Türkiye Klinikleri Adli Tıp ve Adli Bilimler Dergisi
Turkiye Klinikleri Journal of Forensic Medicine and Forensic Sciences
Turkiye Klinikleri J Foren Sci Leg Med. 2023;20(2):75-85

ORİJİNAL ARAŞTIRMA ORIGINAL RESEARCH

DOI: 10.5336/forensic.2022-93950

Hukukçuların ve Bilişim Sektörü Çalışanlarının, Problemli İnternet Kullanım Davranışları ve Siber Güvenlik ile İlgili Tutumları: Korelasyonel Bir Çalışma

Legists and it Sector Employees Problematic Internet Utilization Behaviors and Approach to Cybersecurity: A Correlational Study

Elif YORGANCIOĞLU[a], Yusuf Tunç DEMİRCAN[a]

[a]İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, Sosyal Bilimler ABD, İstanbul, Türkiye

ÖZET Amaç: 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 tarafından değerlendirmeye çalışılmıştır. **Gereç ve Yöntemler:** 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 Pearson(p); Spearman(s) korelasyon kullanılarak korelasyon analiziyle incelenmiştir. **Bulgular:** 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. 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 erişime engelli sitelere çeşitli yöntemlerle girdiği belirlenmiştir. **Sonuç:** 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 fail veya mağdur konumuna getirebileceği ifade edilmektedir. 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; siber psikoloji; bilişim suçu farkındalığı

ABSTRACT Objective: In this research IT employees', judges', prosecutors' and lawyers' problematic internet utilization behaviors regarding cybersecurity were determined and evaluated by IT law and forensic sciences. **Material and Methods:** 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. Relationship between PİKÖ and KSGS scales are analyzed by correlation analysis using Pearson (p); Spearman(s) correlation. **Results:** 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. 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. **Conclusion:** The fact that individuals have to make fast decisions in cyberspace compared to daily life, they are pushed for misbehavior in digital interaction where behaviors often make individual the perpetrator or victim. The findings will shed light on problematic internet usage behaviors on cybersecurity and studies to be done in this field for groups operating in field of informatics and law.

Keywords: IT; cybercrime; lawyer; cyberpsychology; awareness of cybercrime

Correspondence: Elif YORGANCIOĞLU
İstanbul Üniversitesi-Cerrahpaşa Adli Tıp ve Adli Bilimler Enstitüsü, Sosyal Bilimler ABD, İstanbul, Türkiye
E-mail: elifyorgancioglu@gmail.com

Peer review under responsibility of Turkiye Klinikleri Journal of Forensic Medicine and Forensic Sciences.

Received: 20 Oct 2022 ***Received in revised form:*** 16 Feb 2023 ***Accepted:*** 27 Feb 2023 ***Available online:*** 02 Mar 2023

İnternete erişimini "temel bir insan hakkı" olarak tanıyan yeni dünyada, internete erişim arttıkça internet-bilişim sistemleri üzerinde işlenen suçlar da 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 hâle gelmemiş olmasına ve birçoğu birbirinin yerine kullanılmasına rağmen "siber suç" kavramı görece diğerlerine göre literatürde daha çok kullanılmaktadır.[1] Birçok araştırmacı, siber suç kavramının geniş anlamda kullanılmasının gerekliliğini vurgulamaktadır. Uluslararası Telekomünikasyon Birliği, hukuki bir terim olarak kullanılmadığı sürece "siber suçun" tek bir tanımının olmamasının önemsiz olduğuna vurgu yapmaktadır.[2] Gordon ve Ford, siber suçu; "Bir bilgisayar, ağ veya donanım aygıtı kullanılarak kolaylaştırılan veya işlenen herhangi bir suç" olarak tanımlamıştır.[3] Clough ise dijital teknolojilerin kullanımı yoluyla veya bunlara karşı işlenen her türlü yasaklanmış davranışı kapsayacak şekilde "siber suç" terimini kullanmayı tercih ettiğini ifade etmektedir.[1] Xingan'ın 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."[4] Literatürde en yaygın şekilde kullanılan terim "cybercrime" (siber suç) olup; makalemizde siber suç, bilişim suçu anlamında kullanılmaktadır.

1960'lı yıllarda çok sayıda kişi ve işletme aynı bilgisayarı kullandığından, üzerinde depolanan veriler, programlar korunmasızdı ve bilgisayar korsanlığının kapıları da ilk kez bu yıllarda aralanmaya başlanmıştır.[5] 1980'li yıllarda ise Federal Soruşturma Bürosu, bilgisayar korsanlarının ilk yüksek profilli tutuklamalarından bazılarını yapmıştır. 1990'lı yıllarda kişisel bilgisayarlar gittikçe artmış ve bu tarihten itibaren siber suçlar hızlı bir küreselleşme sürecine girmiştir.[6] 2000'li yılların başı ise siber suçların rutinleştiği ve yasal boşluğun birçok ülke yönünden doldurulmaya başlandığı yıllar olmuştur.[6] 2000'li yıllarla birlikte, endüstri 4,0 olarak kabul edilen, endüstri devriminin 4. aşaması bir dijital dönüşüm dalgasını başlatmıştır.[7] Bu dönüşüm, nesnelerin interneti kullanımını hızla artırmış, 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 (Internet of Things) kullanımı olan birçok cihazın sadece işlevselliğe dönük tasarımdan kaynaklanan güvenlik açıkları gibi].[8]

Bugüne gelindiğinde, siber suçların maliyetinin oldukça yüksek olduğu tespit edilmektedir. 2020 tarihinde yayımlanan bir siber güvenlik raporunda, siber suçların maliyetinin, kısmen koronavirüs hastalığı-2019 pandemisinin siber suçlular tarafından bir fırsat olarak kullanılması nedeniyle 2015 yılında 2,7 trilyon eurodan 2020'nin sonunda 5,5 trilyon euroya çıkacağının tahmin edildiği ifade edilmiştir.[8] Raporda bu rakamın, tarihteki en büyük ekonomik servet transferini temsil ettiği ve siber suçların neredeyse tüm büyük yasa dışı uyuşturucuların küresel ticaretinden daha fazla kâr getiren bir suç türü olduğu ifade edilmiştir.[8] 2021 yılı itibarıyla ise siber suçların küresel maliyeti 6,9 trilyon dolar olduğu ifade edilmektedir.[9] 2017-2022 yılları arasında, 5 yıl içerisinde siber suçların oluşturduğu toplam kaybın ise 18,7 milyon dolar olduğu ifade edilmektedir.[9] Trendmicro tarafından yayımlanan Siber Güvenlik Raporu'nda, 2022 yılının ilk yarısında engellenen toplam tehdit sayısı ise 63.789.373.773 olarak açıklanmıştır.[10] Bu rakam, riskin büyüklüğünü gözler önüne sermektedir.

2020 yılında yayımlanan aynı siber güvenlik raporunda, gün geçtikçe siber saldırganların daha karmaşık saldırı araçları kullandığı, özellikle kötü amaçlı yazılımların kullanımında sürekli bir artış olduğu ve son 5 yılda en sık kullanılan saldırı aracı hâline geldiği tespiti yer almıştır.[8] Suç trendlerine yönelik çalışmalarda da sokak suçlarında gözlemlenen düşüşte siber uzamda suç işleyenlerin kriminal aktivitelerini kendilerine ciddi avantaj sağlayan çevrim içi ortamlara yönelttiği, bu sayede de suç oranlarında azalma yaşandığı savunulmakla birlikte, siber suçların artışına ilişkin verilerin de bu iddiayı güçlendirdiği ifade olunmaktadır.[11]

İnternetin dünyadaki en geniş iletişim ağı olması ve internetin mülkiyetinin kimseye ait olamayacağı

gerçeği 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.[12] Özellikle Türkiye'de internet erişiminin engellenmesine konu olaylarda uygulanan tedbirlerin yerindeliği, şekli ve orantılılığı sıklıkla tartışılmış ve davaların konusu olmuştur.[13] Bu tartışmaların ışığında mevzuatta yapılan güncellemeler ve yeni oluşturulan Erişim Sağlayıcılar Birliği gibi otoriteler, sorunun çözümü için bir adım olarak değerlendirilmiştir. Suçluların tespiti amacı gerekçe gösterilerek, bazı kamu otoritelerince tüm internet kullanıcılarının kişisel verilerinin kullanılmasının kişisel verilerin korunması hakkına müdahale niteliğinde olduğu da son yıllarda kamuoyunda ve yargı önünde tartışılan bir hususdur.[14,15] Avrupa'da da suçun işlenmesinin önlenmesi ve suçlunun tespiti için diğer internet kullanıcılarının kişisel verilerinin kullanılıp kullanılamayacağı sıklıkla tartışılmış ve mahkeme kararlarına konu olmuştur.[16]

Lisanssız yazılım kullanımı da bir başka sorun olarak karşımıza çıkmaktadır. 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 Md. 22/3'te özel olarak düzenlenen, eser sahibinin "çoğaltma hakkı"nın ihlali niteliğinde olduğundan, FSEK md. 71 uyarınca suçtur. Sanal Ortamda İşlenen Suçlar Sözleşmesi (Budapeşte Konvansiyonu) uyarınca, lisansız yazılım kullanmak da telif haklarının ihlali kategorisinde bir siber suç çeşididir.

Bilişim teknolojilerinin sürekli gelişmesi karşısında suçların farklı araçlarla işlenmesi noktasında suçlunun tespiti, uygulayıcıların bilgi eksikliği ve yasaların güncel olmaması sebepleriyle 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 sorumluluğunun 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.[17] Siber suç oranındaki artış, gelecekte yasa uygulayıcılarıyla siber güvenlik uzmanlarının iş birliğini daha da zorunlu hâle getirecektir. Bilişim alanında çalışan, hizmet ve ürünleri üreten profesyonellerin ve adalet sistemi süjelerinin bilişim suçları karşısındaki tutumları ve farkındalıklarının ölçülmesi geliştirilecek politikalara ışık tutacaktır.

GEREÇ VE YÖNTEMLER

ÖRNEKLEM

Araştırma evreni, Türkiye'de görev yapan bilişim sektörü çalışanları, hâkim, savcı ve avukatlardan oluşmuştur. Çalışmanın örneklemi ise Türkiye'de yaşayan 230 bilişim sektörü çalışanı ve 270 hâkim/savcı/avukat olmak üzere toplam 500 profesyoneldir.

ARAÇLAR

Kişisel Bilgi Formu: Yapılan araştırmanın amacına dönük olarak literatürde kullanılan anket formları kriter alınarak, araştırmacılar tarafından hazırlanmıştır.[18,19] Katılımcıların demografik özellikleri, çalıştıkları kurumdaki unvanları, interneti kullanım tutumları ve internet üzerinde yaşadıkları mağduriyetler gibi bilgilere ilişkin soru formudur.

Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu: Bilişim suçu düzenlemelerine ilişkin katılımcıların bilişim suçu farkındalıklarını belirleme amacıyla araştırmacılar tarafından hazırlanan bir soru formudur.

Problemli İnternet Kullanımı Ölçeği: Üç faktörlü, 33 maddelik internetin sağlıklı ve sağlıksız olarak kullanım düzeylerini ortaya koymayı amaçlayan ölçektir.[20] 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 5 maddeden oluşmakta, "aşırı kul-

lanım" 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 Problemli İnternet Kullanımı Ölçeği (PİKÖ) için 0,96 bulunmuştur. Alt testlerin iç tutarlığına bakıldığında; aşırı kullanım 0,60, sosyal fayda/rahatlık 0,90, internetin olumsuz sonuçları 0,96 bulunmuştur.

Kişisel Siber Güvenliği Sağlama Ölçeği: İnternet kullanıcılarının siber güvenlik ile ilgili davranışlarını belirlemeye yönelik 5 faktörlü ve 25 maddeden oluşan bir ölçektir.[21] 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 "iz bırakmama" olarak ifade edilmiştir. İç tutarlık için bakılan Cronbach alfa değeri Kişisel Siber Güvenliği Sağlama Ölçeği (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, iz bırakmama 0,48 bulunuştur.

YÖNTEM

Katılımcılara Kasım 2019-Temmuz 2022 yılları arasında çevirimiçi platformlar üzerinden ulaşılmıştır. Çalışmaya katılımcıları dahil etme sürecinde e-posta yoluyla, LinkedIn (LinkedIn Corporation, Amerika Birleşik Devletleri) ve e-posta uygulamaları kullanılmış olup araştırmacı tarafından Google Documents (Alphabet Inc., Amerika Birleşik Devletleri) sitesinde hazırlanan online anket formu bu çalışmada kullanılmıştır. Veriler toplam 500 kişiden toplanmıştır. Bu çalışma Helsinki Deklerasyonunu ilkelerine uygun olarak yürütülmüştür.

İSTATİSTİKSEL ANALİZ

Bu çalışmada sürekli değişkenler için normallik varsayımı, değişkenlerin çarpıklık ve basıklık değerlerinin -1,5 ile +1,5 aralığında olduğu durumlarda kabul edilmiştir. Ayrıca histogram grafikleri de incelenmiştir.[22,23] Normal dağılan değişkenler için bağımsız t örneklem testi uygulanmış ve ortalama±standart sapma (SS) olarak gösterilmiştir. Normal dağılmayan değişkenler için Mann-Whitney U testi uygulanmış ve medyan (%25-75) olarak gösterilmiştir. Kategorik değişkenler için ise ki-kare testi uygulanmış, frekans ve yüzde şeklinde gösterilmiştir. Değişkenler arasındaki ilişkiyi test etmek için normal dağıldığında Pearson (p) korelasyon analizi, dağılmadığında Sperman (s) korelasyon analizi uygulanmıştır. Verilerin istatiksel analizi SPSS 25.0 (Armonk, NY: IBM Corp) programı ile yapılmıştır. İstatistiksel anlamlılık düzeyi (p) 0,05 olarak alınmıştır.

BULGULAR

Ölçeklerin birbirleri arasındaki ilişki incelendiğinde, KSGS kişisel gizliliği koruma ile PİKÖ ve tüm alt ölçekleri arasında negatif yönlü zayıf bir ilişki bulunmuştur (aşırı kullanım r=-0,27; sosyal fayda r=-0,27; internetin olumsuz sonuçları r=-0,34; PİKO total r=-0,34 p<0,001). KSGS ile PİKÖ aşırı kullanım, PİKÖ internetin olumsuz yanları ve PİKÖ arasında negatif yönlü zayıf bir ilişki bulunmuştur (aşırı kullanım r=-0,26; internetin olumsuz yanları r=-0,19; PİKO total r=-0,33; p<0,001). KSGS güvenilmeyenden kaçma ile PİKÖ internetin olumsuz yanları ve PİKÖ arasında ise negatif yönlü zayıf bir ilişki bulunmuştur (internetin olumsuz yanları r=-0,23; PİKO total r=-0,21; p<0,001). KSGS ödeme bilgilerini koruma ile PİKÖ internetin olumsuz yanları arasında ise negatif yönlü zayıf bir ilişki bulunmuştur (internetin olumsuz yanları r=-0,24; p<0,001).

Mesleklerle demografik değişkenler arasındaki ilişki Tablo 1'de incelenmiştir. Katılımcıların %54'ü avukat veya hâkim veya savcı olup (bundan sonra bu gruptan "hukukçu" olarak bahsedilecektir), %46'sı bilişim sektörü çalışanıdır. Katılımcılara, gerekli olduğunu düşündüklerinde hakkında erişim engelleme kararı olan sitelere girip girmeyecekleri sorulduğunda, hukukçuların %71'inin, bilişim sektörü çalışanlarının %71,3'ünün bu sitelere girdikleri yanıtını verdiği belirlenmiştir. Bilişim sektörü çalışanlarının %65,9'unun lisanssız yazılım kullanırken, hukukçuların %57,4'ünün lisanssız yazılım kullandığı belirlenmiştir (Tablo 1).

Ölçeklere göre meslekler arasında farklılık olup olmadığı Tablo 2'de incelenmiştir. Araştırma konusu

TABLO 1: Mesleklerle demografik değişkenler arasındaki ilişki.

	Hukukçu	Bilişim sektörü çalışanı	İstatistik
Yaş ortalaması	32,66	33,5	
Erkek	102 (37,8)	191 (83)	χ^2=104,90 p<0,001
Kadın	168 (62,2)	39 (17)	χ^2=104,90 p<0,001
Bekâr	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)	χ^2=42,63 p<0,001
İnternette geçirilen süre Günde 2-4 saat	131 (48,5)	65 (28,3)	χ^2=42,63 p<0,001
İnternette geçirilen süre Günde 4 saatten fazla	99 (36,7)	151 (65,7)	χ^2=42,63 p<0,001
Lisanssız yazılım kullanma Evet	178 (65,9)	132 (57,4)	χ^2=3,84 p=0,051
Lisanssız yazılım kullanma Hayır	92 (34,1)	98 (42,6)	χ^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 izlenmesi Evet	137 (50,7)	141 (61,3)	
Erişim engelli sitelerin izlenmesi Fikrim yok	100 (37)	50 (21,7)	
Erişim engelli sitelerin izlenmesi Hayır	33 (12,2)	39 (17)	

meslek gruplarının PİKÖ aşırı kullanım ortalamaları, KSGS önlem alma ortalamaları, KSGS ödeme bilgilerini koruma sıra ortalamaları, KSGS iz bırakmama ortalamaları, KSGS total ortalamaları ve Bilişim Suçu Düzenlemelerinin Hukuki Farkındalığına Yönelik Soru Formu (BSF) sıra ortalamaları karşılaştırıldığında, gruplar arasında anlamlı farklılık olduğu tespit edilmiştir (Tablo 2). Hukukçuların aşırı kullanım ortalamaları bilişim sektörü çalışanlarından daha fazladır. Bilişim sektörü çalışanlarının önlem alma ortalamaları hukukçulardan daha fazladır.

BİLİŞİM SEKTÖRÜ ÇALIŞANLARI VE HUKUKÇULAR İÇİN ANALİZLER

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 3, Tablo 4 ve Tablo 5'te verilmiştir.

Bilişim sektörü çalışanları grubunda, KSGS önlem alma, KSGS total ortalamalarına göre; PİKÖ sosyal fayda, KSGS ödeme bilgilerini koruma sıra or-

TABLO 2: Mesleklerle ölçekler arası ilişki.

Değişkenler	Hukukçu	Bilişim sektörü çalışanı	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	10 (8-10)	10(8-10)	U=27045 Z=-2,79 p=0,01**
KSGS iz 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	33 (32-35)	33 (30-35)	U= 26377,5 Z=-2,97 p=0,003**

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

talamalarına göre cinsiyetler arasında anlamlı farklılık bulunmuştur (p<0,05). Buna göre erkeklerin bu 4 faktör yönünden puanlarının, kadınlardan daha fazla olduğu gözlemlenmiştir. Hukukçu grubunda cinsiyetler arasında ölçek ortalamalarına/sıra ortalamalarına göre anlamlı farklılık bulunamamıştır (p>0,05).

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 3). Hukukçu grubunda KSGS önlem alma ve KSGS ortalamaları antivirüs programı kullanan bireylerde fazladır (Tablo 3).

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, internetin olumsuz sonuçları ve PİKÖ total puanları günde 4 saatten daha az vakit geçiren bireylerden daha yüksektir (Tablo 4). Hukukçu grubunda internette günde 4 saatten fazla zaman geçiren bireylerin PİKÖ aşırı kullanım, sosyal fayda, internetin olumsuz sonuçları ve PİKÖ total puanları günde 4 saatten daha az vakit geçiren bireylerden daha yüksektir (Tablo 4).

Hukukçularda ve bilişim sektörü çalışanlarında lisanssız yazılım kullanım durumlarının ölçeklere göre karşılaştırılması incelenmiştir. Bilişim sektörü

TABLO 3: Bilişim sektörü çalışanları ve hukukçular arasında antivirüs programı kullanımı durumunun karşılaştırılması.

	Bilişim sektörü çalışanlarında antivirüs programı kullanımı			Hukukçularda antivirüs kullanımı		
	Antivirüs programı kullanımı		İstatistik	Antivirüs programı kullanımı		İstatistik
	Evet	Hayır		Evet	Hayır	
KSGS önlem alma	22 (19-25)	19 (16-21)	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; **Mann-Whitney U testi; KSGS: Kişisel Siber Güvenliği Sağlama Ölçeği.

TABLO 4: Hukukçularda ve bilişim sektörü çalışanlarında internette geçirilen süreler arasında ölçeklere göre karşılaştırma.

	Hukukçularda internette geçirilen süreler arasında ölçeklere göre karşılaştırma			Bilişim sektörü çalışanlarında internette geçirilen süreler arasında ölçeklere göre karşılaştırma		
	İnternette geçirilen süre		İstatistik	İnternette geçirilen süre		İstatistik
	Günde 4 saat ve daha az	4 saatten fazla		Günde 4 saat ve daha az	4 saatten fazla	
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	13 (10-18)	16 (11-21)	U=6572 Z=-3,07 p=0,002**	13 (10-18)	17 (11-24)	U=4446 Z=-3,18 p=0,001**
PİKÖ internetin olumsuz sonuçları	23 (18-30)	25 (20-41)	U=6984 Z=-2,40 p=0,02**	21 (18-26)	25 (19-37)	U=4665 Z=-2,72 p=0,01**
PİKÖ total	48 (40-61)	52 (43-78)	U=6984 Z=-3,08 p=0,002**	45 (38-55)	55 (42-74)	U=4287,5 Z=-3,50 p<0,001**

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

çalışanlarında PİKÖ internetin olumsuz sonuçları ve PİKÖ total puanları lisanssız yazılım kullananlarda fazla iken, tersine KSGS total puanları kullanmayanlarda daha fazladır (Tablo 5). Hukukçularda PİKÖ aşırı kullanım, sosyal fayda, internetin olumsuz sonuçları ve PİKÖ puanları lisanssız 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 (Tablo 5).

TARTIŞMA

Araştırmada, hem hukukçuların hem de bilişim sektörü çalışanlarının yüksek oranda lisanssız yazılım kullandığı tespit edilmiştir. The Software Alliance'ın (BSA) 2018 yılındaki araştırmasına göre kişisel bilgisayarlarda kullanılan yazılımların %37'sinin lisanssız olduğu tespit edilmiştir.[24] Uluslararası hukukta olduğu gibi telif haklarına ilişkin ihlallerin suç sayılması Türk Hukuku'nda da söz konusudur. Bu kapsamda FSEK'de lisanssız yazılım kullanmak, eser sahibinin çoğaltma hakkının ihlali niteliğinde sayıldığından suç olarak düzenlenmektedir. Lisanssız yazılım kullanmanın suç olmasının yanı sıra lisanssız yazılım kullanmanın siber suç mağduru olma riskini artırdığını söylemek mümkündür.[24] BSA'nın 2018 yılındaki araştırmasında, lisanssız yazılım kullanma nedeniyle kötü amaçlı yazılım bulaşma oranın %29 olduğu tespit edilmiştir.[24] Araştırmamızda da bu durumu destekler şekilde, her iki grup katılımcıların da internetin olumsuz sonuçları puanlarının lisanssız yazılım kullananlarda daha fazla olduğu ortaya çıkmıştır.

Araştırmaya katılan hukukçuların ve bilişim sektörü çalışanlarının lisanssız yazılım kullanımını suç olduğunu düşünmesine rağmen lisanssız yazılım kullanma eğilimleri olduğu belirlenmiştir (Tablo 1). Buna rağmen yapılan araştırmalarda alışkanlık, sosyal çevre desteği, satın alma gücü gibi nedenler lisanssız yazılım kullanmanın ardındaki nedenler olarak görülmektedir.[25] Bununla birlikte, katılımcıların %71,2'sinin erişime engelli sitelere çeşitli yöntemlerle (VPN, DNS değişikliği vs. ile) girdiği belirlenmiştir (Tablo 1). Lisanssız yazılım kullanmadaki yüksek oranın ihlal niteliğinde olan bu tutumda da görüldüğü belirlenmiştir. Çevrim içi 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 et-

TABLO 5: 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	Hayır		Evet	Hayır	
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	15 (10-21)	13 (11-16)	U=6567 Z=-2,68 p=0,01**	17 (11-23)	13 (10-19,25)	U=5592 Z=-1,76 p=0,08**
PİKÖ internetin olumsuz sonuçları	25 (20-37)	21 (17,25-26)	U=5559,5 Z=-4,33 p<0,001**	24,5 (19-36,75)	21 (17-29,25)	U=5185,5 Z=-2,58 p=0,01**
PİKÖ total	53 (43-71)	45 (39-53,75)	U=5596 Z=-4,26 p<0,001**	53,5 (41,25-74)	46 (38-62)	U=5299 Z=-2,34 p=0,02**
KSGS kişisel gizliliği koruma	25,5 (22-29)	28 (24-30,75)	U=6460,5 Z=-2,85 p=0,004**	27 (22-30)	28 (25-31)	U=5246 Z=-2,46 p=0,01**
KSGS güvenilmeyenden kaçma	18 (16-20)	19 (17-20)	U=6605 Z=-2,69 p=0,01**	18 (16-20)	19 (16-20)	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*	21 (18-24)	21 (19-25)	U=6090 Z=-0,76 p=0,45**
KSGS ödeme bilgilerini koruma	9 (8-10)	10 (8-10)	U=6584,5 Z=-2,87 p=0,004**	10 (8-10)	10 (8-10)	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	33 (31-35)	34 (32-35)	U=6686 Z=-2,55 p=0,01**	32 (30-34,75)	33 (30,75-35)	U=5705,5 Z=-1,55 p=0,12**

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

kileşimde hatalı davranışlara kolaylıkla itebileceği, hatta bu hatalı davranışların bireyi çoğu zaman suçun faili ve mağduru konumuna getirebileceği ifade edilmektedir.[26] Bu bağlamda, lisanssız yazılım kullanma ve erişim engelli sitelere girme davranışlarının bulgusunun bu tezle ilişkili olduğu düşünülmektedir.

Araştırmada, her iki katılımcı grup yönünden de önlem alma ve kişisel siber güvenliği sağlama total ortalamalarının antivirüs programı kullanan bireylerde fazla olduğu belirlenmiştir (Tablo 3). 2019 yılında yapılan çalışmada, katılımcıların %65,7'si antivirüs programı kullanmadığını bildirmiştir.[27] Aynı araştırmada, antivirüs programı kullanmayanların siber suç mağduru olma ihtimallerinin daha fazla olacağı ifade edilmiştir.[27] Hedefin suça karşı korunmasız olması, mağdur olma riskini artırmaktadır. Beklenen bir sonuç olarak araştırmada, antivirüs programı kullanan katılımcıların siber güvenliğe önem verdikleri ve önlem aldıkları bu veriyle ortaya konmuştur.

Ocak 2022 tarihinde açıklanan "We Are Social" Raporu'nda Türkiye'de günlük toplam internet kullanım ortalaması 8 saat iken, dünyada günlük internet kullanım ortalaması 6 saat 58 dakika olarak tespit edilmiştir.[28,29] Çalışmamızda, katılımcılara internette geçirdikleri "günlük toplam süre" sorulmuş olup, bu süre içerisine iş ve akademik amaçlı kullanım da dâhildir. Katılımcılardan, internette günde 4 saatten

fazla zaman geçiren bireylerin PİKÖ aşırı kullanım, sosyal fayda, internetin olumsuz sonuç puanları daha az vakit geçiren bireylerden daha yüksektir (Tablo 4). Bu bulguyla örtüşür şekilde, internet ve akıllı telefon bağımlılıklarının siber dolandırıcılık mağduriyeti ile ilişkili olduğu, problemli sosyal medya kullanımlarının siber suç mağduru olma riskini artırdığı yönünde araştırmalar mevcuttur.[30,31] Öztürk'e göre dijital iletişimlerin problemli biçimde kullanımları siber mağduriyetlere neden olabilmekte, siber mağduriyet bir siber travma olarak siber dissosiyasyona da yol açabilmektedir.[32] Erdoğan ve Öztürk'e göre siber mağduriyet, internet bağımlılığı, çocukluk çağı travmaları ve dissosiyasyon ile yakından ilişkilidir.[32]

Bu alana ilişkin profesyoneller olan bilişim sektörü çalışanları ve hukukçulardan oluşan katılımcıların %25'4'ünün siber mağduriyetle karşılaşmış olması tartışmaya değerdir. Siber dolandırıcılık mağduru olan İngiliz avukatların kayıplarının, 2016 yılında 2,53 milyon sterline ulaştığı ifade edilmektedir.[33] Özellikle hukuk büroları, hassas birçok veriye sahip olmaları bakımından siber saldırganlar için zengin bir hedef olarak değerlendirilmektedir.[34] Başka sektörlerdeki şirketlere kıyasen kendilerini koruyacak yetenek ve kaynaklara sahip olmamaları da onların uygun hedef olarak değerlendirilmesine yol açmaktadır.[34] 2019 yılında yapılan araştırmada, kişilerin eğitim düzeyleri arttıkça siber suç mağduru olma ihtimalinin de arttığı ortaya konmuştur.[27] Başkaca araştırmalarda da siber riski bilen kişilerin yine de yüksek siber mağduriyet oranlarına sahip olduğu ortaya konmuştur.[31] Yine 2020 yılında yapılan bir araştırmada, tüketici davranışının siber güvenliğe yardımcı olmadığı, insanların tehlikeleri anlasalar bile bilerek çevrim içi risk aldığı sonucuna ulaşılmıştır.[35] Birçok araştırma, siber dolandırıcılık mağdurlarının çevrim içi 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.[36] 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.[37] Dolandırılma ile ilgili olarak karar verme sürecinde hatalara neden olan motivasyonel ve bilişsel faktörlerden biri olan "aşırı öz güven" de bu sonucu açıklamaya yarayan bir unsur olarak değerlendirilebilir.[32]

SONUÇ

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.[26] 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;[26] katılımcıların lisanssız yazılım kullanım oranlarındaki yükseklik ve erişime engelli sitelere girme davranışları gibi siber kriminal aktivitelerinin nedenini ortaya koymaktadır. Siber uzamda gerçekleşen kriminal aktivitelerin önlenmesi, hukukçuların ve bilişim sektörü profesyonellerinin mutlak iş birliğini gerekli kılmaktadır. Gelecekte bu çalışmanın katılımcı grupların bileşenleri olan alt meslek grupları için ayrı ayrı (özellikle hâkim ve savcılar için), daha geniş sayıda katılımcıya ulaşılarak yapılması ve araştırma sonuçlarının rutin aktiviteler teorisi çerçevesinde tartışılması önerilmektedir.

Finansal Kaynak

Bu çalışma sırasında, yapılan araştırma konusu ile ilgili doğrudan bağlantısı bulunan herhangi bir ilaç firmasından, tıbbi alet, gereç ve malzeme sağlayan ve/veya üreten bir firma veya herhangi bir ticari firmadan, çalışmanın değerlendirme sürecinde, çalışma ile ilgili verilecek kararı olumsuz etkileyebilecek maddi ve/veya manevi herhangi bir destek alınmamıştır.

Çıkar Çatışması

Bu çalışma ile ilgili olarak yazarların ve/veya aile bireylerinin çıkar çatışması potansiyeli olabilecek bilimsel ve tıbbi komite

üyeliği veya üyeleri ile ilişkisi, danışmanlık, bilirkişilik, herhangi bir firmada çalışma durumu, hissedarlık ve benzer durumları yoktur.

Yazar Katkıları

Fikir/Kavram: *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Tasarım:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Denetleme/Danışmanlık:*** *Yusuf Tunç Demircan;* ***Veri Toplama ve/veya İşleme:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Analiz ve/veya Yorum:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Kaynak Taraması:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Makalenin Yazımı:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Eleştirel İnceleme:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;* ***Kaynaklar ve Fon Sağlama:*** *Yusuf Tunç Demircan, Elif Yorgancıoğlu;*

KAYNAKLAR

1. Clough J. Principle of Cybercrime. 2nd ed. Cambridge: Cambridge University Press; 2015.
2. International Telecommunication Union [Internet]. [Cited: October 18, 2022]. Understanding Cybercrime: A Guide for Developing Countries. Available from: [Link]
3. Gordon S, Ford R. On the definition and classification of cybercrime. Journal in Computer Virology. 2006;2(1):13-20. [Crossref]
4. Xingan L. Defining cybercrime based on roles of data processing systems. In: Gifford M, Potts M, eds. Pandora's Box 2016: Law and Technology. St. Lucia: Worldwide Printing Fortitude Valley; 2016. p.127-44.
5. Shinder DL, Tittel E. Scene of the Cybercrime: Computer Forensics Handbook. 1st ed. Rockland: Syngress Publishing Inc; 2002.
6. Johannes Xingan L. Cyber crime and legal countermeasures: a historical analysis. International Journal of Criminal Justice Sciences. 2017;12(2):196-207. [Crossref]
7. Yankın FB. Dijital dönüşüm sürecinde çalışma yaşamı [Work life in digital transformation process]. Trakya Üniversitesi İktisadi ve İdari Bilimler Fakültesi E-Dergi. 2018;7(2):1-38. [Link]
8. European Commission [Internet]. [Cited: November 02, 2022]. Cybersecurity Our Digital Anchor Europen Perspective Report. Available from: [Link]
9. FBI Internet Crime Complaint Centre. FBI Internet Crime Report 2021. [Cited: December 02, 2022]. Available from: [Link]
10. Defending the Expanding Attack Surface [Internet]. Trend Micro Incorporated © 2022 [Cited: October 18, 2022]. Cybersecurity Report. Available from: [Link]
11. Çalıcı C. Türkiye'de Suç Trendleri Tarihsel Kriminolojik Değerlendirme. 1. Baskı. İstanbul: Legal Kitabevi; 2019.
12. Akdeniz Y, Altıparmak K. İnternet: Girilmesi Tehlikeli ve Yasaktır Türkiye'de İnternet İçerik Düzenlemesi ve Sansüre İlişkin Eleştirel Bir Değerlendirme. 1. Baskı. Ankara: İmaj Yayınevi; 2008.
13. T. C. Anayasa Mahkemesi [İnternet]. Youtube LLC Corporation Service Company ve Diğerleri Başvurusu (2014/4705). [Erişim tarihi: 02.10.2022]. Erişim linki: [Link]
14. TBMM Tutanakları. Türkiye Büyük Millet Meclisi [Erişim tarihi: 18.10.2022]. Erişim linki: [Link]
15. Candoğan G. Kişisel Verilerin Korunması. 18.10.2022. Erişim linki: [Link]
16. ECHR [İnternet]. Case of Big Brother Watch and Others v. United Kingdom Application no. 58170/13-62322/14-24960/15. [Erişim tarihi: 02.10.2022]. Erişim linki: [Link]
17. Çobansoy Hızel G. Dijitalleşme Çağında Hukuk. Eskişehir Ticaret Odası. [Erişim tarihi: 02.10.2022]. Erişim linki: [Link]
18. Budak SÖ. Bilişim öğrencilerinin siber suç farkındalığı: Erzurum ili mesleki ve teknik liseler örneği. [Yüksek lisans tezi]. Erzurum: Atatürk Üniversitesi; 2015. [Erişim tarihi: 10.10.2021]. Erişim linki: [Link]
19. Hille P, Walsh G, Cleveland M. Consumer fear of online ıdentity theft scale development and validation. Journal of Interactive Marketing. 2015;30:1-19. [Crossref]
20. Ceyhan E, Ceyhan AA, Gürcan A. Problemli İnternet Kullanımı Ölçeği'nin geçerlik ve güvenirlik çalışmaları [The validity and reliability of the Problematic Internet Usage Scale]. Kuram ve Uygulamada Eğitim Bilimleri. 2007;7(1):387-416. [Link]
21. Erol O, Şahin YL Yılmaz E, Haseski İH. Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması [Personal Cyber Security Provision Scale development]. J Human Sciences. 2015;12(2):75-91. [Crossref]
22. Tabachnick BG, Fidell LS. Using Multivariate Statistics. 6th ed. Boston: Pearson; 2013.
23. Field A. Discovering statistics using IBM SPSS statistics. 4th ed. London: Sage; 2013.
24. The Software Alliance BSA [Internet]. © 2022 BSA. [Cited: October 01, 2022]. Global Software Survey: Software Management Security Imperative Business Opportunity. Available from: [Link]
25. Taşçıoğlu M. Dijital korsanlığa karşı lisans öğrencilerinin olumsuz tutumlarını etkileyen faktörler [Factors affecting negative attitudes of undergraduate students against digital piracy]. Marmara Üniversitesi Öneri Dergisi. 2019;14(52):340-5. [Crossref]
26. Öztürk E. Siber toplumlar ve siber hayatlar: dissosiyojen bir ajan olarak dijital iletişim ağları. Siber Psikoloji. 1. Baskı. Ankara: Türkiye Klinikleri; 2020. p.1-13.
27. Birceviz F. Rutin aktiviteler teorisi bağlamında siber suç mağduriyeti. [Yüksek lisans tezi]. Ankara: T.C. Milli Savunma Üniversitesi; 2019. [Erişim tarihi: 10.12.2021]. Erişim linki: [Link]
28. Recro Digital Marketing [İnternet]. Recro Digital Marketing © 2022 [Erişim tarihi: 22.10.2022]. We are social 2022 Türkiye Sosyal Medya Kullanım Verileri. Erişim linki: [Link]
29. Recro Digital Marketing [İnternet]. Recro Digital Marketing © 2022 [Erişim tarihi: 22.10.2022]. Dünyada ve Türkiye'de Sosyal Medya Kullanımı 2022. Erişim linki: [Link]
30. Herrero J, Torres A, Vivas P, Urueña A. Smartphone addiction, social support, and cybercrime victimization: a discrete survival and growth mixture model. Psychosocial Intervention. 2022;31(1):59-66. [Crossref]
31. Marttila E, Koivula A, Räsänen P. Cybercrime victimization and problematic social media use: findings from a nationally representative panel study. Am J Crim Justice. 2021;46(6):862-81. [Crossref] [PubMed] [PMC]

32. Öztürk E, Derin G. Klinik siber psikolojiden adli siber psikolojiye: Siber travma ve siber re-viktimizasyon. Siber Psikoloji. 1. Baskı. Ankara: Türkiye Klinikleri; 2020. p.14-24.

33. Gibb F. Lawyers are losing more money to cyber fraudsters. The Times. 12 September 2016. [Link]

34. Conte A. Unprepared law firms vulnerable to hackers. Pittsburgh Tribune Review (PA). 14 September 2014. [Link]

35. Interpol [Internet]. BT's Report-CISOs under the spotlight © 2022 [Cited: September 01, 2022]. Cybercrime threat response. Available from: [Link]

36. Drew J, Farrell L. Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs. Police Practice and Research. 2018;19(6):537-49. [Crossref]

37. NASD Investor Education Foundation. Investor fraud study: Final report. [Cited: September 10, 2022]. Available from: [Link]