

İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları*

Malik Aslanyürek

İstanbul Gelişim Üniversitesi
Güzel Sanatlar Fakültesi
malikaslanyurek@gmail.com

Özet

Aktif internet kullanıcı sayısının 2,5 milyara ulaştığı günümüzde internet ve siber ortamda devletin gözetim teknolojilerini kullanması; internet servis sağlayıcılarının ve şirketlerin pazarlama faaliyetleri amacıyla çevrimiçi ortamda bulunan kişisel verilerimizi toplaması; tam olarak neye ve kime hizmet ettikleri bilinmeyen bilgisayar korsanlarının ise kötü amaçlı faaliyetleri internet güvenliği ile çevrimiçi gizlilik alanında birçok ihlale sebep olmaktadır. Çalışmada ülkemizdeki internet kullanıcılarının internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlaller karşısında kanaatlerini ve farkındalıklarını değerlendirmek amacıyla 479 katılımcılı bir anket araştırması gerçekleştirilmiştir. Araştırma bulguları, çevrimiçi gizlilik ve güvenlik ihlalleri karşısında internet kullanıcılarının farkındalık boyutunun yüksek olduğunu; fakat bu ihlaller karşısında internet kullanımından vazgeçme eğilimlerinin düşük olduğunu göstermektedir.

Anahtar Sözcükler: Gözetim, çevrimiçi gizlilik, internet güvenliği, çevrimiçi davranışsal reklamcılık, bilgisayar korsanlığı.

•••••

Makale geliş tarihi: 11.02.2016 • Makale kabul tarihi: 23.03.2016

Maltepe Üniversitesi İletişim Fakültesi Dergisi • © 2016 • 3(1) • bahar/spring: 80-106

* Bu çalışma, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Radyo Televizyon ve Sinema Anabilim Dalı'nda Doç. Dr. Mehmet Sezai TÜRK danışmanlığında yapılmış olan “İnternet Güvenliği ve Çevrimiçi Gizlilik Alanlarında Yaşanan Sorular: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Araştırma” adlı yüksek lisans tezine dayanmaktadır.

Internet and Social Network Users' Opinions and Awareness Regarding Internet Security and Online Privacy

Malik Aslanyürek

İstanbul Gelişim Üniversitesi
Güzel Sanatlar Fakültesi
malikaslanyurek@gmail.com

Abstract

Nowadays, that is very high rate of the internet usage, a lot of infringements are being conducted to in the field of internet security and online privacy because government uses surveillance technology in the internet and cyberspace, internet service providers and companies collect our personal data for the purpose of marketing activities in the online environment, and by reason of malicious activities of the hackers exactly what and whom they serve are unknowable. In this study a survey was conducted on 479 people to assess their convictions and awareness on the face of internet security of users and infringements related to online privacy. Research findings shows that internet users have a high awareness on the face of online privacy and internet security, but they have lower tendency to give up using internet on the face of these infringements.

Keywords: Surveillance, online privacy, internet security, online behavioral advertising, hacking.

•••••

Article arrival date: 09.03.2016 • Article acceptance date: 04.04.2016
Maltepe University Communication Faculty Journal • © 2016 • 3(1) • bahar/spring: 80-106

Gelişen bilgisayar, internet ve akıllı telefon teknolojilerine paralel olarak internet kullanım oranları günden güne artarken; devlet, pazarlama şirketleri ve bilgisayar korsanlarının internet üzerinde gerçekleştirdiği mahremiyet ihlalleri internetin ne kadar güvenli bir ortam olduğu gerçeğini sorgulamamıza sebep olmuştur.

Mevcut araştırmalar incelendiğinde internet güvenliği ve çevrimiçi gizlilik alanlarında yaşanan sorunlara ilişkin olarak yalnızca devlet tarafından gerçekleştirilen gözetim faaliyetleri üzerinde durulduğu diğer unsurların göz ardı edildiği ortaya çıkmaktadır (Tokgöz, 2011; Karakaya, 2014; Karşlıoğlu, 2014). Bu bağlamda yapılan çalışmada gözetim olgusu daha geniş açıdan ele alınarak devlet, reklam şirketleri ve bilgisayar korsanlarının çevrimiçi ortamda gerçekleştirdikleri gözetim faaliyetlerinin sebep olduğu güvenlik ve gizlilik ihlalleri ile ilgili son kullanıcıların farkındalıkları ve kanaatleri üzerindeki etkiler incelenmiştir.

Türkiye'deki internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili olarak; örneklem dâhilinde seçilen Türkiye'deki en popüler beş sosyal medya sitesinde aktif internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili kanaatlerini ve farkındalıklarını ortaya koymak amaçlanmıştır. Buna göre altı adet araştırma sorusu belirlenmiştir. Bu araştırma sorularından beş tanesi kabul edilmiş, bir tanesi ise reddedilmiştir. Bu bağlamda çevrimiçi gizlilik ve güvenlik ihlalleri karşısında internet kullanıcılarının farkındalık boyutunun yüksek olduğu; fakat bu ihlaller

karşısında internet kullanımından vazgeçme eğilimlerinin düşük olduğu ortaya çıkmıştır.

Çevrimiçi ortamda güvenlik ve gizlilik

Güvenlik kavramı

Güvenliğin dünya üzerinde uzlaşmaya varılmış genel bir tanımı yoktur. Güvenliğin çok geniş bir kapsamı olması ve kavramsal olarak farklı perspektiflerden yaklaşılmasından dolayı güvenlik kelimesi bireysel, toplumsal, fiziksel ve sosyal açıdan farklı şekillerde tanımlanabilmektedir. Örneğin: kişi güvenliği, ulusal güvenlik, sosyal güvenlik, bilgi güvenliği, siber güvenlik vb. Türk Dil Kurumu güncel sözlüğüne göre güvenlik sözcüğünün anlamı şu şekildedir: “toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet” (TDK, 2014).

18 ve 19. Yüzyıllardan itibaren güvenlik kavramı üzerinde daha fazla durulmaya başlanmıştır. 1776 yılında yapılan ilk Amerikan anayasasında güvenlik özgürlükle ilişkilendirilmiştir. Fransız ihtilali döneminde yurttaş hakları bildirgesi güvenliği dört temel insan hakkından biri olarak ilan etmiştir (Brauch, 2008).

Bir toplumsal değer olarak güvenlik: tehlike, risk, düzensizlik ve korkunun karşıtı olarak, koruma, risk yokluğu, kesinlik, güvenilirlik, itimat ve güven ile öngörülebilirliğe ilişkin kullanılmaktadır. Bir sosyal bilim terimi olarak “güvenlik anlamca muğlâk ve esnektir”. Arnold Wolfers güvenlik kavramının iki yüzünü işaret etmiştir: “güvenlik, nesnel olarak, kazanılmış değerlere yöneltilen tehditleri ölçmektedir, öznel olarak, bu değerlere saldırılacağı yönünde korkuların olmamasıdır. Art’a göre güvenliğin öznel yönü “tehditler, kaygılar ve tehlikeden uzak olma hissi” anlamına gelmektedir: “güvenlik, böylece, bir bireyin diğerlerinin verebileceği zarardan uzak olduğunu hissettiği bir ruh halidir” (Wolfers ve Art’dan aktaran Brauch, 2008).

Güvenlik ihtiyacına gerek insanın yaşamına devamı için mutlaka giderilmesi gereken fizyolojik ihtiyaçlardan sonra ikinci planda yer vermesi; gerekse insanın psikososyal dünyası açısından daha üst düzey ihtiyaçlarını hissedebilmeleri için karşılanması gereken bir olgu niteliğini getirmesi bakımından, Maslow’un ihtiyaçlar piramidi, şüphesiz güvenlik ihtiyacının insan toplulukları için taşıdığı önemi vurgulayan en gerçekçi bilimsel tespitlerden birisidir (Yalçın, 2009).

Güvenlik kelimesinin ilişkilendirilebileceği kavramlar artmıştır ve gelişen küreselleşme ile birlikte güvenlik sektörleşmiştir. Bunun yanında yeni güvenlik tehlikeleri meydana gelmiş, risk ve hassasiyet alanları oluşmuştur. Bundan dolayıdır ki güvenlik kavramı artık çok farklı alanlarla anılmaya başlanmıştır. Son yıllarda yaşanan teknolojik gelişmelerin beraberinde getirdiği yenilikler geniş bant internet kullanımının yaygınlaşmasını sağlamıştır. Özellikle günümüzde akıllı telefon ve bilgisayar kullanımının inanılmaz rakamlara ulaşmasıyla birlikte artık güvenlik adına farklı kavramlar gelişmiştir. İnternet güvenliği ya da diğer adlarıyla siber güvenlik ve çevrimiçi güvenlik son yıllarda oldukça üzerinde durulması gereken bir konu haline gelmiştir.

Gizlilik (Mahremiyet)

İnsanoğlunun var olduğu ilk günden beri ortaya çıktığına inanılsa da tıpkı güvenlik kavramında olduğu gibi mahremiyet kavramının da üzerinde uzlaşmış evrensel bir tanım mevcut değildir. Bunun sebebi mahremiyet algısının zamansal, kültürel ve toplumsal açıdan değişkenlik göstermesidir. Yine de mahremiyetin “gizli olması ve gizli kalması gereken şey” anlamına geldiğini söyleyebiliriz. Bu ifade aslında mahremiyetin en yalın tanımını oluşturmaktadır.

Alan Westin’e göre “mahremiyet, bireylerin, grupların ya da kurumların sahip oldukları bilginin ne zaman, nasıl ve ne ölçüde diğerlerine aktarılabilceğini kendilerinin belirleme hakkıdır” (Tanılır, 2002: 42). “Mahremiyet bir özerliktir ve yalnız bırakılma hakkını kapsar. Mahremiyet bizimle ilgili bilgiyi kontrol hakkını içerir. Mahremiyet hakkı, sırlarımızı gizleme hakkını ve onları yalnızca özel konuşmalarda paylaşmayı kapsar” (Flaherty, 1992).

Robert Gifford’a göre ise, mahremiyet ya da özel yaşam alanının en iyi tanımlarından birisi, Irwin Altman tarafından yapılmıştır. Altman için mahremiyet (privacy), bir kimsenin kendisine veya grubuna ulaşma çabası üzerindeki seçici kontrolüdür. Mahremiyetin ayırıcı niteliğini ortaya koyan bu tanım, kişinin kendisi hakkındaki bilgiyi ve sosyal etkileşimi üzerindeki hâkimiyetine ilişkin ikiz temayı kapsamaktadır. Üstelik söz konusu tanım mahremiyetin diğer tanımlarını da dışlamamaktadır. Kişilerin hem yalnız başına hem de başkalarıyla birlikte bulunma isteğini dikkate almaktadır. Genel olarak bahsedildiği üzere tek tek bireyler yalnızca

mahremiyet peşinde koşmazlar; aynı zamanda diğerleriyle ilişkiler kurmaya çalışır ve sosyal etkileşim sürecinde isteyerek kendileri hakkındaki bilgileri başkalarıyla paylaşabilirler... Bu niteliğiyle mahremiyet, yalnız başına kalma ile başkalarıyla birlikte bulunma arzuları arasındaki diyalektik bir karşılıklı oyun alanı olarak da tanımlanabilir (Gifford ve Altman'dan aktaran Yüksel, 2003).

Mahremiyet kavramının iyece anlaşılması için, mahremiyet türlerinin açıklanması gerekir. Mahremiyet kavramının türlerini fiziksel, psikolojik ve bilişsel olarak üçe ayırmak mümkündür. Fiziksel mahremiyet ile bireylerin fiziki yaşam koşulları ile alakalı tüm bedeni ve çevresel faktörleri içerisinde barındırdığı alanın mahremiyetini, psikolojik mahremiyet ile bireylerin psikolojik ve ruhsal tüm mahremiyetleri ele alınır. Bilişsel mahremiyet ile son yıllarda devletlerin kişisel sağlık ve şahsi verilerin sağlandığı elektronik ve internet gibi sanal ortamlarda bulunan verilerin mahremiyeti olarak ele alınır (Aksoy, 2013: 22).

Çevrimiçi Gizlilik

Çevrimiçi gizlilik kavramı; internet üzerinde istemli ya da istemsiz bir şekilde paylaşılan kişisel bilgilerin mahremiyeti ve güvenlik seviyesi ile alakalı bir kavramdır. Örneğin bir e-ticaret sitesinden alışveriş yaptığımızda girdiğimiz kredi kartı bilgileri veya herhangi bir internet sitesine ya da sosyal ağa üye olurken girdiğimiz kişisel verilerin güvenliği; bu verilerin kötü amaçlar için üçüncü şahısların eline geçmesi ya da çalınması vb. kaygıları tanımlayan bir kavramdır. Çevrimiçi Gizlilik konusu, internet üzerinde yapılacak birçok aktivite ve atılacak birçok adımda kaygılara sebep olmaktadır. İnternette bir faaliyet içinde yer almadan önce düşünmemize sebep olmaktadır (Techopedia, 2016). Gerçek hayatta mevcut olan güvenlik ve gizlilikle ilgili risklerin çoğu internet alanına taşınmış; bu riskler internette mevcut olan risklerle birleşmiştir. Çevrimiçi Gizlilik konusundaki riskler ve kaygılar aşağıdakileri içerebilir (Aslanyürek, 2015: 23):

- Kişisel bilgilerin farklı yollara farklı amaçlarla hizmet etmek üzerine toplanması (pazarlama, gözetleme, kötüye kullanım vb.)
- Özel hayatın gizliliğini ihlal eden konular
- Diğer hakların ihlalleri

- Kötü amaçlı yazılımlar ve virüsler
- Dolandırıcılık ve çevrimiçi hırsızlık
- Pharming (bilgisayar korsanlarının bilgisayarlara ya da mobil cihazlara sızması ve kişinin bilgisayarını ona fark ettirmeden kötü amaçlar için kullanması, bir nevi asalaklık)
- Sosyal mühendislik
- İktidar organları tarafından gözetim ve denetim amacıyla yapılan uygulamalar.

Günümüzde çevrimiçi gizlilik ve internet güvenliği devlet, pazarlama şirketleri ve bilgisayar korsanları gibi unsurlar tarafından gözetim teknolojileri kullanılarak ihlal edilmektedir.

Kavramsal ve kuramsal çerçevesiyle çevrimiçi gözetim

İngilizce’de surveillance kelimesiyle ifade edilen “gözetim” Fransızca kökenli bir sözcüktür ve Oxford sözlüğünde “insanların aktivitelerini izleme ve gözleme” anlamına geldiği belirtilerek; tanımı “suçlu olduğundan şüphelenilen bir kişi veya suçun işlenmiş olabileceği bir yerin dikkatlice izlenilmesi eylemi” şekline yapılmıştır (Oxford Dictionaries, 2016).

David Lyon’a (2002: 14) göre gözetim; yönetim, koruma ya da yön verme, nüfuz etme gibi amaçlar için hedefi belli, sistematik ve rutin bir şekilde kişisel detaylara dikkat çekmedir. Sistematik ve hedefi belli ifadelerinden kasıt, ara sıra –rasgele– kendiliğinden yapılan araştırmanın olmadığı, kasıtlı ve belli protokol ve tekniklere bağlı olduğudur. Diğer taraftan da gözetim “rutin”dir. Zira bürokratik yönetimlerine ve bazı bilgi teknolojilerindeki gelişmişlik derecelerine bağlı olarak bütün toplumlarda günlük hayatın normal bir parçası haline gelmiştir.

Max Weber’e göre gözetim, emek ve sermayenin arasındaki mücadelenin bir unsurudur. Weber, gözetimin ayrıntılı bir biçimde bilgileri kayıt etme ve dosyalama işlevini sağlama amacının olduğunu belirtmektedir (Aktaran Sucu, 2011).

Anthony Giddens (1995)’e göre gözetim içinde iki olgu barındırır: İlki, bir topluluk ya da kurumun kendisiyle ilgili bilgilerin toplanması ve bu bilgilerle ilgili olan sembolik materyallerin depolanması; ikincisi ise herhangi bir topluluktaki alt kademedekilerin faaliyetlerinin üst kademe de yer alanlar tarafından denetlenmesi (Giddens, 1995: 169).

Gözetim olgusunun tarihsel süreç içerisinde geçirdiği evrim; modernlik öncesi dönemlerde gözetim, moderniteye geçiş sürecindeki gözetim ve modern zamanda gözetim olmak üzere üç başlık altında incelenmektedir. Bu ayrım genellikle çeşitli gözetim pratiklerinin ortaya çıkış durumuna ve insanlığın moderniteye doğru geçirdiği dönüşüme göre şekillenmektedir (Dolgun, 2005).

Yazının ortaya çıkmasıyla birlikte pastoral gözetim olarak da adlandırılan modernlik öncesi gözetim pratikleri ilkel toplulukları, yerleşik uygarlıkları, göçebe toplulukları, askeri devletleri, feodal beylikleri, kilise ve imparatorlukları kapsayan bir türdür. Bu dönemlerde ortaya çıkan gözetim türü sulama kanalları ile tarıma dayalı büyük ölçekli kamu faaliyetleri içindeki işgücünü denetlemek, vergi toplamaya yönelik olarak toplulukla ilgili kayıtlara sahip olmak, göçebe hayat kontrol altında tutmak savaşlara hazır olmak için asker sayısını belirlemek ve monarşik yapı ile mevcut iktidarı desteklemek için nüfusu kayıt altında tutmak gibi amaçlar taşımıştır (Tümurtürkan, 2010).

17. yüzyıldan itibaren ortaya çıkmaya başlayan hastane, ıslahevi, tımarhane ve hapishane gibi kurumlar gözetimin moderniteye geçiş sürecinde farklı bir olguya bürünmesine neden olmuştur. Foucault (2015: 11), gözetimin bu dönüşümü büyük kapatılma olarak isimlendirmiştir. Kuşkusuz bu tarihlerde kapatılma kurumlarının en önemlisi hapishane olmuştur. Bu bağlamda İngiliz mimar ve filozof Jeremy Bentham 1785'te panoptikon (pan: bütün, opticon: gözetlemek) isimli bir hapishane modeli tasarlamıştır (Öztürk, 2012: 138). Panoptikon türü hapishanede gözetleme kulesi ile mahkûmlar kontrol altında tutulmuş ve ne yaptıklarıyla ilgili bilgiler toplanmıştır. Gözetleme kulesi bu anlamda mahkûmlar için bir iktidar simgesi olmuştur (Foucault, 2012: 86).

Gözetim modern döneme kadar tam olarak kurumlaşmamış ve sistematikleşmemiştir. Bu dönemden itibaren kapitalizmle birlikte ortaya çıkan gözetim teknikleri bireyin tüm yaşamını özel/kamu ayrımı yapmadan egemenliği altına almıştır (Dolgun, 2005: 60-61). Modern dönemdeki gözetim pratikleri ilk önce ustabaşlarının işçileri gözetlemesiyle ve aylaklık eden işçileri sürekli uyarmalarıyla ortaya çıkmış. Daha sonra teknolojinin gelişmesi ile ustabaşlarının yaptığı gözetlemenin yerini kameralar almıştır. Fabrikalara yerleştiren kameralar sayesinde işçiler her an kendilerinin gözetlendiklerinin farkında olmakta ve davranışlarına çeki

düzen vermekteydiler. Günümüzde bu tarz kameralar zamanla üretimin yapıldığı fabrikalar dâhil olmak üzere hemen hemen her yere girmiştir.

Teknolojinin gelişmesiyle birlikte bugün gözetim yalnızca sokaklara konulan mobese kameralarıyla değil, aynı zamanda kredi ve banka kartları, uydu teknolojileri, telefon şebekeleri ve en önemlisi de internet üzerinden gerçekleştirilmektedir. Bilgi toplumu olarak adlandırıldığımız bu dönemde iktidarlar her türlü bilgi ve istihbarata sahip olmayı istemekte; internet ve siber uzayı da bu anlamda kullanılmaktadırlar. Enformasyon teknolojileri iktidarlar tarafından birer gözetim teknolojisi olarak da kullanılmaya başlanmıştır.

Mark Poster'ın kullandığı ve David Lyon'un geliştirdiği bir kavram olan süperpanoptikon 20. yüzyılın sonlarına doğru enformasyon teknolojilerinin gelişmesi, telekomünikasyon ve bilgisayardaki yeniliklere paralel olarak sosyal teori içinde ortaya çıkmış bir kavramdır. Bilgisayarlar, bilgisayarlardaki veri tabanları ve bilgisayar vasıtasıyla gerçekleştirilen iletişim panoptikonu hapishaneden çıkarmaktadır. Bilgisayarlar vasıtasıyla bütün toplum her yerde gözetimin nesnesi olmaktadır. Böylece insanlar, uzaktan işlenen sınıflandırılan, çoğaltılan, değerlendirilen ve de pazarlanan bir nesne haline gelmektedir. Kullandığımız GPS cihazları, cep telefonları, sokaklar dâhil her mekâna konulan kameralar, dinleme cihazları, internette yapılan alışverişler, sosyal medya, paylaşım siteleri süperpanoptikon modelinin ayrılmaz teknolojileri haline gelmiştir. Böylece iktidar her yere yayılır. Elektronik parmak izleri ve elektronik verileri temin eden kurumlar insanları sınıflandırmakta ve profillerini çıkarmaktadır (Öztürk, 2013).

Gözetim aracılığıyla internet ortamında güvenlik-gizlilik ihlalleri gerçekleştiren unsurlar ve başvurdukları yöntemler

İnternet güvenliği ve çevrimiçi gizlilik alanında yaşanan ihlalleri gerçekleştiren unsurları devlet, pazarlama şirketleri ve bilgisayar korsanları tarafından gerçekleştirilen internet güvenliği ile çevrimiçi gizlilik alanındaki ihlalleri temel başlıkları altında toplayabiliriz.

Devletler

Günümüzde iktidarı ellerinde bulunduran hükûmetler interneti ve siber uzayı, gözetim aracılığı ile bir toplumsal denetim aracı olarak kullanmaktadır. Siber uzay üzerinde bireylerin yaptıkları her türlü iletişim hükûmetler tarafından gözetlenmekte, bireylerin kullandıkları bilgisayar, cep telefonu vb. gibi iletişim aygıtları üzerinden gönderilen veriler en ince ayrıntısına kadar incelenmektedir. İktidarlar çoğu zaman bu tür gözetim uygulamalarının yapıldığını reddetmemekle beraber, özellikle bu dinleme ve izlemelerin halkı teröre karşı korumak amacıyla yapıldığı söylenmektedir. İktidarlar bu tür bir bahanenin arkasına sığınarak internet güvenliğini ve çevrimiçi ortamdaki kişisel gizliliğimizi ihlal etmektedirler. İktidarların siber uzayın denetleyici ve düzenleyici katmanını oluşturması onların bu alanda diledikleri gibi hareket etmelerini sağlamaktadır.

Günümüzde internet ortamında gerçekleştirilen gözetim faaliyetlerimim öncülüğünü ABD’de bulunan NSA (National Security Agency / Ulusal Güvenlik Dairesi)’in yapmaktadır. NSA, 11 Eylül 2001 tarihinde ABD’de gerçekleşen terörist saldırı sonrasında enformatik gözetimi en üst düzeye çıkartan Total Information Awareness adlı yazılım sistemini hayata geçirerek; ülke içindeki ve dışındaki kişilerin doktor kayıtlarından seyahat bilgilerine, harcama yaptıkları ürün cinsinden yüksek miktardaki banka havalelerine, telefon konuşmalarından dergi aboneliklerine, e-posta mesajlarından internette hangi siteleri ziyaret ettiklerine kadar tüm bilgileri takibe aldı (Dolgun, 2005: 147).

6 Haziran 2013 tarihinden itibaren The Guardian ve The Washington Post gazetelerinde eski NSA çalışanı Edward Snowden’in itirafları üzerine çıkan haberler NSA’in gözetim teknolojilerini nasıl kat kat ileriye taşıdığının bir göstergesiydi. Bu haberlerde Edward Snowden, NSA’in gerçekleştirdiği gözetim faaliyetlerini derinlemesine anlatmış ve bu gözetim faaliyetleri sonucunda ortaya çıkan güvenlik ve gizlilik ihlallerinin öneminden bahsetmiştir. Snowden’in bu ifşası PRISM, XKeyscore ve Tempora gibi internet izleme programlarının yanında ABD ve Avrupa’nın telefon görüşme kayıtlarının alıkonulmasını da ortaya çıkarmıştır (Macaskill, 2013). NSA’in gerçekleştirdiği bu gözetim faaliyetleri günümüzde devletlerin gerçekleştirdikleri gözetim faaliyetlerinin hangi seviyede olduğunu gözler önüne sermektedir. Bunun

sonucunda ortaya çıkan çevrimiçi gizlilik ve güvenlik ihlallerinin internet ortamındaki mahremiyetimizi tehlikeye soktuğu ortaya çıkmaktadır.

Pazarlama Şirketleri

İnternet güvenliği ve çevrimiçi gizliliği gözetim aracılığı ihlal eden unsurlar arasında reklam ve pazarlama şirketleri önemli yer tutmaktadır. Bu tür şirketler çeşitli veri toplama teknikleri kullanarak çevrimiçi ortamda bulunan her türlü kişisel verimizi gizli bir şekilde veri tabanlarına kaydedip kişisel profillerimizi çıkarmaktadırlar. Toplanan bu veriler daha sonra reklam faaliyetleri gerçekleştirmek üzere reklam şirketlerine satılmakta veya verileri toplayan bu şirketler bizzat kendileri bu verileri reklam amaçlı kullanmaktadırlar. Bu tür şirketlerin gerçekleştirdikleri bu faaliyetleri çevrimiçi davranışsal reklamcılık veya hedefli reklamcılık olarak tanımlanmaktadır.

Çevrimiçi davranışsal reklamcılık, bireylerin ilgilerine ve beğenilerine uygun olarak tasarlanmış reklamlar sunmak amacıyla bireylerin çevrimiçi faaliyetlerini izleyen bir uygulamadır. Bu uygulama, şirketlerin reklamlarını müşterilerinin ilgi alanlarına göre daha yakın bir şekilde konumlandırmasını sağlar (Juan Martinez vd. aktaran Cox ve Cline, 2012). Çevrimiçi davranışsal reklamcılık faaliyetleri gerçekleştiren şirketler arasında Google, Facebook, Amazon ve E-bay gibi büyük şirketler bulunmaktadır.

Çevrimiçi davranışsal reklamcılık günümüzde temel olarak arama motoru pazarlaması ve reklamcılığı ile iç içe çalışmaktadır. Arama motoru pazarlaması tekniklerinden birisi olan arama motoru reklamcılığı İngilizce’de “Search Engine Advertising” olarak ifade edilmektedir. Arama motoru reklamcılığı çok yeni ve gelişmekte olan yeni bir kavram olduğu için bazı kaynaklarda arama reklamcılığı, ücretli arama reklamcılığı (Paid Search Advertising), tıklama başına ücretlendirilen reklam, anahtar kelime reklamcılığı terimleriyle de ifade edilmektedir (Arslan, 2013: 50).

Arama motoru reklamcılığı, kullanıcılar işletmelerin arama motorlarından özel bir ödeme yaparak satın aldığı anahtar kelimelere tıkladığında, arama motoru sonuç sayfalarında görünen küçük reklamların konumlandırılması süreci olarak tanımlanmaktadır. Bu süreç reklam verenlere ölçülebilir dönüşümlerle potansiyel müşterilerini çekebilme imkânı sağlamaktadır. Bu nedenle arama motoru reklamcılığı günümüzde çok popüler hale gelmiştir (Mordkovich’ten aktaran Arslan, 2013: 50).

Google'ın Adwords ve AdSense isimli yıllardır işleyen iki reklam platformu bulunmaktadır. Bu platformlardan ilki reklam verenlerin kullandığı ve 2000 yılından beri hizmet veren Adwords isimli platformdur. Adwords ile reklam verenler internet sitelerine keywords (anahtar kelimeler) ile ziyaretçi çekmeyi hedeflerler. Google AdSense hizmeti ise Google tarafından şu şekilde tanımlanmaktadır: “Google AdSense, büyüklükleri ne olursa olsun tüm web sitesi yayıncılarının web sitelerinde hedeflenmiş Google reklamları göstererek para kazanmalarını sağlayan ücretsiz ve kolay bir yöntemdir” (Google AdSense Yardım, 2016). Google AdSense, internet siteleri için milyonlarca reklam veren ve destekleyicinin bulunduğu, internet sitesi sahiplerinin sitelerine reklamlar yerleştirebileceği en büyük reklam sağlayıcısıdır.

Google dışında çevrimiçi davranışsal reklamcılık faaliyetleri yapan bir diğer büyük şirket Facebook'tur. Facebook, yıllar içinde reklam verenlerin hedeflemelerine uygun belli kriterlere göre reklam alımlarını kolayca gerçekleştirmelerini sağlayacak reklam format ve modelleri geliştirmiştir. Reklamın amacına göre, kullanılması istenen ekran tipine göre (mobil, bilgisayar ya da tablet) ve ekranda görünmesi istenen alana göre (sağ reklam alanı ya da “Haber Kaynağı”) ya da reklamın içeriğine göre (metin, resim, video, vb.) reklam verenlere farklı seçenekler sunulmaktadır (Başer, 2014: 36).

Bilgisayar Korsanları

Geçmişten günümüze bilgisayar korsanları, internet güvenliği ve çevrimiçi gizliliğin ihlali konusunda defalarca gündeme gelmişlerdir. Bilgisayar korsanları, bilgisayar tarihi ve internetin ortaya çıkışından itibaren birçok kez internet güvenliği ve çevrimiçi gizlilik ihlallerine imza atmış, çoğu zaman bu ihlalleri niçin ya da kimin için yaptıkları öğrenilememiş, ihlallerin arkasındaki amaçlar çoğu zaman bilinmemiştir. Söz konusu ihlallere uğrayan kurban bazen sıradan bir kullanıcı olurken, bazen bir şirket, bazen bir banka, bazen bir üniversite hatta ve hatta bir devlet kurumu olmuştur. Bilişim tarihi yakından incelendiğinde internetin ortaya çıktığı ilk zamanlardan günümüze dek bilgisayar korsanları irili ufaklı binlerce mağduriyete sebep olmuşlardır. Bilgisayar korsanları gerçekleştirdikleri kötü amaçlı faaliyetlerde yazılım ve programlama bilgilerinin yanında toplum mühendisliği gibi yeteneklerden yararlanmışlardır (Aslanyürek, 2015: 71).

Bilgisayar korsanları genellikle bir saldırıyı gerçekleştirmeden önce hedefle ilgili bilgi toplamaya çalışırlar. Buldukları bilgileri ve açıkları, elde etmek istedikleri şeye ulaşabilmek amacıyla kullanırlar. Düzenlenecek saldırı, hedefe ve elde edilmesi planlanan şeye göre değişmektedir. Örneğin bir korsan, kredi kartı sahteciliğini gerçekleştirebilmek için birden çok yöntem seçebilir. Seçilecek saldırı türü ayrıca korsanın yeteneklerine de bağlıdır. Bir bankanın internet ağına sızmanın ve oradan bir şeyler çalmanın yolları farklıdır. Saldırganın iyi bir toplum mühendisliği yeteneği varsa bankada çalışan bir personeli çeşitli toplum mühendisliği yöntemleri kullanarak kandırabilir ve bankanın internet ağına girmeyi sağlayacak bilgileri ele geçirebilir. Toplum mühendisliği yönü zayıf olan saldırganlarsa, bunun yerine karmaşık ve güçlü bir güvenlik duvarıyla korunan internet ağına sızmak için yazılım bilgisinden ve açıklardan yararlanmak zorunda kalacaktır. Sonuçta tüm bilgisayar korsanları Kevin Mitnick gibi aynı anda hem toplum mühendisliği konusunda, hem telefon sistemleri konusunda hem de yazılım konusunda yetenekli değildir. Fakat bir saldırıya hazırlık aşamasında elde edilebilecek herhangi bir bilgi saldırının kaderini de değiştirecektir. Örneğin, dünyaca ünlü bilgisayar korsanı Kevin Mitnick bir firmaya sızmak için bilgi arayışındayken, çöp kutusunda firmanın sistemine girmeyi sağlayacak bazı kullanıcı adları ve parolalar bulmuştur. Mitnick, tamamen imha edilmesi gereken; fakat imha edilmesi unutulmuş bu kâğıtlar sayesinde firmanın ağına sızmayı başarmıştır (Aslanyürek, 2015: 75).

Elbahadır (2014) bir saldırganın hedef hakkında bilgi bulmak amacıyla yararlanabileceği kaynakları şöyle sıralamaktadır: Whois veritabanlarını sorgulama, IP ve IP veritabanlarını sorgulama, DNS sorgulama, arama motorları ve sosyal medya siteleri (Elbahadır, 2014: 44). Saldırgan için bilgi bulma aşaması bir saldırı için yeterli olmayacağından, saldırganın hedefinin açıklarını tespit etmesi için tarama yapması gerekir. Tarama aşamasında genellikle sunucuların açık portları, kullanılan işletim sistemi ve sistemdeki yazılımsal/donanımsal açıklar taranıp tespit edilir.

Bilgisayar korsanı saldırı düzenleyeceği hedefle ilgili yaptığı araştırmalardan ve taramalardan sonra elde ettiği veriler ışığında saldırısına yön verecek, bu doğrultuda bir saldırı yöntemi ve aracı seçecektir. Günümüzde bilgisayar korsanlarının en çok başvurduğu saldırı yöntemleri şöyledir: cookie hi-jacking, Active-X saldırıları, internet sitelerindeki açıklar, sahte siteler ve tehlikeli ekler, keyloggerlar, şifre ve gizli soru

tahminleri, domain hi-jacking, hizmet dışı bırakma saldırıları (ddos), sql sızmaları, virüs saldırıları, sıfıncı gün sızmaları, toplum mühendisliği (Aslanyürek, 2015: 78).

Pek çok bilgisayar korsanı yukarıdaki yöntemlerden bir ya da birkaçını kullanarak hedefine zarar vermeye çalışacaktır. Usta bilgisayar korsanlarının toplum mühendisliği yönü oldukça güçlü olduğundan kullandığımız cep telefonları ve bilgisayarlarımızda antivirüs yazılımları bulunmasına rağmen dışarıdan gelecek insani tehditlere karşı açık olmalıyız.

Türkiye’de internet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili görüşleri ve farkındalıkları üzerine bir araştırma

Ülkemizde internet güvenliği ve çevrimiçi gizlilik ihlalleri ile ilgili gerçekleştirilmiş çalışmalardan gözetim olgusu üzerinde duran araştırmalar (Tokgöz, 2011; Karakaya, 2014; Karslıoğlu, 2014) yalnızca devlet tarafından gerçekleştirilen gözetim faaliyetlerine odaklanmıştır. Bu konuyla ilgili yapılmış olan diğer çalışmalar (Eriş, 2009; Kara, 2013) ise siber güvenlik olgusu ile devletlerin birbirleriyle yürüttükleri asimetrik savaşlar üzerinde durmuşlardır. Bu çalışmada gözetim olgusuna daha geniş bir perspektiften bakılmış ve devlet tarafından gözetim aracılığı ile gerçekleştirilen ihlallerin yanına reklam şirketleri ve bilgisayar korsanları tarafından gerçekleştirilen ihlaller de dahil edilmiş; bu ihlallerin son kullanıcılar üzerinde yarattığı etkiler irdelenmiştir.

Araştırmanın amacı Türkiye’deki internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili olarak; örneklem dâhilinde seçilen Türkiye’deki en popüler beş sosyal medya sitesinde aktif internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili kanaatlerini ve farkındalıklarını ortaya koymaktır.

Önceden belirttiğimiz gibi daha önce gerçekleştirilen çalışmalar internet güvenliği ve çevrimiçi gizliliği ihlal eden unsurların hepsini aynı anda incelememiştir. Bu anlamda çalışmamız bu üç unsuru aynı çatı altında toplaması açısından önemlidir ve literatüre sağlayacağı yarar son derece açıktır. Önceki çalışmaların genellikle gözetim odaklı olması ve bizim çalışmamızın daha çok güvenlik ve mahremiyet odaklı olması çalışmamızı geçmişte yapılan çalışmalardan ayırmakta; çalışmamıza farklı bir anlam katmaktadır.

Ayrıca çalışmamız çerçevesinde internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik hakkındaki kanaatlerini ve farkındalıklarını inceleme konusunda gerçekleştireceğimiz anket çalışmasından çıkacak sonuçlar, daha sonra bu alanda yapılacak çalışmalara ışık oluşturacaktır.

Araştırmanın amacı doğrultusunda altı adet araştırma sorusu belirlenmiştir:

1. Katılımcıların cinsiyetleri ile interneti kullanma sıklıkları arasında anlamlı bir fark var mıdır?
2. Katılımcıların cinsiyetleri ile yaşanan çevrimiçi gizlilik ihlalleri karşısında internetten vazgeçme eğilimleri arasında anlamlı bir fark var mıdır?
3. Katılımcıların yaşları ile gözetimin güvenlik amaçlı kullanıldığı konusundaki görüş arasında anlamlı bir fark var mıdır?
4. Katılımcıların eğitim durumları ile çevrimiçi ortamda bulunan kişisel verilerin mahremiyetlerinin ihlal edildiğine dair görüşleri arasında anlamlı bir fark var mıdır?
5. Katılımcıların gelir durumu ile gözetimin güvenlik amaçlı kullanıldığı konusundaki görüşleri arasında anlamlı bir fark var mıdır?
6. Katılımcıların gelir durumu ile çevrimiçi gizlilik ihlalleri karşısında internetten vazgeçme eğilimleri arasında anlamlı bir ilişki var mıdır?

Araştırma, yürütülecek olan anket çalışmasında katılımcı olarak yer alan internet ve sosyal medya sitelerindeki aktif kullanıcılarla sınırlandırılmıştır. “We are Social” isimli ajansın yaptığı istatistiksel araştırmaya göre; ülkemizde 40 milyon sosyal medya hesabı bulunmaktadır (Kemp, 2015). Bu sosyal medya hesapları araştırmamızın evrenini oluşturmaktadır. Örneklem homojen olmamakla birlikte her yaş, eğitim ve gelir grubundan katılımcıyı barındırmaktadır. Dolayısıyla örneklem büyüklüğü p ve q değerleri 0,05 alınarak, %5’lik hata payı düşünülerek $\alpha = 0,05$ kabul edilerek 384 olarak hesaplanmıştır. Bu sebeple anket 479 katılımcıya uygulanmıştır. Örneklemdeki sınırlılık, araştırma evreninin tamamının incelemesinin mümkün olmamasındandır.

Araştırma çerçevesinde gerçekleştirilecek olan anket çalışması, ülkemizde en popüler olan Facebook, Twitter ve Google Plus isimli sosyal medya platformları üzerindeki aktif internet kullanıcılarına uygulanmıştır. Bu bağlamda araştırmamızda “Kartopu Örneklem Sistemi” kullanılmıştır.

Çalışmamızın internet ve sosyal medya ile ilgili olmasından dolayı yalnızca aktif internet kullanıcıları çalışmaya dâhil edilmiştir. Sosyal bilimler alanında yapılan çalışmaların tamamen deneyselliğe oturtulamamasından dolayı kaynaklanan bu sınırlılık, çalışmamız için de geçerlidir.

Araştırma Yöntemi ve Bulgular

Anket çalışmasından toplanan verilerin değerlendirilmesi ve analizinde SPSS 21,0 istatistik paket programı kullanılmıştır. Testin güvenilirlik katsayısı 0,811 olarak belirlenmiştir.

Katılımcıların Sosyo-Demografik Özellikleri

Çalışma 263'ü erkek, 216'sı kadın olmak üzere toplam 479 katılımcıya uygulanmıştır. Katılımcıların % 81'lik bölümünü 18-34 yaş arası genç bireyler oluşturmuştur. Anket çalışmasına katılan internet ve sosyal medya kullanıcılarının % 82'sinin Lisans ve Lisansüstü bölümlerden mezun olduğu sonucu ortaya çıkmıştır. Böylece katılımcılarımızın oldukça eğitilmiş bireyler olduğu görülmektedir. Katılımcıların % 82'si düşük ve orta gelir grubunda yer almıştır. Katılımcıların % 79'u ile çoğunluğu bekârdır.

İnternetin ve Sosyal Ağların Kullanımıyla İlgili Bulgular

İnternet siteleri ve sosyal ağları kullanım amacı ve sıklığıyla ilgili önemli bulgular şu şekildedir: Katılımcıların % 89'u çoğu zaman interneti bilgi almak amacıyla kullanmaktadır. Katılımcıların büyük kısmı internete önemli bir bilgilenme alanı olarak bakmaktadır. İnterneti iletişim amacıyla çoğu zaman kullananların oranı % 78'dir. Böylece katılımcıların interneti önemli bir iletişim kanalı olarak gördükleri sonucu ortaya çıkmıştır. Katılımcıların % 68'i internet aracılığı ile bazen alışveriş yaptıklarını belirtmişlerdir. Bu sonuca göre katılımcıların çoğu geleneksel alışveriş alışkanlıklarından vazgeçmemiştir. Günümüzde internet sayesinde bankacılık işlemleri çok kolay ve hızlı bir şekilde gerçekleştirilmektedir. Araştırma bulguları katılımcıların % 80'i ile yüksek bir bölümünün bankacılık işlemlerini internet aracılığıyla gerçekleştirdiği sonucunu ortaya koymaktadır. Bugün internet televizyon, gazete, radyo ve sinema gibi kitlesel iletişim araçlarını tek bir ortamda birleştirmektedir. Bunun

sonucu olarak da internet önemli bir eğlence aracıdır. Nitekim araştırmamıza katılan internet kullanıcılarının % 75'i interneti eğlence amaçlı olarak çoğu zaman kullandıklarını belirtmişlerdir. Bu bağlamda kullanıcıların çeşitli konularla ilgili oluşan ihtiyaçlarını internet ve sosyal medya aracılığıyla giderdiği sonucu ortaya çıkmaktadır.

İnternet Siteleri ve Sosyal Ağlardaki Davranışla İlgili Bulgular

Katılımcıların internet siteleri ve sosyal ağlardaki davranışlarıyla ilgili bulgular şu şekildedir: Bugün internet mobil telefonlar ve tabletler sayesinde hemen hemen her yerde kullanılabilir de katılımcılarımızın % 77'si internete en çok evlerinden eriştiklerini belirtmişlerdir. İnternet siteleri ve sosyal ağ platformlarına üye olurken ya da bu siteleri kullanırken karşımıza kullanım şartları ve gizlilik politikaları isimli uzun metinler çıkmaktadır. Bu metinleri dikkatlice okuyup anlamak sitenin genel kullanımı ve gizlilikle ilgili oluşacak hukuki problemlerin giderilebilmesi açısından önemlidir. Fakat katılımcılarımızın yalnızca % 17'si bu tarz metinleri çoğu zaman okuduklarını belirtmişlerdir. Bu metinlerin çok uzun olması, okunmasının çok uzun zaman alması ve ağır bir hukuksal dille yazılmış olmasından dolayı bu metinlerin okunması internet kullanıcıları tarafından genellikle sıkıcı bulunur. Günümüzde birçok sosyal ağ platformu bulunmaktadır ve bunlar arasında en popüler olanı kuşkusuz Facebook'tur. Katılımcılarımıza hiç kullanmadıkları sosyal ağ platformunu sorduğumuzda % 1 ile Facebook cevabını aldık. Böylece Facebook'un popülaritesinin ne denli yüksek olduğu bir kez ortaya çıkmıştır.

Sosyal Paylaşım Ağlarının Kullanım Amacıyla İlgili Bulgular

Bugün sosyal medya siteleri kullanıcılarına birçok açıdan kolaylık sunmaktadır. Bu siteler çeşitli kullanıcılar tarafından farklı amaçlarla kullanılmaktadırlar. Katılımcıların % 63'ü sosyal ağları bilgilenme amacıyla kullandıklarını belirtmişlerdir. Katılımcıların % 48 ile yaklaşık yarısı sosyal ağları içerik paylaşmak amacıyla aktif olarak kullandıklarını ifade etmişlerdir. Sosyal ağları iletişim amaçlı kullananlar % 55'lik kesimi oluşturmaktadır. Sosyal ağlarda kullanıcılar eğlenceye yönelik içerikler de paylaşabilmektedir (müzik, video, resim, hikâye, makale vb.). Ayrıca Facebook gibi sitelerde oyun da oynanabilmektedir. Buna rağmen katılımcıların yalnızca % 22'si sosyal ağları eğlence amaçlı kullandıklarını belirtmişlerdir. Sosyal ağlar insanların o

anda ne yaptıklarını ve nerede bulduklarını belirtmek için de kullanılmaktadır. Fakat çalışmamızdaki katılımcıların yalnızca % 15'lik bir kısmı çoğu zaman yer bildiriminde bulduklarını belirtmişlerdir. Araştırma bulguları katılımcıların % 62'sinin haftada en az bir kere sosyal paylaşım ağlarında içerik paylaştığı bilgisini ortaya koymuştur.

Katılımcıların Gözetim ve Mahremiyetle İlgili Tutumları

Çalışmamızın en önemli kısmını kuşkusuz katılımcıların internet güvenliği ve çevrimiçi gizlilik ihlalleriyle ilgili görüşleri oluşturmaktadır. Buna göre katılımcıların yarısı internet ve sosyal paylaşım sitelerinin güvenilir bir iletişim ortamı sağladığına inandığını belirtmiştir. İnternet siteleri ve sosyal paylaşım ağlarında kendini daha özgür hissedenlerin oranı ise % 54'tür. Bu tür ortamlarda devlet, pazarlama şirketleri ve bilgisayar korsanları tarafından mahremiyet ihlaline uğradıklarını iddia edenlerin oranı % 52'dir. Yaşanan mahremiyet ihlallerine rağmen internette varlığını sürdürmeye devam edeceğini ifade eden kullanıcıların oranı % 28'dir. Bu konuda kararsız olanların oranı ise % 42 ile oldukça yüksek bir orandır. Sosyal paylaşım sitelerinde sahte profil kullanarak mahremiyet ihlallerine karşı konulabileceğini düşünenlerin oranı % 20 ile düşüktür. Sosyal ağ medyada profillerine kendi kimliğinden farklı bilgiler giren katılımcıların oranı da %10 ile oldukça düşüktür. İnternet siteleri ve sosyal paylaşım ağlarına devlet, pazarlama şirketleri veya bilgisayar korsanları tarafından kişisel verileri toplamaya ve sürekli gözetim yapmaya yönelik buldurulan bir yazılımın varlığını katılımcıların % 74'lük bir bölümü düşünmektedir ve bu oran oldukça yüksek bir orandır.

İktidarı elinde bulduran hükûmetler ve başta ABD olmak üzere birçok büyük devlet gözetim teknolojilerini son derece etkin bir şekilde kullanmaktadır. Bu devletler gözetim teknolojilerini kullandıklarını inkâr etmemekte ve bu teknolojileri halkı terörden korumak için kullandıklarını iddia etmektedirler. Anket çalışmamıza katılan katılımcıların % 91'i yani büyük çoğunluğu amaç ne olursa olsun kişisel verilerin toplanmaması gerektiğini savunmaktadır. Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için bireylerin mahremiyetlerinden taviz verebileceği görüşünü savunanların oranı % 27'dir. Katılımcıların % 51'i ise mahremiyetlerinden ne olursa olsun taviz vermeyeceklerini belirtmişlerdir. Katılımcıların % 86'sı devletlerin güvenlik hedefli izleme yapmasına ve kişilerin haberi olmadan kişisel veri toplanmasına karşıdır.

Katılımcıların İnternet ve Sosyal Medya Kullanıcılarının Gizlilik ve Güvenlik ile İlgili Görüş ve Davranışları Üzerine Çıkarımsal Analizler ve Bulgular

Çalışmamızın temel amacı anketimize katılan internet ve sosyal medya kullanıcılarının çevrimiçi gizlilik ve internet güvenliği alanında yaşanan sorunlara ilişkin kanaatleri ile cinsiyet, medeni durum, yaş, gelir durumu ve eğitim durumu gibi demografik özellikleri arasında anlamlı bir fark olup olmadığını ortaya koymaktır. Nitekim çalışmamızın araştırma sorusu şu şekilde belirlenmiştir: “internet ve sosyal medya kullanıcılarının sosyo-demografik özellikleri ile çevrimiçi gizlilik ve internet güvenliliği alanında yaşanan sorunlara ilişkin kanaatleri arasında anlamlı bir fark vardır.”

Araştırma sorumuzun ve araştırma alt sorularımızın cevabını bulabilmek amacıyla anket verilerine çeşitli analizler uyguladık. Faktör analizi aralarında ilişki bulunan benzer değişkenleri bir arada görmemizi sağlar. Bu nedenle anketimizde yer alan sorulara faktör analizi uyguladık. Bunun sonucunda her biri farklı bir şeyi ölçümleyen beş soru faktörü ortaya çıkmıştır. Böylece bütün sorulara tek tek T Testi ya da Anova Analizi uygulanmak yerine, faktörler altında gruplandırılmış ve birbirine yakın unsurları ölçümleyen soru gruplarına T Testi ve Anova Analizi uygulama şansı yakaladık. Bu durum bize soru faktörlerinde yer alan sorulara verilen cevapların demografik özelliklere göre değişkenlik gösterip göstermediğini analiz etme olanağı sundu.

Soru faktörleri üzerinde gerçekleştirdiğimiz Bağımsız T Testi ve Anova Analizine göre katılımcıların çevrimiçi gizlilik ve internet güvenliği alanında yaşanan sorunlara ilişkin kanaatleri ile demografik özellikleri arasında anlamlı bir fark tespit edilmiştir. Böylece yöneltilen cevapların demografik özelliklere göre değişkenlik gösterdiği ortaya çıkmıştır. Yapılan analizlere göre kadınların erkeklere oranla internet ve sosyal medyada daha aktif oldukları ve bu platformlarda daha çok içerik paylaştıkları ortaya çıkmıştır. Bu bağlamda erkek egemen bir toplumda her türlü ortamda istediklerini ifade edemeyen, çoğu zamanda toplumsal baskı yüzünden bundan çekinen bayanların interneti ve sosyal medyayı önemli bir aktivite alanı olarak gördükleri düşünülebilir.

Bir diğer bulgu yaşanan çevrimiçi gizlilik ihlalleri karşısında kadınların erkeklere oranla internet kullanımından daha az vazgeçmeyi istedikleri sonucudur. Kadın internet ve sosyal medya kullanıcıları internet ve sosyal medya sitelerinde güvenlikleri ve mahremiyetleri ihlal edilse de bu tür ortamlarda varlıklarını sürdüreceklerini belirtmişlerdir. Bu görüşe paralel olarak fikir belirten kadın kullanıcılar için internet ve

sosyal paylaşım sitelerinde var olmak, güvenlikten daha önemlidir; internet ve sosyal medya sitelerinde kadınlar kendilerini daha özgür hissetmektedirler.

Gözetimin devletler tarafından güvenlik amaçlı uygulandığı görüşünü savunanlar gelir durumu açısından değişkenlik göstermektedir. Aylık kazancı 3000-4999 TL ile 5000 TL ve üzeri olan katılımcıların gözetimin devletler tarafından güvenlik amaçlı uygulandığına diğer gelir gruplarında bulunan katılımcılardan daha az inandığı sonucu ortaya çıkmıştır. Düşük gelir grubuna sahip olan 0-999 TL grubundaki katılımcılar ise bunun tam aksini iddia etmekte ve devletlerin bizi güvenliğimizi korumak amacıyla gözetlediğine inandıklarını belirtmişlerdir.

İnternet güvenliği ve çevrimiçi gizlilik ihlalleri karşısında internet kullanımından vazgeçme eğilimi gelir gruplarına göre değişkenlik göstermiştir. 1000-2999 TL gelir grubuna mensup olan katılımcılar çevrimiçi gizlilik ihlalleri karşısında internet kullanımından vazgeçmeyeceklerini, diğer gelir gruplarında bulunan katılımcılarla oranla daha fazla belirtmişlerdir. 1000-2999 TL gelir grubuna mensup katılımcılara göre internet ve sosyal medyada var olmak kişisel güvenlikten daha önemlidir; bu tür ortamlar bireye kendini özgür hissetmektedir. Yukarıdaki görüşün tam aksini ise ayda 5000 TL ve üzeri kazanan katılımcılar oluşturmaktadır. Bu katılımcılara göre internet ve sosyal medyada var olmak kişisel güvenlikten daha önemli değildir.

Yukarıdaki bulgular ışığında internet ve sosyal medya kullanıcıların internet güvenliği ve çevrimiçi gizlilik ihlalleri ile ilgili kanaatlerinin, tutumlarının ve farkındalık düzeylerinin cinsiyetlerine, yaşlarına, gelir ve eğitim düzeylerine göre farklılık gösterdiği sonucu araştırmamızın ana sonucunu oluşturmuştur.

Çalışmamızın bir diğer çarpıcı sonucu ise, internet güvenliği ve çevrimiçi mahremiyet ihlalleri karşısında internet kullanımından vazgeçme eğiliminin oldukça düşük olduğudur. Katılımcıların küçük bir bölümü mahremiyet ihlalleri karşısında internet kullanımından ödün vereceklerini belirtmişlerdir. Ayrıca katılımcıların önemli bir bölümü bu konuda kararsızlık yaşamaktadır. Katılımcıların çoğuna göre internette var olmak özgürlükten daha önemlidir. İnternet kullanıcıları internet ortamında kendilerini daha özgür hissetmektedirler ve onlara göre internette var olmak kişisel güvenlikten daha önemlidir. Yalnız ilginç bir durum söz konusudur ki, katılımcıların çok büyük bir çoğunluğu siber ortamda internet güvenliği ve çevrimiçi gizliliğin devlet, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edildiğini savunmaktadırlar.

Fakat katılımcılar internetten sağladıkları faydanın özgürlüklerinden daha önemli olduğunu ve bu platformda yer almaktan vazgeçmeyeceklerini belirtmişlerdir.

Araştırmanın Sonucu

Bu çalışmada internet ve sosyal medya platformlarında gerçekleştirilen çevrimiçi gizlilik ve internet güvenliği ihlalleri karşısında internet ve sosyal medya kullanıcılarının tutumları, farkındalıkları ve kanaatlerini incelemek amacıyla bir anket çalışması gerçekleştirilmiştir.

Türkiye’de aktif olarak internet ve sosyal medya platformlarını kullanan, kartopu örnekleme sistemi aracılığıyla ulaşılan 14 yaş ve üstü toplam 479 katılımcıya internet üzerinden 44 soruluk bir anket formu uygulanmıştır. Araştırmada sonucunda elde edilen verilerin analizinin tutarlı olması için başta güvenilirlik testi yapılmış ve bu test sonucunda yüksek bir güvenilirlik kat sayısı elde edilmiştir. Bu testin ardından örneklem büyüklüğünün faktör analizi yapmaya uygun olup olmadığını tespit etmek amacıyla KMO ve Bartlett Testi yapılmıştır. Soruların faktörlere göre dağılımını bulmak için faktör analizi gerçekleştirilmiştir. Faktörler belirlendikten sonra yapılacak analizlerde hangi testlerin kullanılacağına karar verebilmek amacıyla normallik testi yapılmıştır. Buna göre verilerin normal dağıldığı sonucu ortaya çıkmıştır. Bu sayede iki bağımsız değişkeni olan verilere Bağımsız T testi, ikiden fazla bağımsız değişkeni olan verilere ise Anova analizi uygulanmıştır.

Gerçekleştirilen analizlere göre katılımcıların çevrimiçi gizlilik ve internet güvenliği alanında yaşanan sorunlara ilişkin kanaatleri ile demografik özellikleri arasında anlamlı bir fark tespit edilmiştir. Böylece yöneltilen cevapların demografik özelliklere göre değişkenlik gösterdiği ortaya çıkmıştır. Bu bağlamda altı araştırma sorusundan beşi değişkenler arasından anlamlı bir fark olması nedeniyle kabul edilmiş; bir araştırma sorusu ise değişkenler arasından anlamlı bir fark olmadığından reddedilmiştir.

Yapılan analizlere göre katılımcıların cinsiyetleri ile interneti kullanım sıklığı arasında anlamlı bir farklılık görülmüştür. Buna göre kadınların erkeklere oranla internet ve sosyal medyada daha aktif oldukları ve bu platformlarda daha çok içerik paylaştıkları ortaya çıkmıştır.

Bir diğer analize göre katılımcıların cinsiyetleri ile yaşanan çevrimiçi gizlilik ihlalleri karşısında internetten vazgeçme eğilimleri arasında anlamlı bir fark tespit edilmiştir. Bu bağlamda kadın internet ve sosyal medya kullanıcıları internet ve sosyal medya sitelerinde güvenlikleri ve mahremiyetleri ihlal edilse de bu tür ortamlarda varlıklarını sürdüreceklerini belirtmişlerdir.

Katılımcıların yaşları ile gözetimin güvenlik amaçlı kullanıldığı konusundaki görüş arasında anlamlı bir fark olduğu tespit edilmiştir. Buna göre 14-17 yaş grubunda yer alan katılımcılar gözetimin yalnızca güvenlik amaçlı yapıldığına dair görüşe sahiptirler.

Katılımcıların eğitim durumları ile çevrimiçi ortamda bulunan kişisel verilerin mahremiyetlerinin ihlal edildiğine dair görüşleri arasında anlamlı bir fark olmadığı yapılan ANOVA Analizi sonucu ortaya çıkmıştır.

Katılımcıların gelir durumu ile gözetimin güvenlik amaçlı kullanıldığı konusundaki görüşleri arasında anlamlı bir fark tespit edilmiştir. Buna göre aylık kazancı 3000-4999 TL ile 5000 TL ve üzeri olan katılımcıların gözetimin devletler tarafından güvenlik amaçlı uygulandığına diğer gelir gruplarında bulunan katılımcılardan daha az inandığı sonucu ortaya çıkmıştır.

Katılımcıların internet güvenliği ve çevrimiçi gizlilik ihlalleri karşısında internet kullanımından vazgeçme eğilimi gelir gruplarına göre anlamlı bir farklılık göstermiştir. 1000-2999 TL gelir grubuna mensup olan katılımcılar çevrimiçi gizlilik ihlalleri karşısında internet kullanımından vazgeçmeyeceklerini, diğer gelir gruplarında bulunan katılımcılarla oranla daha fazla belirtmişlerdir.

Çalışmada katılımcıların devlet, reklam şirketleri ve bilgisayar korsanları tarafından gözetim teknolojileri kullanılarak gerçekleştirilen internet güvenliği ve çevrimiçi gizlilik ihlallerinin farkında oldukları ve yapılan bu ihlallerden memnun olmadıkları sonucu ortaya çıkmaktadır. Buna rağmen katılımcıların internet kullanımından vazgeçme eğilimi düşüklük göstermektedir.

Sonuç

21. yüzyıla girilmesiyle birlikte dünyada ve ülkemizde teknoloji alanında önemli gelişmeler yaşanmış; geniş bant internet bağlantısı ortaya çıkmış, bilgisayar satışları artmış, ilerleyen zamanlarda ise sosyal ağların da hayatımıza girmesiyle birlikte internet

kullanım oranları çok yüksek oranlara ulaşmıştır. Akıllı telefon teknolojisinin ortaya çıkması ve dizüstü bilgisayarların da yaygınlaşması sayesinde bugün insanlık hemen hemen her yerde internete erişebilecek duruma gelmiştir. Bugün internetin sağladığı avantajlar geçmişte insanlığın sahip olduğu birçok geleneksel yöntem terk edilmeye başlanmıştır. İnternet sayesinde mağazalara gitmeden alışveriş yapabilmekte, bankacılık işlemlerimizi şubesiz bankacılık ile birkaç saniyede halledebilmekte, internet üzerinden medyanın her türüne erişebilmekte, sosyal ağlar sayesinde mekân ortaklığı gözetilmeden sosyalleşebilmekteyiz.

Bilişim teknolojilerinin ve internetin günden güne gelişmesi; internetin sunduğu avantajlara her gün bir yenisinin eklenmesi sonucunda kullanım oranlarının çok yüksek oranlara erişmiş olması bugün çevrimiçi ortamda çok yoğun ve hızlı bir enformasyon akışının oluşmasını sağlamıştır. Bu enformasyon akışını farklı amaçlarla gözetim teknolojilerini kullanarak kontrol etmek isteyen devlet, reklam şirketleri ve bilgisayar korsanlarının faaliyetleri internet güvenliği ve çevrimiçi gizlilik ihlallerine sebep olmaktadır. Özellikle 2013 yılının Haziran ayında ortaya çıkan Edward Snowden'in Amerikan Güvenlik Dairesi (NSA) ile ilgili itirafları gözetim teknolojilerinin devletler tarafından ne boyutta kullanıldığının ve bunun sonucunda yaşanan ihlallerin farklı bir seviyeye taşındığının en büyük göstergesidir. Öte yandan Google, Facebook, Yahoo, Amazon ve E-bay gibi birçok büyük şirketin internet ortamında gerçekleştirdikleri çevrimiçi davranışsal reklamcılık faaliyetleri de mahremiyet ihlallerinin diğer ayağını oluşturmaktadır. İnternet üzerinden güvenlik ve gizlilik ihlali gerçekleştiren bir diğer unsur olan bilgisayar korsanlarının da kötü amaçlı faaliyetleri yüzünden her gün binlerce insan mağdur olmaktadır. Böylece internet ve sosyal medyanın gittikçe güvensiz ve mahremiyet anlayışından uzak ortamlar haline gelmeye başladıkları söylenebilir.

Çalışmamızda internet ve sosyal medyayı bir gözetim teknolojisi olarak kullanıp gizlilik ihlalleri gerçekleştiren ve önceki çalışmalarda defalarca karşımıza çıkan devlet unsurunun yanı sıra yine aynı türde ihlaller gerçekleştiren; fakat önceki çalışmalarda kendilerine çok az yer bulmuş pazarlama şirketleri ve bilgisayar korsanlarına yer verdik. Bu unsurların internet ve sosyal medyada gizlilik ihlalleri gerçekleştirenken başvurduğu yöntemleri ele aldık. Bu tür ihlallerin yalnızca devlet aracılığıyla gerçekleştirilmediğini

hatırlatmayı kendimize görev edindik. Böylece ileride internet ve gizlilik ilişkisini farklı şekilde ele almak isteyenlere en azından fikir vermiş olduk.

Çalışmamız kapsamında gerçekleştirdiğimiz anket araştırmasından elde ettiğimiz bulgular araştırmamızın genel sonucuna da yön verdi. Buna göre tüm mahremiyet ihlallerinin farkında olmalarına rağmen anketimize katılan kullanıcıların internet kullanımından vazgeçme eğiliminin düşük kalmaktadır.

Katılımcıların ihlaller karşısında internet ve sosyal medyayı kullanmaktan vazgeçme eğilimlerinin düşüklüğünün nedeni elde edilen verilerin beklenti ve gereksinim kavramlarıyla ilişki kurularak değerlendirildiğinde ortaya çıkmaktadır. Toplumdaki her bireyin farklı gereksinimleri bulunmaktadır. Sosyal teoride gerek egemen, gerekse eleştirel yaklaşımlar içerisinde bireylerin gereksinimleriyle ilgili birçok teori mevcuttur. Bu teorilere göre insanlar, sürekli olarak gereksinimlerini gidermek amacıyla arayış içerisinde bulunmaktadırlar. Bireyler medyadan ve diğer kaynaklardan bu gereksinimlerini gidermek için bir takım beklentilere girerler. Medya aracılığı ile bu gereksinimlerden bazılarını giderirler. Nitekim bilişsel, duygusal, sosyal bütünleşme ve alışkanlık ihtiyaçları bulunan internet kullanıcıları; önemli bir kitle iletişim medyası olan internet ve sosyal medya sayesinde bu ihtiyaçlarını karşılamaktadırlar. Anket çalışmasından elde edilen veriler ve gerçekleştirilen analiz sonuçları da bunu doğrulamaktadır. Dolayısıyla kullanıcılar, internet ve sosyal medyadan elde ettikleri kazanımların ihtiyaçlarını tatmin etmesi nedeniyle, anonimlik ve özgürlük karşısında siber âlemde var olmayı daha fazla istemektedirler.

İnternet ve sosyal medya günümüzde insan hayatında o kadar büyük bir yer kaplamaktadır ki, çoğumuz internete bize sağladığı en az bir önemli kazanım nedeniyle internete bağımlı durumdayız. Bu ortamlarda kişi güvenliğinin ve çevrimiçi gizliliği ihlal edilmesine rağmen internetten kopuşun gerçekleşmemesinin en büyük nedeni de burada yatmaktadır. Kimileri için internet bir gelir kapısıyken, toplum içerisinde kendini ifade yetisinin zayıf olduğu bireyler için, internet ve sosyal medya önemli bir sosyalleşme aracıdır. İnternet kimileri için bir eğlence mekânıyken, kimileri için olmazsa olmaz bir iletişim aracı konumundadır. Bu örnekler daha da çoğaltılabilmektedir. Bu bağlamda bireyler ve internet arasında fayda ve insan hayatını kolaylaştırma üzerine kurulu bu ilişki karşısında özgürlük, anonimlik, güvenlik ve gizlilik gibi kavramların önem seviyesi düşük bir düzeyde kalmaktadır.

Kaynakça

- Aksoy, Şebnem (2013), Hasta Haklarında Mahremiyet ve Özel Hayatın Gizliliği. Yayınlanmamış Yüksek Lisans Tezi, *Beykent Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul.
- Arslan, Müzeyyen (2013), Arama Motoru Reklamcılığının Etkinliği Üzerine Bir Araştırma: Google Adwords Uygulaması. Yayınlanmamış Yüksek Lisans Tezi, *Çağ Üniversitesi Sosyal Bilimler Enstitüsü*, Mersin.
- Aslanyürek, Malik (2015), İnternet Güvenliği ve Çevrimiçi Gizlilik Alanlarında Yaşanan Sorular: İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları Üzerine Bir Araştırma. Yayınlanmamış Yüksek Lisans Tezi, *Gazi Üniversitesi Sosyal Bilimler Enstitüsü*, Ankara.
- Başer, Ayşegül (2014), Sosyal Medya Kullanıcılarının Kişilik Özellikleri Kullanım ve Motivasyonlarının Sosyal Medya Reklamlarına Yönelik Genel Tutumları Üzerindeki: Facebook Üzerine Bir Araştırma. Yayınlanmamış Doktora Lisans Tezi, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul.
- Brauch, Hans Gunther (2008), Güvenliği Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü. *Uluslararası İlişkiler Dergisi*, 5 (18): 1-47.
- Cox, Jeffrey T. and Cline, Kelly M. (2012), Parsing The Demographic: The Challenge Of Balancing Online Behavioral Advertising and Consumer Considerations. *Journal Of Internet Law*, 3 (3): 3-12,
- Dolgun, Uğur (2005), *Enformasyon Toplumundan Gözetim Toplumuna: 21. Yüzyılda Gözetim, Toplumsal Denetim ve İktidar İlişkileri*. Bursa: Ekin.
- Elbahadır, Hamza (2014), *Hacking Interface*. İstanbul: Kodlab.
- Eriş, Ufuk (2009), Türkiye’de Kırıcı (Hacker) Kültürü, Yayınlanmamış Doktora Tezi, *Anadolu Üniversitesi Sosyal Bilimler Enstitüsü*, Eskişehir.
- Flaherty, Casey (1992), *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Amerika Birleşik Devletleri: The University of North Carolina Press.
- Foucault, Michel (2012), *İktidarın Gözü – Seçme Yazılar 4*. Işık Ergüden (Çev.), İstanbul: Ayrıntı Yayınları.
- Foucault, Michel (2015), *Büyük Kapatılma – Seçme Yazılar 3*. Ferda Keskin ve Işık Ergüden (Çev.), İstanbul: Ayrıntı Yayınları.

- Giddens, Anthony (1995), *A Contemporary Critique of Historical Materialism*. 2. Basım, Stanford: Stanford University Press.
- Google Adsense Yardım (2016), Neden AdSense? [Çevrimiçi], *Google*, <https://support.google.com/adsense/answer/9712?hl=tr>, [Erişim Tarihi: 25.03.2016].
- Techopedia (2016), Internet Privacy. [Çevrimiçi], *Techopedia*, <http://www.techopedia.com/definition/24954/internet-privacy>, [Erişim Tarihi: 24.03.2016].
- Kara, Mahruze (2013), *Siber Saldırıları – Siber Savaşlar*. Yayımlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.
- Karakaya, Aslı (2014), *Yeni İletişim Ortamları ile Sömürgeciliğin Dönüşümü Gözetim Olgusu ve Bireylerin Farkındalık ve Teslimiyetleri Üzerine Bir Araştırma*. Yayımlanmamış Yüksek Lisans Tezi, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul.
- Karslıoğlu, Figen (2014), *Siber Gözetim: Toplumsal Denetim Aracı Olarak İnternetin Dönüşümü*. Yayımlanmamış Yüksek Lisans Tezi, *İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul.
- Kemp, Simon (2015), *Digital, Social and Mobile Worldwide in 2015*, [Çevrimiçi], *We Are Social*, <http://wearesocial.com/uk/special-reports/digital-social-mobile-worldwide-2015>, [Erişim Tarihi: 08.02.2016].
- Lyon, David (2002), *Editorial Surveillance Studies: Understanding visibility, mobility and the phenetic fix*. [Çevrimiçi], *Surveillance & Society* <http://www.surveillance-and-society.org/articles1/editorial.pdf>, [Erişim Tarihi: 02.02.2016].
- Macaskill, Ewen (2013), *NSA Files Decoded*. [Çevrimiçi], *The Guardian*, <http://theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1>, [Erişim Tarihi: 07.02.2016].
- Öztürk, Serdar (2012), *Mekan ve İktidar*. Ankara: Phoenix Yayınevi.
- Öztürk, Serdar (2013), *Filmlerle Görünürlüğün Dönüşümü: Panoptikon, Süperpanoptikon, Sinoptikon, İletişim Kuramları ve Araştırmaları Dergisi*, 36: 133-151.
- Sucu, İpek (2011), *Gözetim Toplumunun Karşı Ütopya Yüzü: İktidar Güçleri ve Ötekiler*, *Atatürk İletişim Dergisi*, 2: 125-140.
- Oxford Dictionaries (2016), *Surveillance*. [Çevrimiçi], *Oxford Dictionary Surveillance Definition*, <http://www.oxforddictionaries.com/definition/english/surveillance>, [Erişim Tarihi: 01.02.2016].
- Tanılır, Mehmet Niyazi. (2002), *İnternet Suçları ve Bireysel Mahremiyet*. Ankara: Liberte Yayınları.

Türk Dil Kurumu (2014), Güvenlik. *Türkçe Sözlük (genişletilmiş baskı)*. Ankara: TDK.

Tokgöz, Cemile (2011), Bilişim Çağında Toplumsal Denetim Aracı Olarak Gözetim Olgusu ve Yeni İletişim Ortamlarında Bireyin Gözetim Farkındalığı Üzerine Bir Araştırma. Yayımlanmamış Yüksek Lisans Tezi, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul.

Tümürtürkan, Meral (2010), Gündelik Hayatın Gözetimi: Panoptik Toplumu. *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar*, 3 (2): 1-19.

Yalçın, Ersin (2009), Hizmet Referanslı Güvenlik Anlayışında Meşruiyet ve Hesap Verilebilirlik. *Polis Bilimleri Dergisi*, 11 (1): 1-24.

Yüksel, Mehmet (2003), Modernleşme ve Mahremiyet. *Kültür ve İletişim*, 6 (1): 74-103.