilgisayar suçları" benzeri "bilgisayarlar"a odaklanan tanımlamalar, ağları kapsamayacak olup; "siber suçlar" ya da "sanal suçlar" tanımlamaları özellikle internete odaklanıyor gibi algılanabilecek; "dijital", "elektronik" ve "yüksek teknoloji" suçları tanımlamaları ise nanoteknoloji benzeri diğer yüksek teknoloji suçlarını da kapsayarak ağ tabanlı bilgi teknolojilerinin de ötesine geçebilecektir (Clough, 2015, s. 9). Bununla birlikte Clough (2015, s. 9) bu tarz kavramlara kelime kelime yaklaşmaktan ziyade teknolojinin suçların işlenmesindeki rolüne odaklanan daha geniş, tanımlayıcı kavramlar şeklinde yaklaşmak gerektiğini de belirtmektedir. Dolayısıyla bu noktada hem kapsayıcı olacak olan hem de günlük ve akademik dilde istenilen noktaya atıfta bulunabilecek olan bir tanımlamaya (kavramlaştırmaya) ihtiyaç duyulduğu söylenebilir.

Türkiye'de ve uluslararası alanda bu konuda kullanılan kavramlar incelendiğinde öncelikle Türkiye'de suç türleri ve cezalar konusundaki ana kanun sayılan ve halihazırda yürürlükte bulunan 5237 sayılı Türk Ceza Kanunu (TCK)'na bakılabilir. 5237 sayılı TCK'nın siber suçlarla ilgili olan Onuncu Bölümü "Bilişim Alanında Suçlar" başlığını taşımaktadır. Dolayısıyla 5237 sayılı TCK'nın yukarıda bahsedilen kavramlar içerisinde "Bilişim Suçları" kavramını benimsediği söylenebilecektir. Bunun yanında Türkiye'deki kanun uygulayıcı konumundaki birimlere bakıldığında ise ilk olarak Emniyet Genel Müdürlüğü bünyesinde siber suçlarla ilgilenen ana birimin 2011 yılında "Bilişim Suçlarıyla Mücadele Daire Başkanlığı" adıyla kurulduğu görülmektedir (EGM, 2016). Bununla birlikte bu Daire Başkanlığının adı 2013 yılında İçişleri Bakanlığının oluruyla "Siber Suçlarla Mücadele Daire Başkanlığı" olarak değiştirilmiştir (EGM, 2016). Yine Türkiye'de 81 İl Emniyet Müdürlüklerinin altında siber suçlarla ilgilenen birimlerin her biri de mevcut durumda "Siber Suçlarla Mücadele Şube Müdürlüğü" adı altında faaliyet göstermektedirler. Diğer yandan Türkiye'deki bir diğer kanun uygulayıcı birim olan Jandarma Genel Komutanlığı'na bakıldığında ise merkezde "Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı Siber Suçlarla Mücadele Şube Müdürlüğü", İl Jandarma Komutanlıklarında ise "Siber Suçlarla Mücadele Kısımları" şeklinde yapılanıldığı görülmektedir (Jandarma Genel Komutanlığı, 2017). Dolayısıyla Türkiye'de kanunda "Bilişim Suçları" kavramı benimsenmişken kanun uygulayıcı makamların ise "Siber Suçlar" kavramına yönelmiş oldukları görülmektedir.

Amerika Birleşik Devletleri (ABD)'ne bakıldığında ise öncelikle Adalet Bakanlığı'nda siber suçlarla ilgilenen birim olarak Criminal Division (Ceza Dairesi) altında "The Computer Crime and Intellectual Property Section" (Bilgisayar Suçları ve Fikri Mülkiyet Birimi)'nin bulunduğu görülmektedir. Aynı şekilde ABD kanunlarına bakıldığında ise ABD Yasası'nın Suç Kontrolü ve Kanun Uygulama başlıklı 34. başlığı altındaki Özel Suçların Önlenmesi başlıklı 3. alt başlık içerisinde yer alan 301. Bölümün "Bilgisayar Suçları ve Fikri Mülkiyet Suçları" başlığını taşıdığı görülmektedir. Bununla birlikte ABD'de istihbarattan ve kanun uygulayıcı birim olmaktan sorumlu olan Federal Soruşturma Bürosu (FBI)'nun altında "Suç, Siber, Müdahale ve Hizmetler Şubesi" adlı bir birimin bulunduğu, bu birimin altında ise "Cyber Division (Siber Dairesi)" biriminin faaliyet gösterdiği görülmektedir (FBI, 2017a). Aynı şekilde FBI'ın web sayfasında "neyi soruşturuyoruz" başlığı altında da "siber suçlar" kavramına yer vermiş olduğu

görülmektedir (FBI, 2017b). Dolayısıyla ABD kanunlarında "bilgisayar suçları" kavramı kullanılmakta iken kanun uygulayıcı birimin ise "siber suçlar" kavramını kullanmakta olduğu görülmektedir.

Diğer yandan Avrupa Birliği'nde ise "siber suçlar" kavramının benimsenmiş ve kullanılmakta olduğu söylenebilir (European Commission, 2017). Avrupa Birliği'nin siber suçlarla mücadele için "Avrupa Birliği Siber Güvenlik Stratejisi" ile "Council of Europe – Convention on Cybercrime (Avrupa Konseyi – Siber Suçlar Sözleşmesi)"ı oluşturmuş olduğu ve yine Avrupa Birliği Polis Teşkilatı Europol içerisinde ise 2013 yılından bu yana European Cybercrime Centre (Avrupa Siber Suç Merkezi)'ın faaliyet göstermekte olduğu görülmektedir (Europol, 2017).

Dolayısıyla özellikle Türkiye, ABD ve Avrupa Birliği örnekleri incelendiğinde her ne kadar farklı ülkelerde farklı kavramlar daha yoğunluklu olarak kullanılıyor olsa da "siber suçlar" kavramının diğer kavramlara göre daha ağırlıklı olarak kullanılmakta olduğunu söylemek mümkündür.

Bunlara ilave olarak "siber suçlar" kavramını diğer kavramlara nazaran daha öne çıkaran başka bazı hususlardan da söz etmek mümkündür. İlk olarak örneğin bu çalışmanın ana konusunu oluşturan siber suç korkusu literatürü incelendiğinde literatürde "siber suçlar" kavramının oldukça ağırlıkta olduğunu söylemek mümkündür (bkz. Alshalan, 2006; Clough, 2015; Gordon & Ford, 2006; P. Grabosky, Smith, & Urbas, 2004; Holt & Bossler, 2008; Meško & Bernik, 2011; Wall, 2008a; Yu, 2014). İkinci olarak her ne kadar "siber" kavramı teknik olarak internet ile bağlantılı suçlarla sınırlı olsa da, daha geniş olarak bağımsız bilgisayarlar tarafından işlenen suçlar için de kullanılmaktadır (P. N. Grabosky, 2007, p. 2'den akt. Clough, 2015, p. 9). Üçüncü olarak her ne kadar "siber" kavramı İngilizce kökenli bir kavram olsa da günümüzde Türkiye'de ve diğer ülkelerde (örneğin AB ülkeleri vb.) günlük dile girmeyi başarmış ve yoğun şekilde de kullanılır hale gelmiştir.

Dolayısıyla bu çalışmada da tüm bu nedenlerden ötürü "siber suçlar" kavramı benimsenmiştir. Bununla birlikte Türkiye'de özellikle hukuk alanında yoğun şekilde kullanılmakta olan "bilişim suçları" kavramının da diğer tanımlamalara nazaran daha kapsayıcı ve kullanıma uygun bir tanımlama olduğunu söylemek mümkündür.

2.1.4. Siber Suç Tanımlaması

Her şeyden önce literatürde çoğu siber suçların geleneksel suçların yeni yöntemlerle işlenen versiyonları olduğu ve dolayısıyla "old wine in new bottles (yeni kaplardaki eski şaraplar)" benzetmesini taşıyabileceği belirtilmektedir (Brenner, 2006, s. 384; P. N. Grabosky, 2001). Yani örneğin hırsızlık ya da dolandırıcılık suçunun internet üzerinden işlenmesi geleneksel bir suç türünün yeni bir yöntem ile işlenmesi olarak görülebilecek ve dolayısıyla siber suçlar da son tahlilde bir geleneksel suç çeşidi olmuş olacaktır. Fakat bununla birlikte eski şarapların yeni kaplarda sunumu şeklinde tarif edemeyeceğimiz ve tümüyle yeni olan siber suçlar da bulunmaktadır ki, örneğin DDOS saldırıları bu siber suçlara bir örnek teşkil eder (Brenner, 2006, s. 384). Dolayısıyla siber suçlar konusunda yapılacak olan tanımlamaların eski suçlar ile birlikte bu yeni suçları da kapsaması gerekmektedir.

İkinci olarak yine siber suçlar konusundaki bir tanımlamanın yalnızca internete ya da başka bir ağa bağlı olan bilgisayarları vb. değil hiçbir ağa bağlı olmayan bilgisayarları vb. de içermesi gerekmektedir (Brenner, 2006, s. 386). Zira siber suçlar herhangi bir ağa bağlı olmayan ve tamamen bağımsız olarak çalışmakta olan bilgisayarlarda da işlenebilen suçlar olarak karşımıza çıkmaktadırlar.

Bu bağlamda siber suç konusundaki tanımlamalar incelendiğinde ilk olarak Avrupa Konseyi Siber Suçlar Sözleşmesine bakılabilir. Avrupa Konseyi Siber Suçlar Sözleşmesi (COE Convention on Cybercrime) 1. Bölümü altında yer alan "tanımlar" başlıklı maddesinde "bilgisayar verisi", "bilgisayar sistemi", "servis sağlayıcı" ve "trafik verisi" tanımlarına yer vermekle birlikte siber suç tanımına yer vermemiştir (Europe, 2001, s. 4). Bununla birlikte giriş bölümünde "bilgisayar sistemlerinin, ağların ve bilgisayar verilerinin gizlilik, bütünlük ve erişilebilirlikleri aleyhine olan fiiller ile bu sistemler, ağlar ve verilerin kötüye kullanımı" olarak adlandırılan fiilleri caydırmak ve suç olarak tanımlamak için bu sözleşmenin gerekli olduğuna değinilmekle esasen açıkça olmasa da bir siber suç tanımı yapmakta olduğu söylenebilecektir (Europe, 2001, s. 2). Avrupa Konseyi Siber Suçlar Sözleşmesi'nin siber suçlara ilişkin sınıflandırmayı ise aşağıdaki şekilde 4 başlık altında yapmakta olduğu görülmektedir (Europe, 2001, ss. 4-7);

1. Bilgisayar verileri ve sistemlerinin gizlilik, bütünlük ve erişilebilirlikleri aleyhine olan fiiller,
2. Bilgisayarlara ilişkin suçlar,
3. İçeriğe ilişkin suçlar,
4. Kopyalama vb. hakların ihlaline ilişkin suçlar.

Bazı çalışmalar bu sınıflandırmanın kategoriler arasında ayrım yapmak için tek bir kriter kullanılmaması ve bunun da kategoriler arasında çakışmalar oluşturması nedeniyle tümüyle tutarlı olmadığını savunmakta, bununla birlikte yine de bu dört kategorinin siber suç olgusunu tartışmada yararlı bir temel olabileceğini belirtmektedirler (Gercke, 2012, s. 12).

Diğer yandan siber suçlara ilişkin yabancı kökenli bir kavram olmasından da kaynaklı olabilecek şekilde Türk Dil Kurumu sözlüğünde bir karşılık bulunmamaktadır. Bununla birlikte Oxford Sözlüğü (2017) ise siber suçlar için "bilgisayarlar veya internet vasıtasıyla işlenen suç fiilleri" şeklinde bir tanımlamada bulunmaktadır. Bu tanımlama yukarıda bahsedildiği üzere bilgisayarları ve interneti içine alan bir tanımlama olmakla birlikte ağları göz ardı eden bir tanımlama olarak göze çarpmaktadır. Aynı şekilde bu tanımlamanın bilgisayarların hedef olarak kullanıldığı siber suçları da kapsam dışında bırakmakta olduğu söylenebilecektir.

Merriam-Webster (2017) sözlüğü ise oldukça geniş bir tanımlamayla "(hırsızlık, dolandırıcılık, mülkiyet ihlalleri veya çocuk pornografisinin yayılması gibi) elektronik olarak işlenen suçlar" tanımlamasını kullanmaktadır ki bu tanımlamanın biraz da geniş olarak yapılmasından kaynaklanan bir muğlaklığı bulunmaktadır.

Bu tanımlamalarla birlikte Clough (2015, s. 10) terminolojideki değişen kavram kullanımlarıyla birlikte günümüzde tüm bu siber suçlar vb. kavramların neyi kapsamakta olduğuna ilişkin bir uzlaşının da oluşmuş olduğunu ve bunun Amerikan Adalet Bakanlığı'nca da benimsenmiş olan üç aşamalı bir sınıflandırma olduğunu belirtmektedir. Bu sınıflandırma şu şekildedir (US Department of Justice, 1996'dan akt. Clough, 2015, p. 10);

1. Bilgisayarların ya da bilgisayar ağlarının suç faaliyetinin hedefi olduğu suçlar. Örneğin, hacking, malware ve DoS saldırıları.
2. Bilgisayarların suç işlemede bir araç olarak kullanıldığı mevcut suçlar. Örneğin, çocuk pornografisi, taciz etme, telif hakkı ihlali ve dolandırıcılık.
3. Bilgisayar kullanımının suçun işlenmesinin arızi (incidental) bir yönünü oluşturduğu fakat suçun delili olabildiği suçlar. Örneğin, cinayet şüphelisinin bilgisayarında bulunan adresler ya da suçlu ve mağdur arasında cinayetten önce gerçekleşen görüşmelere ilişkin telefon kayıtları. Bu tarz durumlarda bilgisayar suçun işlenmesine özellikle dahil edilmemekle birlikte daha çok bir kanıt havuzu konumunda bulunmaktadır.

Dolayısıyla bu tanımlamadan bilgisayar suçları, bilgisayarla kolaylaştırılmış suçlar ve bilgisayar destekli suçlar olmak üzere üçlü bir sınıflandırmanın ortaya çıktığı görülmektedir (Clough, 2015, s. 10). Kanaatimce bu noktada "bilgisayar" kavramı ile "bilişim sistemi" kavramlarının birbirleriyle aynı noktaya atıfta bulunup bulunmadıkları konusu tartışmaya açılabilir. Eğer bu sınıflandırmada kullanılmakta olan ve ABD kanunlarında da yer almakta olan "bilgisayar" kavramı ile kastedilmek istenen tüm "bilişim sistemleri" ise (ki öyle gözükmektedir) bu noktada çok bir problem oluşmayacaktır. Ancak yine de "bilgisayar" kavramı yerine Türk hukuk sisteminde de kullanılmakta olan "bilişim sistemi" kavramının kullanılması bu noktada daha kapsayıcı bir tanımlama oluşturacak ve bilgisayarlar dışındaki sistemlerin de bu tanımın sınırları içerisine girmesi sağlanmış olacaktır. Nitekim Karagülmez (2011:44'den akt. Hekim & Başıbüyük, 2013, s. 136) de siber suçlar ile ilgili olarak kullanılmakta olan kavramlar her ne kadar birbirlerinden farklı olsalar da bu kavramlar ile anlatılmak istenenin genellikle "bilişim sistemine yönelik veya bilişim sisteminin kullanıldığı suçlar" olduğunu belirtmektedir.

Sonuç olarak siber suçlar konusunda yapılmakta olan tanımlamaların birçoğu esasında benzer noktalara atıfta bulunsalar da bu çalışma açısından bir tanımlamanın benimsenmesi gerekebilir. Bu noktada kanaatimce "siber suçlar" için Avrupa Siber Suçlar Sözleşmesinde açık bir şekilde olmasa da yapılmakta olan tanımlamayı bir miktar değiştirerek "Bilişim sistemlerinin, ağların ve bilişim sistemlerinde yer alan verilerin

gizlilik, bütünlük ve erişilebilirlikleri aleyhine olan fiiller ile bu sistemlerin, ağların ve verilerin kötüye kullanımı" şeklinde bir tanımlama oluşturulabilecektir.

Tüm bu tanımlama tartışmalarıyla birlikte bir tanımlama yapılmasının gerekli olup olmadığı da literatürde tartışılmıştır. Finklea ve Theohary (2015) bu sorunun cevabının bir tanımlama yapılmasının amacının ne olduğuna göre değişeceğini belirtir. Bir yandan eğer siber suçları tanımlamanın amacı çeşitli suçları daha geniş bir siber suç şemsiyesi altında soruşturmak ve kovuşturmak ise şemsiye bir siber suç tanımlaması yapmanın önemi azalabilir ve hangi spesifik aktivitelerin suç oluşturacağını tanımlamak yeterli olabilir (Finklea & Theohary, 2015, s. 16). Fakat diğer yandan siber suçlar ile diğer zararlı aktiviteler arasında bir ayrım yapmak, siber tehditlerin giderek artan çeşitliliği ile mücadele etmek adına spesifik politikalar geliştirmekte yararlı olabilir ki bu noktada da ortak bir tanım geliştirmek daha önem arz eder hale gelebilir (Finklea & Theohary, 2015, s. 16).

Bununla birlikte kanaatimce bir siber suç tanımlaması yapmak her halükarda önemlilik ve gereklilik arz eden bir konudur. Zira özellikle ceza hukuku açısından belirli ve herkesin anlayabileceği netlikte bir suç tanımlaması oluşturmaksızın belirli fiiller karşılığında cezalar öngörmek her şeyden önce kanunlara uygun fiiller işlemek durumunda olan bireyler için bir sorun oluşturacaktır.

Diğer yandan belirli bir konuyu ele almakta olan herhangi bir bilimsel çalışmanın da o konunun kavramsal olarak ne anlama geldiğine ilişkin en azından bir varsayımı kabul etmesi gerekir ki bu da siber suçları konu edinen bu çalışma ya da diğer çalışmalar için siber suçlara ilişkin tanımlamaları irdelemeyi ve en azından belirli özelliklere sahip bir tanımlama üzerinde yoğunlaşmayı zorunlu kılar. Aksi takdirde yapılan çalışmanın kavramsal temeli zayıf olacağından bu kavramsal temel üzerine inşa edilecek olan çalışmanın da zayıf kalması muhtemel olacaktır.

2.2. SİBER SUÇ KORKUSU

2.2.1. Suç Korkusu ve Siber Suç Korkusu

Öncelikle bu tezin Sosyoloji bölümünde yazılmış olan bir tez olması nedeniyle tezin ana konusunu oluşturan suç korkusunun da sosyoloji ile olan ilgisinin ne olduğu tartışılmalıdır. Sosyolojinin başlıca konularından birisini de sosyal olguların incelenmesi oluşturmaktadır. Bu bağlamda suç korkusunun da bir sosyal olgu olduğunu savunan bazı çalışmalardan bahsetmek mümkündür (Conklin, 1975; Goodstein & Shotland, 1980; Hartnagel, 1979; Clarke & Lewis, 1982; Garofalo, 1979; Liska, Sanchirico, & Reed, 1988; Skogan & Maxfield, 1981; Yin, 1985'den akt. Liska & Warner, 1991, s. 1444; Liska, Lawrence, & Sanchirico, 1982; Liska & Warner, 1991). Bu çalışmalar arasında örneğin Conklin, 1975; Goodstein & Shotland, 1980; Hartnagel, 1979 (akt. Liska & Warner, 1991, s. 1444) suç korkusunun toplumda sosyal etkileşimleri yoğunlaştırmaktan ziyade sınırlandırdığını ve kısıtladığını ve bu yüzden de sosyal yardımlaşma ve dayanışmayı azalttığını belirtmektedirler. Aynı şekilde Clarke & Lewis, 1982; Garofalo, 1979; Liska vd., 1988; Skogan & Maxfield, 1981; Yin, 1985 (akt. Liska & Warner, 1991, s. 1444) ise suçtan korkan bireylerin sosyal davranışlarını güvenli zamanlardaki güvenli alanlarla sınırlandırdıklarını, şehrin güvensiz alanlarından ve bu alanlardaki iş yerleri ile meskenlerden kaçındıklarını ve güvensiz alanlarda yaşamaktan kaçınamayan insanların ise sıklıkla kendi evlerinin mahkumları haline geldiklerini ve kendi mahallelerinde sokağa çıkmaktan korktuklarını belirtmektedirler. Yine Hale (1996, s. 2) ise çalışmasında suç korkusunun bireylerin yaşam kaliteleri üzerinde etkiye sahip olduğunu belirtmektedir. Hale (1996, s. 2) ayrıca suç korkusunun toplumda fakirler ve zenginler ya da özel güvenlik önlemleri alabilenler ve alamayanlar arasındaki sosyal bölünmeleri artırabileceğini savunmaktadır. Dolayısıyla tüm bu örneklerden de hareketle suç korkusunun bireylerin sosyal davranışlarını, sosyal etkileşimlerini ve yaşam kalitelerini etkileyen ve toplumda bölünmeler oluşturabilen sosyal bir olgu olduğunu söylemek mümkündür. Bununla birlikte bu örneklerin ve suç korkusu literatüründe yer alan diğer çalışmaların genellikle geleneksel suçlara odaklanan bir yapıda oldukları yukarıda belirtilmiştir. Fakat siber suç korkusuna gelindiğinde ise durumun bireylerin kendi evlerinden çıkmaya korkar hale gelmelerine neden olan bir durumdan daha öte olduğu

söylenebilecektir. Bireyler bu sefer kendi evlerinde veya kendilerini en güvende hissettikleri ortamlarda dahi bir siber suçtan mağdur olma durumuyla karşı karşıya kalabilmektedirler. Dolayısıyla bireylerin sosyal davranışlarını etkileyen bir sosyal olgu olarak suç korkusu, siber suç korkusuna gelindiğinde bireylerin siber ortamdaki davranışlarını ve etkileşimlerini etkileyen bir yapıya bürünmektedir. Bu noktada bireylerin siber alandaki davranışlarının ve bu davranışları etkileyen olguların sosyolojinin sınırları içerisine girip girmediği de tartışılabilir. Bu konuda dijital sosyoloji tartışmalarıyla da birlikte sanal alemin bireyler için bir toplumsal ilişkiler alanı olduğu (Kılıç, 2012), sanal alemde bir "toplumsanallaşma" bulunduğu (Kurt, 2012) ve bireylerin sosyal medya vb. ortamlarda sanal aidiyetler oluşturmakta oldukları (Elitaş & Keskin, 2014) gibi konulara da literatürde değinilmektedir. Dolayısıyla kanaatimce günümüzde bireylerin siber dünyadaki sosyalleşmeleri ve etkileşimleri de en az gerçek dünyadakiler kadar önemli ve incelemeye değer olup, sosyolojinin de sınırları içerisinde yer almaktadır.

Bu değerlendirmelerin ardından suç korkusu konusuna geçilebilir. Suç korkusu, kriminoloji içerisinde bir araştırma konusu olarak suçun kendisinden bağımsız olarak çalışılabilecek ayrı bir alt disiplin haline gelmiştir (Hale, 1996, s. 52). Toplumsal hayatta bireylerin her zaman karşı karşıya kalabilecekleri bir olgu olarak suç olgusunun bireyler üzerinde bir korku oluşturması son derece muhtemeldir. Her ne kadar korku konusu daha çok psikolojinin alanına giren bir konu olsa da davranışsal düzeydeki yansımaları açısından sosyolojik olarak da ele alınması gereken önemli bir konudur. Zira literatürde suç korkusu olarak adlandırılmış olsa da bireylerin suçlar karşısında hissetmiş oldukları duygunun ne olduğu tartışmalıdır. Yani bireyler suçtan korkmakta mıdırlar, endişe mi duymaktadırlar, kaygılanmakta mıdırlar ya da telaşlanmakta mıdırlar? Suç korkusunun Ferraro ve Grange (1987, s. 71) tarafından yapılan tanımı şu şekildedir: "bireylerin başkalarına ya da kendilerine karşı olan suçtan ya da suçla ilişkilendirdikleri sembollerden doğan duygusal reaksiyonlar". Bu tanımda da görüleceği üzere suç korkusu için korku, endişe, kaygı vb. spesifik bir kavram yerine duygusal reaksiyonlar şeklinde şemsiye bir kavram kullanılmıştır. Dolayısıyla bu çalışma açısından da suç korkusunun her türlü korku, endişe, kaygı ve telaşı içine alan bir şekilde kullanılmış olduğu belirtilmelidir. Bu noktada korkunun bir mağduriyet yaşama korkusu olduğu düşünülebilir. Burada bahsedilmekte olan mağduriyet bireyin doğrudan kendisine yönelik

olabileceği gibi dolaylı olarak örneğin bir yakını üzerinden de olabilecektir. Aynı şekilde bireyin kendisiyle hiçbir bağı ya da yakınlığı olmayan bir kişiye karşı işlenecek olan suçtan medya vb. kanalıyla haberdar olarak en azından psikolojik bir mağduriyet yaşaması da ihtimal dahilindedir. Sonuç olarak suç korkusunun suçtan mağdur olma korkusu ve siber suç korkusunun da siber suçlardan mağdur olma korkusu olduğu görülmektedir. Dolayısıyla bu çalışmadaki anket sorularının da bu husus göz önünde bulundurularak hazırlandığı belirtilmelidir.

Literatürde suç korkusu ile risk algısının birbirleriyle karıştırıldıklarına değinilmektedir (Alshalan, 2006, s. 34). Suç korkusunun tanımı yukarıda verilmişken risk algısı ise "bireylerin suç oranlarına ilişkin değerlendirmeleri ve mağduriyet olasılıkları" olarak tanımlanmaktadır (Alshalan, 2006, s. 34). Bu iki kavram oldukça dikkat çekmiş olup, suç korkusu duygusal bir tepkiyi, risk algısı ise bilişsel bir hükmü gerektirmektedir, dolayısıyla da bir mağduriyet riski algılaması, bireyin suçtan korktuğu anlamına gelmemektedir (Alshalan, 2006, s. 34). Bu noktada Ferraro ve Grange (1987, s. 72) suça ilişkin algıları sınıflandırmış ve risk ile korkuyu da birbirlerinden ayırmak adına DuBow (1979)'dan uyarlayarak aşağıdaki şekilde bir tablo hazırlamışlardır:

Tablo 3. Suça İlişkin Algılar (DuBow, 1979'dan uyarlayan Ferraro ve Grange, 1987)

	Algının Türü		
	Bilişsel		**Duygusal**
Referans seviyesi	**Yargılar**	**Değerler**	**Duygular**
Genel	Diğerlerine olan risk; suç veya güvenlik değerlendirmeleri	Diğerlerine olan suçla ilgililik	Diğerlerinin mağduriyeti için korku
Kişisel	Kendine olan risk; öz güvenlik	Kendine olan suçla ilgililik; kişisel tahammülsüzlük	Kendi mağduriyeti için korku

Suç korkusu 1960'lı yıllardan itibaren hem akademik alanda hem de politika oluşturma konusunda başlıca konulardan birisi haline gelmiştir (Hale, 1996, s. 1). Bununla birlikte siber suç korkusu literatürünün ise, siber suçların ortaya çıkışının gerçek suçlara nazaran oldukça yeni olmasının da bir sonucu olarak, suç korkusu literatürüne göre yeni yeni

oluşmakta olduğu ve ondan daha dar olduğu söylenebilir. Suç korkusu literatürü incelendiğinde literatürün özellikle yukarıdaki Şekil 1.'de yer almakta olan geleneksel suçlardan mağdur olma korkusu üzerine oluşmuş olduğu görülmektedir. Diğer yandan siber suç korkusu literatürünün ise yukarıdaki şemada daha çok siber suçlar ve siber alanın yardımıyla işlenen geleneksel suçlardan mağdur olma korkusu üzerine oluşmuş olduğu söylenebilir. Bunun yanında suç korkusu ve siber suç korkusu konusunun birbirleriyle aynı seviyede mi yer aldıkları yoksa aralarında bir hiyerarşi mi olduğu konusu tartışılabilir. Her ne kadar siber suçların da bir suç türü olduğu ve dolayısıyla da suç korkusu konusu altında ele alınabileceği düşünülse de siber suçların, P. N. Grabosky (2001) ve Brenner (2006)'ın da belirttiği gibi "yeni kaplardaki eski şaraplar" olarak adlandırılan formu dışında tamamen yeni ve özgün suçları içermekte olan bir formu da bulunmaktadır ki bu da kanaatimce siber suç korkusunu suç korkusu konusu dışında ve onunla aynı seviyede değerlendirilebilecek bir konuma ulaştırabilecektir.

2.2.2. Siber Suç Korkusunun Belirleyicileri

Suç korkusuna ilişkin belirleyicilerin siber suç korkusu için de geçerli olup olmadığı bir tartışma konusudur (Henson, 2011). Bu konuda yapılmış çalışmalar incelendiğinde bazı belirleyicilerin hem genel olarak suç korkusu hem de siber suç korkusu için ortak belirleyiciler oldukları söylenebilir. Bu belirleyiciler arasında sosyo-demografik özellikler, geçmiş mağduriyet tecrübesi, suç ciddiyeti algısı ve mağduriyet riski algısından söz etmek mümkündür (Henson, 2011). Fakat bunların dışında suç korkusuna özgü olan ve ayrıca siber suç korkusuna özgü olan bazı belirleyicilerden de söz etmek mümkündür. Örneğin Boss vd. (2009, s. 30) siber suçlarda mağdurun suç işlendikten ancak birkaç hafta hatta birkaç ay sonra haberi olabilmesinden hareketle fiziksel çevrenin (bağlam) geleneksel suç korkusunun aksine siber suç korkusu için geçerli bir belirleyici olmadığı sonucuna ulaşmaktadırlar. Diğer yandan internet kullanım davranışlarının ise geleneksel suç korkusuna özgü bir belirleyici olmayıp siber suç korkusu için bir belirleyici olduğu belirtilmiştir (Abdulai, 2016)

Öncelikle Yu (2014, s. 36)'nun yapmış olduğu çalışmada bütün siber suçların siber suç korkusu için aynı belirleyicilere sahip olmadığı sonucuna ulaşılmış olduğu belirtilmelidir. Bir diğer ifadeyle her bir siber suç için birbirlerinden farklı siber suç korkusu

belirleyicileri bulunabilmektedir. Bununla birlikte siber suç korkusu konusunda yapılmış olan çalışmalar incelendiğinde bu çalışmaların siber suç korkusunun muhtemel belirleyicileri olarak bazı başlıklara değinmiş oldukları görülmektedir. Bu başlıkların genel olarak sosyo-demografik faktörler, siber suç bilgisi, internet kullanım davranışları, geçmiş mağduriyet tecrübesi, geleneksel suç korkusu, suç ciddiyeti algısı ve mağduriyet riski algısından oluşmakta oldukları söylenebilir (Abdulai, 2016; Alshalan, 2006; Henson, 2011; Higgins vd., 2008; Roberts vd., 2013; Yu, 2014). Bu noktada daha önce yapılmış olan çalışmalarda bu konuların ne şekilde ele alındığı ve nasıl sonuçlara ulaşıldığına değinmenin faydalı olacağı düşünülmektedir.

2.2.2.1. Sosyo-Demografik Faktörler

Siber suç korkusunun sosyo-demografik belirleyicilerine bakıldığında özellikle cinsiyet, yaş ve ırk değişkenlerinin ön plana çıktığı görülmektedir.

Alshalan (2006, s. 146) çalışmasında kadınların siber suçlardan mağdur olma olasılıklarının daha az olmasına rağmen siber suç korkularının erkeklerden daha fazla olduğu sonucuna ulaşmıştır. Alshalan (2006, s. 146) bunu, kadınların siber suçlar ile cinsel suçları ilişkilendirdikleri varsayımıyla korku genellemesine sahip olmalarına bağlar. Zira bir virüs kapmak ya da hacklenmek kadınların kişisel bilgilerinin ve kimliklerinin çalınması korkusunun artışına neden olabilecek ve böylelikle onlar gizlice izlenebilecek veya taciz edilebileceklerdir (Alshalan, 2006, ss. 146-147). Dolayısıyla Alshalan (2006) için cinsiyetin siber suç korkusu belirleyicilerinden birisi olduğu söylenebilir.

Yaş konusuna bakıldığında ise Alshalan (2006, s. 147) yaşlı bireylerin genç bireylere nazaran daha fazla siber suç korkusuna sahip olduklarını belirtmektedir. Fakat kadınlarda ise genç kadınların yaşlı kadınlara nazaran siber suç korkularının daha fazla olduğu belirtilmektedir (Alshalan, 2006, s. 147). Alshalan (2006, s. 147) bunu yine yukarıda bahsedildiği gibi genç kadınların siber suçları cinsel suçlar ile ilişkilendirebilmeleri ile açıklamaktadır. Sonuç olarak Alshalan (2006)'a göre yaşın da siber suç korkusu için bir belirleyici olabileceği söylenebilir.

Yine Henson (2011, s. 125) da çalışmasında cinsiyetin siber taciz korkusu üzerindeki en tutarlı belirleyiciler arasında bulunduğunu belirtmektedir (kadınlar daha fazla korkmaktadır). Henson (2011, s. 136) ayrıca ilişki durumunun da siber taciz korkusu açısından önemli bir belirleyici olduğunu, bir ilişki içerisindeki bireylerin yalnız bireylere nazaran siber tacizden daha fazla korkmakta olduklarını belirtmektedir.

Abdulai (2016, s. 82) ise üniversite öğrencileri arasındaki kredi/banka kartı dolandırıcılığı mağduriyeti korkusu üzerine yapmış olduğu çalışmada sosyo-demografik faktörler olarak cinsiyet, yaş, evlilik durumu, etnisite ve aile gelir durumuna değinmekte ve bu faktörlerin hiçbirisinin öğrencilerin kredi/banka kartı dolandırıcılığı korkusu üzerinde önemli bir farklılık oluşturmadığını belirtmektedir (yani kadın, yaşı büyük, bekar veya yüksek gelire sahip beyaz olmayan öğrenciler, erkek, yaşı küçük, bekar olmayan ya da düşük gelire sahip beyaz öğrencilere nazaran önemli derecede daha fazla korkuya sahip değillerdir). Bununla birlikte Abdulai (2016, s. 108)'nin her ne kadar analizde önemli çıkmasa da cinsiyetin kredi/banka kartı dolandırıcılığı korkusu ile ilişkili olduğu (kadın öğrencilerde erkek öğrencilere göre neredeyse iki kat daha fazla korku bulunmuştur), fakat bunun dışında iş/çalışma durumu, gelir, yaş, medeni hal, etnik kimlik, öğrenim seviyesi, öğrencilik statüsü (yarı zamanlı-tam zamanlı), oturum statüsü (yerel-uluslararası) ve ikamet yeri (kampüs içi – kampüs dışı) değişkenlerinden hiçbirisinin kredi/banka kartı dolandırıcılığı korkusu ile ilişkili olmadığı sonucuna ulaştığı belirtilmelidir.

Roberts vd. (2013, ss. 1-2) ise yapmış oldukları çalışmada suç korkusunun yaş ve cinsiyet benzeri geleneksel demografik belirleyicilerinin siber kimlik hırsızlığı mağduriyeti korkusu açısından zayıf belirleyiciler olarak gözüktükleri sonucuna ulaşmaktadırlar. Bununla birlikte geleneksel suç korkusu ile internet kullanım davranışları ise görece daha güçlü belirleyiciler olarak bulunmuştur (Roberts vd., 2013, ss. 1-2). Fakat Roberts vd. (2013)'nin çalışmalarının genel olarak siber suç korkusuna değil spesifik olarak tek bir siber suçtan (siber kimlik hırsızlığı) mağdur olmaya ilişkin korkuya odaklanmakta olduğu da dikkate alınmalıdır.

Yu (2014, s. 43)'nun online dolandırıcılık, siber zorbalık, bilgisayar virüsü ve dijital korsanlık korkusu üzerinden yapmış olduğu çalışma ise yukarıda belirtildiği üzere farklı siber suçlara ilişkin korku belirleyicilerinin birbirlerinden farklı olduklarını ortaya koymaktadır. Söz gelimi cinsiyet yalnızca siber zorbalık korkusu açısından bir belirleyici

durumunda iken (kadınlar daha fazla korkmaktadırlar), ırk yalnızca dijital korsanlık korkusu için bir belirleyici durumundadır (kesin olmamakla birlikte ırksal azınlıklar Beyaz/Kafkas'lara göre daha fazla korkmaktadırlar), bununla birlikte yaş ise bu dört siber suçtan hiçbirisi için bir belirleyici olarak bulunamamıştır (Yu, 2014, ss. 41-43).

Henson (2011) ise siber taciz mağduriyeti korkusu üzerine yapmış olduğu çalışmada cinsiyet, ilişki durumu, suçlu tipi ve takip davranışları sıklığının rapor edilen korku seviyesi üzerinde etkili olduğu sonucuna ulaşmıştır. Henson (2011) aynı şekilde geçmiş siber taciz mağduriyeti ile siber taciz mağduriyeti riski algısının da siber taciz mağduriyeti korkusu üzerinde anahtar belirleyiciler arasında yer aldıklarını belirtmektedir.

Higgins vd. (2008) ise yapmış oldukları çalışmada benlik kontrolü, risk algısı ve online mağduriyet korkusu arasında bir ilişki bulunduğu sonucuna ulaşmaktadır. Bu çalışmaya (Higgins vd., 2008, s. 231) göre Facebook kullanımından mağdur olma korkusunu anlamada düşük benlik kontrolü önemli bir konumda yer almaktadır. Daha spesifik olarak, benlik kontrolü ile online mağduriyet korkusu arasındaki bağlantı risk algısı tarafından aracılık edilmektedir.

Ayrıca siber suç korkusu belirleyicisi olabilecek bir diğer konu siber suç bilgisidir. Bununla birlikte bu konuda Abdulai (2016, s. 96) siber suç bilgisi ile spesifik olarak kredi/banka kartı dolandırıcılığı mağduriyeti korkusu arasında önemli bir ilişki bulunmadığı sonucuna ulaşmıştır.

2.2.2.2. İnternet Kullanım Davranışları

Abdulai (2016, ss. 99-100)'nin çalışmasında öğrencilerin internet kullanımı sıklığı ile internette kalma sürelerinin kredi/banka kartı dolandırıcılığı riski üzerinde önemli etkiye sahip olduğu bulunmuştur. İnterneti daha sık kullanan öğrenciler ile internette daha uzun süre kalan öğrenciler interneti daha az kullanan ve internette kalma süreleri daha düşük olan öğrencilere göre daha fazla risk altında bulunmaktadırlar Abdulai (2016, ss. 100-101).

Abdulai (2016, ss. 102-104) aynı zamanda online alışveriş ile online alışveriş sıklığının da öğrencilerin kredi/banka kartı dolandırıcılığı riski üzerinde önemli etkiye sahip olduğu sonucuna ulaşmıştır.

Her ne kadar Abdulai (2016) internet kullanım sıklığı ile internette kalma süresinin kredi/banka kartı dolandırıcılığı riskini artırmakta olduğunu belirtse de Henson (2011, s. 134) siber taciz korkusu açısından internet kullanımı düşük olan öğrencilerin internet kullanımı yüksek olan öğrencilere nazaran siber taciz mağduriyetinden önemli oranda daha fazla korkmakta olduklarını belirtmektedir. Henson (2011, s. 134) bunun interneti daha fazla kullanan öğrencilerin internet kullanımının potansiyel tehditlerini basitçe kabul etmemeleri ile ilişkili olabileceğini belirtir.

Roberts vd. (2013, ss. 1-2) de internet kullanım davranışlarının siber kimlik hırsızlığı korkusu açısından sosyo-demografik faktörlere nazaran göreceli olarak daha güçlü bir belirleyici olduğunu belirtmektedirler. Onlara göre ise (Roberts vd., 2013, s. 20) siber kimlik hırsızlığı korkusu Henson (2011)'un siber taciz korkusu araştırmasının aksine internet kullanımının artmasıyla artmakta ve evde internet kullanan bireylerdeki korku evde internet kullanmayanlara nazaran daha fazla olmaktadır.

Yu (2014, s. 43) ise yapmış olduğu çalışmada online alışveriş, online etkileşim, online yayıncılık ve online indirme gibi internet kullanım davranışlarının da her ne kadar farklı farklı siber suçlar için olsa da siber suç korkusu üzerinde bir belirleyici konumunda olduklarını belirtmektedir.

2.2.2.3. Geçmiş Mağduriyet Tecrübesi

Alshalan (2006, s. 147)'a göre geçmiş mağduriyet tecrübesi siber suç korkusunu artırmaktadır, dolayısıyla da siber suç korkusu için bir belirleyici konumundadır. Bir siber suçtan mağdur olmanın mağdur üzerinde olumsuz etkileri bulunabilir ve bu da mağdur için siber suç korkusu üzerinde etkisi olan bir hassaslaştırma etkisi oluşturur (Alshalan, 2006, s. 147).

Abdulai (2016, s. 96) de geçmiş mağduriyet tecrübesi ile spesifik olarak kredi/banka kartı dolandırıcılığı mağduriyeti korkusu arasında önemli bir ilişki bulunduğu sonucuna

ulaşmıştır. Abdulai (2016, ss. 96-97)'nin çalışmasında geçmişte kredi/banka kartı dolandırıcılığından mağdur olmuş öğrencilerde bu siber suçlardan mağdur olma korkusu, mağduriyet yaşamamış öğrencilere göre daha fazla bulunmuştur.

Aynı şekilde Henson (2011, s. 125) da çalışmasında geçmiş mağduriyetin siber taciz korkusu üzerindeki en tutarlı olarak önemli belirleyicileri arasında bulunduğunu belirtmektedir.

Yu (2014, s. 43) ise mağduriyet tecrübesinin siber zorbalık korkusu ile bilgisayar virüsü korkusu açısından bir belirleyici olduğunu fakat online dolandırıcılık korkusu ile dijital korsanlık korkusu için ise belirleyici olmadığını belirtir.

2.2.2.4. Geleneksel Suç Korkusu

Roberts vd. (2013, ss. 1-2) fiziksel yere dayalı suç korkusunun siber kimlik hırsızlığı korkusu açısından sosyo-demografik faktörlere nazaran göreceli olarak daha güçlü bir belirleyici olduğunu belirtmektedir. Yani geleneksel suç korkusu yüksek olan bireylerde siber kimlik hırsızlığı korkusunun da yüksek olmasını beklemek mümkündür (Roberts vd., 2013, s. 18).

2.2.2.5. Suç Ciddiyeti Algısı

Bireyler siber suçun ciddi bir suç olduğunu düşündüklerinde, onun öyle olmadığını düşünenlere nazaran siber suçlardan daha fazla korkmaktadırlar (Alshalan, 2006, s. 147). Alshalan (2006, s. 147) bunu bireylerin siber suçu ciddi bir suç olarak algıladıklarında onu kendisinden korkmakta oldukları bir geleneksel suç ile ilişkilendirdikleri şeklinde açıklamaktadır. Dolayısıyla suç ciddiyeti algısı da siber suç korkusu açısından bir belirleyici konumuna erişmektedir.

Yine Henson (2011, s. 125) ise suç ciddiyeti algısını dolaylı olarak bir belirleyici kılabilmesi açısından siber taciz korkusu açısından takip davranışlarının sıklığını da önemli bir belirleyici olarak bulunmuştur (Henson, 2011, s. 125). Henson (2011, s. 125)'a

göre takip davranışları sıklığı mağdur açısından suçun ciddiyetine ilişkin algıyı artırabilecek ve bu da mağdur üzerindeki korkuda bir artışa sebep olabilecektir.

Yu (2014, s. 43) ise suç ciddiyeti algısının online dolandırıcılık korkusu ile bilgisayar virüsü korkusu açısından bir belirleyici olduğunu fakat siber zorbalık korkusu ile dijital korsanlık korkusu için ise belirleyici olmadığını belirtir.

2.2.2.6. Mağduriyet Riski Algısı

Mağduriyet riski algısı da yapılan çalışmalarda siber suç korkusunun belirleyicisi olarak bulunan faktörler arasında yer almaktadır. Örneğin Henson (2011, s. 108) siber taciz mağduriyeti üzerine yazmış olduğu tezdeki en önemli ve en güçlü birlikteliklerden birinin siber taciz riski algısı ile siber taciz korkusu arasındaki ilişki olduğunu belirtir. Henson (2011, ss. 108-110) yakın bir partner, bir arkadaş/tanıdık veya bir yabancı tarafından siber taciz edilme riski algısı ile yine yakın bir partner, bir arkadaş/tanıdık veya bir yabancı tarafından siber taciz edilme korkusu arasında istatistiksel olarak önemli ve pozitif bir ilişki bulunduğunu belirtmektedir.

Yu (2014, s. 43) ise mağduriyet riski algısının online dolandırıcılık korkusu ile siber zorbalık korkusu açısından bir belirleyici olduğunu fakat bilgisayar virüsü korkusu ile dijital korsanlık korkusu için ise belirleyici olmadığını belirtir.

Alshalan (2006, s. 147) dolaylı mağduriyetin yani siber suçlardan mağdur olan bir kişiyi tanımanın bireyin mağduriyete karşı olan korunmasızlık hissini güçlendirmediğinden siber suç korkusu için bir belirleyici olmadığını belirtir. Zira bireyler kendilerinin mağdur olmuş olan kişiden daha fazla önlem almakta (daha korunaklı) olduklarını ya da bu tarz bir suçun çok nadir işlendiğini ve kendilerine karşı işlenmeyecek olduğunu düşünerek siber suç korkusu hissetmeyebileceklerdir (Alshalan, 2006, s. 147).

Alshalan (2006, s. 147) internete erişen çocuklara sahip olmanın da siber suç korkusu için bir belirleyici olmadığını belirtmektedir.

Sonuç olarak buradan çıkarılacak en önemli sonuç Yu (2014, s. 43)'nun da ifade ettiği üzere siber suç korkusunun belirleyicileri üzerinde çalışırken suça özel davranmak

gerektiğidir. Yani tüm siber suçlar için belirleyiciler aynı olmayıp her bir siber suç korkusu için farklı belirleyiciler bulunur ve bu da siber suç korkusuna spesifik suçlar temelinde yaklaşmayı zorunlu kılar. Buradan hareketle bu çalışma açısından da oluşturulmuş olan anket soruları spesifik olarak siber suçlardan korkuyu ortaya çıkarma amacını taşımaktadır. Siber suçlar Türk Ceza Kanunu ve ilgili ceza kanunlarından da hareketle ayrı ayrı belirlenmiş ve Ankara'daki teknokent çalışanları açısından bu suçlardan korkma düzeyinin ortaya konulması amaçlanmıştır.

2.3. ÖNLEM ALMA STRATEJİLERİ

Çalışmanın iki ana teması siber suç korkusu ve önlem alma stratejileri olarak belirlenmiştir. Bu iki konunun birlikte alınmasının nedeni, siber suçlardan mağdur olma korkusunun bireyleri bu korkulara karşı belirli stratejiler geliştirmeye yönlendirmesidir. Özellikle teknokent çalışanlarının siber suç korkusunun düzeyi, bu korkunun bireyleri ne tür davranışlara yönlendirdiği, davranış yoğunlukları, bu davranışların çalışılan kurumda ve kurum dışında bir farklılık gösterip göstermediğinin araştırılması, alandaki profesyonellerin bu konudaki yaklaşımlarının tanımlanması ve geliştirilecek önerilere yol gösterici olması açısından önemlidir. Anlaşılacağı üzere şimdiye kadar incelenen literatürde siber suç korkusu ile birlikte önlem alma stratejileri konusuna fazla değinilmemiş olması da bu konunun seçilmesinde rol oynamıştır.

Bireylerin siber suç korkusu ile ilgili olarak geliştirdikleri stratejileri önlem alma ve başa çıkma stratejileri olarak adlandırmak mümkündür. Esasında önlem alma ve başa çıkma stratejileri başlangıçta farklı noktalara atıfta bulunuyor olarak gözükmektedirler. Zira başa çıkma stratejisi belirli bir korkunun ortaya çıkmasının ardından alınan stratejilere atıfta bulunurken, önlem alma stratejileri ise korku oluşmadan önce korkunun oluşmaması adına alınacak olan önlemlere atıfta bulunuyor gibidir. Bununla birlikte korkulduğu için ve korkuyu azaltmak adına geliştirilen fiiller ile korkmamak adına geliştirilen fiiller arasında bir özdeşliğin söz konusu olduğu söylenebilir. Yani siber suç korkusu özelinde siber suç korkusu ile başa çıkma stratejileri ile siber suç korkusuna karşı önlem alma stratejileri esasında birbirleriyle aynı fiiller, önlemler ve stratejileri içermektedirler. Örneğin siber hırsızlıktan mağdur olmaktan korkan bir bireyin bir başa çıkma yolu olarak geliştirmiş olduğu strateji internet ortamında kullanmış olduğu şifreleri

güçlendirmek şeklinde olabilmekte ve bu da esasında bir önlem alma stratejisi ile eşdeğer bir yol olmaktadır. Dolayısıyla bu çalışma açısından da önlem alma ve başa çıkma stratejilerinin aynı noktalara atıfta bulundukları kabul edilmiş ve tez başlığında ise diğerini de kapsayacağı düşüncesiyle bu iki kavramdan önlem alma stratejileri seçilmiştir.

Bu çalışmada Ankara'daki teknokent çalışanlarına uygulanan anket formunda siber suç korkusuna ilişkin önlem alma ve başa çıkma stratejileri olarak oldukça kapsamlı bir soru listesi oluşturulmuştur. Genel olarak kapalı uçlu sorulardan oluşan anket formunda, göz ardı edilmiş olabilecek olan ve katılımcıların kendi geliştirdikleri farklı stratejileri de tespit edebilmek adına açık uçlu bir soruya da yer verilmiştir. Anketlerin çoğunluğunda açık uçlu sorunun cevaplanmamış olması katılımcıların ankete daha fazla zaman ayırmak istememeleri ya da anket sırasında akıllarına bir cevap gelmemiş olması olarak yorumlanabilmekle birlikte ankette yer alan soruların zaten genel stratejileri yeterince kapsamakta olduğu şeklinde de yorumlanabilecektir.

Bu çalışmada siber suç korkusuna ilişkin önlem alma/başa çıkma stratejileri ile ilgili genel olarak aşağıdaki başlıklar ele alınmış olup, ayrıntılı sorular Ek-1'de yer alan anket formunda bulunmaktadır:

1. İnternet üzerinden kişisel ve/veya hassas bilgiler (kimlik bilgileri, kredi/banka kartı bilgileri, adres bilgileri, cep telefonu numarası vb.) kullanılarak gerçekleştirilen online işlemler ve bu işlemlerde kullanılan önlem alma/başa çıkma stratejileri,
2. Sosyal medya hesabı sahipliği ve sosyal medyada kullanılan önlem alma/başa çıkma stratejileri,
3. İş yerinde ve dışında kullanılan elektronik cihazlarda kullanılan önlem alma/başa çıkma stratejileri,
4. Çalışmada kapalı uçlu soru olarak yer almamakla birlikte katılımcıların kendi aldıkları farklı önlemler/stratejiler.

Literatürde bu konuda yapılmış çalışmaların oldukça nadir olduğu daha önce belirtilmişti. Ancak, bu konu kapsamında değerlendirilebilecek bir çalışma olan Abdulai (2016, s. 107) çalışmasında belirlemiş olduğu online güvenlik önlemlerinin tamamının öğrencilerin kredi/banka kartı dolandırıcılığı riski üzerinde pozitif ve artan oranlı bir ilişki içerisinde

bulunduğunu belirtmektedir. Yani bir öğrencinin online güvenlik önlemlerini ne kadar fazla alması, öğrencinin kredi/banka kartı dolandırıcılığı riskini de o kadar fazla hissettiği anlamına gelmektedir (Abdulai, 2016, s. 107). Fakat Abdulai (2016, s. 107) bununla birlikte online güvenlik önlemleri kullanmayan öğrencilerin de yüksek seviyede risk hissettiklerini ortaya koymuştur.

Buradan hareketle online güvenlik önlemi alan öğrenciler ile online güvenlik önlemi almayan öğrencilerin aslında her ikisinin de belli oranda risk hissetmekte oldukları gibi bir sonuca ulaşmak mümkündür. Yani hiç online güvenlik önlemi almayan öğrencilerin yüksek seviyede bir risk hissetmeleri ile online güvenlik önlemini giderek daha fazla alan öğrencilerin giderek daha fazla risk hissetmekte olmaları önemlidir.

3. BÖLÜM ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

Suç korkusunun sosyal bir olgu olduğu konusuna daha önce "Suç Korkusu ve Siber Suç Korkusu" başlığı altında da değinilmiştir. Sosyal bir olgu olarak suç korkusunun suçun bireylerin fiziksel farklılıklarından meydana gelmekte olduğunu savunan bireysel suç teorileri, akıl sağlığı rahatsızlıkları, ruh sağlığı rahatsızlıkları gibi nedenlerden meydana geldiğini savunan psikolojik suç teorileri ya da kromozom sayısının farklı olması, beyin fonksiyonlarının iyi çalışmaması ve kalıtsal problemler gibi etkenlerden kaynaklandığını savunan biyolojik suç teorileri gibi teoriler ile ne derece açıklanabileceği şüphelidir. Zira bu teorilerden herhangi birisinin bu çalışmada tek başına kullanılması bireylerin toplumsal birer varlık olmaları ve hem suçun hem de suç korkusunun toplumsal bir olgu olmasının göz ardı edilmesi anlamına gelecektir. Bu nedenle tüm bu teorilerden ziyade suç korkusunun toplumsal birer varlık olan bireylerin toplumdaki etkileşimleri ve suçun toplum üzerindeki etkilerini inceleyen sosyolojik bir yaklaşımla irdelenmesi, konunun daha iyi anlaşılabilmesi adına önem arz etmektedir. Bu noktada her ne kadar kendi içerisinde eksiklikleri bulunsa da bireylerin toplumsal hayatlarındaki günlük, rutin aktivitelerine odaklanan ve suça bir fırsat olarak yaklaşan Rutin Aktiviteler Teorisinin bu çalışmanın teorik perspektifinin temeli olması tercih edilmiştir.

Daha önce de belirtildiği gibi siber alanda meydana gelen ilerleme ve gelişimler bireylerin günlük hayatlarında önemli değişiklikler meydana getirmişlerdir. Artık çoğu birey günlük hayatlarının önemli bir bölümünü siber dünyadaki siber aktivitelerle geçirmektedirler. Dolayısıyla gerçek dünyalarındaki rutin aktivitelerinin yanında artık siber dünyalarındaki rutin aktiviteleri de bireylerin hayatını şekillendirmektedir. Bireylerin günlük, rutin aktivitelerindeki bu değişimler onların siber suçların bir hedefi haline gelmesi, siber suçlara karşı korunmasız kalmaları ve siber suçlardan mağdur olmaları ya da siber suç korkusu yaşamalarına sebep olabilecektir. Bu anlamda da Rutin Aktiviteler Teorisinin bu çalışma açısından açıklayıcı güce sahip olabilecek bir kuramsal yaklaşım oluşturabileceği değerlendirilmiştir.

Nitekim daha önce de siber suçlar ve siber suç korkusu konusunda yapılmış olan bazı çalışmalarda Rutin Aktiviteler Teorisinden faydalanılmış olduğu görülmektedir (Alshalan, 2006; Bossler & Holt, 2009; Holt & Bossler, 2008; Leukfeldt & Yar, 2016;

Marcum, Higgins, & Ricketts, 2010; Reyns, Henson, & Fisher, 2011a; Williams, 2016; Yar, 2005).

3.1. RUTİN AKTİVİTELER TEORİSİ

Rutin Aktiviteler Teorisi, Rasyonel Seçim Teorisi ile birlikte idari kriminolojinin (administrative criminology - fırsat teorisi veya çevresel kriminoloji olarak da adlandırılmaktadır) iki perspektifinden birini oluşturmaktadır (John & Tierney, 2009, s. 6). Rutin Aktiviteler Teorisi, esasında Rasyonel Seçim Teorisi ile bir çok ortak yöne sahip bulunmakta olup, aralarındaki temel farklılık Rutin Aktiviteler Teorisi'nin bir adım geri atarak suç olaylarını toplumsal bir düzeyde analiz ederken, Rasyonel Seçim Teorisi'nin spesifik ve durumsal olan suç olayları ile ilgilenmesidir (John & Tierney, 2009, s. 14). Bu teoriler klasik gelenek içerisinde yer alabilecek olsalar da klasik kriminoloji temelde bireyi suç işlemekten caydırmak adına daha etkili ve verimli bir ceza adalet sistemi oluşturmaya odaklanırken bu teoriler ise durumsal suç önlemeye odaklanmaktadırlar (John & Tierney, 2009, s. 6). Bununla birlikte yine idari kriminolojinin kontrol teorisinden de temel farkı kontrol teorisinde suçlu motivasyonları ile kontrol fikri arasında bir bağlantı bulunmakta olup, idari kriminolojide ise bu motivasyonlar reddedilmekte ve durumsal suç önleme yoluyla zaten motive olmuş olduğu varsayılan bireyler kontrol edilmeye çalışılmaktadır. (John & Tierney, 2009, s. 6).

Rutin Aktiviteler Teorisi temelde Amerikalı kriminolog Marcus Felson ile ilişkilendirilmektedir (Cohen & Felson, 1979; Felson, 1986b, 1987, 1998, 2000'den akt. John & Tierney, 2009, s. 14).

Genel olarak idari kriminolojide olduğu gibi Rutin Aktiviteler Teorisi, suç davranışının normalde anlaşılan nedenlerini göz ardı ederek bunun yerine, gündelik sosyal hayatı oluşturan "rutin faaliyet" içindeki suç olayları ve kaynakları üzerinde yoğunlaşır (John & Tierney, 2009, s. 14). Rutin Aktiviteler Teorisi'nin varsayımı toplumda her zaman, her ne sebeple olursa olsun, değişen derecelerde suç işlemeye motive olmuş bireylerin bulunacağıdır. Bu motive olmuş bireylerin suç işleyip işlememeleri fırsatlara ve eşlik eden riskler ile ödüllerin rasyonel değerlendirilmelerine bağlıdır (John & Tierney, 2009, s. 14).

Rutin Aktiviteler Teorisi'nin perspektifinden suç sıradan, günlük hayatın (ev, iş, aile hayatı, boş zaman aktiviteleri vb.) rutinlerinden doğan fırsatların bir sonucudur (John & Tierney, 2009, s. 14). Bununla birlikte suç rasgele bir şekilde değil, üç temel faktörün bir araya gelmesiyle sağlanan fırsatlar sonucunda meydana gelmektedir (John & Tierney, 2009, s. 14). Suçun meydana gelmesini sağlayan bu üç temel faktör; motive olmuş suçlu, uygun hedef ve koruyucunun yokluğu'dur (Cohen & Felson, 1979, s. 589). Daha ayrıntılı bir şekilde ifade etmek gerekirse bir suçun meydana gelebilmesi için suça eğilimi olan ve bu eğilimi gerçekleştirebilecek olan bir *suçlu* (saldırgan), bu suçlu için *uygun bir hedef* oluşturan bir kişi veya nesne ve bu suçun gerçekleşmesini engelleyebilecek olan *koruyucuların yokluğu* asgari olarak gerekli bileşenlerdir (Cohen & Felson, 1979, s. 590). Dolayısıyla Cohen ve Felson (1979, s. 589) diğer kriminolojik sorgulamalardan farklı olarak Rutin Aktiviteler Teorisi'nde bireylerin veya grupların neden suça meyilli olduklarını araştırmayarak suça meyilli olmayı verili olarak kabul etmişler ve sosyal aktivitelerin zamansal ve mekânsal birlikteliklerinin bireylerin suça olan meyillerini eyleme dökmelerine yardımcı oldukları durumları incelemişlerdir.

Cohen ve Felson (1979, s. 589) rutin aktiviteler teorisini oluştururken, daha önceleri suç oranlarının genellikle mekânsal bir analizinin yapıldığını belirtmekte ve Hawley (1950)'nin İnsan Ekolojisi Kuramı'ndan da faydalanarak zamanı da teorilerine dahil etmektedirler. Böylelikle Cohen ve Felson (1979, s. 589) bireylerin rutin aktivite örüntülerindeki yapısal değişikliklerin motive olmuş suçlu, uygun hedef ve koruyucuların yokluğu durumlarının farklı zamansal ve mekânsal birlikteliklerini etkileyerek suç oranlarını etkileyebileceğini belirtmektedirler. Bir diğer ifadeyle bir toplumda suçun oluşabilmesi yukarıda sayılan bu üç temel faktörün belirli zaman ve mekanlarda bir araya gelmesi ile mümkün olabilmektedir. Dolayısıyla suçun oluşumunu engellemenin yolu da bireylerin sosyal hayatlarındaki rutin aktivitelerinde yapacakları değişikliklerle bu üç temel faktörün zamansal ve mekânsal olarak bir araya gelmelerini engellemek yoluyla mümkün olabilecektir. Motive olmuş suçlu, uygun hedef ve koruyucuların yokluğu faktörlerinden herhangi birisinin yokluğu bir suçun oluşumunun engellenmesi açısından yeterli olacaktır (Cohen & Felson, 1979, ss. 589, 604). Bu suçların oluşumunun engellenmesi de yine motive olmuş saldırgan, uygun hedef ve koruyucuların yokluğu üçlüsünün bir araya gelmesinin engellenmesi yoluyla mümkün olacaktır (Cohen & Felson, 1979, ss. 589, 604).

Cohen ve Felson tarafından oluşturulan Rutin Aktiviteler Teorisi'nin başlangıç itibariyle gerçek dünyadaki rutin aktiviteler ve dolayısıyla da gerçek suçlar açısından oluşturulmuş olduğu söylenebilir. Zira yapmış oldukları çalışmada Cohen ve Felson (1979, s. 593) rutin aktivitelerin evde, ev dışındaki işlerde ve ev dışındaki diğer aktivitelerde meydana gelebileceğini belirtmektedirler. Cohen ve Felson (1979, s. 593)'a göre 2. Dünya Savaşıyla birlikte ABD'deki rutin aktiviteler evdeki rutin aktivitelerden ev dışındaki diğer aktivitelere (özellikle de ev halkından olmayan üyelerle gerçekleştirilen ev dışı aktiviteler) doğru büyük bir değişim geçirmiştir. İşte Cohen ve Felson (1979, s. 593) bireylerin rutin aktivitelerindeki tam da bu değişimin motive olmuş suçluların koruyucuların yokluğunda uygun hedefler ile zamansal ve mekansal olarak buluşmaları olasılığını artırarak suç oranlarını artırmakta olduğunu savunmaktadırlar. Dolayısıyla rutin aktiviteler teorisinin toplumsal değişimler ile suç oranları arasındaki ilişki konusunda da oldukça açıklayıcı bir yaklaşım sunmakta olduğu söylenebilecektir.

Ayrıca Cohen ve Felson (1979, ss. 590-591) çalışmalarında teknolojiye de değinmekte ve teknolojinin suça meyilli bireylerin suç işleyebilmelerini kolaylaştırıcı bir etkide bulunabileceği gibi, koruyucuların potansiyel suçlularla mücadele etme noktasındaki kabiliyetlerini de artırabileceğini belirtmektedirler. Bununla birlikte o yıllarda henüz siber alanın da ortaya çıkmamış olması nedeniyle rutin aktiviteler teorisi siber dünyadaki rutin aktivitelere değinmemiştir. Fakat siber dünyanın ortaya çıkışının da toplumdaki rutin aktivitelerin değişimi açısından oldukça önemli olduğu söylenebilecektir. Aynen ABD toplumundaki rutin aktivitelerin 2. Dünya Savaşıyla birlikte evdeki rutin aktivitelerden ev dışındaki diğer aktivitelere doğru kaymasında görüleceği üzere, teknolojideki gelişmeler ve siber dünyanın ortaya çıkışıyla birlikte bireylerin günlük rutin aktivitelerinin de siber alana doğru kaymakta olduğu söylenebilecektir. Daha önce aile fertleri ya da arkadaşları ile evde veya ev dışında yüz yüze ilişkiler kurmakta olan bireyler, siber dünyadaki gelişmelerle birlikte siber alanda etkileşim kurmaya, mesajlaşmaya, konuşmaya ve hatta görüntülü görüşmeye başlamışlardır. Daha önce örneğin günlük, haftalık ya da aylık rutin aktiviteleri olarak işe, markete, pazara, çarşıya vb. gitmekte olan bireyler artık online ortamlarda çalışabilmekte, online ortamlarda alışverişlerini gerçekleştirebilmekte, oyun oynayabilmekte ve dolayısıyla rutin faaliyetlerini online ortamlara taşıyabilmektedirler.

İşte Rutin Aktiviteler Teorisince savunulan motive olmuş suçluların koruyucuların yokluğunda uygun hedefler ile zamansal ve mekânsal olarak bir araya gelerek suçu meydana getirmeleri durumu aynen gerçek dünyada olduğu gibi siber dünyada da mümkün olan bir durumdur. Burada her iki duruma da birer örnek vermek gerekirse ilk olarak Rutin Aktiviteler Teorisi bireylerin günlük rutin iş aktivitelerinin onları güvendikleri insanlardan ve değer verdikleri evlerinden ayırdığını belirtmektedir (Cohen & Felson, 1979, s. 591). Yani gerçek dünyadaki rutin aktiviteleri olarak sabah evlerinden ve ailelerinden ayrılarak işe giden bireylerin hem kendileri hem de geride bırakmış oldukları evleri ve aileleri suç işlemeye motive olmuş suçlular için uygun bir hedef haline gelebilmektedir. Bu noktada suçun oluşumunun engellenmesi ya hedefin uygun olmaktan çıkarılması (görünürlüğünün azaltılması gibi) ya da koruyucuların eklenmesi (evin dışına bir köpek konulması, evin dikenli tellerle ya da duvarla çevrilmesi vb.) ile mümkün olabilecektir. Aynı şekilde siber suçlar açısından bakıldığında da yine bireylerin günlük siber rutin aktivitelerinden söz edilebilir. Örneğin gündüz işlerine gitmekte olan bireyler akşam evlerine gelerek internet üzerinden dizi, film vb. izleyebilmektedirler. İşte bireyler internet üzerindeki çok da güvenilir olmayabilen web sayfalarında bulundukları bu akşam saatlerinde, bilgisayarlarında herhangi bir koruyucunun (antivirüs, anti malware, güvenlik duvarı vb.) bulunmadığı durumlarda motive olmuş siber suçlular açısından uygun bir hedef haline gelebilmektedirler. Bununla birlikte siber suçlar açısından bakıldığında motive olmuş suçlu, uygun hedef ve koruyucunun yokluğu durumunun zamansal ve mekânsal olarak bir arada bulunma zorunluluğunun bulunmadığı da savunulmuştur. Reyns, Henson, ve Fisher (2011b, s. 1152) siber taciz örneğinde suçlunun sabah göndermiş olduğu bir e-maili mağdurun akşam açacağı bir durumda zamansal bir birleşimin olmadığını belirtmektedirler. Aynı şekilde Alshalan (2006, s. 146) da siber alanda mekanın internet olduğunu ve suçun oluşumu için de suçlunun hazır bulunuyor olmasının gerekmediğini belirtmektedir. Dolayısıyla siber suçlar açısından bu durum değişebilmektedir. Bunun da belirtilmesinin ardından Rutin Aktiviteler Teorisi'nde her ne kadar siber suçlar açısından bazı noktalarda farklılaşabiliyor olsa da suçun meydana gelebilmesi açısından zamansal ve mekânsal olarak bir arada bulunmaları gerekli görülen bileşenler ayrı ayrı incelenebilir.

3.1.1. Motive Olmuş Suçlu

Rutin Aktiviteler Teorisi, toplumda her zaman suç işlemeye motive olmuş bireylerin bulunacağı varsayımını kabul ederek, suçların meydana gelmesi ve önlenmesinde uygun hedefler ve koruyucuların yokluğu konularına odaklanılması gerektiği yaklaşımını benimsemektedir. Rutin Aktiviteler Teorisi bu yönüyle bireyler neden suç işler (biyolojik suç teorileri, psikolojik suç teorileri, sosyal düzensizlik teorisi vb.) veya bireyler neden suç işlemez (kontrol teorileri) sorularına cevap arayan teorilerden ayrılmakta ve suçlulardan ziyade suç olaylarına odaklanan farklı ve orijinal bir bakış açısı ortaya koymaktadır.

Siber suçlar açısından bakıldığında da Cohen ve Felson (1979)'un toplumda her zaman suç işlemeye motive olmuş bireylerin olacağı varsayımını siber alana taşımak mümkündür (Choi, 2008, s. 45). Zira siber suçluların siber alanda her zaman var olduklarını ve suç işleme motivasyonuna sahip olarak muhtemel mağdurların peşinde dolaştıklarını söylemek abes olmayacaktır (Choi, 2008, s. 45). Bu açıdan bakıldığında Rutin Aktiviteler Teorisinin esasında siber suçlar açısından da uygulanabilir bir yaklaşım içermekte olduğunu söylemek mümkündür.

Siber dünyada her zaman bulunacağı düşünülen siber suçlulara örnek olarak hackerları göstermek mümkündür. Bununla birlikte hackerlık tümüyle siber alandaki suçlu bireyleri tanımlamak için kullanılan bir tanım olmayıp kendi içerisinde sınıflandırmalara tabi tutulmaktadır. Bu sınıflandırmaların en genel olanında hackerlar siyah şapkalı, beyaz şapkalı ve gri şapkalı olmak üzere 3'e ayrılmaktadırlar. Bu sınıflandırmada siyah şapkalılar hackerların çoğunluğunu oluşturan grup olup, yetkisiz ve genellikle kötü niyetli olarak sistemlere sızan bireyleri tanımlarken; beyaz şapkalılar sistem güvenliği için çalışan "etik hackerları" tanımlamakta; gri şapkalılar ise siyah şapkalı ve beyaz şapkalı hackerlar arasında kalan ve motivasyonları belirsiz veya değişmeye eğilimli olabilecek bireyleri tanımlamaktadır (Furnell, 2001, s. 33).

Diğer yandan (Furnell, 2001, s. 34) hackerların daha ayrıntılı bir sınıflandırmayla aşağıdaki şekilde de sınıflandırılabileceğini belirtmektedir:

Siber teröristler: Sistemlere, ağlara ve/veya verilere yönelik tehdit veya saldırı için hacker tipi teknikler kullanan teröristler. Terörizmin diğer formlarında olduğu gibi, siber terörist aktiviteleri belirli bir siyasi veya sosyal ajanda adı altında yürütülürler. Temel amaç tipik olarak karşı tarafı sindirmek veya zorlamak olacaktır (örneğin bir hükumeti).

Siber savaşçılar: Acil servisler, finansal işlemler, ulaşım ve iletişim gibi hayati altyapıyı destekleyen bilgisayar sistemlerine saldırmak için hacking (korsanlık) teknikleri kullanan kişiler. Bu temelde askeri ve savaş bağlamlarında hackingin uygulanmasıyla ilgilidir.

Hacktivistler: Aktivist bir gündemi desteklemek veya ilerletmek için bilgisayar sistemlerine giren hackerlar. Web sitelerinin tahrif edilmesi gibi olaylar genellikle bunlarla bağlantılıdır.

Kötü Amaçlı Yazılım Yazarları: Bir hacker sınıflandırması olmayıp, genellikle onlarla birarada değerlendirilmektedir. Virüsler, solucanlar ve Truva atları gibi kötü amaçlı programlar oluşturmakla sorumlu bireylerdir.

Phreakers: Özellikle telefon ağlarını ve ilgili teknolojileri hacklemeye odaklanan bireyler. Hedefleri, altyapının basit bir şekilde araştırılmasından onun unsurlarını manipüle etmeye kadar değişebilir.

Samurai: Yasal kırma işleri yapmak için işe alınan bireyler, meşru nedenlerle kurumsal bilgisayar sistemlerine sızarlar. Bu hackerlar Sneakers olarak da adlandırılabilir.

Script kiddies: Diğer daha yetkin hackerlar tarafından yazılan kodlar ve programlara dayanan oldukça sınırlı hacking yeteneklerine sahip kimseler. Bu tarz hackerlar genellikle kötü niyetli zarara neden olurlar ve genellikle hacking toplumunun daha yetenekli üyeleri tarafından aşağılanırlar. Bu bireyler Packet Monkeys olarak da adlandırılmaktadır.

Warez d00dz: Telif hakkıyla korunan yazılımları elde edip kopyalarını yasa dışı olarak dağıtan ve cracker'ların bir alt sınıfı olan bireyler. Kullanılan yazım bu haliyle hacker argo'sunun bir temsilcisidir – normal olarak yazıldığında "Wares Dudes". Daha genel olarak bu bireyler Yazılım Korsanları olarak bilinmektedirler.

Bu sınıflandırmada da belirtilen farklı türdeki hackerların gerçekleştirdikleri faaliyetlerdeki motivasyonlarının da farklı olduğunu söylemek mümkündür. Bu konuda

Furnell (2001, s. 35) yapmış olduğu çalışmada hackerlar ve motivasyonlarına ilişkin aşağıdaki şekilde bir tablo oluşturmuştur.

Tablo 4. Hackerlar ve Motivasyonları (Furnell, 2001, s. 35)

	Siber Teröristler	Siber Savaşçılar	Hacktivistler	Malware Yazıcılar	Old School	Phreakers	Samurai	Script Kiddies	Warezd00dz
Meydan Okuma				X	X	X	X		X
Ego				X	X	X		X	X
Casusluk		X		X					
İdeoloji	X	X	X		X				X
Haylazlık				X		X		X	
Para		X		X		X	X		X
İntikam	X		X	X				X	

Rutin Aktiviteler Teorisinde değinilen motive olmuş suçluları ve motivasyonlarını siber suçlar açısından kısmen de olsa bu şekilde açıklamak mümkündür. Bununla birlikte bizim çalışmamız açısından siber suçlular yalnızca bilgisayar korsanları ile sınırlı olmayıp, siber hırsızlar, siber dolandırıcılar, siber taciz, tehdit ve şantaj failleri, siber zorbalık failleri ve kimlik hırsızları gibi Türk Ceza Kanunu ve ilgili kanunlar (Fikir ve Sanat Eserleri Kanunu, TMK, 5651 vb.) tarafından suç sayılan fiilleri işleyen tüm siber suçluları kapsamaktadır.

3.1.2. Uygun Hedef

Rutin Aktiviteler Teorisi'ne göre bir suçun oluşabilmesi için gerekli olan ikinci unsur uygun bir hedeftir. Uygun hedefi esasında motive olmuş suçlunun belirli bir suçu

işleyebilmek adına uygun gördüğü ve gözüne kestirdiği birey, nesne vb. bir hedef olarak tarif etmek mümkündür. Cohen ve Felson (1979, s. 595) uygun bir hedefin ana bileşenleri olarak değerli olması (value), görünür olması (visibility), erişilebilir olması (accessibility) ve hareket kabiliyeti (inertia) olmak üzere dört unsurdan (VIVA) söz etmektedir.

Siber suçlar açısından bakıldığında da motive olmuş bir siber suçlu için uygun bir hedef oluşturan pek çok şeyden söz etmek mümkündür. Örneğin herhangi bir antivirüs programı, güvenlik duvarı (firewall) vb. tarafından korunmayan bilgisayarlar, yeterince güçlü parolalar tarafından korunmayan internet bankacılığı hesapları, kişisel verilerini yeterince güvenilir olmayan dijital ortamlarda saklayan bireyler veya internet vasıtasıyla işlenebilecek olan suçlar hakkında yeterince farkındalığı olmayan bireyler motive olmuş siber suçlular için uygun birer hedef teşkil edebileceklerdir.

Bununla birlikte her ne kadar Rutin Aktiviteler Teorisi bir suçun meydana gelmesi açısından yalnızca motive olmuş suçluyu verili olarak kabul etse de, siber alan açısından uygun hedefin de farklı seviyelerde de olsa verili olarak kabul edilmesi gerektiğini savunan araştırmacılar bulunmaktadır. Bu araştırmacılardan Choi (2008, s. 45), bir internet kullanıcısının internete bağlandığı anda uygun bir hedef olmak için gerekli kriterlerin (VIVA – değerli olma, hareket kabiliyeti, görünür olma, erişilebilir olma) tamamını sağladığını belirtir. Zira online olmak, her ne kadar online ortamdaki yaşam tarzı ve aktivitelere göre değişen seviyelerde de olsa, siber alandaki olası bir mağduriyet için yeterli bir şarttır (Choi, 2008, s. 45).

3.1.3. Koruyucunun Yokluğu

Rutin Aktiviteler Teorisi'ne göre bir suçun oluşabilmesi için gerekli olan üçüncü unsur koruyucunun yokluğudur. Burada koruyucudan kastın uygun bir hedefi motive olmuş suçludan koruyabilecek olan polis, güvenlik görevlisi, eş, akraba, komşu vb. bireyler ile koruma köpeği vb. hayvanlar veya güvenlik kamerası, elektrikli teller, alarm sistemi vb. her türlü canlı veya cansız varlık olduğunu söylemek mümkündür. Koruyucuların suçun oluşumunu önlemeleri ya yalnızca fiziksel olarak var olmaları ile ya da bir tür doğrudan eylemle gerçekleşmektedir (Cohen, Felson, & Land, 1980, s. 97).

Cohen ve Felson (1979, s. 590) suç konusundaki sosyolojik araştırmalarda polis faaliyetlerinin oldukça geniş şekilde analiz edilmesine rağmen, sıradan vatandaşların birbirlerine veya birbirlerinin mülklerine yönelik olan koruyuculuklarının ihmal edildiğini belirtmektedirler. Nitekim bireylerin birbirlerine veya birbirlerinin mülklerine karşı olan koruyuculuklarının en az polis kadar ya da polisten daha fazla olabileceğini söylemek mümkündür. Bu bağlamda sokakta eşleri ya da bir arkadaşları ile gezen bireylerin yalnız başına gezen bireylere göre birbirlerine yönelik koruyucukları daha fazla olabilmekte veya bir apartman yöneticisinin apartmana girip çıkan bireyleri kontrol ederek muhtemel hırsızlara karşı bir koruyuculuk sağlaması mümkün olabilmektedir.

Siber suçlar açısından bakıldığında ise literatürde fiziksel, sosyal ve bireysel koruyuculara değinildiği görülmektedir (Bossler & Holt, 2009; P. N. Grabosky, 2001; Miethe & Meier, 1994). Fiziksel koruyucular antivirüs programları, anti-malware programları ve güvenlik duvarı gibi koruyuculardan oluşmakta olup, gerçek dünyadaki fiziksel koruyuculara benzerlik göstermektedirler. Miethe ve Meier (1994, s. 51) fiziksel koruyuculuğun hedef zorlaştırma (target hardening) aktiviteleri (kapı, pencere kilitleri, pencere demirleri, alarmlar, silah sahipliği vb.), çeşitli fiziksel engelleme faaliyetleri ve kollektif faaliyetlere katılım (mahalle izleme - neighborhood watch programları) gibi konuları içerdiğini belirtmektedirler. Sosyal koruyuculuk ise arkadaşlar, komşular, yayalar, kolluk görevlileri vb. kişilerin yalnızca var olmaları ya da bir saldırıyı durdurmak için yardım sağlamaları olarak açıklanmaktadır (Miethe & Meier, 1994, s. 51). Koruyuculuk altındaki üçüncü başlık olarak değerlendirilebilecek olan bireysel koruyuculuk ise özellikle siber suçlar açısından en önemli koruyuculuk türünü oluşturmaktadır. P. N. Grabosky (2001, s. 248) günümüzde siber alandaki ilk savunma hattının kendini savunmak olduğunun belirtmektedir. Bireysel koruyuculuk içerisinde bireylerin siber alandaki farkındalıklarını arttırmaları, teknolojik gelişmeler ve bu gelişmelerin getirdiği riskler ve tehditler hakkında bilgi sahibi olmaları, kendilerini siber suçlardan korumaya yönelik alabilecekleri önlemleri bilmeleri ve bu önlemleri almaları, siber alandaki aktivitelerinin olası sonuçları hakkında bilgi sahibi olarak hareket etmeleri gibi konuların bulunduğunu söylemek mümkündür.

Burada koruyucuların nitelik ya da niceliğinin suçun oluşumunun tamamen engellenmesi noktasında bir garanti sağlayamayacağı ifade edilmelidir. Söz gelimi bir antivirüs

programı, bir güvenlik duvarı ya da bireylerin farkındalık düzeyleri her ne kadar suçların oluşumunu belli oranda engelleyebilseler de suçlara karşı kesin çözüm olarak değerlendirilememektedirler. Bununla birlikte koruyuculuk fiziksel, sosyal veya bireysel türlerin hangisinde olursa olsun, olası suçlulara karşı maliyeti artırıcı bir etkiye sahip olduğundan (suçluların daha fazla çaba sarf etmesini gerektirmesi, yakalanma ve tutuklanma risklerini artırması vb.) önem arz etmekte ve bireyler açısından mağduriyet ihtimalini de azaltmaktadır (Miethe & Meier, 1994, s. 51).

3.1.4. Rutin Aktiviteler Teorisine Sonradan Eklenen Faktör: Tutucular

Rutin Aktiviteler Teorisi bu haliyle ilk bakışta motive olmuş suçluyu verili olarak kabul etmesi ve suçun oluşum aşamasında doğrudan diğer iki noktaya (uygun hedef ve koruyucunun yokluğu) odaklanması açısından biraz eksik gözükmektedir. Özellikle sosyolojik bir yaklaşımla incelendiğinde toplumdaki bireyleri suç işlemeye motive eden bireysel veya toplumsal hususlar ile suç işlemeye motive olmuş bireylerin henüz motive olmadan ya da motive olduktan sonra motivasyonlarının ortadan kaldırılması yoluyla suçun önlenmesinin mümkün olup olmayacağı konusu tartışmaya açıktır. Bu noktada esasında suçun önlenmesi aşamasında suç işlemeye motive olmuş bireyler de en az diğer iki husus kadar incelemeye değer görülebilir. Tam da bu noktada Marcus Felson teorisini Cornish ve Clarke (1986)'ın Rasyonel Seçim Teorisi ve Brantingham ve Brantingham (1984)'ın Suç Örüntüsü Teorisi ile entegre etme ihtiyacı duymuştur (Medina, 2014, s. 2). Felson aynı zamanda Hirschi (1969)'nin Sosyal Kontrol Teorisi'nden yararlanarak daha önce suçun meydana gelmesi için ortaya koyduğu üç unsura bir dördüncüsünü de eklemiştir: the intimate handler (tutucular) (Medina, 2014, s. 2). Burada tutucular olarak olası suçlular ile duygusal bir ilişkiye sahip olan ve onun üzerinde bir tür kontrol uygulayabilecek olan aile bireyleri vb. bireylerden söz edilmektedir (Medina, 2014, s. 2). Ailesine, sevdiklerine ve topluma sıkı bağlarla bağlı olan bireylerin kendilerini çevreleyen bu insanların etkisiyle suç işleme ihtimalinin azalacağı iddia edilmiştir (Felson, 1986a'dan akt. Dolu, 2012, p. 133).

Sonuç olarak suça ilişkin kriminolojik yaklaşımlar yalnızca suçlu üzerinden suçu izah etmeye çalışırken Rutin Aktiviteler Teorisi suçu, suçlu-mağdur-koruyucu ekseninde ele almış ve suçun aslında bir fırsat olayı olduğunu ortaya koyarak kriminoloji literatüründe

başlı başına bir çığır açmıştır (Cullen & Agnew, 2003, p. 284'den akt. Dolu, 2012, p. 143). Cohen ve Felson (1979, s. 605) Rutin Aktiviteler Teorisi ile birlikte suçluları suç işlemeye motive eden faktörlerin önemini inkar etmeden suç olaylarının kendisine ve onları meydana getiren ön koşullara odaklanmışlardır. Bununla birlikte her ne kadar Rutin Aktiviteler Teorisi ilk başlarda motive olmuş suçluyu verili olarak kabul edip uygun hedef ve koruyucuların yokluğuna odaklansa da daha sonraları suçluların suç işlemelerine engel olabilecek aile bireyleri, arkadaşları, sevdikleri vb. tutucuları da teoriye dahil ederek sosyolojik açıdan daha kapsayıcı bir yaklaşıma ulaşmış ve Rasyonel Seçim Teorisi, Suç Örüntüsü Teorisi, Sosyal Kontrol Teorisi, suç fırsatları ve durumsal suç önleme gibi yaklaşımları da bünyesine katarak ve daha ayrıntılı inceleyerek suç sosyolojisi ve kriminoloji açısından oldukça değerli bir konuma ulaşmış ve yalnızca gerçek suçlar açısından değil siber suçlar açısından da yorumlanabilir ve uygulanabilir bir perspektif sunmuştur.

4. BÖLÜM ANKARA'DAKİ TEKNOKENTLERDE YAPILAN ARAŞTIRMANIN BULGULARI

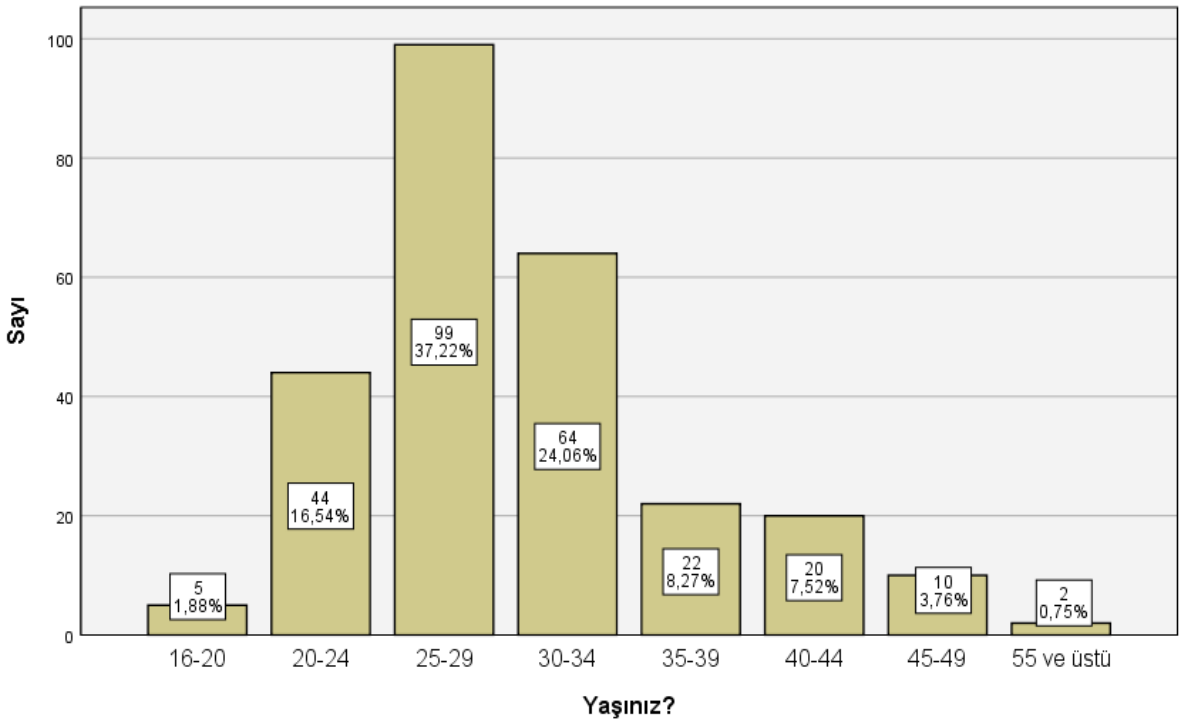
Ankara'daki 4 teknokentin (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışanları ile gerçekleştirilen anket çalışmasına ilişkin bulgular aşağıda betimsel verilerin analizi ve hipotezlerin analizi olmak üzere iki başlık altında sunulmaktadır.

4.1. BETİMSEL VERİLERİN ANALİZİ

4.1.1. Teknokent Çalışanlarının Sosyo-Demografik ve Genel Özellikleri

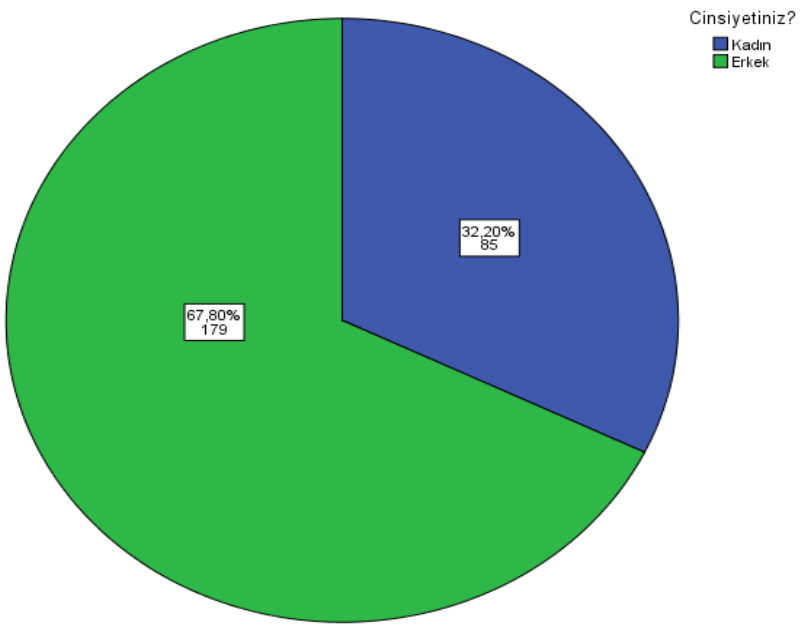
Araştırmaya katılan teknokent çalışanlarının sosyo-demografik ve genel özelliklerine ilişkin grafikler ve tablolar aşağıdaki gibidir.

Grafik 1. Katılımcıların Yaşa Göre Dağılımı



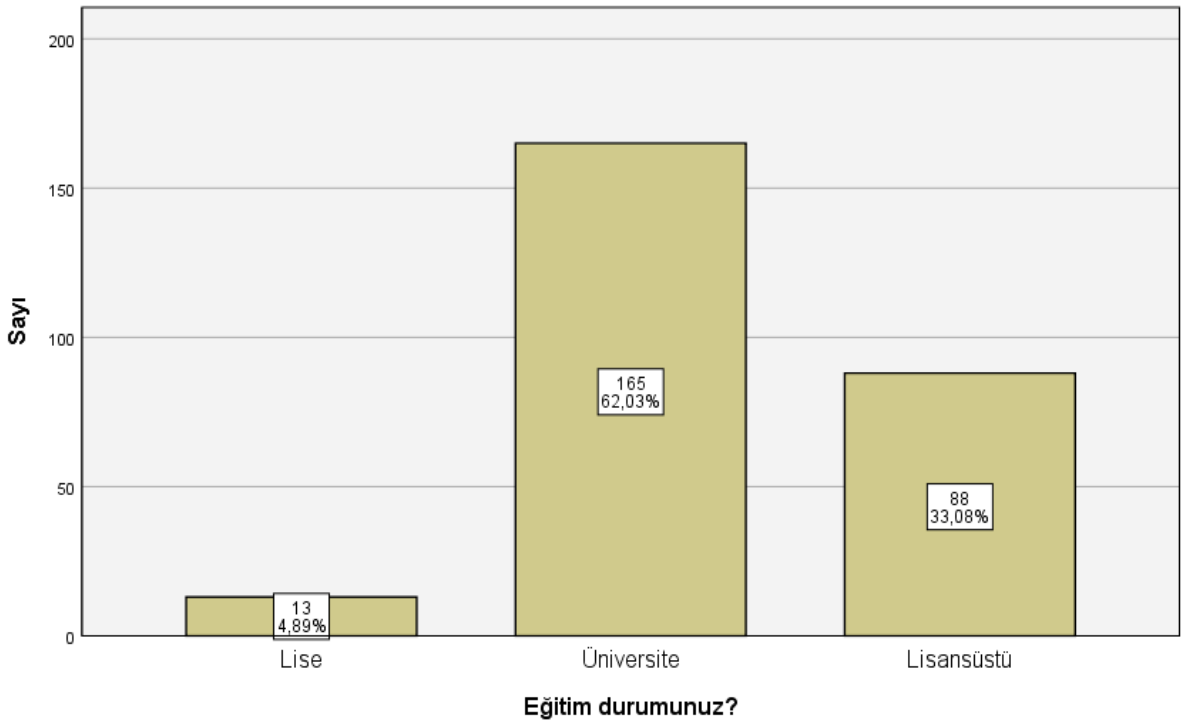
Katılımcıların yaşa göre dağılımı Grafik 1'de gösterilmiştir. Buna göre bu soruya cevap veren katılımcılar arasındaki en yüksek çoğunluk 99 katılımcı ile örneklemin %37,22'sini oluşturan 25-29 yaş arası çalışanlardan oluşmaktadır. Örneklemdeki ikinci en yüksek çoğunluk ise 64 katılımcı ile örneklemin %24,06'sını oluşturan 30-34 yaş arası çalışanlardır. Burada 20-34 yaş arası çalışanların 207 kişi ile örneklemin 4'te 3'ünden daha fazla bir bölümünü (%77,82) oluşturmakta olduğu ve dolayısıyla örneklemin büyük bir çoğunluğunun genç olarak nitelendirilebilecek katılımcılardan oluştuğu görülmektedir.

Grafik 2. Katılımcıların Cinsiyete Göre Dağılımı



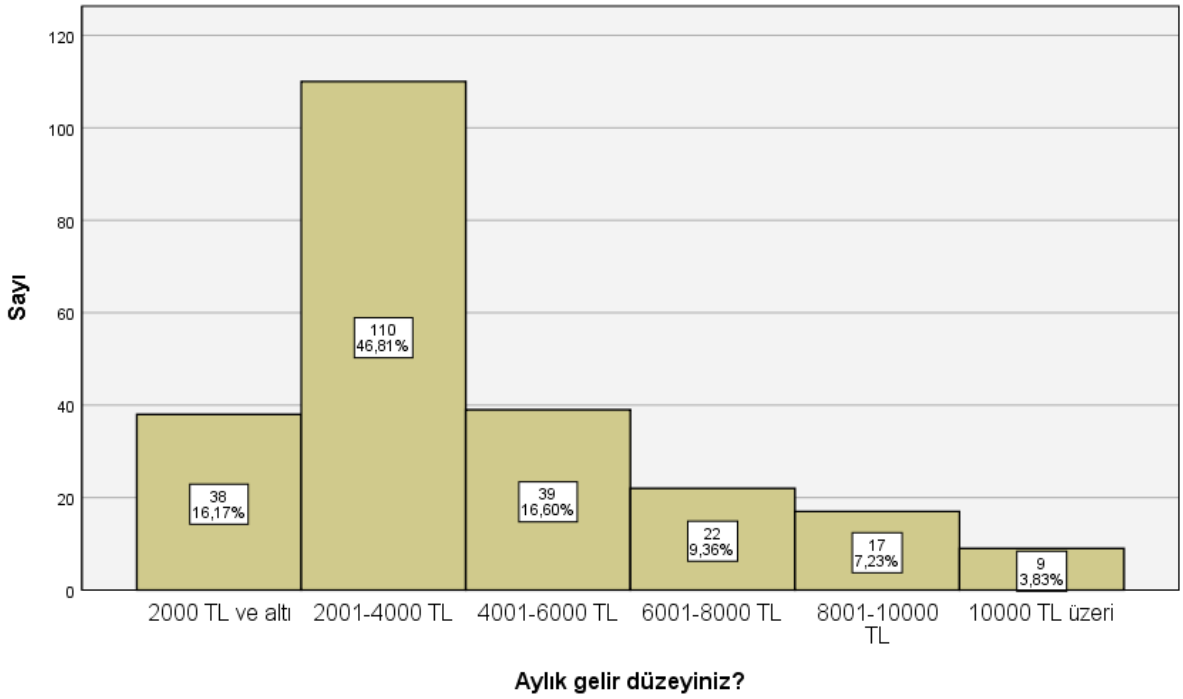
Katılımcıların cinsiyet dağılımı Grafik 2'de gösterilmiş olup, bu soruya cevap veren katılımcıların %32,20'si (85 kişi) kadınlardan, %67,80'i (179 kişi) ise erkeklerden oluşmaktadır.

Grafik 3. Katılımcıların Eğitim Durumlarına Göre Dağılımı



Katılımcıların eğitim durumuna göre dağılımı Grafik 3'de gösterilmiş olup, bu soruya cevap veren katılımcıların %4,89'u (13 kişi) eğitim durumunu lise olarak, %62,03'ü (165 kişi) üniversite olarak ve %33,08'i ise lisansüstü olarak belirtmiştir. Katılımcılar arasında eğitim durumu ilkokul ve ortaokul olan kimse yer almamaktadır. Katılımcıların %95'inden daha fazlası en az üniversite düzeyinde eğitime sahip bulunmakta olup, 3'te 1'lik kısmı da lisansüstü düzeyinde eğitime sahiptir. Dolayısıyla katılımcıların büyük oranda eğitim düzeyi yüksek bireylerden oluşmakta oldukları söylenebilecektir.

Grafik 4. Katılımcıların Aylık Gelir Düzeyine Göre Dağılımı



Katılımcıların aylık gelir düzeyine göre dağılımı Grafik 4'te gösterilmiş olup, bu soruya cevap veren katılımcıların %46,81'inin 2001-4000 TL arasında, %16,60'sının 4001-6000 TL arasında, %16.17'sinin ise 2000 TL ve altında aylık gelire sahip oldukları görülmektedir. 6001-8000 TL, 8001-10000 TL ve 10000 TL ve üzeri aylık gelire sahip olan katılımcı yüzdelerinin her biri %10'dan daha düşüktür. Dolayısıyla katılımcıların yarısına yakını 2001-4000 TL arasında aylık gelire sahip bulunmakta olup, neredeyse %80'i ise 6000 TL ve daha düşük aylık gelire sahiptirler.

Tablo 5. Katılımcıların Çalıştıkları Sektöre Göre Dağılımı

	Sayı	Yüzde	Geçerli Yüzde
Yazılım ve Bilişim Teknolojileri	184	69,2	69,4
Elektrik, Elektronik	42	15,8	15,8
Makine ve Tasarım	6	2,3	2,3
Telekomünikasyon	19	7,1	7,2

Biyoteknoloji	5	1,9	1,9
Enerji	2	0,8	0,8
Medikal & Biyomedikal	13	4,9	4,9
İleri Malzeme	1	0,4	0,4
Gıda	1	0,4	0,4
Kimya	1	0,4	0,4
Sağlık ve İlaç	6	2,3	2,3
Uzay ve Havacılık Teknolojileri	6	2,3	2,3
Çevre	4	1,5	1,5
Savunma Sanayi	31	11,7	11,7
Nanoteknoloji	2	0,8	0,8
Otomotiv	2	0,8	0,8
Tarım	3	1,1	1,1
Madencilik	1	0,4	0,4
Diğer	17	6,4	6,4

Katılımcıların çalıştıkları sektöre göre dağılımı Tablo 5'te gösterilmiş olup, en yoğun olarak çalışılmakta olan ilk 5 sektör sırasıyla Yazılım ve Bilişim Teknolojileri, Elektrik-Elektronik, Savunma Sanayi, Telekomünikasyon ve Medikal-Biyomedikal sektörleridir. Yazılım ve Bilişim Sektöründe çalışmakta olan katılımcılar tüm katılımcıların %69,2'sini oluşturmaktadır. Burada katılımcıların bir kısmı birden fazla sektörde çalışmakta olduklarından çalışılan sektör sayıları toplamı örneklem sayısı olan 266'dan daha fazla çıkmaktadır.

Katılımcıların çalıştıkları şirketteki pozisyonlarına göre dağılımları oldukça geniş bir yelpazede olduğundan burada yer verilememiştir. Bununla birlikte katılımcıların genel müdür, müdür kurucu ortak, uzman, mühendis, danışman, ekip lideri, sekreter, güvenlik görevlisi, stajyer vb. pek çok pozisyonda çalışmakta olup, yoğunluğun en fazla olduğu pozisyonların yazılım, Ar-ge vb. pozisyonlar oldukları görülmektedir.

4.1.2. Teknokent Çalışanlarının Siber Suç Korkusu Düzeyleri

Araştırmaya katılan teknokent çalışanlarının siber suç korkusu düzeylerine ilişkin tablolar aşağıdaki gibidir.

Tablo 6. Katılımcıların Siber Suçlardan Korku Düzeylerine Göre Dağılımları

		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	Toplam Cevap	Cevap-sız	Genel Toplam
Bilgisayar Korsanlığı (Hacking)	Sayı	48	180	30	258	8	266
	Yüzde	18,0	67,7	11,3	97,0	3,0	100,0
	Geçerli Yüzde	18,6	69,8	11,6	100,0		
Denial of Service (DoS) Saldırıları	Sayı	100	138	27	265	1	266
	Yüzde	37,6	51,9	10,2	99,6	0,4	100,0
	Geçerli Yüzde	37,7	52,1	10,2	100,0		
Virüsler, Truva Atları ve Zararlı Yazılımlar	Sayı	55	150	60	265	1	266
	Yüzde	20,7	56,4	22,6	99,6	0,4	100,0
	Geçerli Yüzde	20,8	56,6	22,6	100,0		
Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız	Sayı	43	128	93	264	2	266
	Yüzde	16,2	48,1	35,0	99,2	0,8	100,0
	Geçerli Yüzde	16,3	48,5	35,2	100,0		
Casus Yazılımlar	Sayı	44	154	67	265	1	266
	Yüzde	16,5	57,9	25,2	99,6	0,4	100,0
	Geçerli Yüzde	16,6	58,1	25,3	100,0		
Kimlik Hırsızlığı	Sayı	37	146	81	264	2	266
	Yüzde	13,9	54,9	30,5	99,2	0,8	100,0
	Geçerli Yüzde	14,0	55,3	30,7	100,0		
	Sayı	84	119	62	265	1	266

Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi	Yüzde	31,6	44,7	23,3	99,6	0,4	100,0
	Geçerli Yüzde	31,7	44,9	23,4	100,0		
Siber Zorbalık	Sayı	70	137	59	266	0	266
	Yüzde	26,3	51,5	22,2	100,0	0,0	100,0
	Geçerli Yüzde	26,3	51,5	22,2	100,0		
Bilişim Sistemleri Aracılığıyla Hakaret	Sayı	145	99	22	266	0	266
	Yüzde	54,5	37,2	8,3	100,0	0,0	100,0
	Geçerli Yüzde	54,5	37,2	8,3	100,0		
Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi	Sayı	41	147	78	266	0	266
	Yüzde	15,4	55,3	29,3	100,0	0,0	100,0
	Geçerli Yüzde	15,4	55,3	29,3	100,0		
Siber Hırsızlık	Sayı	45	143	77	265	1	266
	Yüzde	16,9	53,8	28,9	99,6	0,4	100,0
	Geçerli Yüzde	17,0	54,0	29,1	100,0		
Siber Dolandırıcılık	Sayı	76	131	55	262	4	266
	Yüzde	28,6	49,2	20,7	98,5	1,5	100,0
	Geçerli Yüzde	29,0	50,0	21,0	100,0		
Siber Taciz	Sayı	143	93	26	262	4	266
	Yüzde	53,8	35,0	9,8	98,5	1,5	100,0
	Geçerli Yüzde	54,6	35,5	9,9	100,0		
Siber Tehdit ve Şantaj	Sayı	126	107	29	262	4	266
	Yüzde	47,4	40,2	10,9	98,5	1,5	100,0
	Geçerli Yüzde	48,1	40,8	11,1	100,0		
Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu	Sayı	120	113	29	262	4	266
	Yüzde	45,1	42,5	10,9	98,5	1,5	100,0
	Geçerli Yüzde	45,8	43,1	11,1	100,0		
Siber Terörizm	Sayı	89	128	44	261	5	266
	Yüzde	33,5	48,1	16,5	98,1	1,9	100,0
	Geçerli Yüzde	34,1	49,0	16,9	100,0		

Katılımcıların siber suçlardan korku düzeylerine göre dağılımları Tablo 6'da gösterilmiştir. Bu bölümde teknokent çalışanları belirlenmiş olan toplam 16 siber suçtan mağdur olmaktan ne düzeyde korku yaşadıklarını seçmişlerdir. Tabloya göre teknokent çalışanlarının "hiç korku yaşamıyorum" seçeneğini en fazla seçtikleri siber suçlar arasında ilk beş sırayı;

1- Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü) (%54,5 - 145 kişi),
2- Siber Taciz (%54,6 - 143 kişi),
3- Siber Tehdit ve Şantaj (48,1 - 126 kişi),
4- Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu (%45,8 - 120 kişi),
5- Denial of Service (DoS) Saldırıları (%37,7 - 100 kişi) oluşturmaktadır.

Dolayısıyla katılımcıların en az korku yaşadıkları siber suç bilişim sistemleri aracılığıyla hakaret suçudur. İkinci en az korkulan siber suç türü siber taciz olup, bu suçun mağdur olmaktan en az korkulan suçlar arasında yer almasında araştırma örnekleminin %67,80'ini erkeklerin oluşturmakta olmasının etkili olabileceği söylenebilecektir.

Teknokent çalışanlarının "zaman zaman korku yaşıyorum" seçeneğini en fazla seçmiş oldukları siber suçlara bakıldığında ise ilk beş sıra;

1- Bilgisayar Korsanlığı (Hacking) (%69,8 - 180 kişi),
2- Casus Yazılımlar (%58,1 - 154 kişi),
3- Virüsler, Truva Atları (%56,6 - 150 kişi),
4- Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi (%55,3 - 147 kişi),
5- Kimlik Hırsızlığı (%55,3 - 146 kişi) suçlarından oluşmaktadır.

Burada 2., 3., 4. ve 5. Sırada yer alan siber suçların birbirlerine yakın sayıda katılımcı tarafından seçilmiş oldukları ancak ankette "bilişim sisteminize hukuka aykırı olarak girilmesi ve sistemde kalınmaya devam edilmesi olarak adlandırılan bilgisayar korsanlığı (hacking)" şeklinde tarif edilmiş olan suçun ise teknokent çalışanlarının zaman zaman korku yaşadıkları siber suçlar arasında açık ara ilk sırada olduğu görülmektedir.

Teknokent çalışanlarının “genellikle korku yaşıyorum” seçeneğini en fazla seçmiş oldukları siber suçlar arasında ilk beş sırada ise;

1- Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız (%35,2 - 93 kişi),
2- Kimlik Hırsızlığı (%30,7 - 81 kişi),
3- Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi (%29,3 - 78 kişi),
4- Siber Hırsızlık (%29,1 - 77 kişi),
5- Casus Yazılımlar (%25,3 - 67 kişi) bulunmaktadır.

Bununla birlikte ankette katılımcılara yöneltilmiş olan her bir siber suç açısından teknokent çalışanlarınca işaretlenmiş olan “zaman zaman korku yaşıyorum” ve “genellikle korku yaşıyorum” seçenekleri toplamının teknokent çalışanlarının en fazla siber suç korkusu yaşadıkları suçların sıralamasını ortaya koyabileceği söylenebilir.

Bu bağlamda teknokent çalışanlarının “zaman zaman korku yaşıyorum” ve “genellikle korku yaşıyorum” seçeneklerini en fazla işaretlemiş oldukları ilk beş siber suçu;

1- Kimlik Hırsızlığı (%86 - 227 kişi),
2- Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi (%84,6 - 225 kişi),
3- Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız (%83,7 - 221 kişi),
4- Casus Yazılımlar (%83,4 - 221 kişi),
5- Siber Hırsızlık (%83,1 - 220 kişi) oluşturmaktadır.

Dolayısıyla bu sıralamadan teknokent çalışanlarının en fazla korku yaşamakta oldukları ilk beş siber suçun birbirlerine oldukça yakın sayıda işaretlenmiş oldukları ve en fazla korkulmakta olan siber suçun ise ankette “Kişisel Verilerinizin Rızanız Dışında Hukuka Aykırı Olarak Üçüncü Kişilere Verilmesi, Yayılması ya da Bu Verilerin Üçüncü Kişiler Tarafından Ele Geçirilmesi olarak adlandırılabilecek olan Kimlik Hırsızlığı” şeklinde

tarif edilmiş olan siber suç türü olduğu görülmektedir. Bu veriler sonucunda teknokentte çalışan bireylerin özellikle kişisel verileri, elektronik haberleşmeleri, banka veya kredi kartları gibi konulara ilişkin siber suç türlerinden diğerlerine göre daha fazla korkmakta oldukları görülmektedir.

4.1.3. Teknokent Çalışanlarının Geçmiş Siber Suç Mağduriyeti Düzeyleri

Tablo 7. Katılımcıların Son 12 Ay İçerisindeki Siber Suç Mağduriyetlerine Göre Dağılımı

	Sayı	Yüzde	Geçerli Yüzde
Mağdur Olmayanlar	227	85,3	86,6
Mağdur Olanlar	35	13,2	13,4
Toplam	262	98,5	100
Cevapsız	4	1,5	
Genel Toplam	266	100	

Katılımcıların geçmiş siber suç mağduriyetlerine göre dağılımları Tablo 7'de gösterilmiş olup, tabloya göre teknokent çalışanlarından 227 kişi son 12 ay içerisinde herhangi bir siber suçtan mağdur olmamış, 35 kişi ise son 12 ay içerisinde en az bir siber suçtan mağdur olmuştur. Dolayısıyla bu soruya cevap veren teknokent çalışanlarının %86,6 gibi oldukça yüksek bir oranla son 12 ay içerisinde siber suç mağduriyeti yaşamamış olduğu görülmektedir.

Tablo 8. Katılımcıların Son 12 Ay İçerisindeki Siber Suç Mağduriyeti Oranları

	Sayı	Yüzde	Geçerli Yüzde
Bilgisayar Korsanlığı (Hacking) Mağduriyeti	5	1,9	15,2
Denial of Service (DoS) Saldırıları Mağduriyeti	2	0,8	6,1
Virüsler, Truva Atları ve Zararlı Yazılımlar Mağduriyeti	6	2,3	18,2
Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğrama Mağduriyeti	6	2,3	18,2

Casus Yazılımlar Mağduriyeti	1	0,4	3
Kimlik Hırsızlığı Mağduriyeti	1	0,4	3
Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi Mağduriyeti	0	0	0
Siber Zorbalık Mağduriyeti	2	0,8	6,1
Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü) Mağduriyeti	3	1,1	9,1
Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi Mağduriyeti	0	0	0
Siber Hırsızlık Mağduriyeti	2	0,8	6,1
Siber Dolandırıcılık Mağduriyeti	5	1,9	15,2
Siber Taciz Mağduriyeti	4	1,5	12,1
Siber Tehdit ve Şantaj Mağduriyeti	5	1,9	15,2
Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu Mağduriyeti	1	0,4	3
Siber Terörizm Mağduriyeti	0	0	0
Toplam	43	16,5	130,5

Katılımcıların son 12 ay içerisindeki siber suç mağduriyeti oranları Tablo 8'de gösterilmiş olup, anket verilerine göre 35 teknokent çalışanı (2 çalışan hangi suçtan mağdur olduğunu belirtmemiştir) son 12 ay içerisinde toplamda 43 siber suçtan mağdur olmuşlardır. Ayrıca bu soru açısından 3 katılımcı diğer seçeneğini işaretleyerek sırasıyla bilgisayar ortamındaki bilginin kötü amaçlı kullanımı, gerçekte olmayan bir iş ilanı başvurusu ve görüşme için başka bir ülkeye davet ve sahte hesaplardan rahatsız edilme konularından mağdur olduklarını belirtmişlerdir. Yukarıdaki tabloya göre teknokent çalışanlarının son 12 ay içerisinde en yoğun olarak mağdur olmuş oldukları suçların Virüsler, Truva Atları ve Zararlı Yazılımlar (6 kişi), Banka veya Kredi Kartlarının (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğranılması (6 kişi), Bilgisayar Korsanlığı (Hacking) (5 kişi), Siber Dolandırıcılık (5 kişi), Siber Tehdit ve Şantaj (5 kişi) şeklinde devam ettiği görülmektedir.

Tablo 9. Geçmiş Siber Suç Mağduriyetinin Alınan Önlemlerde Meydana Getirdiği Değişiklik

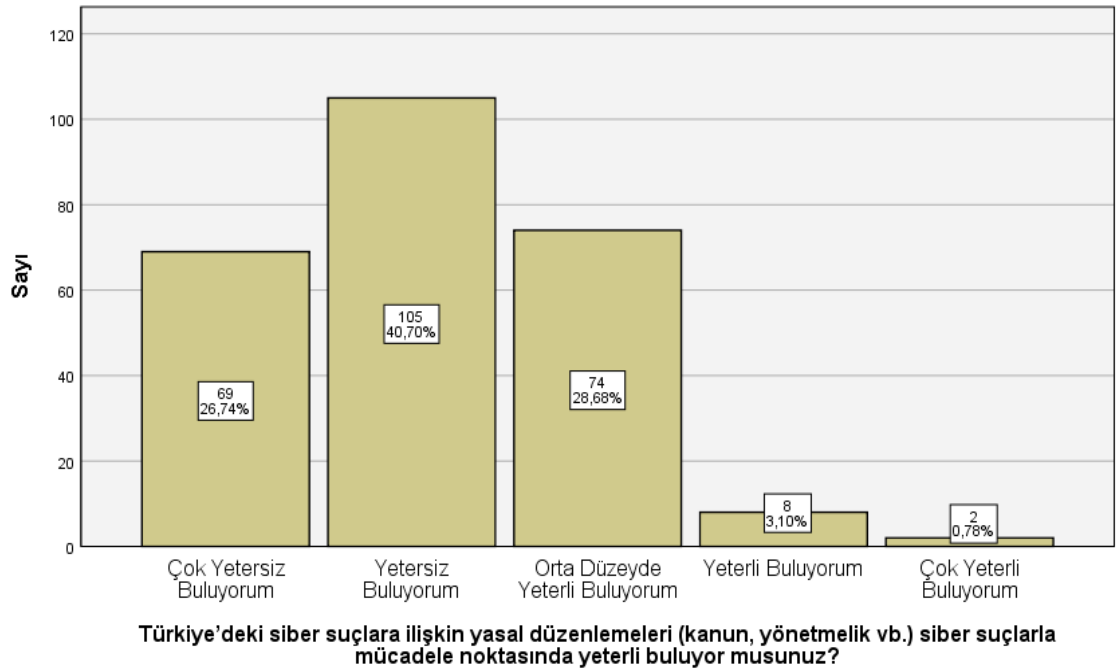
	Sayı	Yüzde	Geçerli Yüzde
Geçmişte de herhangi bir önlem almıyordum, şu anda da almıyorum.	3	1,1	8,6
Geçmişte herhangi bir önlem almıyordum ama şu anda bazı önlemler alıyorum.	10	3,8	28,6
Geçmişte bazı önlemler alıyordum ama şu anda daha az önlem alıyorum.	1	,4	2,9
Geçmişte bazı önlemler alıyordum, şu anda da aynı önlemleri alıyorum.	6	2,3	17,1
Geçmişte bazı önlemler alıyordum ama şu anda daha fazla önlem alıyorum.	15	5,6	42,9
Toplam	35	13,2	100,0
Cevapsız	231	86,8	
Genel Toplam	266	100,0	

Geçmişte siber suç mağduriyeti yaşamış olan Teknokent çalışanlarının yaşamış oldukları mağduriyetin almış oldukları önlemlerde herhangi bir değişiklik meydana getirip getirmediği Tablo 9'da gösterilmiştir. Buna göre geçmişte siber suçlardan Mağdur olmuş 35 teknokent çalışanının yüzde 61,5'lik kısmı (25 kişi) yaşamış oldukları mağduriyet sonrasında almış oldukları önlemleri artırdıklarını belirtmişlerdir.

4.1.4. Teknokent Çalışanlarının Yasal Düzenlemeler ve İşlemlere İlişkin Algıları

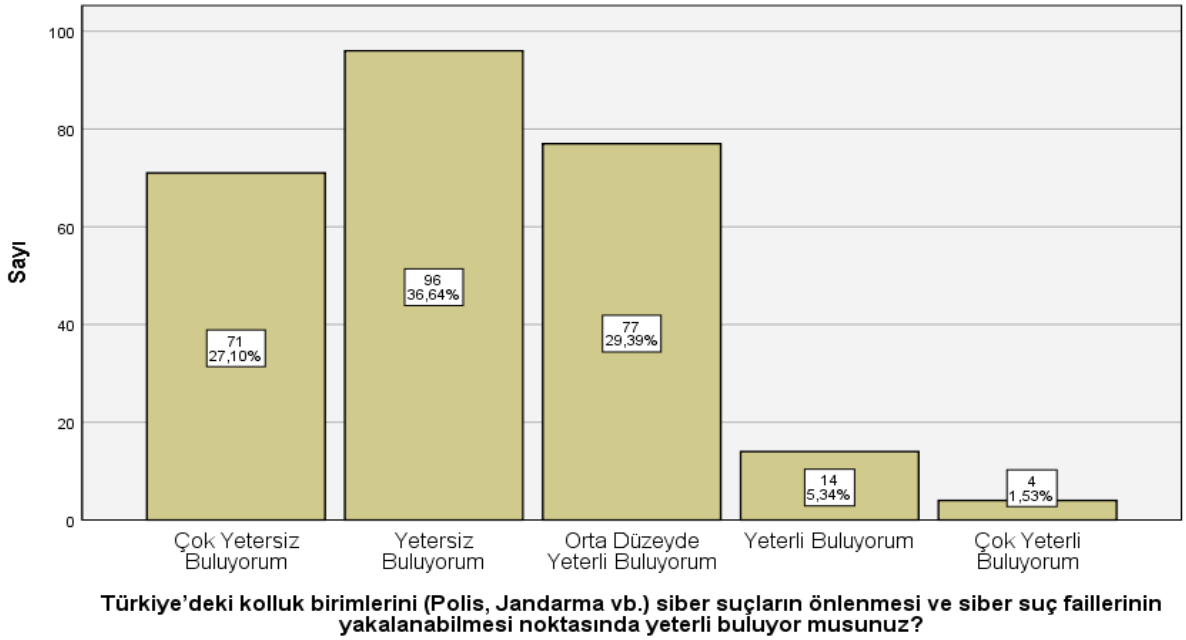
Araştırmaya katılan teknokent çalışanlarının yasal düzenlemeler ve işlemlere ilişkin algıları aşağıdaki grafik ve tablolarda sunulmuştur.

Grafik 5. Katılımcıların Siber Suçlara İlişkin Yasal Düzenlemelere Dair Algıları



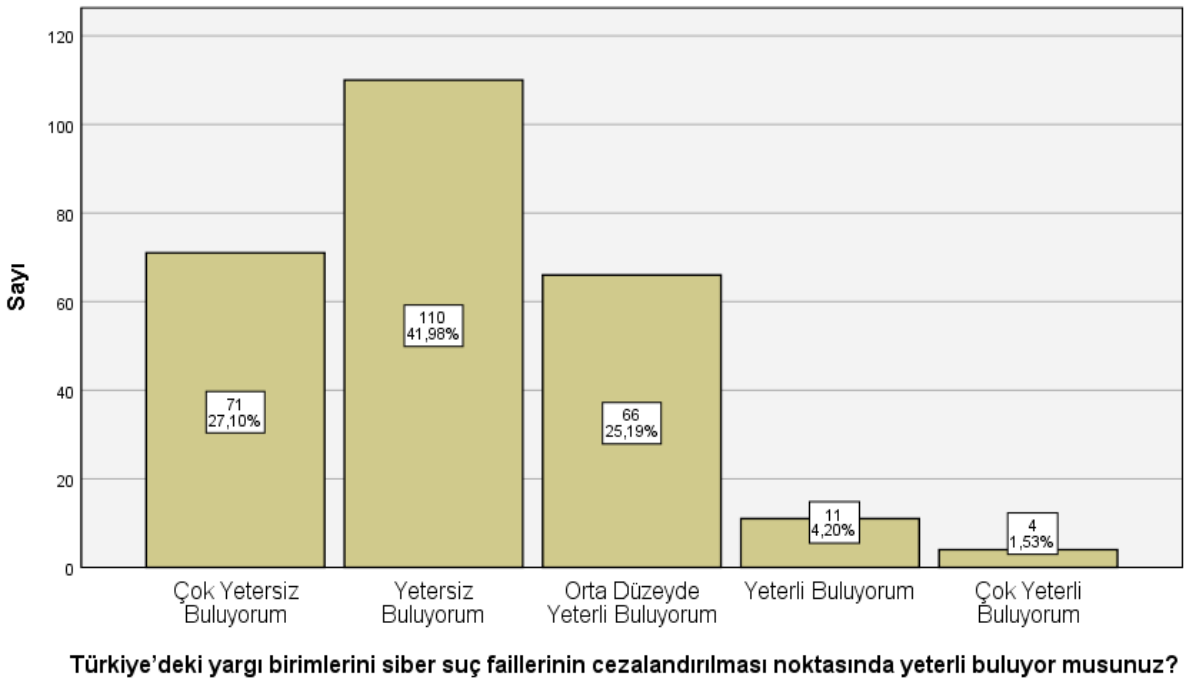
Katılımcıların siber suçlara ilişkin yasal düzenlemelere dair algıları Grafik 5'te gösterilmiştir. Grafiğe göre bu soruya cevap vermiş olan toplam 258 Teknokent çalışanının %67,44'ü (174 kişi) Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yetersiz veya çok yetersiz bulduklarını belirtmişlerdir. Katılımcıların %28,68'i (74 kişi) yasal düzenlemeleri orta düzeyde yeterli bulurken, %3,88 oranı ile oldukça düşük sayıdaki katılımcılar (10 kişi) ise yasal düzenlemeleri yeterli veya çok yeterli bulduklarını belirtmişlerdir. Dolayısıyla Türkiye'deki siber suçlara ilişkin yasal düzenlemelerin (kanun, yönetmelik vb.) katılımcıların çoğunluğu tarafından siber suçlarla mücadele noktasında yeterli bulunmadığı görülmektedir.

Grafik 6. Katılımcıların Siber Suçlar Konusunda Kolluk Birimlerine İlişkin Algıları



Katılımcıların Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli bulup bulmadıkları Grafik 6'da gösterilmiştir. Grafiğe göre bu soruya cevap veren 262 teknokent çalışanının %63,74'ü (167 kişi) Türkiye'deki kolluk birimlerini siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yetersiz veya çok yetersiz bulmaktadır. Türkiye'deki kolluk birimlerini bu konularda orta düzeyde yeterli gören katılımcı oranı %29,39 (77 kişi) iken, yeterli veya çok yeterli bulan katılımcı oranı ise %6,87 (18 kişi)'dir. Dolayısıyla Türkiye'deki kolluk birimlerinin (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında katılımcıların çoğunluğu tarafından yeterli bulunmadığı görülmektedir.

Grafik 7. Katılımcıların Siber Suçlar Konusunda Yargı Birimlerine İlişkin Algıları



Katılımcıların Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli bulup bulmadıkları Grafik 7'de gösterilmiştir. Grafiğe göre bu soruya cevap veren 262 teknokent çalışanının %69,08'i (181 kişi) Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yetersiz veya çok yetersiz bulmaktadır. Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında orta düzeyde yeterli gören katılımcı oranı %25,19 (66 kişi) iken, yeterli veya çok yeterli bulan katılımcı oranı ise %5,73 (15 kişi)'dir. Dolayısıyla Türkiye'deki yargı birimlerinin siber suç faillerinin cezalandırılması noktasında katılımcıların çoğunluğu tarafından yeterli bulunmadığı görülmektedir.

Araştırmanın bu bölümünde katılımcılara "Türkiye'deki siber suçlara ilişkin yasal düzenlemeler, kolluk birimleri ve yargı işlemlerine ilişkin eklemek istediğiniz görüşleriniz varsa lütfen belirtiniz " şeklinde açık uçlu bir soru da yöneltilmiştir. Bu açık uçlu soruya araştırmaya katılan 266 teknokent çalışanının 57'si cevap vermiştir. Bu soruya verilen cevaplardan bir kısmı aşağıda sıralanmıştır:

- “Bilişim dünyası sürekli gelişmekte ve bunun yansıması olarak siber suçlar çeşitlenmekte, aynı kalmamaktadır. Kanunlarda siber suçlar tanımı doğru yapılmalı ve gelişmelere bağlı olarak güncellenmelidir.”
- “Böyle kritik bir işin eğitim düzeyi yüksek ve bu konuda kendini yetiştirmiş kişilere bırakılması çok daha isabetli olabilir.”
- “Bu anlamda yetiştirilmiş tecrübeli kişi ve kurumlara ihtiyaç olduğunu düşünüyorum.”
- “Adaletin olmadığı bir ülkede suçun öneminin olduğunu düşünmüyorum.”
- “Cezalar daha caydırıcı olmalı. Buna ilişkin yasal düzenlemelerde iyileştirmeye gidilmeli.”
- “Birimler yetersiz ve bilgisiz. Kanunlar belirli suçlar için keskin ve net iken kişisel haklar konusunda duyarsız.”
- “Siber suçların da normal suçlardan farklı olmadığının yasal düzenlemelerde netleştirilmesi gerekir. Kolluk birimleri bünyesinde yetkin personel sayısı artırılmalı ve gelişimlerine önem verilmeli.”
- “Siber suçlarla ilgili yetkin personellerin devlete alınmasını veya personellerin masrafları karşılanarak gerekli eğitimleri almasını elzem görüyorum.”
- “Siber suç tanımı doğru yapılamadığı için suçun tespitinde de sıkıntı yaşanıyor.”
- “Yasal düzenlemelerin fikir özgürlüğünü engelleme (muhalif sesleri bastırma) amacına değil gerçek suçlara yönelik olması gerektiğini düşünüyorum.”
- “Ağır maddi ve manevi (hapis) cezaları getirilmeli.”
- “Siber güvenlik için ayrı bir yasa yok, diğer kısımlarda yer verilmiş durumda sadece. Bunlar çok detaylı olmadığı için yetersiz kalıyor. Siber suçlarla ilgili hükümler detaylandırılmalı.”
- “Bazen saniyeler bile önem taşıyor, mücadele daha hızlı olmalı.”
- “Diğer suçlarda olduğu gibi suçluyu siz bulmadığınız sürece gerekli emniyet desteği yok. Suçlunun bulunması için daha ciddi ve odaklı çalışmaları lazım.”

Verilen cevaplar incelendiğinde bu soruya cevap veren katılımcıların büyük bir çoğunluğunun Türkiye’deki yasal düzenlemeler, kolluk birimleri ve yargı işlemlerini yetersiz bulmakta olduğu, kanuni düzenlemelerin netleştirilerek siber suç tanımının doğru yapılması, kolluk birimlerinin eğitimi ve yetkin personel sayısının artırılması, yargı

birimlerinin adil davranması ve cezaların caydırıcı olması gibi konulardaki görüşlerin yoğunlukta olduğu görülmektedir.

Sonuç olarak bu veriler ışığında Ankara'daki teknokent çalışanlarından oluşan katılımcıların Türkiye'deki siber suçlara ilişkin yasal düzenlemeler, kolluk birimleri ve yargı birimlerine ilişkin algılarının genel olarak benzer olduğu ve bu algıların Türkiye'deki yasal düzenlemeler ve birimlerin orta düzeyde yeterli, yetersiz veya çok yetersiz oldukları yönünde ağırlık kazandığı görülmektedir.

4.1.5. Teknokent Çalışanlarının Siber Suç Korkusuna İlişkin Önlem Alma/Başa Çıkma Stratejileri

Bu araştırmada teknokent çalışanlarının siber suç korkusu ile önlem alma/başa çıkma stratejilerini üçe ayırmak mümkündür;

1) İnternet üzerinden kişisel ve/veya hassas bilgilerinizi (kimlik bilgileri, kredi/banka kartı bilgileri, adres bilgileri, cep telefonu numarası vb.) kullanılarak gerçekleştirilen online işlemler ve bunlara ilişkin önlem ve stratejiler,
2) Sosyal medya hesabı sahipliği ve sosyal medyada kullanılan önlemler ve stratejiler,
3) İş yerinde ve iş yeri dışında kullanılan elektronik cihazlarda kullanılan önlem ve stratejiler.

4.1.5.1. Kişisel ve/veya Hassas Bilgiler Kullanılarak Gerçekleştirilen Online İşlemler ve Önlem Alma/Başa Çıkma Stratejileri

Tablo 10. Katılımcıların İnternet Üzerinden Kişisel ve/veya Hassas Bilgileri ile Online İşlem Gerçekleştirme Durumları

	Sayı	Yüzde	Geçerli Yüzde
Gerçekleştirenler	263	98,9	100,0
Gerçekleştirmeyenler	0	0,0	
Cevapsız	3	1,1	
Toplam	266	100,0	

Tablo 10'da internet üzerinden kişisel ve/veya hassas bilgilerini (kimlik bilgileri, kredi/banka kartı bilgileri, adres bilgileri, cep telefonu numarası vb.) kullanarak online işlem gerçekleştirip gerçekleştirmedikleri sorulan teknokent çalışanları arasından bu soruya cevap vermeyen 3 katılımcı dışında kalan 263 katılımcının tamamının online işlem gerçekleştirmekte oldukları yönünde cevap verdiği görülmüştür.

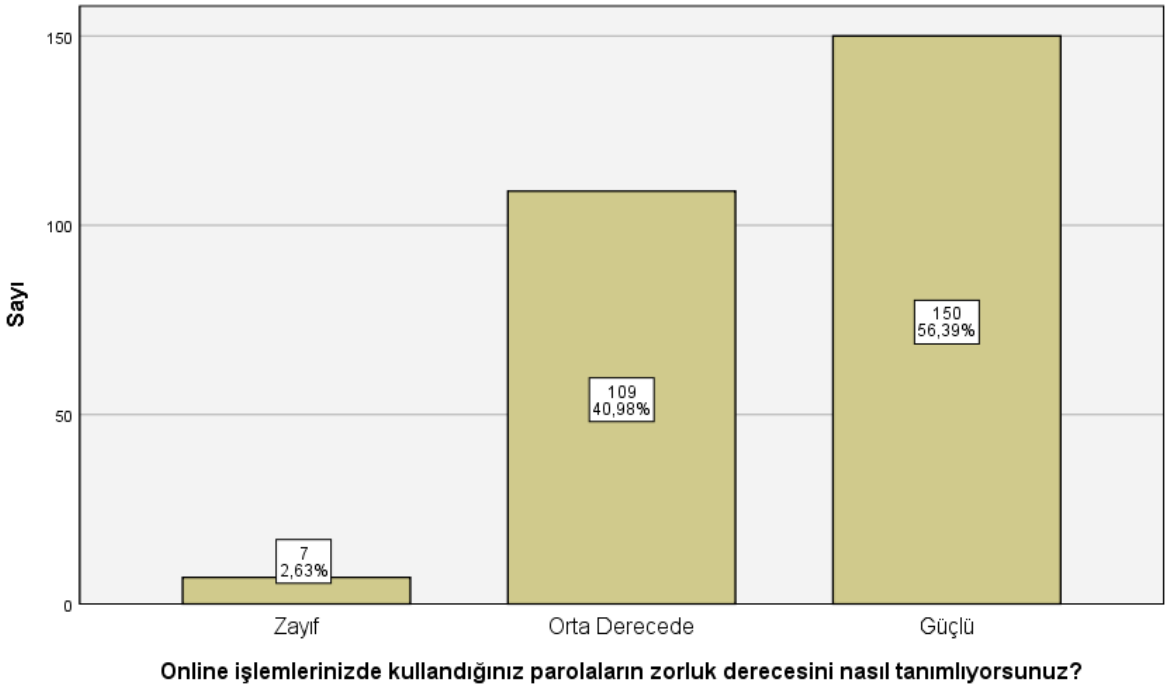
Tablo 11. Katılımcıların İnternet Üzerinden Kişisel ve/veya Hassas Bilgileri ile Gerçekleştirdikleri Online İşlemler

	Sayı	Yüzde	Geçerli Yüzde	Toplam Cevap	Cevapsız	Genel Toplam
İnternet Bankacılığı İşlemleri	251	94,4	95,4	263	3	266
Online Alışveriş	234	88,0	89,0	263	3	266
E-devlet İşlemleri	233	87,6	88,6	263	3	266
E-mail Hesabı İşlemleri	237	89,1	90,1	263	3	266
ÖSYM, MEB, YÖK vb. Sınav İşlemleri (Başvuru, sonuç öğrenme vb.)	188	70,7	71,5	263	3	266
Mobil Operatörünüz (Turkcell, Vodafone, Türk Telekom vb.) ile İlgili Online İşlemler	201	75,6	76,4	263	3	266
Uçak, Otobüs, Tren vb. Online Bilet Rezervasyon, Satın Alma İşlemleri	232	87,2	88,2	263	3	266
Otel, Pansiyon, Turlar vb. Konaklama, Gezi, Seyahat Rezervasyon İşlemleri	191	71,8	72,6	263	3	266
Diğer	3	1,2	1,2	3		

Tablo 11'de bu araştırmaya katılan teknokent çalışanlarının internet üzerinden kişisel ve/veya hassas bilgilerini kullanarak gerçekleştirdikleri online işlemler yer almaktadır. Bu tabloya göre katılımcılar internet üzerinden kişisel ve/veya hassas bilgilerini kullanarak en fazla internet bankacılığı işlemlerini gerçekleştirmekte ve bunu sırasıyla e-

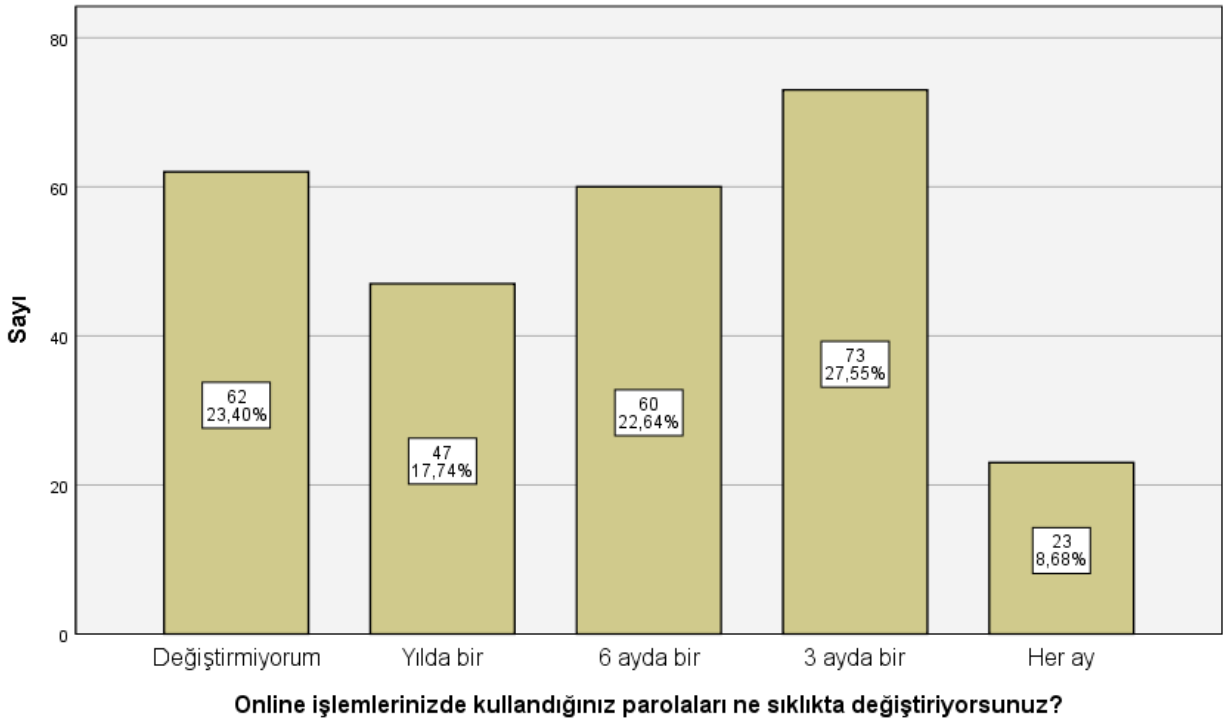
mail hesabı işlemleri, online alışveriş, e-devlet işlemleri, online bilet rezervasyon, satın alma işlemleri, mobil operatörler ile ilgili işlemler, gezi, seyahat rezervasyon işlemleri ve sınav işlemleri takip etmektedir. Bu soruya diğer cevabını veren üç katılımcının biri internet üzerinden her türlü online işlemi gerçekleştirdiğini, ikincisi sinema, tiyatro, konser bilet alımlarını internet üzerinden gerçekleştirdiğini, üçüncüsü ise dijital bir oyun dağıtım platformu olan steam'i kullandığını belirtmiştir. Bu soru birden fazla seçenek işaretlenebilen bir soru olduğundan gerçekleştirilen online işlem sayıları toplamı örneklem sayısı olan 266'dan daha fazla çıkmaktadır.

Grafik 8. Katılımcıların Online İşlemlerinde Kullandıkları Parolaların Zorluk Dereceleri



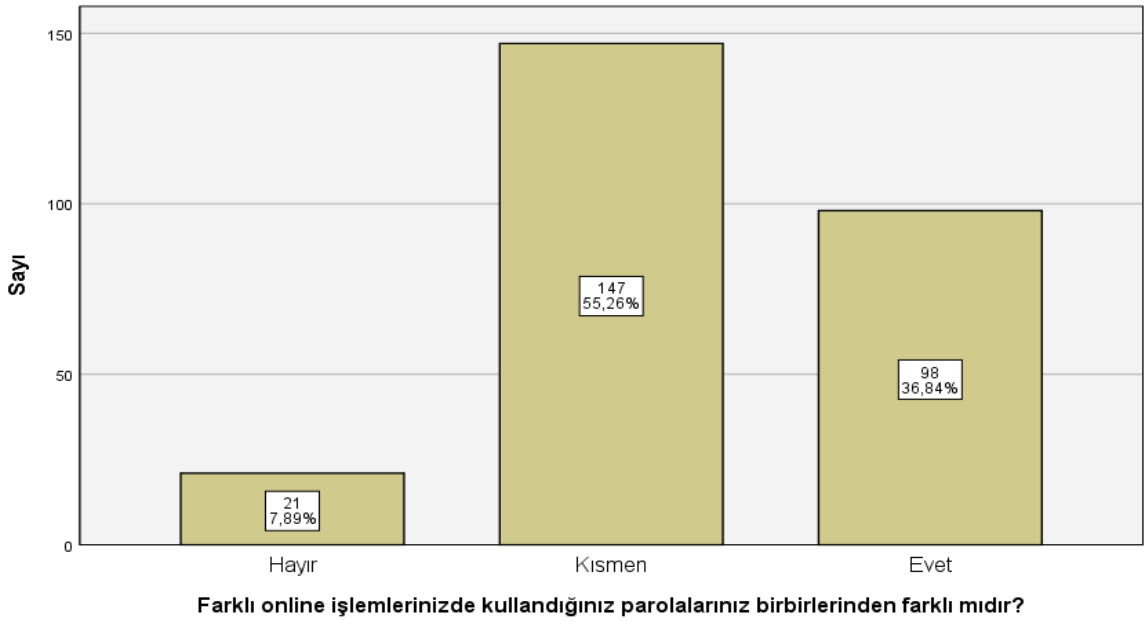
Grafik 8'de araştırmaya katılan ve bu soruya cevap veren 266 teknokent çalışanının online işlemlerinde kullandıkları parolaların zorluk dereceleri gösterilmiştir. Buna göre katılımcıların %2,63'ünü (7 kişi) oluşturan çok küçük bir kısmı haricinde kalan teknokent çalışanlarının tamamı online işlemlerinde orta derece ve güçlü zorluk derecelerine sahip parolalar kullanmaktadırlar. Ayrıca katılımcıların yarısından daha fazlasının da güçlü parolalar kullanmakta oldukları görülmektedir.

Grafik 9. Katılımcıların Online İşlemlerinde Kullandıkları Parolaları Değiştirme Sıklıkları



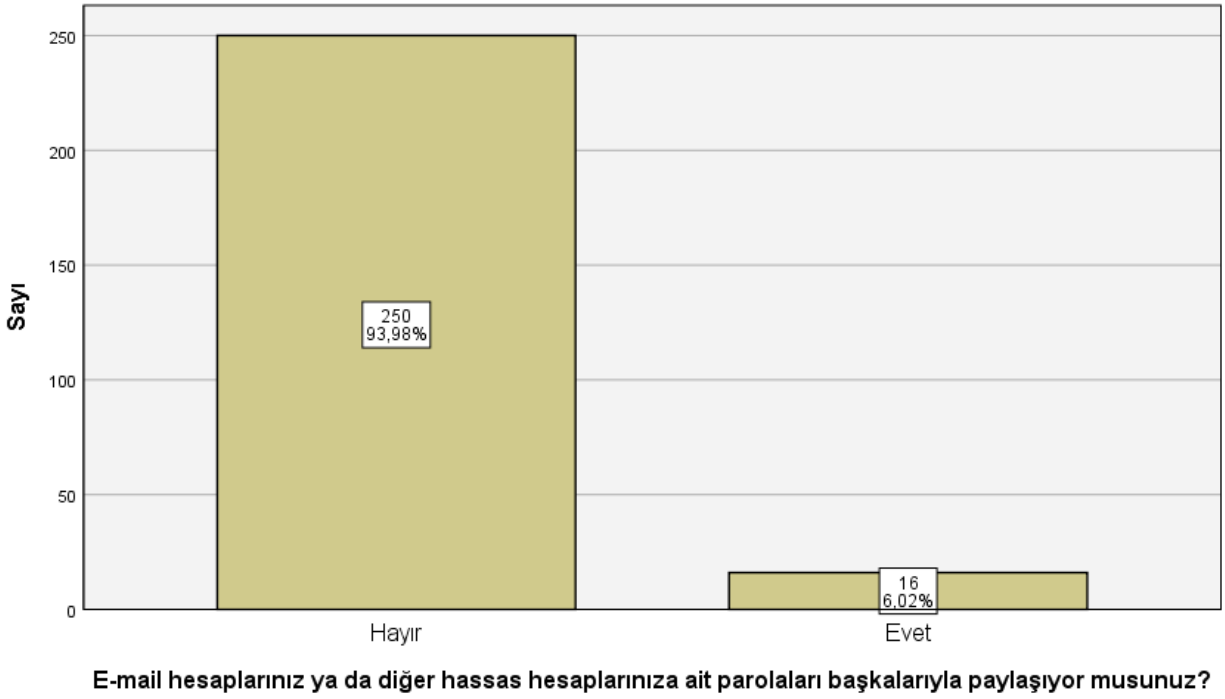
Grafik 9'da araştırmaya katılan 266 teknokent çalışanından bu soruya cevap vermiş olan 265 katılımcının online işlemlerinde kullandıkları parolaları değiştirme sıklıkları yer almaktadır. Grafiğe göre 265 katılımcının %23,40'ı (62 kişi) online işlemlerinde kullandıkları parolaları hiç değiştirmemekte iken, %76,60'ı (203 kişi) ise parolalarını yılda en az bir kez değiştirmektedirler. Parolalarını değiştirmekte olan katılımcılar arasındaki yoğunluk sıralaması ise 3 ayda bir değiştirenler (%27,55 - 73 kişi), 6 ayda bir değiştirenler (%22,64 - 60 kişi), yılda bir değiştirenler (%17,74 - 473 kişi) ve her ay değiştirenler (%8,68 - 23 kişi) şeklindedir.

Grafik 10. Katılımcıların Farklı Online İşlemlerinde Kullandıkları Parolaların Birbirlerinden Farklılık Durumları



Grafik 10'da katılımcıların farklı online işlemlerinde kullandıkları parolaların birbirlerinden farklılık durumları gösterilmiş olup, araştırmaya katılan ve bu soruya cevap veren 266 katılımcının %7,89'u (21 kişi) farklı online işlemlerinde aynı parolayı kullandıklarını belirtirken, % 92,11'i (245 kişi) ise farklı online işlemlerinde birbirlerinden kısmen veya tamamen farklı parolalar kullanmakta olduklarını belirtmişlerdir. Bu soru açısından katılımcıların çoğunluğu %55,26 ile (147 kişi) farklı online işlemlerinde kullandıkları parolaların birbirlerinden kısmen farklı olduğunu belirtmişlerdir.

Grafik 11. Katılımcıların Hassas Hesaplarına İlişkin Parolaları Başkalarıyla Paylaşma Oranları



Grafik 11'de katılımcıların e-mail hesapları ya da diğer hassas hesaplarına ait parolaları başkalarıyla paylaşıp paylaşmama durumları gösterilmiş olup, araştırmaya katılan ve bu soruya cevap veren 266 katılımcının %93,98'i (250 kişi) parolalarını başkalarıyla paylaşmadıklarını, geriye kalan %6,02'lik (16 kişi) kısım ise paylaştıklarını belirtmişlerdir.

4.1.5.2. Sosyal Medya Hesabı Sahipliği ve Önlem Alma/Başa Çıkma Stratejileri

Tablo 12. Katılımcıların Sosyal Medya Hesabı Sahipliği

	Sayı	Yüzde	Geçerli Yüzde
Hayır	27	10,2	10,2
Evet	237	89,1	89,8
Toplam	264	99,2	100,0
Cevapsız	2	0,8	
Genel Toplam	266	100,0	

Tablo 12'de araştırmaya katılan katılımcıların sosyal medya hesabı sahipliği durumları gösterilmektedir. Tabloya göre bu soruya cevap veren 264 teknokent çalışanının %10,2'sinin (27 kişi) sosyal medya hesabı bulunmazken, %89,8'inin (237 kişi) ise en az bir adet sosyal medya hesabı bulunmaktadır. Sosyal medya hesabına sahip olan teknokent çalışanlarının hangi sosyal medya hesaplarına sahip olduklarına ilişkin dağılım ise Tablo 13'te gösterilmektedir.

Tablo 13. Katılımcıların Sahip Oldukları Sosyal Medya Hesabı Türlerine Göre Dağılımı

	Sayı	Yüzde	Geçerli Yüzde	Toplam Cevap	Cevapsız	Genel Toplam
Facebook	208	78,2	79,1	263	3	266
Twitter	149	56,0	56,7	263	3	266
Instagram	187	70,3	71,1	263	3	266
LinkedIn	181	68,0	68,8	263	3	266
Google Plus	112	42,1	42,6	263	3	266
Pinterest	66	24,8	25,1	263	3	266
Reddit	22	8,3	8,4	263	3	266
Snapchat	60	22,6	22,8	263	3	266
Tumblr	15	5,6	5,7	263	3	266
Slideshare	16	6,0	6,1	263	3	266
Diğer (Swarm - 2, Zomato - 1)	3	1,2	1,2	3		

Tablo 13'e göre teknokent çalışanları arasında bu soruya cevap veren katılımcıların en fazla sahip oldukları sosyal medya hesabı türü %79,1 ile (208 kişi) Facebook'tur. Facebook'u sırasıyla bir %71,1 ile (187 kişi) Instagram, %68,8 ile (181 kişi) LinkedIn, %56,7 ile (149 kişi) Twitter, %42,6 ile (112 kişi) Google Plus ve diğer sosyal medya hesapları takip etmektedir. Bu soru birden fazla seçenek işaretlenebilen bir soru

olduğundan sahip olunan sosyal medya hesabı sayıları toplamı örneklem sayısı olan 266'dan daha fazla çıkmaktadır.

Tablo 14. Katılımcıların Sosyal Medya Hesaplarındaki Kişisel Bilgi ve Verileri ile İlgili Önlem Alıp Almama Oranları

	Sayı	Yüzde	Geçerli Yüzde
Önlem almıyorum	37	13,9	15,4
Önlem alıyorum	203	76,3	84,6
Toplam	240	90,2	100,0
Cevapsız	26	9,8	
Genel Toplam	266	100,0	

Tablo 14 katılımcıların sosyal medya hesaplarındaki (Facebook, Twitter, vb.) kişisel bilgi ve verileriyle ilgili siber suç mağduru olmamak adına herhangi bir önlem alıp almadıklarını göstermektedir. Buna göre bu soruya cevap veren katılımcıların %15,4'ü (37 kişi) herhangi bir önlem almadığını belirtirken, %84,6'sı (203 kişi) ise önlem aldıklarını belirtmişlerdir. Önlem aldığını belirten teknokent çalışanlarının hangi önlemleri aldıklarına ilişkin tablo ise aşağıda sunulmuştur.

Tablo 15. Katılımcıların Sosyal Medya Hesapları İle İlgili Almış Oldukları Önlemler

	Sayı	Yüzde	Geçerli Yüzde	Toplam Cevap	Cevapsız	Genel Toplam
Hesabımı kilitli tutuyorum	92	34,6	39,0	236	30	266
Paylaşımlarımı görebilecek kişileri sınırlandırıyorum	149	56,0	62,3	239	27	266
Telefon numaramı hesabıma tanımlıyorum	112	42,1	47,1	238	28	266
Tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmiyorum	142	53,4	59,7	238	28	266

Hesabıma benden habersiz erişimleri engellemek için farklı cihazlardan giriş bildirimlerini aktif hale getiriyorum	133	50,0	55,9	238	28	266
Güvenli gözükmeyen reklam, bağlantı vb. linkleri açmıyorum	145	54,5	61,2	237	29	266
Diğer	12	4,8	4,8	12		

Tablo 15'e göre katılımcıların sosyal medya hesaplarındaki (Facebook, Twitter, vb.) kişisel bilgi ve verileriyle ilgili siber suç mağduru olmamak adına en fazla aldıkları önlem paylaşımlarını görebilecek kişileri sınırlandırmak şeklindedir (%62,3 ile 149 kişi). Bunu güvenli gözükmeyen reklam, bağlantı vb. linkleri açmama (%61,2 ile 145 kişi), tanınmayan kişilerden gelen arkadaşlık isteklerini kabul etmeme (%59,7 ile 142 kişi), hesaba habersiz erişimleri engellemek için farklı cihazlardan giriş bildirimlerini aktif hale getirme (%55,9 ile 133 kişi) ve diğer önlemler takip etmektedir. Ayrıca katılımcılar diğer seçeneği içerisinde 2 aşamalı doğrulama, two factor authentication ve şifreleri kimseyle paylaşmama gibi önlemler de aldıklarını belirtmişlerdir.

4.1.5.3. İş Yerinde ve Dışında Kullanılan Elektronik Cihazlarla İlgili Önlem Alma/Başa Çıkma Stratejileri

Tablo 16. Katılımcıların Elektronik Cihazlarına Parola Koyma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	27	10,2	10,4	Hayır	26	9,8	10,1
Evet	233	87,6	89,6	Evet	231	86,8	89,9
Toplam	260	97,7	100,0	Toplam	257	96,6	100,0
Cevapsız	6	2,3		Cevapsız	9	3,4	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların işyerleri ve dışında kullanmakta oldukları elektronik cihazlara kullanıcı parolası koyup koymama oranları Tablo 16'da gösterilmiş olup, İş yerinde ve dışında kullanılan cihazlarda parola koyma oranlarının parola koymama oranlarına göre oldukça fazla olduğu görülmektedir. Soruya cevap veren katılımcıların %90'a yakını işyerinde ve dışında kullandıkları elektronik cihazlara parola koyduklarını belirtmişlerdir. Bununla birlikte işyerinde ve dışında kullanılan cihazlar açısından oranların birbirine oldukça yakın olduğu da görülmektedir.

Tablo 17. Katılımcıların Online İşlemlerinde VPN Kullanma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	126	47,4	48,5	Hayır	124	46,6	48,2
Bazen	71	26,7	27,3	Bazen	83	31,2	32,3
Evet	63	23,7	24,2	Evet	50	18,8	19,5
Toplam	260	97,7	100,0	Toplam	257	96,6	100,0
Cevapsız	6	2,3		Cevapsız	9	3,4	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların kişisel ve/veya hassas bilgilerinizin ele geçirilmesinden korktukları online işlemlerinde, güvenilir olduğunu düşündükleri bir VPN programı kullanıp kullanmama oranları Tablo 18'de gösterilmiştir. Buna göre katılımcıların yarısına yakını iş yerinde ve dışında kullandıkları elektronik cihazlarda güvenilir olduğunu düşündükleri bir VPN programı kullanmadıklarını belirtmişlerdir. Bununla birlikte katılımcıların yarıdan fazlası ise iş yerinde ve dışında kullandıkları elektronik cihazlarda güvenilir olduğunu düşündükleri bir VPN programı kullanmaktadırlar. Ayrıca bu soru için de katılımcıların işyerinde ve dışında kullandıkları cihazlar açısından oranların birbirine yakın olduğu görülmektedir.

Tablo 18. Katılımcıların Güvenilir Gözükmeyen Web Sayfalarını Ziyaret Etmeyi Sakıncalı Bulma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	34	12,8	12,9	Hayır	32	12,0	12,3
Bazen	67	25,2	25,5	Bazen	75	28,2	28,8
Evet	162	60,9	61,6	Evet	153	57,5	58,8
Toplam	263	98,9	100,0	Toplam	260	97,7	100,0
Cevapsız	3	1,1		Cevapsız	6	2,3	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların güvenilir gözükmeyen web sayfalarını ziyaret etmekte bir sakınca görüp görmeme oranları Tablo 19'da gösterilmiştir. Buna göre bu soruya cevap veren katılımcılar ortalama %87 oranında bazen veya evet cevabı vererek güvenilir gözükmeyen web sayfalarını ziyaret etmekte sakınca gördüklerini belirtmişlerdir.

Tablo 19. Katılımcıların Kullanmadıkları Zamanlarda Bilgisayar Kameralarının Üzerini Kapalı Bulundurma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	188	70,7	73,4	Hayır	170	63,9	65,9
Evet	68	25,6	26,6	Evet	88	33,1	34,1
Toplam	256	96,2	100,0	Toplam	258	97,0	100,0
Cevapsız	10	3,8		Cevapsız	8	3,0	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların bilgisayar kameralarını kullanmadıkları zamanlarda bant, kağıt vb. şeylerle kapalı tutup tutmama oranları Tablo 19'da gösterilmiştir. Tabloya göre katılımcıların çoğunluğu işyerinde ve dışında kullandıkları elektronik cihazlarda bilgisayar

kameralarını kullanmadıkları zamanlarda kapalı tutmadıklarını belirtmişlerdir. Bununla birlikte iş yerindeki elektronik cihazlar için bilgisayar kamerasını kapalı tuttuğunu belirten katılımcı oranı 4'te 1 iken, iş yeri dışındaki elektronik cihazlarda bu oran 3'te 1 düzeyindedir. Dolayısıyla katılımcıların iş yeri dışında kullandıkları elektronik cihazlarda bilgisayar kamerasını kapalı bulundurma oranları iş yerinde kullandıkları elektronik cihazlara göre daha fazladır.

Tablo 20. Katılımcıların Güvenilir Olmayan E-postaları ve Eklerini Açma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	206	77,4	78,9	Hayır	210	78,9	80,8
Bazen	45	16,9	17,2	Bazen	42	15,8	16,2
Evet	10	3,8	3,8	Evet	8	3,0	3,1
Toplam	261	98,1	100,0	Toplam	260	97,7	100,0
Cevapsız	5	1,9		Cevapsız	6	2,3	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların tanımadıkları kişilerden gelen ve güvenilir olmadığını düşündükleri e-posta ve/veya e-posta eklerini açıp açmama oranları Tablo 20'de gösterilmiştir. Tabloya göre bu soruya cevap veren katılımcıların %80 civarının tanımadıkları kişilerden gelen ve güvenilir olmadığını düşündükleri e-posta ve/veya eklerini açmadıklarını görülmektedir. İş yerindeki ve iş yer dışındaki cihazlar açısından katılımcıların davranışları karşılaştırıldığında ise bu konuda oranların birbirlerine oldukça yakın olduğu görülmektedir.

Tablo 21. Katılımcıların Online Alışveriş Yapma Oranları

	Sayı	Yüzde	Geçerli Yüzde
Yapmayanlar	5	1,9	1,9
Yapanlar	255	95,9	98,1
Toplam	260	97,7	100,0
Cevapsız	6	2,3	
Genel Toplam	266	100,0	

Tablo 21'de katılımcıların online alışveriş yapma oranları gösterilmiş olup, tabloya göre bu soruya cevap veren katılımcıların %98,1'lik bir oranla (255 kişi) online alışveriş yapmakta oldukları görülmüştür.

Tablo 22. Katılımcıların Online Alışveriş Sitelerinden Yaptıkları Alışverişlerde Adresin Güvenli Olmasına Dikkat Etme Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	23	8,6	9,2	Hayır	22	8,3	8,8
Nadiren	25	9,4	10,0	Nadiren	26	9,8	10,4
Bazı zamanlar	21	7,9	8,4	Bazı zamanlar	19	7,1	7,6
Çoğu zaman	52	19,5	20,7	Çoğu zaman	52	19,5	20,7
Her zaman	130	48,9	51,8	Her zaman	132	49,6	52,6
Toplam	251	94,4	100,0	Toplam	251	94,4	100,0
Cevapsız	15	5,6		Cevapsız	15	5,6	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların online alışveriş sitelerinden yaptıkları alışverişlerde adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin "https://" ile başlamasına dikkat etme oranları Tablo 22'de gösterilmiştir. Buna göre katılımcılardan bu soruya cevap vermiş olanların %81 civarındaki kısmı bazı zamanlar, çoğu zaman veya her zaman

adres çubuğunun güvenli olmasına dikkat ettiklerini belirtmişlerdir. Adres çubuğunun güvenli olup olmadığına her zaman dikkat ettiğini belirten katılımcı oranının da bu soruya cevap veren katılımcıların %50'sinden daha fazlasını oluşturmakta olduğu görülmektedir. Teknokent çalışanı katılımcıların iş yerindeki ve iş yeri dışında kullanılan elektronik cihazlardaki davranışlarında bir farklılık olup olmadığı incelendiğinde ise bu soru açısından da oranların birbirine oldukça yakın olduğu ve önemli bir farklılık bulunmadığı görülmüştür.

Tablo 23. Katılımcıların İnternet Bankacılığı Hizmetlerini Kullanma Oranları

	Sayı	Yüzde	Geçerli Yüzde
Kullanmayanlar	5	1,9	1,9
Kullananlar	256	96,2	98,1
Toplam	261	98,1	100,0
Cevapsız	5	1,9	
Genel Toplam	266	100,0	

Katılımcıların internet bankacılı hizmetlerini kullanma oranları Tablo 23'te gösterilmiş olup, soruya cevap veren katılımcıların %98,1'inin (256 kişi) internet bankacılığı hizmetlerini kullanmakta oldukları görülmüştür.

Tablo 24. Katılımcıların İnternet Bankacılığı Hizmetlerini Kullanırken Adresin Güvenli Olmasına Dikkat Etme Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	18	6,8	7,1	Hayır	17	6,4	6,7
Nadiren	24	9,0	9,5	Nadiren	25	9,4	9,9
Bazı zamanlar	13	4,9	5,2	Bazı zamanlar	12	4,5	4,8
Çoğu zaman	38	14,3	15,1	Çoğu zaman	42	15,8	16,7
Her zaman	159	59,8	63,1	Her zaman	156	58,6	61,9
Toplam	252	94,7	100,0	Toplam	252	94,7	100,0

Cevapsız	14	5,3		Cevapsız	14	5,3	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların İnternet Bankacılığı hizmetlerini kullanırken adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin "https://" ile başlamasına dikkat etme oranları Tablo 24'te gösterilmiştir. Buna göre katılımcılardan bu soruya cevap vermiş olanların %83 civarındaki kısmı bazı zamanlar, çoğu zaman veya her zaman adres çubuğunun güvenli olmasına dikkat ettiklerini belirtmişlerdir. Adres çubuğunun güvenli olup olmadığına her zaman dikkat ettiğini belirten katılımcı oranının da bu soruya cevap veren katılımcıların %60'ından daha fazlasını oluşturmakta olduğu görülmektedir. Teknokent çalışanı katılımcıların iş yerindeki ve iş yeri dışında kullanılan elektronik cihazlardaki davranışlarında bir farklılık olup olmadığı incelendiğinde ise bu soru açısından da oranların birbirine oldukça yakın olduğu ve önemli bir farklılık bulunmadığı görülmüştür.

Tablo 25. Katılımcıların Elektronik Cihazlarındaki Verilerini Yedekleme Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	55	20,7	21,1	Hayır	59	22,2	22,8
Evet	206	77,4	78,9	Evet	200	75,2	77,2
Toplam	261	98,1	100,0	Toplam	259	97,4	100,0
Cevapsız	5	1,9		Cevapsız	7	2,6	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların elektronik cihazlarındaki verilerini silinme, çalınma vb. durumlara karşı yedekleme oranları Tablo 25'te gösterilmiştir. Buna göre bu soruya cevap veren katılımcıların %78,9'u iş yerinde kullandıkları elektronik cihazlardaki verilerini yedeklediğini belirtirken %77,2'si iş yeri dışında kullandıkları elektronik cihazlardaki verilerini yedeklediğini belirtmiştir. Dolayısıyla katılımcıların büyük çoğunluğu veri yedekleme konusuna hassasiyet göstermekte iken iş yerindeki ve dışındaki cihazlar

açısından yedekleme davranışı oranlarının birbirlerine oldukça yakın olduğu görülmektedir.

Tablo 26. Katılımcıların Bilgisayarlarında Güncel ve Güvenilir Bir Anti-virüs Yazılımı Bulunma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	90	33,8	34,7	Hayır	105	39,5	41,0
Evet	169	63,5	65,3	Evet	151	56,8	59,0
Toplam	259	97,4	100,0	Toplam	256	96,2	100,0
Cevapsız	7	2,6		Cevapsız	10	3,8	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların kullanmakta oldukları bilgisayarda güncel durumda bulanan ve güvenilir bir Anti-virüs yazılımı bulunup bulunmama oranları Tablo 26'da gösterilmiştir. Katılımcılardan bu soruya cevap verenlerin %65,3'ü iş yerinde kullandıkları elektronik cihazlarda güncel ve güvenilir bir Anti-virüs yazılımı bulunduğunu belirtirken, %59'u ise iş yeri dışında kullandıkları elektronik cihazlarda güncel ve güvenilir bir Anti-virüs yazılımı bulunduğunu belirtmiştir. Dolayısıyla katılımcıların iş yerinde kullandıkları elektronik cihazlarında güncel ve güvenilir bir Anti-virüs yazılımı bulunma oranlarının diğerlerine göre daha fazla olduğu görülmektedir. Ayrıca güncel ve güvenilir bir Anti-virüs yazılımı bulunmama oranları teknokent çalışanı katılımcıların iş yeri ve dışında kullandıkları elektronik cihazlar açısından %34,7 ve %41 seviyelerinde olup, katılımcıların 3'te 1'inden daha fazlasını oluşturmaktadır.

Tablo 27. Katılımcıların Bilgisayarlarında Güncel ve Güvenilir Bir Anti-Malware Yazılımı Bulunma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	133	50,0	52,8	Hayır	145	54,5	57,3
Evet	119	44,7	47,2	Evet	108	40,6	42,7
Toplam	252	94,7	100,0	Toplam	253	95,1	100,0
Cevapsız	14	5,3		Cevapsız	13	4,9	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların kullanmakta oldukları bilgisayarda güncel durumda bulunan ve güvenilir bir Anti-Malware yazılımı bulunup bulunmama oranları Tablo 27'de gösterilmiştir. Buna göre bu soruya cevap veren katılımcıların %52,8'i iş yerlerinde kullandıkları elektronik cihazlarda güncel ve güvenilir bir Anti-Malware yazılımı bulunmadığını belirtirken, %57,3'ü iş yeri dışında kullandıkları elektronik cihazlarda bulunmadığını belirtmişlerdir. Dolayısıyla katılımcıların bilgisayarlarında Anti-Malware yazılımı bulunması oranlarının Anti-virüs yazılımlarından farklı olarak daha düşük seviyelerde olduğu görülmektedir.

Tablo 28. Katılımcıların Kullandıkları Elektronik Cihazların İşletim Sistemlerinin Güncel Durumda Olmasına Dikkat Etme Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	42	15,8	16,1	Hayır	47	17,7	18,1
Evet	219	82,3	83,9	Evet	212	79,7	81,9
Toplam	261	98,1	100,0	Toplam	259	97,4	100,0
Cevapsız	5	1,9		Cevapsız	7	2,6	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

Katılımcıların kullanmakta oldukları bilgisayar, cep telefonu, tablet vb. elektronik cihazların işletim sistemlerinin (Windows, OS, Android, iOS vb.) güncel durumda olmalarına dikkat etme oranları Tablo 28'de gösterilmiştir. Buna göre bu soruya cevap veren katılımcıların %83,9'u iş yerinde kullandıkları elektronik cihazların işletim sistemlerinin güncel durumda olmasına dikkat ederken, %81,9'u ise iş yeri dışında kullandıkları elektronik cihazların işletim sistemlerinin güncel durumda olmasına dikkat etmektedirler. Dolayısıyla bu oran iş yerinde kullanılan elektronik cihazlar açısından daha yüksek bulunmakla birlikte aradaki fark çok büyük değildir.

Tablo 29. Katılımcıların Kullandıkları Bilgisayarlarında Açık Durumda Olan Bir Güvenlik Duvarı Bulunma Oranları

İŞ YERİNDE kullanılan elektronik cihazlar				İŞ YERİ DIŞINDA kullanılan elektronik cihazlar			
	Sayı	Yüzde	Geçerli Yüzde		Sayı	Yüzde	Geçerli Yüzde
Hayır	49	18,4	18,9	Hayır	54	20,3	21,0
Evet	210	78,9	81,1	Evet	203	76,3	79,0
Toplam	259	97,4	100,0	Toplam	257	96,6	100,0
Cevapsız	7	2,6		Cevapsız	9	3,4	
Genel Toplam	266	100,0		Genel Toplam	266	100,0	

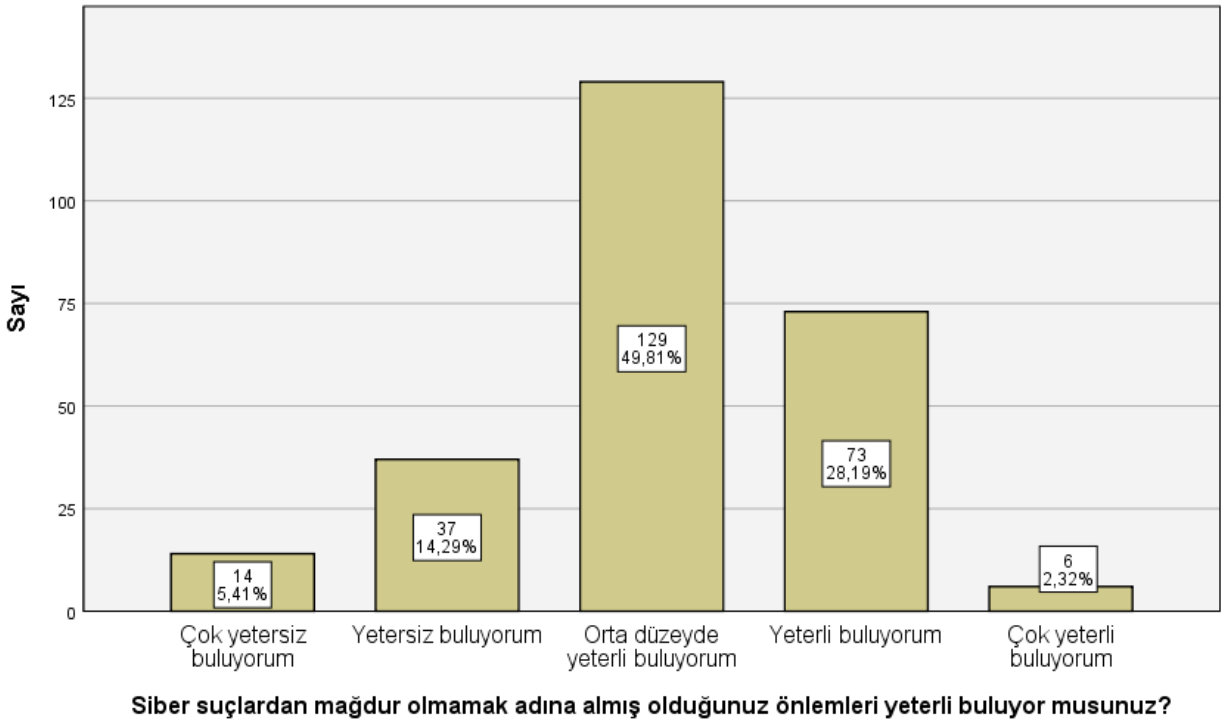
Katılımcıların kullanmakta olduğunuz bilgisayarda açık durumda olan bir Güvenlik Duvarı (Windows güvenlik duvarı vb.) bulunup bulunmama oranları Tablo 29'da gösterilmiştir. Buna göre bu soruya cevap veren katılımcıların %81,1'i iş yerinde kullandıkları elektronik cihazlarda açık durumda olan bir Güvenlik Duvarı bulunmasına dikkat ettiklerini belirtirken, %79'u ise iş yeri dışında kullandıkları elektronik cihazlarda açık durumda olan bir Güvenlik Duvarı bulunmasına dikkat ettiklerini belirtmişlerdir. Dolayısıyla bu oran da iş yerinde kullanılan elektronik cihazlar açısından daha yüksek bulunmakla birlikte aradaki fark çok büyük değildir.

Tüm bu önlem alma/başa çıkma stratejilerine ilişkin sorulara ilaveten katılımcılara bir de açık uçlu soru yöneltilmiş ve bu soruda ankette yer alan konular dışında almış oldukları farklı önlemler/stratejiler varsa belirtmeleri istenmiştir. Bu soruya cevap veren katılımcı

sayısı 27 kişi olup, verilen cevaplardan bir kısmı; Windows işletim sistemi kullanmamak, online alışverişlerde 3D ödeme seçeneği ve limiti sınırlı kredi kartı kullanmak, Linux işletim sistemi kullanmak, açık kaynaklı projeleri tercih etmek, MAC bilgisayar ve IOS işletim sistemi kullanmak, parolamı hatırla seçeneğini hiçbir zaman kullanmamak, lisansı bulunmayan ürün kullanmamak ve Ubuntu işletim sistemi kullanmaktır.

Uygulanan anket çalışmasında yer alan son soru ise katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulup bulmadıklarını belirlemeyi amaçlamaktadır. Bu soruya ilişkin grafik de aşağıda sunulmuştur.

Grafik 12. Katılımcıların Siber Suçlardan Mağdur Olmamak Adına Almış Oldukları Önlemleri Yeterli Bulma Oranları



Grafiğe göre katılımcıların yarısına yakını siber suçlardan mağdur olmamak adına almış oldukları önlemleri orta düzeyde yeterli bulmakta iken, yeterli veya çok yeterli bulan katılımcı oranı %30,51, yetersiz veya çok yetersiz bulan katılımcı oranı ise %19,70'tir.

4.2. HİPOTEZLERİN ANALİZİ

Araştırmada uygulanan anket formuna ilişkin betimsel verilerin analizinin ardından araştırma hipotezlerinin analizine geçilebilir. Bu araştırmada hipotez olarak yer almamakla birlikte araştırmanın bir öngörüsünün "Ankara'daki teknokentlerde (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışan bireyler üzerinde siber suç korkusu bulunduğu" şeklinde olduğu söylenebilir. Buna göre bu öngörüyü araştırmada katılımcılara yöneltilmiş olan toplam 16 adet siber suça ilişkin korku düzeyleri üzerinden incelemek mümkündür.

Bu araştırmaya katılan teknokent çalışanlarının kendilerine yöneltilmiş olan 16 adet siber suça ilişkin korku düzeyleri yukarıdaki bölümde Tablo 6'da gösterilmiştir. Bu tabloya göre ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark'ta çalışmakta olup bu araştırmaya katılan teknokent çalışanlarının kendilerine yöneltilmiş olan 16 adet siber suç türünün 14'ü için %50'den daha fazla oranda "zaman zaman korku yaşıyorum" ve "genellikle korku yaşıyorum" cevabı vermiş oldukları görülmektedir. Bu araştırmaya katılan teknokent çalışanları yalnızca "Bilişim Sistemleri Aracılığıyla Hakaret" ve "Siber Taciz" suçları için sırasıyla %54,5 ve %53,8 oranlarında "hiç korku yaşamıyor olduklarını" belirtmişlerdir. Dolayısıyla araştırmaya katılan teknokent çalışanlarının araştırmada yer alan siber suçların çoğunluğu için korku yaşamakta oldukları, yalnızca iki adet siber suç için ise %50'nin biraz üzerinde bir oranla korku yaşamamakta oldukları görülmüştür.

4.2.1. Katılımcıların Yaşları, Cinsiyetleri, Eğitim Durumları ve Gelir Düzeyleri ile Siber Suç Korkusu Arasındaki İlişki

Yukarıda belirtilen öngörünün ardından araştırmanın ilk hipotezi "bireylerin yaş, cinsiyet, eğitim durumu ve gelir düzeyleri ile siber suç korkuları arasında anlamlı bir ilişki bulunmaktadır" şeklindedir.

Bu hipotezin test edilebilmesi amacıyla ilk olarak katılımcıların yaşları ile siber suç korkusu oranları arasında anlamlı bir ilişki bulunup bulunmadığı çapraz tablolardan ve ki kare analizinden yola çıkılarak incelenmiştir. Araştırmada katılımcılara yöneltilen toplam

16 siber suç türünden denial of service (DoS) saldırıları, bilişim sistemleri aracılığıyla hakaret ve siber taciz korkusu ile yaş arasındaki ilişki için yeterinde veri bulunmadığından ki kare analizi sonucu yorumlanamamaktadır. Bununla birlikte geriye kalan ve ki kare analizi sonuçları yorumlanabilen 13 siber suç korkusu ile yaş arasında ise anlamlı bir ilişki bulunmamaktadır (p>0.05).

İkinci olarak katılımcıların cinsiyetleri ile siber suç korkusu oranları arasında anlamlı bir ilişki bulunup bulunmadığını test etmek amacıyla da çapraz tablolardan ve ki kare analizinden faydalanılmıştır. Analiz sonuçları aşağıdaki tablolarda gösterilmektedir.

Tablo 30. Katılımcıların Cinsiyetleri ile Bilgisayar Korsanlığı Korkusu Arasındaki İlişki

Cinsiyet		Bilgisayar Korsanlığı (Hacking)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	7	60	15	82
	% satır	8,5%	73,2%	18,3%	100,0%
	% sütun	14,6%	33,5%	51,7%	32,0%
	% toplam	2,7%	23,4%	5,9%	32,0%
Erkek	Sayı	41	119	14	174
	% satır	23,6%	68,4%	8,0%	100,0%
	% sütun	85,4%	66,5%	48,3%	68,0%
	% toplam	16,0%	46,5%	5,5%	68,0%
Toplam	Sayı	48	179	29	256
	% satır	18,8%	69,9%	11,3%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	18,8%	69,9%	11,3%	100,0%
P=0,002, df=2 (12,060)					

Tablo 30'da yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile bilgisayar korsanlığı korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir (p<0.05). Tablodaki verilere göre kadınların %91,5'i zaman zaman veya genellikle bilgisayar korsanlığından mağdur olma korkusu yaşarken, erkeklerde bu oran %76,4'tür. Dolayısıyla bilgisayar korsanlığı açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 31. Katılımcıların Cinsiyetleri ile Denial of Service (DoS) Saldırıları Korkusu Arasındaki İlişki

Cinsiyet		Denial of Service (DOS) Saldırıları			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	25	43	15	83
	% satır	30,1%	51,8%	18,1%	100,0%
	% sütun	25,3%	31,2%	57,7%	31,6%
	% toplam	9,5%	16,3%	5,7%	31,6%
Erkek	Sayı	74	95	11	180
	% satır	41,1%	52,8%	6,1%	100,0%
	% sütun	74,7%	68,8%	42,3%	68,4%
	% toplam	28,1%	36,1%	4,2%	68,4%
Toplam	Sayı	99	138	26	263
	% satır	37,6%	52,5%	9,9%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	37,6%	52,5%	9,9%	100,0%
P=0,007, df=2 (10,054)					

Tablo 31'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile denial of service (DoS) saldırıları korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %69,9'u zaman zaman veya genellikle denial of service (DoS) saldırılarından mağdur olma korkusu yaşarken, erkeklerde bu oran %58,9'dur. Dolayısıyla denial of service (DoS) saldırıları açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 32. Katılımcıların Cinsiyetleri ile Virüsler, Truva Atları ve Zararlı Yazılımlar Korkusu Arasındaki İlişki

Cinsiyet		Virüsler, Truva Atları ve Zararlı Yazılımlar			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	11	48	24	83
	% satır	13,3%	57,8%	28,9%	100,0%
	% sütun	20,0%	32,2%	40,7%	31,6%
	% toplam	4,2%	18,3%	9,1%	31,6%
Erkek	Sayı	44	101	35	180
	% satır	24,4%	56,1%	19,4%	100,0%
	% sütun	80,0%	67,8%	59,3%	68,4%
	% toplam	16,7%	38,4%	13,3%	68,4%
Toplam	Sayı	55	149	59	263
	% satır	20,9%	56,7%	22,4%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	20,9%	56,7%	22,4%	100,0%
P=0,058, df=2 (5,703)					

Tablo 32'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile virüsler, truva atları ve zararlı yazılımlar korkusu arasında anlamlı bir ilişki bulunmadığı görülmektedir ($p>0.05$). Bununla birlikte tablodaki verilere göre kadınların %86,7'si zaman zaman veya genellikle virüsler, truva atları ve zararlı yazılımlardan mağdur olma korkusu yaşarken, erkeklerde bu oran %75,6'dır. Dolayısıyla virüsler, truva atları ve zararlı yazılımlar açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 33. Katılımcıların Cinsiyetleri ile Banka veya Kredi Kartlarının (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğranılması Korkusu Arasındaki İlişki

Cinsiyet		Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	8	32	42	82
	% satır	9,8%	39,0%	51,2%	100,0%
	% sütun	18,6%	25,2%	45,7%	31,3%
	% toplam	3,1%	12,2%	16,0%	31,3%
Erkek	Sayı	35	95	50	180
	% satır	19,4%	52,8%	27,8%	100,0%
	% sütun	81,4%	74,8%	54,3%	68,7%
	% toplam	13,4%	36,3%	19,1%	68,7%
Toplam	Sayı	43	127	92	262
	% satır	16,4%	48,5%	35,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	16,4%	48,5%	35,1%	100,0%
P=0,001, df=2 (14,236)					

Tablo 33'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile banka veya kredi kartlarının (ya da bunlara ait bilgilerin) başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğranılması korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %70,9'u zaman zaman veya genellikle bu suç türünden mağdur olma korkusu yaşarken, erkeklerde bu oran %80,6'dır. Dolayısıyla banka veya kredi kartlarının (ya da bunlara ait bilgilerin) başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğranılması açısından korku oranlarının erkeklerde daha yüksek olduğu görülmektedir.

Tablo 34. Katılımcıların Cinsiyetleri ile Casus Yazılımlar Korkusu Arasındaki İlişki

Cinsiyet		Casus Yazılımlar			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	11	44	28	83
	% satır	13,3%	53,0%	33,7%	100,0%
	% sütun	25,0%	28,8%	42,4%	31,6%
	% toplam	4,2%	16,7%	10,6%	31,6%
Erkek	Sayı	33	109	38	180
	% satır	18,3%	60,6%	21,1%	100,0%
	% sütun	75,0%	71,2%	57,6%	68,4%
	% toplam	12,5%	41,4%	14,4%	68,4%
Toplam	Sayı	44	153	66	263
	% satır	16,7%	58,2%	25,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	16,7%	58,2%	25,1%	100,0%
P=0,080, df=2 (5,039)					

Tablo 34'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile casus yazılımlar korkusu arasında anlamlı bir ilişki bulunmadığı görülmektedir ($p>0.05$). Bununla birlikte tablodaki verilere göre kadınların %86,7'si zaman zaman veya genellikle casus yazılımlardan mağdur olma korkusu yaşarken, erkeklerde bu oran %81,7'dir. Dolayısıyla casus yazılımlar açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 35. Katılımcıların Cinsiyetleri ile Kimlik Hırsızlığı Korkusu Arasındaki İlişki

Cinsiyet		Kimlik Hırsızlığı			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	8	40	36	84
	% satır	9,5%	47,6%	42,9%	100,0%
	% sütun	21,6%	27,6%	45,0%	32,1%
	% toplam	3,1%	15,3%	13,7%	32,1%
Erkek	Sayı	29	105	44	178
	% satır	16,3%	59,0%	24,7%	100,0%
	% sütun	78,4%	72,4%	55,0%	67,9%
	% toplam	11,1%	40,1%	16,8%	67,9%
Toplam	Sayı	37	145	80	262
	% satır	14,1%	55,3%	30,5%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	14,1%	55,3%	30,5%	100,0%
P=0,009, df=2 (9,333)					

Tablo 35'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile kimlik hırsızlığı korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %90,5'i zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %83,7'dir. Dolayısıyla kimlik hırsızlığı açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 36. Katılımcıların Cinsiyetleri ile Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerin Yok Edilmemesi Korkusu Arasındaki İlişki

Cinsiyet		Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	28	38	18	84
	% satır	33,3%	45,2%	21,4%	100,0%
	% sütun	33,7%	31,9%	29,5%	31,9%
	% toplam	10,6%	14,4%	6,8%	31,9%
Erkek	Sayı	55	81	43	179
	% satır	30,7%	45,3%	24,0%	100,0%
	% sütun	66,3%	68,1%	70,5%	68,1%
	% toplam	20,9%	30,8%	16,3%	68,1%
Toplam	Sayı	83	119	61	263
	% satır	31,6%	45,2%	23,2%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	31,6%	45,2%	23,2%	100,0%
P=0,865, df=2 (0,289)					

Tablo 36'da yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi korkusu arasında anlamlı bir ilişki bulunmadığı görülmektedir ($p>0.05$). Bununla birlikte tablodaki verilere göre kadınların %66,6'sı zaman zaman veya genellikle mağdur olma korkusu yaşarken, erkeklerde bu oran %69,3'tür. Dolayısıyla yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi açısından korku oranlarının erkeklerde daha yüksek olduğu görülmektedir.

Tablo 37. Katılımcıların Cinsiyetleri ile Siber Zorbalık Korkusu Arasındaki İlişki

Cinsiyet		Siber Zorbalık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	9	48	27	84
	% satır	10,7%	57,1%	32,1%	100,0%
	% sütun	13,0%	35,0%	46,6%	31,8%
	% toplam	3,4%	18,2%	10,2%	31,8%
Erkek	Sayı	60	89	31	180
	% satır	33,3%	49,4%	17,2%	100,0%
	% sütun	87,0%	65,0%	53,4%	68,2%
	% toplam	22,7%	33,7%	11,7%	68,2%
Toplam	Sayı	69	137	58	264
	% satır	26,1%	51,9%	22,0%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	26,1%	51,9%	22,0%	100,0%
P=0,0001, df=2 (17,669)					

Tablo 37'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber zorbalık korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %89,2'si zaman zaman veya genellikle bu suçtan korku yaşarken, erkeklerde bu oran %83,9'dur. Dolayısıyla siber zorbalık açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 38. Katılımcıların Cinsiyetleri ile Bilişim Sistemleri Aracılığıyla Hakaret Korkusu Arasındaki İlişki

Cinsiyet		Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	34	39	11	84
	% satır	40,5%	46,4%	13,1%	100,0%
	% sütun	23,8%	39,4%	50,0%	31,8%
	% toplam	12,9%	14,8%	4,2%	31,8%
Erkek	Sayı	109	60	11	180
	% satır	60,6%	33,3%	6,1%	100,0%
	% sütun	76,2%	60,6%	50,0%	68,2%
	% toplam	41,3%	22,7%	4,2%	68,2%
Toplam	Sayı	143	99	22	264
	% satır	54,2%	37,5%	8,3%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,2%	37,5%	8,3%	100,0%
P=0,006, df=2 (10,234)					

Tablo 38'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber zorbalık korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %59,5'i zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %39,4'tür. Dolayısıyla siber zorbalık açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 39. Katılımcıların Cinsiyetleri ile Elektronik Haberleşmenin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi Korkusu Arasındaki İlişki

Cinsiyet		Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	12	50	22	84
	% satır	14,3%	59,5%	26,2%	100,0%
	% sütun	30,0%	34,0%	28,6%	31,8%
	% toplam	4,5%	18,9%	8,3%	31,8%
Erkek	Sayı	28	97	55	180
	% satır	15,6%	53,9%	30,6%	100,0%
	% sütun	70,0%	66,0%	71,4%	68,2%
	% toplam	10,6%	36,7%	20,8%	68,2%
Toplam	Sayı	40	147	77	264
	% satır	15,2%	55,7%	29,2%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	15,2%	55,7%	29,2%	100,0%
P=0,683, df=2 (0,762)					

Tablo 39'da yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile elektronik haberleşmenin gizliliğinin ihlali, kayda alınması veya ifşa edilmesi korkusu arasında anlamlı bir ilişki bulunmadığı görülmektedir ($p>0.05$). Bununla birlikte tablodaki verilere göre kadınların %85,7'si zaman zaman veya genellikle mağdur olma korkusu yaşarken, erkeklerde bu oran %84,5'tir. Dolayısıyla elektronik haberleşmenin gizliliğinin ihlali, kayda alınması veya ifşa edilmesi açısından korku oranlarının kadınlarda daha yüksek olduğu görülmekle birlikte kadınlar ve erkekler arasındaki korkunun birbirine oldukça yakın düzeylerde olduğu da belirtilmelidir.

Tablo 40. Katılımcıların Cinsiyetleri ile Siber Hırsızlık Korkusu Arasındaki İlişki

Cinsiyet		Siber Hırsızlık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	8	40	35	83
	% satır	9,6%	48,2%	42,2%	100,0%
	% sütun	18,2%	28,0%	46,1%	31,6%
	% toplam	3,0%	15,2%	13,3%	31,6%
Erkek	Sayı	36	103	41	180
	% satır	20,0%	57,2%	22,8%	100,0%
	% sütun	81,8%	72,0%	53,9%	68,4%
	% toplam	13,7%	39,2%	15,6%	68,4%
Toplam	Sayı	44	143	76	263
	% satır	16,7%	54,4%	28,9%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	16,7%	54,4%	28,9%	100,0%
P=0,003, df=2 (11,889)					

Tablo 40’ta yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber hırsızlık korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %90,4’ü zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %80’dir. Dolayısıyla siber hırsızlık açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 41. Katılımcıların Cinsiyetleri ile Siber Dolandırıcılık Korkusu Arasındaki İlişki

Cinsiyet		Siber Dolandırıcılık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	18	39	25	82
	% satır	22,0%	47,6%	30,5%	100,0%
	% sütun	24,0%	29,8%	46,3%	31,5%
	% toplam	6,9%	15,0%	9,6%	31,5%
Erkek	Sayı	57	92	29	178
	% satır	32,0%	51,7%	16,3%	100,0%
	% sütun	76,0%	70,2%	53,7%	68,5%
	% toplam	21,9%	35,4%	11,2%	68,5%
Toplam	Sayı	75	131	54	260
	% satır	28,8%	50,4%	20,8%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	28,8%	50,4%	20,8%	100,0%
P=0,022, df=2 (7,610)					

Tablo 41'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber dolandırıcılık korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %78,1'i zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %68'dir. Dolayısıyla siber dolandırıcılık açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 42. Katılımcıların Cinsiyetleri ile Siber Taciz Korkusu Arasındaki İlişki

Cinsiyet		Siber Taciz			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	26	44	12	82
	% satır	31,7%	53,7%	14,6%	100,0%
	% sütun	18,3%	47,3%	48,0%	31,5%
	% toplam	10,0%	16,9%	4,6%	31,5%
Erkek	Sayı	116	49	13	178
	% satır	65,2%	27,5%	7,3%	100,0%
	% sütun	81,7%	52,7%	52,0%	68,5%
	% toplam	44,6%	18,8%	5,0%	68,5%
Toplam	Sayı	142	93	25	260
	% satır	54,6%	35,8%	9,6%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,6%	35,8%	9,6%	100,0%
P=0,000003, df=2 (25,363)					

Tablo 42'de yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber taciz korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %68,3'ü zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %34,8'dir. Dolayısıyla siber taciz açısından korku oranlarının kadınlarda daha yüksek olduğu ve oranın neredeyse yarı yarıya olduğu görülmektedir.

Tablo 43. Katılımcıların Cinsiyetleri ile Siber Tehdit ve Şantaj Korkusu Arasındaki İlişki

Cinsiyet		Siber Tehdit ve Şantaj			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	25	43	14	82
	% satır	30,5%	52,4%	17,1%	100,0%
	% sütun	20,0%	40,2%	50,0%	31,5%
	% toplam	9,6%	16,5%	5,4%	31,5%
Erkek	Sayı	100	64	14	178
	% satır	56,2%	36,0%	7,9%	100,0%
	% sütun	80,0%	59,8%	50,0%	68,5%
	% toplam	38,5%	24,6%	5,4%	68,5%
Toplam	Sayı	125	107	28	260
	% satır	48,1%	41,2%	10,8%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	48,1%	41,2%	10,8%	100,0%
P=0,0003, df=2 (15,834)					

Tablo 43'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber tehdit ve şantaj korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %69,5'i zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %43,9'dur. Dolayısıyla siber tehdit ve şantaj açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 44. Katılımcıların Cinsiyetleri ile Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu Korkusu Arasındaki İlişki

Cinsiyet		Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	23	47	12	82
	% satır	28,0%	57,3%	14,6%	100,0%
	% sütun	19,5%	41,6%	41,4%	31,5%
	% toplam	8,8%	18,1%	4,6%	31,5%
Erkek	Sayı	95	66	17	178
	% satır	53,4%	37,1%	9,6%	100,0%
	% sütun	80,5%	58,4%	58,6%	68,5%
	% toplam	36,5%	25,4%	6,5%	68,5%
Toplam	Sayı	118	113	29	260
	% satır	45,4%	43,5%	11,2%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	45,4%	43,5%	11,2%	100,0%
P=0,001, df=2 (14,523)					

Tablo 44'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %71,9'u zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %46,7'dir. Dolayısıyla bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Tablo 45. Katılımcıların Cinsiyetleri ile Siber Terörizm Korkusu Arasındaki İlişki

Cinsiyet		Siber Terörizm			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Kadın	Sayı	19	46	17	82
	% satır	23,2%	56,1%	20,7%	100,0%
	% sütun	21,6%	35,9%	39,5%	31,7%
	% toplam	7,3%	17,8%	6,6%	31,7%
Erkek	Sayı	69	82	26	177
	% satır	39,0%	46,3%	14,7%	100,0%
	% sütun	78,4%	64,1%	60,5%	68,3%
	% toplam	26,6%	31,7%	10,0%	68,3%
Toplam	Sayı	88	128	43	259
	% satır	34,0%	49,4%	16,6%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	34,0%	49,4%	16,6%	100,0%
P=0,040, df=2 (6,438)					

Tablo 45'te yer alan veriler incelendiğinde katılımcıların cinsiyetleri ile siber terörizm korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilere göre kadınların %76,8'i zaman zaman veya genellikle korku yaşarken, erkeklerde bu oran %61'dir. Dolayısıyla siber terörizm açısından korku oranlarının kadınlarda daha yüksek olduğu görülmektedir.

Sonuç olarak bu çalışmada katılımcılara yöneltilen toplam 16 siber suç türü içerisinden 12'si için cinsiyetler ile korku oranları arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Ayrıca yine bu 16 siber suç türü içerisinden 14'ü için kadınlarda korku oranları erkeklere göre daha fazla bulunmuşken, yalnızca 2 siber suç türü (banka veya kredi kartlarının ya da bunlara ait bilgilerin başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğranılması ve yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi korkusu) için korku oranları erkekler arasında kadınlara göre daha fazla bulunmuştur.

Üçüncü olarak katılımcıların eğitim durumları ile siber suç korkusu oranları arasında anlamlı bir ilişki bulunup bulunmadığı da yine çapraz tablolardan ve ki kare analizinden yola çıkılarak incelenmiştir. Burada 16 siber suç türü korkusundan ikisi ile (bilgisayar

korsanlığı ve bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu) katılımcıların eğitim durumları arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Kalan 14 siber suç türü korkusu ile katılımcıların eğitim durumları arasında ise anlamlı bir ilişki bulunmamaktadır ($p>0.05$). Eğitim durumu ile aralarında anlamlı bir ilişki bulunan iki siber suç korkusuna ilişkin tablolar aşağıda sunulmaktadır.

Tablo 46. Katılımcıların Eğitim Durumları ile Bilgisayar Korsanlığı Korkusu Arasındaki İlişki

Eğitim durumu		Bilgisayar Korsanlığı (Hacking)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Lise	Sayı	0	11	2	13
	% satır	0,0%	84,6%	15,4%	100,0%
	% sütun	0,0%	6,1%	6,7%	5,0%
	% toplam	0,0%	4,3%	0,8%	5,0%
Üniversite	Sayı	39	104	17	160
	% satır	24,4%	65,0%	10,6%	100,0%
	% sütun	81,3%	57,8%	56,7%	62,0%
	% toplam	15,1%	40,3%	6,6%	62,0%
Lisansüstü	Sayı	9	65	11	85
	% satır	10,6%	76,5%	12,9%	100,0%
	% sütun	18,8%	36,1%	36,7%	32,9%
	% toplam	3,5%	25,2%	4,3%	32,9%
Toplam	Sayı	48	180	30	258
	% satır	18,6%	69,8%	11,6%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	18,6%	69,8%	11,6%	100,0%
P=0,038, df=4 (10,120)					

Bilgisayar korsanlığı korkusu ile katılımcıların eğitim durumları arasındaki ilişki Tablo 46'da gösterilmektedir. Tabloya göre bilgisayar korsanlığı korkusu ile katılımcıların eğitim durumları arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tabloya göre eğitim durumunu lise olarak belirten katılımcılar, eğitim durumunu üniversite ve lisansüstü olarak belirten katılımcılara göre daha fazla oranda bilgisayar korsanlığından zaman zaman veya genellikle korku yaşadıklarını belirtmişlerdir. Hatta eğitim durumunu

lise olarak belirtip de bilgisayar korsanlığından hiç korku yaşamadığını belirten katılımcı bulunmamaktadır. Bununla birlikte eğitim durumunu lisansüstü olarak belirten katılımcılarda ise bilgisayar korsanlığı korkusu (zaman zaman veya genellikle korku yaşayanlar) oranlarının eğitim durumunu üniversite olarak belirten katılımcılara göre daha fazla olduğu görülmektedir.

Tablo 47. Katılımcıların Eğitim Durumları ile Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu Korkusu Arasındaki İlişki

Eğitim durumu		Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Lise	Sayı	1	11	1	13
	% satır	7,7%	84,6%	7,7%	100,0%
	% sütun	0,8%	9,7%	3,4%	5,0%
	% toplam	0,4%	4,2%	0,4%	5,0%
Üniversite	Sayı	75	68	21	164
	% satır	45,7%	41,5%	12,8%	100,0%
	% sütun	62,5%	60,2%	72,4%	62,6%
	% toplam	28,6%	26,0%	8,0%	62,6%
Lisansüstü	Sayı	44	34	7	85
	% satır	51,8%	40,0%	8,2%	100,0%
	% sütun	36,7%	30,1%	24,1%	32,4%
	% toplam	16,8%	13,0%	2,7%	32,4%
Toplam	Sayı	120	113	29	262
	% satır	45,8%	43,1%	11,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	45,8%	43,1%	11,1%	100,0%
P=0,022, df=4 (11,465)					

Bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu ile katılımcıların eğitim durumları arasındaki ilişki ise Tablo 47'de gösterilmektedir. Tabloya göre bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu ile de katılımcıların eğitim durumları arasında anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tabloya göre bu suç türü için eğitim durumunu lise olarak belirten katılımcılar, eğitim durumunu üniversite olarak belirten katılımcılara göre, eğitim durumunu üniversite olarak

belirtenler ise eğitim durumunu lisansüstü olarak belirten katılımcılara göre daha fazla oranda zaman zaman veya genellikle korku yaşadıklarını belirtmişlerdir. Dolayısıyla bu verilere göre katılımcıların eğitim durumları yükseldikçe bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu yaşama oranlarının da düşmekte olduğu görülmektedir.

Dördüncü olarak katılımcıların gelir düzeyleri ile siber suç korkusu oranları arasında anlamlı bir ilişki bulunup bulunmadığı da yine çapraz tablolardan ve ki kare analizinden yola çıkılarak incelenmiştir. Burada 16 siber suç türü korkusundan 6'sı için (bilgisayar korsanlığı, denial of service saldırıları, bilişim sistemleri aracılığıyla hakaret, siber taciz, siber tehdit ve şantaj, bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu) ki kare analizi sonucunu yorumlayabilmek adına yeterli veri bulunmamaktadır. Geriye kalan 10 siber suç korkusu ile katılımcıların gelir düzeyi arasında ise anlamlı bir ilişki bulunamamıştır ($p>0.05$).

4.2.2. Geçmiş Siber Suç Mağduriyeti ile Siber Suç Korkusu Arasındaki İlişki

Araştırmanın ikinci hipotezi "geçmiş siber suç mağduriyeti ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" şeklindedir. Bu hipotez çapraz tablolar ve ki kare analizleri ile değerlendirilmiştir. Analizler sonucunda 16 siber suç türünden 5'i (banka veya kredi kartlarının ya da bunlara ait bilgilerin başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğrama, bilişim sistemleri aracılığıyla hakaret, siber dolandırıcılık, siber taciz ve siber tehdit ve şantaj korkusu) için olan korku ile geçmiş siber suç mağduriyeti arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Geriye kalan 11 siber suç korkusunun ise geçmiş siber suç mağduriyeti ile arasında anlamlı bir ilişki bulunmamaktadır ($p>0.05$). Aralarındaki ilişki anlamlı bulunan siber suç korkusu türlerine ilişkin tablolar aşağıda sunulmuştur.

Tablo 48. Katılımcıların Geçmiş Siber Suç Mağduriyetleri ile Banka veya Kredi Kartlarının (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramaları Korkusu Arasındaki İlişki

Son 12 ay içerisinde herhangi bir siber suçtan mağdur oldunuz mu?		Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Hayır	Sayı	39	117	69	225
	% satır	17,3%	52,0%	30,7%	100,0%
	% sütun	90,7%	93,6%	75,0%	86,5%
	% toplam	15,0%	45,0%	26,5%	86,5%
Evet	Sayı	4	8	23	35
	% satır	11,4%	22,9%	65,7%	100,0%
	% sütun	9,3%	6,4%	25,0%	13,5%
	% toplam	1,5%	3,1%	8,8%	13,5%
Toplam	Sayı	43	125	92	260
	% satır	16,5%	48,1%	35,4%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	16,5%	48,1%	35,4%	100,0%
P=0,0002, df=2 (16,503)					

Tablo 48'e göre katılımcıların son 12 ay içerisinde siber suç mağduru olmuş olmaları ile banka veya kredi kartlarının (ya da bunlara ait bilgilerin) başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğramaları korkusu arasında anlamlı bir ilişki bulunmaktadır. Tabloya göre son 12 ay içerisinde herhangi bir siber suçtan mağdur olmuş olan katılımcılarda banka veya kredi kartlarının (ya da bunlara ait bilgilerin) başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğrama suçundan zaman zaman veya genellikle korku yaşama oranları (%88,6), mağduriyet yaşamayan katılımcılara göre (%82,7) daha fazla bulunmuştur.

Tablo 49. Katılımcıların Geçmiş Siber Suç Mağduriyetleri ile Bilişim Sistemleri Aracılığıyla Hakaret Korkusu Arasındaki İlişki

Son 12 ay içerisinde herhangi bir siber suçtan mağdur oldunuz mu?		Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Hayır	Sayı	132	81	14	227
	% satır	58,1%	35,7%	6,2%	100,0%
	% sütun	93,0%	81,8%	66,7%	86,6%
	% toplam	50,4%	30,9%	5,3%	86,6%
Evet	Sayı	10	18	7	35
	% satır	28,6%	51,4%	20,0%	100,0%
	% sütun	7,0%	18,2%	33,3%	13,4%
	% toplam	3,8%	6,9%	2,7%	13,4%
Toplam	Sayı	142	99	21	262
	% satır	54,2%	37,8%	8,0%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,2%	37,8%	8,0%	100,0%
P=0,001, df=2 (14,124)					

Tablo 49'a göre katılımcıların son 12 ay içerisinde siber suç mağduru olmuş olmaları ile bilişim sistemleri aracılığıyla hakaret korkusu arasında da anlamlı bir ilişki bulunmaktadır($p<0.05$). Tabloya göre son 12 ay içerisinde herhangi bir siber suç mağduriyeti yaşamamış katılımcıların %58,1'i, bilişim sistemleri aracılığıyla hakaret suçu için hiç korku yaşamazken, siber suç mağduriyeti yaşamış olan bireylerde bu oran %28,6'dır. Diğer bir ifadeyle son 12 ay içerisinde siber suç mağduriyeti yaşayanlar yaşamayanlara göre bilişim sistemleri aracılığıyla hakaret suçu için nerdeyse %30 daha fazla oranlarda zaman zaman veya genellikle korku yaşamaktadırlar.

Tablo 50. Katılımcıların Geçmiş Siber Suç Mağduriyetleri ile Siber Dolandırıcılık Korkusu Arasındaki İlişki

Son 12 ay içerisinde herhangi bir siber suçtan mağdur oldunuz mu?		Siber Dolandırıcılık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Hayır	Sayı	70	114	42	226
	% satır	31,0%	50,4%	18,6%	100,0%
	% sütun	92,1%	87,7%	76,4%	86,6%
	% toplam	26,8%	43,7%	16,1%	86,6%
Evet	Sayı	6	16	13	35
	% satır	17,1%	45,7%	37,1%	100,0%
	% sütun	7,9%	12,3%	23,6%	13,4%
	% toplam	2,3%	6,1%	5,0%	13,4%
Toplam	Sayı	76	130	55	261
	% satır	29,1%	49,8%	21,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	29,1%	49,8%	21,1%	100,0%
P=0,029, df=2 (7,080)					

Katılımcıların son 12 ay içerisindeki siber suç mağduriyetleri ile siber dolandırıcılık korkusu arasında da anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da yine son 12 ay içerisinde siber suç mağduriyeti yaşamış olan katılımcıların, yaşamayan katılımcılara göre daha fazla oranlarda siber dolandırıcılık korkusu yaşamakta oldukları görülmektedir.

Tablo 51. Katılımcıların Geçmiş Siber Suç Mağduriyetleri ile Siber Taciz Korkusu Arasındaki İlişki

Son 12 ay içerisinde herhangi bir siber suçtan mağdur oldunuz mu?		Siber Taciz			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Hayır	Sayı	133	75	18	226
	% satır	58,8%	33,2%	8,0%	100,0%
	% sütun	93,0%	81,5%	69,2%	86,6%
	% toplam	51,0%	28,7%	6,9%	86,6%
Evet	Sayı	10	17	8	35
	% satır	28,6%	48,6%	22,9%	100,0%
	% sütun	7,0%	18,5%	30,8%	13,4%
	% toplam	3,8%	6,5%	3,1%	13,4%
Toplam	Sayı	143	92	26	261
	% satır	54,8%	35,2%	10,0%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,8%	35,2%	10,0%	100,0%
P=0,001, df=2 (13,854)					

Katılımcıların son 12 ay içerisindeki siber suç mağduriyetleri ile siber taciz korkusu arasındaki ilişki de anlamlı bir ilişkidir ($p<0.05$). Burada da yine son 12 ay içerisinde siber suç mağduriyeti yaşamış olan katılımcıların, yaşamayan katılımcılara göre %30'dan daha fazla oranlarda zaman zaman veya genellikle siber taciz korkusu yaşamakta oldukları görülmektedir.

Tablo 52. Katılımcıların Geçmiş Siber Suç Mağduriyetleri ile Siber Tehdit ve Şantaj Korkusu Arasındaki İlişki

Son 12 ay içerisinde herhangi bir siber suçtan mağdur oldunuz mu?		Siber Tehdit ve Şantaj			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Hayır	Sayı	115	91	20	226
	% satır	50,9%	40,3%	8,8%	100,0%
	% sütun	91,3%	85,8%	69,0%	86,6%
	% toplam	44,1%	34,9%	7,7%	86,6%
Evet	Sayı	11	15	9	35
	% satır	31,4%	42,9%	25,7%	100,0%
	% sütun	8,7%	14,2%	31,0%	13,4%
	% toplam	4,2%	5,7%	3,4%	13,4%
Toplam	Sayı	126	106	29	261
	% satır	48,3%	40,6%	11,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	48,3%	40,6%	11,1%	100,0%
P=0,006, df=2 (10,184)					

Katılımcıların son 12 ay içerisindeki siber suç mağduriyetleri ile siber tehdit ve şantaj korkusu arasında da anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da yine yukarıdaki tablolarda olduğu gibi son 12 ay içerisinde siber suç mağduriyeti yaşamış olan katılımcıların, yaşamayan katılımcılara göre daha fazla oranlarda zaman zaman veya genellikle siber tehdit ve şantaj korkusu yaşamakta oldukları görülmektedir.

Sonuç olarak geçmiş siber suç mağduriyeti ile aralarında anlamlı bir ilişki bulunan yukarıdaki 5 siber suç korkusunun tamamı için geçmişte siber suç mağduriyeti yaşamış olan bireylerin mağduriyet yaşamamış olan bireylere göre daha fazla korku oranlarına sahip oldukları görülmektedir.

4.2.3. Alınan Önlemleri Yeterli Bulma İle Siber Suç Korkusu Arasındaki İlişki

Araştırmanın üçüncü hipotezi "siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" şeklindedir. Bu hipotezi test edebilmek için "siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?" sorusu ile 16 adet siber suç korkusu sorusu çapraz tablolar ve ki kare analizleri vasıtasıyla değerlendirilmiştir. Buna göre 16 siber suç korkusu içerisinden 4'ü (bilgisayar korsanlığı, bilişim sistemleri aracılığıyla hakaret, siber dolandırıcılık ve siber taciz korkusu) için siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulup bulmama ile siber suç korkusu arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Diğer 14 siber suç korkusu için ise anlamlı bir ilişki bulunamamıştır ($p>0.05$). Aralarındaki ilişki anlamlı bulunan siber suç türlerine ilişkin analizler aşağıda sunulmuştur.

Tablo 53. Katılımcıların Aldıkları Önlemleri Yeterli Bulma Düzeyleri ile Bilgisayar Korsanlığı Korkusu Arasındaki İlişki

Siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?		Bilgisayar Korsanlığı (Hacking)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz buluyorum	Sayı	5	38	6	49
	% satır	10,2%	77,6%	12,2%	100,0%
	% sütun	11,1%	21,6%	20,0%	19,5%
	% toplam	2,0%	15,1%	2,4%	19,5%
Orta düzeyde yeterli buluyorum	Sayı	19	93	11	123
	% satır	15,4%	75,6%	8,9%	100,0%
	% sütun	42,2%	52,8%	36,7%	49,0%
	% toplam	7,6%	37,1%	4,4%	49,0%
Yeterli buluyorum	Sayı	21	45	13	79
	% satır	26,6%	57,0%	16,5%	100,0%
	% sütun	46,7%	25,6%	43,3%	31,5%
	% toplam	8,4%	17,9%	5,2%	31,5%
Toplam	Sayı	45	176	30	251
	% satır	17,9%	70,1%	12,0%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	17,9%	70,1%	12,0%	100,0%
P=0,033, df=4 (10,494)					

Tablo 53'te görüleceği üzere katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri ile bilgisayar korsanlığı korkuları arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Siber suçlardan mağdur olmamak adına almış oldukları önlemleri yetersiz bulanlarda, orta düzeyde yeterli bulanlara göre, orta düzeyde yeterli bulanlarda ise yeterli bulanlara göre bilgisayar korsanlığından mağdur olmaktan hiç korku yaşamama oranlarının daha az olduğu görülmektedir. Bir diğer ifadeyle katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri arttıkça bilgisayar korsanlığı korkularının azalmakta olduğu görülmektedir.

Tablo 54. Katılımcıların Aldıkları Önlemleri Yeterli Bulma Düzeyleri ile Bilişim Sistemleri Aracılığıyla Hakaret Korkusu Arasındaki İlişki

Siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?		Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz buluyorum	Sayı	24	22	5	51
	% satır	47,1%	43,1%	9,8%	100,0%
	% sütun	16,9%	23,2%	22,7%	19,7%
	% toplam	9,3%	8,5%	1,9%	19,7%
Orta düzeyde yeterli buluyorum	Sayı	62	54	13	129
	% satır	48,1%	41,9%	10,1%	100,0%
	% sütun	43,7%	56,8%	59,1%	49,8%
	% toplam	23,9%	20,8%	5,0%	49,8%
Yeterli buluyorum	Sayı	56	19	4	79
	% satır	70,9%	24,1%	5,1%	100,0%
	% sütun	39,4%	20,0%	18,2%	30,5%
	% toplam	21,6%	7,3%	1,5%	30,5%
Toplam	Sayı	142	95	22	259
	% satır	54,8%	36,7%	8,5%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,8%	36,7%	8,5%	100,0%
P=0,018, df=4 (11,892)					

Tablo 54'te katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri ile bilişim sistemleri aracılığıyla hakaret korkuları arasında da anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Burada da katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri arttıkça bilişim sistemleri aracılığıyla hakaret korkusu yaşama oranlarının azalmakta olduğu görülmektedir.

Tablo 55. Katılımcıların Aldıkları Önlemleri Yeterli Bulma Düzeyleri ile Siber Dolandırıcılık Korkusu Arasındaki İlişki

Siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?		Siber Dolandırıcılık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz buluyorum	Sayı	9	28	14	51
	% satır	17,6%	54,9%	27,5%	100,0%
	% sütun	12,2%	21,9%	26,4%	20,0%
	% toplam	3,5%	11,0%	5,5%	20,0%
Orta düzeyde yeterli buluyorum	Sayı	28	70	28	126
	% satır	22,2%	55,6%	22,2%	100,0%
	% sütun	37,8%	54,7%	52,8%	49,4%
	% toplam	11,0%	27,5%	11,0%	49,4%
Yeterli buluyorum	Sayı	37	30	11	78
	% satır	47,4%	38,5%	14,1%	100,0%
	% sütun	50,0%	23,4%	20,8%	30,6%
	% toplam	14,5%	11,8%	4,3%	30,6%
Toplam	Sayı	74	128	53	255
	% satır	29,0%	50,2%	20,8%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	29,0%	50,2%	20,8%	100,0%
P=0,001, df=4 (19,372)					

Tablo 55'te katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri ile siber dolandırıcılık korkuları oranları yer almakta olup, bu iki değişken arasında da anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki oranlardan hareketle siber dolandırıcılık korkusunun da katılımcıların siber

suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri arttıkça azalmakta olduğunu söylemek mümkündür.

Tablo 56. Katılımcıların Aldıkları Önlemleri Yeterli Bulma Düzeyleri ile Siber Taciz Korkusu Arasındaki İlişki

Siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?		Siber Taciz			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz buluyorum	Sayı	19	24	8	51
	% satır	37,3%	47,1%	15,7%	100,0%
	% sütun	13,5%	27,3%	30,8%	20,0%
	% toplam	7,5%	9,4%	3,1%	20,0%
Orta düzeyde yeterli buluyorum	Sayı	64	49	13	126
	% satır	50,8%	38,9%	10,3%	100,0%
	% sütun	45,4%	55,7%	50,0%	49,4%
	% toplam	25,1%	19,2%	5,1%	49,4%
Yeterli buluyorum	Sayı	58	15	5	78
	% satır	74,4%	19,2%	6,4%	100,0%
	% sütun	41,1%	17,0%	19,2%	30,6%
	% toplam	22,7%	5,9%	2,0%	30,6%
Toplam	Sayı	141	88	26	255
	% satır	55,3%	34,5%	10,2%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	55,3%	34,5%	10,2%	100,0%
P=0,001, df=4 (19,372)					

Tablo 56'da katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri ile siber taciz korkusu oranları yer almakta olup, bu iki değişken arasında da anlamlı bir ilişki bulunduğu görülmektedir ($p<0.05$). Tablodaki verilerden hareketle katılımcıların siber suçlardan mağdur olmamak adına almış oldukları önlemleri yeterli bulma düzeyleri arttıkça siber taciz korkularının da azalmakta olduğu görülmektedir.

Sonuç olarak siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulma ile aralarında anlamlı bir ilişki bulunan 4 siber suç korkusunun tamamı için katılımcıların

aldıkları önlemleri yeterli bulma düzeyleri arttıkça siber suç korkularının azalmakta olduğu söylenebilir.

4.2.4. Siber Suçlara İlişkin Yasal Düzenlemeleri, Kolluk Ve Yargı Birimlerini Siber Suçlarla Mücadele Noktasında Yeterli Bulma İle Siber Suç Korkusu Arasındaki İlişki

Araştırmanın dördüncü hipotezi "siber suçlara ilişkin yasal düzenlemeleri, kolluk ve yargı birimlerini siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" şeklindedir. Bu hipotezi test etmek amacıyla anket soruları arasında yer alan "Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli buluyor musunuz?", "Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?" ve "Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli buluyor musunuz?" soruları ile 16 adet siber suç korkusu sorusu arasındaki çapraz tablolar ve ki kare analizleri değerlendirilmiştir.

4.2.4.1. Siber Suçlara İlişkin Yasal Düzenlemeleri Siber Suçlarla Mücadele Noktasında Yeterli Bulma İle Siber Suç Korkusu Arasındaki İlişki

İlk olarak siber suçlara ilişkin yasal düzenlemeleri siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasındaki ilişkide 16 siber suç korkusundan 5'i için ki kare analizi sonucu yeterince veri olmadığından yorumlanamamıştır. Geriye kalan 11 siber suç korkusu sorusunun ise 2'si ile (siber zorbalık ve bilişim sistemleri aracılığıyla hakaret korkusu) siber suçlara ilişkin yasal düzenlemeleri siber suçlarla mücadele noktasında yeterli bulma arasında anlamlı bir ilişki bulunabilmiştir ($p<0.05$). Bu tablolar aşağıda sunulmuştur.

Tablo 57. Katılımcıların Siber Suçlarla İlgili Yasal Düzenlemelere İlişkin Algıları ile Siber Zorbalık Korkusu Arasındaki İlişki

Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli buluyor musunuz?		Siber Zorbalık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	46	86	42	174
	% satır	26,4%	49,4%	24,1%	100,0%
	% sütun	69,7%	64,7%	71,2%	67,4%
	% toplam	17,8%	33,3%	16,3%	67,4%
Orta Düzeyde Yeterli Buluyorum	Sayı	15	46	13	74
	% satır	20,3%	62,2%	17,6%	100,0%
	% sütun	22,7%	34,6%	22,0%	28,7%
	% toplam	5,8%	17,8%	5,0%	28,7%
Yeterli Buluyorum	Sayı	5	1	4	10
	% satır	50,0%	10,0%	40,0%	100,0%
	% sütun	7,6%	0,8%	6,8%	3,9%
	% toplam	1,9%	0,4%	1,6%	3,9%
Toplam	Sayı	66	133	59	258
	% satır	25,6%	51,6%	22,9%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	25,6%	51,6%	22,9%	100,0%
P=0,031, df=4 (10,630)					

Tablo 57'de görüleceği üzere katılımcıların Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli bulma düzeyleri ile siber zorbalık korkuları arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Buna göre Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri yeterli bulan bireylerin zaman zaman veya genellikle siber zorbalık korkusu yaşama oranlarının orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir. Bununla birlikte yasal düzenlemeleri orta düzeyde yeterli bulan katılımcılardaki korku oranları ise yetersiz bulan katılımcılara göre daha fazla bulunmuştur.

Tablo 58. Katılımcıların Siber Suçlarla İlgili Yasal Düzenlemelere İlişkin Algıları ile Bilişim Sistemleri Aracılığıyla Hakaret Korkusu Arasındaki İlişki

Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli buluyor musunuz?		Bilişim Sistemleri Aracılığıyla Hakaret (Sesli, Yazılı veya Görüntülü)			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	95	60	19	174
	% satır	54,6%	34,5%	10,9%	100,0%
	% sütun	67,4%	63,2%	86,4%	67,4%
	% toplam	36,8%	23,3%	7,4%	67,4%
Orta Düzeyde Yeterli Buluyorum	Sayı	37	35	2	74
	% satır	50,0%	47,3%	2,7%	100,0%
	% sütun	26,2%	36,8%	9,1%	28,7%
	% toplam	14,3%	13,6%	0,8%	28,7%
Yeterli Buluyorum	Sayı	9	0	1	10
	% satır	90,0%	0,0%	10,0%	100,0%
	% sütun	6,4%	0,0%	4,5%	3,9%
	% toplam	3,5%	0,0%	0,4%	3,9%
Toplam	Sayı	141	95	22	258
	% satır	54,7%	36,8%	8,5%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	54,7%	36,8%	8,5%	100,0%
P=0,012, df=4 (12,863)					

Tablo 58'de görüldüğü üzere katılımcıların Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli bulma düzeyleri ile bilişim sistemleri aracılığıyla hakaret korkuları arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da yine Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri yeterli bulan bireylerin zaman zaman veya genellikle bilişim sistemleri aracılığıyla hakaret korkusu yaşama oranlarının orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir. Bununla birlikte yasal düzenlemeleri orta düzeyde yeterli bulan katılımcılardaki korku oranları ise yetersiz bulan katılımcılara göre daha fazla bulunmuştur.

Sonuç olarak siber suçlara ilişkin yasal mevzuatı siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasında 2 siber suç türü için anlamlı ilişki bulunmuş, bu iki ilişkide ise birbirlerine benzer şekilde yasal mevzuatı yeterli bulan katılımcıların orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük korku oranlarına sahip oldukları, fakat bunun yanında yetersiz bulan katılımcıların ise orta düzeyde yeterli bulan katılımcılara göre daha düşük korku oranlarına sahip oldukları görülmüştür.

4.2.4.2. Kolluk Birimlerini Siber Suçlarla Mücadele Noktasında Yeterli Bulma İle Siber Suç Korkusu Arasındaki İlişki

İkinci olarak kolluk birimlerini siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasındaki ilişkide analiz sonuçlarına göre 16 siber suç korkusunun 4'ü ile (virüsler, truva atları ve zararlı yazılımlar; yasal süresi dolmasına rağmen yok edilmesi gereken verilerinizin yok edilmemesi; siber dolandırıcılık ve siber terörizm korkusu) kolluk birimlerini siber suçlarla mücadele noktasında yeterli bulma arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Bu tablolar aşağıda sunulmuştur.

Tablo 59. Katılımcıların Kolluk Birimlerine İlişkin Algıları ile Virüsler, Truva Atları ve Zararlı Yazılımlar Korkusu Arasındaki İlişki

Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?		Virüsler, Truva Atları ve Zararlı Yazılımlar			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	38	87	41	166
	% satır	22,9%	52,4%	24,7%	100,0%
	% sütun	70,4%	59,2%	68,3%	63,6%
	% toplam	14,6%	33,3%	15,7%	63,6%
Orta Düzeyde Yeterli Buluyorum	Sayı	9	52	16	77
	% satır	11,7%	67,5%	20,8%	100,0%
	% sütun	16,7%	35,4%	26,7%	29,5%
	% toplam	3,4%	19,9%	6,1%	29,5%
Yeterli Buluyorum	Sayı	7	8	3	18
	% satır	38,9%	44,4%	16,7%	100,0%
	% sütun	13,0%	5,4%	5,0%	6,9%
	% toplam	2,7%	3,1%	1,1%	6,9%
Toplam	Sayı	54	147	60	261
	% satır	20,7%	56,3%	23,0%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	20,7%	56,3%	23,0%	100,0%
P=0,048, df=4 (9,594)					

Tablo 59'da görüldüğü üzere katılımcıların Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli bulup bulmamaları ile virüsler, truva atları ve zararlı yazılımlar korkusu arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada kolluk birimlerini yeterli bulan katılımcılardaki virüsler, truva atları ve zararlı yazılımlar korkusunun orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%61,1). Fakat bunun yanında kolluk birimlerini yetersiz bulanlardaki korku oranları ise orta düzeyde yeterli bulanlara göre daha düşük seviyededir (%77,1).

Tablo 60. Katılımcıların Kolluk Birimlerine İlişkin Algıları ile Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerin Yok Edilmemesi Korkusu Arasındaki İlişki

Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?		Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	54	68	45	167
	% satır	32,3%	40,7%	26,9%	100,0%
	% sütun	65,1%	58,6%	72,6%	64,0%
	% toplam	20,7%	26,1%	17,2%	64,0%
Orta Düzeyde Yeterli Buluyorum	Sayı	19	43	15	77
	% satır	24,7%	55,8%	19,5%	100,0%
	% sütun	22,9%	37,1%	24,2%	29,5%
	% toplam	7,3%	16,5%	5,7%	29,5%
Yeterli Buluyorum	Sayı	10	5	2	17
	% satır	58,8%	29,4%	11,8%	100,0%
	% sütun	12,0%	4,3%	3,2%	6,5%
	% toplam	3,8%	1,9%	0,8%	6,5%
Toplam	Sayı	83	116	62	261
	% satır	31,8%	44,4%	23,8%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	31,8%	44,4%	23,8%	100,0%
P=0,025, df=4 (11,122)					

Tablo 60'ta görüldüğü üzere katılımcıların Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli bulup bulmamaları ile yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi korkusu arasında anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da yine kolluk birimlerini yeterli bulan katılımcılardaki yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi korkusunun orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%41,2). Fakat bunun yanında yine kolluk birimlerini yetersiz bulanlardaki korku oranları ise orta düzeyde yeterli bulanlara göre daha düşük seviyededir (%67,6).

Tablo 61. Katılımcıların Kolluk Birimlerine İlişkin Algıları ile Siber Dolandırıcılık Korkusu Arasındaki İlişki

Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?		Siber Dolandırıcılık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	55	74	34	163
	% satır	33,7%	45,4%	20,9%	100,0%
	% sütun	74,3%	57,4%	61,8%	63,2%
	% toplam	21,3%	28,7%	13,2%	63,2%
Orta Düzeyde Yeterli Buluyorum	Sayı	11	48	18	77
	% satır	14,3%	62,3%	23,4%	100,0%
	% sütun	14,9%	37,2%	32,7%	29,8%
	% toplam	4,3%	18,6%	7,0%	29,8%
Yeterli Buluyorum	Sayı	8	7	3	18
	% satır	44,4%	38,9%	16,7%	100,0%
	% sütun	10,8%	5,4%	5,5%	7,0%
	% toplam	3,1%	2,7%	1,2%	7,0%
Toplam	Sayı	74	129	55	258
	% satır	28,7%	50,0%	21,3%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	28,7%	50,0%	21,3%	100,0%
P=0,015, df=4 (12,409)					

Tablo 61'de görüldüğü üzere katılımcıların Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli bulup bulmamaları ile siber dolandırıcılık korkusu arasında da anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da aynı şekilde yine kolluk birimlerini yeterli bulan katılımcılardaki siber dolandırıcılık korkusunun orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%55,6). Fakat bunun yanında yine kolluk birimlerini yetersiz bulanlardaki korku oranları ise orta düzeyde yeterli bulanlara göre daha düşük seviyededir (%66,3).

Tablo 62. Katılımcıların Kolluk Birimlerine İlişkin Algıları ile Siber Terörizm Korkusu Arasındaki İlişki

Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?		Siber Terörizm			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	60	71	31	162
	% satır	37,0%	43,8%	19,1%	100,0%
	% sütun	69,0%	56,3%	70,5%	63,0%
	% toplam	23,3%	27,6%	12,1%	63,0%
Orta Düzeyde Yeterli Buluyorum	Sayı	18	48	11	77
	% satır	23,4%	62,3%	14,3%	100,0%
	% sütun	20,7%	38,1%	25,0%	30,0%
	% toplam	7,0%	18,7%	4,3%	30,0%
Yeterli Buluyorum	Sayı	9	7	2	18
	% satır	50,0%	38,9%	11,1%	100,0%
	% sütun	10,3%	5,6%	4,5%	7,0%
	% toplam	3,5%	2,7%	0,8%	7,0%
Toplam	Sayı	87	126	44	257
	% satır	33,9%	49,0%	17,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	33,9%	49,0%	17,1%	100,0%
P=0,049, df=4 (9,547)					

Tablo 62'de görüldüğü üzere katılımcıların Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli bulup bulmamaları ile siber terörizm korkusu arasında da anlamlı bir ilişki bulunmaktadır ($p<0.05$). Burada da yukarıdaki üç tabloda görüldüğü gibi kolluk birimlerini yeterli bulan katılımcılardaki siber terörizm korkusunun orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%50). Fakat yine yukarıdaki üç tabloya benzer şekilde kolluk birimlerini yetersiz bulanlardaki korku oranları ise orta düzeyde yeterli bulanlara göre daha düşük seviyededir (%62,9).

Sonuç olarak katılımcıların kolluk birimlerini yeterli bulmaları ile siber suç korkuları arasında dört siber suç türü açısından anlamlı ilişki bulunabilmiş, bu ilişkilerin de

tamamında benzer olarak kolluk birimlerini yeterli bulanların en düşük korku oranlarına sahip oldukları, fakat kolluk birimlerini yetersiz bulanların ise orta düzeyde yeterli bulanlara göre daha düşük korku oranlarına sahip oldukları görülmüştür.

4.2.4.3. Yargı Birimlerini Siber Suçlarla Mücadele Noktasında Yeterli Bulma İle Siber Suç Korkusu Arasındaki İlişki

İkinci olarak kolluk birimlerini siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasındaki ilişkide analiz sonuçlarına göre 16 siber suç korkusunun 2'si ile (siber zorbalık ve siber terörizm korkusu) yargı birimlerini siber suçlarla mücadele noktasında yeterli bulma arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Bu tablolar aşağıda sunulmuştur.

Tablo 63. Katılımcıların Yargı Birimlerine İlişkin Algıları ile Siber Zorbalık Korkusu Arasındaki İlişki

Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli buluyor musunuz?		Siber Zorbalık			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	48	91	42	181
	% satır	26,5%	50,3%	23,2%	100,0%
	% sütun	69,6%	67,9%	71,2%	69,1%
	% toplam	18,3%	34,7%	16,0%	69,1%
Orta Düzeyde Yeterli Buluyorum	Sayı	13	40	13	66
	% satır	19,7%	60,6%	19,7%	100,0%
	% sütun	18,8%	29,9%	22,0%	25,2%
	% toplam	5,0%	15,3%	5,0%	25,2%
Yeterli Buluyorum	Sayı	8	3	4	15
	% satır	53,3%	20,0%	26,7%	100,0%
	% sütun	11,6%	2,2%	6,8%	5,7%
	% toplam	3,1%	1,1%	1,5%	5,7%
Toplam	Sayı	69	134	59	262
	% satır	26,3%	51,1%	22,5%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	26,3%	51,1%	22,5%	100,0%
P=0,012, df=4 (12,863)					

Tablo 63'te katılımcıların Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli bulup bulmamaları ile siber zorbalık korkusu arasında anlamlı bir ilişki bulunduğu görülmektedir (p<0.05). Burada yargı birimlerini yeterli bulan katılımcılardaki siber zorbalık korkusunun orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%46,7). Fakat yargı birimlerini yetersiz bulanlardaki korku oranlarının ise orta düzeyde yeterli bulanlara göre daha düşük seviyede olduğu bulunmuştur (%73,5).

Tablo 64. Katılımcıların Yargı Birimlerine İlişkin Algıları ile Siber Terörizm Korkusu Arasındaki İlişki

Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli buluyor musunuz?		Siber Terörizm			Toplam
		Hiç korku yaşamıyorum	Zaman zaman korku yaşıyorum	Genellikle korku yaşıyorum	
Yetersiz Buluyorum	Sayı	62	83	31	176
	% satır	35,2%	47,2%	17,6%	100,0%
	% sütun	71,3%	65,9%	70,5%	68,5%
	% toplam	24,1%	32,3%	12,1%	68,5%
Orta Düzeyde Yeterli Buluyorum	Sayı	15	39	12	66
	% satır	22,7%	59,1%	18,2%	100,0%
	% sütun	17,2%	31,0%	27,3%	25,7%
	% toplam	5,8%	15,2%	4,7%	25,7%
Yeterli Buluyorum	Sayı	10	4	1	15
	% satır	66,7%	26,7%	6,7%	100,0%
	% sütun	11,5%	3,2%	2,3%	5,8%
	% toplam	3,9%	1,6%	0,4%	5,8%
Toplam	Sayı	87	126	44	257
	% satır	33,9%	49,0%	17,1%	100,0%
	% sütun	100,0%	100,0%	100,0%	100,0%
	% toplam	33,9%	49,0%	17,1%	100,0%
P=0,012, df=4 (12,863)					

Tablo 64'te katılımcıların Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli bulup bulmamaları ile siber terörizm korkusu arasında da anlamlı bir ilişki bulunduğu görülmektedir (p<0.05). Burada da yukarıdaki tabloyla benzer şekilde yargı birimlerini yeterli bulan katılımcılardaki siber terörizm korkusunun

orta düzeyde yeterli bulan ve yetersiz bulan katılımcılara göre daha düşük olduğu görülmektedir (%33,4). Fakat yine yukarıdaki tabloya benzer şekilde yargı birimlerini yetersiz bulanlardaki korku oranları ise orta düzeyde yeterli bulanlara göre daha düşük seviyededir (%64,8).

Sonuç olarak katılımcıların yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli bulmaları ile siber suç korkuları arasında iki siber suç türü açısından anlamlı ilişki bulunabilmiş, bu iki ilişkide de benzer olarak yargı birimlerini yeterli bulanların en düşük korku oranlarına sahip oldukları, fakat yetersiz bulanların ise orta düzeyde yeterli bulanlara göre daha düşük korku oranlarına sahip oldukları görülmüştür.

4.2.5. İş Yerinde ve İş Yeri Dışında Kullanılan Elektronik Cihazlardaki Önlem Alma/Başa Çıkma Stratejileri

Araştırmanın altıncı ve son hipotezi "Teknokent çalışanlarının iş yerlerinde ve iş yerleri dışında kullandıkları elektronik cihazlarda önlem alma/başa çıkma stratejileri arasında anlamlı bir ilişki bulunmaktadır" şeklinde oluşturulmuştur. Öncelikle bu hipotezle ilgili olarak yukarıda betimsel analizlerin yer aldığı kısımda katılımcıların iş yerinde ve iş yeri dışında kullanılan elektronik cihazlarda birbirleriyle oldukça yakın oranlarda önlem alma/başa çıkma stratejileri geliştirdikleri görülmektedir. Bununla birlikte iş yeri ve iş yeri dışındaki cihazlar arasında önlem ve strateji bakımından anlamlı bir ilişki olup olmadığı ise çapraz tablolar ve ki kare analizi vasıtasıyla araştırılmıştır. Burada ki kare analizi sonuçları yorumlanmaya elverişli olan 9 soru açısından iş yerinde ve dışında kullanılan elektronik cihazlar açısından katılımcıların önlem alma/başa çıkma stratejileri arasında anlamlı bir ilişki bulunduğu tespit edilmiştir. Katılımcıların iş yerinde ve iş yeri dışında kullandıkları elektronik cihazlardaki önlem alma/başa çıkma stratejilerine ilişkin oransal verilere ve tablolara yukarıda yer verildiği göz önünde bulundurularak bu kısımda yalnızca ki kare analizi sonuçlarına yer verilecektir. Yapılmış olan ki kare analizi ile ulaşılan sonuçlar aşağıda belirtilmektedir.

1- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında kullanıcı parolası koyup koymama açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (56,661))

2- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında kişisel ve/veya hassas bilgilerinin ele geçirilmesinden korktukları online işlemlerinde, güvenilir olduğunu düşündükleri bir VPN programı kullanıp kullanmamaları açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=4 (294,879))
3- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında güvenilir gözükmeyen web sayfalarını ziyaret etmekte bir sakınca görüp görmemeleri açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=4 (363,612))
4- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında bilgisayarlarının kamerasını kullanmadıkları zamanlarda üzerini bant, kağıt vb. şeylerle kapalı tutup tutmamaları açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (141,198))
5- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında tanımadıkları kişilerden gelen ve güvenilir olmadığını düşündükleri e-postaları ve/veya e-posta eklerini açıp açmamaları ile ilgili olarak ki kare analizi sonucu yorumlanamamaktadır.
6- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında online alışveriş sitelerinden yaptıkları alışverişlerde adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin “https://” ile başlamasına dikkat edip etmemeleri ile ilgili olarak ki kare analizi sonucu yorumlanamamaktadır.
7- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında internet bankacılığı hizmetlerini kullanırken adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin “https://” ile başlamasına dikkat edip etmemeleri ile ilgili olarak ki kare analizi sonucu yorumlanamamaktadır.
8- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında verilerini silinme, çalınma vb. durumlara karşı yedekleyip yedeklememeleri açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (121,846))
9- Katılımcıların iş yerinde ve dışında kullanmakta oldukları bilgisayarları arasında güncel durumda bulanan ve güvenilir bir Anti-virüs yazılımı bulunup bulunmama açısından anlamlı bir ilişki bulunmaktadır. (P=0.000, df=1 (132,006))

10- Katılımcıların iş yerinde ve dışında kullanmakta oldukları bilgisayarları arasında güncel durumda bulanan ve güvenilir bir Anti-Malware yazılımı bulunup bulunmama açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (136,679))
11- Katılımcıların iş yerinde ve dışında kullandıkları elektronik cihazları arasında işletim sistemlerinin (Windows, OS, Android, iOS vb.) güncel durumda olmalarına dikkat etme açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (142,143))
12- Katılımcıların iş yerinde ve dışında kullanmakta oldukları bilgisayarları arasında açık durumda olan bir Güvenlik Duvarı (Windows güvenlik duvarı vb.) bulunması açısından anlamlı bir ilişki bulunmaktadır. (p=0.000, df=1 (120,193))

SONUÇ VE DEĞERLENDİRME

Suç korkusu 1960'lı yıllardan itibaren hem akademik alanda hem de politika oluşturma konusunda başlıca konulardan birisi haline gelmiştir (Hale, 1996, s. 1). Aradan geçen yarım asırdan fazla süre içerinde suç korkusu konusunda hem ulusal hem de uluslararası alanda literatüre katkı oluşturabilecek çok sayıda çalışma yapılmıştır. Suç korkusu konusundaki bu çalışmalar incelendiğinde araştırma konularının geleneksel suçları içermekte olduğu görülmektedir. Bununla birlikte teknolojinin gelişmesi ve özellikle de internetin ortaya çıkmasıyla birlikte siber suçlar giderek önem kazanmış ve birçok noktada geleneksel suçların önüne geçmeye başlamıştır. Buna son zamanlarda akıllanan eşyalar, nesnelerin interneti, kripto paralar, robotik teknolojiler ve yapay zeka gibi konularda meydana gelen gelişmeler eklendiğinde siber suçların işlenme alanlarının ve bireylere verebileceği zararların giderek artmakta olduğunu söylemek mümkündür. Böylesine büyümekte olan bir siber suç tehdidi karşısında bireylerin korku yaşamaları da en az geleneksel suçlardan korku yaşamaları kadar doğal ve olasıdır. Nitekim ABD'de IBM tarafından yapılan bir araştırmada katılımcılar siber suçlardan mağdur olma olasılıklarını fiziksel suçlardan mağdur olmaya göre üç kat daha fazla görmüşlerdir (IBM, 2006). Dolayısıyla siber suç korkusu da tüm bu gelişmelerin de etkisiyle 2000'li yıllarla birlikte literatürde kendisine yer bulmaya başlamıştır. Bununla birlikte siber suç korkusu konusunda uluslararası literatürde yer alan çalışmaların giderek artmakta olduğu gözlemlenmekte fakat ulusal literatürde bu konuda bir eksiklik olduğu görülmektedir. Türkiye'de siber suç korkusu konusu üzerine yüksek lisans veya doktora tezi düzeyinde yapılmış hiçbir çalışmaya rastlanılmamış, yalnızca yakın zamanda bir akademik dergide Erdal Servet Yurtsal (2016) tarafından yayınlanmış ve sosyal ağlardaki suç korkusunu inceleyen bir makale bulunabilmiştir. Dolayısıyla bu çalışma da hem toplumsal anlamda giderek önem kazanmakta olan bir sosyal olgu olarak siber suç korkusuna değinmek, hem de literatüre bir katkı sağlayarak Türkiye'de bu konuda yapılacak olan çalışmaların önünü açmak amacıyla Ankara'daki teknokentler örneği üzerinden siber suç korkusunu ve önlem alma stratejilerini konu edinmiştir.

Siber dünyada yaşanan gelişmelerin bireylerin sosyalleşme alanlarını geleneksel alanlardan siber alanlara doğru kaydırması ve bireylerin günlük rutinlerinin giderek siber alanlarda da yoğunlaşmaya başlaması araştırmada kullanılacak kuramsal çerçevenin de

geleneksel suçların yanında siber suçlar ve siber suç korkusu için de açıklama gücüne sahip bir kuramsal yaklaşım olmasını zorunlu kılmıştır. Bu noktada bu araştırmada bireylerin günlük rutinlerinin ve bu rutinler içerisinde ortaya çıkan suç fırsatlarının suçun oluşumuna neden olduğu yaklaşımını benimseyen ve suçun ortadan kaldırılmasının da motive olmuş suçlu, uygun hedef ve koruyucuların yokluğu üçlüsünden en az birisini ortadan kaldırmakla mümkün olacağını savunan Rutin Aktiviteler Teorisi araştırmanın kuramsal çerçevesini oluşturmuştur.

Araştırmanın teorik ve kuramsal kısmının ardından Ankara'da yer alan ve araştırma için izin alınabilen 4 adet teknokent'te (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışan bireyler üzerinde bir anket çalışması gerçekleştirilmiş ve bu anket çalışmasının sonuçları SPSS 25.0 paket programı üzerinden analiz edilerek hipotezler test edilmiştir.

Araştırmada (sorulara cevap veren) katılımcıların %32,20'sini kadınların, %67,80'ini erkeklerin oluşturduğu, çoğunluğun (%77,82) 20-34 yaş aralığında bulunan bireylerden oluştuğu, eğitim durumunun %95'ten daha fazla oranda üniversite ve üzeri, %33,08 oranında ise lisansüstü olduğu, katılımcıların yarısına yakınının gelir durumunun 2001 – 4000 TL arasında olduğu, genel müdürden stajyer düzeyine kadar çok sayıda pozisyonda çalışan bireylerin katılımcılar arasında yer aldığı ve yazılım ve bilişim teknolojileri sektörünün ise %70'e yakın oranda katılımcıların en fazla çalıştıkları sektör olduğu görülmüştür.

Araştırmanın temel öngörüsünü "Ankara'daki Teknokentlerde (ODTÜ Teknokent, Bilkent Cyberpark, Hacettepe Teknokent ve Gazi Teknopark) çalışan bireyler üzerinde siber suç korkusu bulunmaktadır" oluşturmuştur. Araştırmada katılımcılar kendilerine yöneltilmiş olan toplam 16 adet siber türünden mağdur olmak konusunda %50'den daha fazla oranlarda zaman zaman veya genellikle korku yaşadıklarını belirtmişlerdir. Buradan hareketle araştırma katılımcılarında siber suç korkusunun bulunduğu görülmektedir. Katılımcıların en fazla korku yaşamakta oldukları siber suç türünü "kimlik hırsızlığı" oluştururken, en az korku yaşamakta oldukları siber suç türünü ise "bilişim sistemleri aracılığıyla hakaret" oluşturmaktadır. Meško ve Bernik (2011) tarafından yapılmış olan çalışmada da kimlik hırsızlığı korkusu, bilgisayar virüsleri korkusunun ardından en fazla korku yaşanan ikinci siber suç türüdür. Ayrıca Roberts vd. (2013, s. 320) tarafından

yapılmış olan çalışmada ise bizim çalışmamızda en fazla korkulan 3. siber suç olarak bulunan kredi kartlarının yasa dışı kullanımı suçunun en fazla korkulmakta olan suçlar arasında olduğu belirtilmektedir. Dolayısıyla bu çalışmanın bu anlamda literatürle tutarlı olduğunu söylemek mümkündür.

Araştırmanın ilk hipotezini "bireylerin yaş, cinsiyet, eğitim durumu ve gelir düzeyleri ile siber suç korkuları arasında anlamlı bir ilişki bulunmaktadır" oluşturmuştur. Siber suç korkusunun yaş, cinsiyet, eğitim durumu ve gelir düzeyi ile ilişkisi incelendiğinde öncelikle araştırmada ki kare analizi sonuçları yorumlanabilen 13 siber suç korkusu ile yaş arasında anlamlı bir ilişki bulunamamıştır ($p>0.05$). Bununla birlikte Alshalan (2006, s. 147) ise yapmış olduğu çalışmada yaşlı bireylerin genç bireylere nazaran daha fazla siber suç korkusuna sahip olduğu sonucuna ulaşmaktadır. Yine Alshalan'a göre (2006, s. 147) genç kadınların ise yaşlı kadınlara nazaran siber suç korkuları daha fazladır. Bu noktada bizim çalışmamız açısından yaş ve korku oranları arasında anlamlı ve istikrarlı herhangi bir sonuca ulaşılamamıştır. Bununla birlikte siber suç korkusu konusunda daha geniş kapsamlı olarak yapılacak bir çalışmanın bu konuda daha net sonuçlar verebileceği söylenebilecektir.

Cinsiyet konusuna gelindiğinde ise bu araştırmada katılımcılara yöneltilen toplam 16 siber suç türü içerisinden 12'si için cinsiyetler ile korku oranları arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Ayrıca yine bu 16 siber suç türü içerisinden 14'ü için kadınlarda korku oranları erkeklere göre daha fazla bulunmuşken, yalnızca 2 siber suç türü (banka veya kredi kartlarının ya da bunlara ait bilgilerin başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğranılması ve yasal süresi dolmasına rağmen yok edilmesi gereken verilerin yok edilmemesi korkusu) için korku oranları erkekler arasında kadınlara göre daha fazla bulunmuştur. Bu sonuçlar Alshalan (2006, s. 146)'ın çalışmasında kadınların siber suç mağduru olma ihtimalleri daha düşük olmasına rağmen siber suç korkularının daha fazla olduğu sonucuyla örtüşür niteliktedir. Aynı şekilde Henson (2011, s. 125)'un yapmış olduğu çalışma ile de tutarlı olan bu sonuçlar, Abdulai (2016, s. 82) ve Yurtsal (2016)'ın çalışmalarından ise farklılık göstermektedir. Bununla birlikte Sutton ve Farrall (2004, s. 221) ise yaptıkları çalışmada suç korkusu araştırmalarında cinsiyete dayalı olarak ortaya çıkan sonuçların gerçeği yansıtmayabileceğini, bunun da erkeklerin toplumsal olarak arzu edilen şekilde suç korkusu ile ters ilişkili olacak cevap örüntüleri üretmeleri nedeniyle oluştuğunu

belirtmektedirler. Onlara göre (2004, s. 221) gelecekteki suç korkusu çalışmaları tasarlanırken erkekliğin bu korkuyu maço gizleme (Sutton ve Farrall, 2004, s. 221) özelliği göz önünde bulundurulmalıdır.

Eğitim durumu ile siber suç korkusu ilişkisi incelendiğinde ise bu araştırmada yer alan 16 siber suç korkusundan ikisi ile (bilgisayar korsanlığı ve bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu) katılımcıların eğitim durumları arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Burada bilgisayar korsanlığı için korku sıralaması en yüksekten en aza doğru lise, lisansüstü ve üniversite şeklinde ilerlerken, bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu için ise lise, üniversite ve lisansüstü şeklinde sıralı olarak azalmaktadır. Bununla birlikte her iki korku türünün de eğitim durumunu lise olarak belirtenlerde en yüksek düzeyde olduğu görülmektedir.

Gelir düzeyi konusunda ise araştırmada ki kare analizi sonuçları yorumlanabilen 10 siber suç korkusu ile katılımcıların gelir düzeyi arasında anlamlı bir ilişki bulunamamıştır ($p>0.05$). Roberts vd. (2013, s. 17) tarafından yapılan çalışmada da benzer şekilde siber kimlik hırsızlığı ve benzeri dolandırıcılık faaliyetleri korkusunun yüksek gelire sahip bireylerde daha fazla olacağı hipotezi doğrulanamamıştır.

Araştırmanın ikinci hipotezini ise "geçmiş siber suç mağduriyeti ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" oluşturmuştur. Araştırmada geçmiş siber suç mağduriyeti ile siber suç korkusu ilişkisi incelendiğinde 16 siber suç türünden 5'i (banka veya kredi kartlarının ya da bunlara ait bilgilerin başkalarının eline geçmesi veya sahteciliğinin yapılması yoluyla zarara uğrama, bilişim sistemleri aracılığıyla hakaret, siber dolandırıcılık, siber taciz ve siber tehdit ve şantaj korkusu) için olan korku ile geçmiş siber suç mağduriyeti arasında anlamlı bir ilişki bulunduğu görülmüştür ($p<0.05$). Bu anlamlı ilişkilerin tamamı için de geçmişte siber suç mağduriyeti yaşamış olan bireylerdeki korku oranlarının yaşamamış olan bireylere göre daha fazla olduğu görülmüştür. Nitekim bu sonuçlar Alshalan (2006, s. 147) ve Yurtsal (2016) tarafından yapılan çalışmalarda da ulaşılan geçmiş siber suç mağduriyetinin siber suç korkusunu arttırmakta olduğu sonucu ile tutarlı durumdadır.

Araştırmanın üçüncü hipotezi "siber suçlardan mağdur olmamak adına alınan önlemleri yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" şeklindedir.

Burada katılımcıların almış oldukları önlemleri yeterli bulmaları ile 16 siber suç korkusu içerisinden 4'ü (bilgisayar korsanlığı, bilişim sistemleri aracılığıyla hakaret, siber dolandırıcılık ve siber taciz korkusu) arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Burada da yine bu anlamlı ilişkilerin tamamında ortak olarak katılımcıların aldıkları önlemleri yeterli bulma düzeyleri arttıkça siber suç korkularının azalmakta olduğu görülmektedir.

Araştırmanın dördüncü hipotezi ise "siber suçlara ilişkin yasal düzenlemeleri, kolluk ve yargı birimlerini siber suçlarla mücadele noktasında yeterli bulma ile siber suç korkusu arasında anlamlı bir ilişki bulunmaktadır" şeklindedir. Araştırma sonuçlarına göre ki kare analizi sonuçları yorumlanabilen 11 siber suç korkusundan 2'si ile (siber zorbalık ve bilişim sistemleri aracılığıyla hakaret korkusu) siber suçlara ilişkin yasal düzenlemeleri yeterli bulma arasında, 16 siber suç korkusunun 4'ü ile (virüsler, truva atları ve zararlı yazılımlar, yasal süresi dolmasına rağmen yok edilmesi gereken verilerinizin yok edilmemesi, siber dolandırıcılık ve siber terörizm korkusu) kolluk birimlerini yeterli bulma arasında ve 16 siber suç korkusunun 2'si ile de (siber zorbalık ve siber terörizm korkusu) yargı birimlerini yeterli bulma arasında anlamlı bir ilişki bulunmuştur ($p<0.05$). Bu anlamlı ilişkilerin tamamında da ortak olarak yasal düzenlemeleri, kolluk ve yargı birimlerini yeterli bulan katılımcıların en düşük korku oranlarına sahip oldukları, fakat yetersiz bulanların ise orta düzeyde yeterli bulanlara göre daha düşük korku oranlarına sahip oldukları görülmüştür.

Araştırmanın son hipotezini ise "teknokent çalışanlarının iş yerlerinde ve iş yerleri dışında kullandıkları elektronik cihazlarda önlem alma/başa çıkma stratejileri arasında anlamlı bir ilişki bulunmaktadır" oluşturmuştur. Burada katılımcılara yöneltilen 12 sorudan ki kare analizi sonuçları yorumlanmaya elverişli olan 9 soru açısından iş yerinde ve dışında kullanılan elektronik cihazlardaki önlem alma/başa çıkma stratejileri arasında anlamlı bir ilişki bulunduğu tespit edilmiştir ($p<0.05$). Burada da katılımcıların çoğunluğunun iş yerinde ve işyeri dışında kullandıkları elektronik cihazlarda benzer önlem alma/başa çıkma stratejileri kullandıkları görülmüştür.

Dolayısıyla bu çalışmanın Ankara'daki teknokent çalışanlarının siber suç korkuları ve önlem alma stratejileri üzerine önemli sonuçlar ortaya koyduğu ve gelecekte siber suç korkusu konusunda yapılacak olan çalışmalarda da bu çalışmadan yararlanılabileceği

söylenebilir. Bununla birlikte gelecekte yapılacak olan çalışmaların daha geniş kapsamlı olarak daha farklı yaş, meslek vb. gruplardan bireyleri içerecek şekilde, belirli bir bölge, il veya ülkenin tamamı için korku oranlarını ortaya çıkarabilecek nitelikte gerçekleştirilmesi, nicel verilerin yanında nitel verileri de araştırmaya dahil eden karma çalışmalarla katılımcıların korku düzeylerinin hem içeriden hem de dışarıdan değerlendirilmesi ve korkunun bireylerin toplumsal hayatlarına olan etkilerini daha ayrıntılı olarak ele alan çalışmalar yapılması tavsiye edilebilir.

KAYNAKÇA

Abdulai, M. (2016). *Determinants of fear of cybercrime victimisation: A study of credit/debit card fraud among students of the University of Saskatchewan* (Yüksek Lisans Tezi). University of Saskatchewan, Saskatchewan.

Akgüç, Ö. (2004). *Mahremiyet açısından elektronik gözetim ve denetim: Tüketicinin denetimi, gözetimi ve online alışveriş siteleri üzerine bir uygulama* (Yüksek Lisans Tezi). Ankara Üniversitesi, Ankara.

Alshalan, A. (2006). *Cyber-crime fear and victimization: An analysis of a national survey* (Doktora Tezi). Mississippi State University, Mississippi.

Ashton, K. (2009). That 'internet of things' thing. In the real world things matter more than ideas. *RFiD Journal*, 22.

Aslanyürek, M. (2015). *İnternet güvenliği ve çevrimiçi gizlilik alanlarında yaşanan sorunlar: İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları üzerine bir araştırma* (Yüksek Lisans Tezi). Gazi Üniversitesi, Ankara.

Audit Commission for Local Authorities in England and Wales. (1998). *Ghost in the machine: An analysis of IT fraud and abuse*. Audit Commission.

Bernik, I., Dobovšek, B., & Markelj, B. (2013). To fear or not to fear on cybercrime. *IIASS: Innovative Issues and Approaches in Social Sciences, 6*(3), 7-17.

Boss, S. R., Kirsch, L. J., Angermeier, I., & Boss, R. (2009). Familiarity breeds content: How fear of cybercrime influences individual precaution-taking behavior. *Paper presented at the IFIP TC8 International Workshop on IS Security Research*, Capetown, South Africa.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400.

Brantingham, P. J., & Brantingham, P. L. (1984). *Patterns in crime*. New York: Macmillan.

Brenner, S. W. (2006). At light speed: Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law and Criminology*, 97, 379.

Burden, K., & Palmer, C. (2003). Internet crime: Cyber crime-A new breed of criminal? *Computer Law & Security Review*, *19*(3), 222-227.

Choi, K.-s. (2008). *Structural equation modeling assessment of key causal factors in computer crime victimization* (Doktora Tezi). Indiana University of Pennsylvania, Pennsylvania.

Clough, J. (2015). *Principles of cybercrime*: New York: Cambridge University Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588-608.

Cohen, L. E., Felson, M., & Land, K. C. (1980). Property crime rates in the United States: A macrodynamic analysis, 1947-1977; with ex ante forecasts for the mid-1980s. *American Journal of Sociology*, *86*(1), 90-118.

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal: Rational choice perspectives on offending*. New York: Springer-Verlag.

CSEW. (2017). *Crime in England and Wales: Year ending June 2017*. Erişim tarihi: 14.11.2017, https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/june2017.

Cullen, F. T., & Agnew, R. (2003). *Criminological theory: Past to present - Essential readings* (Second Edition ed.). Los Angeles, CA: Roxbury Publishing Company.

Çardak, B. (2011). *Kentlerde yaşayan kadınlarda suç mağduru olma korkusu üzerine nitel bir çalışma* (Yüksek Lisans Tezi). Kara Harp Okulu Komutanlığı Savunma Bilimleri Enstitüsü, Ankara.

Çetin, D. (2010*). A study of fear of crime in two districts of Ankara* (Doktora Tezi). Orta Doğu Teknik Üniversitesi, Ankara.

Dolu, O. (2012). *Suç teorileri: Teori, araştırma ve uygulamada kriminoloji*. Ankara: Seçkin.

EGM. (2016). *Siber Suçlarla Mücadele Daire Başkanlığı*. Erişim tarihi: 26.11.2017, https://www.egm.gov.tr/sayfalar/sibersuclarlamucadeledairebaskanligi.aspx.

Eğilmez, M. (2017). *Kripto paralar, bitcoin ve blockchain*. Erişim tarihi: 19.11.2017, http://www.mahfiegilmez.com/2017/11/kripto-paralar-bitcoin-ve-blockchain.html.

Elitaş, T., & Keskin, S. (2014). Sanal aidiyet bağlamında zihinsel diaspora: Facebook örneği. *Atatürk İletişim Dergisi*, (7), 161-186.

Council of Europe (2001). *Convention on cybercrime*. Budapest, November, 23.

European Commission. (2017). *Cybercrime*. Erişim tarihi: 02.12.2017, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en.

Europol. (2017). *European Cybercrime Centre - EC3*. Erişim tarihi: 02.12.2017, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

FBI. (2017a). *Leadership & Structure*. Erişim tarihi: 02.12.2017, https://www.fbi.gov/about/leadership-and-structure.

FBI. (2017b). *What we investigate*. Erişim tarihi: 02.12.2017, https://www.fbi.gov/investigate/cyber.

Felson, M. (1986a). Linking criminal choices, routine activities, informal control, and criminal outcomes. In R. V. C. Derek B. Cornish (Ed.), *The reasoning criminal: Rational choice perspectives on offending* (pp. 119-128). New York: Springer-Verlag.

Felson, M. (1986b). Routine activities, social controls, rational decisions, and criminal outcomes. In D. B. C. a. R. V. Clarke (Ed.), *The reasoning criminal* (pp. 302-327). New York: Springer Verlag.

Felson, M. (1987). Routine activities and crime prevention in the developing metropolis. *Criminology*, *25*(4), 911-932.

Felson, M. (1998). Crime and everyday life. In (2nd Edition ed.). CA: Thousand Oaks, CA: Pine Forge Press.

Felson, M. (2000). The routine activity approach as a general crime theory. In S. S. Simpson (Ed.), *Of crime & criminality: The use of theory in everyday life* (Vol. 2, pp. 160-167). Thousand Oaks, CA: Pine Forge Press.

Ferraro, K. F., & Grange, R. L. (1987). The measurement of fear of crime. *Sociological Inquiry*, *57*(1), 70-97.

Finklea, K. M., & Theohary, C. A. (2015). *Cybercrime: Conceptual issues for congress and US law enforcement*.

Furedi, F. (2006). *Culture of fear revisited*: A&C Black.

Furnell, S. (2001). The problem of categorising cybercrime and cybercriminals. *Paper presented at the 2nd Australian information warfare and security conference*.

Gaziarifoğlu, Y. (2009). *Suç mağduriyeti korkusu ve algılanan suç mağduriyeti riskinin değerlendirilmesi* (Yüksek Lisans Tezi). İstanbul Üniversitesi, İstanbul.

Gercke, M. (2012). Understanding cybercrimes: Phenomena, challenges and legal response: *International Telecommunication Union*.

GFI. (2015). *US cyber security survey: Fear of cyber crime up 66 percent*. Erişim tarihi: 11.09.2017, https://www.gfi.com/company/press/2015/02/us-cyber-security-survey-fear-of-cyber-crime-up-66-percent.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13-20.

Gökulu, G. (2011). *Perceived risk of victimization and fear of crime: A case study of METU students* (Doktora Tezi). Middle East Technical University, Ankara.

Grabosky, P., Smith, R. G., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge: Cambridge University Press.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? S*ocial & Legal Studies*, *10*(2), 243-249.

Griffin, A. (2017). *Facebook's artificial intelligence robots shut down after they start talking to each other in their own language*. Erişim tarihi: 19.11.2017,

http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology*, *4*(2), 79-150.

Hawley, A. (1950). *Human ecology: A theory of community structure*. New York: Ronald.

Hekim, H., & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, 135-158.

Henson, B. (2011). *Fear of crime online: examining the effects of online victimization and perceived risk on fear of cyberstalking victimization* (Doktora Tezi). University of Cincinnati, Cincinnati.

Henson, B., & Reyns, B. W. (2015). The only thing we have to fear is fear itself… and crime: the current state of the fear of crime literature and where it should go next. *Sociology Compass*, *9*(2), 91-103.

Higgins, G. E., Ricketts, M. L., & Vegh, D. T. (2008). The role of self-control in college student's perceived risk and fear of online victimization. *American Journal of Criminal Justice*, *33*(2), 223.

Hirschi, T. (1969). *Causes of delinquency*. Berkeley and Los Angeles: University of California Press.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25. doi:10.1080/01639620701876577.

IBM. (2006). IBM Survey: *Consumers think cybercrime now three times more likely than physical crime*. Erişim tarihi: 04.11.2017, https://www-03.ibm.com/press/us/en/pressrelease/19154.wss.

Jandarma Genel Komutanlığı. (2017). *Hırsızlık ve dolandırıcılık olaylarında alınması gereken bireysel önlemler ve tavsiyeler*. Erişim tarihi: 02.12.2017, http://www.jandarma.gov.tr/asayis/suc_ks/Tedbirler.htm.

John, T., & Tierney, J. (2009). *Key perspectives in criminology*. Berkshire: McGraw-Hill Education.

Karagülmez, A. (2009). *Bilişim suçları ve soruşturma-kovuşturma evreleri*. Ankara: Seçkin Yayıncılık.

Karakaya, O. (2015). *Liseli gençlerde suç mağduru olma korkusu: Ankara örneği* (Yüksek Lisans Tezi), Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı, Ankara.

Karslıoğlu, F. (2014). *Siber gözetim: Toplumsal denetim aracı olarak internetin dönüşümü* (Yüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Anabilim Dalı, İstanbul.

Kılıç, N. S. (2012). Toplumsal ilişkiler alanı olarak sanal âlem üzerine Schutzcu bir çözümleme. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *14*(1), 139-150.

Kosukoğlu, N. (2011). *Criminalizing the dangerous others in Istanbul: The middle class and the fear of crime in the 2000's* (Yüksek Lisans Tezi), Boğaziçi Üniversitesi Atatürk İlkeleri ve İnkılap Tarihi Enstitüsü, İstanbul.

Kul, M. (2009). *Toplumda suça ilişkin korkunun yapılaşması* (Doktora Tezi). Ankara Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı, Ankara.

Kurt, İ. (2012). Toplumsallaşma sürecinin 'toplumsanallaşma' bağlamındaki yolculuğu. *Bayburt Eğitim Fakültesi Dergisi*, *7*(1).

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. doi:10.1080/01639625.2015.1012409

Lilley, P. (2002). *Hacked, attacked & abused: Digital crime exposed*. London: Kogan Page Publishers.

Liska, A. E., Lawrence, J. J., & Sanchirico, A. (1982). Fear of crime as a social fact. *Social Forces, 60*(3), 760-770.

Liska, A. E., & Warner, B. D. (1991). Functions of crime: A paradoxical process. *American Journal of Sociology, 96*(6), 1441-1463.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410. doi:10.1080/01639620903004903

Medina, J. E. (2014). Felson, Marcus. The Encyclopedia of Theoretical Criminology.

Merriam-Webster. (2017). *Cybercrime*. Erişim tarihi: 31.12.2017, https://www.merriam-webster.com/legal/cybercrime.

Meško, G., & Bernik, I. (2011). Cybercrime: Awareness and fear - Slovenian perspectives. *Paper presented at the 2011 European Intelligence and Security Informatics Conference (EISIC).*

Mevlütoğlu, M. A. (2016). *Robotik teknolojileri sektör raporu*. Erişim tarihi: 19.11.2017, https://www.stm.com.tr/documents/file/Pdf/9.Robotik%20Teknolojileri_2016-08-03-11-00-47.pdf.

Miethe, T. D., & Meier, R. F. (1994). *Crime and its social context: Toward an integrated theory of offenders, victims, and situations*. Suny Press.

Morgan, S. (2017). *2017 Cybercrime report*. Erişim tarihi: 14.11.2017, https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

National Crime Agency. (2016). Cyber crime assessment 2016. Erişim tarihi: 14.11.2017, http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.

Ngo, F., & Jaishankar, K. (2017). Commemorating a decade in existence of the International Journal of Cyber Criminology: A research agenda to advance the scholarship on cyber crime. *International Journal of Cyber Criminology*, *11*(1).

Ohm, P. (2007). The myth of the superuser: Fear, risk and harm online. *UC Davis L. Rev.*, 41, 1327-1402.

Öztürk, M. (2015). *Sosyolojik açıdan suç korkusu ve yaşam memnuniyeti: Mersin ili örneği* (Doktora Tezi), Cumhuriyet Üniversitesi, Sosyal Bilimler Enstitüsü, Sosyoloji Anabilim Dalı, Sivas.

Oxford University Press (2017). *Cybercrime*. Erişim tarihi: 31.12.2017, https://en.oxforddictionaries.com/definition/cybercrime.

Radda, S. I., & Ndubueze, P. N. (2013). Fear of on-line victimization among undergraduate students: A comparative study of two selected urban universities. *African Journal of Criminology & Justice Studies*, 7.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011a). Being pursued online. *Criminal Justice and Behavior*, *38*(11), 1149-1169. doi:10.1177/0093854811421448

Reyns, B. W., Henson, B., & Fisher, B. S. (2011b). Being pursued online: Applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. *Psychiatry, Psychology and Law*, *20*(3), 315-328.

Stuart, H. (2014). *Americans fear hacking more than any other crime, poll finds*. Erişim tarihi: 11.09.2017, https://www.huffingtonpost.com/2014/10/28/hacking-fear-poll_n_6057100.html.

Sutton, R. M., & Farrall, S. (2004). Gender, socially desirable responding and the fear of crime: Are women really more anxious about crime? *British Journal of Criminology*, *45*(2), 212-224.

Wall, D. S. (2008a). Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime. *Information, Communication & Society*, *11*(6), 861-884.

Wall, D. S. (2008b). Cybercrime, media and ınsecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22*(1-2), 45-63.

Williams, M. L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology*, *56*(1), 21-48. doi:10.1093/bjc/azv011

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, *8*(1), 36.

Yurtsal, E. S. (2016). Fear of crime in social networks: Facebook example. *Güvenlik Bilimleri Dergisi*, *5*(2), 93-112.

EK 1: ARAŞTIRMADA KULLANILAN ANKET FORMU

"SİBER SUÇ KORKUSU ve ÖNLEM ALMA STRATEJİLERİ: ANKARA'DAKİ TEKNOKENTLER ÖRNEĞİ" (YÜKSEK LİSANS TEZİ)

ANKET SORULARI

A. DEMOGRAFİK VE GENEL SORULAR

1. Yaşınız?

1) 16-20 2) 20-24 3) 25 -29 4) 30-34 5) 35-39
6) 40-44 7) 45-49 8) 50-54 9) 55 ve üstü

2. Cinsiyetiniz?

1) Kadın 2) Erkek

3. Eğitim durumunuz?

1) İlkokul 2) Ortaokul 3) Lise 4) Üniversite 5) Lisansüstü

4. Aylık gelir düzeyiniz?

1) 2000 TL ve altı 2) 2001 TL – 4000 TL 3) 4001 TL – 6000 TL
4) 6001 TL – 8000 TL 5) 8001 TL – 10000 TL 6) 10000 TL üzeri

5. Çalıştığınız kurumdaki pozisyonunuz?

……..

6. Çalıştığınız kurum hangi sektörde faaliyet göstermektedir?

1) Yazılım ve Bilişim Teknolojileri
2) Elektrik, Elektronik
3) Makine ve Tasarım
4) Telekomünikasyon
5) Biyoteknoloji
6) Enerji
7) Medikal & Biyomedikal
8) İleri Malzeme
9) Gıda
10) Kimya

11) Sağlık / İlaç
12) Uzay ve Havacılık Teknolojileri
13) Çevre
14) Savunma Sanayi
15) Nanoteknoloji
16) Otomotiv
17) Tarım
18) Madencilik
19) Diğer (……)

B. SİBER SUÇ KORKUSU İLE İLGİLİ SORULAR

Aşağıda sıralanan siber suç türlerinden mağdur olma konusunda sizin durumunuzu en iyi yansıtan ifadeyi seçiniz.

7- Bilişim Sisteminize Hukuka Aykırı Olarak Girilmesi ve Sistemde Kalınmaya Devam Edilmesi olarak adlandırılan "**Bilgisayar Korsanlığı (Hacking)**":

1) Bilgisayar Korsanlığı (Hacking)'den mağdur olma konusunda **hiç korku yaşamıyorum**
2) Bilgisayar Korsanlığı (Hacking)'den mağdur olma konusunda **zaman zaman korku yaşıyorum**
3) Bilgisayar Korsanlığı (Hacking)'den mağdur olma konusunda **genellikle korku yaşıyorum**

8- Bilişim sistemlerinin erişilebilirliğine yönelik hizmeti engelleme saldırıları olarak adlandırılan "**Denial of Service (DOS) Saldırıları"** (Örneğin ulaşmak istediğiniz bir internet sitesi sunucusuna çok sayıda sahte bağlantı ile yüklenilerek sizin gerçek bağlantınızın o sunucuya erişebilirliğinin engellenmesi, ya da şahsınıza ait bir internet sitesi sunucusuna erişimin bu tarz bir saldırıyla engellenmesi):

1) Denial of Service (DOS) Saldırıları'ndan mağdur olma konusunda **hiç korku yaşamıyorum**
2) Denial of Service (DOS) Saldırıları'ndan mağdur olma konusunda **zaman zaman korku yaşıyorum**

3) Denial of Service (DOS) Saldırıları'ndan mağdur olma konusunda **genellikle korku yaşıyorum**

9- Virüsler, Truva Atları ve Zararlı Yazılımlar:

1) Virüsler, Truva Atları ve Zararlı Yazılımlar'dan mağdur olma konusunda **hiç korku yaşamıyorum**
2) Virüsler, Truva Atları ve Zararlı Yazılımlar'dan mağdur olma konusunda **zaman zaman korku yaşıyorum**
3) Virüsler, Truva Atları ve Zararlı Yazılımlar'dan mağdur olma konusunda **genellikle korku yaşıyorum**

10- Banka veya Kredi Kartlarınızın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramanız:

1) Banka veya Kredi Kartlarımın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramak konusunda **hiç korku yaşamıyorum**
2) Banka veya Kredi Kartlarımın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramak konusunda **zaman zaman korku yaşıyorum**
3) Banka veya Kredi Kartlarımın (ya da bunlara ait bilgilerin) Başkalarının Eline Geçmesi veya Sahteciliğinin Yapılması Yoluyla Zarara Uğramak konusunda **genellikle korku yaşıyorum**

11- Kişisel Verilerinizin Rızanız Dışında Hukuka Aykırı Olarak Kaydedilmesi suçunu oluşturan **Casus Yazılımlar** (Keylogger – Klavyeden basılan tüm tuşları kaydeden bir casus yazılım, Screenlogger – Ekranın tamamının ya da bir bölümünün anlık görüntüsünü kaydedebilen bir casus yazılım vb.):

1) Casus Yazılımlar'dan mağdur olma konusunda **hiç korku yaşamıyorum**

2) Casus Yazılımlar'dan mağdur olma konusunda **zaman zaman korku yaşıyorum**
3) Casus Yazılımlar'dan mağdur olma konusunda **genellikle korku yaşıyorum**

12- Kişisel Verilerinizin Rızanız Dışında Hukuka Aykırı Olarak Üçüncü Kişilere Verilmesi, Yayılması ya da Bu Verilerin Üçüncü Kişiler Tarafından Ele Geçirilmesi olarak adlandırılabilecek olan **Kimlik Hırsızlığı**:

1) Kimlik Hırsızlığı'ndan mağdur olma konusunda **hiç korku yaşamıyorum**
2) Kimlik Hırsızlığı'ndan mağdur olma konusunda **zaman zaman korku yaşıyorum**
3) Kimlik Hırsızlığı'ndan mağdur olma konusunda **genellikle korku yaşıyorum**

13- Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerinizin Yok Edilmemesi (Hakkınızda açılan ve takipsizlikle sonuçlanan bir soruşturmada iletişiminizin tespiti ve dinlenmesi sonucu elde edilen ve kanunen yok edilmesi gereken kayıtların yok edilmemesi vb.):

1) Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerimin Yok Edilmemesi konusunda **hiç korku yaşamıyorum**
2) Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerimin Yok Edilmemesi konusunda **zaman zaman korku yaşıyorum**
3) Yasal Süresi Dolmasına Rağmen Yok Edilmesi Gereken Verilerimin Yok Edilmemesi konusunda **genellikle korku yaşıyorum**

14- Siber Zorbalık (Bilgisayar, cep telefonu, vb. elektronik cihazlar vasıtasıyla ısrarcı, tekrar eden ve zarar verici nitelikteki davranışlar; dijital ortamlarda rızanız olmadan fotoğraflarınızın yayınlanması, parolalarınızın ele geçirilmesi, spam içeren ya da bulaşıcı e-postalar almanız, sürekli rahatsız

edilmeniz, alay edilmeniz, hakarete uğramanız, web sitenizin hacklenmesi vb.):

1) Siber Zorbalık'tan mağdur olma konusunda **hiç korku yaşamıyorum**
2) Siber Zorbalık'tan mağdur olma konusunda **zaman zaman korku yaşıyorum**
3) Siber Zorbalık'tan mağdur olma konusunda **genellikle korku yaşıyorum**

15- **Bilişim Sistemleri Aracılığıyla Hakaret** (Sesli, Yazılı veya Görüntülü):

1) Bilişim Sistemleri Aracılığıyla Hakarete Uğramak konusunda **hiç korku yaşamıyorum**
2) Bilişim Sistemleri Aracılığıyla Hakarete Uğramak konusunda **zaman zaman korku yaşıyorum**
3) Bilişim Sistemleri Aracılığıyla Hakarete Uğramak konusunda **genellikle korku yaşıyorum**

16- **Elektronik Haberleşmenizin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi:**

1) Elektronik Haberleşmemin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi konusunda **hiç korku yaşamıyorum**
2) Elektronik Haberleşmemin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi konusunda **zaman zaman korku yaşıyorum**
3) Elektronik Haberleşmemin Gizliliğinin İhlali, Kayda Alınması veya İfşa Edilmesi konusunda **genellikle korku yaşıyorum**

17- Bilişim Sistemleri Aracılığıyla Hırsızlık olarak adlandırılabilecek olan **Siber Hırsızlık** (Banka hesabınızdaki paranın internet bankacılığı parolanız kullanılarak çalınması, vb.):

1) Siber Hırsızlık'tan mağdur olmak konusunda **hiç korku yaşamıyorum**

2) Siber Hırsızlık'tan mağdur olmak konusunda **zaman zaman korku yaşıyorum**
3) Siber Hırsızlık'tan mağdur olmak konusunda **genellikle korku yaşıyorum**

18- Bilişim Sistemleri Aracılığıyla Dolandırıcılık olarak adlandırılabilecek olan **Siber Dolandırıcılık** (Online bir alışveriş sitesinde satılıyor gözüken ancak gerçekte olmayan bir ürünü almak için para ödemenizin sağlanması suretiyle dolandırılmanız, vb.):

1) Siber Dolandırıcılık'tan mağdur olmak konusunda **hiç korku yaşamıyorum**
2) Siber Dolandırıcılık'tan mağdur olmak konusunda **zaman zaman korku yaşıyorum**
3) Siber Dolandırıcılık'tan mağdur olmak konusunda **genellikle korku yaşıyorum**

19- Siber Taciz (Sosyal medya, e-mail vb. yoluyla tacize uğramak):

1) Siber Taciz'den mağdur olmak konusunda **hiç korku yaşamıyorum**
2) Siber Taciz'den mağdur olmak konusunda **zaman zaman korku yaşıyorum**
3) Siber Taciz'den mağdur olmak konusunda **genellikle korku yaşıyorum**

20- Siber Tehdit ve Şantaj (Sosyal medya, e-mail vb. yoluyla tehdit ve/veya şantaja uğramak):

1) Siber Tehdit ve/veya Şantaj'dan mağdur olmak konusunda **hiç korku yaşamıyorum**
2) Siber Tehdit ve/veya Şantaj'dan mağdur olmak konusunda **zaman zaman korku yaşıyorum**

3) Siber Tehdit ve/veya Şantaj'dan mağdur olmak konusunda **genellikle korku yaşıyorum**

21- Bilişim Sistemleri Aracılığıyla İşlenen Nefret ve Ayrımcılık Suçu:

1) Bilişim Sistemleri Aracılığıyla Nefret ve/veya Ayrımcılığa maruz kalmak konusunda **hiç korku yaşamıyorum**
2) Bilişim Sistemleri Aracılığıyla Nefret ve/veya Ayrımcılığa maruz kalmak konusunda **zaman zaman korku yaşıyorum**
3) Bilişim Sistemleri Aracılığıyla Nefret ve/veya Ayrımcılığa maruz kalmak konusunda **genellikle korku yaşıyorum**

22- Siber Terörizm (Örneğin acil yardım, polis, hastaneler ve itfaiyelerin çalışmasının engellenmesi; e-hizmet veren kamu kurumlarının çalışamaz hale getirilmesi; bankacılık, telekomünikasyon, elektrik, su, doğalgaz, ulaşım vb. sistemlerin tahrip edilmesi, vb.):

1) Siber Terörizm'den mağdur olmak konusunda **hiç korku yaşamıyorum**
2) Siber Terörizm'den mağdur olmak konusunda **zaman zaman korku yaşıyorum**
3) Siber Terörizm'den mağdur olmak konusunda **genellikle korku yaşıyorum**

C- GEÇMİŞ SİBER SUÇ MAĞDURİYETİ İLE İLGİLİ SORULAR

23- Son 12 ay içerisinde yukarıda size yöneltilen sorularda yer alan herhangi bir siber suçtan mağdur oldunuz mu?

1) Hayır (Cevabınız hayırsa 25. soruya geçiniz!)
2) Evet (Lütfen hangisi/hangileri olduğunu rakamları ile belirtiniz): …….

3) Yukarıda yazılanlar dışında bir siber suçtan mağdur olmuş iseniz lütfen belirtiniz:

…….

24- Geçmişte yaşamış olduğunuz bu mağduriyet, siber suçlardan mağdur olmamak adına almış olduğunuz önlemlerde herhangi bir değişiklik meydana getirdi mi?

1) Geçmişte de herhangi bir önlem almıyordum, şu anda da almıyorum.
2) Geçmişte herhangi bir önlem almıyordum ama şu anda bazı önlemler alıyorum.
3) Geçmişte bazı önlemler alıyordum ama şu anda daha az önlem alıyorum.
4) Geçmişte bazı önlemler alıyordum, şu anda da aynı önlemleri alıyorum.
5) Geçmişte bazı önlemler alıyordum ama şu anda daha fazla önlem alıyorum.

D- YASAL DÜZENLEMELER VE İŞLEMLERE İLİŞKİN ALGI

25- Türkiye'deki siber suçlara ilişkin yasal düzenlemeleri (kanun, yönetmelik vb.) siber suçlarla mücadele noktasında yeterli buluyor musunuz?

1) Çok Yetersiz Buluyorum
2) Yetersiz Buluyorum
3) Orta Düzeyde Yeterli Buluyorum
4) Yeterli Buluyorum
5) Çok Yeterli Buluyorum

26- Türkiye'deki kolluk birimlerini (Polis, Jandarma vb.) siber suçların önlenmesi ve siber suç faillerinin yakalanabilmesi noktasında yeterli buluyor musunuz?

1) Çok Yetersiz Buluyorum
2) Yetersiz Buluyorum

3) Orta Düzeyde Yeterli Buluyorum
4) Yeterli Buluyorum
5) Çok Yeterli Buluyorum

27- Türkiye'deki yargı birimlerini siber suç faillerinin cezalandırılması noktasında yeterli buluyor musunuz?

1) Çok Yetersiz Buluyorum
2) Yetersiz Buluyorum
3) Orta Düzeyde Yeterli Buluyorum
4) Yeterli Buluyorum
5) Çok Yeterli Buluyorum

28- Türkiye'deki siber suçlara ilişkin yasal düzenlemeler, kolluk birimleri ve yargı işlemlerine ilişkin eklemek istediğiniz görüşleriniz varsa lütfen belirtiniz.

……
……
……
……
……
……
……

E- BAŞA ÇIKMA/ÖNLEM ALMA STRATEJİLERİNE İLİŞKİN SORULAR

29- İnternet üzerinden kişisel ve/veya hassas bilgilerinizi (kimlik bilgileri, kredi/banka kartı bilgileri, adres bilgileri, cep telefonu numarası vb.) kullanarak ne gibi online işlemler gerçekleştiriyorsunuz?

1) Kişisel ve/veya Hassas Bilgilerimi Kullanacağım Hiçbir Online İşlem Gerçekleştirmiyorum
2) İnternet Bankacılığı İşlemleri

3) Online Alışveriş

4) E-devlet İşlemleri

5) E-mail Hesabı İşlemleri

6) ÖSYM, MEB, YÖK vb. Sınav İşlemleri (Başvuru, sonuç öğrenme vb.)

7) Mobil Operatörünüz (Turkcell, Vodafone, Türk Telekom vb.) ile İlgili Online İşlemler

8) Uçak, Otobüs, Tren vb. Online Bilet Rezervasyon, Satın Alma İşlemleri

9) Otel, Pansiyon, Turlar vb. Konaklama, Gezi, Seyahat Rezervasyon İşlemleri

10) Diğer ……..

30- Online işlemlerinizde kullandığınız parolaların zorluk derecesini nasıl tanımlıyorsunuz?

1) Zayıf 2) Orta Derece 3) Güçlü

31- Online işlemlerinizde kullandığınız parolaları ne sıklıkta değiştiriyorsunuz?

1) Değiştirmiyorum
2) Yılda bir
3) 6 ayda bir
4) 3 ayda bir
5) Her ay

32- Farklı online işlemlerinizde kullandığınız parolalarınız birbirlerinden farklı mıdır?

1) Hayır 2) Kısmen 3) Evet

33- E-mail hesaplarınız ya da diğer hassas hesaplarınıza ait parolaları başkalarıyla paylaşıyor musunuz?

1) Hayır 2) Evet

34- Şahsınıza ait sosyal medya hesabınız bulunuyor mu, bulunuyorsa lütfen hangisi/hangileri olduğunu belirtiniz.

1) Sosyal medya hesabım bulunmuyor (36. Soruya Geçiniz!)
2) Facebook
3) Twitter
4) Instagram
5) LinkedIn
6) Google Plus
7) Pinterest
8) Reddit
9) Snapchat
10) Tumblr
11) Slideshare
12) Diğer……

35- Sosyal medya hesaplarınızdaki (Facebook, Twitter, vb.) kişisel bilgi ve verilerinizle ilgili siber suç mağduru olmamak adına ne gibi önlem/önlemler alıyorsunuz?

1) Herhangi bir önlem almıyorum
2) Hesabımı kilitli tutuyorum
3) Paylaşımlarımı görebilecek kişileri sınırlandırıyorum
4) Telefon numaramı hesabıma tanımlıyorum
5) Tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmiyorum
6) Hesabıma benden habersiz erişimleri engellemek için farklı cihazlardan giriş bildirimlerini aktif hale getiriyorum
7) Güvenli gözükmeyen reklam, bağlantı vb. linkleri açmıyorum
8) Diğer ……

LÜTFEN İŞ YERİNİZDE VE İŞ YERİNİZ DIŞINDA KULLANDIĞINIZ ELEKTRONİK CİHAZLAR İÇİN AYRI AYRI CEVAPLANDIRINIZ!	**İş yerinizde kullandığınız elektronik cihazlar**	**İş yeriniz dışında kullandığınız elektronik cihazlar**
36- Cep telefonu, bilgisayar, tablet vb. elektronik cihazlarınıza genellikle kullanıcı parolası koyuyor musunuz?	1) Hayır 2) Evet	1) Hayır 2) Evet
37- Kişisel ve/veya hassas bilgilerinizin ele geçirilmesinden korktuğunuz online işlemlerinizde, güvenilir olduğunu düşündüğünüz bir VPN programı kullanıyor musunuz?	1) Hayır 2) Bazen 3) Evet	1) Hayır 2) Bazen 3) Evet
38- Güvenilir gözükmeyen web sayfalarını ziyaret etmekte bir sakınca görüyor musunuz?	1) Hayır 2) Bazen 3) Evet	1) Hayır 2) Bazen 3) Evet
39- Bilgisayarınızın kamerasını kullanmadığınız zamanlarda üzerini bant, kağıt vb. şeylerle kapalı tutuyor musunuz?	1) Hayır 2) Evet	1) Hayır 2) Evet
40- Tanımadığınız kişilerden gelen ve güvenilir olmadığını düşündüğünüz e-postaları ve/veya e-posta eklerini açıyor musunuz?	1) Hayır 2) Bazen 3) Evet	1) Hayır 2) Bazen 3) Evet
(Online Alışveriş yapmıyorsanız 42. soruya geçiniz!) **41-** Online alışveriş sitelerinden yaptığınız alışverişlerde adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin "https://" ile başlamasına dikkat ediyor musunuz?	1) Hayır 2) Nadiren 3) Bazı zamanlar 4) Çoğu zaman 5) Her zaman	1) Hayır 2) Nadiren 3) Bazı zamanlar 4) Çoğu zaman 5) Her zaman

(İnternet Bankacılığı hizmetlerini kullanmıyorsanız 43. soruya geçiniz!) **42-** İnternet Bankacılığı hizmetlerini kullanırken adres çubuğunda güvenli olduğunu gösteren asma kilit bulunmasına ve adresin "https://" ile başlamasına dikkat ediyor musunuz?	1) Hayır 2) Nadiren 3) Bazı zamanlar 4) Çoğu zaman 5) Her zaman	1) Hayır 2) Nadiren 3) Bazı zamanlar 4) Çoğu zaman 5) Her zaman
43- Bilgisayar, cep telefonu, tablet vb. elektronik cihazlarınızdaki verilerinizi silinme, çalınma vb. durumlara karşı yedekliyor musunuz?	1) Hayır 2) Evet	1) Hayır 2) Evet
44- Kullanmakta olduğunuz bilgisayarda güncel durumda bulanan ve güvenilir bir *Anti-virüs* yazılımı bulunuyor mu?	1) Hayır 2) Evet	1) Hayır 2) Evet
45- Kullanmakta olduğunuz bilgisayarda güncel durumda bulunan ve güvenilir bir *Anti Malware* yazılımı bulunuyor mu?	1) Hayır 2) Evet	1) Hayır 2) Evet
46- Kullanmakta olduğunuz bilgisayar, cep telefonu, tablet vb. elektronik cihazların işletim sistemlerinin (Windows, OS, Android, iOS vb.) güncel durumda olmalarına dikkat ediyor musunuz?	1) Hayır 2) Evet	1) Hayır 2) Evet
47- Kullanmakta olduğunuz bilgisayarda açık durumda olan bir *Güvenlik Duvarı* (Windows güvenlik duvarı vb.) bulunuyor mu?	1) Hayır 2) Evet	1) Hayır 2) Evet

48- Siber suçlardan mağdur olmamak adına almış olduğunuz farklı önlemler/stratejiler varsa lütfen belirtiniz.

1- ……
……

……
……

2- ……
……
……
……
……

3- ……
……
……
……
……

4- ……
……
……
……
……

5- ……
……
……
……
……

F- ALINAN ÖNLEMLERİN YETERLİ BULUNUP BULUNMADIĞI

49- Siber suçlardan mağdur olmamak adına almış olduğunuz önlemleri yeterli buluyor musunuz?

1) Çok Yetersiz Buluyorum
2) Yetersiz Buluyorum
3) Orta Düzeyde Yeterli Buluyorum
4) Yeterli Buluyorum
5) Çok Yeterli Buluyorum

EK 2: ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYOLOJİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 11/07/2018

Tez Başlığı : Siber Suç Korkusu ve Önlem Alma Stratejileri: Ankara'daki Teknokentler Örneği

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 183 sayfalık kısmına ilişkin, 11/07/2018 tarihinde ~~şahsım~~/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 9 'dur.

Uygulanan filtrelemeler:

1- ☒ Kabul/Onay ve Bildirim sayfaları hariç
2- ☐ Kaynakça hariç
3- ☐ Alıntılar hariç
4- ☒ Alıntılar dâhil
5- ☐ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

11.07.2018
Tarih ve İmza

Adı Soyadı: Yunus YILMAZ
Öğrenci No: N14229162
Anabilim Dalı: Sosyoloji
Programı: Tezli Yüksek Lisans

DANIŞMAN ONAYI

UYGUNDUR.

Doç. Dr. Ayça GELGEÇ BAKACAK
(Unvan, Ad Soyad, İmza)

EK 3: ETİK KOMİSYON ONAYI

T.C.
HACETTEPE ÜNİVERSİTESİ
Rektörlük

29 Haziran 2017

Sayı : 35853172/ 433-2315

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Enstitünüz Sosyoloji Anabilim Dalı yüksek lisans programı öğrencisi **Yunus YILMAZ**'ın **Doç. Dr. Ayça GELGEÇ BAKACAK** danışmanlığında yürüttüğü **"Siber Suç Korkusu ve Başa Çıkma Stratejileri: Ankara'daki Teknokentler Örneği"** başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun **20 Haziran 2017** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Rahime M. NOHUTCU
Rektör a.
Rektör Yardımcısı

"Öğrenci İşlerine Yazışmasını Yapalım 03-07-2017"

Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
Telefon: 0 (312) 305 3001 - 3002 • Faks: 0 (312) 311 9992
E-posta: yazimd@hacettepe.edu.tr • www.hacettepe.edu.tr

Ayrıntılı Bilgi için:
Yazı İşleri Müdürlüğü
0 (312) 305 1008