T.C.

İSTANBUL ÜNİVERSİTESİ-CERRAHPAŞA

ADLİ TIP VE ADLİ BİLİMLER ENSTİTÜSÜ

Danışman

Dr. Öğr. Üyesi Y. Tunç Demircan

BİLİŞİM SEKTÖRÜ ÇALIŞANLARI VE MUHAKEME SÜJELERİNDE BİLİŞİM SUÇU FARKINDALIĞI

SOSYAL BİLİMLER ANABİLİM DALI

DOKTORA TEZİ

Av. ELİF YORGANCIOĞLU

İSTANBUL, 2022

BİLİŞİM SEKTÖRÜ ÇALIŞANLARI VE MUHAKEME SÜJELERİNDE BİLİŞİM SUÇU FARKINDALIĞI

ÖZET

Teknolojik değişimler bilişim suçlarının işleniş artışını hızlandırmış ve bilişim suçlarını çeşitlendirmiştir. Bilişim suçlarının hukuk düzenindeki karşılıkları ve kişilerin suça yol açabilecek problemli internet kullanım davranışları siber psikoloji ile bilişim ve teknoloji hukuku tarafından incelenmeye devam edilmektedir. Bu çalışmanın amacı bilişim sektörü çalışanları ile hâkim, savcı ve avukatların problemli internet kullanım davranışları ve siber güvenlik ile ilgili tutumlarının belirlenerek, bilişim hukuku ve adli bilimler tarafından değerlendirilmesidir. Araştırmanın örneklemi Türkiye'de yaşayan bilişim sektörü çalışanları ve hâkim/savcı/avukatlardır. Araştırmada Kişisel Bilgi Formu, Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu, Problemli İnternet Kullanımı Ölçeği (PİKÖ), Kişisel Siber Güvenliği Sağlama Ölçeği (KSGS) kullanılmıştır. Araştırmanın örneklem grubunu oluşturan 500 kişinin %54'ü avukat, hâkim, savcı, %46'sı bilişim sektörü çalışanıdır. Katılımcıların sorulara verdikleri cevapların ölçeklere göre değişip değişmediği bağımsız örneklemler t testi ve Mann Whitney-U testi kullanılarak incelenmiştir. PİKÖ ve KSGS ölçekleri arasındaki ilişki; veriler normal dağıldığı koşullarda Pearson(p) korelasyon analizi, veriler normal dağılmadığı şartlarda ise Spearman(s) korelasyon katsayısı analizi kullanılarak incelenmiştir. Araştırmada; PİKÖ Aşırı Kullanım ortalamalarına göre hukukçuların Aşırı Kullanım Ortalamalarının bilişim sektörü çalışanlarından daha fazla, bilişim sektörü çalışanlarının KSGS Önlem Alma, Ödeme Bilgilerini Koruma, İz Bırakmama puan ve ortalamalarının hukukçulardan fazla olduğu görülmüştür. İnternette günde 4 saatten fazla zaman geçiren bireylerin internetin aşırı kullanım ile internetin olumsuz sonuçlarını daha fazla deneyimlediği belirlenmiştir. Katılımcıların, %59.6'sı lisanssız yazılım kullanmanın suç olduğunu düşünmesine rağmen, %62'lik kullanım oranıyla, katılımcıların lisansız yazılım

kullanma eğilimleri olduğu belirlenmiştir. Katılımcıların %71,2'sinin ise erişime engelli sitelere çeşitli yöntemlerle girdiği belirlenmiştir. Yapılan çalışmalarda; bireylerin günlük hayata kıyasla siber alanda, daha değişken ve mobil bir ortamda olmalarından ötürü daha hızlı karar vermek durumunda olmalarının, onları dijital iletişim ve etkileşimde hatalı davranışlara kolaylıkla itebilmesine, hatta bu hatalı davranışların bireyi çoğu zaman suçun faili ve mağduru konumuna getirebileceği ifade edilmektedir. Siber kimlik kuramından siber suçlara bakıldığında, siber uzamda suça maruz kalmak bir siber travmaya neden olabilmekte siber travmalar da siber dissosiyasyona yol açabilmektedir. Rutin aktiviteler teorisi bağlamında motive olmuş suçlu uygun hedef ve koruyucuların yokluğu unsurlarının siber suçları açıklamaya yardımcı olduğu belirlenmiştir. Çalışmamızda elde edilen bulguların, bilişim ve hukuk alanında faaliyet gösteren meslek grupları özelinde, problemli internet kullanım davranışları ile siber güvenlik ile ilgili tutumlara ve bu alanda yapılacak çalışmalara ışık tutacağı düşünülmektedir.

Anahtar Kelimeler: Bilişim; siber suç; avukat; hakim; savcı; bilişim hukuku; bilişim suçu farkındalığı; siber psikoloji; siber dissosiyasyon.

AWARENESS OF CYBERCRIME AMONG IT SECTOR EMPLOYEES AND CRİMİNAL PROCEDURE AGENTS

ABSTRACT

Technological changes have accelerated and diversified the increase in the commission of cybercrimes. The legal definitions of cybercrimes and problematic internet usage behaviors of individuals that may lead to crime continue to be examined by cyber psychology and IT law. The aim of this study is to determine the problematic internet usage behaviors and cyber security attitudes of IT sector employees, judges, prosecutors and lawyers and to evaluate them within the framework of IT law and forensic sciences. The sample of the study consists of IT sector employees and judges/prosecutors/attornies at law living in Turkey.In this research Personal Information Form, Questionnaire for Legal Awareness of Cybercrime Regulations, Problematic Internet Utilization Scale (PİKÖ), Ensuring Personal Cybersecurity Scale (KSGS) used. 54% of 500 people constituting the sample of research are legists, 46% are IT employees. Whether the answers given by the participants changed according to the scales was examined using the independent sample t test and the Mann Whitney-U test. The relationship between the PIKÖ and KSGS scales was analyzed by correlation analysis using Pearson (p) and Spearman (s) correlation. In the research according to PİKÖ Over-Use averages, it is observed that average of Over-Use of legists is higher than IT employees, scores for KSGS Precautionary Measures, Payment Information Protection, Leave no Trace indicators of IT employees are higher than legists. Individuals spending more than 4 hours a day on internet have higher PİKÖ overuse and negative results compared to individuals spending less time. Although %59.6 of the participants think using unlicensed software is a crime, it has been determined that unlicensed software usage ratio is %62. It's found that 71.2% of participants accessed blocked sites using various methods. In the researches that are conducted, it is stated that the fact that individuals have to make faster decisions in cyberspace compared to daily life due to being in

a more variable and mobile environment, can easily push them to erroneous behaviors in digital communication and interaction, and even these erroneous behaviors can often make the individual the perpetrator and victim of crime. From the perspective of cyber identity theory, exposure to crime in cyberspace can lead to cyber trauma. Cyber traumas can also lead to cyber dissociation. From the perspective of routine activities theory, the elements of crime; motivated offender, appropriate target and protectors help to explain cybercrime. It is thought that the findings obtained in our study will shed light on problematic internet use behaviors and attitudes towards cyber security and the studies to be conducted in this field, specific to the professional groups operating in the field of IT and law.

Keywords: IT; cybercrime; lawyer; jugde; prosecutor; IT law; awareness of cybercrime; cyber dissociation; cyber psychology.

ÖNSÖZ

Tez yazım sürecinde her sorunum karşısında çözüm üreten ve desteğini hiçbir zaman esirgemeyen değerli Danışmanım Dr.Öğr.Üyesi Tunç Demircan'a

Öğrenciliğim ve tez yazım sürecimde sabırla öğrettikleri, akademik ve insani ilhamı, eşsiz nezaketi için kıymetli Hocam Prof. Dr. Erdinç Öztürk'e,

Eleştiri ve önerileri için değerli Hocam Dr. Öğr. Üyesi Mustafa Okudan'a

Sorularımı hiçbir zaman yanıtsız bırakmayan ve süreçteki kaygımı yatıştıran değerli Hocam Doç. Dr. Can Çalıcı'ya,

Yolumu açan değerli dostum Dr. Nergis Kulaksızoğlu Mercan'a, sıkılmadan her telefonuma yanıt veren, her aşamada yazım sürecime destek veren kıymetli arkadaşım Ar. Gör. M.Emin Yıldız'a,

Veri analizindeki desteği için Begüm Çiğsar'a

Sabırları ve destekleri için Hatice ve Melih Onural'a, varlıklarıyla her zaman desteklerini hissettiğim Ezgi ve Hakan Özdemir'e,

Her zaman bana benden çok inan annem Saadet ve babam Sabri Yorgancıoğlu'na,

Sabrı, ilgisi, desteği ve yoldaşlığı için eşim Doğu Dost Onural'a ve beni sabırla bekleyen biricik kızım İda'ya

Teşekkürü borç bilirim.

Av. Elif Yorgancıoğlu

İÇİNDEKİLER

ÖZET i
ABSTRACT iii
ÖNSÖZ v
İÇİNDEKİLER vi
TABLOLAR VE ŞEKİLLER LİSTESİ ix
KISALTMALAR x
1. GİRİŞ VE AMAÇ 1
2. GENEL BİLGİLER 8
2.1. Siber Suç 8
2.1.1. Siber Suç Kavramı ve Tanımlanması 8
2.1.2. Siber Suç Türleri (Sınıflandırması) 12
2.1.2.1. Bilgisayar Veri veya Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanılabilirliğine İlişkin Suçlar 14
2.1.2.1.1. Yasadışı erişim 14
2.1.2.1.2. Yasadışı müdahale 15
2.1.2.1.3. Verilere müdahale 17
2.1.2.1.4. Sisteme müdahale 17
2.1.2.1.5. Cihazların kötüye kullanımı 18
2.1.2.2. Bilgisayarlarla bağlantılı suçlar 19
2.1.2.2.1. Bilgisayarla bağlantılı sahtecilik 19
2.1.2.2.2. Bilgisayarla bağlantılı dolandırıcılık 20
2.1.2.3. İçerikle bağlantılı suçlar 21
2.1.2.3.1. Çocuk pornografisiyle bağlantılı suçlar 21
2.1.2.4. Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar 22
2.1.3. Siber Suçların İşlenme Biçimleri 23
2.1.3.1. Zararlı yazılımlar/kötü amaçlı yazılımlar 23
2.1.3.1.1. Virüsler 23
2.1.3.1.2. Solucanlar 24
2.1.3.1.3. Truva atı 24
2.1.3.1.4. Arka kapılar 25
2.1.3.1.5. Fidye yazılımları 25
2.1.3.1.6. Korsan amaçlı kullanılan yazılımlar 26

2.1.3.1.7. Robotlar 26
2.1.3.1.8. Casus yazılımlar 26
2.1.3.2. Dos-DDoS saldırıları 27
2.1.3.3. Oltalama 27
2.1.3.4. İstem dışı alınan elektronik postalar 27
2.2. Türk Hukukunda Bilişim Suçları 28
2.2.1. TCK'nın Bilişim Alanında Suçlar Bölümünde Düzenlenen Suçlar (Doğrudan) 28
2.2.1.1. Bilişim sistemine girme (m.243) 28
2.2.1.2. Sistemi engelleme, bozma verileri yok etme veya değiştirme (m.244) 29
2.2.1.3. Banka veya kredi kartlarının kötüye kullanılması (m.245) 29
2.2.1.4. Yasak cihaz veya programlar 30
2.2.1.5. Tüzel kişiler hakkında güvenlik tedbiri uygulanması 30
2.2.2. Bilişim Sistemleri Aracılığıyla İşlenebilen Suçlar (Dolaylı) 30
2.2.2.1. TCK'da yer alan bilişim suçu dolaylı düzenlemeleri 31
2.2.2.1.1. Bilişim sistemlerinin kullanılması suretiyle hırsızlık 31
2.2.2.1.2. Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık 31
2.2.2.1.3. Haberleşmenin gizliliğini ihlal 31
2.2.2.1.4. Kişiler arası konuşmaların dinlenilmesi kayda alınması 32
2.2.2.1.5. Kişisel verilerin hukuka aykırı ele geçirilmesi, kaydedilmesi 33
2.2.3. Fikir ve Sanat Eserleri Kanunu Düzenlemeleri 34
2.2.4. 5651 Sayılı Kanun Düzenlemeleri 35
2.2.5. Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (Dezenformasyon Yasası) 38
2.2.6. Elektronik İmza Kanunu Düzenlemeleri 40
2.3. Siber Suçlarla İlgili Uluslararası Düzenlemeler 40
2.3.1. Siber Suçlarla Mücadelede Devletlerin İşbirliğini Düzenleyen Mevcut Bölgesel Anlaşmalar 40
2.3.1.1. Avrupa konseyi siber suçlar sözleşmesi 41
2.3.1.2. Diğer bölgesel anlaşmalar 42
2.4. Regülasyon Kurumu Olarak Bilgi Teknolojileri İletişim Kurumu 42

2.4.1. Yapısı ve Görevleri 42
2.4.2. BTK'nın Ulusal Siber Olaylara Müdahale Merkezi (USOM) 43
2.4.3. BTK'nın Abone Verisi Toplama İşlemleri 44
2.5. Araştırmanın Katılımcıları Muhakame Süjeleri ve Bilişim Sektörü Çalışanlarına İlişkin Tanımlamalar 45
2.5.1. Hakim, Savcı ve Avukat 45
2.5.2. Bilişim Sektörü Çalışanı 46
2.6. Siber Psikoloji ve Siber Suçlarla İlişkili Temel Kavramları 48
2.7. Siber Suçların Değerlendirmesinde Rutin Aktiviteler Teorisi 50
3. GEREÇ VE YÖNTEM 54
3.1. Araştırmanın Modeli ve Deseni 54
3.2. Evren ve Örneklem 54
3.3. Veri Toplama Araçları 54
3.4. Araştırma Prosedürü 56
3.5. İstatistiksel Analiz 56
4. BULGULAR 57
4.1. Ölçekler Arasındaki İlişki 57
4.2. Mesleklere Göre Analizler 59
4.2.1. Mesleklerle Demografik Değişkenler Arasındaki İlişki 59
4.3. Bilişim Sektörü Çalışanları ve Hukukçular İçin Analizler 64
4.3.1. Cinsiyetler Arasında Ölçeklere Göre Karşılaştırma 65
4.3.2. Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma 66
4.3.3. Anti-Virüs Programı Kullanım Durumlarını Ölçeklere Göre Karşılaştırma 68
4.3.4. İnternette Geçirilen Süreler Arasında Ölçeklere Göre Karşılaştırma 69
4.3.5. Lisanssız Yazılım Kullanım Durumlarını Ölçeklere Göre Karşılaştırma 70
4.4. Siber Mağduriyete İlişkin Analizler 71
4.5. Bilişim Suçu Hukuki Farkındalığına İlişkin Bulgular 73
5. TARTIŞMA 76
6. SONUÇ VE ÖNERİLER 88
7. KAYNAKLAR 90
8. EKLER 106
EK 1 106
9. ÖZGEÇMİŞ 115

TABLOLAR VE ŞEKİLLER LİSTESİ

Tablo I. Ölçekler Arasındaki İlişki 57
Tablo II. Katılımcıların Mesleklerine Göre Demografik Özellikleri 59
Tablo III. İnternete Bağlanılan Yere İlişkin Tablo 61
Tablo IV. Katılımcıların Bilgisayarlarında Kullandığı İşletim Sistemi 61
Tablo V. Katılımcıların Akıllı Telefonlarında Kullandığı İşletim Sistemi 62
Tablo VI. Katılımcıların Akıllı Telefonlarında Kullandığı Uygulamalar 62
Tablo VII. Sosyal Medya Platformları Kullanım Oranları 63
Tablo VIII. Ölçeklerin Mesleklere Göre Karşılaştırılması 63
Tablo IX. Bilişim Sektörü Çalışanlarında Cinsiyetler Arasında Ölçeklere Göre Karşılaştırma 65
Tablo X. Hukukçular İçin Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma 66
Tablo XI. Bilişim Sektörü Çalışanları İçin Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma 67
Tablo XII. Bilişim Sektörü Çalışanları Ve Hukukçular Arasında Anti Virüs Programı Kullanımı Durumunun Karşılaştırılması 68
Tablo XIII. Hukukçularda ve Bilişim Sektörü Çalışanlarında İnternette Geçirilen Süreler Arasında Ölçeklere Göre Karşılaştırma 69
Tablo XIV. Hukukçularda Ve Bilişim Sektörü Çalışanlarında Lisanssız Yazılım Kullanım Durumlarını Ölçeklere Göre Karşılaştırma 70
Tablo XV. Katılımcıların Uğradığı Siber Mağduriyet Türleri Tablosu 72
Tablo XVI. Siber Mağduriyet Bildiren Katılımcılara İlişkin Tablo 72
Tablo XVII. Siber Mağduriyete Uğrayanlar İle Uğramayanlar Arasında Ölçekler Açısından Farklılık Olup Olmadığının Tespitine İlişkin Tablo 73
Tablo XVIII. BSF Formunun Bilişim ve Hukuk Sektöründeki Dağılımı 73

KISALTMALAR

AİHS	: Avrupa İnsan Hakları Sözleşmesi
ASSS	: Avrupa Konseyi Siber Suç Sözleşmesi
AYM	: Anayasa Mahkemesi
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CMK	: Ceza Muhakemesi Kanunu
COE	: Counsil of Europe
EHK	: Elektronik Haberleşme Kanunu
IoT	: Internet of Things
ISS	: İnternet Servis Sağlayıcı
ITU	: International Telecommunication Union
KSGS	: Kişisel Siber Güvenliği Sağlama Ölçeği
KVKK	: Kişisel Verilerin Korunması Kanunu
PİKÖ	: Problemli İnternet Kullanımı Ölçeği
SOME	: Siber Olaylara Müdahale Ekibi
STH	: Sabit Telefon Hizmeti
TCK	: Türk Ceza Kanunu
USOM	: Ulusal Siber Olaylara Müdahale Merkezi
5651 sayılı Kanun	: İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun

1. GİRİŞ VE AMAÇ

Bilgisayar ve iletişim teknolojilerindeki gelişmeler günümüzde insanlık tarihi açısından önemli bir dönüm noktası olarak kabul edilmektedir. Diğer bir deyişle, teknoloji dünyayı değiştiren tarihsel bir unsurdur. Her geçen gün bilgisayarlar ve bilgisayarlı sistemlerin depoladığı ve işlediği veriler artış göstermekte, insanların internet üzerinde gerçekleştirdiği aktivitelerle sanal dünyadaki nüfus gün geçtikçe artmaktadır. (Dijle ve Doğan, 2011) İnternete erişimi "temel bir insan hakkı" olarak tanıyan yeni Dünyada, internete erişim arttıkça İnternet-bilgisayar üzerinde işlenen suçlarda artmakta ve çeşitlenmektedir.

Bu suçları tanımlamak için günümüze kadar, "bilgisayar suçu", "bilgisayar bağlantılı suç", "internet suçları" "yüksek teknoloji suçları" "bilgi çağı suçları", "net suçları", "siber suç", "dijital suç" gibi kavramlar kullanılmıştır. Hâlâ hiçbir terimin gerçekten yaygın hale gelmemiş olmasına ve birçoğunun birbirinin yerine kullanılmasına rağmen, 'siber suç' kavramı görece olarak diğerlerine göre literatürde daha çok kullanılmaktadır. (Clough, 2015) Birçok araştırmacı siber suç kavramının geniş anlamı temsil edecek şekilde kullanılması gerekliliğini önermekle, Uluslararası Telekomünikasyon Birliği, hukuki bir terim olarak kullanılmadığı sürece "siber suç"un tek bir tanımının olmamasının önemli olmadığına vurgu yapmaktadır. (ITU, 2011)

Gordon ve Ford, siber suçu "bir bilgisayar, ağ veya donanım aygıtı kullanılarak kolaylaştırılan veya işlenen herhangi bir suç" olarak tanımlamıştır. (Gordon ve Ford, 2006) Clough, ise dijital teknolojilerin kullanımı yoluyla veya bunlara karşı işlenen her türlü yasaklanmış davranışı kapsayacak şekilde "siber suç" terimini kullanmayı tercih ettiğini ifade etmektedir. (Clough, 2015) Li'nin tanımına göre; siber suç, "kitle iletişim araçları, işletim mekanizması, oluşum yeri, aktarım kanalı, hedeflenen nesne, çok amaçlı araç olarak kullanılan veya diğer suçların hazırlanmasında kullanılan veri işleme sistemlerini içeren bir tür geleneksel veya geleneksel olmayan suç biçimidir." (Li, 2016) Literatürde en yaygın şekilde kullanılan

terim “cybercrime” (siber suç) olup tez çalışmamızda siber suç, bilişim suçu anlamında kullanılmaktadır.

1960’larda çok sayıda kişi ve işletme aynı bilgisayarı kullandığından, üzerinde depolanan veriler, programlar korunmasızdı ve bilgisayar korsanlığının kapıları da ilk kez bu yıllarda aralanmaya başlanmıştır. (Shinder ve Tittel, 2002). 1980'lerde ise Federal Bureau of Investigation (FBI) bilgisayar korsanlarının ilk yüksek profilli tutuklamalarından bazılarını yapmıştır. 1990’larda kişisel bilgisayarlar gittikçe artmış ve bu tarihten itibaren siber suçlar hızlı bir küreselleşme sürecine girmiştir. (Li, 2017) 2000’lerin başı ise siber suçların rutinleştiği ve yasal boşluğun birçok ülke yönünden doldurulmaya başlandığı yıllar olmuştur. (Li, 2017) Bununla birlikte 2000’li yıllarla birlikte, endüstri 4.0 olarak kabul edilen, endüstri devriminin dördüncü aşaması bir dijital dönüşüm dalgasını başlatmıştır. (Yankin FB, 2018) Bu dönüşüm nesnelerin interneti kullanımını hızla arttırmış, ev içinde ve yaşamın her alanında birçok cihaz internete bağlanmıştır. Bu dönüşüm süreci içerisinde her yeni teknolojik gelişme yeni güvenlik açıkları da meydana getirmiştir. Nesnelerin interneti kullanımı (Internet of Things) [IoT] olan birçok cihazın tasarımdan kaynaklanan güvenlik açıkları olabileceği çünkü bu cihazların birçoğunun aslında hedeflenen işlevselliğini sağlamaya odaklanarak kısıtlı bütçeyle tasarlandığı ifade edilmiştir. Bu yüzden de bu cihazlarda siber güvenlik konusuna çok az önem verildiği ifade olunmuştur. (European Commission, 2020)

Bugüne gelindiğinde siber suçların maliyetinin oldukça yüksek olduğu tespit edilmektedir. Detica’nın 2011 yılında yayınladığı raporda siber suçların Birleşik Krallık'a maliyetinin 27 milyar doları bulduğu ifade edilmiştir. (Detica Report, 2011) 2020 tarihinde yayımlanan bir siber güvenlik raporunda siber suçların maliyetinin, kısmen COVID-19 pandemisinin siber suçlular tarafından bir fırsat olarak kullanılması nedeniyle, 2015'te 2,7 trilyon Euro’dan 2020'nin sonunda 5,5 trilyon Euro'ya çıkacağının tahmin edildiği ifade edilmiştir. (European Commission, 2020) Raporda bu rakamın, tarihteki en büyük ekonomik

servet transferini temsil ettiği ve siber suçların neredeyse tüm büyük yasadışı uyuşturucuların küresel ticaretinden daha fazla kar getiren bir suç türü olduğu ifade edilmiştir. (European Commission, 2020) Trend Micro 2021 yılında dünya genelinde engellediği saldırıları sayısının 94 milyardan fazla olduğunu açıklamıştır.(Trend Micro, 2021) Trend Micro, 2022'nin ilk yarısında engellenen toplam tehdit sayısını ise 63 milyardan fazla olarak açıklanmıştır. (Trend Micro, 2022) Bu rakamlar riskin büyüklüğünü gözler önüne sermektedir.

2020 tarihinde yayımlanan siber güvenlik raporunda, gün geçtikçe siber saldırganların daha karmaşık saldırı araçları kullandığı; özellikle, kötü amaçlı yazılımların kullanımında sürekli bir artış olduğu ve son beş yılda en sık kullanılan saldırı aracı haline geldiği tespiti yer almıştır. (European Commission, 2020) Avrupa Komisyonu'nun yayımladığı verilere göre, her gün ortalama 10 yeni virüs keşfedilmektedir. (Avrupa Komisyonu, 2006) Suç trendlerine yönelik çalışmalarda da sokak suçlarında gözlemlenen düşüşte, siber uzamda suç işleyenlerin kriminal aktivitelerini kendilerine ciddi avantaj sağlayan çevrimiçi ortamlara yönelttiği, bu sayede de suç oranlarında azalma yaşandığı savunulmakla birlikte siber suçların artışına ilişkin verilerin de bu iddiayı güçlendirdiği ifade olunmaktadır. (Çalıcı, 2019)

Uluslararası teknoloji danışmanlık firması Detica tarafından gerçekleştirilen bir çalışmada, sanal ortamda işlenen suçların yüzde 80'lik bir bölümü koordineli bir şekilde gerçekleştiği tespit edilmiştir. (Detica Report, 2011) Detica'nın yayınladığı rapora göre dijital suçun % 5'i "geleneksel" olarak nitelendirilen suç örgütlerince gerçekleştirilmektedir. (Detica Report, 2011)

Siber suç aynı zamanda bir endüstri de doğurmuştur. Siber suç konusunun kendisi, gelişmekte olan, tutarlı bir ekonomik varlık olarak son zamanlarda gündeme gelmektedir. Bilinen diğer tüm endüstriyel sektörler gibi, küresel siber suç endüstrisinin de satıcıları (siber suç faaliyetlerini yürütmek için araçlar olan donanım ve yazılımları oluşturanlar), alıcıları (siber

suç faaliyetlerini fiilen yürütmek amacıyla bu tür donanım ve yazılımları satın alan kişiler ve ülkeler) ve dağıtım sistemleri vardır. (Sanford, 2016)

İnternetin dünyadaki en geniş iletişim ağı olması ve internetin mülkiyetinin kimseye ait olamayacağı gerçeği (Akdeniz ve Altıparmak, 2008) bağlamında internet üzerinden haberleşme, ifade özgürlüğü gibi temel hak ve özgürlüklerin korunması ile suç tanımlaması, suçlunun tespiti, suçun işlenmesinin önlenmesi arasındaki denge sıklıkla tartışmaların konusu olmaktadır. Özellikle Türkiye'de internet erişiminin engellenmesine konu olaylarda (AYM, 2014e) uygulanan tedbirlerin yerindeliği, şekli ve orantılılığı sıklıkla tartışılmış ve davaların konusu olmuştur. Erişim engelleme kararlarının uygulanmasında rol alan Erişim Sağlayıcılar Birliği (ESB) gibi otoriteler bazı sorunların çözümü için bir adım olarak değerlendirilse de birliğin kuruluş aşaması Anayasa Mahkemesi (AYM) ve Danıştay önüne taşınmıştır. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (5651 sayılı Kanun) 2007 yılında yürürlüğe girmiş ama 2007 yılından bu yana 2008, 2013, 2014, 2015, 2016, 2018, 2019, 2020, 2021, 2022 yıllarında olmak üzere birçok kez değişikliğe uğramıştır. Bu değişikliklerin de konusu olan Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) 5651 Kanun'un uygulamasından doğan hak ve yükümlülükleri de önemli bir inceleme alanını oluşturmaktadır. BTK'nın abone verilerini toplama ve saklama biçim ve yöntemlerinin kişisel verilerin korunması hakkına müdahale niteliğinde olup olmadığı da bu tezde değerlendirilecektir. Sosyal medya kullanıcılarının kişisel verilerin veri sahiplerinin rızası olmaksızın kullanılması konusu da siber suçlar kapsamında tartışılmaktadır. Facebook'un milyonlarca kullanıcısının verilerini başka şirketlere sattığı iddiası üzerine Facebook hakkında ABD'de dava açılmıştır.(Facebook'a Cambridge Analytica Davası, 2018)

Covid-19 pandemisi dijital dönüşümün hızı ve ölçeğini değiştirdiği gibi siber suçların hedeflerini de etkilemiştir. Pandemi nedeniyle zor koşullarda çalışan sağlık kuruluşları, 2021'de

fidye yazılımı saldırılarından çok etkilenmiş ve bankacılık ve devlet kurumlarından sonra en çok fidye yazılım tehdidinden etkilenen üçüncü sektör olmuştur. (Trend Micro, 2021) Sağlık kuruluşları birçok hastanın hassas nitelikteki kişisel verisini barındırdığından siber saldırganlar için birer veri hazinesi olarak değerlendirilmiştir. (Trend Micro, 2021) Rapor'da 2020 yılına kıyasen engellenen kötü amaçlı yazılımlarda %382'lik bir artış olduğu tespit edildiği ifade edilmiştir (Trend Micro, 2021). Ülkemizdeki Bilgi Teknolojileri İletişim Kurumu'nun (BTK) siber güvenlik uygulamaları, Ulusal Siber Olaylara Müdahale Merkezi (USOM), güvenli internet uygulaması da bu çalışma kapsamında incelenecektir.

Lisanssız yazılım kullanımı da bilişim suçları kapsamında ele alınan bir başka konudur. Yazılım, 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) uyarınca ilim ve edebiyat eseri kategorisinde eser olarak tanımlanmaktadır (FESK md. 2). FESK ilgili maddeler yönünden "özel ceza yasası" niteliği taşımaktadır. Lisanssız yazılım kullanmak, FSEK m. 22/3'te özel olarak düzenlenen, eser sahibinin "çoğaltma hakkı"nın ihlali niteliğinde olduğundan, FSEK m. 71 uyarınca suçtur. Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Konvansiyonu) uyarınca lisansız yazılım kullanmak da telif haklarının ihlali kategorisinde bir siber suç çeşididir. BSA'nın 2016 yılında yayımladığı raporda, Dünya yıllara göre lisanssız yazılım indirme oranları ortalaması 2015 yılında %39, 2013 yılında %49, 2011 yılında %42, 2009 yılında %43 iken Türkiye'de yıllara göre lisanssız yazılım indirme oranları 2015 yılında %58, 2013 yılında %60, 2011 yılında %62, 2009 yılında %63'tür. (BSA, 2016) Türkiye'de lisanssız yazılım kullanım oranlarının Dünya ortalamasının oldukça üzerinde olduğu görülmektedir.

Toplumsal değişimler tarihte hiçbir zaman bugünkü kadar hızlı olmamıştır. Değişim öylesine hızlıdır ki insanlık bu durumun sosyolojik, psikolojik etkileriyle başa çıkmaya çalışırken hukuk düzenini de bu değişime uydurmak zorundadır. Hukuk, her zaman yasal kavramları ve yasal çerçeveyi etkilemeye çalışan sosyal değişimlere hızlı şekilde cevap vermelidir. Bilişim teknolojilerinin sürekli gelişmesi karşısında suçların farklı araçlarla

işlenmesi noktasında suçlunun tespiti, uygulayıcıların bilgi eksikliği ve yasaların güncel olmaması sebepleri ile ciddi sorunlara yol açmıştır. 1990'lı yıllarda internet üzerinden yapılan yayınlarda suç isnadının yanlış kimselere yapılması yargılamalarda birçok karmaşaya sebep olmuştur. Bugün bile erişim sağlayıcı, içerik sağlayıcı, yer sağlayıcı kavramlarının yasa uygulayıcıları tarafından açık şekilde bilinmiyor oluşu ve veri merkezi işletmeciliğinin yasal sorumluluğu mevzuatımızda açıkça tanımlanmamış olması, soruşturma ve kovuşturma aşamalarında çeşitli karışıklıklara neden olmaktadır. Teknolojik gelişmeler karşısında hukukun güncelliğinin yakalanamaması esasen suç olarak tanımlanması gerekli olan bir eylemin suç olarak tanımlanmamasından, kusur izafe edilemeyecek kimselerin suçlu sayılmasından, devletin vergi gelirinden mahrum kalmasına kadar uzanan geniş bir yelpazede olumsuz sonuçlar doğurabilmektedir. (Çobansoy ve Hızel, 2019) Türk Ceza Kanunu'nun 10. Bölümünde "Bilişim alanında suçlar" düzenlenmiştir. 2021 yılında TCK'nın bilişim alanında suçlar bölümünde düzenlen suçlara ilişkin toplamda 123.245 karar verilmiştir. Bunların 19.947 tanesi kamu davası açılmıştır. (Kaya, 2022) Siber suç oranındaki artış, gelecekte yasa uygulayıcılarıyla siber güvenlik uzmanlarının iş birliğini daha da zorunlu hale getirecektir. Bilişim alanında çalışan, hizmet ve ürünleri üreten profesyonellerin ve adalet sistemi süjelerinin bilişim suçları karşısındaki tutumları ve farkındalıklarının ölçülmesi geliştirilecek politikalara ışık tutacaktır.

Araştırmada, bilişim sektörü çalışanları ile hâkim, savcı ve avukatların problemli internet kullanım davranışları ve siber güvenlik ile ilgili tutumları belirlenerek, bilişim hukuku ve adli bilimler çerçevesinde değerlendirilmektedir.

Bu çalışmanın hipotezleri şunlardır:

Hipotez 1: Siber güvenliği sağlama değişkeni açısından bilişim sektörü çalışanları ile hakim, savcı ve avukatlar arasında istatiksel açıdan anlamlı bir fark yoktur.

Hipotez 2: Katılımcıların lisanssız yazılım kullanımları ile kişisel siber güvenliği sağlamaları arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki bulunmaktadır.

Hipotez 3: Katılımcıların lisanssız yazılım kullanımları ile siber mağduriyetleri arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki bulunmaktadır.

Hipotez 4: Katılımcıların internette geçirdikleri süre ile problemli internet kullanımları arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki vardır.

Hipotez 5: Katılımcıların interneti aşırı kullanımları ile siber mağduriyetleri arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki vardır.

Hipotez 6: Katılımcıların antivirüs programı kullanımları ile kişisel siber güvenliği sağlamaları arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki vardır

2. GENEL BİLGİLER

2.1. Siber Suç

2.1.1. Siber Suç Kavramı ve Tanımlanması

Siber suçların gelişimi göz önüne alındığında literatürde birçok tanımlamaya rastlamak mümkündür. Siber suçu tanımlamak, kavramsal bir çerçeveye oturtmak için birçok çalışma yapılmıştır. Bilgisayar suçları ile siber suçların farklı kavramlar olduğu değerlendirilmektedir. Bilgisayar suçu, internet ve network ağlarından önce de varolan ve failin bilgisayar ile bilgisayarlardan yararlanarak işlediği suçlar olarak tanımlanırken, siber suçlar ise network (en yaygın örneği internettir) üzerinde ve bilgisayar üzerinde işlenen suçlar olarak ifade edilmektedir. (Moitra, 2005) Siber suçların kavramsal olarak gelişimi 4 aşamada değerlendirilmiştir.

İlk Aşama: İlk tanımlamalar arasında *'bilgisayar suçu', 'bilgisayar bağlantılı suç'* veya *'bilgisayar kaynaklı suç'* vardır. (Clough, 2015) Bu grupta bilgisayar benzersiz bir suç hedefi veya aracı olarak tanımlanmaktadır. (Clough, 2015) *"Bilgisayar suçu"* terimi, özellikle internetin ticari kullanıma açılmadığı 1990'lı yıllardan önce, yasa ve yönetmeliklerin yanı sıra akademik yazılarda da yaygın olarak kullanılmaktadır. (Li, 2016) İkinci Aşama: Dijital teknoloji daha yaygın hale geldikçe, 'yüksek teknoloji' veya 'bilgi çağı' suçu gibi terimler eklenmiştir. (Clough, 2015). 2000'li yılların başında yayımlanan yazınlarda bu kavramlara yer verildiğini görmekle literatürde bu dönem sonrasında çok sahiplenilmediğini görmekteyiz. Üçüncü Aşama: İnternetin ortaya çıkışıyla 'siber suç'[1] ve 'internet' veya 'net' suçu kavramlarını getirmiştir. (Clough, 2015) Avrupa Konseyi Siber Suçlar Sözleşmesi'nin (ASSS) yasama süreciyle birlikte bu siber suç (cybercrime) kavramı yaygın şekilde kullanılmaya başlanmıştır. Ön ek olarak kullanılan "siber-" kelimesi çok basitçe bilgisayar anlamına gelmektedir. (Li,

[1] Siber suç İngilizce literatürde "cybercrime" şeklinde birleşik bir kelime olarak ifade edilmektedir. Siber kelimesinin İngilizce karşılığı olan "cyber" bir ön ek olarak da başkaca kavramları tanımlamak için kullanılmaktadır.

2016) Cambridge sözlüğünde *"özelllikle internet ilişkisi dahilinde, bilgisayarı içeren, kullanan ya da bilgisayarla ilgili olan,"* (Cambrige University Press, 2022) şeklinde ifade edilmektedir. "Siber-" kelimesi kullanımı için genel eğilim ağ bağlantılı bilgisayarları ifade etme yönündedir.(Li, 2016) Bir kavram olarak söz edilen "sibersuç" (cybercrime) ve bir ön ekle kullanılan "siber suç" tanımlamasının aslında farklı anlamlar içerdiği literatürde ifade edilmektedir. Smith, Grabosky ve Urbas, sıfat olarak kullanılan "siber"in, önek olarak kullanılan "siber-"e eşit olmadığını savunmuştur. (Smith ve ark., 2009) Yani onlara göre "siber suç" (cyber crime), "sibersuç"(cybercrime) demek değildir. "Siber suçu" (cybercrime) "yeni yöntemlerle işlenen yeni suçları kapsayabilecek tekil bir suç kavramı" ve "siber suçu" ise "yeni teknolojiler kullanılarak işlenen geleneksel suçları içeren bir tür suç için tanımlayıcı bir terim" olarak görmüşlerdir. (Smith ve ark., 2009) Siber suç (cyber crime) kavramını dijital teknolojilerin kullanımı yoluyla veya bunlara karşı işlenen her türlü yasaklanmış davranışı kapsayacak şekilde kullanmayı tercih ettiklerini ifade etmişlerdir. (Smith ve ark. 2009) Bunun dışında birçok yazar bu kavramları birbirleri yerine kullanmaktadır. Siber suç (cybercrime), siber suç, internet suçu, net suçu kavramları da birçok yazar tarafından birbiri yerine kullanılmıştır. (Li, 2016) Dördüncü Aşama: Gelinen aşamada kullanılan terimler giderek çeşitlenmiş bulunmaktadır. Bunların arasında 'dijital', 'elektronik' (veya 'e-'), 'sanal', 'BT', 'yüksek-teknoloji' (high-tech) ve 'teknoloji destekli' suçlar yer almaktadır. (Clough, 2015)

Bu kavramlar sınırları belirsiz şekilde geniş anlamlar içerebilmektedir. (Clough, 2015) Bazı yazınlarda siber suçu dijital suçların bir çeşidi şekilde ifade edildiğini görebilmekteyiz. (Lazarus ve ark. 2022) Adli tıp alanında dijital delillerin toplanması ile ilgili yapılan araştırmalarda "dijital suç" kavramının sıklıkla kullanıldığını görmekteyiz. (Al Mutawa ve ark., 2019). Dijital suç kavramına gelen eleştiriler dijital kelimesinin anlamından kaynaklanmaktadır. "Dijital"in, "bilgilerin elektronik olarak, genellikle birler ve sıfırlar şeklinde sayılar biçiminde kaydedildiği veya gönderildiği bir sistem kullanmak" anlamına

gelmesi sebebiyle bir suçun “dijital” olmasının pek mümkün olamayacağı çünkü bir suçun işlenme süreci bilginin işlenme biçiminden farklı olduğu ifade edilmektedir. (Li, 2016)

Elektronik suç (e-suç) kavramının bilgisayarlardan veya bilgisayar ağlarından ziyade (mikro) elektronikle ilgili suç olaylarının özelliklerini vurgulamakta, interneti tüm telekomünikasyon sistemlerinin sadece bir parçası olarak görmektedir. (Li, 2016) Sanal suç kavramında ise odağın, bir suçun işlendiği yer, topluluk veya internetin yarattığı ortamı tespit etmeye yönelik olduğu değerlendirilmektedir.(Li, 2016) Sınırları belirsiz şekilde geniş anlamlar içermesi yönünden bu tanımlamalara çeşitli eleştiriler gelmektedir. Örneğin, "yüksek teknoloji suçu", ağ bağlantılı bilgi teknolojisinin ötesine geçerek nanoteknoloji ve biyomühendislik gibi diğer "yüksek teknoloji" gelişmeleri içerebilir. (Clough, 2015) “Bilişim suçu” “bilgisayar suçu” “bilgisayar kaynaklı suçlar” “siber suç” “internet suçu” “dijital suçlar” “yüksek teknoloji suçları” gibi birçok terime rastlamakla, kelimenin tam anlamıyla alındığında, her terim en az bir eksiklikten muzdarip olmaktadır. Ancak bu tür terimlere harfi harfine değil, suçun işlenmesinde teknolojinin rolünü vurgulayan geniş tanımlayıcı terimler olarak yaklaşılması gerekliliği vurgulanmaktadır. (Clough, 2015)

Veri işleme sistemlerinin kullanıcıları ve istismarcıları yeni alanlara yayıldıkça, yıllar içinde siber suçun farklı tanımları ortaya çıkmıştır. Sınıflandırma için birleşik bir tanım ya da evrensel olarak kurulmuş bir yaklaşım olduğu söylenemez.(Li, 2016) Hâlâ hiçbir terimin gerçekten yaygın hale gelmemiş olmasına ve birçoğunun birbirinin yerine kullanılmasına rağmen, 'siber suç' kavramı görece olarak diğerlerine göre literatürde daha çok kullanılmaktadır.(Clough, 2015) Uluslararası Telekomünikasyon Birliği, hukuki bir terim olarak kullanılmadığı sürece “siber suç”un tek bir tanımının olmamasının önemli olmadığına vurgu yapmaktadır. (ITU, 2011) Siber suçun geniş bir tanımının ceza hukuku reformunda bir takım avantajları olduğu gibi geniş bir tanım, maddi ceza hukukuna dayalı ceza usul hukukunun da değiştirilmesine yardımcı olmaktadır. (Li, 2016)

Bu anlamda siber suç kavramının geniş anlamı temsil edecek şekilde kullanımı kanaatimizce de yerindedir. Bununla birlikte Türk Ceza Kanun'unda (TCK) benimsenen terim "bilişim suçu"dur. Bu sebeple tez çalışmasında başlık olarak bilişim suçu terimi seçilmiştir. Literatürde sıklıkla siber suç kavramı kullanılması nedeniyle bu çalışmada siber suç bilişim suçu yerine kullanılacaktır.

Li'nin tanımına göre; siber suç, *"kitle iletişim araçları, işletim mekanizması, oluşum yeri, aktarım kanalı, hedeflenen nesne, çok amaçlı araç olarak kullanılan veya diğer suçların hazırlanmasında kullanılan veri işleme sistemlerini içeren bir tür geleneksel veya geleneksel olmayan suç biçimidir".* (Li, 2016) Siber suç tanımlarının gelişiminde önce bilgisayar, sonra "ağ" "internet" kavramı baskınken gelecekteki dönüşümün daha hızlı ve daha büyük olabileceği öngörüsüyle bugün bu terimler yerine "veri işleme sistemleri" teriminin dahil edilmesi gerektiği üzerinde durmaktadır. (Li, 2016) Li'ye göre siber suç tanımı, dijital bilgi unsurunu içermeli veya veri işleme sistemlerinin bir parçası olmalıdır. Bir suç, veri işleme sistemleri aracılığıyla işlenemiyorsa siber suç değildir. Siber suç tanımında bir önemli unsur da geleneksel ve geleneksel olmayan biçimde işlenebilmesi bağlamıdır. (Li,2016) Bu ayrımı ve tanımlamayı yapabilmek için veri işleme sistemleri suçta kilit unsur ise suç bilişim suçlarına girmektedir.(Li,2016) Clough, ise dijital teknolojilerin kullanımı yoluyla veya bunlara karşı işlenen her türlü yasaklanmış davranışı kapsayacak şekilde 'siber suç' terimini kullanmayı tercih ettiğini ifade etmektedir. (Clough, 2015) Gordon ve Ford, siber suçu "bir bilgisayar, ağ veya donanım aygıtı kullanılarak kolaylaştırılan veya işlenen herhangi bir suç" olarak tanımlamıştır. (Gordon ve Ford, 2006)

Li'ye göre, bilişim suçları ile geleneksel suçlar arasındaki ilişkiye göre bilişim suçları, geleneksel suçların ikamesi olarak bilişim suçları ve geleneksel suçların tamamlayıcısı olarak bilişim suçları olarak ikiye ayrılabilir. (Li, 2016) Siber suçların tanımlanması kadar sınıflandırması da siber suçları anlamak için önemlidir.

2.1.2. Siber Suç Türleri (Sınıflandırması)

Doktrinde birden fazla siber suç sınıflandırmasına rastlamak mümkündür. Bazı sınıflandırmalarda bilgisayar suçları, bilgisayar tarafından kolaylaştırılan suçlar ve bilgisayar destekli suçlar olmak üzere üçlü bir sınıflandırma bulunduğu ifade edilmektedir. (Clough, 2015) Bu sınıflandırmada siber suçların eşsiz yeni bir suç türü mü olduğu yoksa geleneksel suçların yeni bir biçimde işlenişi mi olduğu sorusunu gündeme getirmektedir. (Clough, 2015) Burada ayırıcı özellik suçun, bilgisayar olmadan hiçbir şekilde var olamayacak olmasıdır. Gerçek 'siber suçlar', yani bilgisayar olmadan hiçbir şekilde var olamayacak suçlar, bilgisayarlara ve bilgisayar ağlarına karşı işlenen suçlar olarak tanımlanmaktadır. (Clough, 2015) Yukarıda sözü edilen üçlü sınıflandırma biçimi Avustralya, Kanada, Birleşik Krallık ve uluslararası düzeyde de kullanıldığı görülmektedir. (Clough, 2015)

Gordon ve Ford'un sınıflandırmasına göre, bilgisayar ya da cihaz suçun aracısı, suçun kolaylaştırıcısı ya da suçun hedefi olabilir; hatta suç sadece bilgisayarda ya da sanal olmayan başka yerlerde de işlenebilir. (Gordon ve Ford, 2006) Gordon ve Ford, siber suçları Tip 1 ve Tip 2 olarak kategorize etmektedir. Bu sınıflandırmaya göre Tip I siber suç aşağıdaki özelliklere sahiptir:

"1. Mağdurun bakış açısından genellikle tekil ya da ayrı bir olaydır.

2. Genellikle tuş vuruşu kaydediciler, virüsler, rootkitler veya Truva atları gibi suç yazılımlarının kullanıcının bilgisayar sistemine girmesiyle kolaylaştırılır" (Gordon ve Ford, 2006)

Tip II siber suçlar, siber takip ve taciz, çocuk istismarı, gasp, şantaj, borsa manipülasyonu, karmaşık kurumsal casusluk ve çevrimiçi terörist faaliyetler planlama veya yürütme gibi faaliyetleri içerir, ancak bunlarla sınırlı değildir. (Gordon ve Ford, 2006) Tip II siber suçun özellikleri şunlardır:

"1. Genellikle suç yazılımı sınıflandırmasına uymayan programlar tarafından kolaylaştırılır. Örneğin, konuşmalar IM (Anında Mesajlaşma) istemcileri kullanılarak gerçekleştirilebilir veya dosyalar FTP protokolü kullanılarak aktarılabilir.

2. Kullanıcının bakış açısından genellikle tekrarlanan iletişimler veya olaylar vardır." (Gordon ve Ford, 2006)

Siber suçların sınıflandırması açıklanırken Avrupa Konseyi Siber Suç Sözleşmesi (ASSS) (Convention on Cybercrime, 2001) sınıflandırması esas alınacaktır. Aşağıda detayları açıklanacak olan ASSS 1 Temmuz 2004 tarihinde yürürlüğe girmiş olup Türkiye ASSS'yi 10 Kasım 2010 tarihinde imzalamıştır. 6533 sayılı Kanunla "Sanal Ortamda İşlenen Suçlar Sözleşmesi" adıyla onaylanmıştır. ASSS siber suçları dört kategoriye ayırmaktadır.

1. **Kategori: Bilgisayar Veri veya Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanılabilirliğine İlişkin Suçlar**

- Yetkisiz (yasadışı) erişim (madde 2)
- Yetkisiz (yasadışı) müdahale (madde 3)
- Verilere müdahale (madde 4)
- Sistemlere müdahale (madde 5)
- Cihazların kötüye kullanımı (madde 6)

2. **Kategori: Bilgisayarla Bağlantılı (Bilgisayar Aracılığıyla İşlenebilen) Suçlar**

- Bilgisayar aracılığıyla sahtecilik (madde 7)
- Bilgisayar aracılığıyla dolandırıcılık (madde 8)

3. **Kategori: İçerikle Bağlantılı Suçlar**

- Çocuk pornografisi (madde 9)

4. **Kategori: Fikri Mülkiyet Haklarının İhlaline İlişkin Suçlar**

- Telif Hakları ve Bağlantılı Hakların İhlal Edilmesi (madde 10)

2.1.2.1. Bilgisayar Veri veya Sistemlerinin Gizliliğine, Bütünlüğüne ve Kullanılabilirliğine İlişkin Suçlar

2.1.2.1.1. Yasadışı erişim

Doktrinde ‘’illegal access’’ olarak ifade edilen hukuka aykırı erişim kavramının Türk doktrininde yetkisiz erişim olarak da kullanıldığı görülmektedir. (Ketizmen, 2008) ASSS ile Birleşmiş Milletler (BM) düzenlemelerinde “illegal access” kavramı kullanılmıştır. ASSS’nin Açıklayıcı Raporu’nda “yetkisiz erişim”/ ”yasadışı erişim” tanımlanmıştır. Açıklayıcı Rapora göre (COE, 2001; Eralp, 2022) "Yasadışı erişim", bilgisayar sistemleri ve verilerinin güvenliğine (yani gizliliği, bütünlüğü ve kullanılabilirliği) yönelik yüksek tehditler ve saldırılara ilişkin temel suçları kapsar. Yalnızca yetkisiz izinsiz giriş, yani "hackleme", “cracking”veya “computer trespass” ilke olarak yasa dışı olmalıdır. İzinsiz giriş, sistem ve verilerin meşru kullanıcıları için engellere yol açabilir ve düzletmek için yüksek maliyetlere veya yıkıma neden olabilir. Bu yetkisiz girişler, gizli verilere (parolalar, hedeflenen sistemle ilgili bilgiler dahil) ve sırlara erişime, sistemin bir ödeme yapılmaksızın kullanılmasına izin verebilir ve hatta bilgisayar korsanlarını bilgisayarla ilgili dolandırıcılık veya sahtecilik gibi bilgisayarla ilgili daha ciddi suç türlerini işlemeye teşvik edebilir. (Eralp, 2022)

Açıklayıcı Rapora göre "erişim", bir bilgisayar sisteminin bütününe veya herhangi bir bölümüne (donanım, bileşenler, kurulu sistemin depolanmış verileri, dizinler, trafik ve içerikle ilgili veriler) girilmesi anlamına gelmektedir. (Eralp, 2022) Sisteme yalnızca bir e-posta veya dosya gönderilmesini gibi işlemler erişim anlamına gelmemektedir. "erişim", kamusal telekomünikasyon ağları aracılığıyla veya bir kuruluş içindeki bir LAN (yerel alan ağı) veya Intranet gibi aynı ağ üzerindeki bir bilgisayar sistemine bağlı olduğu başka bir bilgisayar sisteminin girilmesini kapsar. (Eralp, 2022) Fiilin ayrıca "haksız olarak" işlenmesi gerekir. (Eralp, 2022)

Yasadışı erişim suçu TCK'da düzenlenen suç türlerinde ayrıca değinileceği üzere TCK m. 234'te düzenlenen "Bilişim Sistemine Girme ve Kalma Suçu"na karşılık gelmektedir. TCK m.243'te düzenlenen bilişim sistemine girme veya kalma suçu, 24.03.2016 tarihli, 6698 sayılı Kanun'un 30.maddesiyle yapılan değişiklikle seçimlik hareketli olarak düzenlenmiş ve ASSS'nin 2.maddesiyle uyumlu hale gelmiştir. (Çetin, 2021)

ASSS'nin 2. maddesinde,

"Madde 2- Yasadışı Erişim Taraflardan her biri, bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişimi, kasten yapıldığı zaman, kendi iç hukuku kapsamında cezai bir suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir. Taraflardan biri, söz konusu suçun, bilgisayar verilerini elde etmek veya başka bir sahtekâr niyetle veya bir bilgisayar sistemine bağlı başka bir bilgisayar sistemiyle ilişkili olarak güvenlik tedbirlerinin ihlal edilmesi suretiyle işlenmiş olmasını şart koşabilir" şeklinde düzenlenmiştir.

"Hack" olarak da literatürde günlük dilde yer bulan yasadışı erişim, bilgisayar suçlarında, ilk suç olarak tanımlanan eylemlerden biri olmuştur. (Chawki, 2005) Bilişim sistemine girme suçu bilişim suçlarından en yaygın olarak karşılaşılan suç tipidir. (Topçuoğlu, 2022)

2.1.2.1.2. Yasadışı müdahale

ASSS'nin 3. maddesinde tanımlanan Yasadışı Müdahale TBMM'de onaylanan metninde "Yasadışı Araya Girme" şeklinde çevrilmiştir. ASSS'nin 3. maddesi şu şekildedir:

"Taraflardan her biri, bilgisayar verileri taşıyan bir bilgisayar sisteminden elektromanyetik dalgalarla yayılma da dahil olmak üzere, bilgisayar verilerinin bir bilgisayar sisteminden diğer bir bilgisayar sistemine veya bir bilgisayar sisteminin kendi içinde umuma kapalı olarak iletimi esnasında teknik yöntemler kullanılarak gerçekleştirilen araya girme fiilinin, haksız yere ve kasten yapıldığı zaman, kendi iç hukuk kapsamında cezai suç olarak tanımlanması için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir.

Taraflardan biri söz konusu suçun sahtekarlığa yönelik veya başka bir bilgisayar sistemine bağlı bir bilgisayar sistemiyle ilişkili olarak işlenmiş olmasını şart koşabilir."

Açıklayıcı Rapor'da bu hükmün iletişim verisinin mahremiyeti hakkının korunmasının amaçlandığı ifade edilmiştir. Avrupa İnsan Hakları Sözleşmesi (AHİS) m. 8'e dayanak olarak gösterilmiştir. Bu madde ile düzenlenen suçta, kişiler arasındaki telefon görüşmelerinin geleneksel olarak dinlenmesi ve kaydedilmesi ile iletişimin mahremiyetinin ihlalinin temsili olduğu, bu madde ile, AHİS m. 8'de düzenlenen "yazışmaların gizliliği ilkesini", telefon, faks, e-posta veya dosya aktarımı yoluyla her türlü elektronik veri aktarımına da uygulandığı ifade edilmiştir. (Eralp, 2022) Cezai müeyyideye tabi olması içinse, bu tür müdahalenin "kasıtlı" ve "haksız biçimde" gerçekleştirilmiş olması aranmaktadır. (Eralp, 2022)

TCK'nın 132. maddesinde "Haberleşmenin gizliliğini ihlal suçu" ve 133. maddesinde "Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu" düzenlenmiştir. TCK 132. maddesinin gerekçesinde, bu suçun temel şeklinin gizliliğin sadece dinlemek veya okumak suretiyle ihlal edilmesi olduğu, nitelikli şeklinin, bu gizlilik ihlâlinin iletişim içeriklerinin yani görüşmelerin veya yazılanların kayda alınması suretiyle yapılması olduğu ifade edilmektedir. (Sevük, 2008)

TCK 133. maddede düzenlenen konuşma, madden aynı ortamda veya yüz yüze gerçekleştirilen konuşmadır. Doktrinde, insanlar arasında, araya vasıta konmak suretiyle gerçekleştirilen konuşmaların, telefon ve internet üzerinden gerçekleşmesinin TCK uyarınca "konuşma" değil, "haberleşme" olduğu, bu vasıtalarla yapılan konuşmalara yapılan müdahalenin, TCK m. 132 Haberleşmenin gizliliğini ihlal suçu bağlamında değerlendirilmesi gerektiği ifade edilmektedir. (Göktürk, 2016) Bu bakımdan Sözleşmede düzenlenen Yasa dışı araya girme suçu TCK'da düzenlenen "Haberleşmenin gizliliğini ihlal suçu"na karşılık gelmektedir.

2.1.2.1.3. Verilere müdahale

Verilere müdahale suçu ASSS'nin 4. maddesinde düzenlenmiştir. Bu madde gereğince bilgisayar verilerine zarar verilmesi, verilerin silinmesi, değiştirilmesinin iç hukuk kapsamında suç olarak düzenlenmesi gerekmektedir. ASSS'nin 4. maddesi şu şekildedir:

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

Açıklayıcı Rapor'da hükmün amacının, bilgisayar verilerini ve programlarını da, maddi nesneler gibi, kasten zarar verme girişimlerine karşı korumak olduğu ifade edilmektedir. (Göktürk, 2016) Verilere müdahaleye karşılık gelen fillerin "tahrip etmek" ve "bozmak" olduğu, özellikle bu eylemin veri ve programların bütünlüğünün ya da bilgi içeriğinin olumsuz şekliyle değiştirilmesiyle ilişkili olduğu vurgulanmaktadır. (Eralp, 2022) Verilerin erişilmez kılınması, verilerin tutulduğu bilgisayara ya da veri taşıyıcısına erişimi olan bir kimse için verilerin ulaşılabilirliğini engelleyen veya verilerin erişimini sonlandıran herhangi bir eylemdir. Virüsler ve truva atları gibi zararlı yazılımların sisteme entegre edilmesi ve sonuçta verilerin değiştirilmesinin bu hüküm kapsamında değerlendirilmesi gerektiği ifade olunmuştur. (Eralp, 2022)

TCK'nın 244. maddesinde "Sistemi engelleme, bozma, verileri yok etme veya suçu düzenlenmiştir. Bu kapsamda TCK 244. maddesinin 2. fıkrası ASSS'nin 4. maddesinde düzenlenen Verilere Müdahale Suçuna karşılık gelmektedir.

2.1.2.1.4. Sisteme müdahale

Sisteme müdahale suçu ASSS'nin 5. maddesinde düzenlenmektedir. Bu madde sistemin işleyişinin veriler yoluyla engellenmesine ilişkindir. ASSS'nin TBMM tarafından onaylanan 5. maddesi şu şekildedir:

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

Açıklayıcı Rapor'da "engelleme" teriminin, bilgisayar sisteminin doğru biçimde işleyişine müdahale niteliğindeki eylemler için kullanılmış olduğu; engellemenin, bilgisayar verilerine yeni veriler eklemek, bilgisayar verilerini başka yerlere iletmek, zarar vermek, silmek, bozmak, değiştirmek veya erişilmez kılmak yoluyla yapılmış olması gerektiği ifade edilmiştir. (Eralp, 2022) Engellemenin ayrıca "ciddi ölçüde" olması gerektiği ve haksız biçimde yapılmış olması gerektiği vurgulanmıştır. (Eralp, 2022) Rapor'da sistemi kullanma veya diğer sistemlerle etkileşim kabiliyeti üzerinde ciddi biçimde zararlı etkiye sahip olacak şekilde, boyutta veya sıklıkta veri gönderilmesini "ciddi" olarak değerlendirilmiştir. Buna örnek olarak "hizmet reddi" saldırıları oluşturan programlar, sistemin çalışmasını engelleyen veya ciddi biçimde yavaşlatan virüsler gibi zararlı yazılımlar veya sistemin çalışmasını engellemek için bir alıcıya çok sayıda e-posta ileten programlar aracılığıyla olması verilmiştir. (Eralp, 2022)

Anılan sözleşme maddesi TCK'nın "*Sistemi engelleme, bozma, verileri yok etme veya değiştirme"* başlıklı 244. maddesine karşılık gelmektedir. Dos-DDoS saldırıları benzeri siber saldırılarla sistemin ağırlaştırılması, erişilmez hale getirilmesi, kilitlenmesi, cihazın fiziki varlığının ortadan kaldırılması, sistemi şifreleme ya da mevcut şifresinin değiştirilmesi bu suça yol açabilecek eylemlerdir. (Aköz, 2018)

2.1.2.1.5. Cihazların kötüye kullanımı

ASSS'nin 6. maddesi Cihazların Kötüye Kullanımı Suçunu düzlemektedir. Bu madde ile Sözleşmede ele alınan yasadışı erişim, yasadışı müdahale, verilere müdahale, sistemlere müdahale suçlarının işlenebilmesi amacına yönelik olarak tasarlanmış bir cihaz, bir bilgisayar

programı, sahte erişim şifreleri ve benzerlerinin üretimi, pazarlaması, kullanım amacıyla tedarik edilmesi ve bulundurulması yasaklanmıştır. (Eralp, 2022) Bu cihaz ve programların tedarik edilmesi ve bulundurulması bağımsız bir suç olarak düzenlenmiştir. Bu suçta sözü edilen erişim araçları çoğunlukla hacker araçlarıdır. (Eralp, 2022) Anılan madde düzenlenişi itibariyle temel hazırlık işlemleri niteliğindeki fiilleri cezalandırılmasını öngörmektedir. (Kaya ve Çakır, 2020) TCK 254/A "Yasak cihaz ve programlar" başlıklı maddesinde yer alan hüküm anılan sözleşme hükmüne karşılık gelmektedir.

2.1.2.2. Bilgisayarlarla bağlantılı suçlar

2.1.2.2.1. Bilgisayarla bağlantılı sahtecilik

ASSS'nin 7. maddesinde düzenlenen Bilgisayarla Bağlantılı Sahtecilik suçu hukuki süreçlerle ilgili olan verilere müdahale edilmesini düzenlemektedir. ASSS'de bu suç aşağıda belirtildiği şekilde tanımlanmıştır:

"Taraflardan her biri özgün olmayan verilerle sonuçlanan yeni veri girme, verileri değiştirme, silme veya engelleme eylemlerinin, söz konusu verilerin yasal açıdan özgün verilermiş gibi kabul edilmesi veya işlem görmesi niyetiyle, kasten ve haksız yere gerçekleştirildiği zaman, verilerin doğrudan okunabilir ve anlaşılabilir olup olmadığına bakılmaksızın, bu eylemlerin kendi iç hukukunda cezai suç olarak tanımlanabilmesi için gerekli olabilecek yasama tedbirlerini ve diğer tedbirleri kabul edecektir."

Açıklayıcı Rapor'da bu suçla, fiziki evraklar ilgili sahteciliğe benzer bir suç düzenlemek amacı güdüldüğü ifade edilmiştir. (Eralp, 2022) Bilgisayarlarla ilintili sahtecilik, verilerin içindeki bilgilerin hakikatine dayalı hukuki süreç esnasında verilerin delil niteliklerini değiştirmek için hukuka aykırı şekilde veri oluşturulması ya da tutulan verilerin değiştirilmesi suretiyle ilgilileri yanıltmaktır. (Eralp, 2022) Bu suçla, korunan hukuki yarar, hukuki süreçlerde mühim olarak değerlendirilebilecek elektronik verilerin emniyeti ve geçerliliğidir.

2.1.2.2.2. Bilgisayarla bağlantılı dolandırıcılık

ASSS orijinal metninde anılan suç "Computer-related fraud" olarak ifade edilmektedir. İngilizce "fraud" kelimesi Türkçe'ye dolandırıcılık, düzenbazlık, sahtekarlık kelimeleriyle çevrilmiştir. (Cambrige University Press, 2022b) Bu kavram, sıklıkla bilişim dünyasında doğrudan İngilizce olarak "fraud" kelimesi ile kullanılmaktadır.

ASSS'nin 8. maddesi aşağıdaki şekildedir:

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

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

a.bilgisayar sistemlerine veri girişi yapmak, verileri değiştirmek, silmek veya engelleme,

b. bir bilgisayar sisteminin ışleyişine herhangi bir müdahalede bulunma…"

Açıklayıcı Rapor'da teknolojik devrimle birlikte kredi kartı dolandırıcılığı da dahil olmak üzere dolandırıcılık türevi malvarlığına karşı işlenen suçları işleme fırsatlarının çoğaldığı, bilgisayar sistemlerinde karşılık bulan, yönetilen varlıkların da (fonlar, mevduat paraları), geleneksel malvarlığı şekilleri gibi dolandırıcılığın ereği haline geldiği ifade edilmiştir. (Eralp, 2022)

TCK m.157'de dolandırıcılık suçunun basit şekli düzenlenmiş olup 158. maddede de dolandırıcılık suçunun nitelikli halleri düzenlenmiştir. TCK m.158/1-f hükmü ile, dolandırıcılık suçunun *"bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle*" işlenmesi ağırlaştırıcı neden olarak düzenlenmiştir.

Doktrinde dolandırıcılık suçunun bilişim sistemleri ve bankaların araç olarak kullanılması suretiyle işlenmesinin bir arada düzenlenerek, ağırlaştırıcı neden olarak belirlenmesinin

kanunun yapım tekniği bakımından hatalı olduğu yönünde görüşler mevcuttur. Söz konusu işleniş biçimlerinin ayrı birer suç olarak düzenlenmesinin söz konusu olabileceği görüşleri mevcuttur. (Korkmaz, 2020) Bununla birlikte TCK'nın 245. maddesinde banka ve kredi kartlarının kötüye kullanılması suçu düzenlenmiştir. Söz konusu maddede 3 ayrı suç tipi düzenlenmiştir. (Okuyucu Ergün, 2013) TCK m. 157/1-f hükmü ve TCK 245. maddelerinin sözleşmenin 8. maddesine karşılık geldiği söylenebilecektir.

2.1.2.3. İçerikle bağlantılı suçlar

2.1.2.3.1. Çocuk pornografisiyle bağlantılı suçlar

ASSS'nin 9. maddesinde, *"bir bilgisayar sistemi üzerinden dağıtımını yapmak amacıyla çocuk pornografisi üretmek, bir bilgisayar sistemi üzerinden çocuk pornografisi sunmak veya erişilebilir hale getirmek, bir bilgisayar sistemi üzerinden çocuk pornografisinin dağıtım veya iletimini yapmak, kendisi veya başkası için bir bilgisayar sistemi üzerinden çocuk pornografisi temin etmek, bir bilgisayar sisteminde veya bilgisayar verileri depolama aygıtında çocuk pornografisi bulundurmak"* eylemlerinin ülkelerin iç hukukunda suç olarak tanımlanması gerekliliği düzenlenmiştir. Bu madde ile çocuk pornografisinin elektronik biçimde üretilmesi, barındırılması ve yayımının biçimleri suç olarak tanımlanmıştır. (Eralp, 2022)

ASSS'de bilgisayar sisteminde ya da bilgisayar verilerinin tutulduğu başka aygıtlarda, çocuk pornografisi barındırmak suç olarak tanımlanmıştır. Açıklayıcı Rapor'da çocuk pornografisi bulundurmanın bu yöndeki içerik için talebi arttıracağı ifade edilerek, üretimden barındırmaya değin tüm fiiller için ceza öngörmenin, çocuk pornografisi varlığını eksiltmede etkili olacağı değerlendirilmiştir. Sözleşmede sözü edilen "cinsel biçimdeki müstehcen eylem"in hakikat olmasının ya da sistem benzetimi yoluyla sanal biçimde üretilmiş olmasının önemi olmadığı vurgulanmıştır. (Eralp, 2022)

Türkiye BM Çocuk Hakları Sözleşmesi'nin (ÇHS) tarafı olup ÇHS m. 34'te çocukların pornografik amaçlarla kullanılmasının önüne geçmek için amacıyla devletlerin gerekli yasal

önlemleri alması gerekliliği düzenlenmiştir. "Çocuk Haklarına Dair Sözleşmeye Ek Çocuk Satışı, Çocuk Fahişeliği Ve Çocuk Pornografisi İle İlgili İhtiyari Protokol" m. 1 uyarınca taraf devletler çocuk pornografisini yasaklayacaklardır. Protokol'ün 3 maddesine göre, çocuk pornografisinin yasaklanmasına konu eylemler belirtilmiştir. (Taneri, 2018)

Bu doğrultuda TCK'nın 226. maddesinde müstehcenlik suçu düzenlenmiştir. Bu maddede *"müstehcen görüntü, yazı veya sözleri içeren ürünlerin üretiminde çocukları, temsili çocuk görüntülerini veya çocuk gibi görünen kişileri kullanmak"* yasaklanmıştır. 5651 sayılı Kanun m. 8/1-a bendinde, internette müstehcenlik suçunu içeren yayınlar hakkında içeriğin yayından çıkarılması veya erişimin engellenmesi kararı verileceği belirtilmiştir. 5651 sayılı Kanunun 8 maddesinin devam eden fıkralarında içeriğin çıkarılması ve erişimin engellenmesi kararını yerine getirmemenin idari ve cezai müeyyideleri belirlenmiştir. (Taneri, 2018)

2.1.2.4. Telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar

ASSS'nin 10. maddesinde Paris Antlaşması, Ticaretle Bağlantılı Fikri Mülkiyet Hakları Antlaşması ve WIPO Telif Hakları Antlaşması kapsamında telif haklarının ihlalinin kasten, ticari düzeyde ve bir bilgisayar sistemi vasıtasıyla gerçekleştirilmesinin suç olarak düzenlenmesi gerekliliği düzenlenmiştir. Açıklayıcı Rapor'da telif hakkı ihlallerinin internette en yaygın olarak işlenen suçlardan biri olması, eserlerin telif hakkı sahibinin onayı olmadan internette çoğaltılmasının ve yayılmasının sıklıkla görülmesine vurgu yapılmıştır. (Eralp, 2022)

Lisanssız yazılım kullanımı da bu başlık altında suç olarak değerlendirilmektedir. Yazılım, 5846 sayılı Fikir ve Sanat Eserleri Kanunu (FSEK) uyarınca ilim ve edebiyat eseri kategorisinde eser olarak tanımlanmaktadır (FESK md. 2). FESK ilgili maddeler yönünden "özel ceza yasası" niteliği taşımaktadır. Lisanssız yazılım kullanmak, FSEK m. 22/3'te özel olarak düzenlenen, eser sahibinin "çoğaltma hakkı"nın ihlali niteliğinde olduğundan, FSEK m. 71 uyarınca suçtur. Günümüzde geleneksel eserlerle birlikte birçok eser dijital olarak

üretilmeye başlanmıştır. Özellikle son dönemlerde Non Fungible Token (NFT) adı verilen dijital eserler de fikri mülkiyet hakları kapsamında sıklıkla gündeme gelmektedir.

2.1.3. Siber Suçların İşlenme Biçimleri

Bilişim suçlarının işlenme yöntemleri teknolojik gelişmeler karşısında çeşitlenmekte ve artmaktadır. (Aköz, 2018) Bilişim suçlarının işlenme biçimlerindeki artış siber suçların hukuk düzeninde zaman zaman yeniden farklı biçimlerde tanımlamalarının yapılmasını gerekli kılmaktadır. Her durumda yeni işleniş biçimleri yeni hukuk kurallarını gerekli kılmasa da suçun tanımlanması, suçun soruşturulması, delillerin toplanması adına siber suçların işleniş biçimlerinin araştırılması önem arz etmektedir. Bu sebeple siber suçların işlenme biçimlerinin araştırılması siber suçlarla mücadele için büyük önem taşımaktadır. (Stratonov ve ark., 2021) Bu başlıkta siber suçların en yaygın işlenme biçimleri ele alınacaktır.

2.1.3.1. Zararlı yazılımlar/kötü amaçlı yazılımlar

Kötü amaçlı yazılımlar İngilizce bilişim terminolojisinde *"malware/ malicious software"* olarak ifade edilmektedir. Zararlı yazılım, sistemler üzerinde kötü amaçlar gerçekleştiren tüm yazılımlar için kullanılan genel bir terimdir. (Yesir, 2021) Zararlı yazılımlar sistem ve uygulama programlarındaki açıklardan ve zafiyetlerden faydalanarak saldırı başlatmaktadırlar. (Samet ve Aslan, 2018) Zararlı yazılımlar, başka bilgisayar veya bilişim sistemlerine geçerek bu sistemlerde; yavaşlama, kendini kopyalayarak sistemi çalışamaz hale getirme, bilgileri başka sistemlere gönderme gibi çeşitli etkiler meydana getirirler ve yayılma amacı güderler. (Birceviz, 2019) Zararlı yazılımlar en çok karşılaşılan siber saldırı türlerinden birisidir. Aşağıda belli başlı zararlı yazılım türleri açıklanacaktır.

2.1.3.1.1. Virüsler

Sistemlere zarar verebilecek, ilk akla gelen zararlı yazılım virüslerlerdir. (Aköz, 2018) Kendi kendine çoğalabilen girdiği sistemleri çalışmaz hale getirebilen yazılımlardır. (Samet ve Aslan, 2018) Virüsler 3 temel evreden oluşurlar. Bunlar çoğalma, programın tetiklenmesi ve

önceden amaçlanan zararın verilmesidir. (Samet ve Aslan, 2018). Taşınabilir bellekler, e-posta spamları, iletişim programlarından gönderilen mesajlar aracılığıyla bulaşabilmektedirler. Virüsler etkinleştirilene dek hareketsizdirler. Virüsleri diğer kötücül yazılımlardan ayıran temel özellik insanlar tarafından etkileştirilmeye gereksinim duymasıdır. (Canbek ve Sarıoğlu, 2007) Virüs bulaştığının ilk belirtileri sistemdeki yavaşlama olarak ifade edilmektedir.

2.1.3.1.2. Solucanlar

Solucanlar İngilizce olarak gündelik ve teknik dilde genellikle computer worms ya da kısaca worms olarak ifade edilirler. Kullanıcı etkisi olmaksızın kendiliğinden işlevselleşen ve kopyasını ağ bağlantısı olan başka bir sisteme kopyalayabilen yazılım türlerinin genel adıdır. (Dülger, 2004) Virüslerin aksine artmaları için başka programlara ihtiyaçları yoktur, entegre olduğu sistemde gizlenmek amacıyla kendi dosyalarını silerler. (Samet ve Arslan, 2018) E-posta, FTP ve HTTP gibi internet hizmetleri solucanların yayılmasında en çok kullanılan yöntemlerdir. (Canbek ve Sarıoğlu, 2007) Solucanlar, başka dosyaları değiştirmez ama aktif biçimde bellekte bekler ve kendilerini kopyalamaya devam ederler. (Canbek ve Sarıoğlu, 2007)

2.1.3.1.3. Truva atı

Truva atlarının İngilizce teknik dilde kullanımın "trojan horse"tur. Truva atları kullanıcılar tarafından internette ücretsiz kullanılan basit programlar ya da ekran koruyucular gibi uygulamalar aracılığıyla kullanıcının cihazına bulaşmaktadırlar. (Akarslan, 2015) Çoğunlukla faydalı bir programa ekli biçimde varlığını gösterir. Kendiliğinden artma özellikleri bulunmamaları ve zararlı olmayan kodmuş gibi görünmeleri sebebiyle virüslerden ayrılmaktadır.(Dülger, 2004) Virüslere benze şekilde truva atları da virüsler gibi kendi başlarına etkinleşemezler, insan etkileştirmesine gereksinim duyarlar. (Canbek ve Sarıoğlu, 2007) Genel Truva atları dışında, PSW Truva atları, Truva arka kapıları, tıklayıcılar gibi çeşitleri de vardır. (Canbek ve Sarıoğlu, 2007)

2.1.3.1.4. Arka kapılar

İngilizce teknik dilde *"backdoors"* olarak adlandırılırlar. Geleneksel güvenlik mekanizmalarını atlatarak, sistemin dışarıdan erişilmesine olanak sağlayan programlardır. Arka kapılar çoğunlukla Truva atları kullanılarak saldırının etkisi altına almak istenen sistemlere yüklenir ve sadece arka kapıyı yazan, koyan kişiler tarafından bilinirler.(Samet ve Arslan, 2018) Bir uygulama içindeki veritabanları ve dosya sunucuları gibi kaynaklara uzaktan erişim sağlanır ve faillere uzaktan sistem komutları verme ve kötü amaçlı yazılımları güncelleme olanağı verir. Arka kapılar, sıklıkla truva atları ile karıştırılabilmekle, truva atı, yararlı bir program gibi görünmekteyse de arka kapılar, sadece sisteme erişimi sağlayan gizlenmiş yapılardır. (Canbek ve Sarıoğlu, 2007)

2.1.3.1.5. Fidye yazılımları

Günümüzde sıkça karşılaşılan bir siber saldırı türüdür. Çoğunlukla gasp amacıyla kullanılmaktadır. Saldırı gerçekleştiğinde, kötü amaçlı yazılım ekranı engeller veya depolanan verileri şifreler ve kullanıcıya ekrandan ödeme detaylarını içerir şekilde bir fidye talebi görüntülenir. (İstanbul Bilgi Üniversitesi, 2022) Saldırgan, mağdurdan, bilgi-belgelerine yeniden erişim vermek için para ödemesini talep eder. Saldırgan ödeme yöntemi olarak genellikle iz sürülememesi kripto paraları seçer. (İstanbul Bilgi Üniversitesi, 2022)

Fidye yazılımlar tüm kullanıcılar için büyük bir tehdit oluşturmaktadır. Özellikle hedefli fidye yazılımı saldırıları siber suçlular için oldukça kazançlı hale gelmiştir. Milyonlarca dolarlık fidye ödemelerine yol açan büyük fidye yazılımı saldırıları, giderek artan sayıda kötü niyetli kimseleri fidye yazılımı alanına çekmiştir. (Symantec, 2021) WannaCry dünyada en çok bilinen ve en çok zarara neden olmuş fidye yazılımlarından birisidir. Covid 19 Pandemisi ise saldırganlar yeni bir hedef seçmiş ve fidye yazılım çeteleri sağlık sektörünü hedef almışlardır. (Symantec, 2021)

2.1.3.1.6. Korsan amaçlı kullanılan yazılımlar

Rootkits olarak da ifade edilen korsan amaçlı yazılımlar, tehdit düzeyi en yüksek kötü amaçlı yazılımlardandır. Esas gayesi, artmak değil, mevcut olduğu sistemde saklanmaktır. (Samet ve Arslan, 2018) Saldırganlarca bir hedef bilgisayar veya ağı kontrol etmek amacıyla kullanılan, sisteme yönetici düzeyinde erişim hakkı veren yazılımlardır. (Kaspersky, 2022) Saldırganlar bu yazılımı belirledikleri sistemlere yüklemek ve saldırmak için sıklıkla kimlik avı veya başka bir sosyal mühendislik saldırısı türünü kullanırlar. (Kaspersky, 2022)

2.1.3.1.7. Robotlar

Botnet, tek bir merkezden kontrol edilecek biçimde bu merkeze bağlı zombi bilgisayar topluluğudur. (Aköz, 2018) Botnet'ler "açıklı" bilgisayar ve sistemlere veri ileterek bu makinaları kontrol altına alıp, gerçekleştirecekleri başka saldırılarda aracı olarak kullanılırlar.(Samet ve Arslan, 2018) BTK tarafından yetkilendirilmiş işletmecilerin, İSO 27001 sertifikasına sahip olma zorunluluğunda, yerine getirmesi gereken yükümlülüklerine paralel şekilde Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği düzenlenmiş ve 13 Temmuz 2014 tarihli ve 29059 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Yönetmeliğin 2. maddesinde, köle bilgisayar, *"Herhangi bir amaçla kullanılmak üzere, zararlı yazılımlar veya kötü niyetli kişiler tarafından uzaktan yönetilen internete bağlı bilgisayar"* olarak tanımlanmıştır.

2.1.3.1.8. Casus yazılımlar

Casus yazılımlar, *"spyware"* yüklendiği bilgisayarda, tuş kayıtlarını, erişilen internet sayfalarını kaydederek, sabit diskindeki verileri taramadan geçirmek benzeri işlemlerle kişilerin e-posta, banka vb. şifrelerini çalabilir ya da ağ ve sistem kaynaklarını tüketen, sayfalara erişimi yavaşlatan, bilgisayarın genel olarak ağır işlemesi benzeri sonuçları olan fiiller gerçekleştirebilir. (Ortadoğu Teknik Üniversitesi, 2019) "Keylogger" bu yazılım türüne

örnektir. “Keylogger” her tuş vuruşunu kayıt ederek ve bu topladığı verileri saldırganlara ileten yazılımlardır. (Samet ve Arslan, 2018)

2.1.3.2. Dos-DDoS saldırıları

DoS (Denial of Service - Hizmet/Servis Dışı Bırakma) saldırısı hizmet aksatma metodudur. Bu metotta sisteme arka arkaya ve sistematik şekilde saldırı gerçekleşir ve sistem kimseye hizmet veremez hale gelir.(Dülger, 2015) DDoS (Distributed Denial of Service - Dağıtık Hizmet/Servis Dışı Bırakma) atağında önceden tasarlanmış bir makine üzerinden hedef sisteme saldırı gerçekleştirilir ve sistem hizmet veremez hale getirilir. Zombi adlı araçla birlikte kullanılarak saldırının boyutu arttırılır ve saldırgan gizlenir. (Dülger, 2015) Türkiye’de birçok internet servis sağlayıcı siber güvenlik hizmetleri kapsamında bu yaygın saldırı biçimden korunmak için bir ürün olarak Dos-DDoS güvenlik hizmetleri vermektedir.

2.1.3.3. Oltalama

Oltalama, hedef kullanıcıların kişisel/gizli bilgilerini ifşa etmelerini sağlamak için gerçekleştirilen saldırı biçimidir. (ITU, 2011) Çoğunlukla mevcut resmi internet sitesi veya uygulamanın bir benzeri yapılarak kurbanın buralara girdiği bilgiler art niyetli bilgisayar korsanlarınca çalınır. Bir diğer yöntem ise e-mail üzerinden bir kısım bilgilerin güncellemesinin talep edilmesi ve hedefin kimsenin bunu fark etmeyip istenen bilgileri gönderilen forma girmesi ile bilgiler saldırgana iletilmiş olur.(Ocak ve ark., 2014)

2.1.3.4. İstem dışı alınan elektronik postalar

İstem dışı postalar İngilizce teknik ve gündelik dilde “spam” olarak adlandırılırlar. Spamlar ilgililerine istekleri dışında gönderilen aynı veya benzer içerikli, genelde reklam amaçlı ya da müstehcen içerikli mesajların geniş kitlelere iletilmesi amacı güden e-postalardır. (Birceviz, 2019) Bu amaçlarla kişilerin e-posta hesaplarına istemedikleri mesajlarla meşgul edilmektedir. Karşılaşılma sıklığı nedeniyle günlük hayatta e-posta kullanıcılarını en çok sıkıntı duydukları siber saldırı türüdür. (Canbek ve Sarıoğlu, 2007)

Bu örnekler arttırılabilecek olup belli başlı siber saldırı türleri bu şekildedir.

2.2. Türk Hukukunda Bilişim Suçları

Bilişim suçları, doktorinde (Aköz, 2018), TCK sistematiğinde ve Yargıtay Ceza Genel Kurulu(YGCK) kararlarında doğrudan ve dolaylı bilişim suçları biçiminde bir ayrıma tabi tutulmaktadır. (Orta, 2015) Çalışmamızda, Türk Hukukunda bilişim suçları bu sistemetikte incelenecektir.

2.2.1. TCK'nın Bilişim Alanında Suçlar Bölümünde Düzenlenen Suçlar (Doğrudan)

2.2.1.1. Bilişim sistemine girme (m.243)

TCK'nın 243. maddesinde "Bilişim sistemine girme" suçu düzenlenmiştir. Maddede *"bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak girmek veya orada kalmak"* suç olarak düzenlenmiştir. Dördüncü fıkrada ise *"bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izlemek"* ayrı bir suç türü düzenlenmiştir. Bilişim sistemine girme suçuyla korunmakta olan hukuki değer bilişim sistemlerinin güvenliği, bilişim sisteminin verilerinin gizliliği olup korunan hukuki değer özel hayatın gizliliği, haberleşme hürriyeti ile yakından ilişkilidir.(Topçuoğlu, 2022) Kanunda açıkça belirtilmediğinden, failin cezalandırılabilmesi için erişilen bilişim sisteminin ayrı bir güvenlik önlemiyle korunuyor olması şartı aranmamalıdır.(Dülger, 2020) Madde 243'ün üçüncü fıkrasında bilişim sistemine hukuka aykırı olarak erişim sebebiyle sistemde yer alan bilgilerin zarara uğraması halinde cezanın artırılacağı ifade edilmiştir. Bu fıkrada ayrıcı bir nokta olarak, belirtilen neticenin gerçekleşmesinde failin kastının varlığı aranmamaktadır. Eğer failin bu fıkrada bahsedilen eylemi gerçekleştirme kastı varsa, TCK m. 244'te yer alan suç oluşacaktır. (Topçuoğlu, 2022)

2.2.1.2. Sistemi engelleme, bozma verileri yok etme veya değiştirme (m.244)

Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu TCK m. 244.'te düzenlenmiştir. Bu maddeye göre, *"(1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."*

244. maddede iki ayrı suçun düzenlendiğini görmekteyiz. Birinci fıkrada düzenlenen suçun oluşabilmesi için sistemin işleyişinin engellenmesi ya da bozulması gerekmektedir. Bu fıkrada düzenlenen suç neticeli suçtur. (Akbulut, 2016) Birinci fıkrada yer alan suçta, kullanıcılarının sistemin sorunsuz çalışmasındaki yararları korunmaktadır. İkinci fıkrada ise, veriler üzerinde tasarruf yetkisi olan kişilerin verilerin bozulmadan, engellenmeden müdahalesiz kullanmasındaki yararı korunmaktadır. (Akbulut, 2016)

2.2.1.3. Banka veya kredi kartlarının kötüye kullanılması (m.245)

TCK'da, bilişim sistemlerine karşı suçlar başlığı altında düzenlenen bir suç tipi olarak banka veya kredi kartlarının kötüye kullanılması hususu düzenlendiyse de ASSS'de bu suça karşılık gelen, bir bilişim suçu türü bulunmamaktadır. M. 245 her ne kadar TCK sistematiğinde bilişim alanında suçlar bölümünde yer almışsa da anılan suçla korunan hukuki değerin bireyin malvarlığı olması ve m. 245'te düzenlenen suçların ortak noktasının bilişim alanı olmaması sebebiyle, kanaatimizce, söz konusu maddenin bilişim alanında suçlar bölümünde değil malvarlığına karşı suçlar bölümünde düzenlenmesi gerekmektedir.(Aköz, 2018) Söz konusu

suç tipin bilişim alanında suçlar bölümünde yer alan suçlardan en çok işleneni olduğu ifade edilmektedir.(Aköz, 2018)

2.2.1.4. Yasak cihaz veya programlar

Yasak cihaz ve programlar başlıklı TCK 245/A hükmü şu şekildedir:

"Madde 245/A- (Ek: 24/3/2016-6698/30 md.)(1) Bir cihazın, bilgisayar programının, şifrenin veya sair güvenlik kodunun; münhasıran bu Bölümde yer alan suçlar ile bilişim sistemlerinin araç olarak kullanılması suretiyle işlenebilen diğer suçların işlenmesi için yapılması veya oluşturulması durumunda, bunları imal eden, ithal eden, sevk eden, nakleden, depolayan, kabul eden, satan, satışa arz eden, satın alan, başkalarına veren veya bulunduran kişi, bir yıldan üç yıla kadar hapis ve beşbin güne kadar adli para cezası ile cezalandırılır. "

ASSS'nin 6. maddesinde "Cihazların kötüye kullanımı" suçu düzenlenmiştir. Sözleşmenin ilgili maddesiyle uyumlu şekilde TCK'da anılan düzenleme yapılmıştır. Söz konusu suçta herhangi bir zarar neticesi öngörülmediğinden 'tehlike' suçu olarak nitelendirilmektedir. (Aköz, 2018)

2.2.1.5. Tüzel kişiler hakkında güvenlik tedbiri uygulanması

TCK'nın bilişim alanında suçlar bölümünde yer alan son düzenlemesi m.246'dır.

"Madde 246- (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur."

TCK m. 60 uyarınca bir suç sebebiyle tüzel kişiliğe güvenlik tedbiri uygulanması ancak kanunun ayrıca belirttiği durumlarda söz konusu olabilmektedir. Bilişim alanında suçlar bölümünde yer alan suçlarla ilgili olarak TCK. m.246 uyarınca tüzel kişilere güvenlik tedbiri uygulanabilecektir. (Aköz, 2018)

2.2.2. Bilişim Sistemleri Aracılığıyla İşlenebilen Suçlar (Dolaylı)

Teknolojik gelişmelerdeki büyük hız nedeniyle bilgisayar sistemlerinin hayatımızın her alanında kullanmaya başlamamız ve bir anlamda neredeyse hayatının kendisinin siber ortama

taşınması nerdeyse her suç tipinin siber ortamda ya da bilişim sistemleri aracılığıyla işlenmesini olanaklı hale getirmektedir. Bu bölümde üzerinde durulan suçlar günlük yaşamda sıklıkla karşımıza çıkmakta olan suçlardan oluşmaktadır.

2.2.2.1. TCK'da yer alan bilişim suçu dolaylı düzenlemeleri

2.2.2.1.1. Bilişim sistemlerinin kullanılması suretiyle hırsızlık

Bilişim suçları ve malvarlığına karşı suçlar arasında yakın bir ilişki vardır. Bilişim sistemleri kullanılması suretiyle suç işlenmesi halinde karşımıza korunan hukuki yararın malvarlığının korunması olduğu birçok suç tipi çıkmaktadır. TCK'nın Malvarlığına karşı suçlar başlıklı 10. bölümünde hırsızlık suçu düzenlenmiştir. 142. maddede hırsızlık suçunun nitelikli halleri sayılmış 142/2-e'de suçun *"bilişim sistemleri kullanılması suretiyle"* işlenmesi halinde cezanın arttırılması öngörülmüştür.

2.2.2.1.2. Bilişim sistemlerinin kullanılması suretiyle dolandırıcılık

TCK'nın Malvarlığına karşı suçlar bölümünde dolandırıcılık suçu düzenlenmiş m.158'de ise dolandırıcılık suçunun nitelikli halleri müstakil suç olarak düzenlenmiştir. Dolandırıcılık suçunun *"f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle"* işlenmesi halinde üç yıldan on yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunacağı ifade edilmiştir.

Sıklıkla karşılaşılan bilişim sistemleri aracılığıyla dolandırıcılık eylemlerinin bir örneği, 'phishing' (oltalama) yönteminin özelliklerini taşıyan, saldırganın bir kimseye ait sosyal medya, mail hesabının parolalarını elde ederek, bu kişi ile ilgili kimselere kendisini hesap sahibi gibi tanıtarak belli bir fayda sağlamasıdır. (Dülger,2015)

2.2.2.1.3. Haberleşmenin gizliliğini ihlal

TCK'nın "Kişilere Karşı Suçlar" kısmının dokuzuncu bölümü olan "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" bölümünde düzenlenen maddenin metni şu şekildedir:

“ *Madde 132- (1) Kişiler arasındaki haberleşmenin gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Bu gizlilik ihlali haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, verilecek ceza bir kat artırılır. (2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın hukuka aykırı olarak alenen ifşa eden kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. (Ek cümle: 2/7/2012-6352/79 md.) İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.”*

Haberleşmenin gizliliğini ihlal suçu Anayasa’nın 22. maddesiyle korunan haberleşme hürriyeti hakkında müdahale ile doğrudan ilişkindir. TCK’nın 132. maddesinde düzenlenen haberleşmenin gizliliğini ihlal suçu ASSS 3. maddesinde tanımlanan Yasadışı Müdahale suçuna karşılık gelmektedir. TCK m.132’de her türlü araçla yapılan haberleşme açısından bir koruma sağlanmaktadır. (Sevük, 2008) Gelişen teknoloji karşısında her türlü haberleşmenin ilgili maddenin korunması altında olacaktır. Telefon, e-posta, internet üzerinde her tür uygulama aracılığıyla yapılan haberleşme bu kapsamda ele alınmalıdır. Haberleşme içeriklerinin kayda alınması suretiyle gerçekleştirilmesi, bu suçun nitelikli halini oluşturmaktadır. (Sevük, 2008)

Doktrinde haberleşmenin gizliliğini ihlal suçu bilişim sistemine girmek suretiyle gerçekleştirildiyse, bilişim sistemine girme suçu (TCK m.243) ile haberleşmenin gizliliğini ihlal suçu (132/1) bakımından fikri içtimanın söz konusu olacağı ifade edilmektedir. (Sevük, 2008)

2.2.2.1.4. Kişiler arası konuşmaların dinlenilmesi kayda alınması

TCK’nın 133. maddesinde düzenlenmiştir.

“Madde 133- (1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Katıldığı aleni olmayan bir söyleşiyi,

diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur."

TCK'nın 133. maddesinde yüz yüzelik aranmakta olup bu suç ASSS'de düzenlenen "yasadışı müdahale" kapsamında değerlendirilmemektedir. (Akpek, 2015)

2.2.2.1.5. Kişisel verilerin hukuka aykırı ele geçirilmesi, kaydedilmesi

TCK sisteminde kişisel verilerin korunması amacına yönelik suçlar düzenlenmiştir. Kişisel Verilerin Korunması Kanunu'nun (KVKK) Suçlar başlıklı 17. maddesinde kişisel verilere ilişkin suçlar bakımından TCK'nın 135. ve 140. maddeleri arasındaki maddelerin uygulanacağı ifade edilmiştir. TCK'nın 136. maddesinde kişisel verilerin hukuka aykırı biçimde vermek ve ele geçirmek suç olarak düzenlenmiştir. 2019 yılında yapılan bir düzenlemeyle madde metnine ikinci fıkra eklenmiştir. İkinci fıkrada, Ceza Muhakemesi Kanunu'nun (CMK) 236. maddesinde ikincil mağduriyetin önüne geçmek amacıyla düzenlenen mağdurun tanık olarak dinlenmesi ve suçun etkisiyle psikolojisi bozulmuş çocuğun dinlenmesi esnasında alınan görüntü ve ses kaydının hukuka aykırı olarak ele geçirmek ve yaymak da suçun ağırlaştırıcı nedeni olarak düzenlenmiştir.

TCK'da düzenlenen ve bilişim sistemleri kullanılarak işlenen diğer suçlar şu şekilde sıralanabilir:

TCK Kişilerin Huzur ve Sukutunu Bozma (TCK m. 123), Israrlı Takip (123/A) ,Kumar oynanması için yer ve imkan sağlama, Cinsel Taciz, Hakaret (TCK m.125), Özel hayatın gizliliğini ihlal (TCK m.134), Haberleşmenin engellenmesi (TCK m.124), İntihara yönlendirme, tehdit, şantaj, müstehcenlik, göreve ilişkin sırrın açıklanması, suç delillerini yok

etme gizleme ve değiştirme (TCK m.281), gizliliğin ihlali (TCK m.285), ses ve görüntülerin kayda alınması (TCK m.286), Cumhurbaşkanına hakaret (TCK m.299), Devletin egemenlik alametlerini aşağılama (TCK m. 300), Türk Milletini, Türkiye Cumhuriyeti Devletini, Devletin kurum ve organlarını aşağılama (TCK m.301).Diğer Kanunlarda yer alan dolaylı bilişim suçları aşağıda açıklanacaktır.

2.2.3. Fikir ve Sanat Eserleri Kanunu Düzenlemeleri

ASSS m. 10 uyarınca telif hakkı ve bununla bağlantılı hakların ihlaline ilişkin suçlar düzenlenmiştir. ASSS sistematiğinde siber suçlar açıklanırken söz konusu maddeye detaylı şekilde değinilmiştir. FESK ilgili maddeler yönünden "özel ceza yasası" niteliği taşımaktadır. FSEK m. 71'de eseri, yapımı hak sahiplerinin izni olmaksızın, işleme, çoğaltma, değiştirme ve ses, görüntü nakline yarayan araçlarla kamuya açık hale getirmek, çoğaltılan ve işlenenleri yayımlamak, satmaya hazır hale getirmek depolamak suç olarak düzenlenmiştir. Maddenin 6. fıkrasında da eserin yapımın tanınmış bir başkası adına çoğaltmak yaymak fiilleri suç olarak düzenlenmiştir. Bu kapsamda FSEK'te lisansız yazılım kullanma çoğaltma hakkının ihlali niteliğinde sayıldığından suç olarak düzenlenmektedir. Literatürde lisanssız yazılım kullanımı kavramı yerine yazılım korsanlığı kavramının kullanıldığı da görülmektedir. Fikri mülkiyet haklarının korunması tartışmalarında; fikri mülkiyet haklarının sıkı biçimde korunmasının üretkenliği sağlayan faktörler üzerindeki olumlu etkisi sayesinde ekonomik kalkınmayı kolaylaştırdığı savına karşı, sıkı fikri mülkiyet haklarının yoksul ülkelerin kalkınma sürecine çok zarar verdiği savı kullanılmaktadır (Asongu, 2021) 2020 yılı itibariyle ABD'de yazılım sektörünün, gayri safi yurt içi hasılaya 1,6 trilyon dolardan fazla katkı sağlamakta olduğu ve 14 milyon dolarlık yüksek ücretli işi desteklediği ifade edilmektedir. (The Software Alliance BSA, 2020) BSA, ekonomiye bu denli katkısı olan yazılım sektörünün paydaşları için iyi korunan fikri mülkiyet sisteminin önemini vurgulayarak; fikri mülkiyet haklarının, ticari markaların ve ticari sırların korunduğu iyi işleyen bir fikri mülkiyet sisteminin, yazılım geliştiricilerine

yatırım yapmaları ve yaratıcı, yenilikçi enerjilerini inovasyona harcamaları için önemli bir teşvik olduğu görüşündedir. (The Software Alliance BSA, 2020) Bu madde kapsamındaki lisansız yazılım kullanma suçuna ayrıca tartışma bölümünde detaylı biçimde değinilecektir.

FESK'in 72. maddesinde, kanunda sayılan hakların korunması amacıyla eser, yapım, yayımların kullanımının kontrolünü sağlamak amacıyla kullanılan erişim kontrolü ya da parola korumasını benzeri koruma önlemlerini etkisiz hale getirmeye yönelik ürün ve araçları üretmek, satmak ve pazarlamak suç olarak düzenlenmiştir. Söz konusu maddenin TCK 254/A Yasak Cihaz ve programlar maddesiyle aynı hukuki faydaya sahip olduğu bu bağlamda madenin kullanımının bugüne kadar görülmediği ve kaldırılması gerektiği yönünde görüşler bulunmaktadır.(Aköz, 2018)

Kanun Ek m. 4'te eser sahiplerinin bağlantılı hak sahiplerinin, kanundan doğan hakları, ses, görüntü nakline yarayan araçlarla içerik sağlayıcılar tarafından ihlal ediliyorsa önce içerik sağlayıcıya başvuru yapılarak içeriğin kaldırılması talep edileceği, 3 gün sonunda ihlal devam ediyorsa Savcılığa başvuru yapılarak hizmet sunan ISS'in ilgili içerik sağlayıcıya verdiği hizmetin durulması erişimin engellemesi istenebilecektir. Uygulamada sıkça başvurulan bir koruma tedbiridir. Hakim onayı olmaksızın erişim engelleme kararı uygulanması tartışmalıdır.(Aköz, 2018)

2.2.4. 5651 Sayılı Kanun Düzenlemeleri

Kanun, internet ortamında yapılan yayınların düzenlenmesine ve içerik, yer, erişim sağlayıcıların yükümlülüklerine ilişkindir. Kanun'un uygulama alanı özellikle erişimin engellenmesinde söz konusu olmaktadır. Kanun içerik, yer, erişim sağlayıcıların yükümlülüklerini detaylı biçimde düzenlemiştir. 5651 sayılı Kanun'da yapılan erişim ve yer sağlayıcıların yükümlülüklerine ilişkin kimi düzenlemeler AYM incelemesine tabi tutularak iptal edilmiştir. Bugüne kadar birçok kez değişiklik geçiren 5651 sayılı Kanun uygulamada sıklıkla başvurulan bir yasal düzenlemedir.

5651 sayılı Kanun sistematiğinde erişim engelleme koruma tedbiri olarak, idari tedbir olarak, kişisel başvuru üzerine verilebilmektedir. (Görkemli, 2015)

Kanun'un 8. maddesi uyarımca, TCK'da yer alan, m.84 İntihara yönlendirme, m.103/1 Çocukların cinsel istismarı, m. 190 Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma, m.194 Sağlık için tehlikeli madde temini, m.226 Müstehcenlik, m.227 Fuhuş, m.228 Kumar oynanması için yer ve imkân sağlama suçları, 25/7/1951 tarihli ve 5816 sayılı Atatürk Aleyhine İşlenen Suçlar Hakkında Kanunda yer alan suçlar, 7258 sayılı Kanunda yer alan suçlar, 2937 sayılı Kanunu m.27/1 m.27/2'de yer alan suçların oluştuğu hususunda yeterli şüphe bulunan suçlarda içeriğin çıkarılması ve/veya erişimin engellenmesi kararı verilir.

M. 8/A'da ise yaşam hakkı ile kişilerin can ve mal güvenliğinin korunması, millî güvenlik ve kamu düzeninin korunması, suç işlenmesinin önlenmesi veya genel sağlığın korunması sebeplerinden en az birine bağlı olarak gecikmesinde sakınca bulunan hallerde başkanlığın içeriği çıkartma veya engelleme kararı verilebileceği 24 saat içinde hakim onayına sunulacağı hüküm altına alınmıştır.

M.9'da internet ortamında yapılan yayın içeriği nedeniyle kişilik haklarının ihlal edildiğini kişilerilerin içerik ve yer sağlayıcısına ulaşarak içeriğin kaldırılmasını isteyebileceği ya da Sulh Ceza Hakimliğine başvurabileceği hüküm altına alınmıştır. Bu başvuru kapsamında verilen engelleme kararı ESB'ye tebliğ edilmekle ESB tarafından uygulanmak üzere ilgili erişim sağlayıcılara gönderilmektedir.

M.9/A ise kişiler özel hayatın gizliliğini ihlal sebebiyle doğrudan BTK'ya başvurarak erişimin engellenmesini isteyebilir. Kurum bu talebi ESB'ye bildirir. Başvurucu 24 saat içinde talebini Sulh Ceza hakimine sunar. Hakim karar verir ve kararı BTK'ya gönderir. Aksi durumda karar kendiliğinden kalkar. Gecikmesinde sakınca bulanan hallerde BTK başkanın emri üzerine BTK tarafından engelleme yapılır ve karar hakim onayına sunulur.

Kanun'un 9. maddesi gereği, kişisel hakların ihlali halinde Sulh Ceza Hakimliği tarafından verilen içeriğin çıkarılmasını ve/veya erişimin engellenmesini kararlarını erişim sağlayıcılara göndermekle yükümlü Erişim Sağlayıcılar Birliği'nin (ESB) kuruluşu oldukça tartışmalı geçmiştir. 6518 sayılı Kanun'un 90. maddesiyle 5651 sayılı Kanun'a 6/A maddesi eklenerek Erişim Sağlayıcılar Birliği başlıklı madde eklenmiş bu maddede ESB ve görevleri tanımlanmıştır. 6518 Sayılı Kanun'un 100. maddesi ile 5651 sayılı Kanun'a Geçici 3. madde eklenerek ESB'nin kuruluşunun usulü düzenlenmiştir. Geçici 3. maddeye göre Kanun'un yayımından itibaren BTK tarafından yetkilendirilmiş erişim sağlayıcıların en az ¼'nün katılımıyla imzalanan Tüzüğün ESB'yi kurmak için BTK'ya sunulması gerekmekteydi. BTK'nın Tüzüğü uygun bulması halinde ESB'nin kuruluşunun gerçekleşeceği hüküm altına alınmıştı. Maddeye göre Birliğin kuruluşunun tamamlanamaması halinde yetkilendirilmiş tüm işletmecilere bir önceki takvim yılındaki net satışlarının yüzde biri oranında idari para cezası uygulanacağı düzenlenmekteydi. Kanun amacına uygun olarak, erişim engelleme konusunda sivil insiyatifi harekete geçirme çabası ile, BTK tarafından yetkilendirilmiş 116 işletmecinin katılım ve onayı ile bir Tüzük hazırlanarak BTK'ya sunulmuşsa da BTK'nın 30.04.2014 tarih ve 2014/DK-TİB/236 sayılı kararı ile, bu işletmecilerin Tüzüğü yerine 12 büyük işletmeci tarafından hazırlanan Tüzüğü onaylayarak ve ESB'yi faaliyete geçirilmiştir. Kuruluş sürecinin mevzuata aykırı gerçekleştirildiği, ESB'nin Kanunun aradığı şekil şartları ile esasa aykırı olarak kurulduğu gerekçesiyle kararının iptali talebiyle Serbest Telekomünikasyon İşletmecileri Derneği (TELKODER) tarafından Danıştay'da dava açılmıştır. Danıştay ESB'nin mevzuata aykırı kurulduğundan bahisle işlemin yürütmesinin durdurulması kararı vermiştir. Yürütmenin durdurulması kararına rağmen ESB faaliyetlerine devam etmiştir. Bunun üzerine 5651 sayılı Kanun'da 15.04.2015 tarihinde değişikliğe gidilerek 2. fıkraya *"bu maddenin yürürlük tarihi itibarıyla abonesi bulunan"* ifadesi eklenmiştir. Geçmişe etkili olacak şekilde yürürlüğe sokulan düzenlemeyi değerlendiren Danıştay İdari Dava Daireleri Kurulu Kanun'da yapılan

değişikliğin Anayasa'ya aykırı olduğu gerekçesiyle somut norm denetimi uygulanmak üzere 04.05.2015 tarihli kararıyla Anayasa Mahkemesi'ne başvurmuştur. Danıştay'ın AYM'ye başvuru kararında *"yürütmenin durudurulması kararı ile hukuka aykırılığı tespit edilmiş dava konusu işleme, anılan yargı kararlarını bertaraf edecek şekilde yasal dayanak oluşturulduğu anlaşıldığından anılan düzenlemeler Anayasa'nın 2. Maddesindeki hukuk devleti ilkesiyle bağdaşmamaktadır"* ifadelerine yer vermiş, devamında "*yasama erkinin kamu yararına değil, belli bir özel çıkarı korumaya, bunun için yargı kararlarını engellemeye yönelik kullandığını ortaya koymaktadır"* denilmiştir. AYM ise 19 Ekim 2016 tarihinde Resmi Gazetede yayımlanan kararıyla düzenlemeyi anayasaya aykırı bulmayarak ret kararı vermiş, yapılan düzenlemenin "önceki düzenlemeyi açıklayıcı, tereddütleri giderici" olduğunu ifade etmiştir. Sonuç olarak 116 erişim sağlayıcının imzası ile hazırlanarak BTK'ya sunulan tüzük kabul edilmemiş, 12 işletmeci imzası ile hazırlanan tüzük kabul edilerek ESB kurulmuştur. Kanunda öngörülen yeter sayıya ulaşmadan imzalanan tüzüğün kabulüne ilişkin işlemin yürütmesinin durdurulmasına karar verilmesinin ardından yasa koyucu tarafından geriye yürüyen kanun çıkartarak yargı kararlarını etkisiz kılmak suretiyle ESB'nin kurulmuş olduğu değerlendirilmektedir. Kanun'un güttüğü amaç doğrultusunda sivil insiyatifi harekete geçirme çabası ile 116 işletmeci bir araya gelerek ESB'yi kurmak istemişse de yargı kararına rağmen yapılan yasal değişiklikle bu mümkün olmamıştır. ESB'nin yalnızca erişim engelleme kararlarını uygulayan bir kuruluş olmasının ötesinde demokratik bir yapıyla erişim engelleme uygulamaları konusunda söz sahibi olabilecek bir kurum olması beklentisi karşılanamamıştır.

2.2.5. Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun (Dezenformasyon Yasası)

"Fake news"-"sahte haber" kavramı dünyada sosyal medyanın etkinliğini arttırmasından bu yana tartışılmakta ve kimi ülkelerde hukuki düzenlemelerin konusu olmaktadır. "Post Truth" dönemi olarak da adlandırılan sahte haberlerin sosyal yaşama yön vermeye başladığı dönemde

sahte haberlerin hukuksal düzenlemelere konu olması da hız kazanmıştır.(Gedikli, 2020) Sahte haberlerin dünyanın birçok yerinde siyasal amaçlar için kullanıldığı özellikle, Myanmar ve Endonezya'daki etnik gerilimleri alevlendirmek için kullanıldığına dair ciddi iddialar gündeme gelmiştir.(Akinwotu, 2005)

ASSS'de yalan haber kavramına yer verilmemiş olması ya da ek protokollerde düzenlenmemesi Sözleşmenin bu yönüyle eksik kaldığı eleştirilerini ortaya çıkarmıştır. (Smith ve Perry, 2021) Ocak 2018'de Avrupa Komisyonu, çevrimiçi dezenformasyonun yayılmasına karşı mücadele konusunda tavsiyede bulunmak üzere üst düzey bir uzmanlar grubu atamış ve bir Rapor yayımlanmıştır.(Ünal, 2021) Bu Raporda dezenformasyonla mücadele için şeffaflığın ve medya okuryazarlığının yaygınlaştırılmasının öneminin altı çizilmiştir vurgulanmıştır.(Ünal, 2021) BM İnsan Hakları Konseyinin 2021 yılında hazırladığı Rapor'da Dezenformasyon karmaşık, çok yönlü ve ciddi sonuçları olan bir olgu olduğu, insanların demokratik kurumlara olan güvenini yok edeceği, kamu bilgi rejimlerinin zayıf olduğu ve bağımsız araştırmacı gazeteciliğin kısıtlandığı yerlerde geliştiği, bireyleri güçsüzleştirerek, bilgi arama, alma, paylaşma ve görüş oluşturma özerkliklerini ellerinden alacağı ifadeleri yer almıştır. (Smith ve Perry, 2021)

Türkiye'de ise dezenformasyon yasası olarak bilinen "Basın Kanunu ile Bazı Kanunlarda Değişiklik Yapılmasına Dair Kanun" 18 Ekim 2022 tarih 31987 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Kanun'un 29. maddesi ile "*Halkı yanıltıcı bilgiyi alenen yayma*" başlığıyla TCK'ya 217/A maddesi eklenmiştir. Madde metni şöyledir:

"MADDE 217/A- (1) Sırf halk arasında endişe, korku veya panik yaratmak saikiyle, ülkenin iç ve dış güvenliği, kamu düzeni ve genel sağlığı ile ilgili gerçeğe aykırı bir bilgiyi, kamu barışını bozmaya elverişli şekilde alenen yayan kimse, bir yıldan üç yıla kadar hapis cezasıyla cezalandırılır. (2) Fail, suçu gerçek kimliğini gizleyerek veya bir örgütün faaliyeti çerçevesinde işlemesi hâlinde, birinci fıkraya göre verilen ceza yarı oranında artırılır."

Kanun'un 30. maddesiyle de CMK 286. maddesine ekleme yapılmıştır. Kanun'un 32.,33.,34.,35. maddesiyle 5651 sayılı Kanun'da değişiklik yapılmıştır.

Dezenformayon yasasının uygulanmasına ilişkin henüz ortaya çıkan bir örnek bulunmamakla toplumda yasanın nasıl uygulanacağı geniş kitlelerce tartışılmaktadır. Sahte haberlerin yarattığı tehlikenin önemi akılda tutulmakla, dezenformasyonla mücadele için ulusal yasama çalışmalarına ışık tutacak uluslararası düzenlemelerin önemli olduğunu, söz konusu uluslararası düzenlemelerde dezenformasyonla mücadele önlemlerine başvuruda hak ve özgürlükler bağlamındaki sınırların net biçimde belirlenmesi gerektiğini değerlendirmekteyiz. AB Raporu'nda da vurgulandığı üzere sahte haber ve dezenformasyonun geniş olumsuz etkilerinin önüne geçmenin yalnızca yasal düzenlemelerle değil, sivil toplum, akademi çalışmaları, medya-okur yazarlığının geliştirilmesi ve başkaca eylemler yoluyla farkındalık çalışmaları ile mümkün olabilecektir.

2.2.6. Elektronik İmza Kanunu Düzenlemeleri

Elektronik İmza Kanun'un imza oluşturma verilerinin izinsiz kullanımı başlıklı 16. maddesi elektronik imzanın sahibinin rızası dışında mza oluşturma verisi veya imza oluşturma aracını elde eden, veren, kopyalayan ve bu araçları yeniden oluşturanlar ile izinsiz elde edilen imza oluşturma araçlarını kullanarak izinsiz elektronik imza oluşturanların cezaladırılacağı hüküm altına alınmıştır. M. 17 ise sahte elektronik sertifika düzenlemek suç olarak düzenlenmiştir.

2.3. Siber Suçlarla İlgili Uluslararası Düzenlemeler

2.3.1. Siber Suçlarla Mücadelede Devletlerin İşbirliğini Düzenleyen Mevcut Bölgesel Anlaşmalar

Sınırların ötesindeki doğası gereği, siber suç olgusunun gelişimi, küresel açıdan ele alınması gereken özel bir örnektir.(Li, 2016) 1980'lerin başından beri OECD, BM, Avrupa Konseyi, G8 ve Interpol dahil olmak üzere uluslararası kuruluşlar tarafından yürütülen bir dizi

çalışma, siber suçların sunduğu zorluklar hakkında neredeyse küresel bir farkındalığa yol açmıştır. Küresel doğası göz önüne alındığında Siber suçlar açısından, etkili bir düzenlemeye ulaşılacaksa, ülkeler arasında asgari bir uyumun sağlanması oldukça önemlidir.(Clough, 2015) Bu bağlamda siber suçlar uluslararası düzenlemelerinde konusu olmuştur. ASSS en geniş katılımlı, en önemli uluslararası düzenlemedir. (Vatis, 2010)

2.3.1.1. Avrupa konseyi siber suçlar sözleşmesi

ASSS yasal bir belgenin ötesinde taraflardan yüzlerce uygulayıcının deneyimlerini paylaşmasına ve acil durumlar da dahil olmak üzere belirli durumlarda bu Sözleşmede öngörülen özel hükümlerin ötesinde işbirliğini kolaylaştıran ilişkiler oluşturmasına izin veren bir çerçeve olarak tanımlanmaktadır. (Convention on Cybercrime, b.t.) ASSS (Aynı zamanda Budapeşte Sözleşmesi-Budapest Convetion olarak da anılmaktadır.) Avrupa Konseyi Bakanlar Komitesi onayı ile 8.11.2001 tarihinde kabul edilmiştir. Devletlerin imzasına 23.11.2001 tarihinde Budapeşte'de açılan Sözleşme, 1.7.2004 tarihinde yürürlüğe girmiş olup bu alandaki ilk uluslararası sözleşmedir. Avrupa konseyi üyesi 47 ülke ve Avrupa Konseyi Üyesi olmayan 31 ülke olmak üzere toplamda 78 ülke tarafından imzalanmıştır. (Convention on Cybercrime, b.t.)

Türkiye sözleşmeyi 10.11.2010'da imzalamış ve 29.09.2014 tarihinde de yürürlüğe girmiştir.(Aliusta ve Bezer, 2018) Türkiye'nin sözleşmeye ilişkin 8 maddelik çekince ve beyanı bulunmaktadır. (Karakurt Eren, 2020) Türkiye'nin taraf olduğu bu Sözleşmenin adı, Sözleşmenin uygun bulunmasına ilişkin 6533 sayılı Kanunda ve ekinde Sanal Ortamda İşlenen Suçlar Sözleşmesi olarak ifade edilmiştir. Ancak Sözleşmenin İngilizce metinde Sözleşmenin adı "Convention on Cybercrime"olarak yer almaktadır. Yukarıda açıklandığı üzere Sözleşmede siber suçlar 4 kategoride ele alınmıştır.

1 Mart 2006'da, Sözleşme nefret söylemine ilişkin Ek Protokol yürürlüğe girmiştir. 21 Mayıs 2021 tarihi itibariyle Ek Protokol, 30 Avrupa Konseyi üyesi de dahil olmak üzere 33

ülke tarafından onaylanmıştır. Sözleşmeye ek elektronik delillerin ifşasına ilişkin ikinci Ek Protokol 12.05.2022 tarihinde imzaya açılmıştır.

2.3.1.2. Diğer bölgesel anlaşmalar

Siber suçlarla mücadelede devletlerin işbirliğini düzenleyen mevcut diğer bölgesel anlaşmalar şunlardır (Yatsyshyn, 2018)

- 21.12.2010 tarihli Bilgi Teknolojisi Suçlarıyla Mücadele Arap Sözleşmesi (Arab Convention on Combating Information Technology Offences)
- 01.06.2001 tarihli Bağımsız Devletler Topluluğu Üye Devletleri Arasında Bilgisayar Bağlantılı Suçlarla Mücadelede İşbirliği Anlaşması (Agreement On Cooperation Between The Member States Of The Commonwealth Of Independent States İn Combating Computer-Related Crime)
- 16.07.2009 tarihli Şanghay İşbirliği Örgütü'nün Uluslararası Bilgi Güvenliği Sağlama Alanında İşbirliği Anlaşması (Agreement On Cooperation in The Field Of Providing International Information Security Of The Shanghai Cooperation Organization)
- 27.06.2014 tarihli Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi (Convention on Cybersecurity and Protection of Personal Data of the African Union)

2.4. Regülasyon Kurumu Olarak Bilgi Teknolojileri İletişim Kurumu

2.4.1. Yapısı ve Görevleri

BTK, Türkiye'de telekomünikasyon sektörünü düzenleyip denetleyen kamu tüzel kişiliğine haiz, idarî ve mali bağımsızlığa sahip özel bütçeli bir "bağımsız idari otorite" ya da diğer bir adıyla "düzenleyici ve denetleyici kurum"dur. 2813 sayılı Telsiz Kanunu'nda değişiklik yapan 4502 sayılı kanun ile "Telekomünikasyon Kurumu" kurulmuş olup 5809 sayılı Elektronik Haberleşme Kanun (EHK) ile kurumun adı Bilgi Teknolojileri ve İletişim Kurumu olarak değiştirilmiştir.(Kuruluş BTK, 2017) BTK, Türkiye'nin ilk regülasyon kurumu olarak

bilinmektedir.(Kuruluş BTK, 2017) 2005 yılında Türk Telekom'un özelleştirilmesi ile telekomünikasyon sektöründe serbestleşme süreci başlamıştır. BTK da sektörün denetlenmesi ve düzenlenmesi adına regülasyon kurumu olarak görev yapmaya başlamıştır.

2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun m. 5 uyarınca Bilgi Teknolojileri ve İletişim Kurulu, Kurumun karar organıdır. Kurul Başkanı BTK'nın da başkanıdır. Kurum, ana hizmet, danışma ve yardımcı hizmet birimlerinden oluşur. Hizmet birimleri yönetmelikle belirlenir. Bilgi Teknolojileri ve İletişim Kurumu Teşkilât Yönetmeliği'nin 19. maddesinde ise BTK'nın hizmet birimleri tanımlanmıştır. 2813 sayılı Bilgi Teknolojileri ve İletişim Kurumunun Kuruluşuna İlişkin Kanun, Kurumun yasalarla verilen görevleri yerine getirmek ve yetkileri kullanmak üzere kurulmuş olduğunu ifade eder. EHK'nın 6. maddesi ise BTK'nın görev ve yetkilerini düzenler. BTK'nın görevleri; yetkilendirme koşullarını belirlemek ve yetkilendirme işlerini yürütmek, tüketici haklarını korumak, rekabetin kurallarını tesis etmek ve korunmak, siber güvenliği sağlanmak, denetleme, uzlaştırma ve bilgi teknolojileri işlemlerini gerçekleştirmek olarak sınıflandırılabilir. (Gürkan, 2013) Ulusal siber güvenliğin korunması da BTK'nın görevi kapsamında sayılmıştır. BTK'nın aynı zamanda iletişimi telekomünikasyon yolu ile istihbari ve önleme amaçlı dinlemek ve kayda almak yetki ve görevi vardır. BTK'nın istihbari ve önleme amaçlı iletişimin denetlenmesi yetkilerinden doğan bir "iletişim denetim merkezi" yapısı olduğunu da söylemek mümkündür. BTK'nın bu yapısı 5651 sayılı Kanun'dan doğan erişim engellemelere ilişkin görev ve yetkileriyle de perçinlenmektedir

2.4.2. BTK'nın Ulusal Siber Olaylara Müdahale Merkezi (USOM)

BTK bünyesinde 2013 yılında kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM) siber olaylara müdahale konusunda ulusal ve uluslararası koordinasyon çalışmalarını yürütmekle görevlidir. (USOM Hakkımızda, 2022) Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev Ve Çalışmalarına Dair Usul Ve Esaslar Hakkında Tebliği'nde ise USOM'un

görevleri belirlenmiştir. Kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (Kurumsal SOME)'ler, düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum ve kuruluşlar bünyesinde (Sektörel SOME)'ler oluşturulmuştur. USOM bir iletişim portalı üzerinden üzerinde Kurumsal ve Sektörel SOME'lerle iletişim kurmakta bu portal üzerinden siber olaylara ilişkin mesajlar gönderilmektedir. (USOM Hakkımızda, 2022) Zararlı yazılımlara ilişkin yapılan analizler hakkında USOM tarafından SOME'lere bilgi verilmekte SOME'lerin gereken önlemleri almaları talep edilmektedir. SOME'ler de gereken önlemleri aldıktan sonra USOM'a geri bildirimde bulunmaktadır. Özellikle ISS'lerin SOME'lerine yapılan bildirimlerde zafiyet ilişkisi tespit edilen ISS'e tahsisli ve/veya müşterileri tarafından kullanılan IP'lerden kamu kurumlarına ya da kritik sektörlere(enerji, haberleşme, ulaşım, su, elektronik haberleşme altyapılarına ait kurum ve kuruluş) ilişkin olanları varsa IP'lere karşılık gelen kuruluşun bilgisi istenmektedir. USOM ve SOME'ler arasındaki koordinasyonun işlerlikli halde bulunması ulusal siber güvenlik adına oldukça önemlidir. (T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, 2014)

2.4.3. BTK'nın Abone Verisi Toplama İşlemleri

BTK'nın elektronik haberleşme regülasyon kurumu olarak siber güvenliğin sağlanması, milli güvenlik amaçlarına yönelik kimi uygulamalarının hukukiliği zaman zaman tartışmaya açılmıştır. Özellikle BTK tarafından yetkilendirilmiş İnternet servis sağlayıcıları (ISS), sabit telefon hizmeti (STH) sunan işletmelerinden talep ettiği veriler hakkında bazı dönemlerde davalar açılmıştır. Siber güvenliğin sağlanması amacına yönelik uygulamalar zaman zaman kişisel verilerin korunması, haberleşmenin gizliliği, özel hayatın gizliliği ilkeleri ile çatışmıştır.

Bu uygulamalardan Bilgi Teknolojileri İletişim Kurulu'nun Abone Desen Yapısı Kurul kararı ve işletmecilerce toplanan ISS log verilerinin BTK'ya iletilmesine yönelik uygulamaları internet abonelerinin kişisel verilerinin ISS'ler aracılığıyla toplanarak BTK'ya aktarılması

hususunu içermektedir. (Eroğlu, 2022b) Trafik verilerin toplanması ve BTK'ya aktarılması hususunda Türk Hukuk mevzuatı açısından trafik verilerinin toplanması ve BTK'ya aktarılmasını öngören yasal düzenlemeler AYM (AYM, 2015a) (AYM, 2015b) ve Danıştay (TC Danıştay, 2019) tarafından iptal edilmiştir. Ayrıca, Türkiye'deki tüm internet kullanıcılarının trafik verilerinin toplanmasını öngören BTK işleminin, ASSS'de değinilen kriterler bulunmaksızın "genel ve ayrım gözetmeksizin" toplanmak istenmesi demokratik bir toplumda meşru sayılamayacağından hukuka uygunluk koşullarını da taşımadığı değerlendirilmektedir.

2.5. Araştırmanın Katılımcıları Muhakame Süjeleri ve Bilişim Sektörü Çalışanlarına İlişkin Tanımlamalar

2.5.1. Hakim, Savcı ve Avukat

Ceza muhakemesinde süje, muhakeme sürecinde yalnız başına iş ve işlem gerçekleştirebilen kişidir. (Centel ve Zafer, 2006). Ceza muhakemesinde muhakeme süjeleri savunma makamı, iddia makamı ve yargılama makamıdır. Ceza muhakemesinde süjelik şahıs ve makam olarak söz konusu olabilmektedir. (Centel ve Zafer, 2006). Çalışmamızda muhakeme süjeleri ile kast edilen bireysel süjelik değil müdafii (avukatlar), savcılar ve hakimlerdir.

1136 sayılı Avukatlık Kanunu'nun 1. ve 2. maddesine göre avukatlık, her türlü hukuki mesele ve anlaşmazlıkların adalet ve hakkaniyete uygun olarak çözümlenmesini ve hukuk kurallarının tam olarak uygulanmasını yargı organları nezdinde sağlayan, yargının kurucu unsurlarından olan bağımsız savunmayı serbestçe temsil eden, kamu hizmeti ihtiva eden serbest bir meslektir. Türkiye Cumhuriyeti'nde avukat olabilmek için hukuk fakültesinden mezun olarak avukatlık stajını tamamlayarak staj bitim belgesi almış bulunmak gereklidir.

Cumhuriyet savcıları ise, suç işlendiğini iddia ederek başsavcılık dına yargı makamına başvuran toplumsal iddia makamındaki süjedir. (Centel ve Zafer, 2014) Hakim ise

mahkemelerin bağımsızlığı ve hakimlik teminatı esaslarına göre görev yapan, görevinde bağımsız, Anayasaya, kanuna ve hukuka uygun olarak vicdani kanaatine göre hüküm veren yargılama makamını işgal eden kişidir. Hakim ve Savcı Kanunu'nun 8. ve 13. maddesine göre Türkiye'de adli yargı hâkim ve savcı olabilmek için, hukuk fakültesinden mezun olmak, hukuk mesleklerine giriş sınavında başarılı olmak, hakim savcı yardımcılığı süresince başarılı olmak gerekmektedir. İdari yargıda hakim olmak için, hukuk fakültesinden mezun olmak veya hukuk bilgisine programlarında yeterince yer veren siyasal bilgiler, idari bilimler, iktisat ve maliye alanlarında en az dört yıllık yüksek öğrenim yapmış idari yargı ön sınavında başarılı olmak ve her iki yargı türü için de hakim savcı yardımcılığı süresince başarılı olmak şartları gerekmektedir.

2.5.2. Bilişim Sektörü Çalışanı

Araştırmamıza katılan bilişim sektörü çalışanı deyiminden bilişim iş kolunda çalışan uzmanlardır. Araştırmamıza katılan bilişim sektörü çalışanları katılımcıların bildirdikleri görev ve pozisyonlara göre 6 gruba ayrılmıştır. İlk grupta network/sistem/güvenlik/altyapı/teknik/bilgi işlem departmanı çalışanları, ikinci grupta proje yöneticisi/iş analisti/iş geliştirmeci/data analisti/çözüm mimarı unvanı ile çalışanlar, 3. grupta mali/idari işler/hukuk-regülasyon/insan kaynakları departmanında çalışanlar/üst düzey yönetici olarak çalışanlar, 4. grupta çalışanlar yazılım departmanı çalışanları, 5. grup satış/pazarlama/üretim departmanı çalışanları, 6. grup diğer çalışanlar olarak gruplandırılmıştır. Bu başlıkta araştırmamızın katılımcısı olmuş veya belli başlı bilişim sektörü çalışanlarının iş tanımlarından söz edilecektir.

Bilişim sektöründe insan kaynakları istihdamında en göze çarpan özellik kişilerin her zaman ilgili pozisyona özgülenmiş bir lisans eğitimi almış olma zorunluluğu olmamasıdır. Bilişim de yaşanan hızlı gelişmeler yeni meslek gruplarını da ortaya çıkarmakta fakat bu uzmanlığı karşılayacak lisans eğtitimleri aynı hızda yaygınlaşamamaktadır. Sektörel insan

kaynağı açığı çoğu zaman belli başlı yetkinliklere sahip olunmasıyla kapanmaya çalışılmaktadır. Bunlardan en göze çarpanı yazılım uzmanlığıdır. Yazılım uzmanı, yazılım programlarını tasarlayan kişidir. (Yazılım uzmanı, 2022) Yazılım uzmanları için beklenen lisans eğitimi çoğunlukla yazılım mühendisleri, bilgisayar mühendisliği gibi görünse de bilgisayar ya da yazılım mühendisi olmayıp belli başlı sertifikalara sahip, belli başlı programları kullanabilen, çok katmanlı sistem ve yazılım mimarisi konularına hakim kimselerin yazılım uzmanı olabilmesi söz konusudur. Network uzmanı, bir çok farklı bilgisayar ve cihazlardan oluşan ağın aynı anda uyumlu çalışmasını sağlamasında görev almaktadır. (Network uzmanı, 2022) Network uzmanları genellikle bilgisayar mühendisliği, elektronik ve haberleşme mühendisliği ile enformatik gibi lisans bölümlerinde mezun olmaktadır. (Network uzmanı, 2022) Sistem uzmanı sunucuların çalışmasına yönelik işlemlerden sorumlu olarak çalışan kişidir. Bilgisayar ve diğer mühendisliklerden mezun olan kişiler olabileceği gibi gerekli sertifikalara sahip kişililer de sistem uzmanı olarak görev yapabilmektedir. (Sistem Uzmanı, 2022) Ağ ve siber güvenlik uzmanı (araştırmamızdaki katılımcıların çoğu kısaca kendini güvenlik uzmanı olarak tanıtmıştır), elektronik bilgi sisteminin korunmasını sağlayan kişidir. Aynı zamanda bu görevdeki kimseler "etik hacker" "eğitimli hacker" görevlerini de üstlenmektedir. Ağ ve Siber Güvenlik Uzmanlığı için başta bilgisayar olmak üzere, yazılım mühendisliği, matematik, veri analizi, bilgisayar teknolojileri gibi konularda eğitim alınmalıdır. (Siber güvenlik uzmanı, 2022) Özellikle yönetsel düzeyde görev yapan İngilizce'de "chief ınformation security officers" olarak tanımlanan kısacaca "CİSO" olarak adlandırılan "baş bilgi güvenliği sorumlusu" verilerinin korunması, altyapı ve varlıkların kötü niyetli kimselerden korunmasını denetleyen bir yönetici pozisyonudur. (Ciso, 2022) CİSO'ların yaptıkları işin önemi gün geçtikçe artmaya devam etmektedir.(Interpol, 2022) Altyapı sorumlusu/teknisyeni, çoğunlukla elektronik haberleşme sektöründe fiber optik ağların kurulum, bakım onarım, test süreçlerinden sorumlu saha personelleridir. Bilgi işlem uzmanı, sadece teknoloji şirketleri değil

teknolojiyi kullanan veya büyük miktarda veri akışının gerçekleştiği işletmelerde ve kamu kurumlarında yer alan bir pozisyondur. Kurumun bilgisayar ve yazılım ağlarını korumak için kullandığı teknoloji sistemlerini kurmak, yönetmek ve sorunlarını gidermekten sorumludur. (It specialist, 2022) Çoğunlukla bilgisayar teknolojisine ilişkin ön lisans bölümlerinden mezun olmak bu pozisyonda çalışmak için yeterlidir. Proje yöneticisi, bir projenin başından sonuna kadar olan süreci yöneten personel ve müşterilerle iletişim kurması, kararlar alması ve projenin programa uygun ilerlemesini izlemesi sağlayan kişidir. (Proje yöneticisi,2022)

2.6. Siber Psikoloji ve Siber Suçlarla İlişkili Temel Kavramları

Siber Psikoloji: Siber psikoloji; insanların interneti nasıl ve ne için kullandıklarını, internet, teknoloji, bilgisayar kullanıcıları ile olan tüm etkileşimimizi, aynı zamanda teknolojinin davranışlarımıza ve ruh halimize olan etkilerini incelemektedir. (Öztürk ve Derin, 2020) Siber psikolojinin çıktılarından siber suçlara ilişkin birçok tanımın yapılmasında faydalanılmaktadır. Siber suçlarda faillerinin motivasyonlarının belirlenmesi ve mağdurların, siber mağduriyetlerinin nedenlerinin belirlenmesi siber psikolojinin inceleme alanına girmektedir. Bu açıdan siber suçların anlaşılması bağlamında destek alınan bir bilim dalı olarak siber psikoloji önemli bir yer tutmaktadır. Öztürk ve arkadaşlarına göre, siber suçların psikolojik dinamikleri, öncelikle klinik psikolojinin temel yaklaşımları çerçevesinde değerlendirildikten sonra adli ve siber psikolojinin temel yaklaşım ve kuramlarıyla desteklenmelidir.(Öztürk ve ark., 2020) Bu başlıkta tartışma bölümünde siber suçlarla ilişkilendirilecek bazı siber psikoloji kavramları açıklanacaktır.

Siber Uzam: Siber uzam, bireysel ve kolektif insan zihninin bir izdüşümü olarak psikolojik bir alan olarak tanımlanmaktadır. (Suler, 2017) Suler'e göre hem bilinçli hem de bilinçsiz olarak ekran portallarımızın diğer tarafındaki bu alanı psikolojimizin bir uzantısı, kişiliklerimizi, inançlarımızı ve yaşam tarzlarımızı yansıtan bir bölge olarak algılarız.(Suler, 2017) Geleneksel teoriler bağlamında, dijital dünya benzersiz bir psikolojik alandır çünkü

bilginin işlenmesinde benzeri görülmemiş bir hız sağlayan bilgisayarlar tarafından aracılık edilir ve bu da geleneksel medyada mümkün olmayan çok çeşitli deneyimler ve etkileşim düzeyleri ile sonuçlanır. (Suler, 2017) Bilgisayar tarafından oluşturulan farklı alanların tasarımı, benlik ve ötekinin öngörülen tezahürünü ve etkileşimini şekillendirmekte, dolayısıyla bu alanların psikolojik etkisini belirlemektedir. (Suler, 2017)

Siber Travma ve Siber Disososiyasyon: Siber suç mağdurları mağduriyetleri sonucu siber travmaya maruz kalırlar. (Öztürk ve Derin, 2020) Siber travma karşısında bireyin uygun tepki verememesi onu travmatize eder.(Öztürk ve Derin, 2020) *"Disosiyasyon normalde bütünlük içerisinde olan bilinç, bellek, kimlik ya da çevreyi ve kendini algılama işlevlerinden en az birinde kopma, kesinti, ya da değişmeler olmasıdır."*(Şar, 2014) Öztürk'e göre, gelişen teknoloji ve siber uzamın kötüye kullanımı siber dissosiyasyona neden olmaktadır.(Öztürk, 2020) Öztürk'e göre siber dissosiyatif yaşantılar, teknoloji çağının *"narsistik, teşhirci, izleyici, rekabetçi ve merhametsiz doğasında"* kişilerin ruh dünyasını koruyan bir savunma mekanizması olarak gelişmekte zamanla siber dissosiyasyona dönüşmektedir.(Öztürk, 2020) Dijital çağda bir siber hayatı bir de gerçek hayatı bulunan olan kişi, bağımlı ruhsal yapısıyla siber hayatı ile gerçek hayatı arasında ikircikli bir duruma sürüklenir ve kişi hem çocukluk çağı travmalarının etkisiyle hem de *"yakın zamanlarda yaşadığı aktüel ve siber travmalarının etkisiyle bu iki yaşamı dissosiye etmeye başlar".* Yani kişi, siber yaşantısı ile gerçek yaşantısını birleştiremeyerek, bölünür. (Öztürk, 2020). Kişinin siber kimliğinin bir alter kişilik olarak yaşamını kontrol etmesi söz konusu olmaktadır. (Öztürk, 2020) Bu durum siber disosiyasyon olarak nitelenmektedir.

İnternet Bağımlılığı: Sağlıklı internet kullanımı kullanıcının herhangi bir rahatsızlık hissetmeden, uygun bir zaman aralığında, sadece kullanıcının hedefine ulaşmak için internet kullanımı olarak tanımlanmaktadır. (Davis, 2001) İnternet bağımlılığı internetin sağlıksız, aşırı veya uygun olmayan biçimlerde kullanımı olarak tanımlanmaktadır. (Arısoy, 2009). İnternet

bağımlılığı Amerikan Psikiyatri Birliği'nin ruhsal bozuklukları sınıflandırma sistemi olan DSM-5'te yer almamakta fakat internet oyun bağımlılığı DSM-5 3. bölümünde tanımlanmaktadır. (Bozkurt ve ark 2016) İnternet bağımlılığı ise bugüne kadar diğer bağımlılık tanı kriterleri uyarlanmak suretiyle tanımlanmaya çalışılmıştır. (Young, 1996; Tao ve ark 2010; Goldberg, 1996) İnternet bağımlılığı ve internettin aşırı kullanımı ilişkili fakat aynı kavramlar değillerdir. Araştırmamızda internet bağımlılığı ölçülmemekte sadece katılımcıların problemli internet davranışları ölçülmeye çalışılmaktadır.

2.7. Siber Suçların Değerlendirmesinde Rutin Aktiviteler Teorisi

Lawrence Cohen ve Marcus Felson tarafından oluşturulmuş, diğer kriminolojik yaklaşımların aksine suçluya değil suç olayına yoğunlaşan teoridir. (Dolu, 2011) Suç fırsatlarının insanların rutin faaliyetlerine bağlı olarak ortaya çıkmaktadır. Bu teoriye göre suç aslında bir fırsat olayıdır. (Dolu, 2011) Cohen ve Felson'a 2. Dünya Savaşı sonrası gelişmiş Batı ülkelerindeki artan suç oranlarının nedenini, bireysel ve toplumsal yaşamda meydana gelen sosyokültürel, ekonomik, teknolojik gelişmeler ve yaşam tarzlarındaki değişmelerle bağlantılı olduğunu ifade etmiştir. (Cohen ve Felson, 1979) Suçu açıklamak için zamansal ve mekanı işaret eden durumsal faktörler üzerinden yoğunlaşılması gerektiğini ifade etmişlerdir. Cohen ve Felson'a göre, mağdurlar ve suçlular arasında da zamansal ve mekânsal açıdan simbiyotik bir ilişki bulunmaktadadır. (Cohen ve Felson, 1979) Suçu oluşturan unsurların 1-motive olmuş suçlu 2-uygun hedef 3-uygun hedefi koruyacak koruyucuların yokluğu unsurlarından oluştuğu; bu üç unsurun bir arada bulunması halinde suçun oluşacağını savunmuşlardır. (Dolu, 2011) Daha sonra bu faktörlerin yanına bir de dördüncü faktör "tutucular" eklenmiştir. (Felson, 1986) Uygun hedefi çekici kılan unsurların; hedefin görünürlüğü, hedefin değerli ve arzu edilebilir olması, hedefin suça karşı korumasız olması,

hareket kabiliyeti, hedefin müsait ve erişilebilir olması olduğu ifade edilmektedir. (Birceviz, 2019)

Motive olmuş suçlu, (potansiyel mağdurlar/uygun hedef ve koruyucuların yokluğu unsurları ile birlikte) suça yol açan nedensel üçlüden biridir. Siber suçlarda da bu görülebilir bir gerçekliktir.(Li, (2017a) Rutin aktiviteler teorisinin siber suçları açıklama kapasitesi üzerine teorik bir değerlendirme Yar tarafından yapılmıştır. (Yar, 2005). Motive olmuş suçlular (hackerlar, dolandırıcılar, siber korsanlar, siber takipçiler), uygun hedeflerin varlığı (tehlikeye açık bilgisyar sistemleri, kişisel bilgiler, çevirimiçi ödeme satın alma hizmetleri), koruyucular (forum moderatörleri, ağ yöneticileri, güvenlik duvarları, antivirüs programları, sanal özel ağlar, kimlik doğrulama sistemleri gibi) bağlamında aktüel dünyaya benzer unsurların siber uzamda da siber suçları açıklamaya elverişli olabileceği ifade edilmiştir. (Yar, 2005). Fakat hedefin uygunluğuna ilişkin unsurların değerlendirilmesi noktasında aktüel dünyada anlamlı olan kimi unsurların siber mağduriyeti açıklamak için doğrudan aktarımının mümkün olmadığı ifade edilmektedir. Bu sebeple teorinin siber suçları ölçme kapasitesinin geniş veri setleri ile test edilmesi gerekliliği ifade edilmiştir. (Leukfeldt ve Yar, 2016) Marcum ve arkadaşları, istenmeyen cinsel içerikli materyal, istenmeyen cinsel olmayan taciz ve istenmeyen cinsel talep suçları yönünden uygun hedef unsurlarından görünürlük (anlık mesajlaşma ve sosyal ağ siteleri gibi çevrimiçi etkinlikler), erişilebilirlik (sosyal ağ sitelerinde paylaşılan on iki bilgi türü) ve suça karşı koruyucuları (bilgisayar kullanırken odada bulunan kişiler, ebeveynler tarafından filtreleme veya izleme yazılımı kullanımı) incelemiş ve motive olmuş suçlulara maruz kalmayı ve hedef uygunluğunu artıran davranışlara katılmanın, ölçülen üç tür mağduriyet olasılığını artırdığı sonucuna varmıştır. (Marcum ve ark., 2010)

Leukfeldt ve Yar (Leukfeldt ve Yar, 2016) büyük bir veri seti ile rutin aktiviteler teorsinin siber suçları açıklama yeteneğini incelemiştir. Uygun hedef unsurları olan (görünürlük, erişilebilirlik, değer, eylemsizlik, hedefin korunuruluğu) 6 siber suç tipi yönünden

ele almıştır. Araştırma sonuçlarına göre görünürlük altı siber suçun tamamında rol oynamaktadır. Çevrimiçi rutin faaliyetler siber suç mağduriyetinde açıkça bir rol oynamaktadır. Değer ve koruyuculuk değişkenleri düşük sayıda anlamlı değişkene sahip bulunmuştur. Her üç siber suç kategorisinde de mağdurların genellikle çevrimiçi ortamda daha fazla zaman geçirmiş olmalarıdır. Bu durum özellikle "internet kullanım sıklığı" ve hedefli tarama ve doğrudan iletişim gibi günlük faaliyetler değişkenlerine yansımaktadır. Dolayısıyla daha kapsamlı bir şekilde çevrimiçi olmak, çevrimiçi suçların mağduru olma şansını artırmaktadır.

Li, rutin aktiviteler bağlamında motive olmuş siber saldırganların yasadışı siber aktivitelerindeki ilk sırada yer alan motivasyonları şu başlıklar altında incelemiştir: Serbest bilgi akışının sağlanması, egonun özgür ifadesini gerçekleştirmek, teknik meydan okumayı kabul etmek, yeni bilgi arama merakı, sistem güvenliği ve esnekliğinin test edilmesi, siber uzayda maceraya atılmak, programlama becerilerini uygulama ve gösterme, potansiyel olarak savunmasız cihazlara karşı geçici saldırılar, nefretten hacklemek, finansal kazanç elde etmek veya ödemeden kaçınmak için bilgisayar korsanlığı, eğitim nedenlerinden dolayı, yasadışı faaliyetlerin ortaya çıkması, akademik sonuçları değiştirmek için bilgisayar korsanlığı, taciz ve cinayet amaçlı motivasyon, siyasi hareketin harekete geçirilmesi, siber savaş başlatmak, bilgisayarlaşma karşıtı eylemler için motive olmuş, siber robin hoodlar, haksız rekabetle motive olmuş, tuzak pazarlamanın yürütülmesi, kendini savunma motivasyonuyla, eğlence için bilgisayar korsanlığı, istihdamla ilgili motivasyonlar, hacker topluluğu için hackleme, bilgi sistemlerinde bulunan kanıtların yok edilmesi, cinsel amaçlı kötüye kullanım, sapkınlık karşıtı, karmaşık güdüler, belirsiz sebepler, (motive olmamış ancak) psikolojik depresyondan etkilenmiş olanlar (Li, 2017a). Hackerlar siber uzamda sık karşılaştığımız motive olmuş suçlu tiplerindendir. Hackerların siber suç motivasyonları birçok farklı biçimde açıklanmıştır. Jordan ve Taylor, hackerlar arasında altı ortak tutum bulunduğunu ifade etmiştir. Bunlar; bağımlılık, merak, bilgi arama heyecanı, erişim yeteneği, akran tanıma ve güvenlik boşluklarını tespit

etmedir. (Jordan ve Taylor, 1998) Kiger ve arkadaşları, hacker motivasyonlarının para, eğlence, ego, amaç, sosyal gruplara giriş ve statü olduğunu ifade etmiştir. (Kiger ve ark., 2004) Fötinger ve Ziegler için hackerlarda temelde aşağılık duygusu bulunmaktadır. (Fötinger ve Ziegler, 2004) Maiwald, hacker motivasyonlarının meydan okuma arayışı, açgözlülük ve kötü niyet ya da vandalizm olmak üzere üç gruba ayrıldığı sonucuna varmıştır. (Maiwald, 2003)

3. GEREÇ VE YÖNTEM

3.1. Araştırmanın Modeli ve Deseni

Bu araştırma, bilişim sektörü çalışanları ile hukuk sektörü çalışanları arasında bilişim suçu farkındalığı, kişisel siber güvenliği sağlama ve problemli internet kullanımı ilişkisini genel tarama modeli türlerinden biri olan ilişkisel tarama modeli kullanarak araştırmaktadır. İlişkisel tarama modelinin seçilme sebebi ise iki grup arasındaki değişimi birlikte inceleyebilmektir. Çalışmada iki farklı sektör çalışanlarının kişisel siber güvenlik, problemli internet kullanım ölçekleri ve bilişim suçu farkındalığı açısından anlamlı farklılık olup olmadığı incelenmiştir.

3.2. Evren ve Örneklem

Araştırmanın evreni Türkiye'de çalışan bilişim sektörü çalışanları, hakim, savcı ve avukatlardır. Araştırmanın örneklemini ise Kasım 2019-Temmuz 2022 yılları arasında ulaşılan 230 bilişim sektörü çalışanı 270 hakim/savcı/avukat olmak üzere toplam 500 kişi oluşturmaktadır. Araştırma sorular yöneltmek suretiyle sistemli veri toplama tekniği olarak bilinen online soru formu cevaplandırılması yöntemi ile gerçekleştirilmiştir. Online soru formu bir soru cevaplandırılmadan diğer soruya geçilemeyecek şekilde dizayn edilmiş olup katılımcıların hepsinin her soruyu yanıtlayarak soru formunun tamamlaması sağlanmıştır.

3.3. Veri Toplama Araçları

Kişisel Bilgi Formu: Yapılan araştırmanın amacına dönük olarak, araştırmacı ve tez danışmanı tarafından literatürde konuya ilişkin yayınlarda kullanılan anket formları kriter alınarak (Budak, 2015; Hille ve ark., 2015) hazırlanmıştır. Katılımcıların demografik özellikleri, çalıştıkları kurumdaki unvanları, interneti kullanım tutumları ve internet üzerinde yaşadıkları mağduriyetler gibi bilgilerin alınabileceği bir soru formudur. Soru formu 23 maddeden oluşmaktadır.

Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu: Bilişim suçu düzenlemelerine ilişkin katılımcıların bilişim suçu farkındalıklarını belirleme amacıyla hazırlanan bir soru formudur. Soru formu 8 maddeden oluşmaktadır.

Problemli İnternet Kullanımı Ölçeği: Üç faktörlü, 33 maddelik internetin sağlıklı ve sağlıksız olarak kullanım düzeylerini ortaya koymayı amaçlayan ölçektir. (Ceyhan ve diğerleri, 2007) Birinci faktör 17 maddeden oluşmakta, "internetin olumsuz sonuçları" olarak adlandırılmaktadır. İkinci faktör ise 10 maddeden oluşmakta, "sosyal fayda/sosyal rahatlık" olarak adlandırılmaktadır. Üçüncü faktör ise ve 2'si olumlu (tersten puanlanan) ve 3'ü olumsuz anlamda ifadelendirilen toplam 5 maddeden oluşmaktadır. Bu faktör ise "aşırı kullanım" olarak adlandırılmaktadır. Beşli likert tipinde "Tamamen uygun", "Oldukça uygun", "Biraz uygun", "Nadiren uygun" ve "Hiç uygun değil" seçeneklerinden oluşan bir derecelendirme ölçeği kullanılmıştır. İç tutarlık için bakılan Cronbach alfa değeri PİKÖ için 0.96 bulunmuştur. Alt testlerin iç tutarlığına bakıldığında; Aşırı Kullanım 0.60; Sosyal Fayda/Rahatlık 0.90; İnternetin Olumsuz Sonuçları 0.96 bulunuştur. Ölçek güvenilir bulunmuştur. Faktör analizinin yeterliliğini sınamak üzere yapılan analiz sonucunda KMO (Kaiser Meyer Olkin) değeri 0.97 bulunmuş örneklemin yeterli olduğu görülmüştür. Üç faktörlü yapıdaki ölçeğin varyansın %60.69'unu açıkladığı belirlenmiştir. Madde 6, 7 ve 10 olması gereken gruplarda yer almaması sebebiyle analizden çıkarılmıştır.

Kişisel Siber Güvenliği Sağlama Ölçeği: İnternet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik 5 faktörlü ve 25 maddeden oluşan bir ölçektir. (Erol ve ark.,2015) Ölçekte 10 maddeden oluşan 1. faktör "Kişisel Gizliliği Koruma", 4 maddeden oluşan 2. faktör "Güvenilmeyenden Kaçınma", 5 maddeden 3. faktör "Önlem Alma", 2 maddeden oluşan 4. faktör "Ödeme Bilgilerini Koruma" ve 4 maddeden oluşan 5. faktör ise "İz Bırakmama" olarak ifade edilmiştir. İç tutarlık için bakılan Cronbach alfa değeri KSGS için 0.76 bulunmuştur. Alt testlerin iç tutarlığına bakıldığında; Kişisel Gizliliği Koruma 0.76;

Güvenilmeyenden Kaçma 0.78; Önlem Alma 0.80; Ödeme Bilgilerini Koruma 0.90; İz Bırakmama 0.48 bulunuştur. Ölçek güvenilirdir. Faktör analizinin yeterliliğini sınamak üzere yapılan analiz sonucunda KMO değeri 0.79 bulunmuş örneklemin yeterli olduğu görülmüştür. Beş faktörlü yapıdaki ölçeğin varyansın %57.54'ünü açıkladığı belirlenmiştir. Madde 7 ve 8 olması gereken gruplarda yer almaması sebebiyle analizden çıkarılmıştır.

3.4. Araştırma Prosedürü

Katılımcılara Kasım 2019-Temmuz 2022 yılları arasında çevirimiçi platformlar üzerinden ulaşılmıştır. Çalışmaya katılımcıları dahil etme sürecinde e-posta yoluyla, LinkedIn ve e-posta uygulamaları kullanılmış olup araştırmacı tarafından Google Documents sitesinde hazırlanan online anket formu bu çalışmada kullanılmıştır. Veriler toplam 500 kişiden toplanmıştır.

3.5. İstatistiksel Analiz

Verilerin istatiksel analizi SPSS (Statistical Package for Social Sciences) 25.0 programı ile yapılmıştır. Anketlerden aktarılan veriler üzerinden öncelikle katılımcıların demografik yapılarının anlaşılması için tanımlayıcı istatistikler yapılmıştır.

Normallik varsayımı değişkenlerin çarpıklık ve basıklık değerlerinin -1.5 ile +1.5 aralığında olduğu durumlarda kabul edilmiştir. Ayrıca histogram grafikleri de incelenmiştir.(Tabachnick ve Fidell, 2013; Field, 2013) Analizler normallik varsayımının sağlanması durumunda bağımsız gruplar t testi (Ort±SS gösterimi ile ortalama ve standart sapmalar verilmiştir), aksi durumda ise Mann Whitney-U testi (tablolarda sıra ortalamaları verilmiştir) kullanılarak incelenmiştir. Meslekler ile sorular arasındaki ilişki ise Ki-Kare analizi ile incelenmiştir. PİKÖ ve KSGS ölçekleri arasındaki ilişki korelasyon analizi ile incelenmiştir. Normallik varsayımının sağlanması durumunda Pearson(p); sağlanmaması durumunda ise Spearman (s) korelasyonu kullanılmıştır.

4. BULGULAR

4.1. Ölçekler Arasındaki İlişki

Tablo I. Ölçekler Arasındaki İlişki

		PİKO Aşırı Kullanım	PİKO Sosyal Fayda	PİKO İnternetin Olumsuz	PİKO
KSGS Kişisel Gizliliği Koruma	r	-,266p	-,270 s	-,337 s	-,343 s
	p	,000	,000	,000	,000
KSGS Önlem Alma	r	-,172s	-,017 s	-,157 s	-,130 s
	p	,000	,705	,000	,003
KSGS İz Bırakmama	r	-,101s	-,069 s	-,139 s	-,120 s
	p	,024	,125	,002	,007
KSGS	r	-,259s	-,194 s	-,360 s	-,326 s
	p	,000	,000	,000	,000
KSGS Güvenilmeyenden Kaçma	r	-,138 s	-,141 s	-,231 s	-,206 s
	p	,002	,002	,000	,000
KSGS Ödeme Bilgilerini Koruma	r	-,110 s	-,092 s	-,244 s	-,187 s
	p	,014	,040	,000	,000

PİKO:Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği

KSGS Kişisel Gizliliği Koruma ile PİKO ve tüm alt ölçekleri arasında negatif yönlü zayıf bir ilişki vardır($p<0.001$). KSGS Önlem Alma ile PİKO Aşırı Kullanım, PİKO İnternetin olumsuz Yanları ve PİKO arasında negatif yönlü oldukça zayıf bir ilişki vardır($p<0.001;p<0.001;0.003$). KSGS İz Bırakmama ile PİKO Aşırı Kullanım, PIKO İnternetin olumsuz Yanları ve PİKO arasında negatif yönlü oldukça zayıf bir ilişki vardır($p=0.02;0.002;0.01$). KSGS ile PİKO Aşırı Kullanım, PİKO İnternetin olumsuz Yanları ve PİKO arasında negatif yönlü zayıf bir ilişki vardır($p<0.001$). KSGS ile PİKO Sosyal Fayda arasında negatif yönlü oldukça zayıf bir ilişki vardır. KSGS Güvenilmeyenden Kaçma ile PİKO Aşırı Kullanım ve PİKO Sosyal Fayda arasında negatif yönlü oldukça zayıf bir ilişki ($p=0.002$); KSGS Güvenilmeyenden Kaçma ile PİKO İnternetin olumsuz Yanları ve PİKO arasında ise negatif yönlü zayıf bir ilişki vardır($p<0.001$). KSGS Ödeme Bilgilerini Koruma ile PİKO Aşırı

Kullanım, PİKO Sosyal Fayda, PİKO arasında negatif yönlü oldukça zayıf bir ilişki ($p=0.01;0.04;p<0.001$); KSGS Ödeme Bilgilerini Koruma ile PİKO İnternetin olumsuz Yanları arasında ise negatif yönlü zayıf bir ilişki vardır($p<0.001$).

4.2. Mesleklere Göre Analizler

4.2.1. Mesleklerle Demografik Değişkenler Arasındaki İlişki

Tablo II. Katılımcıların Mesleklerine Göre Demografik Özellikleri

	Hukukçu N(%)	**Bilişim Sektörü Çalışanı N (%)**	**İstatistik**
Erkek	102(37.8)	191(83)	x^2= 104.90 p<0.001
Kadın	168(62.2)	39(17)	x^2= 104.90 p<0.001
Bekar	128(47.4)	114(49.6)	
Evli	142(52.6)	116(50.4)	
İnternette Geçirilen Süre Günde 2 saat ve daha az	40(14.8)	14(6.1)	x^2=42.63 p<0.001
İnternette Geçirilen Süre Günde 2-4 saat	131(48.5)	65(28.3)	x^2=42.63 p<0.001
İnternette Geçirilen Süre Günde 4 saatten fazla	99(36.7)	151(65.7)	x^2=42.63 p<0.001
Lisanssız Yazılım Kullanma **Evet**	178(65.9)	132(57.4)	x^2=3.84 p=0.051
Lisanssız Yazılım Kullanma **Hayır**	92(34.1)	98(42.6)	x^2=3.84 p=0.051
Siber Mağduriyete Uğrama Durumu **Evet**	83(30.7)	44(19.1)	
Siber Mağduriyete Uğrama Durumu **Hayır**	187(69.3)	186(80.9)	
Erişime Engelli Sitelere Girme **Evet**	192(71.1)	164(71.3)	
Erişime Engelli Sitelere Girme **Hayır**	78(28.9)	66(28.7)	
Erişim Engelli Sitelerin İzlenmesi **Evet**	137(50.7)	141(61.3)	
Erişim Engelli Sitelerin İzlenmesi **Fikrim Yok**	100(37)	50(21.7)	
Erişim Engelli Sitelerin İzlenmesi **Hayır**	33(12.2)	39(17)	
Yaş Ortalaması	32.66±7.03	33.5±9.37	
Toplam	270	230	

Mesleklerle demografik değişkenler arasındaki ilişki Tablo II'de incelenmiştir. Katılımcıların, %54'ü avukat veya hâkim veya savcı olup (bundan sonra bu gruptan "hukukçu" olarak bahsedilecektir), %46'sı bilişim sektörü çalışanıdır. Bilişim sektörü çalışanlarının 91'i Network/Sistem/Güvenlik/Altyapı/Teknik/Bilgi İşlem Departmanı çalışanı, 21'i Proje Yöneticisi/İş Analisti/İş Geliştirmeci/Data Analisti/Çözüm Mimarı Unvanı ile çalışanlar, 47'si Mali/İdari İşler/Hukuk-Regülasyon/İnsan Kaynakları departmanında çalışanlar/Üst Düzey Yönetici olarak çalışanlar, 31'i Yazılım Departmanı Çalışanları, 19'u Satış/Pazarlama/Üretim Departmanı çalışanları, 14'ü de diğer çalışanlardır.

Katılımcılara gerekli olduğunu düşündüklerinde hakkında erişim engelleme kararı olan sitelere girip girmeyecekleri sorulduğunda hukukçuların %71'i, bilişim sektörü çalışanlarının %71,3'ü bu sitelere girdikleri yanıtını verdiği belirlenmiştir. Aynı zamanda hukukçuların %50,7'si, bilişim sektörü çalışanlarının ise % 61,3'ü erişime engelli sitelerin izlendiğini düşündüğünü belirtmiştir. Bilişim sektörü çalışanlarının %65,9'nun lisanssız yazılım kullanırken, hukukçuların %57,4'nün lisanssız yazılım kullandığı belirlenmiştir. (Tablo II).

Katılımcılara internet ortamında en az kez bir mağduriyetle karşılaşıp karşılamadıkları sorulduğunda hukukçu katılımcıların %30,7'si, bilişim sektörü çalışanlarının %44'ü en az bir kez siber mağduriyetle karşılaştıklarını bildirmişlerdir. Siber mağduriyet bildiren katılımcıların mağduriyetleri sonucunda ne yaptıkları sorulduğunda katılımcıların %29,1'i şikayetçi olmuş (adli-idari makamlara ya da ilgili kuruma şikâyet edenler), %10'u şikayetçi olmuş (adli-idari makamlara ya da ilgili kuruma şikâyet edenler) ve aynı zamanda önlem almış, %44,5'i sadece önlem almış, %16,4'nün hiçbir şey yapmamış olduğu belirlenmiştir.

Tablo III. İnternete Bağlanılan Yere İlişkin Tablo

Değişkenler	Hukukçu N (%)	Bilişim Sektörü Çalışanı N (%)
Sadece Evden	3(1.1)	14(6.1)
Sadece İşten	3(1.1)	1(0.4)
Sadece Cep Telefonundan	13(4.8)	2(0.9)
Evden ve Cep Telefonundan	23(8.5)	16(7)
Evden ve İşten	6(2.2)	4(1.7)
İşten ve Cep Telefonundan	1(0.4)	4(1.7)
Evden, İşten ve Cep Telefonundan	152(56.3)	145(63)
Evden, İşten, Cep Telefonundan ve Diğer Kamuya Açık Kaynaklardan	68(25.2)	45(19.6)
Toplam	270	230

Katılımcılara internete bağlanma yerleri sorulmuş olup hukukçu katılımcıların %4.8'i sadece cep telefonundan, %56.3'ü evden, işten ve cep telefonundan bağlandığını belirtmişlerdir. Bilişim sektöründe çalışan katılımcılardan evden, işten ve cep telefonundan cevabını verenlerin oranı %63'tür. İnternete evden, işten ve cep telefonundan ve kamuya açık kaynaklardan bağlandığı cevabını veren hukukçu katılımcıların oranı %25.2 iken bu oran bilişim sektörü çalışanlarında %19.6'dır. (Tablo III)

Tablo IV. Katılımcıların Bilgisayarlarında Kullandığı İşletim Sistemi

Değişkenler	Hukukçu N (%)	Bilişim Sektörü Çalışanı N (%)
Check Point	0	1(0.4)
Linux	1(0.4)	6(2.6)
Linux ve Windows	0	3(1.2)
Mac OS	18(6.7)	22(9.6)
Windows	251(93)	197(85.7)
Toplam	270	230

Katılımcılara bilgisayarlarında hangi işletim sistemini kullandıkları sorulmuş hukukçu katılımcıların %93'ü, bilişim sektörü katılımcıların %85,7'si Windows cevabını vermiştir.

Tablo V. Katılımcıların Akıllı Telefonlarında Kullandığı İşletim Sistemi

Değişkenler	**Hukukçu N (%)**	**Bilişim Sektörü Çalışanı N (%)**
Android	121(44.8)	128(55.7)
BlackBerry OS	2(0.7)	0
Ios	146(54.1)	102(44.3)
Windows Phone	1(0.4)	0
Toplam	270	230

Katılımcılara akıllı telefonlarında hangi işletim sistemini kullandıkları sorulmuş hukukçu katılımcıların %54.1'ü, bilişim sektörü katılımcıların %44.3'ü Ios cevabını vermiştir. (Tablo V)

Tablo VI. Katılımcıların Akıllı Telefonlarında Kullandığı Uygulamalar

Değişkenler	**Hukukçu (%)**	**Bilişim Sektörü Çalışanı Frekans(%)**
Bankacılık	221(81.9)	206(89.6)
Sosyal Medya	231(85.6)	193(83.9)
Alışveriş	156(57.8)	144(62.6)
Oyun/Müzik	158(58.5)	137(59.6)
İletişim	252(93.3)	210(91.30)
Yemek	54(20)	66(28.70)
Sağlık	66(24.4)	82(35.65)
Haber	106(39.26)	110(47.83)
Seyahat	73(27.04)	84(36.52)
İş	146(54.07)	157(68.26)
Diğer	5(1.85)	2(0.87)

Katılımcıların akıllı telefonlarında kullandıkları uygulamalar Tablo VI'de gösterilmiştir. Hukukçu ve bilişim sektörü çalışanları arasında en çok kullanılan uygulamanın iletişim uygulamaları olduğu tespit edilmiştir. Onları sosyal medya ve bankacılık uygulamalarının izlediği görülmektedir.(Tablo VI)

Tablo VII. Sosyal Medya Platformları Kullanım Oranları

Değişkenler		N	%
Sosyal medya platformları kullanım oranları	Instagram	391	78,2
	Facebook	158	31,6
	LinkedIn	227	45,4
	Twitter	284	56,8
	Youtube	359	71,8
	Pinterest	45	9
	Snapchat	13	2,6
	Diğer	27	5,4

Katılımcıların kullandıkları sosyal medya uygulamaları Tablo VII'de incelenmiştir. En çok kullanılan sosyal medya uygulamasını Instagram olup onu Youtube izlemektedir.

Tablo VIII. Ölçeklerin Mesleklere Göre Karşılaştırılması

Değişkenler	Hukukçu (270)	Bilişim Sektörü Çalışanı (230)	İstatistik
PİKÖ Aşırı Kullanım	12.25±3.51	11.53±3.53	t=2.27 **p=0.02***
KSGS Önlem Alma	17.12±4.47	20.67±3.88	t= -9.52 **p<0.001***
KSGS Ödeme Bilgilerini Koruma	235.67	267.91	U=27045 Z=-2.79 **p=0.01****
KSGS İz Bırakmama	7.12±2.14	7.69±2.10	t= -2.99 **p= 0.003***
KSGS TOTAL	72.40±9.62	76.74±9.89	t=-4.97 **p<0.001***
BSF	267.81	230.18	U= 26377.5 Z= -2.97 **p= 0.003****

* t testi; ** Whitney-U testi; PİKÖ: Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği; BSF: Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu.

Ölçeklere göre meslekler arasında farklılık olup olmadığı Tablo VIII'da incelenmiştir. Bu kısımda meslek grupları arasında ölçekler açısından farklılık olup olmadığı incelenmiştir. Normallik varsayımının sağlanması durumunda bağımsız gruplar t testi (Ort±SS gösterimi ile ortalama ve standart sapmalar verilmiştir), aksi durumda ise Mann-Whitney U testi (tablolarda

sıra ortalamaları verilmiştir) (Field, 2013) kullanılmıştır.Araştırma konusu meslek gruplarının; PİKÖ Aşırı Kullanım ortalamaları, KSGS Önlem Alma ortalamaları, KSGS Ödeme Bilgilerini koruma sıra ortalamaları, KSGS İz Bırakmama ortalamaları, KSGS Total ortalamaları ve BSF sıra ortalamaları karşılaştırıldığında gruplar arasında anlamlı farklılık olduğu tespit edilmiştir (Tablo VIII). PİKÖ Aşırı Kullanım ortalamalarına göre hukukçular ile bilişim sektörü çalışanları arasında anlamlı farklılık vardır($p=0.02$). Hukukçuların Aşırı Kullanım ortalamaları bilişim sektörü çalışanlarından daha fazladır. KSGS Önlem Alma ortalamalarına göre meslek grupları arasında anlamlı farklılık vardır($p<0.001$). Bilişim sektörü çalışanlarının Önlem Alma ortalamaları hukukçulardan daha fazladır. KSGS Ödeme Bilgilerini koruma sıra ortalamalarına göre meslek grupları arasında anlamlı farklılık vardır($p=0.01$). Bilişim sektörü çalışanlarının Ödeme Bilgilerini Koruma puanları hukukçulardan daha fazladır. KSGS İz Bırakmama ortalamalarına göre meslek grupları arasında anlamlı farklılık vardır($p=0.003$). Bilişim sektörü çalışanlarının İz Bırakmama ortalamaları hukukçulardan daha yüksektir. KSG ortalamalarına göre meslek grupları arasında anlamlı farklılık vardır($p<0.001$). Bilişim sektörü çalışanlarının KSGS ortalamaları hukukçulardan daha yüksektir. BSF sıra ortalamalarına göre meslek grupları arasında anlamlı farklılık vardır($p=0.003$). Bilişim sektörü çalışanlarının BSF puanları hukukçulardan daha düşüktür.

4.3. Bilişim Sektörü Çalışanları ve Hukukçular İçin Analizler

Bu bölümde bilişim sektörü çalışanları ve hukukçular arasında sorulara verdikleri cevapların ölçeklere göre değişip değişmediği incelenmiştir. Analizler hukukçu ve bilişim sektörü gruplarına göre ayrı ayrı yapılmıştır. Sonuçlar Tablo IX, Tablo X, Tablo XI, Tablo XII, Tablo XIII ve Tablo XIV'te verilmiştir.

4.3.1. Cinsiyetler Arasında Ölçeklere Göre Karşılaştırma

Tablo IX. Bilişim Sektörü Çalışanlarında Cinsiyetler Arasında Ölçeklere Göre Karşılaştırma

	Cinsiyet		İstatistik
	Erkek (191)	**Kadın (39)**	
PİKÖ Sosyal Fayda/Sosyal Rahatlık	121.76	84.82	U=2528 Z=-3.17 **p=0.002****
KSGS Önlem Alma	21.13±3.44	18.46±5.04	t=3.15 **p=0.003***
KSGS Ödeme Bilgilerini Koruma	119.30	96.87	U=2998 Z=-2.26 **p=0.02****
KSGS	77.57±9.39	72.69±11.34	t=2.85 **p=0.01***

* t testi; ** Whitney-U testi; PİKÖ: Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği

Bilişim sektörü çalışanları grubunda, KSGS Önlem Alma, KSGS Total ortalamalarına göre; PİKÖ Sosyal Fayda, KSGS Ödeme Bilgilerini Koruma sıra ortalamalarına göre cinsiyetler arasında anlamlı farklılık bulunmuştur ($p<0.05$). Buna göre erkeklerin PİKÖ Sosyal Fayda, KSGS Önlem Alma, KSGS Ödeme Bilgilerini Koruma ve KSGS puanlarının, kadınlardan daha fazla olduğu gözlemlenmiştir. Diğer ölçeklere göre erkek ve kadın arasında herhangi bir farklılık bulunamamıştır($p>0.05$).Hukukçu grubunda ise cinsiyetler arasında ölçek ortalamalarına/sıra ortalamalarına göre anlamlı farklılık bulunamamıştır ($p>0.05$).

4.3.2. Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma

Tablo X. Hukukçular İçin Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma

	Medeni Hal		İstatistik
	Bekar (128)	Evli (142)	
PİKÖ Aşırı Kullanım	13.12±3.72	11.46±3.13	t=3.93 **p<0.001***
PİKÖ Sosyal Fayda/Sosyal Rahatlık	161.39	112.16	U=5774 Z=-5.19 **p<0.001****
PİKÖ İnternetin Olumsuz Sonuçları	163.17	110.56	U=5546 Z=-5.54 **p<0.001****
PİKÖ	163.26	110.48	U=5535 Z=-5.55 **p<0.001****
KSGS Güvenilmeyenden Kaçma	122.45	147.27	U=7417 Z=-2.70 **p=0.01****
KSGS Ödeme Bilgilerini Koruma	125.69	144.35	U=7832 Z=-2.13 **p=0.03****
KSGS	70.92±10.02	73.72±9.07	t=-2.41 **p=0.02***

* t testi; ** Whitney-U testi; PİKÖ: Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği.

Hukukçu grubunda PİKÖ Aşırı Kullanım ve KSGS ortalamalarına göre evli ve bekar bireyler arasında anlamlı farklılık bulunmuştur ($p<0.05$). PİKÖ Aşırı kullanım ortalamaları bekârlarda daha fazla iken aksine KSGS ortalamaları evlilerde daha fazladır. PİKÖ Sosyal fayda, İnternetin Olumsuz Sonuçları, PİKÖ, KSGS Güvenilmeyenden Kaçma ve Ödeme Bilgilerini Koruma puanları medeni durumlar arasında farklılık göstermektedir($p<0.05$). PİKÖ Sosyal Fayda, İnternetin Olumsuz sonuçları ve PİKÖ puanları bekârlarda daha fazla iken tersine KSGS Güvenilmeyenden kaçma ve Ödeme Bilgilerini Koruma puanları evlilerde daha fazladır.

Tablo XI. Bilişim Sektörü Çalışanları İçin Medeni Durumlar Arasında Ölçeklere Göre Karşılaştırma

	Medeni Hal		İstatistik
	Bekar (114)	**Evli(116)**	
PİKÖ Aşırı Kullanım	12.46±3.54	10.61±3.30	t=4.11 **p<0.001***
PİKÖ Sosyal Fayda/Sosyal Rahatlık	129.48	101.76	U=5018 Z=-3.17 **p=0.002****
PİKÖ	129.26	101.97	U=5043 Z=-3.11 **p=0.002****
KSGS Güvenilmeyenden Kaçma	104.18	126.63	U=5321 Z=-2.63 **p=0.02****
KSGS Önlem Alma	104.04	126.76	U=5305 Z=-2.61 **p=0.01****
KSGS İz Bırakmama	7.27±2.29	8.10±1.81	t=-3.05 **p=0.003***
KSGS	75.11±10.57	78.34±8.94	t=-2.50 **p=0.01***

* t testi; ** Whitney-U testi; PİKÖ: Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği.

Bilişim sektörü çalışanları grubunda, PİKÖ Aşırı Kullanım, KSGS İz Bırakma ve KSGS ortalamalarına göre evli ve bekâr bireyler arasında anlamlı farklılık vardır($p<0.05$). PİKÖ Aşırı Kullanım ortalamaları bekâr bireylerde evlilerden daha yüksektir. Fakat KSGS İz bırakma ve KSGS ortalamaları evlilerde daha fazladır. PİKÖ Sosyal Fayda, PİKÖ, KSGS Güvenilmeyenden Kaçma ve KSGS Önlem Alma sıra ortalamalarında gruplar arasında anlamlı farklılık vadır($p<0.05$). PİKÖ Sosyal Fayda ve PİKÖ puanları bekârlarda daha yüksek iken tersine, KSGS Güvenilmeyenden kaçma ve KSGS Önlem Alma puanları evlilerde daha fazladır.

4.3.3. Anti-Virüs Programı Kullanım Durumlarını Ölçeklere Göre Karşılaştırma

Tablo XII. Bilişim Sektörü Çalışanları Ve Hukukçular Arasında Anti Virüs Programı Kullanımı Durumunun Karşılaştırılması

Bilişim Sektörü Çalışanlarında Antivirüs Programı Kullanımı (230)				**Hukukçularda Antivirüs Kullanımı (270)**		
	Antivirüs Programı Kullanımı		İstatistik	Antivirüs Programı Kullanımı		İstatistik
	Evet(165)	**Hayır(65)**		**Evet(176)**	**Hayır(94)**	
KSGS Önlem Alma	131.65	74.50	U=2697.5 Z=-5.91 p<0.001	18.63±4.02	14.31±3.89	t=8.51 **p<0.01***
KSGS TOTAL	77.91±9.88	73.77±9.35	t=2.90 p=0.004	74.07±9.70	69.27±8.69	t=4.02 **p<0.001***

* t testi; KSGS: Kişisel Siber Güvenliği Sağlama Ölçeği.

Bilişim sektörü çalışanları ve hukukçular arasında antivirüs programı kullanımı durumunun ölçeklere göre karşılaştırması incelenmiştir. Bilişim sektörü çalışanları grubunda KSGS Önlem alma ve KSGS Total ortalamaları/sıra ortalamaları antivirüs programı kullanan bireylerde daha fazladır (Tablo XII). Hukukçu grubunda KSGS Önlem alma ve KSGS ortalamaları anti virüs programı kullanan bireylerde fazladır (Tablo XII).

4.3.4. İnternette Geçirilen Süreler Arasında Ölçeklere Göre Karşılaştırma

Tablo XIII. Hukukçularda ve Bilişim Sektörü Çalışanlarında İnternette Geçirilen Süreler Arasında Ölçeklere Göre Karşılaştırma

Hukukçularda internette geçirilen süreler arasında ölçeklere göre karşılaştırma				**Bilişim sektörü çalışanı internette geçirilen süreler arasında ölçeklere göre karşılaştırma.**		
	İnternette Geçirilen Süre		İstatistik	İnternette Geçirilen Süre	İstatistik	
	Günde 4saat ve daha az(171)	**4 saatten fazla(99)**		**Günde 4 saat ve daha az (79)**	**4 saatten fazla (151)**	
PİKÖ Aşırı Kullanım	11.70±3.31	13.19±3.66	t=-3.43 p=0.001	10.38±3.23	12.13±3.55	t=-3.67 **p<0.001***
PİKÖ Sosyal Fayda/Sosyal Rahatlık	124.43	154.62	U=6572 Z=-3.07 p=0.002	96.28	125.56	U=4446 Z=-3.18 **p=0.001****
PİKÖ İnternetin Olumsuz Sonuçları	126.84	150.45	U=6984 Z=-2.40 p=0.02	99.05	124.11	U=4665 Z=-2.72 **p=0.01****
PİKÖ Total	124.37	154.73	U=6984 Z=-3.08 p=0.002	94.27	126.61	U=4287.5 Z=-3.50 **p<0.001****

* t testi; ** Whitney-U testi; PİKÖ:Problemli İnternet Kullanım Ölçeği

Hukukçularda ve bilişim sektörü çalışanlarında internette geçirilen süreler arasında ölçeklere göre karşılaştırma incelenmiştir. Bilişim sektörü çalışanları grubunda internette günde 4 saatten fazla zaman geçiren bireylerin PİKÖ Aşırı Kullanım, Sosyal Fayda, İnternetin Olumsuz Sonuçları ve PİKÖ Total puanları günde 4 saatten daha az vakit geçiren bireylerden daha yüksektir. Hukukçu grubunda internette günde 4 saatten fazla zaman geçiren bireylerin PİKÖ Aşırı Kullanım, Sosyal Fayda, İnternetin Olumsuz Sonuçları ve PİKÖ Total puanları günde 4 saatten daha az vakit geçiren bireylerden daha yüksektir. KSGS ve alt ölçeklerine göre internette geçirilen süreler değişmediğinden anlamlı sonuç elde edilememiş tabloya eklenmemiştir.

4.3.5. Lisanssız Yazılım Kullanım Durumlarını Ölçeklere Göre Karşılaştırma

Tablo XIV. Hukukçularda Ve Bilişim Sektörü Çalışanlarında Lisanssız Yazılım Kullanım Durumlarını Ölçeklere Göre Karşılaştırma

Hukukçularda lisanssız yazılım kullanımı				**Bilişim sektörü çalışanlarında lisanssız yazılım kullanımı.**		
	Lisanssız Yazılım Kullanımı		İstatistik	Lisanssız Yazılım Kullanımı		İstatistik
	Evet(178)	**Hayır(92)**		**Evet (132)**	**Hayır(98)**	
PİKÖ Aşırı Kullanım	12.81±3.58	11.15±3.12	t=3.95 **p<0.001***	11.87±3.46	11.07±3.60	t=1.70 p=0.09
PİKÖ Sosyal Fayda/Sosyal Rahatlık	144.61	117.88	U=6567 Z=-2.68 p=**0.01****	122.14	106.56	U=5592 Z=-1.76 P=0.08
PİKÖ İnternetin Olumsuz Sonuçları	150.27	106.93	U=5559.5 Z=-4.33 **p<0.001****	125.22	102.41	U=5185.5 Z=-2.58 **p=0.01****
PİKÖ Total	150.06	107.33	U=5596 Z=-4.26 **p<0.001****	124.36	103.57	U=5299 Z=-2.34 **p=0.02****
KSGS Kişisel Gizliliği Koruma	125.79	154.28	U=6460.5 Z=-2.85 **p=0.004****	106.24	127.97	U=5246 Z=-2.46 **p=0.01****
KSGS Güvenilmeyenden Kaçma	126.61	152.71	U=6605 Z=-2.69 **p=0.01****	11.07	121.47	U=5883 Z=-1.20 p=0.23
KSGS Önlem Alma	16.52±4.18	18.29±4.79	t=-3.15 p=**0.002****	112.64	119.36	U=6090 Z=-0.76 p=0.45
KSGS Ödeme Bilgilerini Koruma	126.49	152.93	U=6584.5 Z=-2.87 **p=0.004****	115.89	114.97	U=6416.5 Z=-0.12 p=0.90
KSGS Total	70.70±9.13	75.68±9.73	t=-4.16 **p<0.001***	75.87±9.06	77.91±10.84	t=-1.51 p=0.13
BSF	127.06	151.83	U=6686 Z=-2.55 p=0.01**	109.72	123.28	U=5705.5 Z=-1.55 p=0.12

* t testi; ** Whitney-U testi; PİKÖ:Problemli İnternet Kullanım Ölçeği; KSGS:Kişisel Siber Güvenliği Sağlama Ölçeği; BSF: Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu.

Hukukçularda ve bilişim sektörü çalışanlarında lisanssız yazılım kullanım durumlarını ölçeklere göre karşılaştırılması incelenmiştir. Bilişim sektörü çalışanlarında PİKÖ İnternetin Olumsuz Sonuçları ve PİKÖ Total puanları lisansız yazılım kullananlarda fazla iken tersine

KSGS Total puanları kullanmayanlarda daha fazladır. Hukukçularda PİKÖ Aşırı Kullanım, Sosyal Fayda, İnternetin olumsuz sonuçları ve PİKÖ puanları lisansız yazılım kullananlarda daha fazladır. KSGS Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçma, Önlem Alma, Ödeme Bilgilerini Koruma, BSF ortalamalarına/sıra ortalamalarına göre gruplar arasında anlamlı farklılık bulunmuştur ($p<0.05$). Lisanssız yazılım kullanmayan bireylerin KSGS Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçma, Önlem Alma, Ödeme Bilgilerini Koruma, BSF puanları daha fazladır. 298 katılımcı "lisanssız yazılım kullanmak suçtur" önermesine kesinlikle katıldığını bildirmiştir.

4.4. Siber Mağduriyete İlişkin Analizler

Katılımcılara *"şimdiye kadar internet ortamında mağdur edecek en az bir olayla karşılaştınız mı?"* diye sorulmuş, hukukçu katılımcıların 83'ü (%30.7) bilişim sektörü çalışanlarının 44'ü (%19.1) mağdur olduğunu bildirmiştir. (Tablo II) Siber mağduriyet bildiren katılımcılara kaç kez internet ortamında mağduriyet yaşadıkları sorulmuş, siber mağduriyete uğradığını bildiren katılımcıların 11 kişisi 1 kez, 27 kişisi 1'den fazla kez siber mağduriyete uğradığını bildirmiştir. Siber mağduriyet bildiren katılımcıların mağduriyetleri sonucunda ne yaptıkları sorulduğunda katılımcıların %29,1'i şikayetçi olmuş (adli-idari makamlara ya da ilgili kuruma şikâyet edenler), %10'u şikayetçi olmuş (adli-idari makamlara ya da ilgili kuruma şikâyet edenler) ve aynı zamanda önlem almış, %44,5'i sadece önlem almış, %16,4'nün hiçbir şey yapmamış olduğu belirlenmiştir. Siber mağduriyete uğradığını bildiren katılımcılardan 21. soruda bu mağduriyetin en olduğunun açıklanması istenmiştir. Katılımcıların verdiği cevapların gruplandırmasına ilişkin tablo aşağıdaki şekildedir:

Tablo XV. Katılımcıların Uğradığı Siber Mağduriyet Türleri Tablosu

	Frekans (N)	Yüzde (%)
Siber Dolandırıcılık	32	6,4
Kimlik hırsızlığı, kişisel verilerin izinsiz kullanılması	36	7,2
Siber taciz	16	3,2
Finans ve kart bilgilerinin çalınması	10	2
Virüsler ve diğer türde kötü amaçlı yazılımlar kullanarak bilgisayarları hedef alan suç faaliyetleri.	19	3,8
Siber gasp	3	0,6
Spam	4	0,8

Katılımcıların bildirdikleri siber mağduriyetler Tablo XV.'teki şekilde kategorize edilmiştir. Kimlik hırsızlığı ve siber dolandırıcılık en çok bildirilen siber mağduriyet türleridir.

Tablo XVI. Siber Mağduriyet Bildiren Katılımcılara İlişkin Tablo

Değişkenler	Frekans (N)	Yüzde (%)
Cinsiyet		
Erkek	66	52
Kadın	61	48
Eğitim		
Lise	5	3.9
Lisans	89	70.1
Lisansüstü	33	26
Medeni Hal		
Bekar	68	53.5
Evli	59	46.5
Meslek Grubu		
Hukuk	83	65.4
Bilişim	44	34.6
Antivirüs Programı Kullanımı		
Evet	93	73.2
Hayır	34	26.8
Lisanssız Yazılım Kullanımı		
Evet	83	65.4
Hayır	44	34.6
Erişim Engelli Sitelere Girme		
Evet	95	74.8
Hayır	32	25.3
İnternette Geçirilen Süre		
4 saat ve daha az	69	54.3
4 saatten fazla	58	45.7

Siber mağduriyete uğrayanların %65.4'ü lisanssız yazılım kullanmaktadır. Siber mağdruiyete uğrayanların % 74.8'i de erişime engelli sitelere girmektedir.Siber mağduriyet bildiren katılımcıların % 73.2'si anti virüs programı kullanmaktadır.

Tablo XVII. Siber Mağduriyete Uğrayanlar İle Uğramayanlar Arasında Ölçekler Açısından Farklılık Olup Olmadığının Tespitine İlişkin Tablo

	İnternet Mağduriyeti Yaşama		İstatistik
	Evet	**Hayır**	
PİKÖ Aşırı Kullanım	13.04±3.25	11.54±3.55	t=4.21 p<0.001*
PİKÖ Sosyal Fayda/Sosyal Rahatlık	273.02	242.83	U=20825 Z=-2.04 p=0.04**
PİKÖ İnternetin Olumsuz Sonuçları	282.62	238.88	U=19352.5 Z=-3.09 p=0.002**
PİKÖ	286.62	238.20	U=19098 Z=-3.26 p=0.001**

* t testi; ** Whitney-U testi; PİKÖ:Problemli İnternet Kullanım Ölçeği;

PİKÖ Aşırı Kullanım ortalamalarına göre internette mağduriyet yaşayan bireyler ile yaşamayan bireyler arasında anlamlı farklılık vardır (p<0.001). Mağduriyet yaşamış bireylerin Aşırı Kullanım ortalamaları mağduriyet yaşamamış bireylerden daha fazladır. Sosyal Fayda/Sosyal Rahatlık, İnternetin Olumsuz Sonuçları ve PİKÖ sıra ortalamalarına göre gruplar arasında anlamlı farklılık vardır (p=0.04; 0.002;0.001). İnternet mağduriyeti yaşan bireylerin Sosyal Fayda/Sosyal Rahatlık, İnternetin Olumsuz Sonuçları ve PİKÖ puanları internet mağduriyeti yaşamayan bireylerden daha fazladır.

4.5. Bilişim Suçu Hukuki Farkındalığına İlişkin Bulgular

Tablo XVIII. BSF Formunun Bilişim ve Hukuk Sektöründeki Dağılımı

BSF Maddeleri	Hukuk	Bilişim
Madde 1: "Üçüncü bir kişi tarafından şahsi bilgisayarıma /tabletime/cep telefonuma izinsiz şekilde erişilerek bir dosyamın silinmesi suç oluşturur"		
Kesinlikle Katılmıyorum	----	1(0.4)
Katılmıyorum	----	1(0.4)

Kararsızım	6(2.2)	2(0.9)
Katılıyorum	15(5.6)	18(7.8)
Kesinlikle Katılıyorum	249(92.2)	208(90.4)
Madde 2:"Üçüncü bir kişi tarafından şahsi bilgisayarıma /tabletime/cep telefonuma izinsiz şekilde erişilerek bir dosyamın silinmesi suç oluşturur"		
Kesinlikle Katılmıyorum	---	1(0.4)
Katılmıyorum	1(0.4)	---
Kararsızım	5(1.9)	3(1.3)
Katılıyorum	15(5.6)	11(4.8)
Kesinlikle Katılıyorum	249(92.2)	215(93.5)
Madde 3:"Lisanssız yazılım kullanmak suçtur"		
Kesinlikle Katılmıyorum	5(1.9)	1(0.4)
Katılmıyorum	11(4.1)	10(4.3)
Kararsızım	43(15.9)	37(16.1)
Katılıyorum	50(18.5)	45(19.6)
Kesinlikle Katılıyorum	161(59.6)	137(59.6)
Madde 4: "Hırsızlığın bilişim sistemini kullanmak suretiyle gerçekleştirilmesi hırsızlığın basit haline göre daha ağır ceza gerektirir"		
Kesinlikle Katılmıyorum	2(0.7)	9(3.9)
Katılmıyorum	2(0.7)	12(5.2)
Kararsızım	16(5.9)	42(18.3)
Katılıyorum	41(15.2)	43(18.7)
Kesinlikle Katılıyorum	209(77.4)	124(53.9)
Madde 5: "Kişisel verilerimin izinsiz şekilde işlenmesi suç oluşturur"		
Kesinlikle Katılmıyorum	2(0.7)	1(0.4)
Katılmıyorum	2(0.7)	---
Kararsızım	4(1.5)	5(2.2)
Katılıyorum	18(6.7)	21(9.1)
Kesinlikle Katılıyorum	244(90.4)	203(88.3)
Madde 6: Hakkında erişim engelleme kararı olan bir internet sitesine (IP değişikliği, DNS değiştirme, URL maskeleme, proxy kullanma ya da VPN kullanma gibi yöntemlerle) erişilmesi suç oluşturmaz		
Kesinlikle Katılmıyorum	43(15.9)	43(18.7)
Katılmıyorum	23(8.5)	20(8.7)
Kararsızım	45(16.7)	56(24.3)
Katılıyorum	75(27.8)	47(20.4)
Kesinlikle Katılıyorum	84(31.1)	64(27.8)
Madde 7: "Bilişim sistemleri aracılığıyla sosyal medyada hakarete uğramak hakaretin basit haline göre daha fazla cezayı gerektirir"		
Kesinlikle Katılmıyorum	19(7)	12(5.2)
Katılmıyorum	8(3)	15(6.5)
Kararsızım	34(12.6)	55(23.9)
Katılıyorum	54(20)	44(19.1)
Kesinlikle Katılıyorum	155(57.4)	104(45.2)

Madde 8: "Elektronik imzamın rızam dışında kullanılması suç oluşturur"		
Kesinlikle Katılmıyorum	2(0.7)	1(0.4)
Katılmıyorum	1(0.4)	---
Kararsızım	4(1.5)	4(1.7)
Katılıyorum	12(4.4)	16(7)
Kesinlikle Katılıyorum	251(93)	209(90.9)

Tablo XVIII'de Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formuna katılımcıları verdiği cevapların oranları gösterilmiştir. Katılımcıların "*Lisanssız yazılın kullanmak suçtur"* önermesine kesinlikle katılıyorum diyen hukukçu katılımcıların sayısı 168'dir. (Tablo XVIII) BSF formunda "*Lisanssız yazılım kullanmak suçtur*" önermesine "kesinlikle katılıyorum" diyen 158 kişi ise lisanssız yazılım kullanmaktadır. *"Hakkında erişim engelleme kararı olan bir internet sitesine (IP değişikliği, DNS değiştirme, URL maskeleme, proxy kullanma ya da VPN kullanma gibi yöntemlerle) erişilmesi suç oluşturmaz*" önermesine kesinlikle katılmıyorum diyen yani erişim engelli sitelere giremenin suç olduğunu düşünen 43 bilişim sektörü çalışanı 43 de hukukçu bulunmaktadır. BSF formunda "*Hakkında erişim engelleme kararı olan bir internet sitesine (IP değişikliği, DNS değiştirme, URL maskeleme, proxy kullanma ya da VPN kullanma gibi yöntemlerle) erişilmesi suç oluşturmaz"* önermesine "*kesinlikle katılmıyorum"* diyen 42 kişi ise erişim engelli sitelere girmektedir.

5. TARTIŞMA

Çalışmamızın bu bölümde, katılımcılardan elde edilen bulgular, literatür ile birlikte karşılaştırılarak açıklanacaktır.

Eylül 2020'de bağımsız araştırma şirketi Davies Hickman Partners, sekiz ülkedeki 4.016 tüketiciyle ve çeşitli sektörlerde ve rollerde çalışan 715 işletme yöneticisiyle bir anket çalışması yapmıştır. (Interpol, 2022) Bu araştırmanın British Telekom desteğiyle gerçekleştirilmiş, sonucu Interpol tarafından yayımlanmıştır. (Interpol, 2022) Katılımcılara genel olarak, geçen yıl kuruluşunuz için aşağıdakilerden hangisi daha önemli hale geldi sorusuna, katılımcıların %58'i "veri ve ağ güvenliğini iyileştirmek" cevabını vermiştir. Bu araştırmada, siber güvenliğin, koronavirüs krizinden sonra iş liderleri için artık bir numaralı öncelik olduğu ortaya konmuştur. (Interpol, 2022) Siber güvenliğin sağlanması kuruluşlar açısından da en önemli amaç haline gelmiştir. Araştırmamızda bilişim sektörü çalışanlarının Önlem Alma ortalamaları, Ödeme Bilgilerini Koruma puanları, İz Bırakmama ortalamaları, kişisel siber güvenliği sağlama total ortalamalarının hukukçulardan daha yüksek olduğu ortaya konmuştur. (Bkz. Tablo VIII). Bu bulguyla 1. hipotezimizin aksine siber güvenliği sağlama değişkeni açısından bilişim sektörü çalışanları ile hakim, savcı ve avukatlar arasında istatiksel açıdan anlamlı bir fark vardır. İnterpol araştırmasının katılımcıların %33'ü bilgisayarlarına erişmek için parola kullanmayı unuttuklarını ya da asla kullanmadıklarını, % 45'i kişisel bilgilerini içeren kağıtlarını imha etmeyi unuttuklarını ya da asla imha etmediklerini, %46'sı yazılımların güncel olduğunu kontrol etmeyi unuttuklarını ya da asla kontrol etmediklerini, %54'ü çerezleri temizlemeyi unuttuklarını ya da asla temizlemediklerini, %57'si cihazları şifre hatırlatması için yetkilendirmeyi unuttuklarını ya da asla yetkilendirmediklerini ifade etmişlerdir. (Interpol, 2022) Siber güvenliğin sağlanması siber suç mağduriyetinin önlenmesinde önemli bir koruyucu olduğu karşımıza çıkmaktadır

BSA'nın 2016 yılında yayımladığı raporda, Dünya'da yıllara göre lisanssız yazılım indirme oranları ortalaması 2015 yılında %39, 2013 yılında %49, 2011 yılında %42, 2009 yılında %43 iken Türkiye'de yıllara göre lisanssız yazılım indirme oranları 2015 yılında %58, 2013 yılında %60, 2011 yılında %62, 2009 yılında %63'tür. (BSA, 2016) BSA'nın 2016 tarihli araştırmasında Türkiye Ortadoğu- Afrika bölgesi ülkeleri içerisinde değerlendirilmiş, Türkiye'de yıllara göre lisansız yazılım kullanım oranlarının bölge ortalamasının üzerinde olduğu tespit edilmiştir. (The Software Alliance BSA, 2016) Aynı araştırmada Amerika Birleşik Devletleri'nde ise bu oranın 2015 yılında 17, 2013 yılında %19, 2011 yılında %19, 2009 yılında %21 olduğu belirlenmiştir. (The Software Alliance BSA, 2016) Avrupa ülkeleri ortalaması ise 2015 yılında 28, 2013 yılında %29, 2011 yılında %32, 2009 yılında %34'tür. The Software Alliance (BSA)'nın 2018'deki araştırmasına göre kişisel bilgisayarlarda kullanılan yazılımların %37'sinin lisanssız olduğu tespit edilmiştir. (The Software Alliance BSA, 2018).

Araştırmamızda, lisanssız yazılım kullanmayan bireylerin KSGS Kişisel Gizliliği Koruma, Güvenilmeyenden Kaçma, Önlem Alma, Ödeme Bilgilerini Koruma, bilişim suçu farkındalığı puanlarının daha fazla olduğu ortaya konulmuştur. (Bkz. Tablo XIV) 2. hipotezimizi destekler biçimde katılımcıların lisanssız yazılım kullanımları ile kişisel siber güvenliği sağlamaları arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki bulunmuştur. Uluslararası hukukta olduğu gibi telif haklarına ilişkin ihlallerin suç sayılması Türk Hukuku'nda da söz konusudur. 2011 yılında Türkiye'de yapılan bir çalışmada katılımcıların %72,5'nin lisansız yazılım kullandığını ortaya koymuş, katılımcıların %29,6'sı internetten müzik, film, oyun dosyaları indirmenin suç olduğunu bilemediği ifade etmiştir. (Dijle, Doğan, 2011) Araştırmamızda ise hem hukukçuların hem de bilişim sektörü çalışanlarının yüksek oranda lisanssız yazılım kullandığı tespit edilmiştir. (Bkz.Tablo II) Araştırmamızda 298 katılımcı "*lisanssız yazılım kullanmak suçtur"* önermesine kesinlikle katıldığını bildirmiş olup

katılımcılardan "*Lisanssız yazılın kullanmak suçtur"* önermesine kesinlikle katılıyorum diyen hukukçu katılımcıların sayısı 168 olduğu belirlenmiştir. (Bkz.Tablo XVIII) BSF formunda yer alan "*Lisanssız yazılım kullanmak suçtur"* önermesine *"kesinlikle katılıyorum"* diyen 158 kişi ise lisanssız yazılım kullanmaktadır.

Lisanssız yazılım kullanmanın suç olmasının yanı sıra lisanssız yazılım kullanmanın siber suç mağduru olma riskini arttırdığını söylemek mümkündür. (The Software Alliance BSA, 2018). BSA'nın 2018'deki araştırmasında, lisanssız yazılım kullanma nedeniyle kötü amaçlı yazılım bulaşma oranın %29 olduğu tespit edilmiştir. (The Software Alliance BSA, 2018). Araştırmamızda da bu durumu destekler şekilde her iki grup katılımcıların da internetin olumsuz sonuçları puanları lisansız yazılım kullananlarda daha fazla olduğu ortaya çıkmıştır. (Tablo XIII) Siber mağduriyet bildiren katılımcıların %65.4'nün de lisanssız yazılım kullandığı belirlenmiştir. (Bkz. Tablo XVI) 3. hipotezimizi destekler biçimde katılımcıların lisanssız yazılım kullanımları ile kişisel siber güvenliği sağlamaları arasında istatiksel açıdan pozitif yönde anlamlı bir ilişki vardır. Araştırmaya katılan hukukçuların ve bilişim sektörü çalışanlarının lisanssız yazılım kullanmanın suç olduğunu düşünmesine rağmen lisansız yazılım kullanma eğilimleri olduğu belirlenmiştir. (Bkz. Tablo II; Tablo XVIII). BSF formunda yer alan "Lisanssız yazılım kullanmak suçtur" önermesine "kesinlikle katılıyorum" diyen 158 kişi ise lisanssız yazılım kullanmaktadır. Yani araştırmamızdaki 158 katılımcı lisanssız yazılım kullanmayı kesinlikle suç olarak nitelese de yine de lisanssız yazılım kullanmaktadır. Buna rağmen yapılan araştırmalarda alışkanlık, sosyal çevre desteği, satın alma gücü gibi nedenlerin lisanssız yazılım kullanmanın ardındaki nedenler olarak görülmektedir. (Taşçıoğlu,2019) Lisanssız yazılım kullanımının en önemli nedenin ekonomik nedenler olduğu değerlendirilmektedir.

Güncel literatür incelendiğinde, yazılım korsanlığının-lisanssız yazılım kullanımının yaygınlaşmasına ilişkin önemli ve haklı endişeler olmasına rağmen, yazılım endüstrisinde fikri

mülkiyet haklarının korunmasına yönelik stratejiler konusunda henüz bir fikir birliği bulunmamaktadır. (Asongu, 2021) Asongu, çalışmasında mevcut yazılım korsanlığı seviyeleri dikkate alınarak fikri mülkiyet hakları rejimlerinin yazılım korsanlığını azaltmak için teknoloji ile nasıl etkileşime girdiğini incelenmiştir. (Asongu, 2021) Bu çalışmada önemli bir bulgu olarak fikri mülkiyet yasalarının düzeltici etkisinin yüksek düzeyde yazılım korsanlığı olan ülkelerde daha fazla olduğunu göstermiştir. (Asongu, 2021) Yazılım korsanlığı ile mücadelede genel politikaların benimsenmesinin, ilgili ülkedeki mevcut teknoloji ve yazılım korsanlığı seviyelerine bağlı olmadıkça başarılı olma ihtimali düşük olacağı değerlendirilmiştir. (Asongu, 2021) BSA, yazılım sektörünün büyüklüğü ve ekonomiye katkısı göz önüne alındığında iyi korunan fikri mülkiyet sisteminin önemli olduğunun bu sayede yazılım geliştiricilerinin enerjilerini ve yatırımlarını inovasyona harcayabileceği görüşündedir.(The Software Alliance BSA, 2020)

Her ne kadar BSA'nın lisanssız yazılım verileri literatürde en çok kullanılan veriler olsa da 1997 yılında Türkiye'de faaliyetlerine başlayan (Nebil, 2017) ve 2017 yılında faaliyet izni yenilenmeyen (Nebil, 2017) BSA'nın Türkiye'de korsan yazılım kullanımına karşı mücadele adına 2000'lerin başında yürüttüğü süreç oldukça tartışmalıdır. Birçok işletme, internet kafe BSA Türkiye'nin lisanssız yazılımla mücadele adında ciddi baskılarla karşılaşmış ve lisanssız yazılım kullanımına ilişkin ceza tehditleri altında kullanımından daha çok lisans almaya zorlanmıştır. (Nebil, 2009) Microsoft'un lisanssız yazılım kullanımına karşı sürdürdüğü tartışmalı işlemler bugün de devam etmektedir. Özellikle veri merkezi işletmecilerinin kullandığı yazılım ürünlerinin sözleşmeleri büyük yazılım şirketleri tarafından müzakere edilmeden kabul edilmesi istenmektedir. (Candoğan, 2020) Micorsoft ürünlerine ilişkin olan "The Microsoft Services Provider License Agreement" sözleşmeleri kapsamında sunulan hizmetlerin lisans denetimleri gerçekleştirilirken, veri merkezlerinde mevcut tüm sunuculara erişim yetkisi talep edilmektedir. Özellikle veri merkezlerinin kamu kuruluşları, banka ve

finans kuruluşu müşterileri yönünden bu müşterilere ait sistemlere erişerek denetim gerçekleştirmelerinin 411 sayılı Bankacılık Kanunu, 6493 sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun ve ilgili diğer mevzuat kapsamında müşterilere ait bankacılık sırları ve kişisel bilgilerin denetçi firmanın erişimine açılması hukuka aykırı olduğu gibi telafisi imkansız zararlar doğurabileceği değerlendirilmektedir. Bu ve benzeri lisans denetimi uygulamaları karşısında Türk Hukuk sisteminin ve idarelerin işletmecilerin ve bireylerin kişisel verilerini ve ticari sırlarını korumayı önceliklendirmeleri gerekmektedir. Global yazılım şirketlerine olan mecburiyet çoğu zaman haklar dengesini bozmakta hatta kimi zaman siber güvenlikle riskler doğurmaktadır. (Yılmaz E., 2021) Bu durum uygun ücretle erişilebilir, yerli ve milli yazılımlara olan ihtiyacın önemini daha çok ortaya çıkarmaktadır.

Lisanssız yazılım kullanımından sonra katılımcıların siber kriminal aktivitelerinden birinin de erşime engelli sitelere girme davranışları olduğu tespit edilmiştir. Erişime engelli sitelere "yalnızca erişme eylemi" Türk Hukukunda suç olarak düzenlenmemektedir. 5651 sayılı Kanun uyarınca söz konusu engellemeleri gerçekleştirmeyen içerik, yer veya erişim sağlayıcılarının sorumluları için idari cezalar öngörülmüştür. Araştırmamızdaki katılımcıların %71,2'sinin erişime engelli sitelere çeşitli yöntemlerle (VPN, DNS değişikliği vs. ile) girdiği belirlenmiştir (Bkz. Tablo II). Lisanssız yazılım kullanmadaki yüksek oranın ihlal niteliğinde olan bu tutumda da görüldüğü belirlenmiştir. Katılımcılara sorulan"*Hakkında erişim engelleme kararı olan bir internet sitesine (IP değişikliği, DNS değiştirme, URL maskeleme, proxy kullanma ya da VPN kullanma gibi yöntemlerle) erişilmesi suç oluşturmaz"* önermesine hukukçu katılımcıların %15.9'u bilişim sektörü katılımcılarının % 18.7'si kesinlikle katılmadığını bildirmiştir. Yani bu oranlardaki katılımcılar erişime engelli sitelere çeşitli yöntemlerle erişmenin suç olduğunu düşünmektedir. Hukukçu katılımcıların %50.7'si, bilişim sektörü katılımcılarının da % 61.3'nün erişime engelli sitelerin izlendiğini düşünmektedir.

(Bkz. Tablo II) Bu bulgu kriminal aktivitenin otorite tarafından izlendiği algısının yüksekliğini de ortaya koymaktadır. Buna rağmen katılımcıların erişime engelli sitelere girme tutumunun da yüksek oranda olduğunu değerlendirmekteyiz. Bunun arkasındaki nedenin internetin mülkiyetinin kimseye ait olamayacağı düşüncesi, otoritenin siber uzamda varlığını kabul etmeme gibi nedenlerle açıklanabilir. Araştırma evreninin Türkiye olması sebebiyle bugüne kadar Türkiye'de verilen ve kamuoyunda tartışılan AYM tarafından da iptal edilen Youtube, Twitter gibi sosyal medya mecralarının "tamamının erişime engellenmesi" kararlarına (AYM, 2014) karşı olumsuz bakış açısının (Akdeniz ve Altıparmak, 2008) devam eden erişim engelleme uygulamalarında kullanıcı tutumlarını belirlemiş olabileceği de değerlendirilmelidir.

Çevrimiçi kriminal aktivitelerin hukukçular ve bilişim sektörü çalışanları arasında da yüksek oranda görülmesi önemli bir bulgudur. Yapılan çalışmalarda; bireylerin günlük hayata kıyasla siber alanda, daha değişken ve mobil bir ortamda olmalarından ötürü daha hızlı karar vermek durumunda olmalarının, onları dijital iletişim ve etkileşimde hatalı davranışlara kolaylıkla itebilmesine, hatta bu hatalı davranışların bireyi çoğu zaman suçun faili ve mağduru konumuna getirebileceği ifade edilmektedir. (Öztürk ve diğerleri, 2020) Bu bağlamda lisanssız yazılım kullanma ve erişim engelli sitelere girme davranışlarının bulgusu bu tezle de ilişkili olduğu düşünülmektedir. Interpol'ün araştırmasında saldırıların karmaşık olması gerekmediğini örneğin konu satırında 'LinkedIn' içeren kimlik avı e-postalarının açılma oranı neredeyse %50 olduğu ifade edilmiştir. (Interpol, 2022) Bu örnekte olduğu gibi siber uzamda hızlı karar vermenin sonucu olduğu düşünülen kimlik avı e-postalarının açılması gibi iletişimde hatalı davranışlar siber mağduriyet riskini de arttırmaktadır. (Öztürk ve diğerleri, 2020)

Ocak 2022'de açıklanan "We Are Social" Raporu'nda Türkiye'de günlük toplam internet kullanım ortalaması 8 saatken (Recro Digital Marketing, 2022a) Dünya'da günlük internet kullanım ortalaması 6 saat 58 dakika olarak tespit edilmiştir. (Recro Digital Marketing, 2022b) Çalışmamızda katılımcılara internette geçirdikleri "günlük toplam süre" sorulmuş olup bu süre

içerisine iş ve akademik amaçlı kullanım da dahildir. Katılımcılardan internette günde 4 saatten fazla zaman geçiren bireylerin PİKÖ aşırı kullanım, sosyal fayda, internetin olumsuz sonuç puanları daha az vakit geçiren bireylerden daha yüksek bulunmuştur. (Bkz. Tablo XIII) 4. hipotezimizi doğrular biçimde internette geçirilen süreler ile problemli internet kullanımı arasında anlamlı ilişki saptanmıştır. Bu bulguyla örtüşür şekilde internet ve akıllı telefon bağımlılıklarının siber dolandırıcılık mağduriyeti ile ilişkili olduğu (Urueña ve ark., 2022), problemli sosyal medya kullanımlarının siber suç mağduru olma riskini artırdığını yönünde araştırmalar (Marttila ve ark., 2021) mevcuttur. Öztürk'e göre, dijital iletişimlerin problemli biçimde kullanımları siber mağduriyetlere neden olabilmekte, siber mağduriyet bir siber travma olarak siber dissosiyasyona da yol açabilmektedir. (Öztürk, 2020) Öztürk'e göre siber mağduriyet, internet bağımlılığı, çocukluk çağı travmaları ve dissosiyasyon ile yakından ilişkilidir.(Erdoğan ve Öztürk, 2020) Choi'nin araştırmasına göre, riskli çevrimiçi davranışlar ve riskli çevrimiçi boş zaman etkinlikleri virüs mağduriyeti olasılığını artırmaktadır.(Choi, 2008) Rutin aktiviteler teorisi bağlamında Leukfeldt ve Yar'ın araştırmasında, belirlenen üç siber suç kategorisinde de mağdurların genellikle çevrimiçi ortamda daha fazla zaman geçirmiş olduğu tespit edilmiştir. (Leukfeldt ve Yar, 2016) Bu durum özellikle "internet kullanım sıklığı" ve hedefli tarama ve doğrudan iletişim gibi günlük faaliyetler değişkenlerine yansımaktadır. (Leukfeldt ve Yar, 2016) Dolayısıyla daha kapsamlı bir şekilde çevrimiçi olmak, çevrimiçi suçların mağduru olma ihtimalini artırmaktadır. (Leukfeldt ve Yar, 2016) Araştırmamızda, hukukçuların aşırı kullanım ortalamalarının bilişim sektörü çalışanlarından daha fazla olduğu tespit edilmiştir. (Bkz.Tablo VIII). Siber mağduriyet bildiren katılımcıların % 34.6'sı bilişim sektörü çalışanıyken %65.4'nün hukukçu olduğu belirlenmiştir. Araştırmamızda, siber mağduriyet yaşamış katılımcıların aşırı kullanım ortalamaları mağduriyet yaşamamış bireylerden daha fazla olduğu bulgusuna ulaşılmıştır. (Bkz. Tablo XVII) İnternet mağduriyeti yaşan bireylerin Sosyal Fayda/Sosyal Rahatlık, İnternetin

Olumsuz Sonuçları ve PİKÖ puanları internet mağduriyeti yaşamayan bireylerden daha fazladır. (Bkz. Tablo XVII) Bu bulgular, 5.hipotezimiz olan, katılımcıların interneti aşırı kullanımları ile siber mağduriyetleri arasında istatiksel açıdan pozitif yönde anlamlı bir ilişkinin olduğunu doğrulamaktadır. (Bkz. Tablo XVI)

Bu alana ilişkin profesyoneller olan bilişim sektörü çalışanları ve hukukçulardan oluşan katılımcıların mesleki profesyonelliklerine rağmen %25'4'nün siber mağduriyetle karşılaşmış olması tartışmaya değerdir. Başkaca araştırmalarda da siber riski bilen kişilerin yine de yüksek siber mağduriyet oranlarına sahip olduğunu ortaya konmuştur. (Drew ve Farrell, 2018) Yine 2020 yılında yapılan bir araştırmada siber güvenlik sorunun boyutlarının hem profesyoneller hem de tüketiciler tarafından anlaşıldığının tespit edildiği ifade edilmiştir. (Interpol, 2022) Aynı araştırmada tüketici davranışının siber güvenliğe yardımcı olmadığı, insanların tehlikeleri anlasalar bile bilerek çevrimiçi risk aldığı sonucuna ulaşılmıştır. (Interpol, 2022) Birçok araştırma siber dolandırıcılık mağdurlarının çevrimiçi ortamda göreceli risklerinin hem farkında olduklarını hem de doğru bir şekilde tanımlayabildiklerini doğrulamaktadır. Buna kıyasen diğer suç türleri üzerine yapılan araştırmalar, bireylerin doğru risk algılarına sahip olmadıklarını ve gerçek riske göre risk seviyelerini olduğundan fazla tahmin etme eğiliminde olduklarını sıklıkla ortaya koymuştur. (Drew ve Farrell, 2018) Leukfeldt ve Yar'ın araştırmalarında, kötü amaçlı yazılım mağduriyeti riskinin daha yüksek eğitim seviyesine ve ücretli işe sahip kişilerde daha yüksek olduğu tespit edilmiştir. (Leukfeldt ve Yar, 2016) Yine siber suçları rutin aktiviteler bağlamında ölçen bir başka çalışmada eğitim seviyesi arttıkça siber suç mağduriyetinin arttığı tespit edilmiştir. (Birceviz, 2019) Finansal okuryazarlık ve dolandırıcılık mağduriyeti arasındaki ilişkiyi inceleyen araştırmalarda, en bilgili kişilerin dolandırıcılık kurbanı olma olasılığının daha yüksek olduğu bulunmuş ve araştırmacılar bu durumu "bilme-yapma" boşluğu olarak yorumlamışlardır.(NASD, 2006) Araştırmamızda hukukçuların bilişim suçu farkındalıklarına ilişkin puanları bilişim sektörü çalışanlarına

kıyasen beklenen bir sonuç olarak daha yüksektir.(Bkz. Tablo VIII) Aynı zamanda hukukçular (%30.7) bilişim sektörü çalışanlarına (%19.1) göre daha çok siber suç mağduru olmaktadır.. (Tablo II) Dolandırılma ile ilgili olarak karar verme sürecinde hatalara neden olan motivasyonel ve bilişsel faktörlerden biri olan "aşırı özgüven" de bu sonucu açıklamaya yarayan bir unsur olarak değerlendirilebilir. (Öztürk ve Derin, 2020)

Slovenya'da yapılan bir çalışmada tüm katılımcıların (% 98.9) güvenlik duvarlarını kullandığını, % 94.9'u antivirüs programlarını kullandıklarını ifade etmiştir (Mesko ve Bernik, 2011) Choi'nin araştırmasına göre, teknik yeterliliğe sahip bir koruyucusu olan üniversite öğrencilerinin virüs mağduriyeti riski azalmaktadır. (Choi, 2008) Araştırmamızda her iki grup katılımcı yönünden de anti virüs programı kullanan bireylerin kişisel siber güvenliği sağlama ve kişisel siber güvenlikte önlem alma puanlarının daha fazla olduğu tespit edilmiştir. (Bkz. Tablo XII). 6. hipotezimizi doğrular biçimde antivirüs programı kullanımı ile kişisel siber güvenliği sağlama arasında pozitif yönlü anlamlı bir ilişki vardır. Fakat araştırmamızda siber mağduriyet bildiren katılımcıların %73.2'sinin aynı zamanda anti virüs programı kullandığı belirlenmiştir. (Bkz. Tablo XVI) Siber mağduriyete uğrayan bireylerin ise mağduriyet yaşamadan önce anti virüs programı kullanıp kullanmadığı ise ayrıca sorulmamıştır. Bu yüzden bu bulguyla anti virüs programı kullanımı ve siber mağduriyet arasındaki ilişkisellik tam olarak açıklanamayacaktır. Bir başka araştırmada da rutin aktiviteler teorisi bağlamında koruyucular değişkenin ölçülebilmesi için suç mağduriyeti yaşamış şahıslara sorunn "Mağduriyet yaşamadan önce anti virüs programı kullanıyor muydunuz?" şeklinde sorulması önerilmiştir.(Birceviz, 2019) Çalışmamızda da benzer eksikliğin varlığından söz edilebilecektir. Yine antivrüs programının koruyucu unsur olarak suçu önlemedeki etkisinin belirli siber suç tipleri yönünden olduğu da bilinmektedir. Bu bağlamda antivirüs kullanımı ve siber mağduriyet ilişkisi ölçülürken siber suç türleri belirlenerek, her suç türü için ayrı ayrı değerlendirme yapmak doğru olacaktır.

Birceviz'in araştırmasında en çok mağduru olunan siber suç türünün maddi getirisi olan suçlar olduğu, e-posta veya sosyal medya hesaplarının çalınması gibi suçların daha seyrek görüldüğü ortaya konmuştur (Birceviz, 2019). Bizim araştırmamızda ise "kimlik hırsızlığı, kişisel verilerin izinsiz kullanılması" ve "siber dolandırıcılık"ın en çok bildirilen iki siber mağduriyet türü olduğu tespit edilmiştir. (Bkz. Tablo XV) Her iki araştırma kıyaslandığında araştırma evrenlerinin farklı olması ve sorunun soruluş şekli gibi unsurlar yönünden farklılaşmasının bu farklı sonucu doğurduğu değerlendirilmektedir. Araştırmamızda bildirilen mağduriyet türleri sıralamasında rutin aktiviteler teorisi bağlamında maddi kazanca yol açacak siber dolandırıcılık mağduriyetinin yüksek olarak bildirilmesi bağlamında, bu sonucun uygun hedefte bulunması gereken unsurlar erişilebilirlik ve arzu edilebilirlikle açıklanabileceği düşünülmektedir. Kimlik hırsızlığı ve kişisel verilerin izinsiz kullanımına yönelik bildirilen mağduriyet oranın yüksekliği ise kişisel verilerin de maddi karşılığı olan verilere dönüşmüş olması yönünden siber failler için uygun hedef olarak açıklanabilir.

Leukfeldt ve Yar'ın araştırmasına göre yaşın bilgisayar korsanlığı mağduriyeti üzerinde önemli bir etkisi vardır; bir kullanıcı ne kadar gençse risk o kadar yüksektir. (Leukfeldt ve Yar, 2016) Aynı araştırmaya göre, cinsiyet ve eğitim seviyesi gibi diğer arka plan özelliklerinin herhangi bir etkisi yoktur. Bizim araştırmamızda da cinsiyet ve medeni hal ile siber mağduriyet arasında anlamlı bir ilişki bulgusuna rastlanmamıştır. (Bkz. Tablo XVI)

Araştırmamızda en çok kullanılan uygulamaların en başında iletişim ve sosyal medya uygulamaları bulunduğu belirlenmiştir. (Bkz. Tablo VI) İletişim ve sosyal medya uygulamalarının kullanımı kişilerin görünürlük ve erişilebilirliklerini arttırmaktadır. Çevrimiçi görünürlüğün tüm değişkenleri iki yüksek teknoloji suçundan en az birini etkilediği, çevirimiçi iletişim platformları (Skype vb.) üzerinden doğrudan iletişim kurmanın ve çevrimiçi forumlarda ve sosyal ağ sitelerinde aktif olmanın, bilgisayar korsanlığı mağduriyeti riskinin artmasına yol açtığı ortaya konulmuştur.(Leukfeldt ve Yar, 2016) Araştırmamızda sosyal medya kullanımı

ve iletişim uygulamaları kullanımlarının siber mağduriyete etkisi ölçülmemiş olsa da bunların kullanımının siber mağduriyete etki eden bir risk faktörü olduğu not edilmelidir.

İnterpol araştırmasına göre, kurumsal düzeyde mağduriyete bakıldığında, yöneticilerin %75'i kuruluşlarına her yıl daha fazla güvenlik tehdidi olduğunu ifade etmiştir. (Interpol, 2022) Interpol araştırmasında, yöneticilerin %84'ü kuruluşlarının son 2 yılda veri hırsızlığı / kaybı veya bir ağ güvenliği olayına maruz kaldığını ifade etmiştir. (Interpol, 2022) Yöneticilerin %49'u verileri çalmaya çalışan profesyonel bilgisayar korsanları yönünden kuruluşlarının geçen yıl boyunca daha fazla risk altında olduğunu, yöneticilerin % 49'u tüketicileri kandıran dolandırıcılar yönünden kuruluşlarının geçen yıl boyunca daha fazla risk altında olduğunu, yöneticilerin %43'ü siyasi gündemi olan hacktivistler yönünden kuruluşlarının geçen yıl boyunca daha fazla risk altında olduğunu, yöneticilerin %43'ü dark web'te kuruluşların verilerini satması yönünden kuruluşlarının geçen yıl boyunca daha fazla risk altında olduğunu, yöneticilerin % 23'ü müşterilerin hata yapması yönünden kuruluşlarının geçen yıl boyunca daha fazla risk altında olduğunu ifade etmişlerdir. (Interpol, 2022)

Siber suçlarda mücadelede karşılaşılan güçlüklerden biri siber suçların aydınlatılmasında yaşanan gecikme olmaktadır. Stratonov ve arkadaşları, özellikle bankacılık alanında saldırıya uğrayan idareler ve ticari kuruluşların, suç işleyen bir şüphelinin kimliğini tespit edilmesine sıklıkla güvenmediklerini; bir siber suçun niteliğini belirlemenin zorluğunun ve bireysel soruşturma işlemlerinin özellikleri nedeniyle soruşturma aşamasında bazı sorunlar ortaya çıktığını ifade etmektedir. (Stratonov ve ark., 2021) Ayrıca siber suç türlerini tespit edebilecek, önleyebilecek ve bunlarla mücadele edebilecek bilgiye sahip teknik personel sayısının az olmasının da suçla mücadeledeki güçlüklerden biri olarak ifade etmektedirler. (Stratonov ve ark., 2021)

Siber suçlarda yaşanan artış ve çeşitlenme siber suçların önlenmesi için yasa koyucuları ulusal yasalarında yeni düzenlemeler yapmaya itmektedir. Özellikle yeni nesil siber suç

düzenlemeleri bazı devletlerin ulusal yasaları yönünden eleştirilere maruz kalmaktadır. Yeni nesil siber suçların geleneksel müteselsil suçlarda farklılaştığı, hazırlık işlemlerinin suç konusu yapılması, iştirak hükümlerinin uygulanmasında geleneksel ceza hukukundaki teroik açıklamaları tutarsızlaştırdığı yönünde eleştiriler bulunmaktadır. (Yong, 2019) Bu açıdan yeni nesil bilişim suçlarına yönelik yasal düzenlemelere eleştiriler yeni siber suç türlerinin ortaya çıkardığı zararının büyük olmadığı, yasanın ikinci derece gereklilikleri esnek olduğu, adli uygulama kriterleri belirsiz olduğu ve bu nedenle yasa hükümlerine nadiren başvurulduğu ve suçun kapsamının gereksiz yere genişletildiği yönündedir. (Yong, 2019) Çözüm için mevzuatın etkinliğinden tam anlamıyla faydalanabilmek adına, bilişim suçlarının yapısına uygun makul yargı kuralları oluşturması gerektiği, bu tür suçların kurucu unsurlarını makul bir şekilde daraltması gerektiği ve ikinci derece gerekliliklerin yorumlanmasını kategorize ederek ve sınırlandırmak gerektiği ifade edilmektedir. (Yong, 2019)

6. SONUÇ VE ÖNERİLER

Sosyal değişimi de beraberinde getiren teknoloji, dünyayı değiştiren tarihsel bir unsurdur. Adli psikoloji alanında çalışan uzmanlar, dijital iletişim ağları ya da teknoloji araçlı iletişimler, günümüz toplumunda bireylerin hem psikolojik hem de sosyolojik ve politik boyutlarda oldukça önemli psikososyopolitik dönüşümlerine neden olmakta olduğunu, siber dissosiyasyonu, hem normlaştırmakta hem de normalleştirdiğini ifade etmektedir.(Öztürk, 2020) Katılımcıların aşırı kullanım ortalamaları, problemli internet kullanımları ve siber mağduriyet oranlarına ilişkin resim siber dissosiyasyonun da kapılarını aralamaktadır. Siber alanda bireylerin hızlı karar vermeleri nedeniyle oluşan hatalı davranışlarının yüksek oranda kriminal aktivitelere dönüşebilmesi gerçeği; (Marttila ve ark., 2021) katılımcıların lisanssız yazılım kullanım oranlarındaki yükseklik ve erişime engelli sitelere girme davranışları gibi siber kriminal aktivitelerinin nedenini ortaya koymaktadır. Bununla birlikte aktüel dünyadakine benzer şekilde motive olmuş suçlu, uygun hedef ve koruyucuların yokluğunda da siber uzamda siber suç olayı gerçekleşmektedir. Özellikle aşırı kullanımın, siber güvenlik önlemlerinin yokluğunun siber suç mağduriyet riskini arttırdığı araştırmamızda ortaya konulmuştur. Hem eğitimli hem de araştırma alanına ilişkin profesyonel kişilerden oluşan katılımcıların yüksek oranda kriminal aktivite bildirmiş olmaları, kişilerin siber uzamda daha kolay kriminalize olunabildiğini ortaya koymaktadır. Siber suçları açıklamada siber kimlik kuramı ve rutin aktiviteler teorisinin önemi bu araştırmadaki bulgularla da ortaya konmuştur.

Diğer araştırmalar incelendiğinde araştırmamızın birçok özgün yönü olduğu ortaya çıkmaktadır. Bilişim sektörü çalışanları ve hukukçuların birlikte bilişim suçlarına ilişkin tutumlarına yönelik bir araştırmaya rastlanmamıştır. Sonuçlar ve yöntem geliştirilmeye açık olsa da motive olmuş suçlu, uygun hedef ve koruyucuların yokluğu unsurları siber suçları önemli ölçüde açıklayabilmektedir.

Araştırmamızda siber suç farkındalığına ilişkin soru formunun beşli likert tipte yapılmış olmasının bazı sınırlılıklar oluşturduğu anlaşılmıştır. Katılımcıların bir eylemin suç olup olmadığını cevaplandırmaları için soruların üçlü likert tipte sorulmasının daha anlamlı sonuçlar vereceği düşünülmektedir. Bununla birlikte bundan sonra yapılacak çalışmalarda, siber mağduriyet ve antivirüs ilişkisinin ölçülebilmesi açısından antivirüs programının siber mağduriyet öncesinde kullanılıp kullanılmadığı da katılımcılara sorulması gerektiği düşünülmektedir. Siber mağduriyetin rutin aktiviteler teorisi bağlamında değerlendirlebilmesi için suç tipleri belirlenerek unurlar her suç tipi için ayrı ayrı ölçülmelidir.

Siber suçların hem ulusal hem uluslarası düzeyde yasal zemine kavuşturulması siber suçlar karşısında bireyleri koruyabilecek en önemli mekanizmalardır. Yasaların varlığı kadar toplumlarda bilişim okuryazarlığının arttırılması, siber suçların önlenmesinde önemli bir faktördür. Teknolojinin hızlı gelişimi karşısında yasa koyucunun reaksiyonel yasalar yapma girişimleri uzun vadede adaletin sağlanması amacına ulaşmayı gerçekleştirememektedir. Bu tip yasama girişimleri güvenlik ve özgürlük dengesinde de önemli ölçüde sorunlar yaratmaktadır. Siber suçların soruşturulması, kovuşturulması aşamalarında ve siber suçların önlenmesi amaçlarıyla idarelere verilen yetkilerin sınırlarının mutlak biçimde çizilmiş olması gereklidir. Aksi takdirde siber suçların önlenmesi amacı, büyük bir gözetim ve denetim toplumunu ortaya çıkarma tehlikesini barındırmaktadır.

Siber uzamda gerçekleşen kriminal aktivitelerin önlenmesi hukukçuların ve bilişim sektörü profesyonellerinin de mutlak iş birliğini gerekli kılmaktadır.

7. KAYNAKLAR

Ağ ve siber güvenlik uzmanı nedir? (2022) Kariyer. 10 Aralık 2022 tarihinde https://www.kariyer.net/pozisyonlar/ag+ve+siber+guvenlik+uzmani/nedir adresinden erişildi.

Akarslan, H. (2015). *Bilişim suçları*. Ankara: Seçkin Yayıncılık.

Akbulut, B. (2016). Sistemi engelleme, bozma, verileri yok etme veya değiştirme. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi, 24*(2), 7-55. https://doi.org/10.15337/SUH.2017.0

Akdeniz, Y., & Altıparmak, K. (2008). *İnternet: Girilmesi tehlikeli ve yasaktır Türkiye'de internet içerik düzenlemesi ve sansüre ilişkin eleştirel bir değerlendirme*. Ankara: İmaj Yayınevi.

Akinwotu, E. (2021). Facebooks role in Myanmar and ethiopia under new scrutiny. The Guardian. 12 Ekim 2022 tarihinde https://www.theguardian.com/technology/2021/oct/07/facebooks-role-in-myanmar-and-ethiopia-under-new-scrutiny adresinden erişildi.

Aköz, B. C. (2018). *Türk ceza kanunu kapsamında bılişim suç ve cezaları ile örnek yargısal kararların analizi ve mevzuat önerıleri.* Uzmanlık tezi, Bılgi Teknolojileri ve İletişim Kurumu, Ankara.

Akpek, H. O. (2015). *Siber suçlar sözleşmesinin getirdikleri ve iç hukuk açısından konuya yaklaşım.* Yüksek lisans tezi, İstanbul Bilgi Üniversitesi, İstanbul.

Al Mutawa, N., Bryce, J., Franqueira, V.N.L., Marrington, A. & Read, J.C. (2019). Behavioural digital forensics model: Embedding behavioural evidence analysis into the investigation of digital crimes. *Digital Investigation, 28,* 70-82.

Aliusta, C., & Benzer, R. (2018). Avrupa siber suçlar sözleşmesi ve Türkiye'nin dahil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *4*(2), 35-42.

Arısoy, Ö. (2009). Internet addiction and its treatment. *Current Approaches In Psychiatry*, *1*, 55-67.

Asongu Simplice A. (2021) Global software piracy, technology and property rights ınstitutions. *Journal of the Knowledge Economy*. 12:1036–1063. https://doi.org/10.1007/s13132-020-00653-1

Avrupa Komisyonu İnternet Okuryazarlığı El Kitabı. (2006) 10 Ekim 2022 tarihinde https://www.coe.int/t/dghl/StandardSetting/InternetLiteracy/InternetLiteracyHandbook_2_TR.asp#KM16 adresinden erişildi.

Birceviz, F. (2019). *Rutin aktiviteler teorisi bağlamında siber suç mağduriyeti.* Yüksek lisans tezi, T.C. Milli Savunma Üniversitesi, Ankara.

Bozkurt H., Şahin S., & Zoroğlu S. (2016). İnternet Bağımlılığı: Güncel bir gözden geçirme. *Journal Of Contemporary Medicine*, *6*(3), 235-247 DOI: 10.16899/ctd.6630

BTK Kuruluş. (2017,15 Aralık). Kuruluş. 19 Ekim 2022 tarihinde https://www.btk.gov.tr/kuruluş adresinden erişildi.

Budak, Ö. S. (2015). *Bılışım Öğrencılerinin siber suç farkındalığı: Erzurum ili mesleki ve teknik liseler örneği*. Yüksek lisans tezi, Atatürk Üniversitesi, Erzurum.

Cambrige University Press. (2022a). Cyber. 10 Ekim 2022 tarihinde https://dictionary.cambridge.org/dictionary/english/cyber adresinden erişildi.

Cambrige University Press. (2022b). Fraud. 10 Ekim 2022 tarihinde https://dictionary.cambridge.org/tr/sözlük/ingilizce-türkçe/fraud adresinden erişildi.

Canbek, G., & Sarıoğlu, Ş. (2007). Kötücül ve casus yazılımlar: kapsamlı bir araştırma. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22*(1), 121-136

Candoğan, G. (2020) (Çevirimiçi) 10 Aralık 2022 tarihinde https://turk-internet.com/tekeller-mi-kuresellesmeyi-kuresellesme-mi-tekelleri-guclendiriyor-microsoft-ornegi-uzerinden-sokaktaki-insanin-kuresellesmey-itirazini-anlamaya-calismak/ adresinden erişildi.

Centel, N., & Zafer, H. (2006) *Ceza muhakemesi hukuku*. 4. Baskı. İstanbul: Beta Basım

Ceyhan, E., Ceyhan, A.A., & Gürcan, A. (2007). Problemli İnternet Kullanımı Ölçeği'nin geçerlik ve güvenirlik çalışmaları. *Kuram ve Uygulamada Eğitim Bilimleri, 7*(1), 390-416.

Chawki, M. (2005). A Critical look at the regulation of cybercrime, A comparative analysis with suggestions for legal policy, 12 Ekim 2022 tarihinde https://www.coursehero.com/file/10024719/Critical/ adresinden erişildi.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1): 308–333.

Ciso ne iş yapar? (2022) Bilişim Profesyonelleri. 10 Aralık 2022 tarihinde https://bilisimprofesyonelleri.com/ciso-is-tanimi-bir-ciso-ne-yapar/ adresinden erişildi.

Clough, J. (2015). *Principles of cybercrime.* 2nd edition. Cambridge: University Press.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*, 588-608.

Council of Europe (2001). Convention on cybercrime. 23 Kasım 2001. 10 Eylül 2021 tarihinde https://rm.coe.int/1680081561 adresinden erişildi.

Council of Europe (2001). Explanatory report to the convention on cybercrime. 13 Şubat 2022 tarihinde https://rm.coe.int/16800cce5b adresinden erişildi.

Counsil of Europe (2001) Convention on cybercrime (ETS No. 185) explanatory report. 25 Eylül 2021 tarihinde http://conventions.coe.int/Treaty/en/Reports/Html/185.htm adresinden erişildi

Çağlayan, R. (2013). *İdare hukuku dersleri*. Ankara: Adalet Yayınevi.

Çakmak, Z. (2011). Bağ*ımsız İdarı̇ otorite olarak enerji piyasası düzenleme kurumu*. Yayımlanmamış doktora tezi, Ankara Üniversitesi, Ankara.

Çalıcı, C. (2019). *Türkiye'de suç trendleri tarihsel kriminolojik değerlendirme*. 1. baskı İstanbul: Legal Kitabevi.

Çankaya, H., & Cengiz, E. (2018). Biyopolitik açıdan kişisel verilerin korunması. *Memleket Siyaset Yönetim, 13*(29), 135-156.

Çetin, M. S. (2021). Yargıtay kararları ışığında bilişim sistemine girme veya kalma suçu (TCK m. 243). *Türkiye Adalet Akademisi Dergisi, 12*(45), 1-28.

Çobansoy Hızel, G. (2019) Yeni teknolojiler hukuk ve insan hakları. Eskişehir Ticaret Odası. 02 Ekim 2022 tarihinde https://etonet.org.tr/uploads/bolgesel-sektorel/125-201911/KAPAK/Dijitalleşme%20Çağında%20Hukuk-Gökçe%20ÇOBANSOY.pdf adresinden erişildi.

Davis, R. A. (2001). A cognitive-behavioral model of pathological internet use. *Computers in Human Behavior, 17*(2),187-95

Detica Report. (2011). (Çevirimiçi) Organised crime in the digital age. 12 Ağustos 2022 tarihinde http://www.baesystemsdetica.com/resources/organised-crime-in-the-digital-age/ adresinden erişildi.

Dijle, H., & Doğan, N. (2011). Türkiye'de bilişim suçlarına eğitimli insanların bakışı. *Bilişim Teknolojileri Dergisi, 4*(2), 43-53.

Doğu, A. H. (2016). *Bilişim hukuku - Bilgi ve iletişim*. Bursa: Ekin Basım Yayın Dağıtım.

Dolu, O. (2011). *Suç teoriler: Teori, araştırma ve uygulamada kriminoloji*. 3. baskı. Ankara: Seçkin Yayıncılık.

Drew, J. M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research, 19*(6), 537-549. https://doi.org/10.1080/15614263.2018.1507890

Dülger, M. V. (2004). *Türk ceza hukukunda bilişim suçları*. Yüksek lisans tezi, İstanbul Üniversitesi, İstanbul.

Dülger, M. V. (2020). *Bilişim suçları ve internet iletişim hukuku*. Ankara: Seçkin Yayıncılık.

Dülger, M.V. (2015). *Bilişim suçları ve internet iletişim hukuku.* Ankara: Seçkin Yayıncılık.

ECHR. (2000, 4 May) Rotaru v. Romania, Application no. 28341/95.

ECHR. (2018, 24 April) Benedict v. Slovenia, Application no. 62357/14.

ECHR. (2021, 25 May) Case of big brother watch and others v. The United Kingdom, Application no. 58170/13 62322/14 24960/15.

Eralp, Ö. (2022). Avrupa Konseyi siber suç sözleşmesi – Açıklayıcı memorandum [İnternet ve Hukuk Platformu -İ v H P- çevirisi]. 07 Kasım 2022 tarihinde https://www.eralp.av.tr/avrupa-konseyi-siber-suc-sozlesmesi-aciklayici-memorandum-internet-ve-hukuk-platformu-i-v-h-p-cevirisi/ adresinden erişildi.

Erdoğan, B., & Öztürk, E. (2020). *Siber psikopatolojiler, siber psikoloji.* 1. baskı. Ankara: Türkiye Klinikleri.

Eroğlu, D. (2022a) Belgeleriyle BTK-gate (4) | Kitlesel gözetim aralıksız devam ediyor: İşte BTK'nın bir günde hakkımızda öğrendiği her şey, Medyascope. 12 Eylül 2022 tarihinde https://medyascope.tv/2022/08/10/belgeleriyle-btk-gate-4-kitlesel-gozetim-araliksiz-devam-ediyor-iste-btknin-bir-gunde-hakkimizda-ogrendigi-her-sey/ adresinden erişildi.

Eroğlu, D., (2022b) Belgeleriyle BTK-Gate (1): Türkiye'deki tüm kullanıcıların internet hareketleri, yaklaşık bir buçuk yıldır, kimlikleri ve kişisel verileriyle birlikte BTK'ya akıyor, Medyascope. 12 Eylül 2022 tarihinde https://medyascope.tv/2022/07/21/belgeleriyle-btk-gate-turkiyedeki-tum-kullanicilarin-internet-hareketleri-yaklasik-bir-bucuk-yildir-kimlikleri-ve-kisisel-verileriyle-birlikte-btkya-akiyor/ adresinden erişildi.

Erol, O., Şahin, Y. L., Yılmaz, E., & Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *Journal of Human Sciences, 12*(2), 75-91.

European Commission. (2020). Cybersecurity our digital anchor europen perspective report. 02 Kasım 2022 tarihinde https://ati.ec.europa.eu/news/what-way-forward-towards-cyber-secure-future adresinden erişildi.

Facebook'a Cambridge Analytica Davası. (2018). DW. 10 Ağustos 2022 tarihinde https://www.dw.com/tr/facebooka-cambridge-analytica-davası/a-46810401 adresinden erişildi.

Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. 4th edition. London: Sage.

Fötinger, C. S., & Ziegler, W. (2004) *Understanding a hacker's mind: a psychological insight into the hijacking of identities.* Danube-University Krems, Austria: RSA Security.

Gedikli, A. T. (2020). Karşılaştırmalı hukukta internet ortamındaki asılsız bilgi paylaşımlarının önlenmesi. *Bilişim Hukuku Dergisi, 2*(2), 221-257.

Goldberg, I. (1996) Internet addiction disorder (IAD): Diagnostic criteria. 10 Ağustos 2022 tarihinde http://www-usr, rider, edu/~suler/psycyber/ supportgp.html adresinden erişildi.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20. doi: 10.1007/s11416-006-0015-z.

Göktürk, N. (2016). Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması suçu (TCK M. 133). *Türkiye Adalet Akademisi Dergisi,* (24), 149-198.

Görkemli, B. (2015). *Yargı kararları ışığında Türk Hukuku'nda internet erişminin engellenmesi.* Birinci Baskı. Ankara: Adalet Yayınevi.

Gürkan, M. F. (2013). Düzenleyici ve denetleyıci kurum olarak bilgi teknolojileri ve iletişim kurumu (BTK). *İnönü Üniversitesi Hukuk Fakültesi Dergisi, 4*(2), 333-356.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing, 30*, 1-19.

Interpol. (2022) BT's Report-CISOs under the spotlight ©2022. Cybercrime threat response. 01 Eylül 2022 tarihinde https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response adresinden erişildi.

It Specialist Description. (2022). İndeed. 10 Aralık 2022 tarihinde https://www.indeed.com/hire/job-description/it-specialist adresinden erişildi

ITU. (2011). Understanding cybercrime: A guide for developing countries. 18 Ekim 2022 tarihinde https://www.itu.int/ITU-D/cyb/ adresinden erişildi.

İstanbul Bilgi Üniversitesi. (2018). *Avrupa veri koruma mevzuatı el kitabı*. İstanbul: İstanbul Bilgi Üniversitesi.

İstanbul Bilgi Üniversitesi. (2022). Fidye yazılımı nedir? Nasıl korunulur? 09 Ekim 2022 tarihinde https://it.bilgi.edu.tr/en/security/ransomware/ adresinden erişildi.

Jordan, T., & Taylor, P. A. (1998). Sociology of hackers, *Sociological Review*, *46*(4), 757-81.

Kabataş Yılmaz, B. (2019). *Türk hukukunda telekomünikasyon yoluyla yapılan iletişimin denetlenmesi tedbiri*. Yayımlanmamış yüksek lisans tezi, İstanbul Üniversitesi İstanbul.

Karadeniz, Y. (2022). Avrupa konseyi sanal ortamda işlenen suçlar sözleşmesi ve Türk Hukuku'nda karşılığı. *Güvenlik Bilimleri Dergisi, 11*(1), 109-134.

Karakurt Eren, A. (2020). Bilişim alanında suçların veya bilişim sistemlerinin araç olarak kullanıldığı diğer suçların işlenmesi amacıyla cihaz, program, şifre ya da güvenlik kodlarının üretilmesi, yayılması veya bulundurulması suçu. *Türkiye Adalet Akademisi Dergisi, 11*(43), 219-246.

Kaspersen, H., & Schwerha J. (2011). EU/COE joint project on regional cooperation against cybercrime. 10 Eylül 2022 tarihinde https://www.combattingcybercrime.org/files/virtual-library/international-cooperation/article-15-–conditions-and-safeguards-under-the-budapest-convention-on-cybercrime.pdf adresinden erişildi.

Kaspersky. (2022). Rootkit nedir – Tanım ve açıklama. 09 Ekim 2022 tarihinde https://www.kaspersky.com.tr/resource-center/definitions/what-is-rootkit adresinden erişildi.

Kaya, İ. S., & Çakır, A. (2020). Yasak Cihaz ve Programlar Suçu. İ*stanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi,* 19(38), 32-55.

Kaya, M. B. (2022) Bilişim suçları istatistikleri: İstatistiklerle bilişim suçları: Siber suçlara genel bir bakış. 9 Eylül 2022 tarihinde https://mbkaya.com/bilisim-suc-istatistik-turkiye-siber-guvenlik/ adresinden erişildi.

Keskin, S. (2001). Avrupa konseyi siber suç sözleşmesinde ceza muhakemesine ilişkin hükümlerin değerlendirilmesi. *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası, 59*(1-2), 155-180.

Ketizmen, M. (2008). *Türk ceza hukukunda bilişim suçları.* Ankara: Adalet Yayınevi.

Kılıç, M. S., Uluyol, Ç., Ocak M. A., Karataş, E., Gökçearslan, Ş., Çubukçu, A., Aytekin, A., Doğan, T., Yalçın, N., Çakır, H., Benzer, R., & Yalman, Y. (2014). *Güncel tehdit: Siber suçlar*. Ankara: Seçkin Yayıncılık.

Kızılkaya, E. (2022) BTK'dan "BTK-gate" açıklaması geldi, hukukçulara göre suç işleniyor, Juorno, 12 Ekim 2022 tarihinde https://journo.com.tr/btkgate-btk-cevap adresinden erişildi.

Kiger, M., Arkin, O., & Stutzman, J. (2004). *Profiling. In The Honeynet Project Know Your Enemy: Learning about Security Threats*. Boston: Addison Wesley.

Korkmaz, F. (2020). Dolandırıcılık suçunun bilişim sistemlerinin araç olarak kullanılması suretiyle işlenmesi. *Ankara Üniversitesi Hukuk Fakültesi Dergisi, 69*(3), 1415-1436.

Kosta, E., & Valcke, P. (2006). Retaining the data retention directive. *Computer Law & Security Review, 22*(5), 370-380.

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice, 61*(3), 381-398. https://doi.org/10.1111/hojo.12485

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Devıant Behavıor, 37*(3), 263–280 Http://Dx.Doi.Org/10.1080/01639625.2015.1012409

Li, X. (2016). Defining cybercrime based on roles of data processing systems. Gifford M. Potts M (Ed.), *Pandora's box 2016: Law and technology* içinde. St. Lucia: Worldwide Printing Fortitude Valley, 127-144.

Li, X. (2017). Cyber crime and legal countermeasures: A historical analysis. *International Journal of Criminal Justice Sciences, 12*(2), 196-207. doi: 10.5281/zenodo.1034658.

Li, X. (2017a). A review of motivations of ıllegal cyber activities. *Criminology & Social Integration Journal, 25*(1), 110-126.

Maiwald, E. (2003). *Network Security: A Beginner's Guide*, second edition, California, USA: McGraw- Hill Osborne Media.

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.

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: findings from a nationally representative panel study. *American Journal of Criminal Justice, 46*(6), 862-881. doi: 10.1007/s12103-021-09665-2

Mesko, G., & Bernik, I. (2011, September 12-14). *Cybercrime: Awareness and fear, slovenian perspectives*, Proceedings of the 2011 European Intelligence and Security Informatics Conference, Athens, Greece, DOI 10.1109/EISIC.2011.12

Moitra, S. (2005). Developing policies for cybercrime. *European Journal of Crime, Criminal Law and Criminal Justice, 13*(3), 435-464.

NASD Investor Education Foundation. (2006). Investor fraud study: Final report. 10 Eylül 2022 tarihinde http://www.sec.gov/news/press/extra/seniors/nasdfraudstudy051206.pdf adresinden erişildi.

Nebil, F. (2009). (Çevirimiçi) 05 Temmuz 2020 tarihinde https://turk-internet.com/microsoft-120-nin-ustunde-internet-cafe-basti-ve-tazminat-lisans-parasi-istedi-3/ adresinden erişildi.

Nebil, F. (2017). (Çevirimiçi) 05 Temmuz 2020 tarihinde https://t24.com.tr/yazarlar/fusun-sarp-nebil/yillarca-pazarda-sikinti-yaratan-bsanin-turkiyedeki-faaliyet-izni-yenilenmedi,17024 adresinden erişildi.

Nebil, F. (2018). (Çevirimiçi). 05 Temmuz 2022 tarihinde http://www.turk-internet.com/portal/yazigoster.php?yaziid=59945 adresinden erişildi.

Network uzmanı nedir? (2022) Kariyer. 10 Aralık 2022 tarihinde https://www.kariyer.net/pozisyonlar/network+uzmani/nedir adresinden erişildi.

Okuyucu Ergün, G. (2013). Banka veya kredi kartlarının kötüye kullanılması. *Prof. Dr. Nur Centel'e Armağan, 19*(2), 1065-1086.

O'Malley, G. (2013). Hacktivism: cyber activism or cyber crime. *Trinity College Law Review, 16,* 137-160.

Orta Doğu Teknik Üniversitesi. (2019) Spyware nedir? 12 Eylül 2022 tarihinde https://faq.cc.metu.edu.tr/tr/sss/spyware-nedir adresinden erişildi.

Orta, M. (2015). *Bilişim suçları ve elektronik delillerin toplanması muhafazası değerlendirilmesi sunulması (Adli Bilişim).* Ankara: Yetkin Yayınları.

Öztürk, B. & Erdem, M. R. (2008). *Uygulamalı ceza muhakemesi hukuku*. 12. baskı. Ankara: Seçkin Yayıncılık.

Öztürk, E. (2020). *Siber toplumlar ve siber hayatlar: dissosiyojen bir ajan olarak dijital iletişim ağları [Cyber societies and cyber lives: Digital communication networks as a dissociogenic agent]*. *Siber psikoloji.* 1. baskı. Ankara: Türkiye Klinikleri.

Öztürk, E., & Derin, G. (2020). *Klinik siber psikolojiden adli siber psikolojiye: Siber travma ve siber re-viktimizasyon. Siber psikoloji*. 1. baskı. Ankara: Türkiye Klinikleri.

Öztürk, E., Ateş, A., & Erdoğan, B. (2020). *Siber suçların hukuksal yönleri ve psikolojik dinamikleri. Siber psikoloji.* 1. baskı. Ankara: Türkiye Klinikleri.

Project Manager Description. (2022). İndeed. 10 Aralık 2022 tarihinde https://www.indeed.com/hire/job-description/project-manager?co=US adresinden erişildi.

Recro Digital Marketing. (2022a). Recro digital marketing ©2022. We are social 2022 Türkiye sosyal medya kullanım verileri. 22 Eylül 2022 tarihinde https://recrodigital.com/we-are-social-2022-turkiye-sosyal-medya-kullanimi-verileri/ adresinden erişildi.

Recro Digital Marketing. (2022b). Recro digital marketing ©2022. Dünyada ve Türkiyede sosyal medya kullanımı 2022. 22 Eylül 2022 tarihinde https://recrodigital.com/dunyada-ve-turkiyede-internet-sosyal-medya-kullanimi-2022/ adresinden erişildi.

Resmi Gazete. (2014a, 9 Ağustos). Milletlerarası sözleşme. 12 Ekim 2022 tarihinde https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm adresinden erişildi.

Resmi Gazete. (2014b, 9 Ağustos). Sanal ortamda işlenen suçlar sözleşmesi. 07 Kasım 2022, tarihinde https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm adresinden erişildi.

Samet, R., & Aslan, Ö. (2018). Kötü amaçlı yazılımlar ve analizi. Sağıroğlu Ş. ve Alkan M. (Ed). *Siber güvenlik ve savunma farkındalık ve caydırıcılık* içinde. 1. baskı, Ankara: BGD Siber Güvenlik ve Savunma Kitap Serisi, 225-251.

Sanford, L. (2016). *Moskowitz, cybercrime and business strategies for global corporate security*. Oxford: Elsevier Inc.

Sevük, H. Y. (2008). Haberleşmenin gizliliğini ihlal suçu. *Dicle Üniversitesi Hukuk Fakültesi Dergisi*, *12*(16-17-18-19), 159-195.

Shinder, D.L., & Tittel, E. (2002). *Scene of the cybercrime: Computer forensics handbook.* Rockland: Syngress Publishing Inc.

Sistem Uzmanı Nedir? (2022) Kariyer. 10 Aralık 2022 tarihinde https://www.kariyer.net/pozisyonlar/sistem+uzmani/nedir adresinden erişildi.

Smith, R., & Perry, M. (2021). Fake news and the convention on cybercrime. *Athens Journal of Law, 7* (3), 335-358.

Smith, R.G., Grabosky, P., & Urbas, G. (2009). *Cyber criminals on trial*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511481604

Stratonov, V., Slinko D., & Slinko S.(2021). Some types of computer crime and cybercrime in Ukraine. *Access to Justice in Eastern Europe*, 3(11) 191–197. DOI: 10.33327/AJEE-18-4.3-n000078

Suler, J. (2017). The dimensions of cyberpsychology architecture. *Boundaries of Self and Reality Online: Chapter 1, 2017*: 1-23. DOİ: 10.1016/B978-0-12-804157-4.00001-3

Symantec. (2021). Symantec threat hunter team, the threat landscape in 2021. 09 Ekim 2022 tarihinde https://symantec.drift.click/Threat_Landscape_2021_Whitepaper adresinden erişildi.

Şar, V. (2014). Disosiyatif Bozukluklar. Tükel R., Çakır S. (Ed.), *Psikiyatri*. İstanbul: Nobel Tıp Kitapevi, 67-72.

T.C. Anayasa Mahkemesi. (2015c, 19 Mart). Esas Sayısı 2014/180 Karar Sayısı 2015/30.

T.C. Anayasa Mahkemesi. (2015d, 12 Kasım). Esas Sayısı 2015/32 Karar Sayısı 2015/102.

T.C. Anayasa Mahkemesi. (2014, 29 Mayıs). Youtube LLC corporation service company ve diğerleri başvurusu (2014/4705). 02 Ekim 2022 tarihinde https://kararlarbilgibankasi. anayasa.gov.tr/BB/2014/4705 adresinden erişildi.

T.C. Anayasa Mahkemesi. (2014a, 25 Haziran). Tuğba Arslan Başvurusu, Başvuru numarası. 2014/256.

T.C. Anayasa Mahkemesi. (2014b, 09 Nisan). Esas Sayısı 2013/122, Karar Sayısı 2014/74.

T.C. Anayasa Mahkemesi. (2014c, 02 Ekim). Esas Sayısı 2014/149 Karar Sayısı 2014/151.

T.C. Anayasa Mahkemesi. (2014d, 25 Aralık). Esas Sayısı 2014/74 Karar Sayısı 2014/201.

T.C. Anayasa Mahkemesi. (2014e, 29 Mayıs). Youtube LLLC Corporation Service Company ve Diğerleri Başvurusu, Başvuru numarası: 2014/4705.

T.C. Anayasa Mahkemesi. (2015a, 02 Ekim). Esas Sayısı 2014/149 Karar Sayısı 2014/151.

T.C. Anayasa Mahkemesi. (2015b, 08 Aralık). Esas Sayısı 2014/87 Karar Sayısı 2015/112.

T.C. Anayasa Mahkemesi. (2021, 30 Haziran). Ertan Erçıktı Başvurusu, Başvuru no. 2018/14040.

T.C. Anayasa Mahkemesi. (2022, 16 Mart). Metin Kayaokay Başvurusu, Başvuru no. 2019/7831.

T.C. Danıştay. (2019, 12 Aralık). 13. Daire Esas Sayısı 2013/239 Karar Sayısı 2019/4266.

T.C. Rekabet Kurumu. (b.t.). Rekabet kurumu hakkımızda. 07 Kasım 2022, tarihinde https://www.rekabet.gov.tr/tr/Sayfa/Kurumsal/hakkimizda adresinden erişildi. (b.t.).

T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı. (2014). Sektörel SOME kurulum ve yönetim rehberi. 20 Aralık 2021 tarihinde https://dsy.usom.gov.tr/usom/19/02/ 190211090404_Sektorel%20SOME%20Rehberi.pdf adresinden erişildi.

T.C. Yargıtay. (2015, 17 Haziran). HGK Esas Sayısı 2014/56 Karar Sayısı 2015/1679, (Lexpera).

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics*. 6th edition. Boston: Pearson.

Taneri, G. (2018). Müstehcenlik suçu. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi, 13* (1), 561-624.

Tao, R., Huang, X., Wang, J., Zhang, H., Zhang, Y., & Li, M. (2010). Proposed diagnostic criteria for internet addiction. *Addiction, 105*(3), 556-564.

Taşçıoğlu, M. (2019). Dijital korsanlığa karşı lisans öğrencilerinin olumsuz tutumlarını etkileyen faktörler. *Öneri Dergisi, 14*(52), 340-355. doi: 10.14783/Maruoneri.594966

TBMM. (2022, 1 Haziran). Türkiye Büyük Millet Meclisi Dijital Mecralar Komisyonu Tutanak Dergisi 1 Haziran 2022 Çarşamba 9. Toplantısı. 12 Ekim 2022 tarihinde https://www5.tbmm.gov.tr/develop/owa/komisyon_tutanaklari.goruntule?pTutanakId=2970 adresinden erişildi.

The Software Alliance BSA. (2016). Global software survey: Seizing opportuntiy through licence complience. 20 Eylül 2022 tarihinde https://globalstudy.bsa.org/2016/downloads/studies/BSA_GSS_US.pdf adresinden erişildi.

The Software Alliance BSA. (2018) Global software survey: Software management security imperative business opportunity ©2022. 10 Eylül 2022 tarihinde https://gss.bsa.org adresinden erişildi

The Software Alliance BSA. (2020) Priorities in Intellectual Property. 15 Ekim 2022 tarihinde https://www.bsa.org/policy-filings/bsa-priorities-in-ip adresinden erişildi.

Topçuoğlu, P. (2022). *Türk ceza kanunu kapsamında bilişim sistemine girme suçu*. Yüksek lisans tezi, Bahçeşehir Üniversitesi, İstanbul.

Trend Micro Incorporated. (2021). Navigating new frontiers trend micro 2021 annual cybersecurity report. 10 Şubat 2022 tarihinde https://documents.trendmicro.com/assets/rpt/rpt-navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report.pdf adresinden erişildi.

Trend Micro Incorporated. (2022). Defending the expanding attack surface: Trend micro 2022 midyear cybersecurity report. 18 Ekim 2022 tarihinde https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/defending-the-expanding-attack-surface-trend-micro-2022-midyear-cybersecurity-report adresinden erişildi.

Urueña, A., Torres, A., Vivas, P. & Herrero, J. (2022). Smartphone addiction, social support, and cybercrime victimization: A discrete survival and growth mixture model. *Psychosocial Intervention, 31*(1), 59-66. https://doi.org/10.5093/pi2022a3

USOM Hakkımızda. (2022). BTK. 09 Eylül 2022 tarihinde https://www.usom.gov.tr/hakkimizda adresinden erişildi.

Ünal, M. B. (2021) Seçili ülke örneklerinde sosyal medya şirketlerinin yasal yükümlülükleri. 10 Ekim 2022 tarihinde https://www5.tbmm.gov.tr/yayinlar/Secili_ulke_orneklerinde_sosyal_medya_sirketlerinin_yasal_yukumlulukleri.pdf adresinden erişildi.

Ünal, O. G. (2011). *Bilgisayarlarda bilgisayar programlarında ve kütüklerinde arama kopyalama ve elkoyma.* Yayımlanmamış yüksek lisans tezi, Gazi Üniversitesi, Ankara.

Vatis, M.A. (2010). *The Council of Europe Convention on Cybercrime.* Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy, National Academies Press, 219-220.

Yankın, F.B. (2018). Dijital dönüşüm sürecinde çalışma yaşamı [Work life in digital transformation process]. *Trakya Üniversitesi İktisadi ve İdari Bilimler Fakültesi E-Dergisi*, *7*(2), 1-38.

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

Yazılım Uzmanı Ne iş yapar? (2022) 10 Aralık 2022 tarihinde https://www.kariyer.net/pozisyonlar/yazilim+uzmani/nedir adresinden erişildi.

Yesir, S. (2021). *Zararlı yazılım tespiti için yazılım davranış analizi*. Yüksek lisans tezi, Gebze Teknik Üniversitesi, Kocaeli.

Yılmaz, E. (2021) 10 Aralık 2022 tarihinde https://turk-internet.com/microsoft-ve-fortinet-aciklarini-kullanan-iranli-hackerlara-karsi-uyari-yayinlandi/ adresinden erişildi.

Yılmaz, O. B. (2021). *Türkiye ve Avrupa Birliği'nde kişisel verilerin korunması ve uygulanacak hukuk*. Yayımlanmamış yüksek lisans tezi, Beykent Üniversitesi, İstanbul.

Yong, P. (2019). Legislation on the new types of cybercrime and ıts application. *Social Sciences in China, 40*(3), 152-173, DOI: 10.1080/02529203.2019.1639961

Young, K. (1996). Internet addiction: The emergence of a new clinical disorder. *Cyber Psychology and Behavior, 3*, 237-244.

Yatsyshyn, M.Y. (2018). Modern approaches to cybercrime classification in International Law. 10 Aralık 2022 tarihinde https://conference.nau.edu.ua/index.php/Congress/Congress 2018/paper/viewFile/5271/4276 adresinden erişildi.

8. EKLER

EK 1

SİBER SUÇ FARKINDALIĞI ve PROFESYONELLERİN TUTUMLARI

BİLGİLENDİRİLMİŞ GÖNÜLLÜ KATILIM FORMU

Değerli Katılımcı,

Bu araştırma, İstanbul Üniversitesi Cerrahpaşa Adli Tıp Enstitüsü Sosyal Bilimler Anabilim Dalı Dr. Öğretim Üyesi Y. Tunç Demircan danışmanlığında Sosyal Bilimler Doktora Programı öğrencisi Elif Yorgancıoğlu tarafından doktora tez çalışması olarak yürütülmektedir. Söz konusu araştırma için; bilişim sektörü çalışanlar hakim, savcı ve avukatlar tarafından siber suçların nasıl algıladığını tespit etmeyi hedeLeyen bir görüşme formu kullanılmaktadır.

Çalışmaya katılım gönüllülük esasına dayanmaktadır. Yaklaşık 10 dakika sürecek araştırma kapsamında 4 adet soru formu yanıtlamanız için sizinle paylaşılacaktır. Soru formu; Kişisel Bilgi Formu, Problemli İnternet Kullanım Ölçeği, Kişisel Siber Güvenliği Sağlama Ölçeği, Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu olmak üzere 4 bölümden oluşmaktadır. Sorulara vermiş olduğunuz yanıtlar araştırmacı tarafından gerek bilgisayar ortamında gerekse basılı olarak itina ile saklanacak olup veriler sadece akademik amaçlı kullanılacaktır.

Soru formunda isminiz sorulmamakta ve kimliğinizin ortaya çıkmasına sebep olabilecek herhangi bir soru, yönlendirme veya alan bulunmamaktadır. Mümkün olduğunca madde atlamamanız ve soruları yarım bırakmamanız büyük önem arz etmektedir. Araştırma ile ilgili herhangi bir sorunuz için

araştırmacıya ..... adresinden ulaşabilirsiniz. İlginiz ve katkılarınız için teşekkür ederiz.

Bilgilendirilmiş Gönüllü Olur Formu'ndaki tüm açıklamaları okudum. Bu araştırmaya kendi isteğimle, gönüllü olarak katılıyorum ve soruları cevaplamaya başladıktan sonra istediğim zaman katılmaktan vazgeçebileceğim hakkında bilgilendirildim. Bana anlatılan bu araştırmaya verilen ölçekleri yanıtlayarak, herhangi bir baskı ve zorlama olmaksızın kendi rızamla katılmayı ve verdiğim bilgilerin bilimsel amaçlı yayımlarda kullanılmasını kabul ediyorum.

Çalışmaya katılmayı kabul ediyorum.

*****
Gerekli

KİŞİSEL BİLGİ FORMU

1- Cinsiyetiniz?*
Yalnızca bir şık işaretleyin.

- ◯ Kadın
- ◯ Erkek

2- Yaşınız?*
.....

3- Eğitim durumunuz nedir? (Son mezun olduğunuz okul) *
Yalnızca bir şık işaretleyin.

- ◯ Lise
- ◯ Üniversite
- ◯ Lisansüstü
- ◯ Doktora

4- Medeni durumunuz nedir?

- ◯ Evli
- ◯ Bekar
- ◯ Boşandım
- ◯ Dul

5- Mesleğiniz nedir?*
Yalnızca bir şık işaretleyin.

- ◯ Bilişim Sektör Çalışanı
- ◯ Avukat
- ◯ Hakim
- ◯ Savcı

6- Bilişim sektörü çalışanı iseniz çalıştığınız kurumdaki pozisyonunuz/göreviniz?
…….

7- İnternete hangi kaynaklar üzerinden bağlanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
Uygun olanların tümünü işaretleyin

- ◯ Bağlanmıyorum
- ◯ Evden
- ◯ İş yerinden
- ◯ Internet kafeden
- ◯ Cep telefonuyla
- ◯ Kamuya açık Wi-Fi alanlarından (Cafe- Belediye hotspot'u- havalalanı hotspot'u vb.)
- ◯ Diğer ise belirtiniz

8- İnterneti en çok hangi amaçlarla kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

- ◯ Haber Okumak
- ◯ Video izlemek
- ◯ TV/Dizi/Film izlemek
- ◯ Araştırma Yapmak
- ◯ Sosyal Medyada Zaman Geçirmek
- ◯ İş Yapmak
- ◯ Diğer ise belirtiniz

9- Bilgisayarımda antivirüs programı kullanıyorum.
Yalnızca bir şık işaretleyin. *

- ◯ Evet
- ◯ Hayır

10- 9. soruya verdiğiniz cevap evet ise hangi antivirüs programını kullanıyorsunuz?
Yalnızca bir şıkkı işaretleyin.

- ◯ Avast
- ◯ Norton
- ◯ Kaspersky
- ◯ Mcafee
- ◯ Diğer:

11- Bilgisayarınızda hangi işletim sistemini kullanıyorsunuz? *
Yalnızca bir şıkkı işaretleyin.

- ◯ Microsoft Windows
- ◯ Linux
- ◯ Mac OS
- ◯ Amiga OS
- ◯ Diğer:

12-Akıllı telefonunuzda hangi işletim sistemini kullanıyorsunuz?

- ◯ Ios
- ◯ Androıd
- ◯ BlackBerry OS
- ◯ Windows Phone
- ◯ Diğer

13-Akıllı telefonunuzda hangi uygulamaları aktif olarak kullanıyorsunuz?
Uygun olanların tümünü işaretleyin.

- ◯ Bankacılık/Finans uygulamaları
- ◯ Oyun uygulamaları
- ◯ İletişim uygulamaları (E-posta, mesajlaşma vb)
- ◯ İş uygulamaları

- ◯ Sosyal medya uygulamaları
- ◯ Alışveriş uygulamaları
- ◯ Müzik uygulamaları
- ◯ Yemek uygulamaları
- ◯ Sağlık uygulamaları
- ◯ Haber uygulamaları
- ◯ Seyahat uygulamaları
- ◯ Diğer:

14-Hangi sosyal ağları aktif olarak kullanıyorsunuz? *

Uygun olanların tümünü işaretleyin.

- ◯ Facebook
- ◯ Twitter
- ◯ Youtube
- ◯ Instagram
- ◯ Linkedin
- ◯ Wordpress
- ◯ Pinterest
- ◯ Tumblr
- ◯ Snapchat
- ◯ Diğer:

15-İnternette ne kadar süre vakit geçiriyorsunuz?*

Yalnızca bir şıkkı işaretleyin.

- ◯ Günde 2 saat ve daha az
- ◯ Günde 2-4 saat
- ◯ Günde 4 saatten fazla

16. İhtiyaç duyduğunuzda bilgisayarınızda lisanssız yazılım kullanır mısınız?* (Örneğin: Microsoft Office ürünleri vb.)

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır

17. Gerekli olduğunu düşündüğünüzde hakkında erişim engelleme kararı olan sitelere girer misiniz? (Örn; Wikipedia)

- ◯ Evet
- ◯ Hayır

18. Erişime engelli sitelerin izlendiğini düşünüyor musunuz?*

Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır
- ◯ Fikrim Yok

19. Şimdiye kadar internet ortamında sizi mağdur edecek en az bir olayla karşılaştınız mı?*
Yalnızca bir şıkkı işaretleyin.

- ◯ Evet
- ◯ Hayır

20. Evet ise kaç kez internet ortamında mağduriyet yaşadınız.

……..

21. Evet ise bu mağduriyetin ne ve/veya neler olduğunu kısa bir şekilde açıklayınız.

…….

22- 19. soruya cevabınız evet ise mağduriyetiniz sonucunda ne yaptınız? Kısaca açıklayınız. (Örn; "Uğradığım siber saldırı konusunda şikayetçi oldum ve antivrüs programı kullanmaya başladım", "Güvenli olmadığını düşündüğüm siteleri ve uygulamaları kullanmadım", "Hiçbir şey yapmadım" gibi.....)

……

23-Sosyal medya hesaplarınızdaki (Facebook, Twitter, vb.) kişisel bilgi ve verilerinizle ilgili bilişim suçu mağduru olmamak adına ne gibi önlem/önlemler alıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz.)*
Uygun olanların tümünü işaretleyin.

- ◯ Herhangi bir önlem almıyorum
- ◯ Hesabımı kilitli tutuyorum
- ◯ Paylaşımlarımı görebilecek kişileri sınırlandırıyorum
- ◯ Telefon numaramı hesabıma tanımlıyorum
- ◯ Tanımadığım kişilerden gelen arkadaşlık isteklerini kabul etmiyorum
- ◯ Hesabıma benden habersiz erişimleri engellemek için farklı cihazlardan giriş bildirimlerini aktif hale getiriyorum
- ◯ Güvenli gözükmeyen reklam, bağlantı vb. linkleri açmıyorum Sosyal medya hesabım yok
- ◯ Diğer: …….

Problemli İnternet Kullanım Ölçeği

(PİKÖ)

Açıklama: Bu anket, bireylerin internet kullanım davranışlarını betimlemek için hazırlanmıştır. Sizden istenen, internet kullanırken genellikle gösterdiğiniz davranışları dikkate alarak, aşağıdaki ifadelerden her birinin size uygunluk derecesini belirlemenizdir

Bu amaçla, ilk önce her bir ifadeyi okuyunuz ve daha sonra her bir ifadenin karşısındaki **"Tamamen Uygun", "Oldukça Uygun", "Biraz Uygun" "Nadiren Uygun",** ve **"Hiç Uygun Değil"** seçeneklerinden kendi durumunuza uygun olan bir seçeneği belirleyiniz. Bu seçeneği belirledikten sonra o seçeneğe ait parantezin içerisine çarpı (X) işareti koyunuz.

Lütfen, hiçbir maddeyi boş bırakmayınız. Yanıtlarken kendi internet kullanım davranışlarınızı olduğu gibi yansıtmanız, sonuçların daha sağlıklı değerlendirilmesine katkıda bulunacaktır. Yanıtlarınız ile bu bilimsel araştırmaya katıldığınız için teşekkürler.

24- *Her satırda yalnızca bir şıkkı işaretleyin**

	Tamamen Uygun	Oldukça Uygun	Biraz Uygun	Nadiren Uygun	Hiç Uygun Değil
İnternet bağlantımı kesmeye her karar verdiğimde kendi kendime "birkaç dakika daha" diyorum….....					
İnternette geçirdiğim zaman çoğunlukla uyku süremi azaltıyor					
İnternet ortamında elde ettiğim saygıyı günlük yaşamımda bulamıyorum.					
İnternette, diğer ortamlara göre daha kolay ilişki kuruyorum					
İnternette ismimi gizlemek beni daha özgür kılıyor					
Çok istememe rağmen interneti uzun süre kullanmaktan bir türlü vazgeçemiyorum.					
İnternete gerekmedikçe girmekten kaçınıyorum					
Yalnızlığımı internetle paylaşıyorum					
Tekrar internete girene kadar kendimi huysuz, karamsar, rahatsız ve huzursuz hissediyorum					
Problemlerimden bunaldığımda sığındığım en iyi yer internettir					
Birisi internette ne yaptığımı sorduğunda savunmacı ve gizleyici oluyorum					
Planladığımın dışında fazladan bir dakika bile interneti kullanmıyorum.					

İnternette bağlantı kurduğum insanlara kendimi daha iyi anlatıyorum					
İnternete giremediğim zaman, internette olmayı düşünmekten kendimi alıkoyamıyorum					
İnternette, kontrol benden çıkıyor					
İnternet yüzünden yemek yemeyi unuttuğum zamanlar oluyor					
İnternette daha fazla vakit geçirmek için günlük işlerimi ihmal ediyorum					
Sosyal aktiviteler için para harcamaktansa internete erişmek için harcamayı tercih ediyorum					
Sürekli ziyaret ettiğim internet sitelerine bir gün dahi girememeye tahammül edemiyorum					
İnternet kullandığım süre boyunca her şeyi unutuyorum					
Yapmam gereken işler çoğaldıkça, internet kullanma isteğim de o ölçüde artıyor					
İnternet, yapmam gerekenleri ertelemek için vazgeçilmez bir araçtır					
İnternet kullanımım, benim için önemli kişilerle olan ilişkilerimde problem yaşamama neden oluyor					
İnternet kullanırken başkalarının beni meşgul etmesine öfkeleniyorum					
İnterneti kullanmasam bile sürekli aklımda					
İnternette kendimi çok özgür hissediyorum					
İnternette çok fazla zaman geçirdiğim için başarım düşüyor					
İnternet kullanmayı bırakamadığım için randevularıma veya derslerime geç kalıyorum					
Sabahları uyandığımda bir an önce internete bağlanmak istiyorum					
İnternet kullanırken zamanın nasıl geçtiğini hiç anlayamıyorum					
İnternet beni kendisine esir ediyor					
İnternet ortamında genellikle kendimi huzurlu hissediyorum					
İnternet yoluyla iletişim kurmayı, yüz yüze iletişim kurmaya tercih ediyorum					

Kişisel Siber Güvenliği Sağlama Ölçeği

İnternet ve bilişim sistemlerini kullanırken genellikle gösterdiğiniz davranışları dikkate alarak, aşağıdaki ifadelerden kendinize en uygun seçeceği işarertleyin.

25- *Her satırda yalnızca bir şıkkı işaretleyin.**

	Hiçbir Zaman	Nadiren	Arasıra	Sık Sık	Her Zaman
Web sayfalarında güvenlik bağlantılarını (https://) ve sertifikalarını kontrol ederim					
Kullandığım yazılımları güncellerim.					
Bilgisayarımda antivirus yazılımı bulundururum					
Şifrelerimi belirlerken basit dizilimler kullanmaktan kaçınırım					
İnternet şifrelerimin tümünün aynı olmasına dikkat ederim					
Web tarayıcımın güvenlik ayarlarını düzenlerim					
E- posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım					
Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim					
İnternet üzerinden yapılan para ve kontör isteklerini dikkate almam.					
Tanımadığım kişilerden gelen sosyal ağ arkadaşlık isteğini kabul etmem.					
Güvenmediğim sitelere üye olmam					
Tanımadığım kişiler ile web kamerası kullanarak sesli ve görüntülü iletişim kurarım					
İnternet ortamında gerektiğinde kişisel bilgilerimi (TC No,Doğum tarihi,Gsm No vb.)paylaşırım					
Web geçmişimi temizlerim					
İnternet bankacığı işlemlerini şahsi bilgisayarımdan yaparım.					
Online alışveriş işlemlerini şahsi bilgisayarımdan yaparım					
Tanımadığım kişilerden gelen e-posta eklerini açarım					
Sosyal paylaşım sitelerinde kişisel bilgilerime yer veririm					
İnternet üzerinden yer bildirimi yaparım					
Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım					
Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım					
Güvenmediğim sitelerden dosya indirmem					
Sosyal ağlarda yer alan reklamlar üzerinden alışveriş yaparım					
Sosyal ağ - e-posta gibi hesaplarda işim bittiğinde oturumu kapatırım					
Güvenmediğim sitelerden dosya indirmem					

Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu

Bilişim suçu düzenlemelerine ilişkin düşüncelerinizi belirleme amaçlı bazı ifadeler sunulmuştur. Her cümleyi okuduktan sonra tabloda ilgili ifadeye katılma durumunuzu belirtiniz.

26- *Her satırda yalnızca bir şıkkı işaretleyin**

	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılıyorum
Üçüncü bir kişi tarafından şahsi bilgisayarıma izinsiz şekilde erişilmesi suç oluşturur					
Üçüncü bir kişi tarafından şahsi bilgisayarıma/tabletime/cep telefonuma izinsiz şekilde erişilerek bir dosyamın silinmesi suç oluşturur					
Lisanssız yazılım kullanmak suçtur					
Hırsızlığın bilişim sistemini kullanmak suretiyle gerçekleştirilmesi hırsızlığın basit haline göre daha ağır ceza gerektirir					
Kişisel verilerimin izinsiz şekilde işlenmesi suç oluşturur					
Hakkında erişim engelleme kararı olan bir internet sitesine (IP değişikliği, DNS değiştirme, URL maskeleme, proxy kullanma ya da VPN kullanma gibi yöntemlerle) erişilmesi suç oluşturmaz					
Bilişim sistemleri aracılığıyla sosyal medyada hakarete uğramak hakaretin basit haline göre daha fazla cezayı gerektirir					
Elektronik imzamın rızam dışında kullanılması suç oluşturur					

9. ÖZGEÇMİŞ

Kişisel Bilgiler :

Adı : Elif
Soyadı : Yorgancıoğlu
E-posta Adresi :

Eğitim Durumu :

Derece	Bölüm/Program	Üniversite	Yıl
Lisans	Hukuk	T.C. Marmara Üniversitesi	2004-2008
Yüksek Lisans	Adli Tıp Enstitüsü Sosyal Bilimler ABD	T.C.İstanbul Üniversitesi	2009-2013
Doktora	Adli Tıp ve Adli Bilimler Sosyal Bilimler ABD	T.C. İstanbul Üniversitesi.-Cerrahpaşa	2016-2022

İş Deneyimi :

Yıl	Kurum	Görev
2014- Halen	Grid Telekomüniksyon Hiz. A.Ş.	Hukuk ve Regülsyon Yöneticisi
2013-2014	Doğa Bilişim Grup- Doğa Grup	Avukat

Akademik Deneyim :

Yıl	Üniversite/Bölüm/Program	Ders	Görev
2017-2018	Altınbaş Üniversitesi/Sosyal Hizmetler Bölümü	Hukuka Giriş	Misafir Öğretim Üyesi
2018	Esenyurt Üniversitesi/Fizik Tedavi ve Rehabilitasyon Bölümü	Sağlık Hukuku	Misafir Öğretim Üyesi

Yayınlar :

Yorgancıoğlu E.& Demircan T.Y. (2023). Bilgi teknolojileri ve iletişim kurumu tarafından toplanan internet trafik verilerinin kişisel verilerin korunması hakkı bağlamında değerlendirilmesi. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi.* Hukuk Sayısı Yaz (Eylül)