MALİK ASLANYÜREK

DİJİTAL MAHREMİYETİN ÇÖKÜŞÜ

ÇEVRİMİÇİ GİZLİLİK VE GÜVENLİK TEHDİTLERİNE YÖNELİK FARKINDALIK

ÇİZGİ KİTABEVİ | e-Kitap

DİJİTAL MAHREMİYETİN ÇÖKÜŞÜ

ÇEVRİMİÇİ GİZLİLİK VE GÜVENLİK TEHDİTLERİNE YÖNELİK FARKINDALIK

Malik ASLANYÜREK

ÇİZGİ KİTABEVİ

Çizgi Kitabevi Yayınları (e-kitap)

Aralık 2024

ISBN: 978-625-396-389-7
Yayıncı Sertifika No: 52493

KÜTÜPHANE BİLGİ KARTI
- Cataloging in Publication Data (CIP) –
ASLANYÜREK, Malik
DİJİTAL MAHREMİYETİN ÇÖKÜŞÜ
ÇEVRİMİÇİ GİZLİLİK VE GÜVENLİK TEHDİTLERİNE YÖNELİK
FARKINDALIK

ÇİZGİ KİTABEVİ

Sahibiata Mah.	Konevi Mh.	Siyavuşpaşa Mh.
M. Muzaffer Cad. No:41/1	Larende Cad. No:20/A	Gül Sk. No: 15 B
Meram/**Konya**	Meram/**Konya**	Bahçelievler/**İstanbul**
(0332) 353 62 65	(0332) 353 62 66	(0212) 514 82 93

www.cizgikitabevi.com
/ cizgikitabevi

İÇİNDEKİLER

ÇİZELGELERİN LİSTESİ

ŞEKİLLERİN LİSTESİ

RESİM LİSTESİ

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

ABD	Amerika Birleşik Devletleri
ANOVA	Analysis of Variance
ARPANET	Advanved Research Projects Agency Network
CIA	Central Intelligence Agency
DDOS	Distributed Denial of Service Attack
DNS	Domain Name System
DPI	Deep Packet Inspection
ENIAC	Electronic Numerical Integrator And Computer
FBI	Federal Bureau of Investigation
IP	International Protocol Number
ISP	Internet Service Provider
MIT	Massachusetts Institute of Technology
NASA	National Aeronautics and Space Administration
NSA	National Security Agency
PSN	Play Station Network
SEO	Search Engine Optimization
SQL	Structured Query Language
TDK	Türk Dil Kurumu
UNIVAC	Universal Automatic Computer
Vb.	Ve Benzeri
WWW	World Wide Web

ÖNSÖZ

Bu kitap çalışması, Gazi Üniversitesi Sosyal Bilimler Enstitüsü Radyo Televizyon ve Sinema Anabilim Dalı yüksek lisans öğrencisi Malik Aslanyürek[1] tarafından hazırlanan, danışmanlığını Doç. Dr. Mehmet Sezai Türk'ün yürüttüğü ve Aralık 2015'te tamamlanan *"İnternet güvenliği ve çevrimiçi gizlilik alanlarında yaşanan sorunlar: İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları üzerine bir araştırma"* başıklı yüksek lisans tezinden türetilmiştir.

[1] Malik Aslanyürek, Kırklareli Üniversitesi Sosyal Bilimler Meslek Yüksekokulu, Görsel-İşitsel Teknikler ve Medya Yapımcılığı Bölümü, Öğr. Dr. malikaslanyurek@gmail.com ORC-ID: 0000-0001-8415-0337

1.GİRİŞ

2000'li yılların başından itibaren önce dünyada, daha sonra ülkemizde geniş bant internet bağlantısı kullanımı yaygınlaşmaya başlamıştır. Bilişim teknolojilerinde peş peşe yaşanan gelişmeler, önce masaüstü ve dizüstü bilgisayar fiyatlarının düşmesine; daha sonraysa taşınabilirliğe imkân sağlayacak işlemcilerin tasarlanmasıyla birlikte, tablet bilgisayarların üretilmesi ve cep telefonlarının akıllı hale gelmesi, internet kullanımını yalnızca ev, okul, iş yeri ve internet kafe gibi yerlerle sınırlı olmaktan çıkarmıştır. GSM operatörlerinin kapsama alanlarının da çok geniş bir alana yayılması ve cep telefonlarında 3G gibi yüksek hızda internet kullanımını sağlayacak teknolojilerin yaygınlaşmasıyla birlikte, insanlar hemen hemen her yerde internete erişmeye başlamışlardır. Yaşanan bu gelişmelerle beraber internet kullanım oranı dünya genelinde çok yüksek bir orana ulaşmıştır.

"We are Social" isimli ajansın 2015 yılına ait internet kullanımına ilişkin yaptığı istatistiki değerlendirmelerde, dünya üzerinde 3 milyar insanın internet kullandığı belirtilmiştir. Ülkemizde ise bu sayı 37 milyonunun üzerinde olup, nüfusa göre oranı %49'dur. Günümüzde insanların mekândan bağımsız bir şekilde sosyalleşmelerine imkân veren sosyal medya siteleri ise bu kullanım oranının büyük bir kısmını teşkil etmektedir. Aktif kullanıcı istatistiklerine göre en popüler ilk 10 sosyal medya platformu arasında zirvede yer alan Facebook'un, 1 milyar 366 milyon aktif kullanıcısı bulunmaktadır. Türkiye genelinde sahte hesaplar dâhil olmak üzere 40 milyon aktif sosyal medya hesabı mevcuttur. Dünya

genelinde internete erişimin %51'i ise mobil cihazlar üzerinden sağlanmaktadır (wearesocial.net).[2]

Bugün internet yeni bir sosyalleşme alanı yaratmanın dışında kullanıcılarına birçok avantaj sunmaktadır. Artık her türlü bankacılık işlemi internet üzerinden yapılmakta, insanlar mağazalara gitmeden alışverişlerini sanal mağazalar üzerinden gerçekleştirmekte, gazete ve dergiler internet üzerinden okunmakta, dizi ve filmler internet üzerinden izlenmekte, hatta çeşitli okulların eğitim faaliyetleri bile internet üzerinden yapılmaktadır. İnternet ve siber uzay, iş, eğitim, sanat ve eğlence vb. alanlarını içine katarak günden güne daha da büyümektedir. Geçmişte faaliyetlerini klasik yöntemlerle sürdüren birçok işletme gerçek mağazalarını kapatıp, sanal mağazalar üzerinden hizmet vermeye başlamaktadır.

İnternet ve siber uzayın bu denli genişlemesi ve kullanıcı sayılarının bu denli yüksek oranlara ulaşması beraberinde inanılmaz büyüklükte bir enformasyon akışını getirmiştir. Gerçekleşen bu enformasyon akışındaki her bilgiye hâkim olmak isteyen devletlerin ve iktidarı elinde bulunduran hükûmetlerin, panoptik bir alan olarak internet ve siber uzay üzerinde son derece sistematik gözetim ve denetim faaliyetleri gerçekleştirmektedir. Hükûmetler bu gözetim faaliyetlerini teröre karşı, halkın refahı için yaptıklarını söyleseler de; internet üzerindeki her sıradan kullanıcıya potansiyel bir terörist gözüyle bakılması bireylerin internet üzerinde özgürce dolaşmasını kısıtlamaktadır. Bazı kuruluşlar ise internet ve siber uzay üzerinde bulunan kişisel verileri toplayıp, pazarlama ve reklam faaliyetleri yapan şirketlere satmaktadırlar. İnternet ortamında bir meta gibi alınıp satılan kişisel bilgilerimiz, internetteki pazarın kendini yeniden üretmesini

[2] "We Are Social" isimli ajans her yıl düzenli olarak internet kullanım istatistiklerini detaylı bir şekilde internet sitesi üzerinden yayınlamakta ve ülkelere göre çok detaylı kullanım oranları sunmaktadır.

sağlamakta ve potansiyel bir tüketici olan internet kullanıcılarına kendi mahrem bilgileri ve davranışları kullanılarak pazarlama faaliyetleri yürütülmektedir. Diğer yandan tam olarak kime hizmet ettikleri bilinemeyen ve "Hacker" (kırıcı) olarak bilinen bilgisayar korsanlarının internet üzerindeki sahtecilik ve dolandırıcılık gibi kötü amaçlı aktiviteleri internet güvenliğimizi ve çevrimiçi gizliliğimizi tehdit etmektedir.

Son yıllarda ABD'de özellikle eski CIA (Merkezi İstihbarat Teşkilatı) ve NSA (Ulusal Güvenlik Dairesi) çalışanı Edward Snowden'in itirafları ve açıklamaları ile internet üzerinde yaşanılan güvenlik ve çevrimiçi gizlilik konusundaki bazı skandallar yazılı ve görsel medyada geniş bir yer edinmiştir. Dünya genelinde ve ülkemizde gerçekleşen bu skandallar bize çevrimiçi ortamda yer alan kişisel bilgilerimizin hiç de güvenli bir şekilde korunamadığını; bu bilgilere devlet, pazarlama şirketleri ve bilgisayar korsanlarının çeşitli yöntemler kullanarak erişebildiği gerçeğini göstermiştir. Bu bağlamda internet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik üzerine olan kanaatlerinin ve farkındalıklarının ölçülmesinin gerektiğini düşündük ve çalışmamızı bu temel üzerine kurguladık.

Çalışmamızın "Temel Kavramlar" bölümünde, çalışmamızla alakalı olan "Güvenlik", "Gizlilik", "Siber ve Siber Uzay", "Çevrimiçi Gizlilik", "Kişisel Bilgi" ve "Bilgi Güvenliği" gibi temel kavramları tanımlanmış; ayrıca "Bilgisayar" ve "İnternet"in ortaya çıkışı ve gelişimi ele alınmıştır.

Sonraki bölüm olan "İnternet Güvenliği ve Çevrimiçi Gizliliği İhlalleri Gerçekleştiren Unsurlar" başlıklı bölümde devlet, pazarlama şirketleri ve bilgisayar korsanlarının internet güvenliği ve çevrimiçi gizliliğimizi nasıl ihlal ettikleri teknoloji basınından alınan haberler ve makaleler ışığında detaylıca işlenmiştir. Devlet ve hükûmetlerin internet üzerinde ne türde gözetim ve denetim faaliyetleri gerçekleştirdikleri,

hangi yöntemleri ve teknolojileri kullandıkları irdelenmiştir. Bu bölümde geçmişten günümüze gözetim pratiklerinin tarih içindeki dönüşümünden bahsedilmiştir. Gözetime sosyal teorideki ünlü kuramcıların kuramları ve kavramlarıyla yaklaşılmıştır. Pazarlama şirketlerinin kişisel verilerimizi nasıl topladıkları ve bu verilerden ne şekilde yararlandıkları açıklanmış, toplanan veriler sayesinde gerçekleştirilen çevrimiçi davranışsal reklamcılık faaliyetlerine değinilmiştir. Diğer bölümde ise internet güvenliği ve çevrimiçi gizlilikle ilgili bir diğer tehdit olan bilgisayar korsanlarının tarih sahnesinde ortaya çıkışı ve gelişimi detaylıca ele alınmıştır. Ayrıca bu bölümde bilgisayar korsanlarının bize karşı kullandıkları saldırı tekniklerine ve bu saldırılarda izledikleri aşamalara da geniş olarak değinilmiştir. Bu bölümün son kısmında ise internet güvenliği ve çevrimiçi gizliliğimizi korumak amacıyla ne yapacağımıza dair öneriler bulunmaktadır.

Çalışmanın son kısmında ise internet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik hakkındaki kanaatlerini ve farkındalıklarını inceleyen bir anket çalışması gerçekleştirilmiştir. Çalışmada internet ve sosyal medya sitelerinin hangi amaçla ve hangi sıklıkla kullanıldığı, çevrimiçi kişisel bilgilerin güvenlik amaçlı kullanımında katılımcıların tutumları, kişisel bilgilerin toplanması karşısında katılımcıların farkındalık düzeyleri ile internet kullanımından vazgeçme eğilimleri ölçümlenmiş ve bu yönergelerin sosyo-demografik değişkenlere göre farklılaşma düzeyi araştırılmıştır.

Problem Durumu

Son yıllarda yükselen kullanıcı şikâyetleri ve özellikle yazılı/görsel basında geniş yer bulan bu konuyla ilgili haberler, internet güvenliği ve çevrimiçi gizlilik konusundaki çalışmaların artmasını sağlamıştır. Yurt dışında bu konularla ilgili birçok anket çalışması yürütülmüştür. Ülkemizde internete

güvenliği ve çevrimiçi gizlilikle ilgili yürütülen çalışmalar ise genellikle interneti Foucault'un kullandığı Panoptikon metaforuyla "panoptik bir alan" olarak görmüş ve gözetim odaklı çalışmalar gerçekleştirilmiştir. Biz ise bu çalışmayı yalnızca "gözetim" ile sınırlamayıp, daha geniş bir yaklaşım türü benimseyerek özel şirketlerin kişisel veriler üzerindeki pazarlama faaliyetleri ve bilgisayar korsanlarının kötü amaçlı aktivitelerini de dâhil ederek internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlallere daha geniş bir perspektiften bakmayı tercih ettik.

Yurt dışında yapılan çalışmalarda genellikle bazı akademisyenler konuya spesifik bir şekilde yaklaşmış ve internet güvenliği ile çevrimiçi gizliliği ihlal eden unsurlardan yalnızca biri üzerine odaklanıp, çalışmalarını bu şekilde yürütmüşlerdir.

Ülkemizde yapılan çalışmalar ise genellikle yalnızca "gözetim" konusu üzerine odaklanmıştır. Yaptığımız literatür taramasında Marmara Üniversitesi Gazetecilik Anabilim Dalı Bilişim Bilim Dalı öğrencisi olan Cemile Tokgöz'ün 2011 yılında "Bilişim çağında toplumsal denetim aracı olarak gözetim olgusu ve yeni iletişim ortamlarında bireyin gözetim farkındalığı üzerine bir araştırma" başlığı altında bir yüksek lisans tezi çalışması bağlamında 441 katılımcıya bir anket çalışması uyguladığı tespit edilmiştir. Bu çalışma tam anlamıyla "gözetim" odaklı bir çalışma olup internet güvenliği ve çevrimiçi gizlilik ihlallerini oluşturan "devlet, pazarlama şirketleri ve bilgisayar korsanları" üçlüsünden yalnızca "devlet" başlığı üzerine gerçekleştirilmiş bir çalışmadır.

2014 yılında yine Marmara Üniversitesi Gazetecilik Anabilim Dalı Bilişim Bilim Dalında yüksek lisans öğrencisi olan Aslı Karakaya "Yeni iletişim ortamları ile sömürgeciliğin dönüşümü, gözetim olgusu ve bireylerin farkındalık ve teslimiyetleri üzerine bir araştırma" başlığı altında bir yüksek lisans tezi çalışması bağlamında 416 katılımcıya bir anket çalışması

uygulamıştır. Bu çalışma da "gözetim" odaklı olup yine "devlet" unsuru ile ilgilenmiş ve internetin devletler tarafından kullanılan "yeni bir sömürge aracı" olduğu tezini savunmuştur.

İki çalışma da incelendiğinde yalnızca hükûmetlerin gerçekleştirdiği "gözetim pratikleri" üzerine durulmuş; iki çalışma mahremiyet odaklı olsa da internet güvenliği ve çevrimiçi gizliliği ihlal eden diğer unsurlar olan "pazarlama şirketleri" ve "bilgisayar korsanları"ndan hiç söz edilmemiştir.

Özellikle Aslı Karakaya (2014)'ün gerçekleştirdiği çalışmada çıkan sonuçlar ise önemlidir. Aslı Karakaya'nın yaptığı anket çalışmasına göre, katılımcıların yarısı internet ve sosyal paylaşım ağlarında gözetlendiklerini bildikleri halde bu ortamlarda var olmaya devam edeceklerini belirtmişlerdir. Katılımcıların %27'si ise sosyal ağlarda varlığını sürdürüp sürdürmeme konusunda kararsız kalmıştır. Bu bağlamda, bireylerin büyük bir kısmı maruz bırakıldıkları gözetim karşısında sosyal paylaşım ağlarından genellikle vazgeçmemekte, çok küçük bir kesim böyle bir durumda söz konusu ağların kullanımını bırakacağını ifade etmiştir. Çoğunluk ise gözetim karşısında farkındalık sahibi olarak bilinçli bir şekilde teslimiyet göstermektedir. Çalışmadan çıkan bir başka önemli sonuç ise; bireyler için sosyal ağlarda var olmanın gözetim unsurundan daha önemli olduğu sonucudur. Buna göre, bireyler kendilerine ait bilgilerin depolandığının farkında olmakta, bilgisayarlarında casus yazılım barındırma ihtimalini yüksek görmekte, mahremiyetlerinin ihlal edildiğini bilmekte; fakat bunlar karşısında internet ve sosyal paylaşım ağları kullanımından vazgeçmemektedir. Bu tercihle bireyler yine bilinçli bir teslimiyet davranışı göstermektedir.

Diğer çalışmalar incelendiğinde 2009 yılında Anadolu Üniversitesi İletişim Anabilim Dalı öğrencisi olan Ufuk Eriş'in "bilgisayar korsanları" üzerine gerçekleştirdiği

"Türkiye'de kırıcı (hacker) kültürü" isimli bir doktora tezi çalışmasına rastlanılmıştır. Bu çalışma ülkemizde bilgisayar korsanlarıyla ilgili yapılmış detaylı ve içerik açısından önemli bir çalışma olmakla birlikte, tez çerçevesinde yürütülen araştırma sıradan internet kullanıcıları yerine ülkemizdeki önemli hacker sitelerine üye olan 258 üyeye yönelik yürütülmüştür. Bu bağlamda, bu çalışmanın konusu bizim çalışmamıza benzemesine rağmen, odak noktasının farklı olmasından dolayı gerçekleştirilen çalışma, bizim çalışmamızla kısmi olarak paralellik göstermektedir.

Yaptığımız kapsamlı literatür taramasında internet güvenliği ve çevrimiçi gizlilik üzerine farklı alanlarda gerçekleştirilmiş birkaç çalışmaya rastlasak da genellikle bu çalışmalar ülkelerin birbirlerine karşı yürüttükleri "Siber Savaş"lar üzerine odaklanmıştır. Biz ise ülkelerin birbiriyle gerçekleştirdiği mücadelelerden çok, bu mücadelelerin sıradan internet kullanıcıları üzerinde yarattığı etkiye odaklandık. Kısacası bizim çalışmamız, ülkelerin birbirleri üzerinde gerçekleştirdikleri gözetim faaliyetlerinin ve bu alandaki yarışın sıradan internet kullanıcılarının internet güvenliğini ve çevrimiçi gizliliğini, bu anlamda mahremiyetlerini nasıl ihlal ettiğini odak noktası olarak almıştır.

Yukarıdaki bilgiler ışığında ülkemizde henüz internet güvenliği ve çevrimiçi gizlilik alanında "devlet", "pazarlama şirketleri" ve "bilgisayar korsanları" tarafından yapılan ihlalleri birleştirmiş bir çalışma bulunmamaktadır. Hatta "pazarlama şirketleri"nin gerçekleştirdiği ihlaller konusunda hem dünyada hem de ülkemizde yapılmış çalışmalar çok sınırlıdır. 1-2 akademik yazıyı geçmeyen bu çalışmaların sayısının, internet üzerindeki pazarlama ve reklamcılık faaliyetlerinin günden güne artmasına paralel olarak yükseleceği tahmin edilmektedir. Çalışmamızın ülkemiz açısından özellikle "pazarlama şirketleri" ve "bilgisayar korsanları"nın gerçekleştirdiği mahremiyet ihlalleriyle ilgili kısıtlı literatüre katkı

yapması beklenmektedir. Aynı zamanda çalışmamızın mahremiyet ihlallerini gerçekleştiren bu üç unsuru, yani "devlet", "özel sektör" ve "bilgisayar korsanları"nı tek çatıda toplaması açısından literatüre yeni bir soluk getireceğini düşünmekteyiz.

Araştırmanın Amacı

Gelişen bilgisayar, internet ve akıllı telefon teknolojilerine paralel olarak internet kullanım oranları günden güne artarken; "devlet", "pazarlama şirketleri" ve "bilgisayar korsanları"nın internet üzerinde gerçekleştirdiği mahremiyet ihlalleri internetin ne kadar güvenli bir ortam olduğu gerçeğini sorgulamamıza sebep olmuştur. Bu bağlamda çalışmamız internet güvenliği ve çevrimiçi gizlilik ihlallerini gerçekleştiren bu üç unsuru aynı çatıda birleştirmesinden dolayı literatüre önemli bir katkı sağlayacaktır. Ayıca gerçekleştireceğimiz anket çalışması internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilikle kanaatlerini ve farkındalıklarını ölçmesi açısından da ayrı bir önem taşımaktadır.

Genel amaç, Türkiye'deki internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili kanaatlerini ve farkındalıklarını ortaya koymaktır. Özel amaç ise; örneklem dâhilinde seçilen Türkiye'de en popüler beş sosyal medya sitesinde (Facebook, Twitter, Google Plus, Pinterest ve Foursquare) aktif internet ve sosyal medya kullanıcılarının internet güvenliği ile çevrimiçi gizlilik alanındaki ihlallerle ilgili kanaatlerini ve farkındalıklarını ortaya koymaktır.

Alt amaçlar;

1. Katılımcıların demografik özellikleri açısından internet güvenliği ve çevrimiçi gizlilik ihlalleri ile ilgili farkındalıkları düzeyleri arasındaki farklılıklar.

2. İnternet ve sosyal medya sitelerinin demografik özelliklere göre kullanım amacı ve sıklıkları.

3. İnternet güvenliği ve çevrimiçi gizlilik alanındaki ihlallerin güvenlik hedefli gerçekleştirilmesi karşısında katılımcıların tutumları.

4. İnternet güvenliği ve çevrimiçi gizlilik alanında yapılan ihlallerine karşı katılımcıların özgürlük hassasiyetleri.

5. İnternet ve sosyal medya sitelerinin katılımcılar tarafından ne ölçüde güvenilir bulundukları.

6. Katılımcıların internet ve sosyal medya sitelerinin internet güvenliği ve çevrimiçi gizlilik alanlarında ihlaller yapıp yapmadıkları hakkındaki düşünceleri ve

7. İnternet güvenliği ve çevrimiçi güvenlik alanlarında meydana gelen ihlaller karşısında katılımcıların interneti kullanma konusunda vazgeçme eğilimlerini ölçmek amaçlanmıştır.

Yukarıdaki yönergeleri, yürütülen anket çalışması çerçevesinde ölçmek çalışmamızın genel amacını ortaya koymak açısından önemlidir.

Yukarıda verilen amaçlar doğrultusunda çalışmamızın genel araştırma sorusu şu şekilde belirlenmiştir: İnternet ve sosyal medya kullanıcılarının sosyo-demografik özellikleri ile çevrimiçi gizlilik ve internet güvenliği alanında yaşanan sorunlara ilişkin kanaatleri arasında anlamlı bir fark vardır. Bu bağlamda araştırmamızın alt araştırma soruları şu şekilde oluşturulmuştur:

1. Katılımcıların cinsiyetleri ile interneti kullanma sıklıkları arasında anlamlı bir fark var mıdır?

2. Katılımcılarım 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?

Araştırmanın Önemi

2000 yılından itibaren hızlı gelişmeye başlayan bilgisayar, internet ve cep telefonu teknolojilerine paralel olarak günümüzde dünyada inanılmaz bir internet kullanım oranına erişilmiştir. Çalışmamızın giriş bölümünde belirttiğimiz üzere bugün dünyada 3 milyardan fazla internet kullanıcısı ve 1,5 milyar civarında aktif sosyal medya hesabı bulunmaktadır. 3G/4G gibi mobil teknolojileri sayesinde bugün işte, okulda, yolda, kafede, hatta deniz kenarında kısacası her yerde internete yüksek hızlarda bağlanabilmekteyiz. Bu denli yüksek kullanım oranlarının sonucunda internet üzerinde inanılmaz bir enformasyon akışı olmakta ve bu enformasyon akışına bazı unsurlar sahip olmak istemektedir.

Günümüzde bu enformasyona sahip olmak isteyen unsurlar sırasıyla "devlet", "pazarlama şirketleri" ve "bilgisayar korsanları"dır. Devletler ve iktidarları elinde bulunduran hükûmetler interneti bir toplumsal denetim mekanizması olarak kullanmakta ve gözetim yoluyla kişisel bilgisayarlarımıza ve cep telefonlarımıza sızılmaktadır. Özel kuruluşlar ise kişisel verilerimizi pazarlama amaçlı olarak toplamakta ve çevrimiçi davranışsal reklam faaliyetleri gerçekleştiren reklam

şirketlerine satmaktadırlar. Öte yandan tam olarak kime ve neye hizmet ettikleri bilinmeyen bilgisayar korsanları ise internet üzerinde sahtecilik ve dolandırıcılık gibi çeşitli kötü amaçlı faaliyetler yapmakta ve onlar da bilgisayarlarımıza ve cep telefonlarımıza sızmaktadırlar. Bilgisayar korsanlarının zarara sebep olan kötü eylemleri bazen yalnızca eğlence amaçlı bile gerçekleştirilmektedir. Bu bağlamda bu üç ana unsur (devlet, pazarlama şirketleri ve bilgisayar korsanları) ayrı olarak internet güvenliğini ve çevrimiçi gizliliğimiz ihlal etmekte; internet ortamındaki mahremiyetimize ve özgürlüğümüze darbe vurulmaktadır.

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.

Ayıca 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.

Çıkan sonuçlar bağlamında yapılacak öneriler, internet ve sosyal medya kullanıcılarının internet ve siber uzaydaki güvenliklerini/gizliliklerini korumak adına bir rehber niteliği de taşıyacaktır.

Varsayımlar

Çalışmamız kapsamında seçtiğimiz örneklem grubunun, araştırma evrenini yeterince temsil ettiği ve örneklem üzerinden evrene genelleme yapılabileceği varsayılmaktadır.

Sınırlılıklar

Araştırma, yürütülecek olan anket çalışmasında katılımcı olarak yer alacak internet ve sosyal medya sitelerindeki aktif kullanıcılarla sınırlandırılmıştır. "We are Social" isimli ajansın yaptığı istatistiksel araştırmaya göre; ülkemizde 40 milyon sosyal medya hesabı bulunmaktadır. Bu sosyal medya hesapları araştırmamızın evrenini oluşturacaktır. 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 α= 0,05 kabul edilerek 384 olarak hesaplanmıştır. Bu sebeple 384'ün üzerinde katılımcıya anket uygulanacaktır. 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 uygulanacaktır. Anket, bu sosyal medya platformları üzerinden katılımcılara gönderilecek ve katılımcılar da anket bağlantısını diğer kişilere gönderebileceklerdir. Bu bağlamda araştırmamızda "Kartopu Örneklem Sistemi" kullanılacaktır.

Çalışmamızın İnternet 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.

2. TEMEL KAVRAMLAR VE TARİHÇE

Bu bölümde çalışmamızda kullanılacak olan temel kavramlar, gerçekleştirilen literatür taraması sonucunda elde edilen veriler ışığında tanımlanacak ve ele alınacaktır

2.1. Güvenlik Kavramı

Güvenliğin dünya üzerinde uzlaşıya 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.

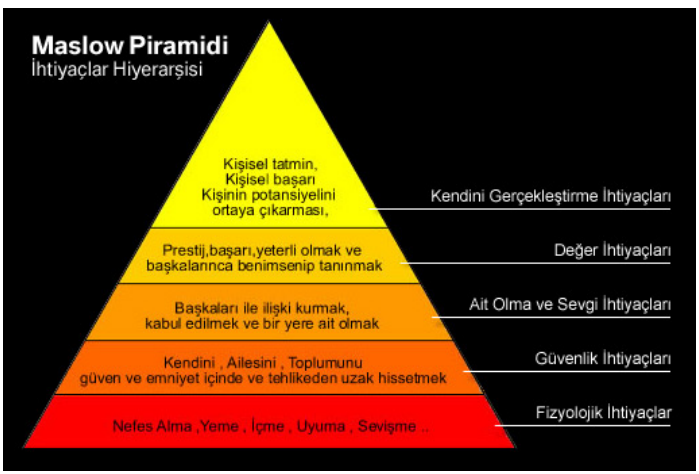
Türk Dil Kurumu güncel sözlüğüne göre "güvenlik" sözcüğünün anlamı şu şekildedir: "Toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet" (tdk.gov.tr).

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).

Hümanisttik Felsefenin kurulmasında büyük katkıları olan ve Psikoloji Bilimiyle ilgili önemli eserler veren Abraham Maslow, insanın kendini gerçekleştirebilmesi için motivasyona (güdülenme) sahip olması gerektiğini söyler. Motivasyonun sağlanması ancak insanın belirli bir hiyerarşiye göre kategorilere ayrılmış ihtiyaçlarını gidermesiyle mümkündür. Bunu daha iyi ortaya koyabilmek için Maslow, İhtiyaçlar Hiyerarşisi Teorisi'ni geliştirmiştir. Bu teoriye göre insanın sınırsız ihtiyaçları vardır ve bu ihtiyaçların biri giderildiğinde yeni bir ihtiyaç ortaya çıkar. Maslow teorisinde bu ihtiyaçları belirli bir hiyerarşiye göre gruplandırmıştır. Bu ihtiyaçlar beş basamaktan oluşan "İhtiyaçlar Hiyerarşisi Piramidi" aracılığıyla gösterilir:



Şekil 2.1. Maslow'un İhtiyaçlar Hiyerarşisi Piramidi

Buna göre en alttan başlayarak ilk basamakta "Fizyolojik İhtiyaçlar" yer alır. Fizyolojik İhtiyaçlar insanın yaşamını devam ettirebilmesi için gidermesi gereken nefes, besin, su, cinsellik, uyku, denge, boşaltım gibi ihtiyaçlar yer alır. İkinci basamakta "Güvenlik İhtiyaçları" vardır. Bu ihtiyaçlar vücut, iş, kaynak, etik, aile, sağlık ve mülkiyet güvenliğidir. Piramidin üçüncü basamağında arkadaşlık, aile, cinsel yakınlık gibi "Ait olma, sevgi, sevecenlik" ihtiyaçları yer alır. Dördüncü basamakta ise statü, başarı, itibar, kendine saygı, diğerlerinin saygısı, başkalarına saygı gibi "Değer verilme/Saygınlık İhtiyaçları" yer alır. Piramidin en son basamağında ise erdem, yaratıcılık, doğallık, problem çözme, önyargısız olma, gerçeklerin kabulü gibi "Kendini Gerçekleştirme İhtiyaçları" yer alır. (Maslow, 1943)

Maslow oluşturduğu İhtiyaç Hiyerarşisinin ikinci basamağına "Güvenlik İhtiyacı"nı koyar. Maslow bu ihtiyacı, fizyolojik ihtiyaçlardan sonra gelen en önemli ihtiyaç olarak görmüştür. Güvenlik ihtiyacı, korunma, barınma, korku ve kaygıdan uzak durma ve bunun içinde kural ve yasalara olan gereksinimlerden meydana gelmektedir. İnsan tehlike ve yoksunluklara karşı savunma gereksinimi içindedir (Maslow, 1943).

İnsanın kendisinin (vücut ve sağlık) ve sahip olduğu şeylerin (sağlık, aile, iş, ahlak, mülk) güvende olması gerekir. Kişinin kendisini fiziksel ve psikolojik açıdan güvende hissetmesi üst ihtiyaçları duymasına zemin hazırlayacaktır. Güvenliğin tesis edilmediği durumlarda ise insanın kendisini gerçekleştirmesine bir sekte vurulacak ve bu da insanın kendisini gerçekleştirme yolundaki güdülenmesine zarar verecektir.

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 nitelemesini getirmesi

bakımından, Maslow'un ihtiyaçlar piramidi, şüphesiz güvenlik ihtiyacının insan toplulukları için taşıdığı önemi vurgulayan en gerçekçi bilimsel tespitlerden birisidir (Yalçın, 2009).

İnsanoğlu var olduğu günden bu yana güvenlik ihtiyacını gidermek adına yöntemler geliştirmektedir. İlk insanların mağara kovuklarında yaşaması bunun ilk örneğidir. Bu, henüz devlet ve özel mülkiyet kavramlarının gelişmediği dönemlerde bile insanoğlunun güvenlik ihtiyacına ne kadar önem verdiğinin en somut örneğidir. Özel mülkiyet ve devlet kurumunun gelişmesi ilerleyen yıllarda güvenlik ihtiyacı kavramının anlamını değiştirmiştir. Güvenlik ihtiyacı bireysellikten çıkıp, evrenselleşmiştir. Kişi güvenliğini ve mülkiyeti korumak için kanunlar yapılmış; toplumu korumak içinse ordular kurulmuştur. Endüstriyelleşmeyle birlikteyse "sosyal güvenlik" kavramı ortaya çıkmıştır.

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 kullanımın 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.

2.2. Gizlilik (Mahremiyet) Kavramı

İnsanoğlunun var olduğu ilk günden beri ortaya çıktığına inanılsa da tıpkı "güvenlik" kavramında olduğu gibi

"mahremiyet" kavramının da üzerinde uzlaşılmış 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 aktarılabileceğini 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).

Mahremiyetin alanı kültürden kültüre ve aynı toplum içerisinde zamandan zamana değişiklik gösterir. Mahremiyet kavramının birçok insan için aynı anlama gelmemesi ve özel yaşam sınırları içerisinde kalan konuların kişiden kişiye zamandan zamana ve kültürden kültüre değişiklik göstermesi, kavramın tanımlanmasını ve sınırlarının belirlenmesini güçleştirmektedir. Kavramsal olarak 'mahrem' kelimesi samimi, içli dışlı, herkes tarafından bilinmemesi gereken, söylenmeyen, gizli şey anlamına gelmektedir (Göle, 2001: 128).

Robert Gifford'a göre ise, "mahremiyet" ya da "özel yaşam alanı"nın 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 insan özgürlüğünün bir parçası olduğundan, mahremiyetin ihlali aynı zamanda özgürlüğün ihlalidir. Mahremiyetin korunmadığı yerde özgürlük yaşanamaz. Eğer güvenli bilgi ve iletişim ortamına sahip olunmazsa, özgür bir biçimde haberleşme mümkün olmaz ve özgür ifade hakkı korunamaz. Kontrol edilme duygusu birey üzerinde engelleyici bir etkiye sahip olabilir (Tanılır, 2002: 45).

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).

2.3 Bilgisayarın Ortaya Çıkması ve Tarihi Gelişimi

İkinci Dünya Savaşı sırasında savaş gemilerinde, tanklarda ve avcı uçaklarında kullanılmak üzere büyük miktarda top üretilmişti. Bu topların gerektiği gibi kullanılabilmesi için topçuların topu doğru yöne nişanlamaları ve top namlusunu doğru açıda kaldırmaları, yalnızca hedefin konumunu değil, ayrıca havanın sıcaklığını ve rüzgârın karakterini de hesaba

katmaları gerekiyordu. Tüm bunların hesaplanabilmesi çok zordu. ABD Ordu Donatım Departmanı Balistik Araştırma Laboratuvarı, matematik notları iyi olan yüksekokul mezunu yüzlerce kadını, binlerce diferansiyel denklemini çözüp ateş cetvelleri hazırlamaları amacıyla görevlendiriyordu. Bu kadınlara en gelişmiş elektromekanik hesap makineleri verilmiş olsa bile her cetvelin hesaplanması yaklaşık üç ayı buluyordu. 1942'de Pennsylvania Üniversitesi Moore Mühendislik Okulu'ndan yetenekli bir mühendis olan John Mauchly, Ordu Donatım Departmanı'na gönderdiği bir notta, mermi uçuş yolu denklemlerini saatler yerine birkaç saniyede çözebilecek yüksek hızlı vakum tüpleriyle çalışan elektronik bir hesap makinesi inşa edebileceğini belirtmişti. 1943'te Maucly ve arkadaşlarıyla bu amaçla bir sözleşme yapıldı. Böylece İlk bilgisayar olan "ENIAC" (Electronic Numerical Integrator And Computer - Elektronik Sayısal Entegreli Hesaplayıcı) icat edilmiş olacaktı.

Ne yazık ki bu makine savaşın bitmesinden birkaç ay sonrasına 1945-46 kışına kadar tam anlamıyla hazır hale getirilememişti. Bu devasa boyuttaki bilgisayar 167 m² yer kaplıyordu, 30 ton ağırlığındaydı ve saate 150 kilowatt elektrik tüketiyordu. ABD bu makinenin yapımı için 450.000 dolar harcamıştı. Bu hantal ve ağır makine çalışıyordu; fakat o zamanlar yalnızca hızlı hesap işlemleri yapmaya yarıyordu. Bir saniye içinde on basamaklı 333 adet sayıyı çarpabiliyor ve daha önceden çözümü saatler alan bir uçuş yolu denklemini yirmi saniyede çözebiliyordu. (Crowley ve Heyer, 2010: 461, 462)

Savaş sona ermişti; ama soğuk savaş başlıyordu. 1945-46 kışında ENIAC'ın gerçekten işe yarayıp yaramayacağından endişe eden ABD yetkilileri, makinenin bir hidrojen bombasının yapılıp yapılmayacağını hesaplayacak şekilde yeniden programlanmasını talep ettiler. Fizikçilerin yıllarca çalışmasını gerektirecek bu hesaplamalar birkaç hafta içinde

tamamlanınca, soğuk savaşın karmaşık, yüksek hızda hesaplamalara yönelik askeri arzuları arttıracağı ortaya çıktı. Böylece ABD soğuk savaşın henüz başladığı dönemlerde rakibi Sovyetler Birliği'ne karşı teknolojik anlamda önemli bir üstünlük kurmuştu.

İlerleyen yıllarda ömrü kısa süren DEVAC isimli bir bilgisayar daha üretildi. ENIAC'ı üreten Eckert ve Mauchly, ticari olarak bilgisayar üretebilmek üzere bir şirket kurdular. 1951'de seri bir şekilde üretilen ve ticari anlamda satışa ilk sunulan bilgisayar UNIVAC I de onların eseriydi. Bu bilgisayarın giriş-çıkış birimleri manyetik bant idi ve bir yazıcıya sahipti (bilgiustam.com). UNIVAC I'in ilk müşterisi ABD'de faaliyet gösteren bir nüfus bürosu oldu.

"IBM" (International Business Machines; Uluslararası İş Makineleri) isimli firma bilgisayar tarihinde üst üste devrimler gerçekleştirerek, deyim yerindeyse bilgisayar tarihinin kaderini değiştirmiştir. IBM bir ekrana ve depolama alanına sahip olabilen ilk kişisel bilgisayarı 1952'de üretmiştir. IBM-701 isimli model saniyede 2200 çarpım işlemi yapabilmekteydi. Bu devrimin merkezinde, toplama, çarpma, stoklama ve kıyaslama işlemlerinin elektronik olarak yapılmasını sağlayacak şekilde elektrik sinyallerinin değiştirilmesine imkân tanıyan elektronik tüp vardı (meful.net).

Buraya kadar adı geçen tüm bilgisayarlar çok ağır ve devasa boyutlardaydı. IBM firması 1958'den itibaren bilgisayarda vakum tüpleri yerine diyot ve transistorları kullanmaya başlamıştır. Bununla birlikte daha küçük, hafif ve daha az ısınan bilgisayarlar pazarlanmış, bilgi depolama ortamları olarak disk ve tamburlar kullanılmaya başlanmıştır (bilisimtarihi.com).

İlerleyen yıllarda bilgisayar üreten birçok firma ortaya çıktı. Bilgisayarlar 60'lı yıllarda daha önce görülmemiş bir biçimde seri üretiliyordu; fakat hala evlere girebilecek kadar küçülmemişlerdi ve maliyetleri azalmamıştı. 1970'lere

varıldığında tümleşik devre uygulayımı ve Intel 4004 gibi mikroişlemcilerin geliştirilmesi sayesinde bir kez daha büyük bir başarım ve güvenilirlik artışının yanı sıra, maliyet düşüşü de yaşandı (tr.wikipedia.org). Böylece gitgide sayıları artan bilgisayar üreticisi firmalar birbirleriyle yarışıyor, en nihayetinde ilk kişisel bilgisayarları üreterek, bilgisayarların evlerimize girmesine zemin hazırlıyorlardı.

1975 yılında ilk kişisel bilgisayar "MITS Altair 8800" üretilmişti. Fakat bu bilgisayar satın alındığında yanında klavye ve monitör bile gelmiyordu. 480 dolar gibi nispeten ucuz sayılabilecek bir satış fiyatı olmasına rağmen, bu bilgisayarı satın alanlar, bilgisayarın parçalarını birleştirerek montajını kendileri yapmak zorundaydılar. Bu can sıkıcı bir durumdu. Ayrıca bu bilgisayarın tuhaf bir görüntüsü vardı; üzerinde ışıklar ve düğmeler bulunan tuhaf bir metal kutuya benziyordu (lowendmac.com).

1977 yılında iki rakip firma Apple ve IBM'in yeni modelleri ortaya çıkmıştı. Apple II isimli bilgisayarın 1300 dolarlık bir satış fiyatı vardı; fakat bu bilgisayarın da yanında henüz bir monitör verilmiyordu. IBM'in 5100 isimli bilgisayarı ise ilk portatif bilgisayardı. Üzerinde 5 inç boyutunda bir monitör bulunduruyordu, 25 kg ağırlığa sahipti, günümüzde sıradan bir dizüstü bilgisayardan 10 kat daha ağırdı. İlk portatif bilgisayar denemesi olan bu cihaz 20 bin dolarlık çok yüksek satış fiyatı nedeniyle ticari açıdan pek başarılı olamadı.

Yine 1977 yılında Commodore adlı firmanın ürettiği, aynı zamanda bir monitöre de sahip olan "Commodore PET" adlı, gerçek anlamda ilk kişisel bilgisayar sayılacak cihaz müthiş bir satış başarısı yakaladı. Dünya genelinde 2 milyondan fazla satan bu bilgisayarla birlikte bilgisayarlar hızla evlerde de yerlerini almaya başlamıştır (commodore.ca).

1945'ten itibaren başlayan bilgisayar tarihi donanım anlamındaki gelişimini ilk bilgisayar olan ENIAC'ın gelişiminden itibaren yazılımsal anlamda da hızla sürdürmüştür. 1956

yılında "Fortran" programlama dilinin geliştirilmesiyle birlikte bilgisayarda büyük bir yazılım devrimi olmuştur. İlk bilgisayarlarda kullanılan birinci ve ikinci nesil programlama dillerinin öğrenilmeleri ve uygulanmaları zordu ve hata durumlarını yönetmek sıkıntılıydı. Diğer taraftan belirli bir işlemci/makine için yazılan kod, farklı yapıdaki başka bir makinede çalışmıyor, tamamen yeniden yazılması gerekiyordu. "Fortran"la başlayan üçüncü nesil ve akabinde gelen "COBOL, BASIC, C, C++, Delphi, Java" gibi programlama dilleriyle birlikte, yazılım geliştirme makine bağımlılığından kurtarılmıştır. Yazılan programlar farklı makinelerde de kullanılmaya başlanmıştır.

Üçüncü nesil dillerin programlama anlamında çok ciddi ilerlemeler sağlamasına rağmen, ticaret ve iş yaşamında özel durumlara yönelik hızlı çözümler geliştirebilme ihtiyacı dördüncü nesil programlama dillerinin gelişimine neden olmuştur. Kullanımı çok daha kolay, daha az kod yazarak yönergeler, hazır şablonlar ve sihirbazlar sayesinde belirli ihtiyaçlarda uzmanlaşmış pratik çözümler geliştirmeye yönelik olarak "SQL, Oracle, PostScript, RPG-II, SPSS, Borland Delphi, MATLAB's GUIDE, Windows Forms, Powerbuilder, Progress Dynamics, ColdFusion" gibi programlama dilleri ortaya çıkmıştır. Bu diller rapor üreteci (generator), form üreteci, vaka tasarımı, veri yönetimi, istatiksel analiz, vb. alanlarda uygulamalar geliştirmeye yöneliktir (chip.com.tr).

Programlama dillerinin gelişmesiyle birlikte bilgisayarlarda kullanılmak üzere tasarlanan çeşitli işletim sistemleri (Unix, Amiga, DOS, MS DOS, Windows, Mac OS X) ortaya çıkmıştır. Bu işletim sistemleri günümüzde kullandığımız her türlü bilgisayar, akıllı cep telefonları ve sunucularda kullanılmaktadır (tr.wikipedia.org).

2.4. İnternetin Ortaya Çıkması ve Tarihsel Gelişimi

İkinci Dünya Savaşı'nın sona ermesinin üstünden 12 sene geçmişti ve artık dünyanın iki büyük gücü Amerika Birleşik Devletleri ile Sovyetler Birliği güçlerini soğuk savaş arenası üzerinde teknoloji aracılığıyla yarışmaktaydı. 4 Ekim 1957'de Sovyetler Birliği dünya yörüngesine ilk yapay uyduyu (Sputnik) yerleştirmesi ve ardından 3 Kasım 1957'de bu sefer canlı bir köpekle birlikte Sputnik II'yi uzaya göndermesi, o güne kadar iki kutuplu dünyada yaşanan rekabette lider konumda olduğunu düşünen ABD'nin ilk defa nükleer tehdidi hissetmesine sebep olmuştu. Bunun üzerine ABD Yönetimi Şubat 1958'de ABD'nin rekabet gücünü geliştirmeye katkı yapması amacıyla "Advanced Research Projects Agency (İleri Araştırma Projeleri Kurumu)"i yani kısa adıyla ARPA'yı kurdu. Bu kurumun en önemli amacı Sovyetler Birliği'nin ispatlanmış teknolojik üstünlüğünü alt etmekti (Bıçakçı, 2013: 5).

Amerika'nın en büyük üniversitelerinden biri olan "Massachusetts Institute of Tecnology" (Massachusetts Teknoloji Enstitüsü – MIT)'de görev yapan J.C.R. Licklider "Galaktik Ağ" adında bir kavramı tartışmaya açmıştır. Licklider bu kavramla küresel olarak birbirine bağlanmış bir sistemde herkesin herhangi bir yerden veri ve programlara ulaşabilmesini ifade etmiştir. Licklider daha sonra ARPA'nın başına geçmiştir. MIT'de araştırmacı olarak çalışan Lawrance Roberts ile Thomas Merrill, bilgisayarların ilk kez birbirleri ile 'konuşmasını' ise 1965 yılında gerçekleştirmiştir. 1966 yılı sonunda Roberts ARPA'da çalışmaya başlamış ve "ARPANET" isimli projesi önerisini yapmıştır. ARPANET çerçevesinde ilk bağlantı 1969 yılında dört merkezle yapılmış ve ana bilgisayarlar arası bağlantılar ile internetin ilk şekli ortaya çıkmıştır (armaweb.com.tr).

ARPA tarafından finanse edilen bu projenin ilk amacı; önemli bir bölümünün kesintiye uğraması veya saldırıya maruz kalması durumunda bile faaliyete devam edebilecek bir

ağ yaratmaktır. ARPANET, sorun halinde otomatik olarak ağ trafiğini diğer irtibatlı sistemlere yönlendirerek gerekli bilgiyi kesintisiz bir şekilde aktarmak üzerine tasarlanmıştır (Yılmaz ve Salcan, 2008: 35).

1970'lerdeki yükselişinin öncesinde iki bilgisayar arasındaki iletişim ayrılmış bir devre veya önceden atanmış bir bant genişliği gerektirirdi. Bu doğrudan bağlantı, hiçbir veri iletilmezken bile o kaynakların başka hiç kimse tarafından kullanılmaması anlamına geliyordu. UCLA'dan Stanford'a olan ilk bağlantı 1972'de kırık düğümlü bir bağlantıya dönmüştü. Çok geçmeden dünya genelinden üniversiteler ve araştırma merkezleri bu ilk ağa (ARPANET) katıldılar veya bunun yerine kendi ağlarını yarattılar.

Tek bir ağ üzerinden cihazlar arasında gönderilen paket serileri internetin amaçları yönünden "internet" sayılmaz. İnternet birçok farklı ağı bağlamak anlamına gelir, bu durumda ARPANET'ten başka çeşitli bilgisayar ağları çok geçmeden ortaya çıktı ancak özerk kaldı (Singer ve Friedman, 2015: 34-35).

Ağların farklı teknolojiler kullanması sıkıntı yaratıyordu. Bu farklılıkları çözmek ve verimli iletişimi sağlayabilmek amacıyla çeşitli çözümler arandı. 1973 yılında Stanford'ta profesör olan Vint Cerf ve ARPA'da görevli olan Robert Khan ortak bir iletişim protokolü geliştirdiler. Bu protokole TCP (Transport Control Protocols) adı verilmiştir.1972'de BBN teknik danışmanlık firmasından Ray Tomlinson mesaj okumak, yazmak ve göndermek için temel bir program yarattı. Bu ilk e-postanın denemeleriydi (Singer ve Friedman, 2015: 35-36). Bundan dört sene sonra İngiltere Kraliçesi II. Elizabeth 26 Mart 1976'da Kraliyet Sinyal ve Radar Kurumu'ndan ilk e-postayı atarak, iletişimin yeni bir boyuta taşınmasına şahitlik etti (Bıçakçı, 2013: 7).

E-posta'nın resmi olarak ilk kez atıldığı tarihlerde bile internetten sınırlı sayıda insan faydalanıyordu. Bunun iki

sebebi vardı; henüz bilgisayarlar tam olarak yaygınlaşmamıştı ve ABD'nin internet üzerindeki etkisi devam ettiğinden internet tam anlamıyla evrenselleşememişti.

İlerleyen yıllarda ABD interneti demokratikleştirdi ve özgürleştirdi. Bunda yalnızca ABD'nin değil, internetin gelişmesi sırasında katkıda bulunan diğer ülkelerin de payı vardı. İnternetin yönetimi bağımsız bir vâkıfa devredildi. Bu özgürleştirmeden sonra internet 1977'de farklı firmalardan gelen kişisel bilgisayar modellerinin üretiminin akabinde dünya geneline yayılmaya başladı. 1983 yılında ise ARPANET, askeri ve sivil olmak üzere ikiye bölündü; bununla beraber günümüzdeki internet yapısının temelleri atılmış oldu ve yayılması daha da hızlandı.

1989'da İsviçre'de bulunan CERN (Avrupa Araştırma Merkezi)'nde çalışan bir araştırmacı HyperText Transfer Protokolü (HTTP)'nü ve URL'leri geliştirdi. Böylece bildiğimiz anlamdaki World Wide Web (WWW) ortaya çıktı. Bu buluş başta hiç ilgi görmese de kısa bir süre sonra internetin günümüze taşınan en önemli devrimlerinden biri oldu (cern.ch).

Başlarda ABD Savunma Kuvvetleri'nin bir haberleşme ağı olarak düşünülen ve bu şekilde tasarlanan internet, daha sonra bir araştırma ve eğitim ağına dönüştü. Bugünün dünyasında ise internetin kullanma amacı çok farklı boyutlara ulaşmıştır. Bugün internet, kamu, özel ve ticari iletişim için bir yapı haline gelmiştir ve süratle gelişmektedir (Yılmaz ve Salcan, 2008: 37).

2.5 Siber ve Siber Uzay Kavramları

"Siber" kavramı "sibernetik" kökeninden gelmektedir. İlk olarak 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleyen Sibernetik biliminin kurucusu sayılan Louis Couffignal tarafından kullanılmıştır (tr.wikipedia.org).

"Siber Uzay" kavramı ilk defa 'sibernetik' ve 'uzay' kelimelerinin bir karışımı olarak William Gibson tarafından kısa bir hikâyede 1982 yılında kullanılmıştır. Gibson bu kavramı iki yıl sonra "Neuromancer" isimli romanında "her ulusta, milyarlarca meşru operatör tarafından günlük olarak karşılıklı olarak tecrübe edilen halüsinasyon… İnsanlık sistemindeki her bir bilgisayarın kasasından alınan verilerin grafik gösterimi. Tasavvur edilemez karmaşa. Aklın yetersizliğine uzanan ışık hatları, verilerin küme ve takımyıldızları" olarak ifade etmiştir (Singer ve Friedman, 2015: 28).

"Siber Uzay" Amerikan Savunma bakanlığınca: "İnternet'in bulunduğu, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan, birbirine bağlı bilgi teknolojileri altyapılarının olduğu küresel bir alan" olarak tanımlanmıştır. Diğer bir tanımlama da ise şu şekilde geçmektedir: "insanların bilgisayarlar ve telekomünikasyon sistemleri aracılığıyla herhangi bir coğrafi sınırlamaya maruz kalmadan tamamen birbirine bağlı olma durumudur" (Hildreth). Bir bakıma internete bağlı bilgisayarlar, bilişim sistemi altyapıları, medikal sistemler, elektrik iletim hatları, nükleer santraller, doğalgaz santralleri gibi kritik altyapılar da siber uzayı oluşturan yapı taşlarıdır (siberguvenlik.org.tr).

Singer (2014/2015), "Siber Uzay"ı en basit anlamıyla şu şekilde tanımlamıştır: "İçerisinde bilginin çevrimiçi olarak saklandığı, paylaşıldığı ve iletildiği, bilgisayar ağlarının (ve arkalarındaki kullanıcıların) âlemidir" (Singer ve Friedman, 2015: 29).

Bıçakçı (2013)'ya göre Siber Uzay katmanlardan oluşmaktadır. Bilgisayarlar, akıllı telefonlar, televizyonlar, oyun konsolları, uydu sistemleri ve ağ ortamında bulunan bütün elektronik aletler ile onları oluşturan elektronik parçalar "fiziksel katmanı" oluşturur. "Kodlar Katmanı ve Yazılım" ise "1-0" düzleminde oluşan programlama dilleri ve programları

kapsamaktadır. "İçerik Katmanı" 1 ve 0'ların birleşerek oluşturulan verileri; fotoğraf, video, office dosyaları vb. gibi içerikleri kapsamaktadır. Ayrıca bir de internet ve içeriğinin nasıl kullanılması gerektiğini düzenleyen bir "düzenleyici katman" da mevcuttur. (Bıçakçı, 2013: 11).

2.6. Çevrimiçi Gizlilik (Online Privacy) Kavramı

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.com).

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 (en.wikipedia.org)[3]:

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

[3] İngilizce Wikipedi'de bulunan Internet Privacy (Çevrimiçi Gizlilik) maddesinden çevrilip, çalışmamızla ilgili olan kısımlar derlenip çalışmamıza eklenmiştir. İlgili maddeye http://en.wikipedia.org/wiki/Inter-net_privacy bağlantısından ulaşılabilir.

- 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.

Çevrimiçi Gizlilik konusu, bu konuyla ilgili ortaya çıkan ihlaller ve bu ihlallerle baş etmek için neler yapılabileceği çalışmamızın ilerleyen kısımlarında daha detaylı bir şekilde ele alınacaktır. "Çevrimiçi Gizlilik" kavramı, "Kişisel Bilgi" ve "Bilgi Güvenliği" kavramları ile yan yana geldiğinde anlam kazanmaktadır.

2.7. Kişisel Bilgi

Kişisel bilgi, belirli veya kimliği belirlenebilir olmak kaydıyla, bir kişiye ait bütün verileri ifade eder. Bu veriler, bir kimsenin kimliğine, etnik ve kültürel kökenine, fiziksel özelliklerine, sağlık, öğrenim ve iş durumuna göre olabilmekle birlikte, bir kişinin şahsi ve ailesel hayatına ait olan bilgiler ve diğer kişilerle gerçekleştirdiği iletişim de kişisel bilgi vasfındadır. Bir şahsın ikamet, emniyet, kredi kartı ve banka kayıtları ile şahsi ideoloji ve görüşleri, yaşam tarzı, aynı zamanda alışveriş bilgileriyle alakalı bütün veriler kişisel bilgi kapsamına girer (Aksoy, 2008: 1).

Bu bağlamda kişisel bilgi bir kimseyle ait olan veya olabilecek bütün verileri kapsamaktadır. Bir şahısla alakalı biyolojik, fizyolojik, sosyolojik, psikolojik ve ekonomik tüm bilgiler şahısların kişisel bilgilerini oluşturur.

2.8. Bilgi Güvenliği

Bilgi güvenliği, çevrimiçi ortamlarda verilerin veya bilgilerin saklanması ve taşınması sırasında, bilgilerin bütünlüğünün bozulmadan, yetkisiz erişimlerden korunması amacıyla, güvenli bir bilgi işleme platformu oluşturma çabalarının tümünü ifade eder. Bunun yerine getirilmesi için, uygun güvenlik politikası belirlenmeli ve hayata geçirilmelidir. Bu politikalar, etkinliklerin sorgulanması, erişimlerin takip edilmesi, yapılan değişiklerin kaydedilmesi, silme işlemlerine karşı önlem alınması gibi bazı kullanım senaryolarına indirgenebilir (Canbek, 2006).

Bilgi güvenliği, bilginin zararlardan korunması, farklı teknolojilerin doğru hedeflerle kullanılıp, verilerin istenmeyen kişilerin eline geçmesine mani olmak şeklinde tanımlanabilmektedir.

Haberleşme ve bilgi güvenliğini sağlamanın ilk şartı, haberleşme emniyetinin ihtiyaçlarını ve sisteme yönelik tehditleri belirleyerek bir analiz yapmaktır. Tehdit unsuru, gizlilik dereceli bilgilere, elektronik ve diğer araçlarla erişmeyi, haberleşme akışını kesmeyi, sistem içerisine sahte ve yanlış bilgi sokmayı amaçlar. Bilgi sistemlerinde, gizlilik dereceli bilgiler ve elektronik donanım; yetkisiz kullanma ve bozulmaya karşı çok duyarlı, yerlerine yenilerinin konulması pahalı ve güç olduğundan casusluk ve sabotaj için cazip hedeflerdir (Yılmaz ve Salcan, 2008: 28).

Singer (2014/2015), bilgi güvenliğinin üç amacı olduğunu belirtir. Buna "CIA üçlüsü" adı verilir (Confidentially, Integrity, Availability). "Confidentially" gizlilik demektir; verinin özel muhafazasını ifade eder. Mahremiyet sadece sosyal veya siyasi bir hedef değildir. O bilgiyi korumak son derece önemlidir. Sadece iç sırlar ve hassas kişisel veriler iyi korunmamalıdır, işlemlere dair veriler de şirketler ya da bireyler arasındaki ilişkiler hakkında detayları ortaya çıkarabilir. "Integrity" bütünlük anlamına gelir. Bütünlük sistem içerisindeki

verinin, yetki olmadan uygun olmayan bir şekilde değişiklik yapılmaması ya da değiştirilmemesi demektir. Sadece bir güven meselesi değildir. Sistemin hem kullanılabilir hem de beklendiği şekilde davranacağına dair güven olmalıdır. "Availability" ise kullanılabilirlik anlamına gelir. Burada da yine, kullanılabilirliği bir güvenlik sorunu yapan sadece bozulan sistem değildir, yazılım hataları bilgisayarlarımıza her zaman olur. Eğer birisi kullanılabilirlik eksikliğini suiistimal ederse bu bir güvenlik sorununa dönüşür (Singer ve Friedman, 2015: 57-58).

Günümüzde bilgi güvenliği, verilerin zarar görmesini, istenmeyen kişiler tarafından çalınmasını ve silinmesini önlemek amacıyla çevrimiçi ortamda değişik yöntemlerle sağlanmaktadır. Verilerin bulunduğu bilgisayarlar, sabit diskler ve veri tabanları güvenlik şirketlerinin ürettiği farklı güvenlik sistemleri tarafından korunmaktadır; fakat bu sistemlerin ne kadar doğru ve kararlı çalıştıkları konusunda soru işaretleri vardır. Ayrıca bilgi güvenliği konusunda en zayıf unsurun "insan" olduğu unutulmamalıdır.

3. İNTERNET GÜVENLİĞİ VE ÇEVRİMİÇİ GİZLİLİK İHLÂLLERİ GERÇEKLEŞTİREN UNSURLAR

İnternet güvenliği ve çevrimiçi gizlilik alanında yaşanan ihlalleri gerçekleştiren unsurları üç temel başlık altında toplayabiliriz. Gözetim aracılığı ile iktidarları elinde bulunduran hükûmetlerin "devlet" ayağıyla yaptığı ihlaller bu başlıklardan ilkini oluşturmaktadır. Çevrimiçi kişisel verileri pazarlama amacıyla toplayan ve satan firmaların yaptığı ihlalleri "pazarlama şirketleri" ayağıyla yapılan ihlaller başlığı altında toplayabiliriz. Üçüncü başlıkta tam olarak neye ve kime hizmet ettiklerini bilmediğimiz, kimlikleri hakkında çok az bilgi sahibi olduğumuz "bilgisayar korsanları" yer almaktadır. Çalışmamızın bu bölümünde "devlet", "pazarlama şirketleri" ve "bilgisayar korsanları" tarafından gerçekleştirilen internet güvenliği ile çevrimiçi gizlilik alanındaki ihlalleri başlıklar halinde ele alıp, tüm detaylarıyla inceleyeceğiz.

3.1 Devlet ve Hükûmetler

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 didik didik edilmektedir. İktidarların görüşlerine ya da toplumsal düzeni tehdit ettiğine inanılan bir veriye rastlanıldığında

hemen müdahale edilmektedir. 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.

İnternetin doğuşu aslında ABD'de Pentagon için askeri yazışmaların güvenli bir şekilde yapılmasına olanak sağlayacak yeni bir teknolojinin gerekliğiyle ortaya çıkmıştır. İlerleyen yıllarda gelişen bilişim teknolojileriyle birlikte internet, yalnızca Amerikan ordusunun askeri yazışmaları dışında pek çok amaca hizmet etmeye başlamıştır. Evrenselleşen internet, bilişim teknolojilerinin getirdiği imkânlarla ve bilgisayar satışlarının artmasıyla birlikte çok farklı bir anlam kazanmıştır.

İnternetin Pentagon dışına çıkıp, diğer devlet kurumlarına, bu kurumlardan üniversitelere ve daha sonra tüm dünyaya yayılması büyük bir enformasyon akışının oluşmasını da beraberinde getirmiştir. İnternet, böylece devlete ve iktidara "fayda" dışında potansiyel olarak "zarar" verebilecek bir konuma gelmiştir.

İnternet kullanıcıları arasında her türlü etnik grup, sosyokültürel yapı ve ideolojinin mevcut olması; marjinal görüşlerin de internet içinde kendine bir yer edinmesi, en özgür ve demokratik toplumlarda bile internetin devlet tarafından denetlenmesini ve kontrol edilmesi gerekliliğini getirmiştir. Devlet kendi propagandasını internet üzerinde istediği gibi yapabilirken, aynı durum karşıt görüşler için de geçerlidir. Karşın görüşlü muhalif gruplar da interneti kendi propaganda aracı olarak kullanabilir ya da egemen görüşün ideolojisine internet ortamında karşı çıkabilirler. Bunun sonucunda iktidarlar ve egemen görüş savunucuları kendilerine muhalif

olan seslerin yükselmesini istemeyeceklerdir. İnternet ise bu tür marjinal ve muhalif seslerin yükselmesi için en uygun ortamdır.

İnternet kitle iletişim araçları arasında en hızlı küreselleşen olgudur. Elbette bunda çok hızlı bir enformasyon akışının mevcut olmasının payı büyüktür. Örneğin dünyanın bir ucunda gerçekleşen bir olay anında dünyanın öteki ucundan takip edilebilmektedir. Daha basit bir örnek verecek olursak; dünyanın öteki ucunda ikamet etmekte olan arkadaşımıza bir e-posta aracılığı ile 2-3 saniyede ulaşabilmekteyiz. Bu e-postanın içerisinde ne tür bir bilgi olduğu sıradan bir vatandaşı ilgilendirmezken; devleti son derece ilgilendirebilir. Söz konusu e-postanın içinde sıradan bir arkadaş konuşması da bulunabilir; insanlığı tehdit edecek yeni bir bomba yapımını anlatan bir şema veya iktidarı devirmeye yönelik bir askeri darbe planı da. Bu bağlamda siyasi iktidarı elinde bulunduran hükûmetler, internet ve siber uzay alanında dolaşımda olan her türlü bilgiye ulaşma ve istihbaratı elde etme amacını taşırlar. Bu sayede hükûmetler varlıklarına ters olabilecek herhangi bir bilgiyi tespit ederek, duruma anında müdahale etme şansına sahip olabilirler.

Süperpanoptik bir alan olarak görev yapan internet ve siber uzay iktidarların gözetim pratiklerine hizmet eden önemli bir toplumsal denetim aracı durumundadır. Ülkelerin içinde mevcut olan internet ağları ve verilerin iletebilmesini sağlayan kabloların döşenmesi gibi rutin işler bile devletin izniyle yapılmaktadır. Böylece internet âlemi, diğer adıyla siber âlem, kanunlarla birleştiğinde devletin üzerinde her türlü söz söyleyebileceği, her türlü kararı alabileceği bir ortam halini almıştır. En kısa ifadeyle, devlet her türlü kitle iletişim ortamında uyguladığı denetim ve gözlemi internet üzerinde de uygulamaya başlamış ve gözetim siberleşmiştir. Dışarıda güvenlik kameraları ve mobeseler aracılığıyla yapılan gözetim,

internet âleminde kendini izleme yapan çeşitli programlara ve denetleme sistemlerine bırakmıştır.

Gözetim henüz internet ortaya çıkmadığı zamanlarda da söz konusuydu; fakat bu kavram her yeni bir iletişim aracı icat edildiğinde farklı evrimler geçirmiştir. Gözetimin siberleşmesini ve süperpanoptik bir alan olarak interneti ele almadan önce, bir toplumsal denetim unsuru olan gözetim kavramını ve bu kavramın tarih içindeki dönüşümünü ele almak gerekmektedir. Bu bağlamda gözetim kavramının tanımını yaptıktan sonra, bu kavramın tarih içerisinde geçirdiği evrimi ele almak, gözetim kavramının daha iyi anlamlandırılmasını sağlayacaktır.

3.1.1. Gözetim kavramı

İngilizce'de "Surveillance" kelimesiyle ifade edilen "gözetim" Fransızca kökenli bir sözcüktür ve "insanların aktivitelerini izleme ve gözlemleme" anlamına gelmektedir (fr.wikipedia.org). Oxford sözlüğünde gözetim kavramının tanımı "suçlu olduğundan şüphelenilen bir kişi veya suçun işlenmiş olabileceği bir yerin dikkatlice izlenilmesi eylemi" şekline yapılmıştır. TDK sözlükte ise gözetim için "gözetme işi, nezaret, himaye, hukukta gözaltına alma" denmektedir.

Roger Clarke gözetimin "bir kişinin hareketlerinin yakından izlenmesi" anlamına geldiğini ve bu kelimenin ilk kez 18. Yüzyılın sonlarında kullanıldığını belirtmiştir (rogerclarke.com). Bozkurt (2000) ise sosyal teoride gözetim olgusuyla ilgili şunları belirtmiştir:

> *Sosyal teoride, sistematik izleme olarak adlandırabileceğimiz gözetim konusuna, ilk olarak Karl Marx dikkat çekmiştir. Köleliğin ortadan kalkması ve kapitalizmin gelişimine paralel olarak, emeğin eski yöntemlerle çalıştırılması imkânsızlaşmıştır. Biçimsel olarak özgür hale gelmiş olan işçilerin düşük maliyetle en yüksek üretimi sağlayacak şekilde çalıştırılabilmeleri için,*

kapitalist yöneticiler kendilerini işçileri denetlemek zorunda hissetmişlerdir. Bu sebeple işçileri gözetlemek/izlemek ve disiplin altına alınmış bir güç olarak boyun eğmelerini sağlamak için, günümüzde "yönetim" olarak bildiğimiz şey gelişmiştir. İşçileri fabrikalarda ve atölyelerde bir araya getirme fikri sık sık, teknik verimliliği azamiye çıkarmanın, makinaların tam kullanımını sağlamanın bir yolu olarak görülmüştür (Bozkurt, 2000: 69).

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 (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 kademede yer alanlar tarafından denetlenmesi (Giddens, 1995: 169).

David Lyon'a 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 (Lyon'dan aktaran Karakaya, 2014: 74).

Foucault ise gözetimi çalışmamızın ileriki bölümlerde ele alacağımız "Panoptikon" metaforu üzerinden ele almıştır.

3.1.2. Gözetimin tarih içindeki evrimi

Kuramcıların çoğu gözetim olgusunun tarih içinde evrimini üç başlık altında incelerler. Bu ayrım genellikle çeşitli

gözetim pratiklerinin ortaya çıkış durumuna ve insanlığın moderniteye doğru geçirdiği dönüşüme göre şekillenmektedir. Dolgun (2005), çalışmasında gözetimin tarih içindeki evrimini "Modernlik Öncesi Dönemlerdeki Toplumsal Denetim ve Gözetim Pratikleri, "Moderniteye Geçiş Sürecindeki Batı Toplumlarındaki Kapatılma Pratikleri" ve "Modern Kurumlarda Teknik Gözetim Pratiklerinin Kurumsallaşması" başlıkları altında toplamıştır. Biz de çalışmamızda gözetimin tarih içindeki evrimini "Modernlik Öncesi Dönemlerde Gözetim", "Moderniteye Geçiş Sürecindeki Gözetim" ve "Modern Zamanda Gözetim" başlıkları altında ele alacağız.

3.1.2.1. Modernlik öncesi dönemlerde gözetim

Çalışmamızın önceki bölümünde belirttiğimiz gibi Anthony Giddens'e göre gözetim içinde iki unsur barındırır. Bunların ilki, bir toplumu veya kurumu oluşturan bireylerle ilgili verilerin toplanması ve kayıt altına alınması. İkincisi ise, bir toplumda veya kurumda yer alan alt kesimdeki kişilerin üst kesimde yer alan kişiler tarafından denetlemesidir. Bu bağlamda bu unsurlardan ilkine ait olan "verilerin toplanması ve kayıt altına alınması" yazının icadından itibaren başlamıştır.

Yazının bir kayıt altına alma aracı olarak ortaya çıkması ile egemenlik ilişkileri ve gözetim arasında direkt bir bağlantı vardır. Gözetim faaliyetlerine yönelik olarak yazı, hem bir kayıt sistemi olarak topluluğa ait verilerin derlenmesinde hem de hiyerarşik bir tabakalaşma yoluyla alt sınıfların denetim altında tutulmasında kilit bir rol oynamıştır. Örneğin, idari alanda uzmanlaşmış bir yönetici kadrosunun ortaya çıkışı, yönetenler ile yönetilenlerin bilgi ve faaliyet alanları arasında kesin bir ayrımlaşmaya yol açmıştır (Dolgun, 2005: 29). Böylece yazı devletin yönetim dili olmuş ve yönetim ile halk arasında bir kopuş gerçekleşmiştir.

Yazı ortaya çıktığı ilk zamanlarda hem batıda hem de doğuda ayrıcalığa sahip çok sınırlı bir kesim tarafından bilinirdi. Mısır'da yalnızca kâtip ve rahipler okuma yazma bilmekte, devletle ilgili kayıtları onlar tutmaktaydı. Bu durum Sümerlerde de benzer şekildeydi. Batı'da ise kilise dil olarak Latinceyi kullanmaktaydı. Bu dil kilise dışında kimse tarafından okunup yazılamıyordu. Dolayısıyla baştan beri Avrupa'da Latince kilise ile halk arasında bir sınır oluşturmuştu. Kilise bu sayede toplum üzerinde baskın oluyordu.

Yazının ortaya çıkmasıyla birlikte "pastoral gözetim" olarak da adlandırılan ilk gözetim pratikleri ilkel toplulukları, yerleşik uygarlıkları, göçebe toplumları, 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).

3.1.2.2. Moderniteye geçiş sürecindeki gözetim

17. Yüzyıldan itibaren ortaya çıkmaya başlayan hastane, ıslahevi, tımarhane ve hapishane gibi kurumlar gözetimin moderniteye geçiş sürecinde farklı bir olguya bürünmesine neden olmuştur. Foucault gözetimin bu dönüşümü "Büyük Kapatılma" olarak isimlendirmiştir. Bu dönem Avrupa'da kapitalistleşmeye doğru giden yolda burjuvazinin yükseldiği dönemdir.

1656 yılında Paris'te bir kararname çıkarılmıştır ve bu kararnameyle birlikte "Genel Hastane" isimli bir kurum kurulmuştur. Birkaç ay sonra Paris nüfusunun %1'ine denk gelen

bir nüfus kendisini bu kurumun içinde kapatılmış olarak bulmuştur. Tıbbi herhangi bir yönü olmayan bu kurum, o dönemlerde filizlenmekte olan monarşi ve burjuva düzenine özgü mutlakıyetçe bir örgütlenmeyle aynı zamanda ortaya çıkmış ve onun yürütme makamı olarak bir süre sonra krallığa ait tüm şehirlere yayılmıştır (Foucault, 1992: 90).

17. yüzyılda başlayan dönüşümle birlikte kapatma pratiği 18. ve 19. Yüzyılda gözetime dayalı daha önemli bir dönüşüm yaşamıştır. Bundan böyle akıl hastaları tımarhaneye, gençler ıslah evlerine, suçlular hapishaneye kapatılacaktır. Bu anlamda bu dönem, kategorik niteliğe sahip ve gözetim temelli farklılıklar üzerine kurgulanmış bir kurumlaşma mekaniğinin doğuşuna şahit olmuştur. (Ferda Keskin'in önsözünden Foucault: 2015, 11)

Bu dönemde ortaya çıkan kapatma kurumları yeni bir anlam kazanırken, düzenin yeniden üretimi açısından sağladıkları yarar iki katına çıkmıştır. Artık bu kurumların hedefi, çalışmayanları kapatmak değil, kapatılmış olanlara iş vermek ve onları çalıştırmaktır. Kuşkusuz buradaki yer değiştirme çok açıktır: Bir yanda istihdamın ve maaşların yüksek olduğu dönemlerde ucuz emek gücünün sağlanması; diğer yanda da baş gösteren ekonomik kriz veya işsizlik dönemlerinde aylaklığın üstesinden gelinerek isyanlara karşı toplumsal korunmanın sağlanması. Bunun kanıtı, ilk kapatma kurumlarının İngiltere'nin en sanayileşmiş şehirlerinde ortaya çıkmasıdır; Lyon ve Paris'teki Genel Hastaneler de buna örnektir. Bu kurumlarda hedeflenen şey, çalışmayı bir meşguliyet haline getirmek değil, üretkenliği sağlamaktır. (Dolgun, 2005: 59).

İktidar düzenine göre gözetlenmenin cezalandırmadan daha etkili ve daha verimli bir silah olduğunun keşfedildiği 18. Yüzyılın sonu ile 19. Yüzyılın başlarında yeni iktidar işleyişi ortaya çıkıyordu. 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;

> *Bu tip hapishane, yöneticilerin mahkûmların eylemlerini ve söylemlerini denetlemelerine imkân veren mimari özelliklere sahipti. Ortak yeme, içme ve eylem alanları olmasına karşın, mahkûmlar, merkezi gözetleme kulesinden görülebilen tek pencereli bireysel hücrelerde tek başlarına tutulmaktaydı. Hücreler gözetleme kulesindeki nöbetçiler tarafından tek bir yerden görülebilmeleri amacıyla dairesel bir şekilde düzenlenmişti. Ayrıca arkadan gelen ışık sayesinde, çevre binadaki hücrelerin içine kapatılmış küçük siluetleri olduğu gibi kavramak mümkündür. Ancak mahkûmlar nöbetçilerin onları ne zaman gözleyip gözetlediklerini bilemekteydiler; çünkü kule pencerelerindeki çekme perde, nöbetçilerin görülmelerini engellemekteydi. Panoptikon, mahkûmların davranışlarını en üst düzeyde denetlemek için geliştirilmiş bir sistemdi. Devamlı gözetim altında olabileceklerini bilen mahkûmlar, eylemlerini bu bilince göre denetlemek zorundaydı (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. Mahkûmlar her an gözetlendiklerini düşündükleri için hareketlerinde temkinli olmuşlar ve kendilerine söylenenleri yerine getirmeyi tereddüt etmeden kabul etmek zorunda kalmışlardır. Buradaki gözetleme kulesi hapishanede bir tür iktidar rolü oynamaktadır. Bu kulede gözetleyen bir memur olmasa dahi, gözetlenenler üzerinde gözetlendiklerinin bilinçaltların işlenmesi sağlanmıştır (Foucault, 2012: 86).

Foucault'a göre hapishane suçluları namuslu insanlar haline getirmekten çok, yeni suçlular üretmeye yarıyordu. Foucault bu konuyla ilgili şunları söylemiştir:

Birisi hapishaneye girdiği andan itibaren onu lekeli biri haline getiren bir mekanizma işlemeye başlıyordu; hapisten çıktığında yeniden suç işlemeye eğilimli biri olmaktan başka çaresi kalmıyordu. Onu bir muhabbet tellalı, polis ya da muhbir haline getiren sistemin içine zorunlu olarak düşüyordu. Hapishane profesyonelleştiriyordu. Kırlarda dolaşan ve genellikle çok vahşi olan, on sekizinci yüzyılda görülen gezgin çeteler gibi olmak yerine, çok kapalı olan, polisin gayet iyi sızabildiği, siyasi ve iktisadi yararı göz ardı edilemeyecek, esasen şehirli, suç işlemeye eğilimli bir çevre vardır (Foucault, 2012 :26).

Foucault daha sonra Panoptikon'u iktidarların gözetim faaliyetleriyle ilgili bir metafor olarak kullanmıştır. Günümüzde birçok kuramcı interneti ve siber uzayı panoptik bir alan olarak görmektedir. Bu konuyu çalışmamızın ilerleyen bölümlerinde ele alacağız.

3.1.2.3. Modern zamanda gözetim

Gözetim tarihin tüm çağlarında var olmuş ve iktidarların elinde önemli bir toplumsal denetim silahı olarak görev yapmıştır. Fakat gözetim bu döneme kadar tam olarak kurumlaşamamış ve sistematikleşememiştir. Bu dönemden itibaren kapitalizmle birlikte ortaya çıkan gözetim teknikleri bireyin tüm yaşamını özel/kamu ayrımı yapmadan egemenliği altına almıştır:

Kurumsallaşmış şekliyle toplumsal yaşamın merkezi ve yayın bir özelliğini oluşturan teknik gözetim, günümüzdeki anlamıyla 19. Yüzyıla kadar ortaya çıkmamıştı. Bu aşamadan sonra ise, yayılması çok hızlı oldu. Geniş ölçekli sistematik denetime yaslanan bu yayılımın temel unsurlarını, sınai kapitalizm, sanayi kentlerinin artışı ve yoğunlaşma hızı, ulus-devletin iç ve dış tehlikelere karşı korunma güdüsü, askeri örgütlenmeler, devlet idaresi, bürokratik yapılanma ve kapitalist işletme

sayısındaki artışlar gibi bileşenlerin oluşturduğu modern toplumda bulmak mümkündür. Bu unsurlara bağlı olarak, sınıf ilişkileri ile rasyonalize olmuş bir sistemin –veya toplumun- mevcut yapı içine nüfuz edici bir boyutu olarak gözetim, sosyolojik açıdan modernitenin belirleyici özellikleri içinde en önemli unsurlarından birini oluşturur. Önceki dönemlerde, gündelik yaşamda insanların sıradan etkinliklerini böylesine kapsamlı şekilde çevreleyen toplumsal örgütlenmeler söz konusu değildi. Dinsel, geleneksel ve feodal toplumlardaki mevcut uygulamalar, modern toplumla birlikte yoğunlaştırılmış ve sistematik bir hale getirilmiştir (Dolgun, 2005: 60-61).

Foucault (1994/2012)'ya göre: Bir an geldi ki herkesin iktidarın gözü tarafından fiilen algılanması gerekmiştir. Kapitalist tarzda bir toplum tarzı istenmiş, bu mümkün olduğunca yaygınlaştırılmış, mümkün olduğunca verimli bir üretimle birlikte; işbölümünde kimilerinin şu işi, kimilerinin bu işi yapmasına ihtiyaç olduğunda, halkın direniş hareketlerinin, ataletin ya da isyanın, doğmakta olan tüm bu kapitalist düzeni altüst etmesinden korkulduğunda, o zaman, her bireyin somut ve kesin gözetlenmesi gerekli olmuştur. (Foucault, 2012: 157)

Modern tarihlerdeki teknik gözetime yönelik ilk yöntemler kapitalist sistemde hizmet veren fabrika ve atölyelerde çalışan işçilerin sermaye sınıfı adına disipline edilmeleriyle ortaya çıkmıştır. Çalışma yaşamı ve çalışanlar üzerinde gözetim, işin zamanlanması ve çalışma sırasında işçilerin sürekli olarak sınanmaları ve gözlenmeleri gibi yöntemlerle fabrikalarda işlerliğe sokulmuştur. Tarım toplumu içinde her yerde –evde, tarlada- yapılan çalışma; sanayi toplumlarında, binlerce işçiyi çatısı altında barındıran ve disiplinli bir düzen içinde örgütleyen fabrikalarda yapılmaya başlanmıştır. Mekânsal düzenlemedeki amaç, bireylerin aynı anda hem çalışmaya odaklanabilmeleri için kapatılabilecekleri hem de

gözetimi en kolay şekilde gerçekleştirmeye yönelik olarak yerlerinin bilinebileceği belli bir alan içinde sistemli bir şekilde dağılımlarının sağlanmasıdır. Fabrikalar aracılığı ile bu dağılım, belli talepleri olan bir üretim aygıtıyla eklemleştirilmiş olacaktır. Bir sonraki aşamada ise, işbölümü ile uzmanlaşmaya yönelik bir mekânsal düzen anlayışı getirecek olan sistem; bedenlerin dağılımını, üretim aygıtının mekânsal düzenlenişini ve çeşitli faaliyet biçimlerini, gözetime en uygun şekilde ve vardiyalar halinde birbirine bağlar (Dolgun, 2005: 64, 69).

Modern dönemdeki gözetim pratikleri ilk önce ustabaşılarının işçileri gözetlemesiyle ve aylaklık eden işçileri sürekli uyarmalarıyla ortaya çıkmış. Daha sonra teknolojinin gelişmesi ile ustabaşılarının 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. Çok önemli bir gözetim alanı olan internet ve siber uzay üzerinde işleyen gözetim yöntemlerini çalışmamızın ilerleyen bölümlerinde detaylıca ele alacağız.

3.1.3. Gözetime kuramsal ve kavramsal bir bakış "panoptikon, süperpanoptikon, sinoptikon, omnioptikon ve ban-optikon" kavramları

Sosyal bilimlerde gözetim olgusu bazı kuramcılar tarafından bazı kavramlarla ilişkilendirilmiştir. Bu kavramlar gözetim olgusunun modern dünya içinde geçirdiği evrimler sonucu ortaya çıkmıştır. Bu kavramlar "Panoptikon", "Süperpanoptikon", "Sinoptikon", "Omnioptikon" ve "Ban-optikon"dur. Bu kavramları ve ne anlama geldiklerini aşağıda ele alacağız.

3.1.3.1. Panoptikon

Foucault, 1785 yılında Bentham'ın tasarladığı hapishane modeli olan Panoptikon'u sosyal teoride bir metafor olarak kullanmıştır. Bu hapishane modeli daha önce de bahsettiğimiz gibi yöneticilerin mahkûmların davranışlarını denetlemelerini sağlayacak özelliklere sahipti. Bu hapishane dairesel bir biçimde tasarlanmıştı ve ortasında bir gözetleme kulesi bulunmaktaydı. Arkadan gelen ışık ise, hücrelerin içindeki mahkûmların kavranmasını sağlamaktaydı. Mahkûm-lar ise ne zaman gözetlenip gözetlenmediklerini bilmemekteydiler; kuledeki perde hapishanedeki görevlinin mahkûmlar tarafından görülmesini engelliyordu. Bu nedenle mahkûmlar devamlı gözetim altında olabilecekmiş gibi hareket etmekteydi.

Gözetim, bilgi, eğitim, mahkûmların sürekli gözetlenildiğine inandırılma ve böylece iktidarın otomatikleştirilmesi sayesinde işlemektedir. Ancak Foucault, bu sistemin toplumun diğer kurumlarına aktarıldığını savunur. Eğitim kurumları, fabrikalar, hastaneler hapishanelerdeki panoptik sistemi devralmışlar ve iktidarın bakışını kurumsal mekanizmaların merkezlerine yerleştirmişlerdir (Öztürk, 2013).

İktidarın Gözü (1994/2012) isimli yapıtta Michael Foucault, 20. Yüzyılın kapitalist toplum sistemlerinde, artık

iktidarın değişlik gösterdiğinden bahseder. Artık tek kişilik ve yüzünü her zaman gördüğümüz bir kral iktidarının yerini, bilinmeyen stratejilerin hayata geçirildiği açık bir biçimde verilen cezalar yerine, insanların iktidarın yaptığı gözlem dayatması nedeniyle kendi kendini kontrol ettiği görünmeyen bir iktidarın varlığından söz eder. İktidar farklı bir boyuta taşınmıştır. İktidar bundan böyle çok farklı bir otorite biçimi kullanmaktadır. İktidar artık "gözün iktidarıdır". Bu bağlamda Foucault Panoptikon'u bir hapishane modeli olmaktan çok, bir toplumsal denetim modeli olarak görmektedir (Foucault, 2012).

Dolgun (2005)'e göre Panoptikon mimari bir yapıyı ifade etmekten öte, bir sistemin mantığını ve toplumsal denetime yönelik işleyiş mekanizmalarını ortaya koyar. Bu, iç dinamikleriyle ile tüm toplumu dönüştüren ve bireyleri sürekli gözetim altında tutan disipliner bir mekanizmadır. Foucault Panoptik toplumu; ıslah temelli olarak kişisel ve sürekli bir gözetime dayanan, denetim/cezalandırma ve ödüllendirme gibi mekanizmalar yoluyla, bireylerin belli kurallara göre dönüştürülmesini hedefleyen ve direkt bireyler üzerine uygulanan bir iktidar biçimi olarak tanımlar (Dolgun, 2005: 90).

Zygmunt Bauman'ın da belirttiği gibi "bilgi güçtür". Bilgiye sahip olan iktidar, gücü elinde tutar ve altındakileri elinde bulunan bilgilere göre yönetir. Bilgiye sahip olabilmek gözetimin getirdiği bir durumdur. Panoptikon bu açından önem taşımaktadır. Panoptikon'un gözetleme sistemi sadece hapishanelerde uygulanan bir uygulama olmayıp, günümüzde "gözetim toplumu", "denetim toplumu" gibi kavramların yaşamın her alanına egemen olması bakımından önemlidir. Küresel kapitalizm yeni teknolojileri, özellikle de iletişim teknolojilerini aracılığıyla toplumsal denetimi kullanarak, bu denetimi tüm güçlerin önünde daha baskın bir hale getirmektedir. "İktidarın gözü" küreselleşmekte ve toplumsal özgürlükleri yok ederek, baskıcı gözetim toplumunu yerel

iktidarların yardımıyla yeniden biçimlendirmektedir. Küresel panoptikon, yeni emperyal iktidarın "yeni dünya düzeni"dir. Toplumlar, küreselleşme süreci ile birlikte, gözetleyen büyük güç, "Büyük Birader" tarafından teslim alınmıştır, başka bir deyişle herkes "gözaltına" alınmıştır (Sucu, 2011).

Bu bağlamda Panoptikon ile gözetimin çok farklı bir kılıfa büründüğünü söylemek mümkünüdür. Panoptikon sayesinde iktidarların, toplumdaki bireyleri gözetleyebilmeleri için kendilerini göstermelerine gerek kalmamıştır. Bireyler devamlı olarak gözetleniyormuş gibi hareket etmekte; davranış ve söylemlerine buna göre çeki düzen vermektedirler.

3.1.3.2. Süperpanoptikon

George Orwell tarafından yazılan 1949 yılında yazılan "1984" isimli distopik romanında Big Brother (Büyük Abi, Birader) olarak bilinen merkezi bir güç (devlet) insanların her türlü hareketini, attığı her adımı izler ve denetimde tutmaktadır. "1984"te Big Brother, hiçbir bireysel harekete ve en ufak bir aykırılığa bile izin vermemektedir. 1932 yılında Aldous Huxley tarafından yazılan "Brave New World" isimli romanda yine 1984'te yer alan distopik bir toplumsal yapıya benzer bir toplumsal yapı vardır. Bu toplumsal yapıda dünya tek bir iktidar tarafından yönetilmektedir. Biyoteknoloji o kadar gelişmiş ki, insanlar muazzam bir genetik sistemi sayesinde bir merkezde üretilmektedirler. Burada insanların kişiliklerini tamamen kaybettiklerini ve bir robot gibi davrandıkları görülür. Herkesin yanında olduğu ve hiçbir karşıtı bulunmayan bir totaliter devlet yapısı bulunmaktadır. Bu devlet yapısı, aynı zamanda toplumun attığı her adımı izlemekte ve toplum da izlenildiğini bilmekte, adımlarını ona göre atmaktadır. Hatta toplum halinden memnunmuş gibi davranmaktadır. Günümüzden 70-80 yıl öncesinde yazılan bu toplum karşı-ütopyalarında çok gelişmiş teknoloji sayesinde

gözetimin süper-teknolojik bir hal aldığı görülmektedir. Bugün ise tam anlamıyla olmasa da geçmişte yazılan bu romanlardaki toplum yapısına benzer bir yapının içinde yaşamakta olduğumuz söylenebilir.

Enformasyon teknolojilerinin gelişmesiyle birlikte gözetim, bireylerin yaşadıkları hayatın her alanına sirayet etmeye başlamıştır. Bu bağlamda enformasyon teknolojileri iktidarlar tarafından birer gözetim teknolojisi olarak da kullanılmaya başlanmıştır. Süperpanoptikon kavramı da 20. yüzyılın sonlarına doğru enformasyon teknolojilerinin gelişmesi, telekomünikasyon ve bilgisayardaki yeniliklere paralel olarak sosyal teori içinde ortaya çıkmış bir kavramdır. Süperpanoptikon için denetim ve gözetimin siberleşmiş hali diyebiliriz. Süperpanoptikon kavramıyla ilgili Öztürk (2013) şunları söylemektedir:

> *Süperpanoptikon kavramı, Mark Poster'ın kullandığı ve David Lyon'un geliştirdiği 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).*

Süperpanoptikonun üç işlevi bulunmaktadır: tanımlama, sınıflandırma ve değerlendirme (Öztürk, 2013): Tanımlama, kimlik bilgilerimizin elde edilme işlemidir. Bu bağlamda internet sitelerine üye olurken verdiğimiz her türlü kişisel bilgi

ya da kredi kartı başvurusu sırasında ya da banka hesabı açtırdığımız sırada doldurduğumuz formlardaki bilgilerimiz bizim kimlik bilgilerimizi oluşturmaktadır. Bu bilgiler elde edildiğinde ise -bunlar genellikle bilgisayarlardaki veri tabanlarında toplanmaktadır- bir sonraki aşama olan sınıflandırmaya geçilir. Sınıflandırma aşamasında elde edilen kişisel bilgilere göre kişiler belirli profiller altında yerleştirildikten sonra kategorilere ayrılırlar. Sınıflandırmada siber uzay içerisinde yaptığımız her tercih önem taşımaktadır. Bir alışveriş sitesinden aldığımız herhangi bir ürünü düşünebiliriz. Aldığımız ürünlerin türleri ve özellikleri; alışveriş alışkanlıklarımız bu sınıflandırmada önemli bir yer tutar. Değerlendirme işlemi ise ne tür bir yönelimde olduğumuzu tespit etmeye çalışır. Çalışmamızın sonraki bölümlerinde detaylı işleyeceğimiz "pazarlama şirketlerinin çevrimiçi gizliliği ihlal etme türleri"nden biri olan veritabanlı pazarlama faaliyetleri bu kapsamda değerlendirilir. Alışveriş sitelerine tekrar girdiğimizde karşımıza daha önce satın aldığımız ürünlere benzeyen ürünlerin reklamları çıkacaktır. Değerlendirme yalnızca küçük harfle başlayan iktidarı elinde bulunduran pazarlama şirketlerinin yaptığı faaliyetlerle sınırlı değildir. Kişisel bilgilerimizin elde edilip, tercih ve alışkanlıklarımızın bilinmesinden sonra değerlendirme işlemi büyük harfle başlayan İktidarı elinde bulunduran hükûmetler tarafından da yapılmaktadır. Bununla ilgili bir örnek vermek gerekirse; sürekli Marksizm ya da devrimlerle ilgili kitaplar satın alan ve internetten sürekli Marksist sitelere giren bir şahsın potansiyel bir tehlikeli birey olarak değerlendirilmesi olasıdır. Bombalardan hoşlanan ve bombaların nasıl yapıldığını merak eden bir şahsın düzenli olarak bomba yapımı ile ilgili internet sitelerine girmesi ve bu tür araştırmalar yapması sonucu bu tür bir değerlendirmeye tabi tutulması da olasıdır.

Aslında hazırladığımız bu çalışma tam anlamıyla Süperpanoptikon kavramı ile ilişkilidir. Çünkü teknolojiyle sürekli

olarak iç içe yaşayan bizler, internet ve siber uzay sınırlarının içerisinde siyasi iktidarı elinde bulunduran hükûmetler ile ekonomik iktidarı elinde bulunduran büyük şirketler tarafından bir gözetim pratiği olarak Süperpanoptikonun içerisinde birer gözetim nesnesi durumundayız. Bu iktidar erklerinin yaptığı gözetim ve denetim faaliyetlerine bir de kötü niyetli bilgisayar korsanlarının yaptığı kötü faaliyetler eklenince kişisel bilgilerimiz elden ele dolaşmakta, kategorize edilmekte ve mahremiyetimizin tüm sınırları yerle bir edilmektedir.

Süperpanoptik bir alan olarak internet ve siber uzayda siyasi iktidar ile ekonomik tarafından gerçekleştirilen gözetim faaliyetlerini daha geniş olarak örnekleriyle birlikte ele alacağız.

3.1.3.3. Sinoptikon

Foucault sosyal teori içerisinde gözetimle ilgili önemli çalışmalar gerçekleştirmiştir. Gözetim olgusu ise zaman içinde gerçekleşen teknolojik ve toplumsal gelişmelerin etkisiyle farklı bir kılıfa bürünmüştür. Bu bağlamda Foucault'un gözetim kavramıyla ilgili yaptığı katkılar farklı akademisyenler tarafından yeniden ele alınmıştır. Norveçli Sosyal Bilimler Profesörü Thomas Mathiesen 1997 yılında "The Viewer Society: Michel Foucault's 'Panopticon Revisited" isimli makalesinde Foucault'un çağdaş gözetim anlayışına büyük katkıları olduğunu kabul etmiş; fakat Foucault'nun ortaya attığı Panoptikon kavramının yeniden gözden geçirilmesini savunmuştur (Mathiesen, 1997). Mathiesen (1997)'e göre Foucault'nun ortaya attığı Panoptik gözetim anlayışında azınlık, Bentham'ın gözetleme kulesinde olduğu gibi çoğunluğu gözetlemekte, gözetlenen çoğunluk ise gözetleyenin varlığını hissederek davranışlarını ona göre düzenlemekte, kendi kendini kontrol ve disipline etmektedir. Buna rağmen; Mathiesen'nin kendi deyimiyle 'şaşırtıcı bir şekilde' Foucault, bu çalışmalarında

sadece kendi döneminin teknolojisi ile düşünmüş, günümüz iletişim teknolojilerini ve özellikle "Sinoptizm"in zıt ve eşzamanlı gelişen işleyişini görmezden gelmiştir. Mathiesen'e göre Foucault, "kitle medyasının, özellikle günümüzde 100 milyonlarca insanı aynı anda bir araya getirebilme özelliği olan televizyonun, azınlığı izleme ve ona hayran bıraktırma konusundaki büyük gücünü görmezden gelmiştir" (Mathiesen'den aktaran Karakaya, 2014: 85)

Mathiesen (1997)'e göre modern kapitalist iktidar biçimlerinde, 'ruh'un kontrolü aynı zamanda bedenin de kontrolüdür. Dolayısıyla "sözde-demokratik kapitalist" toplumlarda "ruh"un kontrol ve disipline edilmesiyle amaçlanan, "otokontrol yöntemiyle kendi kendini kontrol eden insan tip" yaratmaktır. Bu insan tipi "sözde-demokratik kapitalist topluma tam olarak uyan, sorgulamadan kabul eden insan tipleridir." Mathiesen, bu insan tipini oluşturma işi günümüzde Foucault'nun iddia ettiği gibi Panoptikon'un değil, Sinoptikon'un görevi olduğunu belirtmiştir. Mathisen, bu doğrultuda Panoptikon teriminin günümüz sistemlerini açıklamada yetersiz kaldığını iddia ederek, Yunanca'da, aynı anda, eş zamanlı anlamına gelen "Syn" ve görme anlamına gelen "optic" kelimelerini birleştirerek Synoptic (Sinoptik) kelimesini türetmiştir. Sinoptikon yaklaşımında, Panoptik yaklaşımın aksine "kitle iletişim araçlarının etkisiyle çoğunluk da kolaylıkla azınlığı izleyebilmekte" hatta "onlara hayran kalarak kendilerini onlarla özdeşleştirmektedir." Bu durum kitle iletişim araçlarını kullanan çoğunluğun, seçilmiş ünlüleri izleyerek ve onları örnek alarak 'normalleşmesine' yani mevcut sistemin normlarına, kurallarına uymalarına neden olmaktadır (Mathiesen'den aktaran Karakaya, 2014: 85, 86).

Sinoptikonun temel medyası radyo ve özellikle televizyon gibi araçlardır. Kısaca, iletişim literatüründe "kitle iletişim medyası" olarak nitelendirdiğimiz araçlar Sinoptikon

modelinin temel unsurları arasında yer alır. Geniş alanlara dağılan, birbirinden farklı yaşlara, sınıfsal konumlara, cinsiyetlere, tercihlere, kültürel arka planlara sahip insanlar, kültür endüstrilerince yaratılan aynı mesajlara maruz kalırlar. Mesajların içeriği önemli kişilikler, yıldızlar, kurmaca veya gerçek olaylar olabilir. Buna karşın, mesajların yaratımında alımlayıcıların doğrudan bir katkısı olmaz, onlar katılımcı değildirler; daha çok kendilerine sunulanları alırlar. Sinoptikonda belirleyici olan, görünürlüğün değişmesidir. İnsanlar, az sayıdaki kurgusal veya gerçek karakterleri takip ederler. Televizyon örneğinden gittiğimizde izlenilen karakterlerin izleyicileri izlemeleri ve onlara doğrudan yanıt vermeleri mümkün değildir (Öztürk, 2013).

Televizyon izlemekle insanlar, sadece televizyonda gerçekleşen olaylara ve karakterlere değil, aynı anda diğer izleyicilere de bağlanırlar. Ancak bu bağlanma, gerçek bir iletişim olmaktan çok hayal edilmiş, imgelenmiş bir iletişimdir. İnsanlar hayallerinde birbirlerine bağlanırlar. Bu bağlanmaların önemli sonuçları vardır. Medyadan yayılan mesajlarla kurulan ilişki, disiplin kurulmasına ve içselleşmesine katkı yapar. İktidarın artık özneleri devamlı olarak izlemesine gerek kalmamıştır. Kontrol, sembollerle sağlanır hale gelmiştir. Sembollerle kurulan ilişki aracılığıyla çoğunluk azınlığın dünyasını izler (Öztürk, 2013).

Panoptik yapının yanı sıra Sinoptik bir nitelik kazanan toplum, iktidarın yönetimindeki göz önündekilerle toplumun adeta hareket geçme yetisini köreltmekte, toplumu uysallaştırmaktadır. *Öğrenilmiş çaresizlik* psikolojisindeki uysal bedenler ise bilişim teknolojilerinin toplumsal denetim hedefli bir araç olduğunu bile bile iktidara gönüllü kulluk etmektedirler. Öğrenilmiş çaresizlik kavramıyla ifade edilmek istenen, bireylerin kendi davranışlarının olaylarının sonuçları üzerinde hiçbir etkisi olmayışına inanmaları durumudur.

Yaşanan bu duygusal yetersizlik durumu, bireyin müdahalenin mümkün olduğu anlarda bile yeterli davranışı göstermeyişine neden olmaktadır (Tokgöz, 2011: 138)

Süperpanoptikon dünyasını temsil eden bilgisayar, kısmen Sinoptikon modelinin bazı özelliklerini içinde barındırır: Gazeteleri, televizyon programları, filmleri: kısaca aynen kitle medyasında üretilen ve geniş kitlelere yayılan mesajları bilgisayarda da takip edebiliriz. Aradaki fark, bilgisayarın katılıma daha fazla imkân vermesinden kaynaklanır. Gelgelelim örneğin yıldızlar, önemli kişilikler, olaylar geniş sayıdaki insanlar etrafından kaynaklanır: kurgusal ve gerçek karakterler bilgisayar başındaki insanları göremez. Görme, duyma ve okuma ilişkisinde gören, duyan ve okuyanlar izleyiciler olan "çoğunluktur". Büyük iktidarın araçlarından birisi olan medya orada bekler ve etrafında kümelenen çoğunluk medyaya maruz kalmakla başka bir dünyaya yolculuk yapar. Kısaca Panoptikon'un seyredileni, seyredene dönüşmüştür. Panoptikon insanları bir yere çakıp sürekli izlenme durumuna sokarken, Sinoptikon baskısız, koşulsuz, eğlenceli bir seyretme eylemine sokmuştur. Daha önce azınlık çoğunluğu izlerken, şimdi çoğunluk azınlığı seyretmektedir. Seyredilenler: seçkin yıldızlar, politika, spor, bilim, şov ve iletişim dünyasının seçkin insanlarıdır. Seyredilenler, seyredenlere genel bir hayat tarzının mesajını verirler: bunu kendi hayatlarına kendi hayat tarzlarına dair söylem ve davranışlarla yaparlar; imrenme yaratırlar (Öztürk, 2013)

Bilişim teknolojilerini kendi ideolojileri doğrultusunda kullanan ve toplumlara öncellikle özgürlük bahşederek bir parmak bal çalan iktidarlar, toplumu yerel baskılardan kurtarırken küresel tahakkümlerin pençesine düşürmekte ve bunları toplumun gözetime katılmalarıyla yapabilmektedir. Toplumun kendi gözetimlerine bu şekildeki katılımı ile bilişim teknolojilerinin sağladığı olanaklar bir araya geldiğinde, eski

denetim şekillerine çoğu zaman gerek bile kalmaksızın uysal bedenlerin oluşturduğu uysal toplumlar gözetim ile denetlenebilmektedir (Tokgöz, 2011: 138).

Sinoptikondaki seyretme edimi son derece haz verici olduğundan artık insanları baskıyla yönetmeye de gerek kalmamıştır. İnsanlar seyrederken sürekli eğlendikleri için baskı altında olduklarını bilmezler. Eğlence, artık dünyayı yönetmenin ideolojisi haline gelir. İnsanlar televizyon ekranlarında ve sosyal medyada kendilerinden geçerek gerçek dünyanın gerçek problemlerinden uzaklaşırlar. Bu noktada eğlence artık gerçek ideoloji haline gelir (Öztürk, 2013).

3.1.3.4. Omnioptikon

Emanuel Dimas de Melo Pimenta sosyal teoride gözetim kavramını açıklamaya çalışan yaklaşımlardan Thomas Mathiesen'in geliştirdiği Sinoptikon yaklaşımını ve Bentham'ın ortaya çıkarıp, Foucault'un ileriye götürdüğü Panoptikon yaklaşımını karşılaştırmış; bu yaklaşımlara bir üçüncü yaklaşımın eklemlenmesi gerektiğini öne sürmüştür.

Pimenta, çoğunluğun kitle iletişim araçları vasıtasıyla azınlığı izlediği ve ona imrendiği, medya tarafından eleme işleminden geçirilerek seçilmiş azınlığın çoğunluğun üzerinde düşünsel yönden bir iktidar kurduğu Sinoptikon yaklaşımı ile azınlığın çoğunluğu izleyerek onlar üzerinde tahakküm kurduğu Panoptkikon yaklaşımına, Omnioptikon yaklaşımının da ekleneceğini iddia etmiştir. Pimenta, İngilizce'de "her yerde bulunan" anlamı taşıyan "omnipresence" sözcüğündeki "omni" öbeğini alıp, gözetlemek anlamı taşıyan "opticon" kelimelerini birleştirerek Omnioptikon kelimesini geliştirmiştir. Pimenta (2010)'a göre Omnioptikon, "herkesin herkesi kontrol ettiği" durumunu ifade etmektedir. Pimenta Omnioptikon'u, "Panoption ile Sinoptikon etkisinin birleşmesi ve bu kavramların işbirliğiyle, fakat aynı zamanda, herkesin

herkes tarafından kontrol edildiği bir sistemde izlenmenin belirli bir çerçeveye eklemlendiği" durumunu ifade etmek için geliştirdiğini belirtmiştir (Pimenta, 2010: 272).

Pimenta'ya göre Omnioptikon'un ortaya çıkmasıyla olan şey, sadece çoklu casusluk sistemleri vasıtasıyla Panoptikon'un ve (kitle iletişim araçları aracılığıyla) Sinoptikon fenomeninin birlikte hareket etmesi değil, aynı zamanda sıradan insanlar olarak bilinen bireylerin kişisel röntgencilik, kontrol ve narsisizme geçişleridir (Pimenta'dan aktaran Karakaya, 2010: 99). Günümüzde gözetim sistemleri, bireylerin en mahrem mekânları olan evlerine kadar girmiştir. Çoğu zaman güvenlik gerekçe gösterilerek bireylerin mahremiyetleri ihlal edilmektedir. Pimenta'nın Omniptikon yaklaşımı ile ortaya attığı en önemli fikir gözetimde bireylerin edindiği konumdur. Artık milyonlarca insan gözetim sistemlerini gönüllüce kullanmakta, hem kendileri hakkında detaylı bilgileri internete ve sosyal paylaşım ağlarına yüklemekte hem de başkalarını gözetleyerek onlar hakkındaki bilgileri de özgürce paylaşmaktadırlar (Karakaya, 2014: 99).

3.1.3.5. Ban-optikon

Daha önce çalışmamızda gözetim pratiklerinin ve özellikle de Süperpanoptikon'un kişilerin profillerinin çıkarılmasında, diğer bir ifadeyle fişlenmekte kullanıldığına değinmiştik. Didier Bigo profil çıkarma teknolojilerinin belli başlı gözetim biçimlerine hangi bireylerin tabi tutulacağının belirlenmesinde kullanılmasını "ban-optikon" olarak adlandırmıştır (Bigo, 2006).

Zygmunt Bauman ve David Lyon (2013)'e göre Ban-optikon tabiri, yeni bir "küreselleşmiş güven(siz)lik"in polis, sınır görevlileri ve havayolu şirketleri gibi uluslararası "huzursuzluk yöneticileri"nin gittikçe artan planlı faaliyetlerinden doğuşunun tastamam bir teorik analizinden gelmiştir. Gerek

ticaret gerekse siyaset alanındaki ulus aşırı gözetim ve kontrol bürokrasileri nüfus hareketlerini izlemek ve kontrol etmek için artık gözetim sayesinde belli bir uzaklıkta çalışmaktadırlar. Bu söylemler, uygulamalar, fiziki mimariler ve kurallar birlikte ele alındığında eksiksiz ve bağlı bir aygıt ya da Foucault'nun deyişiyle *dispozitif*'i (müdahale aygıtlarını) oluşturmaktadır. Ortaya çıkan sonuç küresel bir panoptikon değil, Jean-Luc Nancy'nin Agamhen tarafından geliştirilen "ban" (yasak) fikri ile Foucault'nun "optikon"unu birleştiren "ban-optikon"dur. *Dispozitif*, yalnızca belli bir ulus-devletten değil, amorf ve birleşmemiş bir küresel güç demetinden dışlanan insan kategorileri yaratarak kimin hoş karşılanıp kimin karşılanmadığını gösterir. Sanal olarak faaliyet gösteren ban-optikon, *Azınlık Raporu* filmi ve kitabında olduğu gibi veri akışını, özellikle de henüz meydana gelmemiş şeylerle ilgili veri akışını yönlendirmek için ağ bağlantılı veritabanlarını kullanır (Bauman ve Lyon, 2013: 66, 67).

Ban-optikonun stratejik işlevi bir azınlığın profilini "istenmeyen" olarak çıkarmaktır. Ban-optikonun üç özelliği vardır: liberal toplumlar içerisinde istisnai bir güce sahiptir (olağanüstü haller rutinleşmiştir), profiller çıkarır (gelecekteki olası davranışlardan korkulan bazı grupları tedbir olsun diye dışarıda bırakılmış insan kategorilerini ötekileştirir) ve dışlanmayan grupları normalleştirir (malların, sermayenin, bilginin ve insanların serbest dolaşımına inanılmasını sağlar). Ban-optikon, ulus-devletin ötesindeki küreselleşmiş mekânlarda faaliyet gösterir, dolayısıyla iktidarın ve direnişin etkileri artık yalnızca devlet ile toplum arasında hissedilmez (Bauman ve Lyon, 2013: 67).

Bauman (2013)'e göre gözetim teknolojisi günümüzde iki karşıt stratejik amaca hizmet etmekte, iki cephede gelişmektedir: bir cephede hapsetmek (ya da "çitin içine almak"), diğerinde ise dışarıda bırakmak (ya da "çitin dışında

bırakmak"). Sürgün, mülteci, sığınmacı –ya da ekmek ve içme suyu arayan insan- sayısının küresel düzeydeki artışı aslında gözetim teknolojisinin *her iki* türünü de ilerletmektedir (Bauman ve Lyon, 2013: 69).

Sürgün, mülteci, sığınmacı ya da ekmek ve içme suyu arayan insanların hepsi lüzumsuzdur. Hepsi de toplumun ıskartaları veya artıklarıdır. Kısacası, onlar atıktır. "Atık" tanımı gereği "fayda"nın karşıt anlamlısıdır; uygun bir kullanımı olmayan nesneleri adlandırır. Aslında, atığın tek yaptığı şey, aksi takdirde gayet verimli bir biçimde kullanılabilecek olan mekânı kirletmek ve karıştırmaktır. Ban-optikonun temel amacı atığın değerli ürünlerinden ayrılmasını ve çöplüğe gönderilmek üzere işaretlenmesini garantiye almaktır. Bir kez görüş açısına girdi mi, onun –tercihen biyolojik olarak çözünene kadar- orada kalmasıyla panoptikon ilgilenir (Bauman ve Lyon, 2013: 71)

3.1.4. Siber denetim ve siber uzaydaki gözetim faaliyetleri

Siber denetim, siber uzay üzerinde gerçekleşir. Siber uzay ise ağ bağlantısı bulunan tüm internet evrenini kapsar. Siber uzay, ağ bağlantısına sahip kişiler tarafından erişilebilen bir ortamdır, kısacası kamuya açıktır. Kimi bilim çevreleri tarafından internet veya diğer adıyla siber âlem, her türlü fikrin var olduğu ve fikirlerin, toplumsal sorunlar vs. tartışıldığı bir kamusal alandır. Elbette herkese açık olması bakımından internet bir kamusal alana benzese de, iktidarın bu kamusal alan üzerindeki etki ve denetimi internete kamusal alan olarak bakan görüşlerin tartışılmasına sebep olmuştur. Bilişim dünyasında "Dünya yuvarlaktır; siber ağı çevreleyen kablolar Pentagon'da başlayıp Pentagon'da son bulur" gibi ironi taşıyan ifadeler mevcuttur.

Kuşkusuz bilişim dünyasında yukarıdaki sözü doğrular nitelikte birçok unsur bulunmaktadır. Bu unsurlardan belki de en önemlisi, günümüzde öncülüğünü ABD'de bulunan NSA (National Security Agency / Ulusal Güvenlik Dairesi)'in yaptığı internet ve siber uzay üzerinde gerçekleştirilen denetim ve gözetim faaliyetleridir.

İlk zamanlarda diplomatlar ile ordu arasındaki şifreli telsiz görüşmelerini deşifre amacını taşıyan Amerikan Ulusal Güvenlik Dairesi (NSA), Truman'ın talimatıyla 24 Ekim 1952'de kurulmuştur. Ardından tüm dünya üzerindeki telefon görüşmelerini dinlemeye yönelen NSA, zamanla uydu teknolojisinin gelişmesiyle birlikte yer küreyi de gözetler hale gelmiştir. Günümüzde, en gelişmiş teknolojiler ile en yetkin uzman kadrosuna sahip olan NSA, enformatik gözetim açısından doruk noktasını oluşturmaktadır. Bu kurumlar ve kullandıklarını ileri teknoloji yoluyla Sovyet Bloğunun gözetim alına alınmasında ilk adım U-2 uçakları olmuştur. 1960'larda ise, teknolojinin kazandığı ivmeye paralel olarak ortaya çıkan 'yönlü telsiz haberleşmesi' aracılığıyla uydu teknolojiler, radyo sinyallerinin büyük kısmının havadan gönderilmesine yol açmış; uluslararası haberleşmeler de, fiber optik-koaksiyel kablolar yoluyla uydular üzerinden gerçekleşmeye başlamıştır. Enformasyon teknolojilerindeki gelişmelere bağlı olarak NSA, arka arkaya fırlattığı dinleme uyduları Doğu Bloku'nun telsiz haberleşmeleri ile sivil telefon görüşmelerini tümüyle denetim altına almış ve 1990'larda dünyanın çevresinde yüzlerce dinleme uydusu dönmeye başlamıştır. İlk aşamada askeri amaçlı olan bu gözetleme uyduları, daha sonra yatak odalarını bile gözetler hala gelirken; uluslararası telefon/faks/teleks gibi veri bağlantıları, uydu ve bilgisayarlarla sürekli taranır olmuştur (Egmont Koch'tan aktaran Dolgun, 2005: 123, 124).

ABD, 11 Eylül 2001 tarihinde 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. Bu uygulama karşısında, ülkedeki sivil toplum kuruluşlarıyla bazı gazeteciler *"mahremiyetlerin ihlal edildiği ve kişisel yaşamın tecavüze uğradığı"* gerekçesiyle protestolarda bulundularsa da, hükûmeti bu uygulamalardan vazgeçirmek mümkün olmadı (Dolgun, 2005: 147).

Yukarıda değindiğimiz NSA'in gözetim faaliyetleri o kadar ileri gitmiştir ki; NSA'in bu tip gözetim ve denetim faaliyetleri bir parodi olarak 2013 yılının sonunda Ubisoft firması tarafından çıkarılan ünlü bilgisayar oyunu Watch_Dogs'da konu edilmiştir (tr.wikipedia.org). Bu bilgisayar oyununda, oyunun başkahramanı olan Aiden Pearce ünlü bir bilgisayar korsanıdır ve NSA'in ABD genelinde kurduğu gözetim sistemine müdahale edip oyunun bazı görevlerinde Chicago'nun gözetim altyapısını çökertmektedir. Ayrıca bu bilgisayar oyununda Aiden Pearce'ın hükûmet tarafından kurulan gözetim sistemine gizlice girerek sıradan insanların yatak odalarını, salonlarını ve oturma odalarına, kısaca sıradan yaşamlarını gözetlediğini ve dinlediğini görmekteyiz. Bu bilgisayar oyununda NSA'in yaptığı gözetim faaliyetleri kara mizah öğeleriyle birleştirilerek abartılı bir şekilde oyuna uyarlanmıştır.

3.1.4.1. Siber uzayda devlet ile hükûmetler tarafından yapılan gözetime ve denetime teknolojinin sağladığı katkılar

Günümüzde devlet uydu, cep telefonu, istihbarat, güvenlik kameraları, kredi kartları ve banka hesapları, biyometrik sistemler üzerinden kişisel veri toplamaktadır. Bu araçların

üzerine gelişen bilişim teknolojisi sayesinde çok ileri bir seviyeye ulaşan bilgisayarlar ve internet üzerinden toplanan veriler de eklenmiştir.

Yukarıda özetlediğimiz araçlar üzerinden ve çevrimiçi ortam aracılığı ile elde edilen kişisel bilgiler çeşitli yöntemlerle toplanıp veritabanlarına aktarılmakta ve bu bilgilerin birleştirilmesiyle kişisel profiller ortaya çıkmaktadır. Kişisel profilin halk dilinde yaygın olan adı 'fişleme'dir. Bu bağlamda ülkelerin genellikle kendi anayasalarına bile aykırı olan kişisel veri toplama yöntemlerinin gizlice kullanılması internet güvenliği ve çevrimiçi gizlilik anlamında çok büyük ihlallere yol açmaktadır.

Bilişim dünyasında kişisel veri toplamak için birçok yöntemler kullanılmaktadır. Bu veri toplama yöntemleri çok çeşitlidir ve yalnızca devlete özgü değildir. Pazarlama amaçlı kişisel bilgileri satan şirketler ve bilgisayar korsanları da aynı veri toplama tekniklerini kullanmaktadır. Bunun nedeni bu veri toplama tekniklerinin iktidarlar tarafından değil de bilişimin kendi içindeki dinamikler tarafından icat edilmiş olmasıdır. Kısacası bu yöntemlerin bazıları aynı anda hem devlete, hem özel sektöre hem de bilgisayar korsanlarına hizmet eder. Burada üzerinde durulması gereken temel nokta, yukarıda bahsettiğimiz devlet, özel sektör ve bilgisayar korsanları gibi unsurların bu teknolojilere erişebilme yetkinliğine sahip olup olmamasıdır. Kimi ülkeler son zamanlarda iletişim ortamları üzerinden denetim ve gözetim yapabilmek için askeri harcamalarını kısıp, askeri bütçenin bir kısmını bu alanlara kaydırmaktadır. Bu bağlamda ABD, Rusya, Çin ve bazı Avrupa ülkeleri bu tür teknolojilere sahipken; örneğin Afrika kıtasındaki fakir ülkeler, ekonomik güçten yoksun olduklarından dolayı bu tür teknolojilere ulaşmak için yatırım yapamamaktadır.

Devletin çevrimiçi ortamda kişisel bilgileri toplamasını sağlayan yöntemler şu şekilde sıralanabilir:

- E-devlet ve nüfus kayıt sistemleri gibi devlet kurumlarında kişilerin kendi elleriyle girdiği veriler
- Bankacılık işlemleri ve kredi kartları üzerinden yapılan işlemler
- Özel sektördeki harcamalarımız (neyi ne zaman, kaça, nereden aldık). Bu tür bilgiler düzenli olarak devlete aktarılır
- Kişilerin internet sitelerini ziyaret ettiklerinde hard disklerinde tutulan çerezler (cookies)
- İnternette dolaşıldığı sırada kişinin her türlü faaliyetini analiz etmeyi sağlayan DPI (Derin Paket Analizi) sistemi (Çalışmamızın sonraki bölümünde detaylı olarak ele alınacaktır)
- Spyware olarak adlandırılan casus yazılımlar. Bunlar genellikle internetten indirdiğimiz herhangi bir programın içine gizlenirler
- Truva atları ve virüsler
- Sosyal medya ve diğer internet sitelerinin devletlerle paylaştığı kişisel bilgiler, yazışma kayıtları, fotoğraf ve videolar
- Her türlü internet sitesi ve sosyal medyada kendi elimizle girdiğimiz bilgiler ve profillerimiz (Din, ilişki, okunan kitaplar, beğeniler, tutulan takım vs.)
- İnternet sinyallerini ileten ve ağ dolaşımını sağlayan optik kablolar. (Bu kablolar üzerinden her türlü izleme ve dinleme yapılabilir)
- Cep telefonu ve tablet bilgisayarlar aracılığı ile indirilen çeşitli uygulamaların (application) sağladığı veriler
- Bilgisayar, tablet bilgisayar ve akıllı cep telefonlarında kullanılan Microsoft Windows, Apple IOS, Mac OS ve Google Android gibi işletim sistemlerinin bıraktığı arka kapılar
- Google'ın uydu harita sistemi ve Google Street View
- GSM operatörlerinin sağladığı veriler

- Yüz tanıma gibi biyoteknolojik imkânlar.

Yukarıda tek tek sıraladığımız yöntemlerin çokluğundan anlaşılacağı üzere, çevrimiçi ortamlar iktidarı elinde bulunduran devlete, denetim ve gözetim yapılmasını sağlayacak sayısız fırsat sunmaktadır. Bu fırsatlar sayesinde devlet istediği zaman istediği veriye ulaşabilmektedir. Çalışmamızın sonraki bölümünde Amerikan Ulusal Güvenlik Dairesi (NSA)'nin teknoloji sayesinde gerçekleştirdiği gözetimlere, eski NSA çalışanı Edward Snowden'in açıklamaları ışığında yer vereceğiz.

3.1.5. ABD Tarafından Gerçekleştirilen İhlaller

6 Haziran 2013 tarihinde The Guardian adlı gazetede yayımlanan bir haber dünyada büyük bir etki yaratmıştır. Haber Edward Snowden[4] isimli eski bir Amerikan Güvenlik

[4] Edward Joseph Snowden 21 Haziran 1983 yılında Amerika'da doğmuş, Amerikalı bilgisayar uzmanı ve sistem yöneticisidir. Snowden geçmişte Amerikan Merkezi İstihbarat Teşkilatı (CIA) ve Amerikan Ulusal Güvenlik Dairesi (NSA) adına çalışmıştır. Gizli NSA belgelerini medyaya ifşa ederek NSA tarafından yürütülen küresel izleme aletlerinin işletme detaylarını, Beş Göz ortaklarını ve birçok ticari ve uluslararası ortağı ortaya çıkaran NSA sızıntılarını başlatmıştır (tr.wikipedia.org).

Edward Snowden kendisini kurduğu internet sitesinde "Amerikan Güvenlik Dairesi için anlaşmalar yapan bir eski çalışan ve ihbarcı" olarak tanıtmıştır. 200 bin dolar maaş karşılığında çalışmasına rağmen Amerika/Hawaii'deki evini Mayıs 2013'te terk etmiş ve Hong Kong'a giderek gizli belgeleri gazeteci Allen Hamilton'a ulaştırmış ve bu belgelerin basın yoluyla sızmasını sağlamıştır. Bu gizli belgeler NSA'nın Amerika içinde ve dışında kişisel bilgilerin iletişim araçları üzerinden toplanmasını sağlayan sistemin ve bu sistemin yapabileceklerinin ne olduğunu, bu sistem sayesinde kişisel bilgilerin toplanmaya devam edileceğini açıklamıştır (edwardsnowden.com).

Tüm bu açıklama ve itiraflardan sonra Snowden bir casus, hırsız ve vatan haini olarak suçlanmıştır. Bu nedenle Rusya'ya iltica etmek zorunda kalmıştır. "Bu tür şeylerin yaşandığı bir toplumda yaşamak istemiyorum. Yaptığım ve söylediğim her şeyin kayıt altına alındığı bir dünyada yaşamak da istemiyorum" şeklinde bir açıklama yaparak PRISM adlı programı basına

Dairesi (NSA) çalışanın, NSA'in yaptığı gözetleme ve dinleme faaliyetlerinin ifşası üzerineydi. Haberde NSA'in nasıl gizli bir şekilde milyonlarca telefon abonesinin telefon kayıtlarını günlük olarak topladığını anlatmaktaydı (NSA, 6 Haziran 2013).[5] Yapılan bu haberden sonra tüm gözler Amerikan hükûmetine çevrilirken; kısa bir süre sonra haberlere konu olan itirafların sahibi Edward Snowden'i tüm dünyada konuşulmaya başlandı. Elbette NSA'in yaptığı gözetim faaliyetleri telefon kayıtlarını toplamakla sınırlı değildi. Yapılan bu haberi The Guardian ve The Washington Post'ta yapılan bir seri haber daha izledi. Bu gazetelerde yer alan her bir haber, NSA'in gözetim teknolojilerini nasıl kat kat ileriye taşıdığının bir göstergesiydi. Kısa aralıklarla Edward Snowden'in itirafları üzerine yapılan bu haberler teknoloji dünyasında uzun süre boyunca gündemin ilk sırasında yer alırken; diğer yandan gözetim olgusunun sosyal teori içinde yeniden farklı şekillerde tartışılmasını da beraberinde getirmişti.

Snowden'in gizli belgeleri ifşa etmesi Pentagon evraklarını sızdıran Daniel Ellsberg tarafından ABD tarihindeki en önemli sızıntı olarak nitelendirilmiştir. 5 Haziran 2013'te başlayan bir süreç PRISM, XKeyscore ve Tempora gibi internet izleme programlarının yanında ABD ve Avrupa'nın telefon metadatalarının (görüşme kayıtları) alıkonulmasını ortaya

---

sızdıran Snowden, öncelikle ABD'den sınır dışı edilmiş ve akabinde haftalarca birçok ülkeye siyasi sığınma başvurusu yapmıştır. ABD'nin baskısıyla birçok ülke bu sığınma başvurularına ret yanıtı vermiştir (btnet.com.tr). Daha sonra Venezuela tarafından sığınma talebi kabul edilen Snowden bir müddet sonra Rusya'ya iltica etmiştir ve şu anda Rusya'da "geçici mülteci" statüsünde yaşamaktadır.

[5] NSA ile ilgili çıkan tüm haberlere http://www.theguardian.com/world/ interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 bağlantısı üzerinden İngilizce olarak ulaşılabilir. Bağlantıda Edward Snowden ile yapılan detaylı röportajlar mevcuttur. Sitede yer alan haberlerin hepsi bu konuda uzman olan gazetecilerin derinlemesine yaptığı haberlerdir. Birçok önemli bilim adamı, teknoloji uzmanı ve gazetecinin konuyla ilgili analizleri/açıklamaları okunabilir.

çıkardı. Raporlar, Snowden'in NSA çalışanı Booz Allen Hamilton için çalışırken The Guardian ve The Washington Post'a sızdırdığı belgelere dayanmaktadır. Kasım 2013'e kadar The Guardian belgelerin yüzde birini yayımladı (tr.wikipedia.org).

Bu bölümde "devlet" tarafından "gözetim" ve "izleme" yoluyla gerçekleştirilen çevrimiçi gizlilik ihlallerini ve özelde NSA'in genelde Amerikan hükûmetinin gerçekleştirdiği gözetim faaliyetlerini Edward Snowden'in itirafları ve açıklamaları doğrultusunda ele alacağız.

3.1.5.1. Prism

Edward Snowden itiraflarında ve sızdırdığı belgelerde PRISM adlı bir sistemden bahsetmektedir. Bu sistem çeşitli internet sitelerinden toplanan verilerin depolandığı veri tabanlarından biridir.

PRISM, internette en çok kullandığımız servislerin veri tabanlarına bağlı olan bir sistemdir. Snowden'ın sızdırdığı belgelere göre PRISM'e dâhil olan şirketler; Google, Facebook, Microsoft, Apple, Yahoo, AOL, Verizon, Sprint ve AT&T'dir. Bu şirketlerin sisteme dâhil olarak yaptıklarıysa bize ait tüm kişisel bilgilerin PRISM veri tabanına eklenmesine izin vermektir. Bunu nasıl sağladıkları konusundaki teknik detaylar net olmasa da, kesin olarak tüm kişisel bilgilerimizin PRISM'e eklenebildiği bilinmektedir. Bu bilgilerin içerisine özel mesajlaşmalarımız, telefon konuşmalarımız, yazılı-sesli-görüntülü sohbet kayıtlarımız ve bu ağlara verdiğimiz her türlü bilgi dâhildir.

PRISM bilgileri iki farklı şekilde alabilmektedir; içerik ve metadata. İçerik şeklinde aldıkları kullanıcıların direkt olarak internette gördüğü halleridir. Yüklediğimiz tüm fotoğraflar ve videolara, yazdığımız tüm kelimeler gibi. Bunlar her türlü arama sistemiyle incelenebilir ve kullanılabilir olmaktadır.

Örneğin tüm sohbet kayıtlarını alıp içerisinde "tehlikeli kelime" araması yaparak kişilere karşı delil olarak kullanma şansları olmaktadır. Aynı şekilde fotoğraf ve videolarda şüphelilerin yüzlerini arayıp bulduklarında (ya da bulduklarını düşündüklerinde) kişileri onlarla ilişkilendirebilmektedirler. Metadata ise şahıslar tarafından yapılan tüm paylaşımların içerik dışında kalan kısmıdır. Datayı gönderenin ve alıcının kim olduğu, ne zaman ve nereden gönderdiği, alıcının ne zaman ve nerede aldığı gibi. Gönderilen metadataları bir yığın hâline getirip analiz ederek ulaşabilecekleriyse çok daha korkutucu bir hal alabilmektedir. Mesela en çok kimlerle iletişim kurulduğu hangi yolla iletişim kurulduğu, hangi saatlerde iletişim kurulduğu gibi. Bunların bir araya getirilmesiyle kişilerin çevresindeki herkesle olan ilişkinin oldukça detaylı bir haritasına sahip olmak mümkündür (yenimedya.wordpress.com).

Snowden'in PRISM üzerine yaptığı açıklamalardan sonra ABD yönetimi ve Obama bu projeyi sahiplenmiş ve yalnızca yabancıların dinlendiğini/izlendiğini iddia etmiştir. Böylelikle ABD'nin yaptığı bu tür insan hakları ihlallerine meşruluk kazandırılmıştır. ABD yasalarına göre ABD vatandaşı olmayanlara karşı yapılacak bu tarz istihbarat, mahrem verilere izinsiz erişme girişimleri yasadışı kabul edilmiyor (terramedusa.com).

3.1.5.2. Xkeyscore

Xkeyscore, NSA tarafından geliştirilen ve kullanılan bir küresel veri izleme programdır. Bu program sayesinde epostalar, çevrimiçi sohbetler ve internet geçmişi analiz edilebilmektedir. Snowden bu programın sahip olduğu yetenekler sayesinde, herhangi bir kişinin sadece kişisel e-posta adresini bilmenin bile tüm bilgilere ulaşabilmek için yeterli olacağını ifade etmiştir.

NSA'in elindeki e-posta sayesinde izlenen internet kullanıcısının isim, telefon numarası, IP adresi, anahtar kelimeler, internet tarayıcısı veya kullanılan dil gibi bütün verileri çok net bir şekilde takip edebilmektedir. İzlemelerin hiçbir yasal dayanağı olmadığı da Snowden'in yaydığı belgelerde açıkça görülmüştür.

Snowden'in yayınladığı belgelerde, ABD Ulusal Güvenlik Kurumu NSA'nın "XKeyscore" programı vasıtasıyla 2012 yılında 30 günlük bir zaman dilimi içinde 41 milyar veriyi topladığı açıklandı. 2008 yılında XKeyscore'un akıllı sistemini kullanarak 300 teröristin yakalandığı belirtildi.

Dünya genelinde 180 noktada "XKeyscore" programını destekleyen yaklaşık 700 sunucunun olduğu ve söz konusu sunucuların özellikle Avrupa ve Orta Doğu'ya yerleştirildiği de ortaya çıktı. Guardian gazetesi, 700 sunucunun yerleştirildiği 180 noktayı dünya haritası üzerinde yayınladı. "XKeyscore" programını destekleyen sunucunun en yoğun olduğu noktalardan birinin de Türkiye olduğu görülmüştür (btnet.com.tr).

3.1.5.3. Tempora

Snowden'e göre "Tempora" adı verilen sistem PRISM'in İngiltere'de faaliyet gösteren sürümüdür. Bu program tıpkı PRISM gibi internetteki her türlü veriyi ve telefon görüşmelerinin metadatalarını toplamaktadır. Snowden'in iddialarına göre Tempora aslında PRISM'den kat kat fazla veri toplamaktadır.

Snowden'in açıklamalarına göre Tempora her gün 200 fiber optik kablo aracılığıyla 600 milyon telefon görüşmesini kaydederek 1 ay boyunca saklanmaktadır. Saklanan veriler daha sonra aynı programla analiz edilmektedir. Takip edilen internet içerikleri arasında ise PRISM'de olduğu gibi,

kullanıcıların e-postaları, internet aramaları ve Facebook hesapları gibi kişisel bilgi ve işlemleri bulunmaktadır.

PRISM ve Tempora, hem ABD ve İngiltere açısından şüpheli olan şahısların hem de bütün internet kullanıcılarının kişisel bilgilerini takip etmektedir. Tempora'nın elde ettiği bilgiler gerekirse ABD'deki 850 bin çalışanı olan Ulusal Güvenlik Dairesi (NSA) ile de paylaşılmaktadır (dunyabulteni.net).

3.1.5.4. NSA'in arkadaş listelerini toplaması ve dünya liderlerini dinlemesi

14 Ekim 2013 tarihinde The Washington Post gazetesinde yayınlanan bir habere göre NSA aralarında Amerikalıların ve diğer dünya ülkeleri vatandaşlarının bulunduğu milyonlarca kişinin arkadaş listesini eposta hizmetleri ve sohbet uygulamaları üzerinden topladığı ortaya çıkmıştır. Bu sayede NSA küresel bir bilgi ağına ulaşabilmektedir (arstechnica.com).

Yine bir başka haber NSA'nın, aralarında G-20 ülkeleri arasında yer alan dünya liderlerinin telefonlarını dinleyip veri topladığını ortaya çıkarmıştır. Almanya başbakanı Angela Merkel'in de dinlendiği ortaya çıkınca, Almanya hükûmeti bu durumdan çok rahatsız olup sert bir açıklama yapmıştır (zdnet.com).

3.1.5.5. NSA'nın Google veri merkezlerine sızması

30 Ekim 2013 tarihli yine Edward Snowden'in açıklamalarıyla yapılan The Washington Post haberine göre, NSA Google'ın veri merkezlerinin bağlı olduğu hatlara girdiğini ortaya koymuştur. Haberde NSA'in bir şekilde bu kablolara sızıp bilgi topladığı belirtilmiştir. (washingtonpost.com)

3.1.5.6. Gemalto isimli simkart üreticisi firmanın hacklenmesi

Snowden'in iddialarına göre dünyanın en büyük simkart üretici firmalarından biri olan Gemalto, 2010 ile 2011 yılları arasında NSA tarafından hacklenmiştir. Firma yetkilileri yaptıkları açıklamada bu iddiaların doğru olduğunu ve hacklendiklerini kabul etmiş; fakat kripto anahtarlarının çalınamadığının, bu durumun da müşterilerin güvenliğini etkilemeyeceğini ve mağduriyet yaratmayacağını ifade etmişlerdir (wired.com).

Edward Snowden ise, firma yetkililerinin aksine Gemalto'nun hacklendiği sırada bütün kripto anahtarlarının NSA tarafından ele geçirildiğini ve 85 ülkeden 400 GSM operatörünün kullandığı hackli (kırılmış) bu milyonlarca simkartın değişmeden güvenlik tehlikesinin ortadan kalkmayacağını söylemiştir. Snowden'e göre NSA'in sahip olduğu bu anahtarlar sayesinde NSA cep telefonlarımıza anında sızabilmektedir ve havadaki konuşmalarımızı dahi dinleyebilmektedir (wired.com).

3.1.5.7. NSA'in mobil uygulamalar üzerinden cep telefonlarına sızma girişimi

Edward Snowden'in sızdırdığı gizli belgeye göre NSA 2011 ile 2012 yılları arasında Google Playstore, Samsung App Store ve Çin ile Hindistan'da popüler olan UC Browser isimli internet tarayıcısına sızma girişimlerinde bulunmuştur. Bu sızma girişimlerinden milyonlarca kullanıcının etkilendiği belirtilmiştir. Samsung ve Google bu konuda açıklama yapmasa da, Apple, Google ve Microsoft gibi firmalar güvenlik uygulamalarını değiştirmiş, uygulamalarında iki aşamalı güvenlik sistemine geçiş yapmış ve şifreleme algoritmasını değiştirmişlerdir. NSA, bunun üzerine Apple'ı teröristler için telefon üretmekle suçlamıştır (firstlook.org).

3.1.5.8. NSA'nın CISCO markalı modemlere böcek yerleştirmesi

14 Mayıs 2014'te Arstechnica isimli teknoloji sitesinde yapılan haberde NSA'nın Cisco marka routerlara (yönlendirici modem) böcek eklediğiyle ilgili fotoğraflar yayınlanmıştır (arstechnica.com).

Habere göre NSA. Cisco'nun ürettiği ürünlerin fabrika çıkışından sonra sevkiyatını durdurup bütün modemleri tek tek söküp, modemlerin içerisine gizli bir şekilde bilgi kaydı yapılmasını sağlayan bir araç olan böcek yerleştirmiştir. NSA modemlerin içine bilgi kaydetmeye yarayan aracı yerleştirdikten sonra bütün modemleri paketleyip kutularına geri yerleştirip, modemlerin sevkiyatını devam ettirmiştir. Haberde ilgi çeken bir diğer ayrıntı ise çevrimiçi gizliliğimizin ne kadar tehlikede olduğunu gözler önüne sermiştir. Habere göre, NSA diğer ülkelerle iş yapan Amerikan şirketleriyle zor ya da rıza yoluyla ikna edip, üretilen ürünlerin içerisine bilgi kaydetme işlevi gören küçük araçlar yerleştirmiştir. Böylece Amerika'ya diğer ülkelerdeki veri akışını gözetlemek için yeni imkânların yolu açılmıştır. Haberde bu böceklerin gizli bir şekilde verileri kaydedip, verileri müşterilerin ruhu duymadan NSA'in veri tabanlarına aktardığı belirtilmiştir.

NSA'in yürüttüğü bu izleme ve gözlemleme faaliyetlerine karşı internet üzerinde sesler yükselmiş ve büyük kampanyalar yürütülmüştür. Bu kampanyalardan biri de önemli yazılım geliştirme vakıflarından biri olan Mozilla'nın internet sitesinde yürüttüğü imza kampanyasıdır. Mozilla kampanyaya "Stop Watching Us" (Bizi İzlemeyi Bırak) adını vermiştir. Mozilla kampanyada Amerikan hükûmetine verilmek üzere 500 milyon imza toplamayı hedeflemektedir. Ayrıca Mozilla, Amerikan hükûmetine karşı bir açık mektup da yayınlamıştır (optin.stopwatching.us).

3.1.6. Türkiye'de NSA benzeri uygulamalar

Çalışmamızın önceki bölümünde ele aldığımız Edward Snowden'in açıklamaları, itirafları ve yayınladığı belgelerden sonra gözler ülkemize çevrilmişti. Sonuçta Snowden'in açıkladığı belgelerin içerisinde Türkiye'nin izlendiği gerçeği de vardı. Böylece ülkemizde de bu tür uygulamaların olup olmadığı hakkında insanların kafasında soru işaretleri oluşurken, gazeteciler bu konuyu incelemeye aldılar ve Snowden'in yaptığı açıklamalardan bir müddet sonra ülkemizde de bu tür bir uygulama olduğu hakkında spekülasyonlar üst üste geldi. Bu spekülasyonların doğruluğu hakkında kimsenin elinde ciddi bir bilgi olmasa da, Taraf gazetesi yazarı Mehmet Baransu 2013 yılının Haziran ayında kendi gazetesinde bu tür iddiaların yer aldığı belgeli bir haber yaptı.

Mehmet Baransu, haberinde Amerika'da NSA'nın yaptığı uygulamalara çok benzeyen uygulamaların ülkemizde MİT (Milli İstihbarat Teşkilatı) ayağıyla gerçekleştirildiğini iddia ediyordu:

> *Türk Hava Yolları'yla uçan vatandaşlar, Milli Eğitim Bakanlığı'na bağlı kurumlarda okuyan öğrenci ve ailelerinin tüm özel bilgileri, attıkları mailler artık MİT'te. Maillerimizden telefonlarımıza, fotoğraflarımızdan aldığımız puanlara, telefon bilgilerimizden aile ve yakınlarımızın özel hayatına varıncaya kadar tüm bilgiler "Çok Gizli" damgalı bir protokolle MİT'e aktarılıyordu. Anayasa'ya ve Türk Ceza Kanunları'na göre yapılan suç. Buna rağmen "Çok Gizli" damgalı protokol gizlice hayata geçirilmişti.*
>
> *MİT, 2012 yılında, vatandaşların kişisel bilgilerine ulaşmak için Türk Hava Yolları ve Milli Eğitim Bakanlığı ile bir dizi görüşme gerçekleştirdi. Görüşmeler neticesinde her iki kurumdan da detaylı şahıs bilgilerinin düzenli olarak MİT'e aktarılmasına karar verildi. Konuyla ilgili MİT'te sistem kuruldu. Yapılan mutabakat sonucu, Türk Hava Yolları, yurt içi tüm yolcu ve seyahat bilgilerini, kişinin yanında seyahat ettiği şahısların*

kim olduğunu, aktarma, yurtiçi bağlantılı tüm yurtdışı yolcu seyahat ve bilgilerini MİT'e vermeye başladı. Milli Eğitim Bakanlığı yetkilileriyle yapılan görüşmelerde ise ilk ve orta dereceli okullar ile özel kolejlerde çalışan idareci, öğretmen ve diğer tüm personelin, okuyan tüm öğrencilerin bilgileri, notları, velilere ait özel ve tüm bilgiler, telefon numaraları, mailler de MİT'e verilmeye başlandı (bilgicagi.com).

Baransu'ya göre MİT'in yaptığı bu çalışmayla, THY ile seyahat edenler, postanede işlem yapanlar, tapuda kayıtları olanlar, Milli Eğitim'e bağlı kurumlarda okuyan öğrenciler, potansiyel suçlu kabul edilip fişleniyordu. Bununla da yetinilmeyip, ailelerin bilgileri, evden velilerin MEB'in internetine girdiği kişisel bilgisayarlara ulaşım, öğrencilerin arkadaşlarının fotoğrafları ve yüzlerce bilgi MİT'in kontrolüne verilmişti. Bu bilgiler MİT'te toplanıp, arşivleniyordu.

MİT'in gerçekleştirdiği bu çalışma açık bir şekilde özel hayatın gizliliğine müdahale ediyor ve kişisel veriler kişilerin rızası olmadan arşivleniyordu.

3.2. Pazarlama ve Reklam Şirketleri

İnternet güvenliği ve çevrimiçi gizliliği ihlal eden unsurlar arasında pazarlama şirketleri önemli yer tutmaktadır. Bu tür şirketler çeşitli veri toplama teknikleri kullanarak çevrimiçi ortamda bulunan her türlü kişisel verimizi gizli bir şekilde veritabanlarına kaydetmektedirler. Toplanan bu veriler daha sonra reklam faaliyetleri gerçekleştirmek üzere reklam şirketlerine satılmakta veya verileri toplayan bu şirketler bizzat kendileri bu verileri reklam amaçlı kullanmaktadırlar.

İnternet kullanımının günden güne artmasıyla birlikte internet üzerindeki pazarlama ve reklamcılık faaliyetleri de önem kazanmış, Amazon ve eBay gibi büyük alışveriş siteleri ortaya çıkmıştır. Bu tür alışveriş sitelerinin reklamları gezindiğimiz her türlü internet sitesinde karşımıza çıkmaya

başlamıştır. Ne tesadüftür ki internet sitelerinde ve sosyal medyada karşımıza çıkan reklamların çoğu direkt olarak ilgi alanlarımızı ve beğenilerimizi hedef almaktadır. Peki, nasıl olabilir de bu reklamlar bizim ilgi alanlarımızı ve beğenilerimizi hedef alabilmektedir? Reklam şirketleri bizim neyi ne kadar beğendiğimizi nasıl bilebilmektedir? Sorunun cevabı tamamen bu cümlede gizlidir: "Çevrimiçi davranışsal reklamcılık". Reklam sektöründe aynı zamanda "hedefli reklamcılık" ve "veritabanlı reklamcılık" gibi isimlerle de anılan çevrimiçi davranışsal reklamcılık günümüzde reklam sektörünün internetteki en güçlü ayağını oluşturmaktadır.

Biz bu bölümde pazarlama şirketlerinin internet güvenliğimizi ve çevrimiçi gizliliğimizi hiçe sayarak gerçekleştirdiği çevrimiçi davranışsal reklamcılık faaliyetlerini, bu faaliyetler gerçekleştirilirken kullanılan veri toplama tekniklerini ve bu tekniklerle ilişkili kavramları; çevrimiçi davranışsal reklamcılığın dünyada ve ülkemizde nasıl işlediğini ele alacağız.

3.2.1. Yeni bir gözetim pratiği: çevrimiçi davranışsal reklamcılık

Tek kutuplu kalan dünyada kapitalist sistemin belirleyici bir güç haline gelmesi ve küresel nitelikteki ekonomik yapıyı kendi kuralları içerisinde dayatmaya başlaması, bir taraftan keskin bir rekabet ortamını gündeme getirirken, diğer taraftan da istihbarat faaliyetlerinin yönünü değiştirmiştir. Bu anlamda, kapitalist sistem ile gözetim faaliyetleri arasında yeni bir ilişkisellik ortaya çıkmıştır. Gözetim etkinlikleri, 'global ölçekte' hükûmetler ve istihbarat servisleri yoluyla diğer ülkelerdeki büyük şirketler üzerine odaklanırken; 'bireysel ölçekte' de, kişilere ait tüketim profillerinin oluşturulması amacıyla iç piyasalara yönelmiştir (Dolgun, 2005: 235).

İşte yukarıda adı geçen bu "tüketim profilleri oluşturmanın" günümüzdeki en büyük karşılığı bugün önemli bir

pazarlama faaliyeti olan ve internet reklamcılığının bir alt türünü oluşturan "Çevrimiçi davranışsal reklamcılık"tır. 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. Örneğin, bir tüketici bazı ürünleri ve hizmetleri çevrimiçi ortamda gözden geçirirken, firmalar aynı zamanda bir internet sitesinin sahibi olabilir ve bu internet sitesini yönetebilir. Firmaların sahip olduğu ve yönettiği bu internet siteleri tüketicilerin arama sırasında yazdıkları kelimeleri, bu kelimelerin yazıldığı dili ve tüketicinin ziyaret ettiği diğer sitelerin bilgilerini toplayabilirler, ayrıca bu bilgileri üçüncü parti kuruluşlarla paylaşabilirler. Aynı zamanda Facebook gibi birçok sosyal ağ kullanıcılarına haber vermeksizin kullanıcılarının kişisel verilerini toplamakta ve reklam şirketleriyle paylaşmaktadır. (Juan Martinez ve diğerlerinden aktaran Cox ve Cline, 2012).

Çevrimiçi davranışsal reklamcılığın nasıl işlediğini bazı senaryolar ortaya atarak ele alacak olursak: Felsefeye meraklı olan bir internet kullanıcısı çevrimiçi ortamda arama motorlarını kullanarak Google üzerinden bazı felsefecilerin isimlerini aratır veya bu kullanıcı ünlü bir felsefecinin herhangi bir kitabını almak için kitap satan internet sitelerini belirli aralıklarla ziyaret eder. Çevrimiçi davranışsal reklamcılık bu noktada devreye girer; "Derin Paket Analizi" ve çerezler (cookies) gibi teknikleri kullanarak kullanıcının yaptığı aramalarda girdiği kelimeler, ziyaret ettiği internet siteleri ve diğer kullanım bilgileri kaydedilir. Böylece kullanıcının ilgi alanı belirlenmiş olur. Daha sonra kullanıcı herhangi bir internet sitesini ziyaret ettiğinde, ziyaret edilen sitede bulunan reklamlarda kendi ilgi alanı olan "felsefe" ile ilgili reklamlar görür.

Bu senaryolar hemen hemen her türlü ilgi alanları için türetilebilirler. Örneğin; bilgisayar oyunlarıyla ilgilenen bir kullanıcının önüne yine bilgisayar oyunlarıyla ilgili reklamlar çıkacaktır. Bu senaryolar tamamen kullanıcının belirli aralıklarla yaptığı aramalar, ziyaret ettiği internet siteleri ve bu siteleri kullanımıyla ilgili bilgilerin arka planda gizli olarak toplanması ve analiz edilmesinden sonra karşısına çıkarılan kişiye özel reklamlardan oluşur. Bu bağlamda günümüzde çevrimiçi ortamda bulunan insan unsuru, pazarlama şirketleri tarafından gözlemlenerek beğenileri ve ilgi alanları belirlendikten sonra onu potansiyel bir tüketici haline getirilip ürün veya hizmet alması sağlanır.

Çevrimiçi davranışsal reklamcılığa bazı kaynaklarda "veritabanlı pazarlama" adı verilmektedir. Veritabanlı pazarlama; müşterilerin demografik, sosyal, ekonomik vb. verileriyle, satın alma davranışlarına yönelik verilerin, bilgi teknolojileri aracılığı ile takibi, işlenmesi ve analiz edilmesi sonucunda geliştirilen pazarlama çabalarıdır (Verhoef'ten aktaran Haşıloğlu ve diğerleri, 2008).

Günümüzde başını Google, Yahoo ve Bing gibi arama motorları, Facebook gibi sosyal ağlar ve Amazon.com gibi büyük alışveriş sitelerinin çektiği birçok önemli firma çevrimiçi davranışsal reklamcılık ve veritabanlı pazarlama faaliyetleri amacıyla kullanıcıların kişisel verilerini izinsiz bir şekilde toplamaktadır.

Sosyal teoride bu tür pazarlama faaliyetlerinin ve izinsiz şekilde veri toplanmasının ne kadar etik olduğu konusunda sorular sorulmakta, gerçekleştirilen bu faaliyetler gözetim kategorisi altında değerlendirilmekte ve uzun süredir tartışılmaktadır. Nitekim, Zygmunt Bauman ve David Lyon (2013), Akışkan Gözetim isimli kitaplarında veritabanlı pazarlama ve çevrimiçi davranışsal reklamcılığın internetin süperpanoptik yapısından çok iyi bir şekilde yararlandığını belirtmiş ve

dünyanın en büyük alışveriş sitelerinden biri olan Amazon.com'u, şu cümlelerle eleştirmişlerdir:

> *…Müşterilerin profillerine göre yan yana konması, sınıflandırılması ve farklı kategorilerdeki tüketicilere farklı davranılması amacıyla yine büyük ölçekte kişisel veri toplamaya dayalı olarak işleyen detaylı bir yönetim görüyoruz. Amazon.com'un "katılımcı filtreleme" teknikleri sayesinde, bakmakta olduğumuz bir kitabı bizden önce alan kişinin diğer aldığı kitapları söylemesinin bazıları için ne büyük bir nimet olduğunu düşünün. Her işlem kendisiyle ilgili, sonraki müşteri seçimlerine rehberlik etmekte kullanılacak bilgiler üretir ….Ama işler bununla da sınırlı kalmaz; Wish List tüketicilerin kendi kendilerini yönetmelerine, diğerlerine belli bir yüzlerini göstermelerine fırsat verir. Görünen o ki, Amazon.com müşterilerini kendi aralarında süregiden ilişkiler vasıtasıyla ve ayrıca onlara izlenim yönetiminde pay sahibi olmanın zevkini tattırma yoluyla yönetmeyi başarıyor. Sonuçta Amazon.com ihtiyaç duyduğu veriyi elde eder ve müşterilerini Eli Pariser'in etkileyici bir şekilde adlandırdığı üzere "filtre baloncuğu"nun içinde mutlu mesut yaşamaya terk eder. Google'da aynı sözcüğü arayan farklı insanların karşısına farklı sonuçlar çıktığı gayet iyi biliniyor. Bunun sebebi Google'ın arama sonuçlarını daha önceki aramalarınıza bakarak geliştirmesidir. Benzer bir şekilde çok fazla Facebook arkadaşı olan kişiler, yalnızca Facebook'un arkadaşlarıyla olan etkileşim sıklığına bağlı olarak haber almak isteyeceklerini tahmin ettiği kişilerden güncellemeler alıyorlar. Amazon.com elbette bu modele de uyuyor. Pariser'in buna paralel ve haklı kaygısı ise, "kişiselleştirme filtrelerinin, kendi düşüncelerimizle beynimizi yıkayan, alışıldık şeylere karşı arzumuzu tetikleyen ve bilinmeyenin karanlık ülkesinde gizlenen tehlikelere karşı duyarsızlaştıran bir tür görünmez otopropaganda" olduğudur (Bauman ve Lyon, 2013: 121, 122).*

Bauman ve Lyon'un da aralarında bulunduğu önemli bir akademisyen grubu pazarlama faaliyetlerinin, hükûmetler tarafından gerçekleştirilen gözetim pratiklerinden hiçbir farkının bulunmadığını savunmaktadırlar. Onlara göre nasıl hapishane, tımarhane ve getto gibi panoptik unsurlar insanları kategorize edip 'ban-optikon" mekanizması aracılığıyla birbirinden izole ediyorsa; çevrimiçi davranışsal reklamcılık da izinsiz ve gizli bir şekilde kişisel verileri toplayarak bireyleri gözetime tabi tutup ve toplanan veriler sayesinde bireyleri birer potansiyel tüketici olarak filtrelere ayırmaktadır; işine yaramayacak olanlarla da ilgilenmemektedir. Toplumun büyük bir çoğunluğunun bu tür uygulamalardan haberdar olmaması ise üzerinde durulması gereken başka bir unsuru oluşturmaktadır.

3.2.2. Google ve Facebook'un reklamcılık faaliyetleri

Çevrimiçi davranışsal reklamcılık metodunun birçok büyük firma tarafından kullanıldığı bilinmektedir; fakat bu firmalar içerisinde en büyük olanları şüphesiz dünyanın en önemli arama motoru Google ve en büyük sosyal paylaşım platformu Facebook'tur. Bu bölümde Google ve Facebook'un reklam faaliyetlerini ele alacağız.

3.2.2.1. Google'ın reklamcılık faaliyetleri

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

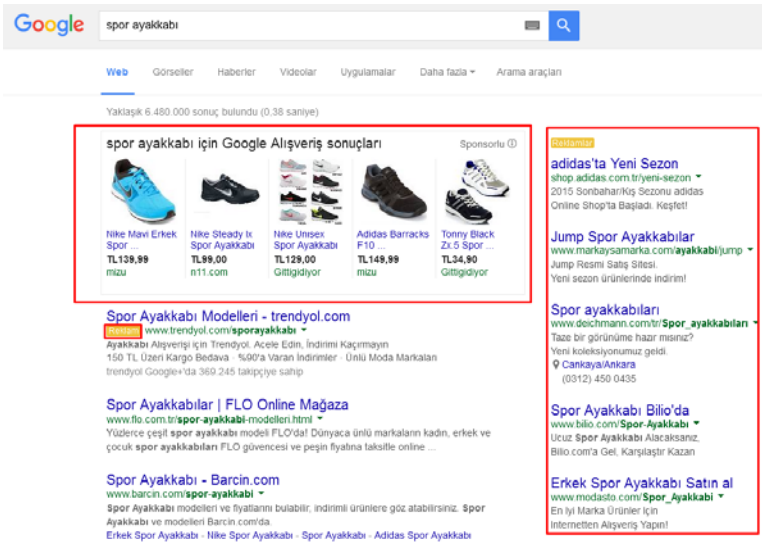
ücretlendirilen reklam, anahtar kelime reklamcılığı terimleriyle de ifade edilmektedir (Arslan, 2013: 50).

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, ABD'deki en büyük internet arama motorudur ve aynı zamanda Avrupa'daki arama pazarını da domine etmektedir. Hâlihazırda uzun süreden beri reklamcılık faaliyetleri gerçekleştiren ve Adwords ile Adsense isimli çok gelişmiş iki arama motoru reklam platformu bulunan Google, 2007 Nisan ayında en büyük getirisini çevrimiçi reklam şirketi "DoubleClick"i 3,1 milyar dolar nakit para karşılığında satın alarak gerçekleştirmiştir. Bu adım ile Google daha büyük bir reklam veren ve reklam gösteren kitlesine kavuşmuş, böylece Google sektördeki rakibi Yahoo'nun önüne geçmiştir. Bu bütünleşme ile medya kuruluşlarının ve reklamcıların aramaları merkezi bir konsol üzerinden yönetmesi sağlanmış, sistem hızı ve hedefli reklamcılığın sonuca ulaşma oranı artmıştır (Zukina, 2015).

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 (en.wikipedia.org). Adwords ile reklam verenler internet sitelerine keywords (anahtar kelimeler) ile ziyaretçi çekmeyi hedeflerler. Bu reklam servisini kullanan reklam verenler bir reklam oluşturup buna bir ya da birkaç anahtar kelime ataması yaparlar. Atanan anahtar

kelime Google'da bir internet kullanıcısı tarafından aratıldığında, reklam veren tarafından oluşturulan reklam arama sonuçlarında üst sırada ya da kenarda görünür. Aramayı gerçekleştiren internet kullanıcısı arama sonuçlarında görüntülenen bu reklama tıklandığında, tıklanılan bağlantı kullanıcıyı reklam verenin ürün ya da hizmet satışı gerçekleştirdiği internet sitesine yönlendirir (Zukina, 2015). Aşağıdaki resimde görüleceği üzere Google'da "spor ayakkabı" kelimesini arattığımızda karşımıza "spor ayakkabı" anahtar kelimesi ile ilişkilendirilmiş reklamlar çıkmaktadır.



Resim 3.1. Google Adwords

Adwords reklam servisi sayesinde reklam verenler sitelerine Arama Motoru Optimizasyonu (SEO) yaptırmadan arama sonuçlarında en üst sıralarda kendilerine yer edinirler. Elbette reklam verenler Adwords'un bu hizmetin karşılığı olarak Google'a tıklama başına ve gösterim başına belirli bir ücret öderler. Ödenen ücret reklam ilişkilendirilen anahtar kelimenin rekabet oranına göre değişkenlik gösterir.

Adwords'un kendi içerisinde çalışma mekanizması farklı olan birçok reklam türü vardır; fakat çalışmamızı asıl ilgilendiren unsur Adwords'tan çok Google'ın diğer reklam platformu Adsense'tir. Google, Adsense hizmetini şu şekilde tanımlamaktadır: "Google AdSense, büyüklükleri ne olursa olsun tüm web sitesi yayıncılarının web sitelerinde hedeflenmiş Google reklamları göstererek para kazanmalarını sağlayan ücretsiz ve kolay bir yöntemdir" (support.google.com). Google Adsense, internet siteleri için milyonlarca reklam veren ve destekleyicinin bulunduğu, internet sitesi sahiplerinin sitelerine reklamlar yerleştirebileceği en büyük reklam sağlayıcısıdır. Bir internet kullanıcısı Google Adsense servisini kullanan bir internet sitesine girdiğinde karşısına daha önce yaptığı arama sonuçlarıyla ilgili reklamlar çıkar. Sistem şu şekilde işler: Bir reklam veren Google'a hangi reklamının görüntüleneceği arama kriterlerini (anahtar kelime), görünecek reklamı ve reklamın tıklandıktan sonra Google'ın alacağı ücret teklifini gönderir. Google ise gerçek zamanlı olarak anahtar kelimeleri "kalite puanı"na göre sıralar ve fiyatlarını belirler. Bu kalite puanı birçok faktöre göre değişkenlik gösterir. En yüksek kalite puanına sahip olan reklam ziyaret edilen internet sitesinde en önce gösterilir. Bir internet sitesi sahibi sitesinde Google Adsense reklamları göstermek istiyorsa bu sisteme dâhil olur; sitesine yazı bazlı ya da banner olarak reklam kodları yerleştirir. Gösterilen reklamların köşesinde "Ads by Google" ibaresi bulunur (Sweeney, 2013). Google'ın reklam yazılımı arama sonuçlarındaki her kelime ve sayfayı tarayıp işler. Böylece bu yazılım, Google'ın reklamları sitelerin içeriğine ve ziyaretçilerin ihtiyaçlarına göre konumlandırmasını sağlamış olur (Kang ve McAllister, 2011).

Örnek olarak, "memurlar.net" internet sitesinde Adsense reklamları barındırılmaktadır. Aşağıdaki resimde görüleceği üzere internet sitesinin sağ, sol ve üst kısımlarında Google Adsense tarafından gösterilen reklam bannerları yer almaktadır.

Resim 3.2. Google Adsense

Resim 3.2'de yer alan reklamlara dikkat ettiğimizde sağda yer alan reklam elektronik eşya satan "Mediamarkt" isimli firmanın reklamıdır. Sitenin üst kısmında bulunan reklam ise Kingston isimli bilgisayar donanımları ve malzemeleri üreten "Kingston" isimli firmanın reklamıdır. Ne tesadüftür ki bu siteyi ziyaret ettiğimiz sırada sürekli olarak teknoloji yayını yapan internet sitelerini ziyaret edip ileride satın almayı düşündüğümüz bilgisayarın bileşenlerini araştırmaktaydık. Dolayısıyla arka planda bizden habersiz olarak kişisel bilgilerimizi ve arama verilerimizi toplayan Google bu verileri işleyip bize ilgi alanlarımızdan biri olan "bilgisayar bileşenleri" ile ilgili reklamlar göstermektedir. Buradan Google'ın reklam yazılımın çok iyi çalışıp bize ilgi alanımıza göre kişiselleştirilmiş reklamlar sunduğunu görüyoruz; fakat bu işin etik olarak son derece tartışmalı bir yaklaşım olduğu su götürmez bir gerçektir.

3.2.2.2. Facebook'un reklamcılık faaliyetleri

İnternette, son yıllarda çevrimiçi toplulukların bir türü olarak sosyal ağ siteleri gittikçe popüler hale gelmiştir. Teknolojinin soğukluğunu internet ortamında insanların bir araya toplanmasıyla ortadan kaldıran sosyal ağ siteleri, geleneksel ortamda insanlar arasında gerçekleşen yüz-yüze iletişimin yarattığı etkinin benzerini sanal ortamda meydana getirmektedir. Her ne kadar geleneksel ortamdaki gibi olmasa da sosyal ağ siteleri farklı bir pazar ortamı ve aslında yeni bir pazarlama iletişimi kanalıdır. Pazarlamacıların henüz keşfetmekte olduğu sosyal ağ siteleri, internet kullanıcıları tarafından çoktan benimsenmiştir. Bunun en önemli nedeni sosyal ağ sitelerinin kullanıcıyı esas alan işbirlikçi bir yapı temelinde kişisel alanlara ve bağlantılara izin vermesidir (Akar, 2010).

Sosyal ağ siteleri, firmaların pazarlama departmanlarında görev yapan yöneticilerin ulaşılmak istenen tüketicilerin tercihlerini, ilgi alanlarını, ihtiyaçlarını ve zevklerini öğrenmesini sağlarlar. Böylece potansiyel tüketicilerin tercihlerine, ilgi alanlarına, ihtiyaçlarına ve zevklerine yönelik etkili reklam olanakları yaratılır. Bu sosyal ağlar içerisinde Facebook kuşkusuz önemli bir yer tutmaktadır.

Sosyal ağ siteleri sadece reklam yapılarını derinden değiştirmekle kalmamış, aynı zamanda geleneksel medya bütçelerinin azaltılmasını da sağlamıştır. Facebook reklamları, kullanıcıların kişisel bilgileri doğrultusunda ana sayfalarında görünmektedir. Kullanıcılar, bu reklamları beğenebilmekte, arkadaşları ile paylaşabilmekte veya bu reklamlara yorum yapabilmektedirler. Böylece, bu reklamlar kullanıcıların ağlarındaki diğer kişilerin de profillerinde görünerek daha geniş kitlelere ulaşabilmektedir (Kazancıoğlu ve diğerleri, 2012).

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). Bu reklamların her birinin gösterim ve tıklama başı ücreti farklı olup, reklam verenin Facebook'a ödeyeceği ücretler reklamın Facebook'ta gösterileceği kitleye göre değişmektedir.[6]

Çalışmamıza Facebook reklamlarını dâhil etmemizin temel amacı, Facebook'un tıpkı Google gibi reklam verenlere kişiye göre özel olarak hazırlanmış reklamlar sunma fırsatını vermesidir. Bu bağlamda Facebook reklamları da çevrimiçi davranışsal reklamcılık kategorisi altındadır. Kullanıcı Facebook reklamlarının hesabındaki sayfada gösterilmesini engelleyemez; fakat içeriğinden rahatsız olduğu bir reklamı şikâyet edebilir. Facebook reklamlarında, kullanıcının Facebook'ta paylaştığı demografik bilgilere göre hedefleme yapılmaktadır. Bunlar; kullanıcının yaşadığı şehir, cinsiyeti, yaşı, ilişki durumu, işyeri veya okul bilgileri gibi kendisi tarafından sisteme girilmiş bilgiler, profilinde veya zaman tünelinde sıraladığı ilgi alanları, bağlantı kurduğu sayfa ve gruplar, ziyaret ettiği sayfalar, gruplar veya kullandığı uygulamalar, kullanıcının gönderileri ve durum güncellemelerindeki anahtar sözcüklerden oluşmaktadır. Facebook bu bilgilere, kullanıcının gönderilerini okumaksızın, otomatik bir sistem ile ulaştığını belirtmektedir. Fakat "Sponsorlu reklam"

[6] Facebook'taki reklam çeşitleri bu çalışmanın asıl konusu olmadığından ve bu çalışmaya sığmayacak kadar Facebook reklam çeşidi bulunduğundan dolayı tüm reklamlara tek tek çalışmamızda yer vermeyeceğiz. Bu reklam çeşitleri detaylı olarak Ayşegül Başer tarafından Marmara Üniversitesi Sosyal Bilimler Enstitüsü bünyesinde hazırlanan "Sosyal Medya Kullanıcılarının Kişilik Özellikleri, Kullanım ve Motivasyonlarının Sosyal Medya Reklamlarına Yönelik Genel Tutumları Üzerindeki Rolü: Facebook Üzerine Bir Araştırma" isimli doktora tezinde ele alınmıştır.

olarak da isimlendirilen bu reklamların etkinliği demografik ve kişisel özellikler ile doğrudan bağlantılıdır (Kara ve Coşkun, 2012). Bu bağlamda tıpkı Google'ın yaptığı gibi kişisel veriler ve beğeniler haber verilmeksizin üçüncü şahıslara aktarılmaktır. Bu durum da etik açısından oldukça tartışmalı bir durumdur.

3.2.3. Derinlemesine paket analizi

"Deep Packet Inspection (DPI)" yani Türkçe anlamıyla "Derinlemesine Paket Analizi", IP (internet protokolü) ağı üzerinde dolaşımda olan veri transferinin habersiz bir şekilde gözlemlenmesini sağlayan bir teknolojidir. IP internetin bilfiil protokolüdür ve sanal olarak internet üzerinde dolaşımda olan gelen ve giden tüm verileri (en özel ağlar dâhil) içerir (Corwin, 2011). DPI (deep packet inspection) teknolojisi katmanlı erişimin bir biçimidir; 'İnternet trafiğinin tanımlanması, sınıflandırılması, gözetlenmesi ve denetlenmesi' için ağ operatörlerine (ya da İnternet servis sağlayıcıları vb.) izin veren bir uygulamadır. Giderek yaygınlaşan DPI teknolojisi, hem ağ tarafsızlığı hem de ifade özgürlüğü tartışmasının sınırlarını çizmek bakımından önemlidir. DPI uygulamaları, hem gizliliği hem de iletişim özgürlüğünü ihlal ederek ifade özgürlüğünü kısıtlayabilmektedir. DPI teknolojisi ile şirketler ve hükûmetler, hangi verilerin, kime ne şekilde ulaşabileceğine ya da ulaştırılmayacağına karar verebilme gücüne sahip olmuşlardır (Aydın ve diğerleri, 2013).

DPI bir organizasyon içinde de kullanılabilir, ulusal düzeyde de. Tek bir organizasyonunun ağındaki akışları izlemek için kullanıldığında, ağ güvenliği, yük dengeleme, internet kullanımının kısıtlanması veya izlenmesi gibi kuruluşa ait özel ihtiyaçlara özel olarak tasarlanmıştır. Öte yandan eğer DPI bir ISP (servis sağlayıcı) tarafından ulusal düzeyde akışları izlemek üzere kullanılırsa, izlemenin 'derinliği' de bu

ölçüde değişir. Ulusal düzeyde DPI kullanımının temel üç alanı vardır (Karlıdağ ve Fidaner, 2011):

Ağ İzleme

Bir ağın, kullanıcıların tamamı, bir kesimi veya tek tek kullanıcılar tarafından nasıl kullanıldığını anlamaktır. Bu, genelde servis sağlayıcılar tarafından eniyileme amacıyla uygulanmaktadır. Eniyileme, servis sağlayıcının "router"larından (yönlendirici) geçen veri içeriğini bir ağ yöneticisi gibi denetleyerek 'iyi' veya 'akli' iletişim akışlarını 'kötü' veya 'yüklü' iletişim akışları karşısında ayrıcalıklandırmayı içerir.

Örneğin servis sağlayıcıları DPI kullanarak, yüklü ağ trafiği isteyen BitTorrent dosya paylaşımı protokolünü sıklıkla kullanan aboneleri tespit edebilir, bu işlemlerden para kesebilir veya tamamen engelleyebilirler. Aynı şekilde akış içeriğinin ISP'lerce tespiti zararlı yazılım engelleme veya telif hakkı korunması gibi farklı politikaları dayatmalarına izin verir. Tekil aboneleri hedefleyen tüm bu kullanımların yanı sıra DPI istatistiksel olarak belirli bir kullanıcı kesiminin ağ kullanımını ciro ile karşılaştırarak ne kadar kar getirdiğini araştırmak için kullanılabilir.

Hedefli Reklamcılık

İkinci kullanım servis sağlayıcıların ticari ortaklıkları ve bu alanda uzmanlaşan DPI şirketleri tarafından yapılan hedefli reklamcılıktır (veya Çevrimiçi Davranışsal Reklamcılık – Online Behavioral Advertising). Hedefli reklam Internet ortamında kullanıcının davranışlarını takip ederek ilgi alanlarının saptanması ve bu ilgi alanlarına göre kendisine reklam gösterilmesidir. Google ve diğer birçok kuruluş hedefli reklam uygulaması yapmaktadırlar. Ancak çoğunun yöntemlerinde DPI yoktur, "hedef"in ilgi alanları arama sözcükleri ve

ziyaret ettikleri web adresleri ile belirlenir. Hedefli reklam için DPI kullanıldığında ise daha "derin" ve daha anlamlı verilerle daha isabetli hedefleme yapılabilir. Bu genelde abonenin bilgisayarına cookie'ler (çerezler) bırakarak yapılır. Bütün abonelere tekil kimlik numaraları verilir ve ilgi alanlarını belirlemek için bütün etkinlikleri kaydedilir. Kullanıcılar teorik olarak bilgilerinin toplanmasını engelleyebilir veya o hizmeti kullanmayı bırakabilir, ama bazı daha karmaşık sistemler cookie'ler silindiğinde dahi kullanıcı hakkında bilgi toplamayı sürdürmektedirler

Gözetim ve Sansür

Üçüncü kullanım ise devletlerce yasal veya yasadışı gözetim ve sansürdür. Bunlar, çocuk pornografisi gibi genel kabul görmüş suçların engellenmesinden, ülkedeki muhalif hareketlerin baskılanması gibi baskıcı eylemlere kadar farklı biçimler alabilir. Genelde amaç ikincisidir ve ilki DPI kurulumunu gerekçelendirmek için kullanılır. Devletler DPI gözetimi için ISP'lerin rıza ve işbirliğine ihtiyaç duyarlar. Bu çoğunlukla fazla zorluk yaratmaz, çünkü ISP'ler çalışabilmek için devlet iznine tabidirler. Sonuç olarak DPI sistemi sınırsızca gözetim için kullanılır ve bu kendini tetikleyen bir merak sonucunda, er ya da geç, ağ kullanıcısının özel yaşamı ihlal edilir.

Yukarıda detaylarıyla birlikte ele aldığımız DPI, günümüzde arama motorlarında yaptığımız her türlü aramayı, aramalarda kullandığımız anahtar kelimeleri, ziyaret ettiğimiz internet siteleri, bu sitelerde geçirdiğimiz zamanı, ilgilerimizi, beğenilerimizi, kısacası her türlü kişisel verimizin ISP (İnternet Servis Sağlayıcıları) eliyle pazarlama ve reklam şirketlerine aktarılmasını sağlayan bir teknolojidir. Bu teknoloji sosyal teori içerisinde internet güvenliğine ve kişisel mahremiyete zarar vermesi sebebiyle sıkça tartışılmaktadır. Ne

yazık ki DPI teknolojisi ülkemizde de açık bir şekilde kullanmaktadır. Sonraki bölümde ülkemizde DPI kullanımını ele alacağız.

3.2.4. Türkiye'de TTNET'in DPI Teknolojisi kullanımı

Ülkemizin en büyük İnternet Servis Sağlayıcısı (ISP) konumunda bulunan TTNET isimli firma son yıllarda Phorm ve Adobur adı verilen hizmetleri başlatarak DPI teknolojisini kullanmış, bu teknoloji sayesinde toplanan kişisel bilgilerimiz pazarlama şirketlerine aktarılmıştır. Aşağıda Phorm ve Adobur'un çalışma mantığını inceleyeceğiz.

3.2.4.1. Phorm

Phorm ilk olarak yazılım ekibi Rusya'da, merkezi ise ABD'nin Delaware eyaletinde bulunan "121Media" isimli şirketin "PeopleOnPage" adıyla dağıttığı ve hızla yaygınlaşan ücretsiz arama çubuğu eklentisiyle adını duyurmuştur. ContextPlus adlı bir reklam motoru üstünde çalışan uygulama, ziyaret edilen sitelerin adresini merkeze yollayıp ziyaretçilerin dijital sicilini çıkartıp ilgi alanlarıyla paralel reklamlar gösteriyordu. Kurması kolay ve kardırması bir hayli zor olan bu arama çubuğu 121 Media'ya milyonlarca dolar kazandırmıştır. Güvenlik yazılımları tarafından kısa sürede casus uygulama sınıfına alınan PeopleOnPage'e karşı ilk şikâyet ABD Ticaret Komisyonu'na 2005'te yapılmıştır. Ardından Kanada'da benzer şekilde şikâyetler gerçekleşmiştir. Bu tür şirketlere karşı açılan davalar sonucunda 2006'da ContextPlus 'müşterilerine yeterince kaliteli hizmet veremediği' gerekçesiyle faaliyetlerini askıya almıştır. Aynı dönemde 121Media da PeopleOnPage uygulamasını kapatıp şirketin ismini Phorm olarak değiştirmiştir. (radikal.com.tr).

Yukarıda kuruluş ve yükseliş hikâyesini anlattığımız Phorm, kendi ifadesiyle kullanıcıların internet deneyimlerini

daha fazla kişiselleştirmeye yarayan bir sistemdir. Aslında sistem böyle masum bir ifadenin arkasına sığınsa da, yaptığı şey tam anlamıyla internet güvenliğini ve çevrimiçi kişisel gizliliği ihlal etmektir.

Sistem şu şekilde işlemektedir: kullanıcıların gezdiği siteler, tıkladıkları reklamlar, izledikleri videolar, doldurduğu formlar vb. aracılığı ile profillenmektedir. Elde edilen profile göre ticari olan/olmayan içerikler sunulmaktadır. Yani İnternette neler yapıldığını ve nasıl davranıldığını izleyip ona uygun reklamlar ve içerikler sunulmaktadır. (enphormasyon.org).

Bir başka ifadeyle bu sistem bizi an ve an izlemektedir. İzleme DPI (Derinlemesine Paket Analizi) olarak bilinen teknolojilerle gerçekleştirilmektedir. Bu teknoloji sadece bilgisayarımız ya da internet tarayıcımızla ilgilenmemektedir. Aynı zamanda internet hattımızı izleyip, gelen giden tüm verilerimizi analiz etmektedir. Bu durumun biz internette dolaşırken başımızda durup monitörümüzü izleyen bir çift gözden farkı yoktur.

Phorm 2011 yılında Avrupa Parlamentosu tarafından alınan kararla[7] Türkiye dâhil, Avrupa'da faaliyetleri yasaklanmasına rağmen TTNET ile anlaşıp ülkemizde son yıllarda faaliyete başlamıştır.

Phorm'un üzerimizden topladığı veriler daha sonra profilleme ve analiz yapan firmalara satmakta, bu firmalar elde ettikleri veriler üzerinde tasnifler yapmaktadır. Toplanan verilerin tam olarak hangi amaçlarda kullanıldığı kesin olarak bilinmemekle beraber, kişisel verilerimizin ve iletişimimizin gizliliği ihlal edilmektedir.

Tüm yurtta yükselen sesler, artan tepkiler ve açılan davalar neticesinde BTK (Bilgi Teknolojileri Kurumu) Phorm

[7] http://csis.org/files/attachments/130828_2EU428-2009ammendments%282011%29.pdf bağlantısından Avrupa Parlamentosu tarafından Phorm ile ilgili alınan karar İngilizce olarak görüntülenebilir.

servisi ve TTNET üzerine bir soruşturma başlatmıştır. Soruşturmanın açılma sebebi BTK tarafından şu şekilde açıklanmıştır:

> *Kişisel verilerin işlenmesine ilişkin olarak Gezinti.com hizmeti aracılığıyla abonelerden/kullanıcılardan alınan onay sürecinde abonelerin/kullanıcıların kişisel bilgilerinin hangi kapsamda ve hangi süre ile işleneceğine ilişkin gerekli açıklamaları yapmayarak ve aboneleri/kullanıcıları eksik bilgilendirerek Elektronik Haberleşme Sektöründe Tüketici Hakları Yönetmeliği'nin "Şeffaflık ve bilgilendirme" başlıklı 6'ncı maddesini, Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmeliğin 'Telekomünikasyonun Gizliliği' başlıklı 8'inci maddesini ve aynı Yönetmeliğin "İzin ve Süre" başlıklı 9'uncu maddesi ve ilgili diğer mevzuat hükümleri kapsamında ihlal ettiği değerlendirilen TTNET AŞ hakkında soruşturma başlatılması…*

Soruşturmanın kararı 14 Aralık 2012 tarihinde açıklanmıştır. Kararda TTNET kullanıcılarının yalnızca rızaları ve onayı alınarak Phorm ve Gezinti hizmetinin kullanılabileceği hususlarına karar verilmiştir.[8] Bu kararla müşterilerine Phorm hizmetini dayatan TTNET uyarılmış oldu.

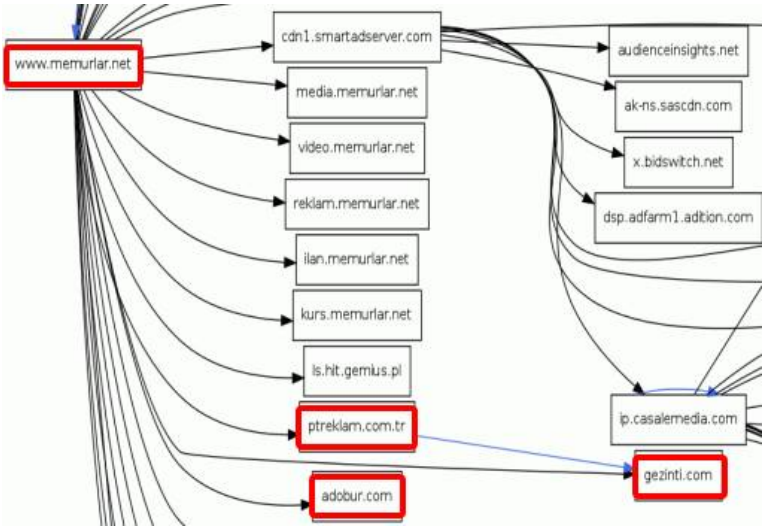
BTK'nın bu uyarısına aldırış etmeyen ve Phorm, sistemiyle çalışmaya devam eden TTNET'e BTK, 24.04.2013 tarihinde "yasaların ve yargı kararlarının öngördüğü durumlar haricinde, haberleşmeye taraf olanların tamamının izni olmaksızın, telekomünikasyonun üçüncü şahıs tarafından dinlenmesi, kaydedilmesi, saklanması, kesilmesi veya gözetimi yasaktır" hükmüne aykırı olarak 1,5 Milyon Türk Lirası tutarında bir para cezası kesmiştir.

[8] http://www.btk.gov.tr/mevzuat/kurul_kararlari/dosyalar/TTNET-PHORM.pdf bağlantılısından BTK'nın TTNET hakkındaki kararına ulaşılabilir.

3.2.4.2. Adobur

Phorm vakasından sonra artan tepkiler, açılan davalar ve kesilen cezalar sonucunda Phorm hizmeti bir müddet için sessiz kalmış, ardından 2014'ün ikinci yarısında ismini Adobur olarak değiştirerek faaliyetlerine tıpkı Phorm ile aynı mantıkta devam etmeye başlamıştır. Kısacası her şey aynı şekilde devam etmiş, değişen tek şey isim olmuştur. Phorm, Adobur adını alarak yalnızca BTK'nın 2012 ve 2013 yıllarında yasak olarak nitelendirmeye başladığı bazı uygulamaları kılıfına uydurup kişisel verilerimizi rızamızı almadan toplamaya yeniden başlamıştır.

Sistem bugün tam olarak şöyle işlemektedir: Yeni bir TTNET abonesi internete girişinde Gezinti.com sitesine yönlendirilir. Gezinti hizmetini kabul edilirse internette yapılan işler kayıt altına alınmaya başlanır. Reddedilirse durum daha da karmaşık bir hal almaya başlar: Sistemden çıkmak için Gezinti hizmetine üç ay boyunca her ay bir kez "hayır" denmesi ve bunun yılda üç kez tekrarlanması gerekmektedir. Başta izin vermeden dâhil olunan 'hizmet'in kullanıcı sözleşmesinde aynen bu şeyler yazmaktadır.



Şekil 3.1. Phorm ve Adobur'un Çalışma Mantığı

Yukarıdaki şekilde Phorm ve Adobur'un çalışma mantığı gösterilmiştir. Örneğin Phorm'un reklam kodunun içerdiği bir siteye girildiğinde ve sitenin kaynak kodları incelendiğinde site içeriğinde "http://ptreklam.com/tag/1.js" gibi bir kod görülür. Bu kod internet kullanıcısını ptreklam.com.tr ve adobur.com'a yönlendirir, bu yönlendirme gezinti.com adresinde son bulur ve yapılan tüm yönlendirmeler arka planda olduğundan kullanıcı bunu anlayamaz. Bu yönlendirmeler sırasında Phorm tarafından elde edilen kişisel veriler yukarıda belirttiğimiz internet siteleri üzerinden merkezdeki veri tabanına aktarılmaktadır.

Adobur'lu sitelere girildiğinde de kullanıcının bilgisayarına önce "OPTED_IN" diye bir çerez (cookie) otomatik olarak yüklenmektedir. Bu Adobur (Phorm) reklam sistemine dâhil olunduğu anlamına gelmektedir. Hemen arkasından da "UID" diye bir çerez yüklenmektedir. Bu çerez Phorm'un müşterilerine verdiği numaradır. Bu numara ile internette

gezilen sayfalar kaydedilip kişisel profiller çıkarılmaktadır (Bekir, 2014).

Adobur ve Phorm'a ait reklam kodları ülkemizin en çok ziyaret edilen haber, ekonomi, spor, magazin ve video sitelerinde yer almaktadır. Büyük bir ziyaretçi kitlesine sahip olan bu sitelere her gün milyonlarca kişi girmekte; bu da Adobur ve Phorm'lu kodların milyonlarca ziyaretçinin bilgisayarlarına yüklenmesi anlamına gelmektedir.

3.3. 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 bilinememiştir. 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.

Medyanın yarattığı yanlış bir algıdan dolayı günümüzde "bilgisayar korsanları" ile "hackerlar" birbirine karıştırılmaktadır. Günümüzde çoğu kişi bilgisayar korsanı ile hackerın aynı kişi olduğunu düşünse de bu aslında doğru değildir. Bilgisayar korsanlığı ile hacker arasındaki anlam karmaşasını ortadan kaldırabilmek için "hack, "hacker" ve "cracker" kavramlarını tanımlamak ve bu kavramların geçirdiği evrimi açıklamak gerekmektedir.

3.3.1. Hack, Hacker ve Cracker Kavramları

"Hack" ve "Hacker" kelimeleri İngilizce olup, dilimizde karşılıkları bulunmamaktadır. Dilimiz için "Hacker"ın karşılığı olarak "kırıcı" kelimesi önerilmektedir. Merriam-Webster

İngilizce Sözlüğünde "Hack" kelimesi "zevk için bilgisayar programı yazmak" ve "bir bilgisayara izinsiz bir şekilde erişmek" tanımları kullanılmıştır (merriam-webster.com). "Hacker" kavramı ise "bir bilgisayara veri toplamak, zarar vermek vb. amaçlarla gizlice giren kişi" olarak tanımlanmıştır (merriam-webster.com).

Cambridge Üniversitesi'nin İngilizce-Türkçe Sözlüğünde ise "Hack" kelimesinin karşılığı olarak "başkasının bilgisayarındaki bilgilere izinsiz erişmek/ulaşmak" tanımlaması yapılmıştır (dictionary.cambridge.org). "Hacker" sözcüğü içinse "bilgisayar korsanı" tanımlaması yapılmıştır (dictionary.cambridge.org). TDK 2015 Güncel Türkçe Sözlükte "Hacker" kavramı kullanılmamış, bunun yerine "Bilgisayar Korsanı" sözcüğü tercih edilmiş ve "bilgisayar ve haberleşme teknolojileri konusundaki bilgisini gizli verilere ulaşmak, ağlar üzerinde yasal olmayan zarar verici işler yapmak için kullanan kimse" şeklinde tanımlanmıştır.

Steven Levy (2010/2014), Hackerlar için "bilgisayar korsanı" yakıştırmasını reddetmiş ve onları "programlamayı hayattaki en önemli şey olarak gören bilgisayar -programcıları ve tasarımcıları- bilgisayar devriminin kahramanları" şeklinde ifade etmiştir (Levy, 2014).

Elbahadır (2014)'a göre Hacker; işletim sistemlerini tam manasıyla bilen, derinliklerine inen, bilgisayarlarla derinlemesine ilgilenen, programlamayı profesyonel düzeyde bilen bilgisayar uzmanlarıdır. Hackerlar bir yapı üzerinde sistem hatası veya sistem açıkları bulabilir, bu açıkların sebeplerini bilir. Hiçbir zaman öğrendikleriyle yetinmez, daima daha fazlasını öğrenme çabası içindedirler. Bu dehalar zarar verme girişimlerinde bulunmazlar (Elbahadır, 2014: 8).

Bilişim dünyasında iyi niyetli hackerları ile kötü niyetli hackerları birbirlerinden ayırmak için "Cracker" kavramı türetilmiştir. Birçok güvenlik uzmanı bilgisayar korsanlarını

"cracker" kavramıyla ifade ederler. Bu kavramın türetilmiş olmasının sebebi; bilgisayar korsanlarının, geçmişte bilgisayar dünyasına çok önemli katkılarda bulunmuş olan hackerların şöhretini sahiplenmeleri ve onlar gibi anılmalarıdır.

Cracker'in dilimizde karşılığı olmamakla birlikte bu kavram için karşılık olarak "çökertici" kelimesi önerilir. Türk Dil Kurumu'nun Yabancı Kelimelere Karşılıklar bölümünde "Cracker" için, "bir başkasının bilgisayarına girmek, ele geçirmek için teknik ve kişisel becerilerini kullanan kişi" denmektedir. Cracker terimi orta düzeyde beceriye sahip ve etik sınırları bulunmayan kişileri tanımlamak için kullanılır (Çakar, 2013: 6).

İnternet Mühendisliği Görev Gücü'nün internet sitesinde bulunan İnternet Kullanıcıları Sözlüğünde crackerlar için, "Bir cracker, bilgisayarlara yetkisiz bir şekilde erişmeye çalışan kişidir. Bu bireyler, genellikle hackerların aksine kötü niyetlidir ve ellerinde kötü amaçlı yazılımlar bulunur" denilmiştir (tools.ietf.org).

Hacker ile cracker konusundaki en çarpıcı ayrım ise, eski hackerların kullandıkları kavramları topladıkları "Jargon File"'da ortaya konulmuştur. Jargon File'da crackerlar için "Bu kişiler bilgisayarlar yetkisiz bir şekilde girerler ve kötü niyete sahiptirler. Crackerlar tembel ve sorumsuzdur, çok akılları yoktur. Ancak güvenliği kırabilmektedirler" denilmiştir.

Uçkan (2014)'a göreyse: "Hacker, bilginin, daha da ötesinde denetim altına alınmamış anlamın peşindedir. Kişisel çıkarların değil. Bedava yazılımla insanların sistemlerine, kişisel çıkar elde etmek için giren kişi, hacker değil, yalnızca cracker'dır ve dediğimiz gibi, şirketlerde ya da hükûmette bunlara daha sıklıkla rastlanır. Heyecan peşindeki veletler ya da seri cinayet işleme cesaretini gösteremeyen psikotik virüs yazıcıları da bulunur içlerinde. Ama bu, etik sahibi bir

hacker'ı sivil topluma karşı bir suçlu kılmaya yetmez" (Uçkan, 2014: 46).

Siber saldırıları kimin yaptığını belirlemek ve hacker ile cracker arasındaki ayrımı daha da somut bir biçimde ortaya koymak için beyaz ve siyah metaforu kullanılmıştır. Buna göre beyaz iyiliği ve masumiyeti, siyah ise kötülüğü temsil edecektir (Kara, 2013: 11). Bu nedenle saldırganlar aşağıdaki gibi şapka renklerine göre gruplandırılırlar:

Black-hat (siyah şapka)

Bu tabir tamamen kötü niyetli, sırf kazanç elde etmek ve karşıya zarar verme eğilimiyle sistemlere sızan, bilgi çalan korsanlar için kullanılır. Bu grubun amacı bilgi çalmak veya zarar vermektir.

White-hat (beyaz şapka)

Bu grup, bilgi bakımından siyah şapkalılardan aşağı kalmamakla beraber; iyi niyetli, zarar vermeyen, amaçları bilgisayar güvenliğini sağlamak olan kişilerden oluşur.

Grey-hat (gri şapka)

Bu gruptaki kişiler kimi zaman beyaz, kimi zaman siyah şapka olabilen, güvenlik amaçlı bile olsa girdikleri sistemin bilgilerini başkalarıyla paylaşabilen gruptur (Elbahadır, 2014: 8).

Crackerlar genellikle "ters mühendislik" alanına hâkimdirler ve programların uygulama dosyalarını değiştirip, yüzlerce dolar değerindeki programları yazdıkları "crack" adı verilen yazılımlarla ücretsiz şekilde kullanılabilecek duruma getirebilecek beceriye sahip kişilerdir. Bu bağlamda

crackerlar yazılım endüstrisine de büyük ölçüde zarar vermektedirler.

Crackerları kendi aralarında kategorize eden kavramlar da bulunmaktadır. Bunlar "Phreaker", "Script Kiddie" ve "Lamer"dir:

Phreaker

Bu kişiler 1970'lerde moda olan ve "Phreaking" akımının temsilcileridirler. "Phreaking" telekomünikasyon (telefon, fax vb.) sistemlerinin nasıl çalıştığı, bu sistemlerin nasıl çökertilebileceği, manipüle edileceği ve bu sistemlere nasıl sızılabileceği konusunda uzmanlaşmak anlamına gelmektedir (en.wikipedia.org).

Script Kiddie

Genellikle lise çağlarındaki gençlerden oluşan kişilerdir. Bu kişiler internette kolayca bulunabilen çeşitli hazır programları ve araçları kullanırlar. Başkaları tarafından yazılmış, bir şeyin nasıl yapılacağını adım adım anlatan dokümanları okur ve uygularlar. Kullandıkları programın nasıl çalıştığını bilmezler ve teknik dokümanlardan anlamazlar. Ellerindeki programları kullanarak olabildiğince fazla bilgisayara zarar vermeye çalışırlar (tr.wikipedia.org).

Lamer

Script Kiddie'lerden daha alt seviyededirler. Hackerlara özenirler ve hacker gibi davranmaya çalışırlar; ancak belli bir bilgi birikimleri yoktur. Ellerindeki araçları sağdan soldan indirirler. Bu araçları nasıl kullanacakları kısmen de olsa bilirler ve zaman zaman tehlikeli olabilirler (Elbahadır, 2014: 8).

3.3.2. Siber Saldırı Aşamaları

Bir siber saldırının aşamaları aşağıda ayrıntılarıyla birlikte ele alınmıştır.

3.3.2.1. Bilgi toplama aşaması

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.

Ülkemizde bilişim güvenliği konusunda oldukça tanınan bir yazar olan Elbahadır (2014) bir saldırganın hedef hakkında bilgi bulmak amacıyla yararlanabileceği kaynakları şöyle sıralamaktadır:

Whois veritabanlarını sorgulama

Alan adlarının (örn: domainadi.com) ya da IP numaranın ait olduğu kişi ve/veya kuruluşun (firmanın) bilgilerini içerir. Domain'in kayıt ve süresinin bitiş tarihi, host edildiği firmanın name server bilgileri de yer alır. Mesela domainadi.com domaini kimin adına kayıtlı mail adresi telefon numarası domaini host eden hosting firmasının name server (ns) bilgilerini gösteren bir sorgulamadır. Bu tip sorgulamaların yapılabileceği whois.com gibi birçok kamuya açık site mevcuttur (tr.wikipedia.org).

IP ve IP veritabanlarını sorgulama

İnternet Protokol Adresi (IP adresi), bilgisayarların veri transferi için birbirini tanıması ve iletişim kurmasını sağlayan, 32 bitlik verilerdir. Bu veriler rakamlardan oluşur. Her IP adresine onluk sayı tabanlarına göre 0-255 arasında olmak üzere xxx.xxx.xxx.xxx şeklinde 4 haneli 8 bitlik rakamlar dizilimi karşılık gelir. Her dizilim noktalarla birbirinden ayrılır ve her bir gruba "oktet" adı verilir. Bir korsan, sızmaya çalışacağı sistemin büyüklüğünü yani "subnets" denilen sisteme bağlı alt ağ bloklarını bilmeden bir profil çıkaramaz. Bunu öğrenmek için hedef sistemin IP adresini öğrenmeye çalışacaktır. Bunu da IP blokunun ait olduğu veritabanlarını sorgulayarak yapacaktır (Elbahadır, 2014: 44, 45).

DNS sorgulama

DNS (Domain Name System / Etki Alanı Ad Sunucusu) internet tarayıcısının adres çubuğuna girdiğiniz site ismini, girmek istediğiniz sitenin gerçekte ikamet ettiği IP adresine çeviren ve internette gezinmeyi tahmin edemeyeceğiniz kadar kolaylaştıran bir sistemdir. Örneğin, hiç kimse şu anda Google'ın ikamet adresi olan 74.125.224.83 adresini tarayıcısına yazmaz. Onun yerine www.google.com yazar ve DNS sunucusu, bu adresi IP adresine yönlendirir (technopat.net). Saldırganın bu veriye ulaşabilmesi için yapması gereken tek şey Windows İşletim Sistemi'nin komut ekranına "nslookup" yazmaktır.

Arama motorları ve sosyal medya siteleri

Geçmişte saldırganların bazı önemli bilgilere erişebilmesi için toplum mühendisliği konusunda oldukça yetenekli olmaları gerekiyordu. Günümüzde ise artık çoğu bilgi bu yetenek kullanılmadan klavyeden birkaç tuşa basabilecek kadar kolay bir şekilde bulunabiliyor. Saldırganlar kuşkusuz bunu Google gibi büyük arama motorlarına ve son yıllarda oldukça popüler olan sosyal medya platformlarına borçlular. P. W. Singer (2014/2015) Siber Güvenlik ve Siber Savaş isimli kitabında bunu şöyle özetlemektedir:

Çevrim içi arama araçları ve sosyal ağlar saldırganlara Tanrı'nın bir lütfudur. Bir cihaz çalmak ve dolayısıyla ürün geliştirme bölümü başkan yardımcısının kim olduğunu öğrenmek mi istiyorsunuz? Eskiden insan kaynaklarındaki resepsiyon görevlisini baştan çıkarmak ve daha sonra çalkalanmış martiniler ve seks gecesinden sonra o uyurken dosyalarına gizlice erişmek için James Bond'u gönderebilirdiniz. Şimdi daha sıkıcı. Sadece ismini bir internet arama motoruna yazın ve o yöneticinin özgeçmişinden kızının evcil iguanasının ismine kadar her şeyi edinebilirsiniz (Singer ve Friedman, 2015: 86).

Günümüzde Google gibi gelişmiş arama motorları sayesinde güvenlik açığı bulunan birçok sitede yer alan kişisel bilgilere, kullanıcı adı ve parolalara bile ulaşmak mümkündür.

3.3.2.2. Tarama

Bir saldırı için saldırganın yukarıdaki yöntemleri kullanarak hedefi hakkında topladığı veriler çoğu zaman yetersizdir. Saldırganın hedefiyle ilgili öğrenmesi gereken birçok şey daha vardır. Saldırgan, bu aşamada hedefiyle ilgili açıkları taramaya başlar. Söz konusu hedef bir internet ağı veya internet sitesiyse yaygın olarak aşağıdaki adımlar izlenilir:

- Ağdaki sunucuların açık portları tarama yapılarak tespit edilir.
- Sunucuda kullanılan işletim sistemi tespit edilir.
- Sistemdeki yazılımsal ve donanımsal açıklar/hassasiyetler tespit edilir.

3.3.2.3. Saldırı yöntemi seçilmesi

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. Saldırı yöntemlerinin aşırı derecede karmaşık teknik bilgi ve kavramlar içermesi nedeniyle çalışmamızın bu kısmında bu yöntemleri en sade haliyle özetleyeceğiz. Günümüzde bilgisayar korsanlarının en çok başvurduğu saldırı yöntemleri aşağıdaki gibidir:

3.3.2.3.1. Cookie hi-jacking

Bu saldırı türünde çeşitli virüs ve trojan gibi yazılımlar kullanılarak internet tarayıcılarına depolanmış olan tanımlama bilgilerini ele geçirmek hedeflenir.

3.3.2.3.2. Active-X saldırıları

Active X adı verilen Windows işletim sistemlerinde bulunan internet tabanlı uygulamaların çalıştırılmasını sağlayan teknolojinin açıklarından faydalanarak bilgisayarlara sızılabilir ya da bilgisayarları ele geçirmeye yönelik çeşitli yazılımlar gizli bir şekilde bilgisayara yüklenebilir.

3.3.2.3.3. İnternet sitelerindeki açıklar

CGI gibi internet sitelerini barındıran sunucular üzerindeki yazılımların çalışmasını sağlayan bazı teknolojilerdeki açıklardan faydalanılıp sunucuya sızılabilir.

3.3.2.3.4. Düzmece siteler ve tehlikeli ekler

Phishing olarak da bilinen "aldatmaca" tekniğidir. Saldırganlar genellikle kurbanlarını, içerisinde kötücül bir yazılım indirmek amacıyla eklemlenmiş bir bağlantı bulunduran "spam" olarak tanımlanan e-postalarla kandırırlar. Kevin Mitnick (2002/2015), Aldatma Sanatı isimli kitabında bu durumu şöyle vurgulamıştır: "Pek çoğumuz bedava bir şeyler elde etmeye o kadar hevesliyiz ki, yapılan öneri ya da verilen söz üzerinde mantıklı düşünemeyecek durumda olabiliyoruz. Bilinçli bir saldırgan, bir şirket ağına girebilmek için bedava bir hediyeye karşı duyduğumuz doğal dürtüye hitap etmek dâhil neredeyse her yolu kullanacaktır" (Mitnick, 2015a: 85). Kimi zaman bu e-postalarda gelen bağlantılar gerçek bir internet sitesini taklit eden bağlantılar içerirler ve gerçek sitelerden geliyormuş gibi kurgulanırlar. Mesela "PayPal.com" internet sitesinden geliyormuş gibi kurgulanan bir sahte e-postada mevcut olan bağlantı dikkatle incelendiğinde "PayPai.com" yazmaktadır. O bağlantıya tıklandığında genellikle ya kredi kartı dolandırıcılığı yapılır ya da bilgisayara kötücül bir yazılım indirilir. Phishing saldırıları bir toplum mühendisi tarafından kurgulandığı zaman çok daha etkili olmaktadır.

3.3.2.3.5. Keyloggerlar

Bunlar bilgisayarda yazdığımız her şeyi (bir sohbet sırasında ya da e-postada) ve o anda ekranda var olan görüntüyü kaydetmeye yarayan casus yazılımlardır. Bu programlar arka planda gizli bir şekilde dinleme yaparlar ve kurbandan topladıkları verileri saldırgana otomatik olarak gönderirler (webopedia.com).

3.3.2.3.6. Şifre ve gizli soru tahminleri

Bu yöntemle bir internet sitesinde ya da e-posta hesabında kullanılan şifre ve gizli soru tahmin edilir, böylece hesap ele geçirilebilir. Burada çoğu zaman toplum mühendisliği yöntemleri devreye girer.

3.3.2.3.7. Domain hi-jacking

İnternet sitelerine ait domainlerin (alan adları) ele geçirilmesidir. Saldırgan çeşitli teknikler kullanarak siteye ait alan adını ele geçirerek birçok açıdan internet sitesini sahiplenmiş olur.

3.3.2.3.8. Hizmet dışı bırakma saldırıları (ddos)

İnternet üzerinden çok sayıda istemci bilgisayar kullanılarak yapılan bir saldırı çeşididir. Çoğunlukla virüs bulaştırılarak zombi haline getirilen bilgisayarların, bir sunucu bilgisayara eş zamanlı ve mümkün olduğunca çok sayıda istek göndermesi, sunucunun kapasitesinin aşılması sonucunda da hizmet veremez hale getirilmesi ilkesine dayanır. Yeterli sayıda zombi bilgisayar mevcut olduğunda ddos saldırılarını engellemenin bilinen bir yolu yoktur. Onbinlerce istemciden sürekli olarak gelen istekler öncelikle yanıtlanmaya çalışılır ve bir süre sonra kapasite aşılarak sunucu devre dışı kalır (tr.wikipedia.org).

3.3.2.3.9. SQL injection (sızma)

SQL injection, internet sitelerinin işleyişiyle ilgili her türlü verilerin kayıtlı olduğu SQL veritabanlarına, çeşitli yöntemlerle sızma ve bu veritabanları üzerinde değişiklik yapılmasıdır.

3.3.2.3.10. Virüs saldırıları

Virüsler bilgi sızdırma, kredi kartı bilgilerini çalma, eğlence, zarar verme vb. amaçlarla yazılmış kötü amaçlı yazılımlardır (Akyıldız, 2013: 35). Virüsler saldırganlar tarafından hedeflerin sistemlerine çeşitli yöntemler kullanarak bırakılırlar ya da hedefin bu virüsleri aldatmaca teknikleri kullanarak indirilmesi sağlanabilir. Çalışmamızın sonraki bölümlerinde "worm" gibi kendini ağlara kopyalayan basit virüslerden ve "Stuxnet" gibi son derece karmaşık yapıya sahip ve aynı anda birçok zarar verme yetisine sahip olan virüslerden bahsedeceğiz. Virüsler bu çalışmaya sığdırılamayacak kadar çeşitlidir ve bugüne güvenlik yazılımları tarafından tespit edilen milyonlarca virüs bulunmaktadır.

3.3.2.3.11. Zero-day exploit

Sıfırıncı gün açığından faydalanmak olarak ifade edilir. Bu saldırı türünde saldırganlar piyasaya sürülmemiş ya da henüz sürülmüş olan yazılım ve donanımların sahip olduğu açıkları tespit edip sistemlere sızmaya çalışırlar. Yazılım ya da işletim sistemi üzerinde kötücül değişiklikler yapıp arka kapılar bırakacak kodlar ekleyebilirler (fireeye.com).

3.3.3. Toplum mühendisliği

Bazen bilgisayar korsanları klavyenin tek bir tuşuna dahi dokunmadan çok büyük sistemlere erişim sağlayabilirler.

Kullandıkları bu yönteme de "Toplum Mühendisliği (Social Engineering)" denir (e-bergi.com).

Dünyanın gelmiş geçmiş en büyük bilgisayar korsanı olarak kabul edilen Kevin Mitnick[9], dünyada toplum mühendisliğini en iyi kullanan bilgisayar korsanı olarak da bilinmektedir. Mitnick (2005/2015), Sızma Sanatı isimli kitabında bu toplum mühendisliği için şöyle demiştir: "Toplum mühendisi veya taşıdığı silahlardan biri olan aldatma sanatında uzman bir saldırgan, insanı yardımseverlik, nezaket, destekleyici olmak, ekip çalışmasına yatkınlık gibi doğal eğilimlerimiz ve bir işin yapılması isteği gibi doğasının en iyi özelliklerini kullanarak insanı ağına düşürür" (Mitnick, 2015b: 257).

Toplum mühendisliğinde yöntemler verinin kaynağına, verinin gizliliğine, verinin nasıl korunduğuna göre değişmektedir. İyi bir toplum mühendisi anlık analiz yaparak ya da uzun zamanlı bir araştırma ile ilgili senaryoyu bilgisi ve hayal gücüyle tasarlar ve uygulamaya koyar. Toplum mühendisliğinde metotlar uygulanacağı kıstaslara göre değişmektedir. Kurbanın merakı, vicdanı, inancı, güveni, acıma duygusu, zaafları (makam, mevki, hırs, para, cinsellik, ego) gibi

[9] Black-hat grubunun en önemli temsilcilerinden olan Kevin Mitnick bir zamanlar dünyanın en çok aranan bilgisayar korsanıydı. Mitnick aynı zamanda dünyanın en ünlü bilgisayar korsanı olarak da bilinmektedir. Öyle ki Mitnick daha önce defalarca FBI tarafından yakalanmış, toplamda beş yıl hapis yatmış ve ona ithafen 2000 yılında "Sanal Korsan" isimli bir sinema filmi bile çekilmiştir. Phreaking akımından gelen Mitnick, telefon sistemleri ile bilgisayar ağları konusundaki bilgisini "toplum mühendisliği" yeteneğiyle birleştirmiş ve kendisini defalarca demir parmaklıkların arkasına atacak birçok suç işlemiştir. Mitnick, aldığı cezaların sonucunda (hapis cezasının dışında üç sene bilgisayar ve telefon kullanmama cezası da almıştır) bilgisayar korsanlığını bırakmıştır. Mitnick siber güvenlik ile toplum mühendisliği konusundaki tecrübelerini ve yaptığı saldırıların hikâyelerini yazdığı Aldatma Sanatı (2002/2015) ve Sızma Sanatı (2005/2015) isimli kitaplarda toplamıştır. Mitnick şu anda hayatını edindiği tecrübeler sayesinde kurduğu güvenlik şirketinden kazanmaktadır.

duygularını kullanarak veri hırsızlığı yapılabilir (bilgiguvenligi.gov.tr).

Mitnick (2002/2015)'e göre güvenliğin en zayıf halkası "insan" unsurudur. Mitnick toplum mühendisleri ve insan unsuruyla ilgili olarak şunları söylemektedir:

> *Toplum mühendisinin güvenlik önemlerini atlatmak amacıyla, bilgisini paylaşacak güvenilir bir kullanıcıyı kandırması ya da hiçbir şeyden kuşkulanmayan bir hedefi ona giriş hakkı tanıması için aldatması gerekir. Güvenilir çalışanlar, hassas bilgileri paylaşmaları için ya da saldırganın içeri sızmasını sağlayacak bir güvenlik açığı yaratmaları için kandırılabildiklerinde, ikna edilebildiklerinde ya da yönlendirilebildiklerinde dünyada hiçbir teknoloji bir şirketi koruyamaz. Tıpkı şifre çözümleyicilerin şifre teknolojilerini bertaraf edecek bir açık bularak, şifrelenmiş bir mesajın içeriğini öğrenebildikleri gibi, toplum mühendisleri de güvenlik teknolojilerini bertaraf etmek için çalışanlarınızı aldatma yöntemi kullanırlar (Mitnick, 2015a: 7).*

Geçmiş olaylara bakıldığında bilgisayar korsanlarının hedefledikleri şirketlerde amaçlarına uygun konumlarda işler bulup, belirli süreler çalıştıkları bilinmektedir. Mitnick dâhil olmak üzere bazı bilgisayar korsanları, hedefledikleri şirket ya da bilgisayarların bulunduğu eğitim kurumlarına kılık değiştirip ve çalışan olarak legal yoldan girebilmesi, bu korsanları toplum mühendisliği alanının en başarıları arasına sokmaktadır. Böylesi avcıların şirkete sızmasını engellemek için uzun deneme süreleri, detaylı araştırma (bu genellikle işe yaramaz, çünkü bilgisayar korsanları yaşayan ve gerçek kişilerin kimliklerini çalma konusunda uzman sayılırlar), sabıka araştırması ya da sınavla işe alım süreci gibi caydırıcı ve uzayıp giden bürokrasiler işe yarayabilmektedir (Çakar, 2013: 37).

Toplum mühendisleri kurbanlarını çoğu zaman güçlü "ikna kabiliyet"leriyle kandırırlar. Çalışanların amiri ya da

patronu gibi şık giyinip "rol tuzakları" hazırlarlar ve kurbanlarının onlara "itaat" etmesini sağlarlar. Hedef şirket ya da kurumun çalışanlarını bilgisayar ağının çöktüğü ve bunun anca o anda şirketin güvenlik uzmanı rolüne bürünmüş toplum mühendisinin yardımıyla çözülebileceği "güvenlik" amacıyla "korku" salarak aldatabilirler. Toplum mühendisleri kurbana bir "rol" biçebilirler ve kurbanlarının bu rolle "özdeşleşme"sini sağlayabilirler. Böylece kurbanlarının kendilerine yardımcı olmalarını sağlayabilirler. Kimi zaman toplum mühendisleri kurbanlarına deneyim, güvenilirlik, dürüstlük veya beğenilirlik gibi bazı özellikler yükleyebilirler. Kurbanlarının kendilerinden "hoşlanma"larını (şık giyimli bir amir kılığına giren bir toplum mühendisinin, şirketin alt pozisyonlarında çalışan bir kadını tavlaması gibi) da sağlayabilirler. Bu yöntemlerden birini veya birkaçını aynı anda kullanıp istedikleri veriye ulaşabilir, çalmak istedikleri şeyi çalabilir veya internet ve bilgisayar sistemlerine sızabilirler.

Dünyanın en ünlü bilgisayar korsanlarının geçmişini incelediğimizde büyük kısmının toplum mühendisliği yeteneklerinin çok güçlü olduğunu görürüz. Çoğu zaman bilgisayar korsanlarının yazılım ve donanım konusundaki bilgilerini toplum mühendisliği yetenekleri ile birleştirdiklerinde ortaya önlenemez saldırılar çıkmaktadır.

3.3.4. Bilgisayar korsanlığının ve siber saldırıların tarihçesi

İlk hackerler 1950 ve 1960'larda Massachusetts Teknoloji Enstitüsü (MIT)'nde çalışan ve bir etik anlayışları bulunan programcılardır. Steven Levy (2010/2014)'e göre bu kişiler gerçek hackerlardır. İlk hackerlar hiçbir zaman kötü niyete sahip değillerdi ve sürekli dev boyutlardaki bilgisayarlarla uğraşır, güvenlik açıkları bulmaya çalışır ve bunları kapatmak

için program yazarlardı. Bu gerçek hackerlar arasında bulunan Dennis Ritchie ve Ken Thampson yaptıkları çalışmalarla günümüzde kullanılan Linux ve Windows işletim sistemlerine programlama anlamında çok büyük katkıda bulacak UNIX işletim sistemini geliştirmişlerdir (e-bergi.com). Steven Levy (2010/2014)'e göre "gerçek hackerların devri" 80'lerin sonunda "gerçek hackerların sonuncusu" olan Richard Stallman ile sona ermiştir (Levy, 2014: 481).

Ancak biz çalışmamızın asıl konusu olmasından dolayı "gerçek hacker"ların tarihinden çok, "kötü amaçlı" bilgisayar korsanlarının tarihi üzerinde duracağız. Bu bağlamda, çalışmamızın bu kısmında bilişim dünyasında önemli izler bırakmış ilk siber saldırılardan ve bu saldırıları gerçekleştiren ilk bilgisayar korsanlarından söz edeceğiz.

John Draper isimli korsan, 1969-1974 yılları arasında telefon ağlarına sızmakla ünlü olmuştur. Draper, yaptığı denemeler sırasında Beyaz Saray'ın telefon hattına sızmayı başarmış ve o dönemki ABD Başkanı Richard Nixon ile bir telefon görüşmesi yapmış ve başkanla "ulusal bir felaket oldu, tuvalet kâğıdım bitti" şeklinde dalga geçmiştir (en.wikipedia.org).

Kevin Mitnick 1981 yılında Amerika'nın en büyük telekomünikasyon şirketlerinden biri olan Pasific Bell'in merkezine arkadaşı Roscoe ile birlikte girmiştir. Bu işi çöp kutuları sayesinde başarmıştır. Mitnick, arkadaşıyla birlikte şirketin çöp kutularını karıştırırken, şirkete ait yazışma ve parolalar içeren belgeler bulmuştur. İçeriye sızabilmesi için gerekebilecek çoğu şeyi çöp kutularından elde eden Mitnick, daha sonra şirket personeli kılığına bürünmüş ve firmaya sızmıştır. Mitnick, firmadan önemli dokümanları çalmış; fakat şirket yöneticilerinin durumu fark etmesi üzerine yakayı ele vermiş ve üç aylık bir hapis cezasına çarptırılmıştır.

Mitnick yine 1985 yılında Amerikan Ulusal Güvenlik Teşkilatı (NSA) bilgisayarlarına sızmış ve bazı yazılımları

çalmıştır. Bir müddet sonra fark edilen Mitnick birkaç yıllık hapis cezası almıştır. Mitnick 1988'de arkadaşları Roscoe ve Lenny ile birlikte Digital Equipments isimli firmanın henüz piyasaya sürmediği VMS isimli işletim sisteminin kaynak kodlarını çalmıştır. Mitnick böylece o dönemde henüz piyasaya sürülmemiş işletim sisteminin ne tür güvenlik açıkları olabileceğini tespit etmiştir. Mitnick bir müddet sonra DOOM isimli bir bilgisayar oyununu çalmak için yine Digital Equipments firmasının ağına sızmış ve FBI tarafından yakalanınca bir yıllık hapis cezası almıştır.

Mitnick'in yaptıkları yukarıdakilerle sınırlı değildir. 1995 yılında Mitnick, NSA'da görevli olan Tsutomu Shimomura isimli bir bilim adamının bilgisayarı dâhil olmak üzere, Fujitsu, Motorola, Nokia ve Sun Microsystems gibi firmaların bilgisayar ağlarına girmiş ve bir müddet sonra yine tutuklanmıştır (edition.cnn.com).

Kayda geçen gerçek anlamdaki ilk siber saldırı ise 1988 yılında yaşanmıştır. Cornell Üniversitesi öğrencilerinden Robert T. Morris, bir bilgisayara bağlanabilecek, sonraki bilgisayara kendini kopyalayabilecek, çeşitli ayrıcalıklar ve güvenlik açıklarını bulabilecek bir program yazmıştır. Daha sonra Morris, bu programı, programın kendisini kopyalaması amacıyla "kazara" çalıştırmıştır. Çalışan program daha sonra kendini ARPANET üzerinde bulunan diğer bilgisayarlara kopyalamaya başlamıştır. Bir müddet sonra bu kopyalamanın yarattığı hasardan doları o tarihte ARPANET'e bağlı olan 88.000 bilgisayarın %10'u, aynı anda çalışamaz duruma gelmiştir. Böylece tarihe geçecek ilk "Worm" (solucan) saldırısı gerçekleştirilmiştir (Yılmaz ve Salcan, 2008: 36). Bu saldırıyı Mitnick'in ilk saldırılarından ayıran temel unsur, saldırının ağ üzerindeki binlerce bilgisayarı etkilemesidir.

1998 yılında o güne kadar ki en büyük internet sahteciliği yaşanmıştır. Kanadalı bir bilgisayar korsanı olan Kenneth H.

Taves 900.000 kredi kartı kullanıcısından bir porno sitesinin aylık ücreti olan 19,95 dolar çekmiş ve toplamda 37,5 milyon dolarlık bir vurguna imza atmıştır. Kredi kartı hesap özetlerinde bu bilgiyi gören kişiler yetkili kurumlara şikâyette bulunmuş, yakalanması üç yıl süren Taves ise 135 aylık hapis cezasına çarptırılmıştır (theage.com.au).

1999 yılında David L. Smith isimli bir bilgisayar korsanı Microsoft Word makro tabanlı bir bilgisayar virüsü oluşturmuştur. Virüs e-postalar aracılığıyla dünya üzerinde hızla yayılmıştır. İnternette mesaj yöntemi ile çoğalan bir makro virüsü olan Melisa, Office 97 ve 2000 dosyalarına bulaşarak yavaş yavaş dosyalara zarar vermeye başlamıştır. Adres listesindeki herkese insanların haberi olmadan gönderilen bu virüs başarılı bir şekilde yayılmıştır (gazetevatan.com).

Yine 1999 yılında Jonathan James henüz 16 yaşındayken, NASA'nın bilgisayar ağına sızmayı başarmış ve bu ağa açık kapılar yerleştiren virüsler bırakmıştır. James daha sonra bu ağdan 1,7 milyon dolar değerinde yazılımlar çalmıştır (tomshardware.com).

2004 yılının Ekim ayında 21 yaşındaki üstün yetenekli bilgisayar korsanı Nicolas Jacobsen, dev bir şirket olan T-Mobile'in hizmet sunucularına girmiştir. Jacobsen, şirketin 16,3 milyon müşterisinin aralarında sosyal güvenlik numaraları, pin kodları, doğum tarihleri ve e-posta şifreleri bulunan kişisel bilgileri ele geçirmiştir (Yılmaz ve Salcan, 2008: 49).

Çin, İran, Rusya ve ABD gibi ülkeler daha önce siber uzaydaki savaş arenasında defalarca karşı karşıya gelmiştir. 2010 yılında ise o zamana kadar tasarlanmış ve şu anda bile itibarını bir nebze olsun kaybetmemiş olan STUXNET isimli en karmaşık virüs bazı ülkeleri siber arenada bir kez daha karşı karşıya getirmiştir. STUXNET bugüne kadar tespit edilmesi en zor, en karmaşık ve farklı şekillerde yayılabilen; aynı anda birkaç virüs türünün yapısını içinde barındıran virüstür.

Bu virüs direkt olarak İran'ın nükleer araştırma tesislerini hedef almış ve tesislerin sistemlerine zarar vermiştir. Virüs dünyadaki birçok ülkeye bulaşmış, sistemlerde yıllarca kalmış ve tespit edilmesi çok uzun süre almıştır (siberbulten.com).

Çalışmamızın bu kısmında geçmişten günümüze dek bilgisayar korsanlığının ve siber saldırıların evrimini bilişim dünyasında kendine önemli yer edinmiş ünlü korsanların bazı saldırılarından örneklerle ortaya koyduk. Görüldüğü üzere ilk saldırılar telefon hatlarına sızma şeklinde başlamışken daha sonra, internet ağlarına sızılmaya başlanmıştır. Mitnick gibi korsanlar toplum mühendisliği yeteneklerini kullanarak çıkar elde etmek için özel şirketlere sızmaya çalışırken; kimi ünlü olmayan bilgisayar korsanları banka müşterilerini hedef alıp dolandırıcılığın yollarını aradılar. Özel şirketleri ve devlet kurumlarını hedef alan saldırılar, bir süre sonra devletlerin ve hükûmetlerin de dâhil olduğu saldırılara dönüşmüşlerdir. İnternet ortamında dolaşan önemli verileri elde etmeye yönelik istihbarat savaşı siber arenaya taşınmıştır. Telefon ağlarına sızma dâhil, sırasıyla örneklerini verdiğimiz her saldırı türü günümüzde ortaya çıkmaya devam etmektedir.

Bazı önemli saldırılara çalışmamızın kapsamıyla uyuşmaması sebebiyle yer vermedik. Bu saldırıların arasında ülkelerin birbirlerine düzenlediği birçok siber saldırı da vardı; fakat biz çalışmamızda ilgisi olması nedeniyle genellikle kişisel verileri hedef alan saldırılara odaklandık. 2013 yılından itibaren gerçekleşen ve internet güvenliği ile çevrimiçi gizliliği ihlal eden güncel saldırılara geniş olarak çalışmamızın sonraki bölümünde yer vereceğiz.

3.3.5. Günümüzde (2013 ve sonrası) dikkat çeken siber saldırılar ve bilgisayar korsanlarının faaliyetleri

Son yıllarda siber saldırılar ve bilgisayar korsanlarının faaliyetlerinde ciddi bir artış gözlemlenmiştir. Teknoloji siteleri ziyaret edildiğinde karşımıza sürekli olarak önemli bir kurumun ağ altyapısının bilgisayar korsanları tarafından çökertildiğine dair haberler çıkmaktadır. 2013 ile günümüze dek gerçekleşen önemli siber saldırıları, dünyanın ve ülkemizin en önemli teknoloji sitelerini referans alarak aşağıda yer verdik.

3.3.5.1. Adobe'nin hacklenmesi

2013 yılının Eylül ayında Photoshop, Premier ve After Effect gibi dünyaca ünlü fotoğraf ve video düzenleme yazılımlarını üreten Adobe isimli firmanın internet sitesi ve veri tabanı siber korsanların hedefi olmuş, bunun sonucunda 38 milyon müşterinin kişisel bilgileri ve şifreleri bilgisayar korsanları tarafından ele geçirilmiştir.

Adobe'nin kullandığı şifreleme algoritmasının zayıf olması ve bunun güvenlik zaafı oluşturması sebebiyle hackerlar kolayca kişisel verilere ve şifrelere ulaşabilmişlerdir. Yaşanan bu gelişme Adobe ve müşterilerinin yaşayabileceği sorunlar dışında yeni sorunlar oluşturabileceği nedeniyle önemlidir. Bilgisayar korsanlarının Adobe internet sitesinde kullanılan şifreleme algoritmasını kolay şekilde çözmeleri, bu şifreleme algoritmasının farklı firmaların internet sitelerinde de kullanılma ihtimalini akla getirecektir. Bilgisayar korsanları, Adobe şifreleme algoritmasını çözen uygulamaları farklı internet siteleri üzerinde deneyebileceklerdir (reuters.com).

3.3.5.2. iCloud isimli uygulamanın hacklenmesi

Cep telefonu, tablet ve bilgisayar üreticisi Apple'ın müşterileri için geliştirdiği bulut tabanlı depolama/yedekleme uygulaması iCloud, 31 Ağustos 2014 tarihinde bilgisayar

korsanlarının hedefi olmuş ve bu uygulamanın korsanlar tarafından hacklenmesi (kırılması) sonucunda aralarında çoğunluğu bayan olmak üzere Jennifer Lawrence, Kate Upton, Justin Verlander, Mary Elizabeth Winstead, Jessica Brown Findlay, Kaley Cuoco ve Kirsten Dunst'ta bulunduğu sinema ve televizyon dünyasından 100'den fazla ünlü ismin 500'e yakın uygunsuz fotoğraf ve videoları 4chan isimli forum sitesinde paylaşılmıştır. Forumda yapılan bu paylaşım dünyada çok büyük bir etki yaratmış ve ünlülerin bu uygunsuz fotoğrafları tüm internet âlemine çok kısa bir süre içinde yayılmıştır. Hatta bu olayın faillerini bulmak için "FBI" (Amerikan Federal Soruşturma Bürosu) devreye girmiştir (telegraph.co.uk).

Bu haber yazılı ve görsel basında çok büyük bir yer bulmuş, dünyaca ünlü gazetelerin ilk sayfalarından verilmiş, ayrıca ana haber bültenlerinin konusu olmuştur. Yaşanan bu gelişmenin ardından gözler dünyanın en büyük telefon ve bilgisayar üretici firmalarından biri olan Apple'a çevrilmiştir. Apple'dan fotoğraf ve videoların sızmasından sonra iki gün boyunca olayla ilgili hiçbir açıklama gelmese de; iki gün sonra Apple olayın doğruluğunu kabul edip aşağıdaki açıklamayı yayınlamıştır:

> *Ünlülerin çalınan fotoğrafları ile ilgili yaptığımız araştırma hakkında bilgi vermek istedik. Bu hırsızlıktan haberdar olunca hemen Apple'ın mühendislerini olayın kaynağını bulmaları için harekete geçirdik. Müşterilerimizin özeli ve güvenliği bizim için en önemli olandır. 40 saati aşan bir araştırma sonra ortaya çıkan şudur ki bu saldırı kişileri hedef almıştır. Hesapları ele geçirilen ünlülerin güvenlik soruları ve şifrelerine yönelik çalışmalar yapıldığı ortaya çıkmıştır. Bu internette çok yaygın olan bir saldırı biçimidir. Haliyle bu saldırıların hiç biri Apple'ın sistemindeki bir açıktan kaynaklanmamaktadır. Buna iCloud® ve Find my iPhone da dâhildir. Şu anda suçluları bulmak için güvenlik güçleri ile beraber çalışmalarımızı*

sürdürüyoruz. Bu tarz saldırılara karşı daha güvenli olmaları için müşterilerimize her zaman iki aşamalı kimlik doğrulamasını tavsiye ediyoruz (iphonedo.net).

Yukarıdaki açıklamada Apple'ın kendisine yöneltilen "güvenlik temelli" eleştirileri reddettiği anlaşılmaktadır. Apple, kendi şifreleme algoritmalarında herhangi bir açık bulunmadığını, aksine fotoğraf ve videoları çalınan ünlülerin kullandıkları şifrelerin kolayca kırılabilecek kadar zayıf olduğunu veya bilgisayar korsanlarının şifreleri elde etmek için phishing ya da sosyal mühendislik yöntemlerinin kullanılmış olabileceğini öne sürmüştür. Ortada kimin haklı olduğuyla ilgili kesin bir şey olmasa da kişisel verilerimizin çevrimiçi ortamda ne kadar güvenli bir şekilde muhafaza edilebileceği konusunda insanların kafasında soru işaretleri oluşmuştur.

Yukarıda detaylarıyla birlikte ortaya koyduğumuz olayın ikinci dalgası 20 Eylül 2014 tarihinde gerçekleşmiştir. Aralarında Jeniffer Lawrence, Kim Kardashian, Vanessa Hudgens, Hope Solo, Aubrey Plaza, Mary-Kate Olsen, Hayden Panettiere ve Leelee Sobieski gibi ünlü isimlerin fotoğraf ve videoları yine aynı şekilde iCloud adlı uygulama üzerinden ele geçirilmiş ve 4chan isimli internet sitesi ile Reddit isimli sosyal paylaşım sitesi üzerinden internet dünyasına yayılmıştır (businessinsider.com).

3.3.5.3. SnapChat isimli uygulamanın hacklenmesi

Henüz iCloud'ın hacklenme olayının şoku atlatılamamışken Ekim 2014'te bu kez en çok kullanılan sohbet uygulamalarından biri olan SnapChat[10] hackerların hedefi olmuştur.

[10] SnapChat Android ve IOS işletim sistemli telefonlarda kullanılan bir sohbet uygulamasıdır. SnapChat'in kendine has bir çalışma mantığı vardır. Bu uygulamada karşıya bir fotoğraf ya da video gönderebiliriz, bu fotoğraf ya da videonun üstüne not ekleme imkânımız da vardır. Yalnız gönderdiğimiz iletiyi karşıdaki kişi bizim belirlediğimiz bir zaman diliminde görür, bu

SnapChat'in hacklenmesi ise şu şekilde gerçekleşmiştir: SnapChat aracılığıyla karşı tarafa gönderilen fotoğraf, video gibi içerikleri otomatik olarak kullanıcıların çevrimiçi hesaplarına yedekleyen üçüncü parti bir yazılım mevcuttur. Bu yazılımı SnapChat kullanan kullanıcıların çoğu SnapChat ile bütünleşik olarak çalıştırıyorlardı. Bilgisayar korsanları bu yazılım üzerinden kullanıcıların çevrimiçi hesaplarına sızmış ve bu hesaplardaki binlerce fotoğraf ve videoyu ele geçirmişlerdir. Buradan ele geçirilen içerikler tıpkı iCloud olayında olduğu gibi yine 4chan isimli forumda yayınlanmıştır. Daha sonra bu içerikler torrent sitelerine yüklenerek tüm dünyanın erişimine açılmıştır (mashable.com).

3.3.5.4. Sony Pictures'ın hacklenmesi

Dünyanın en büyük teknoloji şirketlerinden biri olan ve bilgisayar korsanlarıyla arasındaki sorunlar bitmek bilmeyen Sony, dünya bilişim tarihine damga vuran en büyük siber saldırılardan biriyle karşı karşıya kalmıştır. Bu saldırı 2011 yılında Sony PSN[11] servislerinin bilgisayar korsanları tarafından uzun bir süre devre dışı bırakılmasından bile kat kat büyük bir saldırıdır. Öyle ki bu siber saldırı dünyada en fazla ses getiren saldırılar arasına adını yazdırmıştır.

24 Kasım 2014 tarihinde Sony Pictures[12]'e ait bilgisayarların dış dünya ile bağlantısı kesilmiş ve Sony Pictures'ın

---

zaman dilimi 1 ile 10 saniye arasındadır, bu süreden sonra ileti otomatik olarak silinir.

[11] PlayStation Network (kısaca PSN), çevrimiçi çok oyunculu oyun ve dijital medya ulaştırma servisidir ve PlayStation 3 ve PlayStation Portable video oyunu konsolları için Sony Computer Entertainment tarafından oluşturulmuştur. 2 Haziran 2009 tarihinde dünya çapında 24 milyonun üzerinde PlayStation Network üyesi bulunmaktaydı. PlayStation 3 platformu üzerinden çok oyunculu ve çevrimiçi oyunların oynanabilmesi için PSN kesinlikle gerekmektedir (tr.wikipedia.org).

[12] Sony Pictures Entertainment, Inc. (SPE) Japon teknoloji ve medya şirketi olan Sony'nin yan şirketidir. Kaliforniya'da bulunan şirket sinema filmleri,

internet ağı bilgisayar korsanları tarafından tamamen çökertilmiştir. Sony Pictures'ın internet sitesine girmek isteyen insanlar "Hacked by #GOB" (Guardian of Peace/Barışın Koruyucuları) başlıklı bir mesajla karşılaşmışlardır. Mesajın içeriğinde "Sizi önceden uyarmıştık, bu daha başlangıç. Gizli ve çok gizli olmak üzere tüm iç verilerinizi ele geçirdik Bize boyun eğmezseniz, elimizdeki bütün içerikleri dünyayla paylaşacağız. 24 Kasım saat 23.00'e kadar ne yapacağınız konusunda kararınızı verin" yazmaktaydı. Hackerlar bu mesajın altına Sony'nin istenilen şeyleri yerine getirmediği takdirde verilerin paylaşılacağı linki de eklemişlerdi (thenextweb.com).

Bir müddet sonra ABD'li yetkililer Hollywood'un en ünlü film stüdyolarından biri olan Sony Pictures'a yapılan saldırının Kuzey Kore'yle bağlantılı bilgisayar korsanları tarafından işlendiği sonucuna varmışlardır (nbcnews.com).

Bilgisayar korsanlarının neden böyle bir işe giriştikleri fikri kafalarda dolaşmaktayken, kısa bir süre sonra olayın asıl sebebi anlaşılmıştır. Şirketin yapımını üstlendiği ve Kuzey Kore lideri Kim Jong Un'la ilgili hayali bir suikastın anlatıldığı "The Interview" isimli komedi filmi birilerini çok kızdırmıştı.

Bu olayın ardından Sony'e bilgisayar korsanları tarafından verilen sürenin dolmasıyla birlikte, korsanlar Sony sunucularından topladıkları 100 TB büyüklüğündeki içeriği internete sızdırdılar ve niyetlerinin son derece ciddi olduğunu gösterdiler. Sızan bu verilerin arasında Sony görevlilerinin eposta hesapları ve şifreleri, kredi kartı bilgileri, sosyal güvenlik numaraları gibi kişisel bilgiler de vardı. Saldırının gerçekleştiği gün Sony'de çalışan bazı kişilerin banka hesapları da hacklendi ve kara borsaya düştü (webrazzi.com).

---

televizyon yapımları gerçekleştirmekte ve bu yapımların dağıtımını üstlenmektedir.

Sony Pictures'ın internet ağında yaratılan tahribatın onarılmasının günlerce sürmesi bir kenara; bu saldırıyla birlikte Sony Pictures'ın marka değerini zarara uğratacak çok sayıda "gizli bilgi" sızmıştır.

Bu saldırı sonunda sızan bilgilerden bazılarını derleyecek olursak:

- iCloud'un hacklenmesinden en çok zarar gören sanatçılardan biri olan Jennifer Lawrance'in erkek meslektaşlarından çok daha düşük ücrete çalıştığı ortaya çıktı.
- 1 milyon dolardan yüksek kazanan 17 çalışandan yalnızca biri kadındı.
- Aralarında ünlü artistlerin de bulunduğu 47 bin Sony çalışanın kişisel bilgileri sızdı.
- Sony'nin diğer yapım şirketleriyle birlikte Google'a karşı lobi faaliyetleri yürüttüğü ortaya sızan yazışmalarda ortaya çıktı. Google'ın telif haklarını ihlal eden linkleri arama sonuçlarından kaldırmamasından dolayı Sony'nin Google'a çok kızdığı yazışmalardan anlaşılıyordu.
- Sony'nin hangi film için hangi sanatçıyla ne kadara anlaştığı ortaya çıktı.
- Cleopatra filminde oynamak isteyen Angelina Jolie için Sony'nin üst düzey bir yöneticisinin hakaret içeren yazışmaları ortaya çıktı.
- Sony'nin müzik dağıtım işini bırakmayı düşündüğüne dair bazı yazışmalar ortaya çıkmıştır.
- The Interview dâhil olmak üzere Sony tarafından çekilen birçok film hackerlar tarafından sızdırıldı. Sony, The Interview'in gösterimini iptal etmek zorunda kaldı (theverge.com).[13]

[13] Sony Pictures'ın hacklenmesiyle beraber sızan bilgilerin tam listesine ve olayla ilgili haberlerin hepsine İngilizce olarak http://www.theverge.com/

Yazılı ve görsel medyada büyük yankı uyandıran sızıntıların ardından Sony, gazete ve haber sitelerinden bu konuyla ilgili haber yapmamalarını istemiştir. Ayrıca Twitter başta olmak üzere bazı sosyal medya sitelerindeki kullanıcıların bu olayla ilgili materyalleri sızdırması ve bağlantı paylaşımı yapmaları üzerine Sony, sosyal medya sitelerini tehdit etmiş; bu kullanıcıların üyeliklerinin bloke edilmediği takdirde yasal yollara başvurulacağını açıklamıştır (theverge.com).

Marka değeri ve itibarı sarsılan Sony, bir süre sonra bilgisayar korsanlarının isteklerine boyun eğmek zorunda kalmıştır. Bunun üzerine korsanlar ikna olduklarını ve daha fazla veri sızdırmayacaklarının garantisini vermişlerdir. ABD devlet başkanı Barack Obama, Sony'nin bilgisayar korsanlarına boyun eğmesini ve geri çekilmesini eleştirmiştir (polygon.com).

Yaşanan bu büyük olay teknoloji gündeminden üç ay boyunca düşmemiştir. Yazılı ve görsel basında bu olayın arkasında 12 yaşında Kuzey Kore ordusu tarafından alınan ve bir bilgisayar korsanı olarak yetiştirilmeye başlayan hackerlardan söz ediliyordu. Güney Kore istihbaratında görev alan yetkililere göre Kuzey Kore'de yetiştirilmekte olan Siber Korsanların sayısı 3000'i bulmaktadır. Kuzey Kore'nin pahalı askeri saldırılar yerine, 'asimetrik savaş' yürütebilecek siber saldırı operasyonlarına yönelebileceğine dikkat çekilmiştir (İnternetsiz ülkenin 'hacker' askerleri, 2014).

Sony bu saldırının yaralarını henüz yeni sarmaya başlamışken 2015 yılının başlarında bilgisayar korsanları yine Sony'i hedef almışlardır. Sony'nin geliştirdiği Play Station adlı oyun konsolunun dijital ağı (PSN) korsanlar tarafından DDOS saldırılarına uğramış ve bir müddet devre dışı

2014/12/8/7352581/sony-pictures-hacked-storystream bağlantısından ulaşılabilir.

kalmıştır. Neyse ki Sony bir süre sonra saldırılara karşı önlem almış ve servisini yeniden aktif etmiştir (polygon.com).

3.3.5.5. Spotify'ın hacklenmesi

Dünyada en fazla kullanılan çevrimiçi müzik dinleme platformu Spotify 2014 yılının Mayıs ayında kötü niyetli kişilerin hedefi olmuş ve hacklenmiştir. Milyonlarca kullanıcısı olan bu büyük platformun böyle kötü bir olay yaşaması internet basınında geniş yer bulmuş, özellikle teknoloji sitelerin bu haberin üzerinde fazlasıyla durulmuştur (yahoo.com/tech/).

Bu olayın gerçekleşmesinden sonra Spotify internet sitesinde "kullanıcılarımız için önemli duyulu" başlığı altında bir duyuru yayınlamıştır. Duyuruda olayın üstünde fazla durulmasının gerekmediği, yalnızca bir kullanıcının kişisel bilgilerinin ele geçirildiğini ve bu olayın bir daha yaşanmaması için yeni güvenlik önlemlerinin hayata geçirileceği belirtilmiştir. Duyurunun çalışmamızla ilgili kısımları şu şekildedir:

> *Sistemimize ve şirket içi bilgilerimize bazı izin verilmemiş girişlerin yapıldığını bildiğimizi ve karşılığında gerekli adımları attığımızı sizinle paylaşmak istedik. Bu durumdan haberdar olur olmaz bir araştırma başlattık. Bilgi güvenliği ve data koruma Spotify'da en önem verdiğimiz konular arasında ve bu yazıyı bugün sizinle bu sebeple paylaşıyorum. Elimizdeki veriler sadece bir Spotify kullanıcısına ait bilgilere ulaşıldığını ancak bu bilgiler arasında herhangi bir şifre, finansal veya ödeme bilgisi bulunmadığını gösteriyor. Bu kullanıcımıza ulaşmış bulunuyoruz. Bulgularımızı dayanarak, bu olayın sonucu olarak kullanıcılarımız için herhangi bir artan risk bulunmamakta olduğunu söyleyebiliriz. Buna benzer konuları oldukça ciddiye alıyoruz ve genel bir önlem olarak, önümüzdeki günlerde bazı Spotify kullanıcılarından kullanıcı adı ve şifrelerini tekrar girmelerini isteyeceğiz. Ek bir güvenlik adımı olarak, önümüzdeki günlerde Android uygulamamızın kullanıcılarını yeni sürüme*

geçmeleri konusunda yönlendireceğiz. Eğer Spotify uygulaması tarafından bir üst sürüme geçmek için uyarılırsanız, yönlendirmeleri takip edebilirsiniz (news.spotify.com).

3.3.5.6. Heartbleed açığının keşfedilmesi

7 Nisan 2014'te internet güvenliği ve çevrimiçi gizlilikle alakalı ciddi bir güvenlik açığı fark edilmiştir. Bu açığa "Heartbleed (Kalp Kanaması)" adı verilmiştir. Bu güvenlik açığı internet tarayıcılarında gördüğümüz HTTPS bağlantı protokolü (güvenli bağlantı) kullanan (https:// ile başlayan adresler) internet sitelerini etkilemiştir.

Buna göre; Heartbleed, popüler kriptografik yazılım kitaplığı OpenSSL'deki[14] ciddi güvenlik açığıdır. Heartbleed güvenlik açığını suiistimal eden saldırganlar, OpenSSL'nin bazı sürümlerini kullanan sistemlerin belleğini okuyarak SSL için kullanılan sunucudaki kullanıcı adlarına, şifrelere ve gizli kriptografik anahtarlara ulaşabilmektedir. Kötü amaçlı kullanıcılar, ele geçirilen bu anahtarlar ile sistemdeki bütün iletişimi gözlemleyebilmekte ve sisteme daha fazla zarar verebilmektedirler (trendmicro.com.tr).

Verilen bilgilere göre bu açıktan OpenSSL kullanan mevcut site oranı %66'dır. Bu internet sitelerinin yalnızca %17'si bu açıktan etkilenmişlerdir. OpesSSL alternatiflerini kullanan internet siteleri ise bu açıktan etkilenmemişlerdir (news.netcraft.com).

Bu açıktan etkilenen internet siteleri arasında Facebook, Instagram, Pinterest, Tumblr, Google, Yahoo Gmail, Yahoo Mail, Elsy, GoDaddy, Box, Dropbox, GitHub, OkCupid, SondCloud gibi çok sık kullanılan ve milyonlarca kullanıcısı bulunan birçok internet sitesi vardır. İnternet güvenliği

[14] OpenSSL, internetteki iletişimin gizliliğini korumada kullanılan SSL/TLS şifreleme protokolünün bir uygulamasıdır. OpenSSL, birçok web sitesinde ve e-posta, anlık mesajlaşma ve VPN gibi uygulamalarda kullanılır.

uzmanları yaptıkları açıklamalarda bu açıktan etkilenmiş internet sitelerini kullanan kullanıcılara acilen bu sitelerde kullandıkları parolaları değiştirme çağrısı yapmışlardır (teknokulis.com).

Heartbleed açığı aynı gün yayınlanan güncelleme ile kapatılmış ve OpenSSL tarafından, sunucularında OpenSSL kullanan webmasterlara sunucularına yeni güncellemeyi yüklemeleri tavsiye edilmiştir.

3.3.5.7. ABD kamu personeli bilgilerinin çalınması

Mayıs 2015'te ABD yetkilileri, Çin'de bulunan hackerların Amerikan vatandaşları hakkında soruşturma yürütüp federal hükûmette çalışmaları için temiz belgesi çıkaran federal daireye siber saldırı düzenlediklerini belirttiler. Saldırıdan sonra milyonlarca devlet çalışanının bilgilerinin çalındığı fark edilmiştir. Personel Yönetimi Dairesi (OPM), uzun zamandır yapılan en büyük siber saldırıdan 4 milyona yakın eski ve mevcut federal hükûmet çalışanının etkilenebileceğini söylenmiştir.

ABD'nin insan kaynakları ofisi olarak faaliyet gösteren OPM, aslında bilgisayar korsanları için önemli bir hedeftir. OPM'in bilgisayarlarında çalışanları hakkında sosyal güvenlik numaraları, çalıştıkları kadrolar ve aile bilgileri gibi birçok hassas bilgiler bulunmaktadır. OPM, siber saldırıları Nisan ayında fark ettiklerini ve derhal kontrollerini arttırdıklarını söylemiştir. FBI ve Ulusal Güvenlik Dairesi, hasarın boyutunu tespit etmek için soruşturma açmıştır. Yapılan açıklamalarda hangi tür verilerin çaldırıldığı belirtilmemiştir (Opm hack, 2015).

3.3.5.8. Kaspersky'nin hacklenmesi

2015 yılının Haziran ayında çok ilginç bir olay gerçekleşmiştir. Dünyanın en büyük Çevrimiçi Güvenlik Sistemleri ve

Antivirüs Yazılımları üreticilerinden biri olan Rus şirket Kaspersky, bilgisayar korsanları tarafından büyük bir saldırıya uğramıştır.

Kaspersky yetkilileri tarafından yapılan açıklamada saldırıda kullanılan virüsün daha önce tanımlanamayacak nitelikte çok güçlü ve gelişmiş bir virüs olduğu, bu virüsü geliştirmek için çok büyük bir bedel ödenmesi gerektiği altı çizilmesi gereken bir nokta (computerworld.com).

Kaspersky kurucusu Eugene Kaspersky bu saldırıyla ilgili şöyle bir açıklama yapmıştır:

Size bir iyi bir de kötü haberim var. Şirket içi ağlarda gelişmiş ve kompleks bir saldırı tespit edildi. Kaspersky Lab'a yapılan bu saldırı Kaspersky teknolojilerini öğrenmek için yapıldı. Saldırıyı kimin yaptığını henüz bilmiyoruz fakat eminiz ki bu saldırının arkasında bir devlet var. Biz bu kötü yazılıma Duqu 2.0 ismini verdik. Buradaki saldırı gerçekten çok büyük ve daha önce görülmemiş çok gelişmiş bir yazılım kullanıyor. Bu yazılımı üretmek bile devasa bedeller ister. İyi haber ise, biz bu virüsü erken safhada tespit etmiş bulunuyoruz. Daha da önemlisi, bu saldırı ürünlerimizi ve servislerimizi etkilememiş durumda. Bütün müşterilerimiz güvende.

Kaspersky'a yapılan bu saldırıyı iyi yönde değerlendirerek ürünlerini ve hizmet kalitesini daha da iyileştirmek için kullanacaklarını belirten Eugene Kaspersky, Duqu 2.0 kötü yazılımının arkasındaki kişilerin daha önce de İran'ın nükleer programına saldırı yapanlarla aynı olduğunu tespit edildiğini söylemiştir.

Devletlerin siber güvenlik şirketlerine yaptığı saldırıları "çok çirkin" olarak betimleyen Eugene Kaspersky, tüm devletleri sanal gerçeklik kurallarına ve etik değerlerine saygılı olmaya çağırarak konuyla ilgili araştırmaların derinleşerek devam edeceğini belirtmiştir (turk-internet.com).

Antivirüs yazılımları üreten büyük firmaların bile bu türden saldırılara maruz kalmasının, internet güvenliğinin ve çevrimiçi gizliliğin ne durumda olduğunun sorgulanmasını beraberinde getirecektir.

3.3.5.9. MEB veritabanında bulunan kişisel bilgilerinin sızması

Ülkemizde çevrimiçi gizlilik kavramının ihlal edilmesiyle alakalı bilinen en büyük gelişmeler arasında MEB veritabanında bulunan öğrenci, veli ve öğretmenlerin kişisel bilgilerinin 2013 ile 2015 yılları arasında peş peşe sızdırılması ve çalınması da yer almaktadır. Yaşanan bu gelişmelerin sonucunda MEB veritabanında yer alan milyonlarca vatandaşın kişisel bilgileri kötü niyetli şahıslar tarafından ele geçirilmiş ve bu bilgilerin kötü amaçlar için kullanılabilme durumu ortaya çıkmıştır.

MEB verilerinin sızmasıyla ilgili son yıllarda yaşanan olaylardan ilki 2013 yılının Ağustos ayında gerçekleşmiştir. Buna göre aralarında Alman Lisesi, Avusturya Lisesi, Fevziye Mektepleri, Işık Lisesi gibi kolejlerin de bulunduğu birçok liseye ait veriler ele geçirilmiştir. 2011 yılında 11 milyon öğrencinin TC kimlik numarası, yazılı ve sözlü notları, devamsızlık bilgileri, projeleri ve hatta geçirdikleri hastalıkların bile kötü niyetli kişiler tarafından özel sektöre parayla satılmasından sonra yaşanan en büyük olay bu olmuştur.

Çocuğu Alman Lisesinde okuyan bir velinin ortaya çıkardığı olayda, MEB Bilgi Teknolojileri Daire Başkanlığı'nda bulunması gereken verilerin, kötü amaçlı bir şahıs tarafından özel sektöre satılmak üzere bir internet sitesinde yayınlandığı belirlenmiştir (haberler.com).

2013 yılının Kasım ayında ise Bilgi İşlem Grup Başkanlığı'nın aldığı tüm önlemlere rağmen, aralarında Türkiye'nin gözde kolejlerinin de yer aldığı binlerce öğrencinin e-okul

bilgilerinin ikinci kez internete sızdığı anlaşıldı. Yaşanan bu olayın ardından birçok veli MEB aleyhinde suç duyurusunda bulunmuştur. Bunun üzerine soruşturma başlatılmış ve verileri sızdıran şahıslar hakkında 5 yıla kadar hapis cezası istenmiştir (memurlar.net).

2015 yılının başlarında ise bu konuyla ilgili bir olay daha yaşanmıştır. 15 milyon öğrenci ve binlerce öğretmenin kişisel bilgilerinin bulunduğu MEB bilişim sisteminde bir şifre skandalı yaşanmıştır. MEB'den 81 ilin milli eğitim müdürlüklerine gönderilen bir maille, bakanlığın uyarılarına karşın, sisteme giriş yapılan şifrelerin sosyal medya üzerinden, "bakanlık içindeki kötü niyetli kişilere" verildiği belirtilerek, bakanlık içinden e-posta ile gelen şifre taleplerine yanıt verilmemesini istenmiştir (sondakika.com). Buna karşın MEB bir açıklama yaparak iddiaları reddetmiş ve basında yapılan haberleri "masa başı gazetecilik" ürünü olarak nitelendirmiştir.

2011 yılından başlayarak öğrenci, öğretmen ve velilerin kişisel bilgilerinin MEB bilişim veritabanından defalarca kez sızması ya da çalınması, devlet kurumlarında bilişim sistemlerinin ne ölçüde güvenli olduğu konusunda insanlarda birçok soru işaretleri yaratmıştır.

3.3.5.10. Ankara'da tapu bilgilerinin çalınması

2014 yılı Kasım ayında Ankara'da gerçekleşen bir olaya göre evini satmak için emlak ofisine giden bir vatandaş, bu emlak ofisine adını ve soyadını verdikten sonra emlakçının bilgisayara girerek tüm tapu bilgilerini söylemesiyle şoka uğramıştır. Burada kendisine "Ankara'daki herkesin tapu bilgilerine ulaşabiliriz" bilgisi üzerine vatandaş polise ihbarda bulunmuştur. Organize Suçlarla Mücadele Şube Müdürlüğü ekipleri ihbar üzerine çalışma başlatmıştır. Cumhuriyet Savcılığı'nın talimatıyla teknik-fiziki takip başlatan polis, tapu bilgilerinin organize şekilde elden ele geçtiğini belirlemiştir.

Yapılan çalışmada Ankara'daki 1 milyon 568 bin kişiye ait tapu bilgilerinin çalındığı ortaya çıkmıştır. Tapu verilerini ele geçirenlerin, bu bilgileri ise 500 lira karşılığında sattığı belirlenmiştir. Tapu bilgilerinin başta emlakçılar ile bazı banka, kredi kuruluşlarına satıldığı öğrenilmiştir. Polis, teknik-fiziki takibin ardından operasyon başlatmıştır. Yapılan operasyonun ardından şüpheli şahıslar yakalanmıştır. Operasyonda sabit disklere yüklü vatandaşların tapu bilgileri de ele geçirilmiştir. Emniyetteki işlemlerinin ardından adliyeye sevk edilen şüpheliler 20'şer bin lira kefalet ve adli kontrol şartıyla serbest bırakılmıştır (hurriyet.com.tr).

3.3.5.11. HSBC Bank'ın hacklenmesi

2014 yılının Kasım ayında Türkiye'de bankacılık faaliyetleri gösteren HSBC isimli banka, kendi resmi internet sitesinden bir siber saldırıya uğradığını duyurmuştur. Bu olayda bankaya ait olan yaklaşık 2,7 milyon müşterinin bilgileri çalınmıştır. Çalının bilgiler arasında kart ve hesap numarası, kartların son kullanım tarihleri ve kart sahiplerinin isimleri vardır.

HSBC daha sonra kendi internet sitesinden yaşanan olayla ilgili detaylı bir açıklama yapmıştır. Yapılan açıklama şu şekildedir:

> *Bankamız, yakın zamanda kredi kartları ve banka kartlarına yönelik bir siber saldırı tespit etmiş ve durdurmuştur. Olayın tespit edilmesi üzerine, müşterilerimizin korunması amacıyla ilave bir dizi önlem alınmıştır. Konuyla ilgili olarak başlattığımız inceleme, BDDK ve ilgili diğer resmi kurumlarla ulusal ve uluslararası düzeyde işbirliği içerisinde devam etmektedir. Bankamızın kart operasyonları normal akışına uygun olarak sürmektedir. Söz konusu olay neticesinde, müşterilerimize ait kart ve kartın bağlı bulunduğu hesap numarası, kart son kullanım tarihi ve kart sahibi ismine ulaşılmıştır. Müşterilerimize*

ait başka herhangi bir finansal veya kişisel bilgiye ulaşıldığına dair bir bulgu yoktur. Aynı zamanda, bu olaydan kaynaklanan herhangi bir dolandırıcılık girişimi veya şüpheli işlem tespit edilmemiştir. Müşterilerimiz, bankacılık işlemlerine her zamanki gibi güvenli bir şekilde devam edebilir. Söz konusu olaydan dolayı müşterilerimizden özür dileriz. 74 ülkede faaliyet gösteren, dünyanın en büyük bankalarından HSBC Grubu, bu olay nedeniyle müşterilerimizin herhangi bir finansal riske maruz kalmayacaklarını teyit eder (technopat.net).

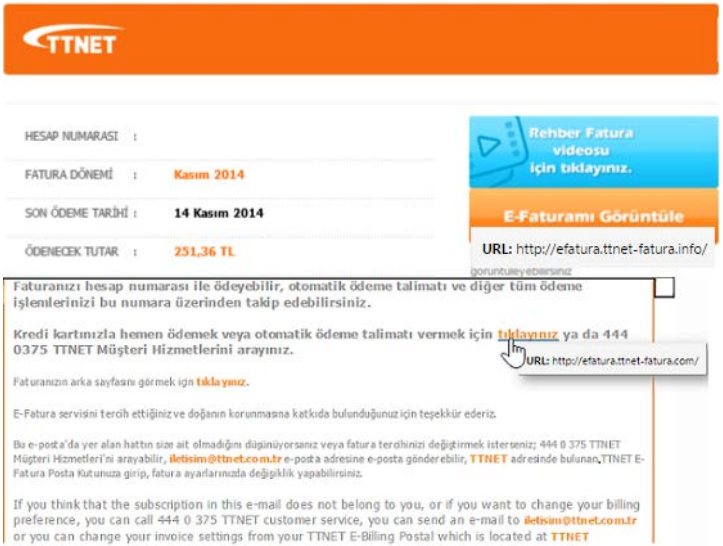
HSBC böylece müşterilerinin kesinlikle hiçbir şekilde finansal açıdan mağdur olmayacaklarını söylemiştir. HSBC, Herhangi bir dolandırıcılık olayının tespit edilmediğinin; ileride tespit edilmesi halindeyse müşterilerinin her türlü zararını karşılayacağını belirtmiştir.

3.3.5.12. Cryptolocker virüsü

2014'ün yaz aylarında ülkemizde Cryptolocker isimli bir virüs ortaya çıkmıştır. Ülkemiz internet kullanıcılarını hedef alan bu virüs, toplum mühendisliği tekniklerinden de yararlanılarak oluşturulmuş üstesinden gelinmesi zor bir virüstür.

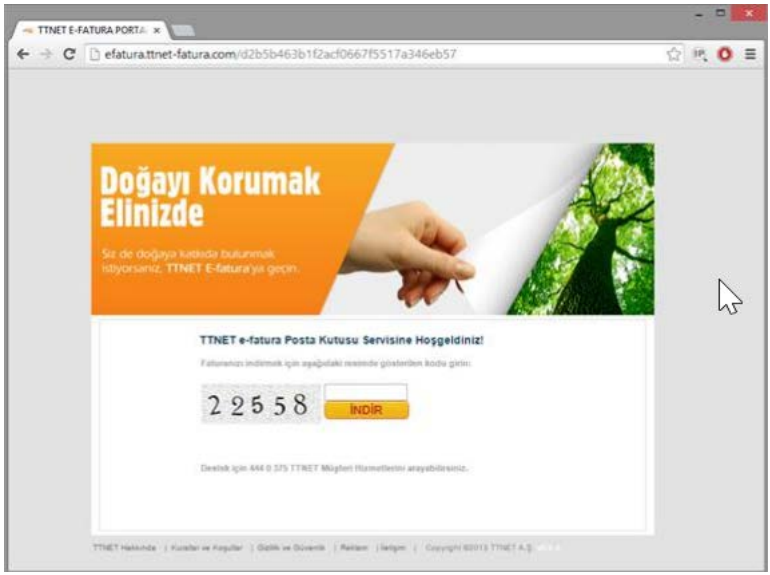
Kendini açık bir şekilde CryptoLocker olarak tanıtan bu yeni zararlı yazılım, yine kullanıcılara ait belli uzantılara sahip dosyaları şifrelemekte ve bu verilerin kurtarılması için kullanıcılardan "Şifre çözme yazılımı" adında bir yazılım satın almalarını istemektedir (bilgiguvenligi.gov.tr).

Bu zararlı yazılımı kodlayan bilgisayar korsanları, internet kullanıcılarına Ttnet ve Superonline gibi internet hizmeti sağlayan kuruluşlarının faturalarını taklit eden sahte e-postalar göndermektedir. Aşağıdaki resim incelendiğinde e-posta içerisinde bulunan bağlantıların http://efatura.ttnet-fatura.info/ gibi sahte ve taklit alan adlarına yönlendirildiği gözlemlenmektedir.



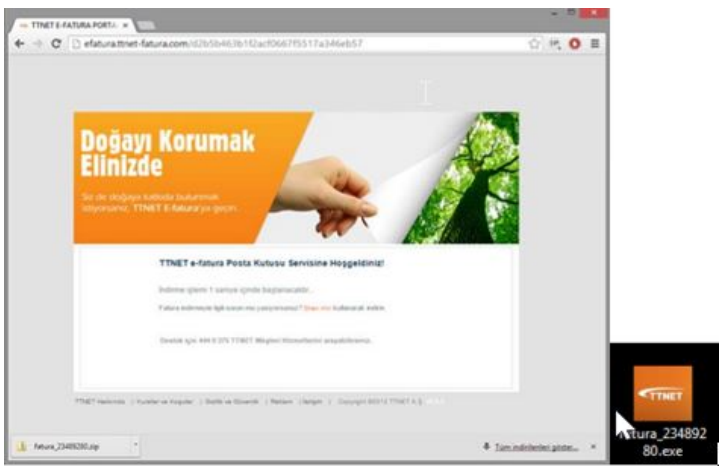
Resim 3.3. Cryptolocker Virüsü İçeren Sahte E-posta

Yukarıdaki resimde gösterildiği üzere fatura tutarı yüksek miktardadır. Faturaların yüksek tutarından ötürü fatura hakkında bilgi almak isteyen kullanıcılar bu faturayı görmek istediklerinde aşağıdaki resimde gösterilen web sitesine yönlendirilmektedir.



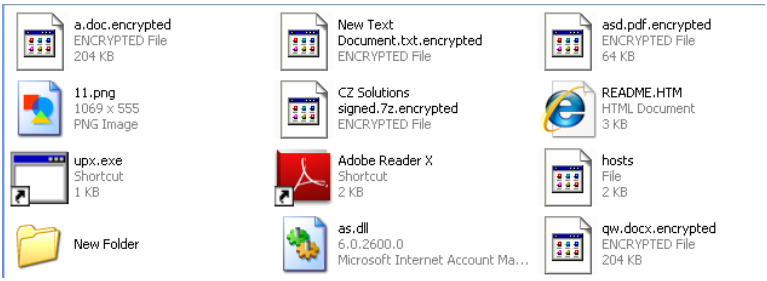
Resim 3.4. Cryptolocker Virüsünü Barındıran Sahte Fatura

Yukardaki resimde gösterilen kodu girip indir butonuna bastıktan sonra ".zip" uzantılı bir dosya inmektedir. Bu dosyanın içinde ise ".exe" uzantılı fatura dosyası (zararlı yazılım) bulunmaktadır.



Resim 3.5. Cryptolocker Virüsünün İndirildiği Bağlantı

İndirilen bu zararlı yazılım çalıştırıldığında ise kullanıcının bilgisayarına virüs bulaşmakta ve bilgisayarda bulunan .doc, .docx, .pdf, .txt, .rar, .7z, .zip uzantılarına sahip olan dosyalar şifrelenmektedir. Şifrelenen dosyaların yeni uzantıları. encrypted (şifrelenmiş) şekline olmaktadır. Aşağıdaki resimde bu durum gösterilmiştir.



Resim 3.6. Cryptolocker Virüsünün Dosyaları Şifrelemesi

Zararlı yazılım bilgisayardaki verileri şifreleme işlemini bitirdikten sonra ekrana aşağıdaki resim gibi bir sayfa çıkarmaktadır. Görüldüğü üzere zararlı yazılım şifrelenen veriler karşılığında 'şifre çözme yazılımı' adı altında bir yazılımın satın alınmasını istemektedir.

Resim 3.7. Cryptolocker Virüsünün Verdiği Uyarı

Yukarıda çıkan bağlantılara tıklandığında aslında tor ağı üzerinde olan, fakat bir tor proxy hizmeti veren sunucu üzerinden erişilebilen kişiye özel bir web sayfasına yönlendirilme yapılmaktadır. Şifre çözme yazılımının satın alınması konusunda ise 96 saat içinde satın alımı durumunda 2398 liradan 1198 liraya kadar indirim yapmaktadır.

Bu virüs ilk yayıldığında antivirüs programlarının büyük bir çoğunluğu tarafından tanınmamıştır. Ayrıca şifrelenmiş dosyaları çözmek üzere satın alınacak yazılımın ödemesinin 'bitcoin'[15] isimli sanal para birimi ile yapılması istenmektedir.

[15] Bitcoin (sembolü: ฿, kısaltma: BTC) herhangi bir merkez bankası, resmi kuruluş, vs. ile ilişiği olmayan elektronik bir para birimidir. 3 Ocak 2009'da hayata geçmiştir. Herhangi bir merkezden üretilmeyen Bitcoinler, Bittorent ağlarına benzer şekilde noktadan-noktaya dağıtık bir ağ özelliği gösterir. Bu ağda gerçekleşen ödemeler diğer noktalara anında ulaşır, böylece hangi

Burada amaç banka ve kredi kartı bilgileri üzerinden bu kötü amaçlı yazılımı yayan bilgisayar korsanının deşifre olmasını engellemektir.

3.3.6. Hacktivizm

Hacktivizm, hack ve aktivizm (eylemcilik) sözcüklerinin birleşiminden türetilmiş bir kavramdır. Hacktivizm karşılığı olarak çoğu zaman "Dijital Aktivizm" sözcüğü kullanılabilmektedir. Hactivizm kısaca; bilgisayar teknolojisinin veya programlama sistemlerinin toplumsal bir soruna yönelik tepki gösterme amaçlı kullanılmasıdır. (Uçkan ve diğerleri, 2014: 28). Eylem türü olarak Hacktivzm'i seçmiş bireylere "Hacktivist" adı verilmektedir.

> *Hacktivizm; bir çeşit siyasi veya toplumsal değişime şiddet içermeyen fakat hukuki olarak tartışmalı siber protestolarıyla ön ayak olma veya direnme fikridir. Bir zamanlar Martin Luther'in yazılı basının devrimsel gücünü mesajını yaymak için kullandığı gibi, hacktivistler de kendi sivil itaatsizlikleri, kışkırtma ve protestolarına yardım etmek için son teknolojiye tıklıyorlar. Ancak geçmişin aksine bu teknoloji anlık olarak, ulusal sınırları aşarak ve anonim olarak işlem yapma imkânı sunuyor (Singer ve Friedman, 2015: 112).*

Hacktivist'lerin bilgisayar korsanlığı alanındaki ustalığı profesyonel hackerlar kadar değildir. Hacktivist'lerin bilgi düzeyi genellikle "script kiddie"lerinki kadardır. Amaçları sistemi hacklemek değil mesajları yaymak olduğundan, genellikle hackleme sürecinin detaylarıyla ilgilenmezler (Çakar, 2013: 8).

---

adresten hangi adrese ödeme yapıldığı kayıtlara geçer. Bu para birimi günümüzde tüm dünyada kullanılmakta ve gerçek para birimlerine çevrilebilmektedir.

Hacktivizm'in geçmişi 1980'lerin ortalarına kadar gitmektedir. Bir örnek vermek gerekirse, "PeaceNet"in ilk sürümü 1986'nın başlarında çıkmıştır. PeaceNet, gerçek anlamda ilk defa, siyasi aktivistlerin birbirleriyle ulusal sınırların ötesinde, görece bir kolaylıkla ve hızda iletişime geçmesini sağlamıştır (izinsizgosteri.net).

Gerçek anlamdaki ilk Hactivizm hareketleri 1997'de görülmüştür. Hacktivistler ile performans sanatçılarını melezleyen bir grup olan "Elektronik Rahatsızlık Tiyatrosu", Chiapas sorununa dikkat çekmeye çalışan mesajlar ile Pentagon ve Meksika hükûmetinin web sitelerini istila eden sanal oturma eylemi düzenlemiştir. Yakın zamanlardaki oturma eylemleri belirli hükûmet binaları gibi fiziki tesisleri, Youtube videoları gibi büyük ebatlı dosyalarla ağ ve bilgisayarları alt etmeye çalışarak hedef almaktır (Singer ve Friedman, 2015: 113). 2004 yılında bir video ortaya çıkmıştır. Bu videoda Huntington Yaşam Bilimleri test laboratuvarlarında av köpeği yavrularının suratlarının tekmelenmesini de içeren bir dizi havyan eziyetleri gözler önüne serilmiştir. Bunun üzerine SHAC (Stop Huntington Animal Cruelty / Huntingon Hayvan Eziyetini Durdurun) isimli bir hacktivist grup bir kampanya organize etti ve bu şirketin internet ağlarına saldırı düzenlendi. Düzenlenen saldırıda şirket müşterilerinin kişisel verileri ve isimleri sızdırıldı.

Günümüzde dünyada bir süredir faaliyet gösteren ve eylemleriyle büyük yankılar uyandıran önemli hacktivist gruplar bulunmaktadır. Bu grupların düzenlediği saldırılar ve yaptıkları eylemler her türlü medya kanalında geniş yer bulmuştur. Dünyada bilinen en büyük hacktivist grup "Anonymous"tur. Öyle ki bu grup Wikileaks sitesinin kurucusu Julian Assange ile dostluk grup onun için eylemler yapmışlardır. Ülkemizde en ünlü hacktivist grup ise Redhack'tir. Bu grup, yaptığı eylemler nedeniyle hükûmet tarafından terör

örgütü olarak ilan edilmiştir. Bu iki grubun yaptıkları eylemleri ve bu eylemlerle ilgili çıkan haberleri aşağıda ele alacağız.

3.3.6.1 Anonymous grubu ve faaliyetleri

"Biz anonimiz, orduyuz, affetmeyiz, unutmayız. Bizi bekleyin"[16]

"Anonymous" (Anonimler), çeşitli siyasi olayları, genellikle devlet teşkilatlarına ait sitelere saldırılar düzenleyerek protesto eden ve yıllardır faaliyet gösteren en büyük hacktivist gruptur. Anonymous geniş isimsiz bir kolektif olarak her türlü insan kavramını temsil etmektedir (tr.wikipedia.org.tr).

Anonymous grubunun geçmişi çok öncelere dayanmaktadır. Bu grubun doğuşundan bahsedecek olursak: Grup kendine İngiltere'de 1570 yılında doğan Guy Fawkes'i[17] idol olarak belirlemiştir. Anonymous eylemlerinde Guy Fawkes maskesini sembol olarak kullanır (ntv.com.tr). Bu maskeye metaforik bir anlam yükleyen Anonymous kendilerini dünyada haksızlıklara karşı gerçekleştirdikleri dijital eylemlerle duyurmuşlardır.

---

[16] Anonymous isimli hacktivist grup kendisini bu sloganla tanımlamaktadır.

[17] Guy Fawkes, Katolik düşünceyle yetişen ve Avrupa'daki mezhep çatışmaları sırasında çıkan "Seksen Yıl Savaşları"nda Katolik İspanya ordusunda yer alıp, Hollandalı Protestean reformculara karşı savaşmıştır. Guy Fawkes ve arkadaşları 5 Kasım 1605'te İngilere Kralı I. James ve yanındaki Protestan aristokratlara karşı barutlu bir saldırı düzenleyeceklerdi. Fakat bu komplo, bir ihbar üzerine başarısızlığa uğramıştır. Bunun sonucunda Guy Fawkes ve arkadaşları işkenceden geçirilerek idam edilmişlerdir. Guy Fawkes kimilerine göre bir anarşist ve devrimci, kimilerine göreyse bir vatan hainidir. Guy Fawkes'in İngiltere tarihinin en büyük devrimcilerinden biri olarak gören çizer David Loyd ve yazar Alan Moore, 1980 yılında bir çizgi karakter yaratılar. Guy Fawkes maskeli çizgi karakter, İngiltere'de faşist bir iktidarı düşürmek için İngiliz parlamentosunu havaya uçuruyordu. Çizer David Lloyd ve yazar Alan Moore'un yarattığı çizgi karekter, 2005 yılında "V for Vandetta" ismiyle sinemaya uyarlanmıştır.

Anonymous'un kuruluşuna dair tam bir tarih yoktur; ancak bu oluşumun kökeninin 1980'lerdeki eski hacker topluluklarına uzandığını gösteren birçok gösterge bulunmaktadır: Eski hackerlar 4chan gibi çevrimiçi ilan panoları etrafından toplanan yeni nesil hacktvistler ile birleşerek Anonymous'un oluşumunu 2000'lerin ortasında gerçekleştirmişlerdir (Singer ve Friedman, 2014: 117, 118).

Anonymous'un dijital aktiviteleri 2008'de başlamıştır. 2010 yılında grup AnonOps isimli aktif bir düğümün "Payback (bir sürtüktür) Operasyonu", "Operasyon Assange'ın İntikamı" ve "Operasyon Tunus" gibi isimlerle harekete geçmesiyle daha ciddi dalgalar yarattı. İlki internet telif hakları üzerine bir savaş olarak, hacktivistlerin internet korsanlığını sınırlamaya çalışırken çok sert ve taviz edici olarak gördüğü çeşitli organizasyonları Anonymous'un hedef almasıyla başladı. Amerikan Sinema Birliği, Amerika Kayıt Endüstrisi Birliği (RIAA), telif hakları hukuk şirketleri ve hatta KISS grubunun solisti Gene Simmons (hedeflenmişti çünkü izinsiz olarak şarkılarını indiren herkesi "dava etmek" ve "evlerini almak" ile tehdit etmişti) web sitelerinin defalarca kapatıldığını ve/veya dosyalarının dünyaya açıldığını gördüler (Singer ve Friedman, 2015: 118, 119). "Operasyon Assange"da PayPal, Bank of America Master Card ve Visa gibi şirketler ABD diplomatik yazışmalarını sızdıran Wikileaks'e yapılan bağışları durdukları ve bu bağışlara el koydukları için hedef alındı. "Operasyon Tunus"ta ise Wikileaks belgelerini ve ülkede gerçekleşen devrim sırasında ayaklanma haberlerini sansürlediği için hedef alındı. Hükûmet kurum ve kuruluşlarının web sitelerine saldırılar düzenlendi (Chen, 2014).

Bir süre sonra Anonymous daha büyük ve daha güçlü hedeflerin peşine düşmeye başladı. Bu durum Anonymous'un adının çıkmasına sebep oldu. İlerleyen süreçte Anonymous bunun bedellerini gerçek şekilde ödemeye başlayacaktı. Dünyanın dört bir yanında eylemlere girişen Anonymous üyeleri

hükûmet ve kanun uygulama kuruluşlarına saldırınca hükûmet kuruluşları eylemlerle ilgili olanları tespit etmeye başladılar. Gerçekleşen polis baskınları sonucunda ABD, İngiltere ve Hollanda gibi ülkelerdeki Anonymous üyeleri cezaevine gönderildi. Bu durum bununla bitmemişti. Anonymous'un başı eski Meksika ordusu komandoları tarafından kurulan bir uyuşturucu karteli olan Los Zetas ile derde girdi. Los Zetas bir Anonymous üyesini kaçırmıştı. Bunun üzerine Hacktivistler eğer üyeleri serbest bırakılmazsa, Los Zetas ve ortakları hakkında geniş bir bilgi dizisini internet üzerinden yayınlayacaklarını belirttiler. Bu tehdit Zetas'ı çok kızdırmıştı. Öyle ki, Zetas bilgilerin ifşasının kendilerine çok büyük zarar vereceğini biliyordu. Eğer bilgiler sızarsa Zetas üyeleri tutuklanabilecek veya karşı çeteler tarafından cinayetlere kurban gidebilecekti. Buna karşılık olarak kartel, bazı üyelerini açığa çıkarmak ve ölümle tehdit etmesi amacıyla Anonymous'u "geri hacklemeye" yardım etmesi için uzmanlar kiraladı. En sonunda, zayıf bir ateşkes durumuna geldiler. Kaçırılan kurban, Zetas'tan açıklanan her isim için on kişinin öldürüleceğini söyleyen çevrimiçi bir tehditle beraber serbest bırakıldı (Singer ve Friedman, 2015: 119, 120).

Anonymous günümüzde eylemlerine halen devam etmektedir. Charlie Hebdo dergisi saldırısının protesto eylemleri dâhil olmak üzere, 2015 yılı içinde bir dizi eylem daha gerçekleştirmişlerdir.

3.3.6.2. Redhack ve faaliyetleri

Türkiye'de ve dünyada faaliyet gösteren, ülkemizin en büyük hack grubu olarak ifade edilen RedHack (Kızıl Hackerlar, Kızıl Hackerlar Birliği), 1997 yılında kurulmuştur. Kendilerini Marksist ve Sosyalist olarak tanımlarlar. Şubat 2012'de Ankara Emniyet Müdürlüğü'nün internet sitesini çökerterek adlarını duyuran grup aynı zamanda Türkiye genelinde

yaklaşık 350'ye yakın emniyet müdürlüğü sitesini geçici bir süreliğine çalışamaz hale getirmiştir. Grubun çekirdek kadrosu 12 kişiden oluşmaktadır (tr.wikipedia.org).

Redhack ülke içinde ve dünya genelinde yüzlerce hackleme faaliyetine imza atmıştır. Redhack birçok faaliyetinde, çalışmamızın önceki bölümünde yer verdiğimiz Anonymous grubuyla ortak olarak çalışmaktadır.

Redhack'in bugüne kadar gerçekleştirdiği faaliyetler arasında en çok göze çarpanlar şunlardır:

- 27 Şubat 2012'de Ankara Emniyet Müdürlüğü'nün internet sitesinin çökertilerek, çok sayıda ihbar ve iç yazışmanın internet ortamında yayınlanması.
- 27 Nisan 2012 tarihinde İnternet servis sağlayıcılarından TTNet'in yaklaşık 2 saat süreyle internet hizmetinin aksatılması. Bunun üzerine açıklama yapan TİB saldırıyı doğruladı fakat internet kesintisi olduğuna dair haberleri yalanladı.
- 2 Mayıs 2012'de Kara Kuvvetleri Komutanlığı'nın sistemine girerek bazı TSK personelinin bilgilerinin ifşa edilmesi.
- 3 Mayıs 2012 tarihinde Milli Eğitim Bakanlığı'nın "Okul sütü-Akıl küpü" adıyla başlattığı süt dağıtım projesinin ilk gününde yüzlerce ilköğretim öğrencisinin zehirlenerek hastanelere kaldırılmasını protesto amacıyla üç süt firmasının aynı gün hacklenme eylemi.
- 14 Mayıs 2012 Anneler Günü nedeniyle "kadına yönelik şiddete" dikkat çekme amacıyla Aile ve Sosyal Politikalar Bakanlığı'nın internet sitesinin hacklenerek, ana sayfasına bildiri konulma eylemi.
- 3 Temmuz 2012'de Dışişleri Bakanlığı'nın dosya paylaşım sitesinin hedef alınması. Saldırı sonucunda Türkiye'de çalışan pek çok yabancı diplomatın kimlik bilgilerinin Dropbox adlı site üzerinden yayınlanması.

- 29 Ekim 2012'de Diyanet İşleri Başkanlığı'nın ana sayfasını hackleyerek hükûmete ve Fethullah Gülen cemaatine yönelik bir dizi eleştirinin yayınlanması.
- 7 Aralık 2012'de Maliye Bakanlığı sitesini hackleyerek memura "temsili olarak" zam yapılması eylemi.
- 8 Ocak 2013 tarihinde Yüksek Öğretim Kurumu (YÖK) sitesini 2. kez hacklemek ve ele geçirdiği yolsuzluk belgelerini yayınlamak.
- 26 Şubat 2013 tarihinde Ankara Büyükşehir Belediye Başkanı Melih Gökçek hakkındaki belgelerin yayınlanması.
- 22 Mart 2013 tarihinde Ankara Büyükşehir Belediyesi'nin sitesinin hacklenmesi.
- 23 Mart 2013 tarihinde İsrail gizli servisi MOSSAD'ın sitesinin Anonymous grubu işbirliğinde çökertilmesi eylemi.
- 24 Mart 2013 tarihinde aralarında üst düzey bürokratların, hâkimlerin olduğu 32 bin İsrail çalışanının isimlerinin, ev ve e-mail adreslerinin ve diğer kimlik bilgilerinin açıklanması eylemi.
- 5 Mayıs 2013'te, İstanbul Valiliği'nin Taksim'de 1 Mayıs gösterilerine izin vermemesi ve göstericilere sert müdahalesi sebebiyle İstanbul Valiliği'nin resmi sitesinin hacklenmesi ve ana sayfasına Vali Mutlu'ya protesto notu bırakılması eylemi.
- 11 Mayıs 2013 tarihinde Hatay Reyhanlı'da yaşanan patlama sonrasında ulusal yas ilan edilmesini isteyerek Hatay Valiliğinin sitesinin çökertilmesi.
- 22 Mayıs 2013 tarihinde Reyhanlı Patlamasıyla ilgili Askeri İstihbarat Belgelerinin yayınlanması.
- 1 Haziran 2013 Gezi Parkı eylemlerinde milletvekillerinin duyarsızlığını gerekçe göstererek milletvekili ve eşlerinin cep ve ev telefon numaralarının yayınlaması eylemi.

- 17 Haziran 2013'te, Tarım Bakanı ve iş adamları arasında yapılan toplantı kaydının yayınlanması eylemi.
- 28 Haziran 2013'te, İstanbul İl Özel İdaresi'nin web sayfasının hacklenmesi ve kullanıcı bilgilerinin twitter'da yayınlanarak sistemde takipçileriyle birlikte değişiklikler yapılması eylemi.
- 14 Ağustos 2013'te, ASKİ Adana Büyükşehir Belediyesi Su ve Kanalizasyon İdaresi'nin hacklenmesi ve kullanıcı bilgilerinin twitter'da yayınlanarak sistemde takipçileriyle birlikte değişiklikler yapılması eylemi.
- Türkiye Büyük Millet Meclisinin internet sitesinin hacklenmesi eylemi.

Siber korsan olarak ifade edilen hackerların faaliyetlerine karşı yürütülen soruşturmaların genellikle olumsuz sonuçlanması ve hackerların yerlerinin (hackerların genellikle işlerini iz bırakmadan yapmalarından dolayı) tespit edilmesinin çok zor olmasına rağmen ülkemizde emniyet güçleri ve savcılıklar Redhack'e karşı soruşturmalar yürütmüştür.[18] Fakat

[18] 21 Mart 2012 tarihinde Özel Yetkili Ankara Başsavcılığı'nın farklı illerde başlattığı operasyonlar sonucunda gözaltına alınan ve Redhack grubu üyesi olduğu iddia edilen 17 kişiden 7'si terör suçları kapsamında tutuklanmıştır. Redhack tarafından yapılan açıklamada tutuklananların grupla ilgisi olmayan insanlar olduğu belirtilmiştir (bianet.org).
8 Ekim 2012 günü savcılık tarafından sunulan ve RedHack'in silahlı terör örgütü olduğu iddianamesini kabul ederek, RedHack hakkında 8,5 yıldan 24 yıla kadar ceza isteminde bulunmuştur. Tutuklu 7 kişiden 4'ü serbest bırakılırken, hâlen aralarında üniversite öğrencilerinin de olduğu 3 kişi tutuklu olarak yargılandı. Dava 26 Kasım 2012 tarihine ertelenmiştir (cumhuriyet.com.tr).
26 Kasım 2012 tarihli davanın görülmesi sonucu RedHack üyesi olduğu iddia edilen 3 üniversite öğrencisi serbest bırakıldı. Mahkeme 26 Şubat 2013 tarihine ertelendi (haberturk.com).
26 Şubat 2013 tarihli 2. mahkemenin görülmesi sonucu, "RedHack davasında bilişim konusunda uzman olan bilirkişilerin bile dosyayı almak istemedikleri"ni açıklayan mahkeme başkanı, bilirkişi bulunması amacıyla davayı 3 Haziran 2013'e erteledi (milliyet.com.tr).

Redhack'e karşı yürütülen uzun süreli operasyon ve soruşturma sonuca ulaşmamış, bununla beraber hiçbir Redhack üyesine ulaşılamamıştır. Bu bağlamda, bu korsanların karanlık kimliği henüz aydınlatılamamıştır.

3.4. İnternet Güvenliği ve Çevrimiçi Gizliliği Korumak İçin Alınabilecek Önlemler

Bu bölümde aralarında birçok ünlü yazılımcı, teknoloji editörü ve internet güvenliği yöneticisinin de bulunduğu uzmanın internet güvenliğimizi ve çevrimiçi gizliliğimizi korumak adına sundukları önerileri sırasıyla ele alacağız.

3.4.1. Özgür yazılım ve açık kaynak kodlu program kullanma

Eskiden bilgisayarlar büyük kurumların tekelindeydi. Üniversiteler, IBM gibi dev firmalar bunlar içerisinde sayılabilir. 1970'lerde yavaş yavaş PC, yani kişisel bilgisayarlar insanların kullanımına açıldıkça bir müddet sonra bir yazılım sektörü doğmaya başlamıştır. Bunun sonucunda daha fazla yazılımcı ortaya çıkmıştır. Richard Stallman[19] da bu yazılımcılardan birisidir.

---

9 Mayıs 2013 tarihinde, Terörle Mücadele Yasası (TMY) ile görevli Ankara Başsavcı Vekilliği, RedHack'in eylemlerinin "şiddet içermediği" gerekçesiyle, görevsizlik kararı verip dosyayı Bilişim Suçları Soruşturma bürosuna göndermiştir (hurriyet.com.tr)

25 Mayıs 2013 RedHack'in Reyhanlı bombalamasıyla ilgili yayınladığı belgelerin sızdırıldığı saatin nöbet saatine gelmesi sebebiyle Amasya komutanlığına bağlı Er Utku Kali tutuklanmış ancak kendisine yönelik "RedHack üyesi olma" "bilgi sızdırma" gibi suçlamaları reddetmiştir. Er Utku Kali suçsuz bulunduğu için serbest bırakıldı (bianet.org).

[19] 1970'lerin ilk yıllarında, yazılım masrafları hızla yükselirken büyümekte olan yazılım endüstrisi, donanım üreticilerinin bilgisayar satışıyla beraber verdikleri "yazılım demetleri", kiraya verilen bilgisayarların kâr getirmeyen yazılım desteğiyle rekabet başlamıştı. Bazı müşterilerin kendi ihtiyaçlarını daha iyi karşılamasıyla "özgür" yazılım masraflarının donanım

Stallman, açık kaynak kodlarının gizlenerek ticarileşmesinin yerine herkesin daha çok katkıda bulunabileceği bir sistem oluşturmak için GPL (GNU General Public Licence) lisans altyapısını öne sürmüştür. GPL lisansı ile hem son kullanıcı hem de yazılım geliştiriciler açısından daha faydalı ve verimli bir yazılım ortamı amaçlanmıştır (tr.wikipedia.org).

Aşağıda Richard Stallman tarafından kurulan "Özgür Yazılım Vakfı"nın manifestosundan alıntılanan bir kısım yer almaktadır:

Özgür yazılım kavramı, kullanıcıların, yazılımı çalıştırma, kopyalama, dağıtma, üzerinde çalışma, değiştirme ve geliştirme özgürlükleriyle ilgili bir kavramdır. Daha açık konuşacak olursak, "özgür yazılım" kavramı, yazılım kullanıcıları dört olmazsa olmaz özgürlüğe sahiplerdir demektir:

- Herhangi bir amaç için yazılımı çalıştırma özgürlüğü (0 numaralı özgürlük).
- Her ne istiyorsanız onu yaptırmak için programın nasıl çalıştığını öğrenmek ve onu değiştirme özgürlüğü (1

masraflarıyla bütünleşmesini istemiyordu. 1970'ler ve 1980'lerde yazılım endüstrisi, bilgisayar programlarını sadece kullanıcıların kodu incelemesi ve değiştirmesini önleyen çalıştırılabilirler şeklinde dağıtmaya başlamasıyla teknik tedbirler almaya başladı. 1980'de copyright kanununun kapsamı bilgisayar programlarını içine aldı (tr.wikipedia.org).

Richard Stallman Eylül 1983'de, Unix-benzeri işletim sistemi oluşturmak amacıyla işletim sistemi çekirdeği (kernel) hariç bir işletim sistemi için gerekli olan tüm yazılımları içeren dev bir özgür yazılım koleksiyonu olan GNU Projesi ni hayata geçirmiştir. 70'lerin sonu ve 80'lerin başında MIT 'de AI (Yapay Zekâ) konusunda çalışmalar yaptığı sırada mesai arkadaşlarının geliştirdikleri yazılımların kaynak kodlarını ticaret amacıyla kapatmalarına karşı isyanı bugüne kadar devam etmektedir. Stallman'a göre yazılım kodlarının gizlenmesi beraberinde birçok sorunu getirmekteydi. Bunlardan en çok yaşananı, bir firma veya şahsın açık kaynak kodlu bir yazılımı alıp birkaç değişiklik yaptıktan sonra kaynak kodunu kapatarak ticari amaçla kullanmasıydı. Böylesi bir döngü dünyadaki tüm geliştirilen yazılımların zamanla kapalı kaynak haline gelmesine yol açabileceği için Stallman MIT 'deki hacker faaliyetlerini ve enerjisini, özgür yazılım savunuculuğuna yöneltmiştir.

numaralı özgürlük). Yazılımın kaynak koduna ulaşmak, bu iş için önkoşuldur.

- Kopyaları dağıtma özgürlüğü. Böylece komşunuza yardım edebilirsiniz (2 numaralı özgürlük).
- Tüm toplumun yarar sağlayabileceği şekilde programı geliştirme ve geliştirdiklerinizi (ve genel olarak değiştirilmiş sürümlerini) yayınlama özgürlüğü (3 numaralı özgürlük). Kaynak koduna erişmek, bunun için bir önkoşuldur (gnu.org).

Stallman'a göre açık kaynak kodlu olmayan program ve işletim sistemlerinin içerisinde ne olduğunu bilemeyiz. Kapalı kod yapısına sahip işletim sistemleri ve programların içerisinde izlenmemizi sağlayan zararlı kodlar ve arka kapılar olabilir. Bu nedenle Stallman insanlara Windows ve IOS gibi işletim sistemlerini kullanmamalarını önermiştir.

Stallman, Malware (zararlı yazılım) kavramının yalnızca virüslerden ibaret olmadığını, asıl zararlı yazılımı Windows, Mac OS gibi işletim sistemlerinin oluşturduğunu belirtmiştir. Ona göre bu tür işletim sistemleri kullanıcıları gizlice takip ve bu sistemlerde Amerikan Güvenlik Dairesi (NSA)'ne bilgi gönderen arka kapılar mevcut. Stallman, yalnız bilgisayarda kullanılan işletim sistemlerini değil, cep telefonlarında kullanılan Google Android ve IOS'u da bu kategoriye dâhil etmektedir. Cep telefonlarına yüklenilen bedava olmayan uygulamaların, el feneri uygulamasının bile içinde şirketlere veriler gönderen kodların varlığından söz etmiştir. Youtube gibi video izleme hizmetlerinin de kötü olma eğilimlerine sahip olduğunu belirten Stallman, bu hizmetlerin kişisel bilgilerin kopyalarını almak ve kullanıcıların izlenip takip edilmesini sağlamak üzere tasarımlandığından bahsetmiştir (theguardian.com).

Bu nedenlerden dolayı Stallman herkesi açık kaynak kodlu Linux gibi işletim sistemlerini ve açık kaynak kodla

oluşturulmuş program ve yazılımları kullanmaya davet etmektedir.

3.4.2. Açık Kaynak kodlu sohbet uygulamaları ve eposta hesapları kullanma

Bilişim dünyasında son günlerde Facebook, Twitter, Google Plus gibi sosyal medya siteleri ile Skype, Whatsapp gibi sohbet programlarının ve Outlook, Yahoo, Gmail gibi eposta hizmetlerinin ne kadar güvenli olduğuna dair tartışmalar yapılmaktadır. Richard Stalmann gibi yazılımcılar ve bu olgunun felsefesini yapan kişiler aslında bu tür hizmetleri hiç kullanmamız gerektiğini; çünkü sosyal medya üzerinden yapılan yazışmaların tek tek okunduğunu, epostaların kontrol edildiğini ve bu uygulamalar üzerinden bizimle alakalı her türlü kişisel verilerin toplanılıp başta ABD hükûmeti olmak üzere, dünyanın birçok ülkede iktidarlara teslim edildiğini belirtmektedirler. Nitekim çalışmamızın önceki bölümlerinde üzerinde detaylı bir şekilde durduğumuz Edward Snowden'in ABD hükûmeti ve NSA ile ilgili açıklamaları, Richard Stallman gibi bilişim felsefecilerinin ne kadar haklı olduğunu kanıtlar niteliktedir. Bu bağlamda dünyada yavaş yavaş çok sık kullanılan hizmetler yerine artık gizliliğe daha fazla önem veren, şifreleme özelliğine sahip sohbet yazılımları ve eposta hizmetleri kullanılmaya başlamıştır.

Jabber olarak bilinen XMPP (Genişletilebilir Mesajlaşma ve Varlık Protokolü) 'e sahip sohbet istemcileri gizliliği ön planda tutmak isteyen kullanıcılar için iyi bir alternatif oluşturmaktadır. Bu tür istemcilerin kullandığı herhangi bir XMPP sunucu, XMPP ağından tamamen izole edilebilir, örneğin sadece yerel bir ağ içerisinde kullanılabilir ve çekirdek XMPP spesifikasyonlarında yer verilen SASL (kimlik doğrulama güvenlik katmanı) ve TLS (iletim katmanı güvenlik

protokolü) ile güçlü ve sağlam bir güvenlik sunarlar (tr.wikipedia.org).

XMPP protokolüne sahip olan ChatSecure, Coccinella, Gajim, InTouch Messenger, Jeti/2, Jitsi, MCabber, Pidgin, Psi ve Tkabber gibi istemciler en çok kullanılan sohbet istemcileri arasındadır (xmpp.org).

En çok kullanılan sohbet uygulamalarından biri olan Whatsapp'ın 2014 yılının Şubat ayında Facebook tarafından satıl alınmasıyla birlikte ve yine 2014 yılında NSA ve Edward Snowden olayının ortaya çıkması sonucunda Whatsapp'ın ne kadar güvenli bir yazılım olduğu tartışmasını gündeme getirmiştir. Ekim 2014'te Whatsapp uygulamasının birkaç saatliğine devre dışı kalması, o tarihlerde ortaya çıkan Telegram isimli Whatsapp benzeri bir uygulamanın kullanım oranında büyük bir yükseliş yaratmıştır.

Telegram'ı geliştiren yazılımcılar kendi yazılımlarının, Whatsapp'tan çok daha güvenli olduğu iddiasıyla gündeme gelmişlerdir. Yazılımın yaratıcıları, yazılımlarının mükemmel olduğuna inanmaktadırlar. İlk önce uygulamada herhangi bir açık bulunması halinde, bu açığı bulan kişiye 100.000 Amerikan Doları ödül vereceklerini açıklamışlardır (theverge.com). Daha sonraysa herhangi bir kullanıcının Telegram'ın güvenlik duvarını aşabilmesi halinde, bu duvarı aşana 200.000 Amerikan Doları vereceklerini belirtmişlerdir.

Bu söylemler dışında Telegram geliştiricilerinin güvenlik konusunda bir iddiaları daha vardı. Geliştiricilere göre bu yazılım üzerinden sohbet eden hiçbir kullanıcının kişisel verileri Amerika ve Rusya gibi dünya devletinin güvenlik daireleri tarafından okunamayacağını iddia etmişlerdir. Geliştiricilerden biri şu söylemde bulunmuştur: "Telegramı geliştirilmesine yardım etmemin bir numaralı sebebi, iletişimin Rus Güvenlik Daireleri tarafından erişilemeyecek olması amacını gütmesidir" (theverge.com).

Telegram geliştiricilerinin arkasında durduğu başka bir durum da Telegram'ın açık kaynak kodlara sahip olmasıdır. Bu iddialı söylemler Whatsapp kullanıcılarının bir kısmının Telegram'a geçiş yapmalarını sağlamıştır. Şu anda kadar Telegram aracılığıyla kişisel verilerin çalınması gibi hiçbir haber bilişim basınında yer almamıştır.

Yukarıda örnek verdiğimiz olaylar göstermektedir ki, izlendiklerini ve takip edildiklerini anlayan toplum yavaş yavaş gizliliği ve güvenliği daha iyi sağlayan alternatif çözümlere yönelmeye başlamıştır.

3.4.3. VPN hizmeti kullanmak

Virtual Private Network (Sanal Özel Ağ) teriminin kısaltılmışı olan VPN, basit bir anlatımla internet üzerinde kurulu bilgisayarlar grubundan oluşmaktadır. Bu özel bilgisayar ağı, örneğin yerel bir ağa fiziksel erişimi bulunmayan, dışarıdaki bir kişi tarafından ağ kaynaklarına erişmekte kullanılabilmektedir. VPN'ler, güvenilmeyen ağlara bağlanırken bağlantıyı şifrelemek ve güvenli hale getirmek için de kullanılmaktadır. Bunun yanında VPN'ler, farklı konumlarda bulunabildiğinden, kullanıcıları ülkelerin kısıtlamalarından (yasaklı web siteleri ve IP'ler gibi) da kurtarmaktadırlar. VPN'lerle kullanılan bağlantı şifreli olduğundan, gönderilen ve alınan tüm veriler şifrelendiğinden, kullanıcıları gözetlemek isteyen unsurlar bu verilere erişemezler. (chip.com.tr).

VPN hizmetini kullanmak için farklı yöntemler vardır. Kimisi ücretli abonelik ile bilgisayara kurulan bir program aracılığıyla kullanıma imkân verirken, kimi hizmetler de İnternet üzerinden link bazında giriş için kullanılmaktadır (pcworld.com.tr).

VPN kullanmanın hem avantajları hem de dezavantajları vardır. Artıları ve eksileri değerlendireceksek, VPN kullanmanın artıları, eksilerinden çok daha fazladır. Eksileri

arasında kaliteli bir VPN hizmeti alabilmek için bu servisi sunan firmalara aylık ya da yıllık olarak belli bir ücret ödenmesi gerekmektedir. Diğer eksi ise VPN hizmetinin yurt dışından sağlanmasından dolayı ve VPN servisi sırasında gelen ve giden verinin uzaktaki sunucular üzerinden geçmesi nedeniyle bağlantı hızı biraz düşüktür.

VPN servisinin avantajlarına gelecek olursak:

- İnternet Servis Sağlayıcılarının Derin Paket Analizi (DPI) yapması engellenir. Bu sayede cihazımıza gelen ve cihazımızdan gönderilen verinin incelenmesinin önüne geçilir.
- IP adresimiz korunur. İnternet siteleri IP adresimizi ve konumuzu okuyamaz. Çünkü IP adresimiz VPN hizmeti kullandığımızda VPN hizmetinin bize sunduğu sunucuların IP adresi olarak görünür.
- Çevrimiçi gizlilik korunur. Hükûmet bizi izlemesi ve denetlemesi engellenir. Özel şirketlerin verilerimizi ele geçirip pazarlamasının önüne geçilir.
- Yasaklı internet sitelerine erişebiliriz. Böylece iktidarların sansürlerine karşı bir önlem almış oluruz.
- Coğrafi hedefleme ve konum bilgisi tespiti engellenir. VPN hizmetlerinin bize atadığı IP adresini kullanmamız sayesinde arama motorları, pazarlama şirketleri ve içerik sağlayıcıları nerede olduğumuzu öğrenemez. Bir nevi sahte IP kullanarak onları kandırmış oluruz.

Kimi bilişim ve teknoloji editörlerine göre, internet güvenliği ve çevrimiçi gizlilik VPN aracılığı ile tam olarak sağlanamaz. Çünkü VPN servisini satan şirketler de, ülkelerin vergi dairelerine kayıtlı kuruluşlardır; hükûmetler istedikleri takdirde VPN şirketleri her türlü bilgiyi sağlamak zorunda kalırlar. Aksi takdirde bu şirketlerin hizmet vermeleri devlet tarafından engellenebilir veya büyük para cezaları ödemek zorunda kalabilirler.

3.4.5. Tor ağı ve tor browser kullanmak

Tor (The Onion Router) ağı çevrimiçi gizliliği korumak adına geliştirilmiş olan anonim bir internet ağıdır. Bu projenin ortaya çıkmasında rol oynayan kuruluşlardan biri de ABD ordusunun bir uzantısı olan "United States Naval Research Labarotory" yani Deniz Harp Araştırma Laboratuvarı'dır. Bir müddet sonra Tor kullanımı sivillere de açılmıştır (tr.wikipedia.org).

Tor üzerinden internete erişmeye çalışıldığı sırada, gönderilen veriler, gidilecek sitenin IP adresi de dâhil katman katman, tekrarlı bir şekilde şifrelenir ve tamamen tesadüfi seçilen tor relay noktalarından geçer. Her relay noktası tekbir şifreleme katmanının şifresini açar ve geri kalan şifreli katmanı bir sonra uğrayacağı noktaya iletir. En sonuncu relay noktası buna 'çıkış noktası' (exit node) denmektedir. Çıkış noktası, en içerideki gizli katmanın şifresini çözer ve kullanıcının bilgisayarından gönderdiği ilk orjinal veriyi istenilen adrese ulaştırır. Bu tesadüfi seçilen relay noktaları ve herbir noktanın kendine düşen belli bir katmanın şifresini çözmesi sebebiyle geriye doğru kullanıcıya ulaşılması çok güçtür. Kullanıcının gerçek ip adresi ve kimliği gizlenmiş bu sayede gizlenmektedir (blog.saklansana.com).

Tor ağına bağlanabilmek için, Firefox internet tarayıcısının düzenlenmiş bir sürümü olan Tor Browser'ı kullanmak gerekir. Bu internet tarayıcısı Tor'un vekil sunucusunun yanı sıra güvenliği sağlamaya yarayan birkaç eklenti de içerir. Tor Browser ve Tor Ağı sayesinde çevrimiçi gizliliğimiz daha iyi korunur. IP adresimiz ve lokasyonumuz gizlenir. Sansürlenmiş her türlü internet sitesine Tor sayesinde ulaşım mümkündür. Fakat Tor'un da tam anlamıyla mükemmel bir güvenlik sağladığı söylenemez. Tor'un az da olsa güvenlik açıkları vardır. Yine de Tor anonimlik için en günümüzde en iyi yazılımdır.

Çevrimiçi gizliliği VPN'nin mi yoksa Tor Ağı'nın mı daha iyi koruduğu sorusunun farklı cevapları vardır. Bu kullanılan VPN hizmetlerinin kalitesine ve şirket politikalarına göre değişmektedir. Tor Ağı'nın en önemli avantajlarından biri ücretsiz olmasıdır. Fakat Tor üzerinden giden ve gelen verinin birçok yoldan geçmesi nedeniyle iletişim çok yavaş bir şekilde sağlanmaktadır. İyi bir VPN servisi içinse yüksek ücretler ödenmektedir. Genellikle VPN hizmetleri Tor'a oranla çok daha hızlıdır. Daha önce de bahsettiğimiz üzere bazı VPN şirketleri verileri ülkelerdeki hükûmetlere sağlayabilirler. Yalnızca bazı ülkelerde hizmet veren VPN şirketleri ayrıcalıklıdır. Bu tür şirketlerinse çok daha yüksek ücret aldıkları ortadadır. Tor Ağı üzerinden bir kişinin gerçek kimliğini herhangi bir ülkedeki normal bir bilişim uzmanının tespit etmesi neredeyse imkânsızdır. Bir kişinin kimliğinin tespit edilebilmesi için o kişiye ait her izin güçlü veri işleme programları aracılığıyla işlenmesi ve birleştirilmesi gerekir. Ayrıca Tor ağının kullandığı karmaşık yapı sayesinde çökertilmesi ya da duraklatılması da çok zordur.

Ne yazık ki Tor ağının sunduğu avantajları kötü niyetlerine alet eden birçok suçlu işlerini Tor üzerinden yürütmektedirler. Tor Ağını kullanarak "Silkroad" isimli bir internet sitesi kuran 24 suçlu, bu site üzerinden uyuşturucu tüccarlığı, kadın tüccarlığı, seri katil kiralama gibi işlere karışmışlardır. Bu suçlular NSA (Amerikan Güvenlik Dairesi) tarafından çeşitli teknik yöntemler yürütülerek zor da olsa yakalanmışlardır.

4. TÜRKİYE'DE İNTERNET VE SOSYAL MEDYA KULLANICILARININ İNTERNET GÜVENLİĞİ VE ÇEVRİMİÇİ GİZLİLİK İLE İLGİLİ GÖRÜŞLERİ VE FARKINDALIKLARI ÜZERİNE BİR ARAŞTIRMA

4.1. Araştırmanın Yöntemi

Araştırmamızda saha araştırması yöntemi kullanılmıştır.

Bu bölümde çalışma kapsamında gerçekleştirilmiş olan araştırmanın evreni ve örneklemi, veri toplama aracı, verilerin analizi ve bulgulara yer verilmiştir. Veri toplama aracındaki sorular yani araştırmanın değişkenleri ve evren-örneklemi gibi bilgilerinin tanımlanması ile araştırmanın kapsamı belirlenmiştir. Daha sonra ise araştırmadan elde edilen bulgular yorumlanmıştır.

4.1.1. Araştırmanın evreni ve örneklemi

Araştırma evreni, internet siteleri ve sosyal medya platformlarının ülkemizdeki aktif kullanıcılarını kapsamaktadır. Bu rakam "We are Social" isimli ajansın 2015 yılına ait internet kullanımı verilerine göre 40 milyon aktif sosyal medya hesabıdır (wearesocial.net). Örneklem ise; 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 α= 0,05 kabul edilerek 384 olarak hesaplanmıştır. Bu sebeple 384"ün

üzerinde katılımcıya anket uygulanmıştır. Toplam 479 kullanıcı ankete katılmıştır.

4.1.2. Araştırma verilerinin toplanması

Çalışma kapsamında hazırlanan ankette yer alan sorular örneklem grubundaki internet ve sosyal medya kullanıcılarına yöneltilmiştir. Araştırmada "Kartopu örnekleme yöntemi" kullanılmıştır. Bu örneklemede önce bir çekirdek örneklem, elverişlilik örneği gibi araştırmayı yapan tarafından kendi keyfine göre bulunur. Ondan sonra ki örneklem elemanları ise daha önce bulunmuş olan (çekirdek elemanlar ve onların seçtiği diğer) elemanlar tarafından bulunurlar. Örnek böylece, sanki karda itilerek büyüyen, bir kartopu gibi büyüme gösterir (tr.wikipedia.org).

Anket soruları katılımcılara ülkemizde popüler olan Facebook, Twitter, Google Plus gibi sosyal medya platformları üzerinden çevrimiçi ortamda gönderilmiş; katılımcılar daha sonra ankete yanıt verdikten sonra, anketi diledikleri kişilere aynı ortamlar üzerinden ulaştırmışlardır.

4.1.2.1. Soru formu ve ölçüm araçları

Araştırmaya katılan internet ve sosyal medya platformları kullanıcılarının internet güvenliği ve çevrimiçi gizlilik hakkındaki kanaatlerini ve farkındalıklarını incelemek amacıyla bir anket formu hazırlanmıştır. Araştırmada Karakaya (2014) tarafından geliştirilmiş olan anket sorularından yararlanılmıştır. Bu sorular çalışmamız çerçevesinde geliştirilmiş, çalışmamızla ilgili olmayan sorular çıkartılmış ve yerlerine -ölçek bütünlüğünü bozmadan- çalışmamızla ilgili olan sorular dâhil edilmiştir. İnternet siteleri ve sosyal medya platformlarındaki katılımcılara bu sorular çevrimiçi ortamda http://goo.gl/forms/G9RyBSefpD bağlantısı kullanılarak

"Google Forms" isimli anket hizmeti kullanılarak gönderilmiştir. Hazırlanan anket formu 25 kişilik bir katılımcı grubuna uygulanıp ön teste tabi tutulmuştur. Bu test aracılığıyla katılımcıların anket sorularını ve cevaplarını ne ölçüde anlayabildikleri ve anketin alanı kapsama becerisi gözlenerek anket formuna son hali verilmiştir. (Testin güvenilirlik katsayısı 0,811 olarak belirlenmiştir.)

Çalışmanın internet ortamıyla ilgili olmasından dolayı anket sorularının bu ortam üzerinden gönderilmesi sorulara hızlı bir şekilde cevap alınmasını sağlamış ve bunun karşılığında maddi anlamda büyük bir maliyet ile karşılaşılmamıştır. Anket linkini alan bazı kullanıcıların anketi yanıtlamaması nedeniyle yeterli kişi sayısına ulaşabilmek için sosyal platformlar üzerinde ciddi ve süreklilik arz eden bir çalışma gerçekleştirilmiştir. Bu bağlamda birkaç gün içerisinde hedeflenen katılımcı sayısına erişilmiştir.

Anket formu "demografik sorular", "internet kullanımına ilişkin sorular", "sosyal medya sitelerinin kullanım sıklığına ilişkin sorular", "internet ve sosyal medya sitelerinin hangi amaçla ve bu amaçlara bağlı olarak sitelerin ne sıklıkta kullanıldığını ölçmeye ilişkin sorular", "kişisel bilgilerin mahremiyetinin ihlal edilip edilmediğiyle ilgili sorular", "gözetimin güvenlik amaçlı kullanımı ile ilgili sorular", "çevrimiçi kişisel bilgilerin toplanması karşısında internet kullanımından vazgeçme eğilimine ilişkin sorular", "çevrimiçi gizlilik ihlalleri karşısında gösterilen tutumla ilgili sorular" olmak üzere yedi bölüme ayrılmaktadır.

Araştırmada 5 faktör çıkarılmış; faktör başına ise en az 3 en çok 8 soru sorulmuştur. Faktörleri oluşturan sorular beşli likert ölçeğinde hazırlanmıştır. Sorular faktörler doğrultusunda pozitif yargı içerecek biçimde yapılandırılmıştır. Çalışmada demografik sorular dâhil olmak üzere toplamda 44 soru sorulmuştur. Sorular aşağıdaki gibi gruplandırılmıştır.

Yedi grup sorudan, ilk iki grup dışında kalan sorular faktörlerimizi oluşturmaktadır:

4.1.2.1.1. Kişisel bilgilere ilişkin sorular

Anketin bu bölümünde katılımcıların yaş, medeni durum, cinsiyet, gelir durumu ve eğitim durumu ile ilgili bilgilerin toplanmasına yönelik kişisel bilgi soruları sorulmuştur.

4.1.2.1.2. İnternet kullanımına ilişkin sorular

Bu bölümde internete nereden en çok erişildiği ve internetin hangi amaçlarla kullanıldığıyla ilgili sorular yöneltilmiştir. İnternete en çok nerede giriyorsunuz (ev, işyeri, internet kafe, kafe-okul vb. mekânlar). İnterneti bilgi, iletişim, alışveriş, bankacılık ve eğlence amaçlarıyla ilgili kullanım sıklığını ölçen sorular (her zaman, sıkça, arada sırada, nadiren, hiçbir zaman).

4.1.2.1.3. Sosyal medya sitelerinin kullanım sıklığı ve amacına ilişkin sorular

Bu bölümde katılımcılara, ülkemizde en popüler olan Facebook, Twitter, LinkedIn, Google Plus ve Foursquare isimli sosyal medya sitelerinin kullanım sıklığını ölçen sorular yöneltilmiştir (bu sorular yine "her zaman, sıkça, arada sırada, nadiren, hiçbir zaman" şeklinde 5 noktalı Likert ölçekte sorulmuştur). Yine bu bölümde katılımcılara Facebook, Twitter, LinkedIn, Google Plus ve Foursquare isimli sosyal medya sitelerini hangi amaçla (bilgi, paylaşım, iletişim, eğlence, iş ve yer bildirimi) ve hangi sıklıkta kullandıklarını ölçen sorular sorulmuştur (bu sorular yine "her zaman, sıkça, arada sırada, nadiren, hiçbir zaman" şeklinde 5 noktalı Likert ölçekte sorulmuştur).

4.1.2.1.4. Kişisel bilgilerin mahremiyetinin ihlal edilip edilmediğiyle ilgili sorular

Bu bölümde katılımcılara devlet, pazarlama şirketleri ve bilgisayar korsanları tarafından internet ve sosyal paylaşım sitelerinde kişisel bilgilerin mahremiyetinin ihlal edilip edilmediğiyle ilgili sorular yöneltilmiştir (Bu sorularda yine kesinlikle katılıyorum, katılıyorum, kararsızım, katılmıyorum, kesinlikle katılmıyorum şeklinde derecelendirilen 5 noktalı likert ölçek kullanılmıştır). Bu bölümden itibaren sorulan sorular çalışmamızın faktörlerine göre hazırlanmış sorulardır.

4.1.2.1.5. Çevrimiçi kişisel bilgilerin güvenlik amaçlı kullanımı ile ilgili sorular

Bu bölümde katılımcılara internet üzerinden elde edilen kişisel verilerin ve devlet tarafından yapılan gözetimin güvenlik amaçlı yapılıp yapılmadığına ilişkin sorular yöneltilmiştir. Katılımcıların kişisel verilerin güvenlik amaçlı toplanmasına ve gözetimin güvenlik amaçlı gerçekleştirildiğine ne kadar katılıp katılmadıkları ölçümlenmiştir (Bu sorularda yine kesinlikle katılıyorum, katılıyorum, kararsızım, katılmıyorum, kesinlikle katılmıyorum şeklinde derecelendirilen 5 noktalı likert ölçek kullanılmıştır).

4.1.2.1.6. Çevrimiçi kişisel bilgilerin toplanması karşısında internet kullanımından vazgeçme eğilimine ilişkin sorular

Katılımcılara çevrimiçi bilgilerin toplanması karşısında izledikleri tutumla ilgili sorular yöneltilmiştir. Kullanıcıların gözetlendiklerini bilseler de internet ve sosyal medyada var olmayı isteyip istemedikleri öğrenilmeye çalışılmıştır (Kesinlikle katılıyorum, katılıyorum, kararsızım, katılmıyorum,

kesinlikle katılmıyorum şeklinde derecelendirilmiş 5 noktalı likert ölçek burada da kullanılmıştır).

4.1.2.1.7. Çevrimiçi gizlilik ihlalleri karşısında gösterilen tutuma ilişkin sorular

Katılımcılara internet ve sosyal medyada gerçekleştirilen mahremiyet ihlalleri karşısında sergiledikleri tutuma ilişkin sorular yöneltilmiştir. Mahremiyet ihlalleri karşısında sosyal medya platformlarında sahte profille mi yoksa gerçek profille mi yer aldıkları öğrenilmeye çalışılmıştır. (Kesinlikle katılıyorum, katılıyorum, kararsızım, katılmıyorum, kesinlikle katılmıyorum şeklinde derecelendirilmiş 5 noktalı likert ölçek burada da kullanılmıştır).

4.2. Araştırma Verilerinin Analizi

Anket çalışmasından toplanan verilerin değerlendirilmesi ve analizinde SPSS 21,0 istatistik paket programı kullanılmıştır. Anketteki tüm sorulara ve ölçekteki önermelere verilen cevaplara ait frekans ve yüzde dağılımları hesaplanmış, bu dağılımlar çizelgeler ile gösterilmiştir.

Ayrıca örneklem büyüklüğünün Faktör Analizi yapmaya uygun olup olmadığını tespit etmek amacıyla KMO Testi ve Bartlett Testi yapılmıştır. Elde edilen sonuçlara göre örneklem büyüklüğünün, Faktör Analizi yapmaya uygun olduğu ortaya çıkmıştır. Böylece değişkenlerin arasında bir ilişki saptanmış ve benzer değişkenleri bir arada görebilmek; soruların faktörlere göre dağılımını tespit etmek amacıyla Faktör Analizi yapılmıştır.

Faktörler belirlendikten sonra yapılacak analizlerde hangi testlerin kullanılacağına karar verebilmek amacıyla "Normallik Testi" yapılmıştır. Çarpıklık ve Basıklık katsayılarının normal dağılıma sahip olduğu tespit edilmiştir.

Çarpıklık ve Basıklık katsayılarının normal dağılıma sahip olması bize Bağımsız T Testi ve ANOVA kullanabilme fırsatı vermektedir. Bu bağlamda çalışmamızda elde edilen verilere Bağımsız T Testi ve ANOVA analizi uygulanmıştır.

4.3. Bulgular ve Yorum

Bu bölümde ankette yer alan sorulara verilen cevapların frekans ve yüzde dağılımları çizelgeler ile gösterilmiş ve yorumlanmıştır. Bu cevapların analiz edilmesi sonucunda elde edilen bulguların yorumlanması ile araştırmanın sonuçlarına ulaşılmıştır.

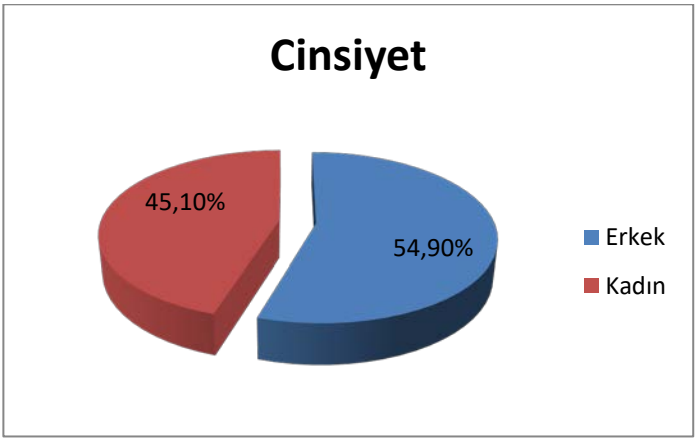
4.3.1. Kullanıcıların sosyo-demografik özellikleri

Bu başlık altında anketimize katılan internet ve sosyal medya kullanıcılarının; cinsiyet, yaş, eğitim durumu, gelir durumu ve medeni durumları çizelgelerle gösterilip yorumlanmaya çalışılmıştır.

4.3.1.1. Kullanıcıların cinsiyetlerine göre dağılımı

Çizelge 4.1. Cinsiyet dağılımı

	Frekans (f)	Yüzde (%)
Erkek	263	54,9
Kadın	216	45,1
Toplam	**479**	**100,0**



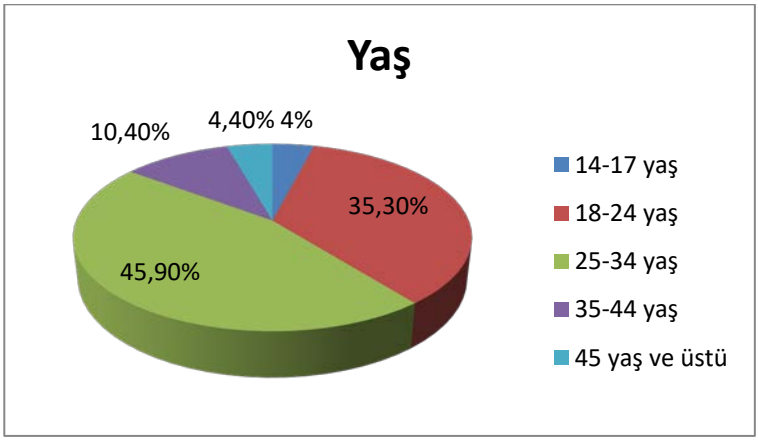
Şekil 4.1. Cinsiyete ilişkin yüzde dağılım grafiği

Katılımcıların %54,9'unu 263 kişi ile erkek kullanıcılar, %45,1'ini ise 216 kişi ile kadın kullanıcılar oluşturmuştur. Bu bağlamda katılımcılar arasında dengeli bir dağılım olduğu söylenebilir.

4.3.1.2. Kullanıcıların yaşa göre dağılımı

Çizelge 4.2. Kullanıcıların yaş dağılımı

	Frekans (f)	Yüzde (%)
14-17 yaş	19	4,0
18-24 yaş	169	35,3
25-34 yaş	220	45,9
35-44 yaş	50	10,4
45 ve üstü	21	4,4
Toplam	**479**	**100**



Şekil 4.2. Yaşa ilişkin yüzde dağılım grafiği

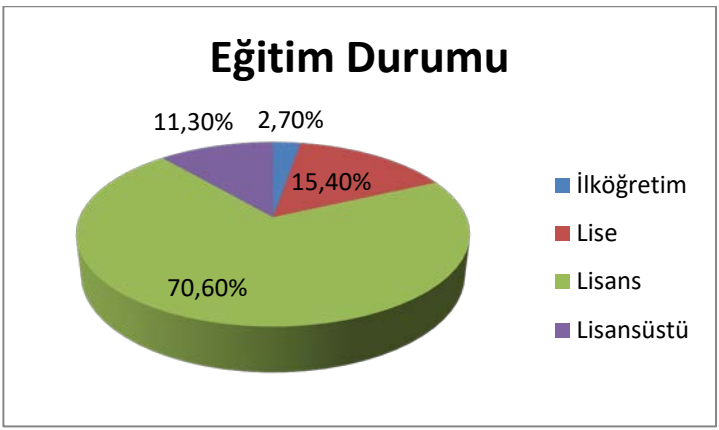
Ergenlik dönemindeki lise öğrencilerinin de internet ve sosyal medyada son derece aktif bir rol oynaması nedeniyle anketimize lise öğrencileri dâhil edilmiş ve bu bireyler 14-17 yaş kategorisinde değerlendirilmiştir. 18-24 yaş kategorileri erken gençlik, 25-34 geç gençlik, 35-44 yaş olgunluk, 45 yaş ve üstü orta yaş ile yaşlılık dönemini temsil etmektedir.

Anket çalışmamıza katılan internet ve sosyal medya kullanıcılarının %45,9'unu 220 kişi ile 25-34 yaş arası kişiler, %35,3'ünü 169 kişi ile 18-24 arası kişiler, %10,4'ünü 50 kişi ile 35-44 yaş arası kişiler, %4,4'ünü 21 kişi ile 45 yaş ve üstü kişiler, son olarak %4'ünü 19 kişi ile 14-17 yaş arası kişiler oluşturmuştur. Bu bağlamda anketimize genel olarak ilginin %81,2 gibi büyük bir oranla gençlerden geldiğini söyleyebiliriz.

4.3.1.3. Kullanıcıların eğitim durumuna göre dağılımı

Çizelge 4.3. Katılımcıların eğitim durumlarının dağılımı

	Frekans (f)	Yüzde (%)
İlköğretim	13	2,7
Lise	74	15,4
Lisans	338	70,6
Lisansüstü	54	11,3
Toplam	**479**	**100,0**



Şekil 4.3. Eğitim durumuna ilişkin yüzde dağılım grafiği

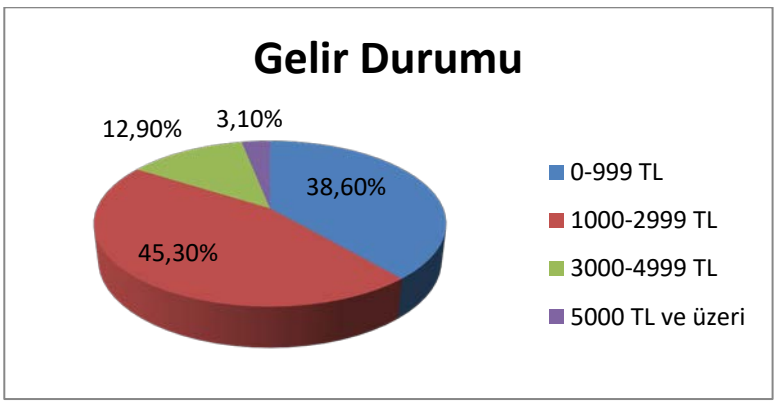
Katılımcıların %70,6'sı 338 kişi ile Lisans, %15,4'ü 74 kişi ile Lise, %11,3'ü 54 kişi ile Lisansüstü, %2,7'yle 13 kişi İlköğretim mezunudur. Bu bağlamda anketimize katılan kullanıcıların %70,6 ile büyük çoğunluğunu üniversitelerin lisans bölümlerinden mezun olanlar oluşturmuştur. Lisans ve Lisansüstü bölümlerden mezun olan kullanıcıların toplam oranı %81,9'dur; bu da göstermektedir ki anketimize katılan

kullanıcıların 5'te 4'ü son derece eğitimli bireylerden oluşmaktadır.

4.3.1.4. Kullanıcıların gelir durumuna göre dağılımı

Çizelge 4.4. Kullanıcıların gelir durumuna göre dağılımı

	Frekans (f)	Yüzde (%)
0-999 TL	185	38,6
1000-2999 TL	217	45,3
3000-4999 TL	62	12,9
5000 TL ve üzeri	15	3,1
Toplam	**479**	**100,0**



Şekil 4.4. Gelir durumuna ilişkin yüzde dağılım grafiği

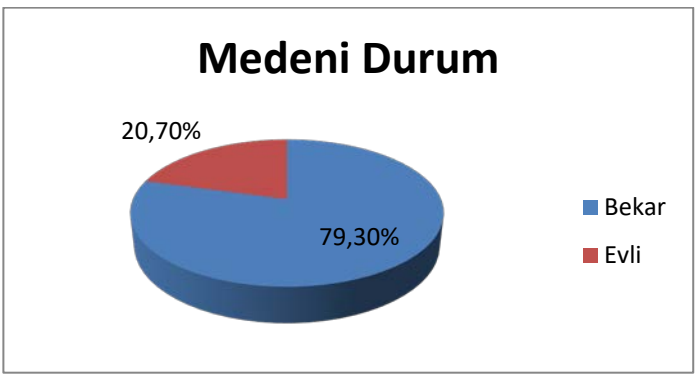
Kullanıcıların %45,3'ünü 217 kişi ile 1000-2999 TL, %38,6'sını 185 kişi ile 0-999 TL, %12,9'unu 62 kişi ile 3000-4999 TL, %3,1'ini 15 kişi ile 5000 TL ve üzeri gelir grubu arasındaki kişiler oluşturmuştur. Çalışmamızın hazırlandığı tarihlerde

ülkemizde net asgari ücret 1000 Türk Lirasıdır (muhasebetr.com). Bu bağlamda çalışmamıza katılan kullanıcıların %38,6'sı asgari ücret ve altında maaş almaktayken; %61,4'ü asgari ücretin üzerinde maaş almaktadır. 3000 TL ve üstünün orta ve yüksek gelir grubu olarak düşünüldüğünde, çalışmamıza katılan kullanıcıların yalnızca %16'sı bu gruba mensuptur. Çalışmamızın çok büyük bir çoğunluğunu %84,2 ile düşük ve orta gelir durumuna sahip olan kullanıcılar oluşturmuştur.

4.3.1.5. Katılımcıların medeni duruma göre dağılımı

Çizelge 4.5. katılımcıların medeni duruma göre dağılımı

	Frekans (f)	Yüzde (%)
Bekâr	380	79,3
Evli	99	20,7
Toplam	**479**	**100,0**



Şekil 4.5. Medeni duruma ilişkin yüzde dağılım grafiği

Anketimize katılan kullanıcıların %79,3'ünü 380 kişi ile bekâr kullanıcılar, %20,7'sini ise 99 kişi ile evli kullanıcılar oluşturmuştur. Buna göre anketimize katılan kullanıcıların büyük bir bölümü bekârdır.

4.3.2. İnternetin Kullanım Amacıyla İlgili Bulgular

Bu bölümde anketimize katılan internet ve sosyal medya kullanıcılarının interneti hangi amaçla (bilgi, iletişim, alışveriş, bankacılık işlemleri ve eğlence) ve ne sıklıkta (hiçbir zaman, nadiren, arada sırada, sıkça, her zaman) kullandıkları çizelgelerle gösterilmiş ve yorumlamaya çalışılmıştır.

4.3.2.1. İnternetin bilgi amacıyla kullanımı

Çizelge 4.6. İnternetin bilgi amacıyla kullanımı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	1	0,2
Nadiren	6	1,3
Arada Sırada	47	9,8
Sıkça	238	49,7
Her Zaman	187	39
Toplam	**479**	**100,0**

Katılımcıların %49,7'si 238 kişi ile "sıkça", %39'u 187 kişi "her zaman", %9,8'i 47 kişi ile "arada sırada", %1,3'ü 6 kişi ile "nadiren", %0,2'si 1 kişi ile "hiçbir zaman" interneti bilgi almak amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın %88,7'si interneti bilgi almak amacıyla çoğu zaman kullanmaktadırlar. Bu verilere göre katılımcılar

tarafından internetin önemli bir bilgilendirme kaynağı olarak dikkate alındığını söyleyebiliriz.

İnternet, bilginin ulaştırılması bakımından her sektör için vazgeçilmez bir öneme sahiptir. Bilginin hem hızlı bir şekilde yayılmasını sağlaması, hem de bilgiye müdahale etmeye olanak tanıyan bir mecra olması bakımından internet, her geçen gün önem kazanmakta ve kullanımı artmaktadır (Vural ve Bat, 2010).

Sosyal paylaşım sitelerine ayrılan vaktin artması ile dijital yerliler (1980 ve sonrası doğumlular) hiçbir zahmete katlanmadan, dünyanın neresinde olursa olsun istedikleri bilgiye ulaşabilmektedir, bu durum bilginin paylaşılmasının bir sonucudur. Web 2.0 uygulamalarının ortaya çıkmasıyla kütüphane kullanıcıları bile kütüphanelere gitmek yerine web teknolojilerini kullanarak kendi verilerini yönetmeye, başka kaynaklardan buldukları zengin bilgileri kendi bilgileriyle bütünleştirmeye ve bu bilgileri başkalarıyla paylaşmaya başlamışlardır. Dolayısıyla dijital yerlilerin artık ihtiyaç duydukları bilgileri dijital olarak temin etmeye başlamışlardır (Kakırman, 2012).

4.3.2.2. İnternetin iletişim amacıyla kullanımı

Çizelge 4.7. İnternetin iletişim amacıyla kullanımı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	2	0,4
Nadiren	16	3,3
Arada Sırada	87	18,2
Sıkça	212	44,3
Her Zaman	162	33,8
Toplam	**479**	**100,0**

Katılımcıların %44,3'ü 212 kişi ile "sıkça", %33,8'i 162 kişi ile "her zaman", %18,2'si 87 kişi ile "arada sırada", %3,3'ü 16 kişi ile "nadiren", %0,4'ü 2 kişi ile "hiçbir zaman" interneti iletişim amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın %78,1'i interneti iletişim amacıyla çoğu zaman kullanmaktadırlar.

Sosyal medya zaman ve mekân sınırlaması olmadan, paylaşımın, tartışmanın esas olduğu bir iletişim şeklidir (Vural ve Bat, 2010). Mobil tabanlı sosyal medyada kelimelerin, görsellerin, ses dosyalarının paylaşılması söz konusu olmaktadır.

Kakırman'a göre coğrafi, fiziksel ve ekonomik engelleri ortadan kaldırması nedeniyle, gerçek hayatta girilmesi mümkün olmayan gruplara girip kişilerin kendilerini daha rahat ifade edebilmeleri bu sitelerin popüler hale gelmesini sağlamıştır (Kakırman, 2012).

İnternet ve sosyal medyanın bir diğer önemli özelliği ise geleneksel medya oluşturulduktan sonra değiştirilemezken (bir dergi makalesi basıldıktan ve dağıtıldıktan sonra aynı makale üzerinde değişiklik yapılamaz); sosyal medyada yorumlar veya yeniden düzenlemeyle anında değiştirilebilir. Geleneksel medya iletişimlerinde zaman farkı sosyal medyaya göre daha uzundur (tr.wikipedia.org).

Sosyal medya geleneksel medyaya göre daha ucuzdur, erişim imkânları daha kolaydır, kullanımı basittir ve üzerinde değişimi kolay olduğundan sabitlik söz konusu değildir (Vural ve Bat, 2010).

İnternetin bu denli toplu ve hızlı bir iletişime olanak vermesi, ucuz olması ve sınırları ortadan kaldırabilmesi nedeniyle bir iletişim aracı olarak kullanımını cazip hale getirmektedir. Nitekim anketimize katılan internet ve sosyal medya kullanıcılarının interneti önemli bir iletişim aracı olarak gördükleri çizelge 4.7.'deki verilerden anlaşılmaktadır.

4.3.2.3. İnternetin alışveriş amacıyla kullanımı

Çizelge 4.8. İnternetin alışveriş amacıyla kullanımı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	57	11,9
Nadiren	136	28,4
Arada Sırada	190	39,7
Sıkça	75	15,7
Her Zaman	21	4,4
Toplam	**479**	**100,0**

Katılımcıların %39,7'si 190 kişi ile "arada sırada", %28,4'ü 136 kişi ile "nadiren", %15,7'si 75 kişi ile "sıkça", %11,9'u 57 kişi ile "hiçbir zaman", %4,4'ü 21 kişi ile "her zaman" interneti alışveriş yapmak amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın yalnızca %20,1 alışverişlerini genellikle internet sitelerinden yapmaktadırlar. Katılımcılarımızın %68,1'i büyük bir çoğunlukla internetten yalnızca bazı zamanlarda alışveriş yapmaktadırlar. Bu veriler ışığında katılımcılarımızın büyük çoğunluğunun geleneksel alışveriş yöntemlerine eğilimli olduğu ortaya çıkmaktadır. Katılımcıların çoğu alışverişlerini internet sitelerindeki sanal mağazalar yerine, gerçek mağazalara gidip yapmaktadırlar.

4.3.2.4. İnternetin bankacılık işlemleri amacıyla kullanımı

Çizelge 4.9. İnternetin bankacılık işlemleri amacıyla kullanımı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	95	19,8
Nadiren	82	19,2
Arada Sırada	101	21,1
Sıkça	128	26,7
Her Zaman	63	13,2
Toplam	**479**	**100,0**

Katılımcıların %26,7'si 128 kişi ile "sıkça", %21,1'i 101 kişi ile "arada sırada", %19,8'si 95 kişi ile "hiçbir zaman", %19,2'si 82 kişi ile "nadiren", %13,2'si 63 kişi ile "her zaman" interneti bankacılık işlemlerini yapmak amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın %80,2'sinin bankacılık işlemlerini internet üzerinden gerçekleştirdiği ortaya çıkmaktadır. İnternet bankacılığı hizmetleri günümüzde banka müşterilerine büyük avantajlar sunmaktadır. İnternet şubesinde, gerçek şubedeki gibi sıra alıp beklemek gerekmemektedir. Ayrıca internet şubesinde yapılan işlemlerin bazısından hiç ücret alınmazken, bazısından ise çok düşük bir ücret alınmaktadır. Son zamanlarda bazı bankalar şubesiz bankacılık sistemindeki alternatif seçenekler kurmuşlardır. Örneğin Finansbank "Enpara", Yapı Kredi Bankası ise "Nuvo" isimli şubesiz bankacılık hizmetleri başlatmışlardır. Bu tür hizmetlerde yapılan hiçbir işlemden ücret alınmamakta ve hesaplara yıllık işletim ücreti uygulanmamaktadır. Buna

paralel olarak yukarıdaki veriler günümüzde internet bankacılığına büyük bir yönelim olduğu görülmektedir. Katılımcılarımızın yalnızca %19,8'lik kısmı internet bankacılığı hizmetlerini "hiçbir zaman" kullanmamaktadır.

4.3.2.5. İnternetin eğlence (müzik, film, oyun vb.) amacıyla kullanımı

Çizelge 4.10. İnternetin eğlence amacıyla kullanımı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	2	0,4
Nadiren	30	6,3
Arada Sırada	87	18,2
Sıkça	196	40,9
Her Zaman	164	34,2
Toplam	**479**	**100,0**

Katılımcıların %40,9'u 196 kişi ile "sıkça", %34,2'si 164 kişi ile "her zaman", %18,2'si 87 kişi ile arada sırada, %6,3'ü 30 kişi ile "nadiren", %0,4'ü 2 kişi ile "hiçbir zaman" interneti eğlence (müzik, film, oyun vb.) amacıyla kullandıklarını belirtmişlerdir. Son yıllarda bant genişliğinin artması, bilgisayar ve cep telefonu teknolojilerinin gelişmesi, 3G/4G gibi internete hemen hemen her yerden erişim fırsatı veren mobil teknolojileri sayesinde internet kullanım oranı çok yüksek rakamlara ulaşmıştır. Artan bant genişliği müzik, film ve oyun gibi içeriklere internet üzerinden kolayca erişilmesini sağlamıştır. Bunun yanında internet üzerinden Spotify ve Deezer gibi servisler düşük bir ücret karşılığında aynı anda yüz binlerce albüme ulaşılmasını ve milyonlarca şarkının çevrimiçi

ortamdan dinlenebilmesini sağlamaktadır. Youtube gibi video izleme siteleri ise milyonlarca videoya bedava erişilmesini sağlamaktadır. Öte yandan artık birçok oyun internet üzerinden çok oyunculu (multiplayer) olarak oynanabilmektedir. Yukarıdaki veriler ışığında katılımcılarımızın %çok büyük bir bölümünün %75,1 ile interneti eğlence amaçlı olarak çoğu zaman kullandığı ortaya çıkmaktadır. Bu bağlamda katılımcıların interneti önemli bir eğlence aracı olarak gördüklerini ve yukarıda geçen içeriklere internet üzerinden erişim sağladıklarını söyleyebiliriz.

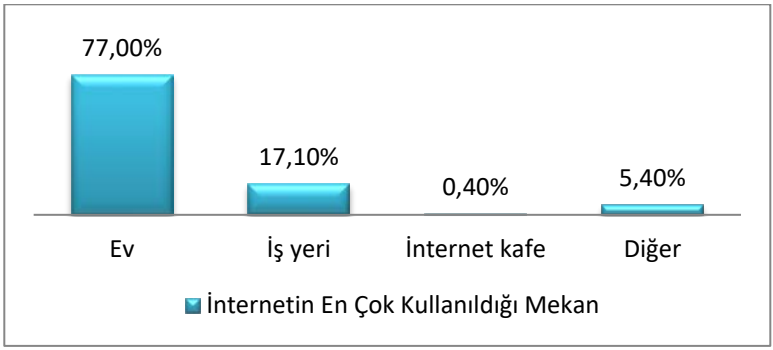
4.3.3. İnternet Siteleri ve Sosyal Ağlardaki Davranışla İlgili Bulgular

Bu bölümde anketimize katılan internet ve sosyal medya siteleri kullanıcılarının, internet siteleri ve sosyal ağlardaki davranışlarına ilişkin bulgular çizelgeyle gösterilmiş ve yorumlanmaya çalışılmıştır.

4.3.3.1. İnternetin en çok kullanıldığı mekân

Çizelge 4.11. İnternetin en çok kullanıldığı mekân

	Frekans (f)	Yüzde (%)
Ev	369	77,0
İş yeri	82	17,1
İnternet kafe	2	0,4
Diğer	26	5,4
Toplam	**479**	**100,0**



Şekil 4.6. İnternetin en çok kullanıldığı mekâna ilişkin yüzde dağılım grafiği

Yaptığımız anket çalışmasında katılımcılara "İnternete en çok nerede giriyorsunuz" şeklinde bir soru yöneltilmiş ve cevap olarak "ev", "iş yeri", "internet kafe" ve "diğer" seçeneklerinden birini vermeleri istenmiştir. Katılımcıların %77'si 369 kişi ile "ev", %17,1'i 82 ile "iş yeri", %5,4'ü 26 kişi ile "diğer", %0,4'ü 2 kişi ile "internet kafe" cevabını vermişlerdir. Verilen yanıtlara göre katılımcıların çok büyük bir bölümü %77 ile interneti evlerinde daha fazla kullandıklarını ifade etmişlerdir. İnternet bağlantısının ülkemizin hemen hemen her noktasına yayılması, bağlantı hızlarındaki yükselme ve fiyatların 2000'li yılların başlarındaki seviyeden aşağı inmesi, bilgisayar teknolojilerinin gelişmesi, bilgisayar fiyatlarında düşüş yaşanması, 3G/4G gibi mobil teknolojilerinin yaygınlaşması ve akıllı telefonların ortaya çıkması interneti hemen hemen tüm evlere girmesini sağlamıştır. Bu bağlamda 2000'li yılların başlarında çok popüler olan internet kafelere olan yönelimin çok fazla düştüğü gözlenmektedir.

4.3.3.2. İnternet siteleri/sosyal ağlara kaydolurken kullanım şartları ve gizlilik politikasını okuma sıklığı

Çizelge 4.12. İnternet siteleri/sosyal ağlara kaydolurken kullanım şartları ve gizlilik politikasını okuma sıklığı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	150	31,3
Nadiren	148	30,9
Arada Sırada	97	20,3
Sıkça	31	6,5
Her Zaman	53	11,1
Toplam	**479**	**100,0**

Katılımcılara "internet siteleri ve sosyal ağlara kaydolurken kullanım şartları ve gizlilik politikasını okur musunuz?" sorusu yöneltilmiş. Katılımcıların %31,3'ü ile 150 kişi "hiçbir zaman", %30,9'u 148 kişi ile "nadiren", %20,3'ü 97 kişi ile "arada sırada", %11,1'i 53 kişi ile "her zaman", %6,5'i 31 kişi ile "sıkça" cevaplarını vermişlerdir. Bu verilere göre %31,3 ile katılımcıların yaklaşık üçte biri internet ve sosyal medya sitelerinin kullanım şartlarını ve gizlilik politikalarını hiçbir zaman okumamaktadırlar. Katılımcıların%17,6'sı gibi küçük bir kesim ise bu tür metinleri çoğu zaman okumaktadır.

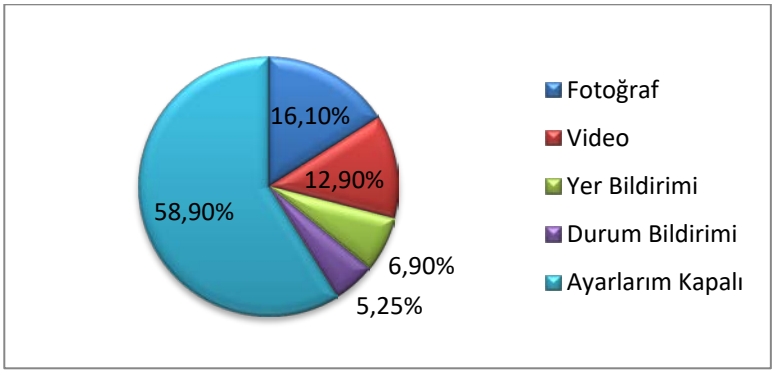
Kullanım şartları ve gizlilik politikası bir internet sitesinin ya da sosyal ağın kullanılmasıyla ilgili şartlardır. Bir kullanıcı bu sitelere üye olmadan önce bu şartları okumalı ve bu şekilde üye olmalıdır. Bu şartlar okunmadan onaylandığı ve siteye üye olunduğu takdirde kullanım şartlarında belirtilen hususlardan doğacak hükümler kullanıcı tarafından peşinen kabul edilmiş olur (en.wikipedia.org). Kısacası bu tür

kullanım şartları ve gizlilik politikaları birer feragatnamedir. Fakat bu tür metinler sayfalar süren uzunlukta oldukları ve hukuksal bir dil kullanıldığından ötürü metinlerin okunması sıkıcı gelebilir ve genellikle kullanıcılar bir siteye üye olurken bunları okumazlar. Çoğu internet sitesi veya sosyal ağın gizlilik politikası dikkatlice incelendiğinde bu metinlerde çevrimiçi gizliliğimize aykırı hükümler bulunduğu ortaya çıkmaktadır. Bir internet sitesine ya da sosyal ağa üye olurken bu tür metinleri okunmaktan kaçınılmaması gerekmektedir, aksi takdirde doğacak herhangi hukuki bir durumda hak iddia etmemiz söz konusu olamaz.

4.3.3.3. Sosyal paylaşım ağlarında katılımcıların bilgisi dışında yer alması istenmeyen içeriğin dağılımı

Çizelge 4.13. Sosyal paylaşım ağlarında katılımcıların bilgisi dışında yer alması istenmeyen içeriğin dağılımı

	Frekans (f)	Yüzde (%)
Fotoğraf	77	16,1
Video	62	12,9
Yer Bildirimi	33	6,9
Durum Bildirimi	25	5,2
Ayarlarım Kapalı Durumdadır	282	58,9
Toplam	**479**	**100,0**



Şekil 4.7. Sosyal paylaşım ağlarında katılımcıların bilgisi dışında yer alması istenmeyen içeriğe ilişkin yüzde dağılım grafiği

Katılımcılara "sosyal paylaşım ağlarında bilginiz dışında sizinle ilgili ne tür içeriklerin yer alması sizi rahatsız eder" sorusu yöneltilmiştir. Katılımcıların %16,1'i ile 77 kişi "fotoğraf, %12,9'u ile 62 kişi "video", %6,9'u ile 33 kişi "yer bildirimi", %5,2'si ile 25 kişi "durum bildirimi" seçeneklerini işaretlemişlerdir. Katılımcıların yarısından fazlası %58,9 ile 282 kişi, bilgileri dışında içerik paylaşılmasını önlemek anlamıyla ayarlarını kapalı duruma getirmişlerdir. Bu bağlamda katılımcıların sosyal ağlardaki gizlilik ayarlarının farkında olduğu söylenebilir. Gizlilik ayarları Facebook gibi sosyal ağlarda kullanıcıların mağdur edilmelerini önlemek amacıyla, kullanıcıların istedikleri gibi ayarlayabilecekleri şekilde oluşturulmuştur.

4.3.3.4. Hiç kullanılmayan sosyal ağ sitelerinin dağılımı

Çizelge 4.14. Hiç kullanılmayan sosyal ağ sitelerinin dağılımı

	Frekans (f)	Yüzde (%)
Facebook	5	1,0
Twitter	136	28,4
LinkedIn	299	62,4
Google Plus	248	51,8
Instagram	135	28,2
Pinterest	372	77,7
Foursquare	297	62,0

Katılımcılara "hiç kullanmadığınız sosyal ağ hangisidir" sorusu yöneltilmiş ve cevap olarak Facebook, Twitter, LinkedIn, Google Plus, Instagram, Pinterest ve Fourquare isimli sosyal ağlardan birini seçmeleri istenmiştir. Katılımcılar arasından 372 kişi "Pinterest" 299 kişi "LinkedIn, 297 kişi ise "Foursquare" isimli sosyal ağları hiç kullanmadıklarını belirtmişlerdir. Yalnızca 5 kişi "Facebook" cevabını vermiştir. Bu veriler ışığında kullanıcıların günümüzün en popüler sosyal ağı olan Facebook'a çok büyük ilgi gösterdiğini ve yalnızca 5 kişinin bu sosyal ağda profili olmadığı saptanmaktadır.

4.3.4. Sosyal Ağlarım Kullanım Amacı ve Sıklığı

Bu bölümde anketimize katılan internet ve sosyal medya siteleri kullanıcılarının, sosyal ağ sitelerini kullanım amacı ve sıklığına ilişkin bulgular çizelgeyle gösterilmiş ve yorumlanmaya çalışılmıştır

4.3.4.1. Sosyal ağlarım kullanım sıklığı

Çizelge 4.15. Sosyal ağları kullanım sıklığı

	Frekans (f)	Yüzde (%)
Hiçbir Zaman	0	0,0
Nadiren	16	3,4
Arada Sırada	71	14,8
Sıkça	196	40,9
Her Zaman	196	40,9
Toplam	**479**	**100,0**

Katılımcılara "hangi sıklıkta sosyal paylaşım sitelerini kullanıyorsunuz" sorusu yöneltilmiştir. Katılımcıların verdikleri cevaba göre oranlar yukarıdaki çizelgedeki gibidir. Katılımcıların %40,9'u ile 196 kişi "her zaman", yine %40,9'u ile 196 kişi "sıkça", %14,8'i 71 kişi ile "arada sırada", %3,4'ü 16 kişi ile "nadiren" sosyal medya sitelerini kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın %81,8'inin büyük bir çoğunlukla sosyal platformlarda aktif olduğu görünmektedir. Bu veriler aynı zamanda araştırma evrenini temsil eden örneklemi vurgulamaktadır. Araştırmamız örneklemi aktif olan internet ve sosyal medya kullanıcılarından seçilmiştir. Böylece ankete katılan kullanıcıların doğru seçildikleri ve araştırmayla paralellik taşıdıkları tespit edilmiştir. Bu sonuç araştırmamızın tutarlılığı açısından önem arz etmektedir.

4.3.4.2. Sosyal paylaşım ağlarının kullanım amaçları dağılımı

Bu bölümde katılımcıların sosyal paylaşım ağlarını kullanım amacı ve dağılımı çizelge ile gösterilip yorumlanmaya çalışılmıştır.

Çizelge 4.16. Sosyal paylaşım ağlarının kullanım amaçları dağılımı

Sosyal paylaşım ağları kullanım amacı ve derecesi		**f**	**%**
Bilgi amaçlı (haber, köşe yazısı vb.) kullanım	Hiçbir zaman	11	2,3
	Nadiren	46	9,6
	Arada sırada	121	25,3
	Sıkça	217	45,3
	Her zaman	84	17,5
	Toplam	**479**	**100**
Paylaşım amaçlı (durum, fotoğraf, video, müzik, vb.) kullanım	Hiçbir zaman	18	3,8
	Nadiren	78	16,3
	Arada sırada	151	31,5
	Sıkça	158	33,0
	Her zaman	74	15,4
	Toplam	**479**	**100**

İletişim amaçlı (Sohbet, beğeni, vb.) kullanım	Hiçbir zaman	15	3,1
	Nadiren	65	13,6
	Arada sırada	132	27,6
	Sıkça	167	34,9
	Her zaman	100	20,9
	Toplam	**479**	**100**
Eğlence amaçlı (Oyun, vb.) kullanım	Hiçbir zaman	129	26,9
	Nadiren	127	26,5
	Arada sırada	118	24,6
	Sıkça	67	14,0
	Her zaman	38	7,9
	Toplam	**479**	**100**
İş amaçlı kullanım	Hiçbir zaman	122	25,5
	Nadiren	119	24,8
	Arada sırada	128	26,7
	Sıkça	83	17,3
	Her zaman	27	5,6
	Toplam	**479**	**100**
Yer bildirimi amaçlı kullanım	Hiçbir zaman	173	36,1
	Nadiren	146	30,5
	Arada sırada	89	18,6
	Sıkça	45	9,4
	Her zaman	26	5,4
	Toplam	**479**	**100**

Katılımcıların %45,3'ü 217 kişi ile "sıkça", %25,3'ü 121 kişi ile "arada sırada", %17,5'i 84 kişi ile "her zaman", %9,6'sı 46 kişi ile "nadiren", %2,3'ü 11 kişi ile "hiçbir zaman" sosyal paylaşım ağlarını bilgi amaçlı kullandıklarını belirtmişlerdir.

Bu bağlamda katılımcıların %62,8 ile hemen hemen üçte ikisi sosyal paylaşım ağlarını bilgi alma amacıyla aktif olarak kullanmaktadır. Katılımcıların çok az bir kısmı %2,3 ile sosyal paylaşım ağlarını bilgi amacıyla kullanmaktadır. Böylece katılımcıların önemli bir bölümünün sosyal medya sayesinde bilişsel ihtiyaçlarını karşıladıkları söylenebilir.

Katılımcıların %33'ü 158 kişi ile "sıkça", %31,5'i 151 kişi ile "arada sırada", %16,3'ü 78 kişi ile "nadiren", %15,4'ü 74 kişi ile "her zaman", %3,8'i 18 kişi ile "hiçbir zaman" sosyal paylaşım ağlarını durum, fotoğraf, video, müzik vb. içerikleri paylaşmak amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcıların %48,4'ü ile yaklaşık yarısı sosyal paylaşım ağlarını içerik paylaşmak amacıyla aktif olarak kullanmaktadır. Yalnız 3,8'lik bir kısım sosyal paylaşım ağlarında içerik paylaşmadığını belirtmiştir. Buna göre katılımcıların bütünleştirici ihtiyaçlarını sosyal medya sayesinde karşıladıkları söylenebilir.

Katılımcıların %34,9'u 167 kişi ile "sıkça", %27,6'sı 132 kişi ile "arada sırada", %20,9'u 100 kişi ile "her zaman", %13,6'sı 65 kişi ile "nadiren", %3,1'i 15 kişi ile "hiçbir zaman" sosyal paylaşım ağlarını iletişim amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcılarımızın %55,8 ile yarısından fazlası sosyal paylaşım ağlarını iletişim amacıyla kullanmaktadır. Sosyal paylaşım ağlarını iletişim amacıyla kullanmayan katılımcıların dağılımı %3,1 ile çok düşük bir dağılım göstermektedir. Yukarıdaki verilere göre sosyal medyayı önemli bir iletişim aracı olarak gören kullanıcılar sosyal medya sayesinde bilişsel, duygusal ve sosyal bütünleştirici ihtiyaçlarını gidermektedirler.

Katılımcıların %26,9'u 129 kişi ile "hiçbir zaman", %26,5'i 127 kişi ile "nadiren", %24,6'sı 118 kişi ile "arada sırada", %14'ü 67 kişi ile "sıkça", %7,9'u 38 kişi ile "her zaman" sosyal paylaşım ağlarını eğlence amacıyla kullandıklarını

belirtmişlerdir. Bu bağlamda katılımcıların yalnızca %21,9'u sosyal paylaşım ağlarını eğlence amacıyla çoğu zaman kullanmaktadır. %26,9'luk kesim ise bu sosyal paylaşım ağlarını eğlence amacıyla hiç kullanmamaktadır ve bu dağılımın katılımcıların önemli bir bölümünü oluşturduğu söylenebilir.

Katılımcıların %26,7'si 128 kişi ile "arada sırada", %25,5'i 122 kişi ile "hiçbir zaman", %24,8'i 119 kişi ile "nadiren", %17,3'ü 83 kişi ile "sıkça", %5,6'sı 27 kişi ile "her zaman" sosyal paylaşım ağlarını iş amacıyla kullandıklarını belirtmişlerdir. Bu bağlamda katılımcıların yalnızca %22,9'unun sosyal paylaşım ağlarını iş amacıyla çokça kullandıkları ortaya çıkmaktadır. Katılımcıların %25,5'i ile önemli bir bölümü sosyal paylaşım ağlarını iş amacıyla kullanmadıklarını belirtmişlerdir. Yukarıdaki oranlara göre sosyal paylaşım ağlarının katılımcılarımız tarafından iş amacıyla pek rağbet görmediği söylenebilir.

Katılımcıların %36,1'i 173 kişi ile "hiçbir zaman", %30,5'i 146 kişi ile "nadiren", %18,6'sı 89 kişi ile "arada sırada", %9,4'ü 45 kişi ile "sıkça", %5,4'ü 26 kişi ile "her zaman" sosyal paylaşım ağlarını yer bildirimi yapmak amacıyla kullandıklarını belirtmişlerdir. Sosyal paylaşım ağlarının bir başka özelliği de o an kullanıcının bulunduğu mekânı ve konum bilgisini paylaşmaya olanak sağlamasıdır. Yukarıdaki oranlara göre katılımcılarımızın yalnızca %15'lik bir bölümü bu özelliği çoğu zaman kullanmaktadır. Katılımcıların %36'1 ile yüksek oranlı bir kesimi ise bu özelliği hiçbir zaman kullanmamaktadır.

4.3.4.3. Sosyal paylaşım ağlarında içerik paylaşılma sıklığı

Çizelge 4.17. Sosyal paylaşım ağlarında içerik paylaşılma sıklığı

	Frekans (f)	Yüzde (%)
Bir haftadan daha fazla	181	37,8
Haftada bir	90	18,8
Üç günde bir	81	16,9
Gün aşırı	69	14,4
Her gün	58	12,1
Toplam	**479**	**100,0**

Katılımcıların %37,8'i 181 kişi ile "bir haftadan daha fazla", %18,8'i 90 kişi ile "haftada bir", %16,9!u ile 81 kişi "üç günde bir", %14,4'ü 69 kişi ile "gün aşırı", %12,1'i 58 kişi ile "her gün" sosyal paylaşım ağlarında içerik paylaştıklarını belirtmişlerdir. Bu bağlamda katılımcıların %62,2'sinin haftada en az bir kere sosyal paylaşım ağlarında içerik paylaştığı ortaya çıkmaktadır.

4.3.5. Katılımcıların Gözetim ve Mahremiyetle İlgili Tutumları

Bu bölümde katılımcıların gözetim olgusu ve mahremiyetle ilgili yöneltilen sorulara verdiği cevapların dağılımı çizelge ile gösterilmiş ve yorumlanmaya çalışılmıştır

Çizelge 4.18. Katılımcıların gözetim ve mahremiyetle ilgili tutumlarının dağılımı

Katılımcıların gözetim ve mahremiyetle ilgili tutumları		**f**	**%**
İnternet ve sosyal paylaşım siteleri kullanıcısına güvenilir bir iletişim ortamı sağlamaktadır	Kesinlikle katılmıyorum	64	13,4
	Katılmıyorum	175	36,5
	Kararsızım	163	34,0
	Katılıyorum	55	11,5
	Kesinlikle Katılıyorum	22	4,6
	Toplam	**479**	**100**
İnternet ve sosyal paylaşım ağlarında daha kendimi özgür hissediyorum	Kesinlikle katılmıyorum	56	11,7
	Katılmıyorum	202	42,2
	Kararsızım	95	19,8
	Katılıyorum	102	21,3
	Kesinlikle Katılıyorum	24	5,0
	Toplam	**479**	**100**
İnternet ve sosyal paylaşım sitelerinde bireylerin mahremiyetleri hükûmetler, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edilmektedir	Kesinlikle katılmıyorum	11	2,3
	Katılmıyorum	80	16,7
	Kararsızım	135	28,2
	Katılıyorum	167	34,9
	Kesinlikle Katılıyorum	100	20,9
	Toplam	**479**	**100**
İnternet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bilsem de varlığımı sürdürmeye devam ederim	Kesinlikle katılmıyorum	69	14,4
	Katılmıyorum	132	27,6
	Kararsızım	142	29,6
	Katılıyorum	120	25,1
	Kesinlikle Katılıyorum	16	3,3
	Toplam	**479**	**100**

İnternet ve sosyal paylaşım sitelerinde var olmak, kişisel güvenlikten daha önemlidir	Kesinlikle katılmıyorum	183	38,2
	Katılmıyorum	203	42,4
	Kararsızım	57	11,9
	Katılıyorum	26	5,4
	Kesinlikle Katılıyorum	10	2,1
	Toplam	**479**	**100**
Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir	Kesinlikle katılmıyorum	104	21,7
	Katılmıyorum	182	38,0
	Kararsızım	99	20,7
	Katılıyorum	59	12,3
	Kesinlikle Katılıyorum	35	7,3
	Toplam	**479**	**100**
İnternet ve sosyal paylaşım sitelerinde bütün bilgileri tutan; hükûmet, pazarlama şirketleri ve bilgisayar korsanları tarafından kullanılan bir yazılım vardır	Kesinlikle katılmıyorum	104	21,7
	Katılmıyorum	182	38,0
	Kararsızım	99	20,7
	Katılıyorum	59	12,3
	Kesinlikle Katılıyorum	35	7,3
	Toplam	**479**	**100**
Sosyal paylaşım sitelerinde devamlı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olması rahatsız edicidir	Kesinlikle katılmıyorum	13	2,7
	Katılmıyorum	74	15,4
	Kararsızım	338	70,6
	Katılıyorum	54	11,3
	Kesinlikle Katılıyorum	0	0,0
	Toplam	**479**	**100**
Bireylerin çeşitli mekânlarda yer bildirimi yapmaları, sosyalleşmek için faydalıdır	Kesinlikle katılmıyorum	66	13,8
	Katılmıyorum	173	36,1
	Kararsızım	110	23,0
	Katılıyorum	115	24,0
	Kesinlikle Katılıyorum	15	3,1
	Toplam	**479**	**100**

Amaç her ne olursa olsun kişisel veriler izinsiz toplanmamalıdır	Kesinlikle katılmıyorum	12	2,5
	Katılmıyorum	13	2,7
	Kararsızım	16	3,3
	Katılıyorum	105	21,9
	Kesinlikle Katılıyorum	333	69,5
	Toplam	**479**	**100**
Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için her birey mahremiyetinden taviz verebilmelidir	Kesinlikle katılmıyorum	101	21,1
	Katılmıyorum	146	30,5
	Kararsızım	102	21,3
	Katılıyorum	100	20,9
	Kesinlikle Katılıyorum	30	6,3
	Toplam	**479**	**100**
Devlet ve devlete bağlı kurumlar gözetim teknolojilerini sadece toplumun güvenliği için kullanır	Kesinlikle katılmıyorum	143	29,9
	Katılmıyorum	140	29,2
	Kararsızım	79	16,5
	Katılıyorum	71	14,8
	Kesinlikle Katılıyorum	46	9,6
	Toplam	**479**	**100**
Güvenli bir ortam için kişisel alanı daraltmaya razı olunabilir	Kesinlikle katılmıyorum	82	17,1
	Katılmıyorum	124	25,9
	Kararsızım	121	25,3
	Katılıyorum	124	25,9
	Kesinlikle Katılıyorum	28	5,8
	Toplam	**479**	**100**
Güvenlik hedefli de olsa kişisel veriler bireyin haberi olmadan elde ediliyorsa bu mahremiyet ihlalidir	Kesinlikle katılmıyorum	15	3,1
	Katılmıyorum	22	4,6
	Kararsızım	32	6,7
	Katılıyorum	143	29,9
	Kesinlikle Katılıyorum	257	55,7
	Toplam	**479**	**100**

Sosyal paylaşım sitelerindeki profilim kendi kimliğimden farklı bilgiler içermektedir	Kesinlikle katılmıyorum	220	45,9
	Katılmıyorum	183	38,2
	Kararsızım	30	6,3
	Katılıyorum	32	6,7
	Kesinlikle Katılıyorum	30	2,9
	Toplam	**479**	**100**

"İnternet ve sosyal paylaşım siteleri kullanıcısına güvenilir bir iletişim ortamı sağlamaktadır" sorusuna katılımcıların %36,5'i ile 175 kişi ile "katılmıyorum", %34'ü 163 kişi ile "kararsızım", %13,4'ü 64 kişi ile "kesinlikle katılmıyorum", %11,5'i 55 kişi ile "katılıyorum", %4,6'sı 22 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıdaki oranlara göre katılımcıların %49,9'u internet ve sosyal paylaşım sitelerinin güvenilir bir iletişim ortamı sağlamadığını düşünmektedir. Ayrıca kararsız katılımcıların oranı ise %34 ile oldukça fazladır. Katılımcıların küçük bir bölümü %16,1 ile internet ve sosyal paylaşım sitelerinin kullanıcısına güvenilir bir iletişim ortamı sağladığına inanmaktadır.

"İnternet ve sosyal paylaşım ağlarında kendimi daha özgür hissediyorum" sorusuna katılımcıların %42,2'si 202 kişi ile "katılmıyorum", %21,3'ü 102 ile "katılıyorum", %19,8'i 95 kişi ile "kararsızım", %11,7'si 56 kişi ile "kesinlikle katılmıyorum", %5'i 24 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Bu bağlamda katılımcıların %53,9 ile yarısından fazlası internet ve sosyal paylaşım ağlarında daha özgür olduklarını düşünmemektedir. Kararsız kullanıcıların %19,8 oranı ise dikkat çekicidir. Katılımcıların dörtte birlik orandan biraz daha fazlası %26,3 ile internet ve sosyal paylaşım sitelerinin kendilerini daha özgür hissettirdiğine inanmaktadırlar.

"İnternet ve sosyal paylaşım sitelerinde bireylerin mahremiyetleri hükûmetler, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edilmektedir" sorusuna

katılımcıların %36,7'si 176 kişi ile "katılıyorum", %28,2'si 135 kişi ile "kararsızım", %16,7'si 80 kişi ile katılıyorum, %16,1'i 77 kişi ile "kesinlikle katılıyorum", %2,3'ü 11 kişi ile "kesinlikle katılmıyorum" cevabını vermişlerdir. Katılımcıların %52,8 ile yarısından fazlası internet ve sosyal paylaşım sitelerinde mahremiyet ihlali yapıldığını düşünmektedir. Kararsızların %28,2'lik oranı ise katılımcıların yaklaşık dörtte birinin internet ve sosyal paylaşım sitelerinde mahremiyet ihlalleri yapılıp yapılmadığı konusunda emin olmadıklarını göstermektedir. Katılımcıların %19 ile yaklaşık dörtte birlikte kısmı internet ve sosyal paylaşım sitelerinde mahremiyet ihlali yapıldığına katılmamaktadırlar.

"İnternet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bilsem de varlığımı sürdürmeye devam ederim" sorusuna katılımcıların %29,6'sı 142 kişi ile "kararsızım", %27,6'sı 132 ile "katılmıyorum", %25,1'i 120 kişi ile "katılıyorum", %14,4'ü 69 kişi ile "kesinlikle katılmıyorum", %3,3'ü 16 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıdaki verilere göre katılımcıların %42'lik bölümü internet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bildikleri takdirde bu tür ortamlarda varlıklarını devam ettirmeyeceklerini belirtmişlerdir. %28,4'lük kesim ise kişisel güvenliğin ihlal edilmesine rağmen internet ortamında ve sosyal paylaşım sitelerinde var olmaya devam edeceklerini belirtmişledir.

"Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir" sorusuna katılımcıların %38'i 182 kişi ile "katılmıyorum", %21,7'si 104 kişi ile "kesinlikle katılmıyorum", %20,7'si 99 kişi ile "kararsızım", %12,3'ü 59 kişi ile "katılıyorum", %7,3'ü 35 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Bu bağlamda katılımcıların %59,7'luk oranla yarısından fazlası bu tür sitelerde sahte profil kullanmanın gerekli olmadığını düşünmektedir.

Katılımcıların %19,7'lik kısmı ile yaklaşık beşte biri bu tür sitelerde sahte profil kullanmanın daha güvenilir olduğunu düşünmektedir.

"İnternet ve sosyal paylaşım sitelerinde bütün bilgileri tutan; hükûmet, pazarlama şirketleri ve bilgisayar korsanları tarafından kullanılan bir yazılım vardır" sorusuna katılımcıların %43'ü 206 kişi ile "katılıyorum", %30,7'si 147 kişi ile "kesinlikle katılıyorum", %19,2'si 92 kişi ile "kararsızım", %5,2'si 25 kişi ile "katılmıyorum", %1,9'u 9 kişi ile "kesinlikle katılmıyorum" cevabını vermişlerdir. Bu bağlamda katılımcıların %73'7'lik kısmına tekabül eden 353 kişi internet ve sosyal paylaşım sitelerinde devlet, pazarlama şirketleri veya bilgisayar korsanları tarafından kullanılan ve bütün kişisel bilgileri tutmaya yarayan bir casus yazılımın var olduğunu düşünmektedirler. %7,1 çok küçük bir kesim bu tür bir casus yazılımın internet ve sosyal paylaşım sitelerine yerleştirilmediği görüşünü savunmaktadırlar.

"Sosyal paylaşım sitelerinde devamlı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olması rahatsız edicidir" sorusuna katılımcıların %70,6'sı 338 kişi ile "kararsızım", %15,4'ü 74 kişi ile "katılmıyorum", %11,3'ü 54 kişi ile "katılıyorum", %2,7'si 13 kişi ile "kesinlikle katılmıyorum" cevabını vermişlerdir. Bu bağlamda katılımcıların üçte ikisinden fazlasının bu konuda kararsız olduğu görülmektedir. Katılımcıların yalnızca %11,3'lük bir kısmı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olmasının rahatsız edici olduğunu düşünmektedir.

"Bireylerin çeşitli mekânlarda yer bildirimi yapmaları, sosyalleşmek için faydalıdır" sorusuna katılımcıların %36,1'i 173 kişi ile "katılmıyorum", %24'ü 115 kişi ile "katılıyorum", %23'ü 110 kişi ile "kararsızım", %13,8'i 66 kişi ile "kesinlikle katılmıyorum", %3,1'i 15 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Bu bağlamda katılımcıların %49,9 ile

hemen hemen yarısı çeşitli mekânlarda yer bildirimi yapılmasının sosyalleşmek için faydalı olmadığını düşünmektedirler. %27,1'lik kesim ise yer bildirimi yapmanın sosyalleşmek açısından faydalı olduğuna inanmaktadır.

"Amaç her ne olursa olsun kişisel veriler izinsiz toplanmamalıdır" sorusuna katılımcıların %69,5'i 333 kişi ile "kesinlikle katılıyorum", %21,9'u 105 kişi ile "katılıyorum", %3,3'ü 16 kişi ile "kararsızım", %2,7'si 13 kişi ile "katılmıyorum", %2,5'i 12 kişi ile "kesinlikle katılmıyorum" cevabını vermişlerdir. Çalışmamızda detaylı şekilde ele alındığı üzere devlet, pazarlama şirketleri ve bilgisayar korsanları çeşitli veri toplama yöntemleri ve araçları kullanarak kişisel verilerimizi toplamaktadırlar. Devletler bunu gözetim aracılığı ile yapmakta ve bu gözetimin ülkenin terör olayları karşısında bütünlüğünü koruyabilmek ya da olası bir terör olayını önleyebilmek adına yaptıklarını söylemektedirler. Diğer yandan pazarlama ve reklam şirketleri bu verileri pazarlama stratejileri kullanmak ya da veri tabanlı reklam faaliyetleri gerçekleştirmek için toplamaktadırlar. Bu bağlamda yukarıdaki oranlara bakıldığında katılımcıların %91,4 ile hemen hemen hepsi bu tür kişisel veri toplama faaliyetlerine karşı oldukları ortaya çıkmaktadır.

"Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için her birey mahremiyetinden taviz verebilmelidir" sorusuna katılımcıların %30,5'i 146 kişi ile "katılmıyorum", %21,3'ü 102 kişi ile "kararsızım", %21,1'i 101 kişi ile "kesinlikle katılmıyorum", %20,9'u 100 kişi ile "katılıyorum", %6,3'ü 30 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıda da belirttiğimiz üzere hükûmetler gözetim teknolojilerini kullanarak her türlü kişisel verileri toplamakta ve bu da önemli bir mahremiyet ihlaline yol açmaktadır. Katılımcıların %51,1'ine tekabül eden 247 kişi suç oranının yüksek olduğu yerlerde dahi mahremiyetlerinden taviz vermek

istemediklerini belirtmişlerdir. Bunun tam aksini belirtenler ise %27,2'lik kısma tekabül eden 130 kişi, suç oranının yüksek olduğu yerlerde toplumsal güvenlik için bireysel mahremiyetlerinden taviz verebileceklerini söylemişlerdir. %21,3'lük dilime sahip olan kararsızların oranı ise dikkat çekicidir.

"Devlet ve devlete bağlı kurumlar gözetim teknolojilerini sadece toplumun güvenliği için kullanır" sorusuna katılımcıların %29,9'u 143 kişi ile "kesinlikle katılmıyorum", %29,2'si 140 ile "katılmıyorum", %16,5'i 79 kişi ile "kararsızım", %14,8'i 71 kişi ile "katılıyorum", %9,6'sı 46 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıdaki oranlara bakıldığında katılımcıların %59,1'ine tekabül eden ve 283 kişi devlet ve devlete bağlı kurumların gözetim teknolojilerini sadece toplumun güvenliği için kullandığına inanmadıklarını ortaya koymaktadır. %24,4'e tekabül eden 117 kişi ise bunun aksini düşünmektedir.

"Güvenli bir ortam için kişisel alanı daraltmaya razı olunabilir" sorusuna katılımcıların %25,9'u 124 kişi ile "katılmıyorum", yine %25,9'u 124 kişi ile "katılıyorum", %25,3'ü 121 kişi ile "kararsızım", %17,1'i 82 ile "kesinlikle katılmıyorum", %5,8'i 28 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıdaki oranlara göre katılımcıların %43'lük bölümüne tekabül eden 206 kişi güvenli bir ortam için kişisel alanın daraltılmasına katılmadıklarını belirtmişlerdir. %31,7'lik bölüme tekabül eden 152 katılımcı ise bunun tam tersini düşünmekte ve güvenli bir ortam için kişisel alanın daraltılmasına razı olunabileceğini belirtmişlerdir. Katılımcıların %25,3'lük bir bölümü ise bu durum karşısında kararsız olduklarını belirtmişlerdir.

"Güvenlik hedefli de olsa kişisel veriler bireyin haberi olmadan elde ediliyorsa bu mahremiyet ihlalidir" sorusuna katılımcıların %55,7'si 267 kişi ile "kesinlikle katılıyorum", %29,9'u 143 kişi ile "katılıyorum", %6,7'si 32 kişi ile

"kararsızım", %4,6'sı 22 kişi ile "katılmıyorum", %3,1'i 15 kişi ile "kesinlikle katılmıyorum" cevabını vermişlerdir. Yukarıdaki oranlara göre katılımcıların çok büyük bir bölümü %85,8'lik bir oran ile oluşturan 410 kişi güvenlik hedefli de olsa kişisel verilerin bireylerin haberi olmadan toplanmasının mahremiyet ihlali olduğunu düşünmektedir. Bunun tam tersini düşünen %7,7'lik kısım ise çok küçük bir kesimi oluşturmaktadır.

"Sosyal paylaşım sitelerindeki profilim kendi kimliğimden farklı bilgiler içermektedir" sorusuna katılımcıların %45,9'u 220 kişi işe "kesinlikle katılmıyorum", %38,2'si 183 kişi ile "katılmıyorum", %6,7'si 32 kişi ile "katılıyorum", %6,3'ü 30 kişi ile "kararsızım", %2,9'u 14 kişi ile "kesinlikle katılıyorum" cevabını vermişlerdir. Yukarıdaki oranlara göre katılımcıların büyük kesimini oluşturan 403 kişi ile %84,1'lik bölüm sosyal paylaşım ağlarında kullandıkları profillerde kendi kimliklerinden farklı bilgiler içermediğini belirtmişlerdir. Yalnızca 46 kişi ile %9,6 orana sahip bir kesim sosyal paylaşım ağlarındaki profillerinin kendi kimliklerinden farklı bilgiler içerdiğini belirtmişlerdir. Bu soruya katılımcıların verdiği cevaplar "Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir" sorusuna verilen cevaplar ile paralellik göstermektedir. Bu bağlamda birbirine benzer sorularda kullanıcıların tutarlı cevaplar verdikleri ortaya çıkmaktadır.

4.4. Çıkarımsal Analizler

Bu bölümde çalışmamız kapsamında elde edilen verilere çıkarımsal analizler uygulanmış ve analizlerin sonuçları belirtilmiştir.

4.4.1. KMO Testi ve Bartlett Testi

Çalışmamızın örneklem büyüklüğünün Faktör Analizi yapmaya uygun olup olmadığını belirleyebilmek amacıyla KMO Testi ve Pörtlet Testi uygulanmıştır.

Çizelge 4.19. KMO Testi ve Bartlett Testi

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,748
Bartlett's Test of Sphericity	Approx. Chi-Square	2180,550
	df	276
	Sig.	,000

KMO Testinden elde edilen **0,748** değerine göre araştırmamızın örneklem büyüklüğünün Faktör Analizi yapmaya uygun olduğu belirlenmiştir. Faktör Analizi yapılabilmesi için gereken en az değer 0,50'dir. 0,50 ile 0,70 arasındaki değerler orta, 0,70 ile 0,80 arasındaki değerler iyi, 0,80 ile 1,00 arasındaki değerler mükemmel anlamına gelmektedir.

Bartlett testi, özgün korelasyon matrisi ile kimlik matrisinin aynı olup olmadığı hipotezini test eden bir testtir. Bu test "değişkenler arası ilişki var mı yok mu?" sorusuna cevap arar. Bu testte elde ettiğimiz p değeri 0,05'ten küçük olduğundan, korelasyon matrisi ile kimlik matrisi arasında anlamlı bir fark olduğu ortaya çıkmaktadır. Bu da değişkenlerin arasında ilişki olduğundan, benzer değişkenleri bir arada görebilmek amacıyla faktör analizi yapabileceğimizi göstermektedir.

4.4.2. Faktör Analizi

Faktör analizi uygulanarak anket sorularının faktörler altındaki dağılımları belirlenmiştir.

Çizelge 4.20. Faktör analizi

	Component				
	Kullanım Sıklığı	Kişisel Bilgilerin Mahremiyeti	Gözetimin Güvenlik Amaçlı Kullanımı	İnternet Kullanımından Vazgeçme Eğilimi	Çevrimiçi Gizlilik İhlalleri Karşısında Gösterilen Tutum
21. Hangi sıklıkla sosyal paylaşım sitelerini Paylaşım amacıyla (Durum, fotoğraf, video, müzik, vb.) ziyaret ediyorsunuz?	,749				
24. Hangi sıklıkla sosyal paylaşım sitelerini İş amacıyla ziyaret ediyorsunuz?	,619				
22. Hangi sıklıkla sosyal paylaşım sitelerini İletişim amacıyla (Sohbet, beğeni, vb.) ziyaret ediyorsunuz?	,614				
20. Hangi sıklıkla sosyal paylaşım sitelerini Bilgi amacıyla (haber, köşe yazısı vb.) ziyaret ediyorsunuz?	,602				
27. Sosyal paylaşım ağlarında hangi sıklıkta içerik paylaşırsınız?	,597				
25. Hangi sıklıkla sosyal paylaşım sitelerini Yer bildirimi amacıyla ziyaret ediyorsunuz?	,581				
12. Hangi sıklıkla sosyal paylaşım sitelerini ziyaret ediyorsunuz?	,494				

23. Hangi sıklıkla sosyal paylaşım sitelerini Eğlence amacıyla (Oyun, vb.) ziyaret ediyorsunuz?	,449					
39. Amaç her ne olursa olsun kişisel veriler izinsiz toplanmamalıdır		,778				
37. Bireylerin evlerinde yer bildirimi yapmaları, tüm adresin açıkça yer alması sebebiyle, güvenlik açısından doğru değildir		,706				
43. Güvenlik hedefli de olsa kişisel veriler bireyin haberi olmadan elde ediliyorsa bu mahremiyet ihlalidir		,666				
35. İnternet ve sosyal paylaşım sitelerinde bütün bilgileri tutan bir yazılım vardır		,396				
42. Güvenli bir ortam için kişisel alanı daraltmaya razı olunabilir			,686			
41. Devlet ve devlete bağlı kurumlar gözetim teknolojilerini sadece toplumun güvenliği için kullanır			,667			
40. Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için her birey mahremiyetinden taviz verebilmelidir			,614			
36. Sosyal paylaşım sitelerinde devamlı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olması rahatsız edicidir			-,484			

29. İnternet ve sosyal paylaşım siteleri kullanıcısına güvenilir bir iletişim ortamı sağlamaktadır			,363		
31. İnternet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bilsem de varlığını sürdürmeye devam ederim				-,730	
32. İnternet ve sosyal paylaşım sitelerinde var olmak, kişisel güvenlikten daha önemlidir				-,582	
33. İnternet ve sosyal paylaşım ağlarında daha kendimi özgür hissediyorum				-,499	
38. Bireylerin çeşitli mekanlarda yer bildirimi yapmaları, sosyalleşmek için faydalıdır				-,387	
44. Sosyal paylaşım sitelerindeki profilim kendi kimliğimden farklı bilgiler içermektedir					-,736
34. Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir					-,639
30. İnternet ve sosyal paylaşım sitelerinde bireylerin mahremiyetleri ihlal edilmektedir					-,507

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 20 iterations.

Çizelge 4.21. Soruların faktörlere göre dağılımı

FAKTÖR	SORULAR
F1 = Kullanım Sıklığı	21. Hangi sıklıkla sosyal paylaşım sitelerini Paylaşım amacıyla (Durum, fotoğraf, video, müzik, vb.) ziyaret ediyorsunuz?
	24. Hangi sıklıkla sosyal paylaşım sitelerini İş amacıyla ziyaret ediyorsunuz?
	22. Hangi sıklıkla sosyal paylaşım sitelerini İletişim amacıyla (Sohbet, beğeni, vb.) ziyaret ediyorsunuz?
	20. Hangi sıklıkla sosyal paylaşım sitelerini Bilgi amacıyla (haber, köşe yazısı vb.) ziyaret ediyorsunuz?
	27. Sosyal paylaşım ağlarında hangi sıklıkta içerik paylaşırsınız?
	25. Hangi sıklıkla sosyal paylaşım sitelerini Yer bildirimi amacıyla ziyaret ediyorsunuz?
	12. Hangi sıklıkla sosyal paylaşım sitelerini ziyaret ediyorsunuz?
	23. Hangi sıklıkla sosyal paylaşım sitelerini Eğlence amacıyla (Oyun, vb.) ziyaret ediyorsunuz?
F2 = Kişisel Bilgilerin Mahremiyeti	39. Amaç her ne olursa olsun kişisel veriler izinsiz toplanmamalıdır
	37. Bireylerin evlerinde yer bildirimi yapmaları, tüm adresin açıkça yer alması sebebiyle, güvenlik açısından doğru değildir
	43. Güvenlik hedefli de olsa kişisel veriler bireyin haberi olmadan elde ediliyorsa bu mahremiyet ihlalidir
	35. İnternet ve sosyal paylaşım sitelerinde bütün bilgileri tutan; hükûmet, pazarlama şirketleri ve bilgisayar korsanları tarafından kullanılan bir yazılım vardır
	42. Güvenli bir ortam için kişisel alanı daraltmaya razı olunabilir

F3 = Gözetimin Güvenlik Amaçlı Kullanımı	41. Devlet ve devlete bağlı kurumlar gözetim teknolojilerini sadece toplumun güvenliği için kullanır
	40. Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için her birey mahremiyetinden taviz verebilmelidir
	36. Sosyal paylaşım sitelerinde devamlı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olması rahatsız edicidir
	29. İnternet ve sosyal paylaşım siteleri kullanıcısına güvenilir bir iletişim ortamı sağlamaktadır
F4 = İnternet Kullanımından Vazgeçme Eğilimi	31. İnternet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bilsem de varlığını sürdürmeye devam ederim
	32. İnternet ve sosyal paylaşım sitelerinde var olmak, kişisel güvenlikten daha önemlidir
	33. İnternet ve sosyal paylaşım ağlarında daha kendimi özgür hissediyorum
	38. Bireylerin çeşitli mekânlarda yer bildirimi yapmaları, sosyalleşmek için faydalıdır
F5 = Çevrimiçi Gizlilik İhlalleri Karşısında Gösterilen Tutum	44. Sosyal paylaşım sitelerindeki profilim kendi kimliğimden farklı bilgiler içermektedir
	34. Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir
	30. İnternet ve sosyal paylaşım sitelerinde bireylerin mahremiyetleri hükûmetler, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edilmektedir

4.4.3. Normallik testi

Soruların faktörlere göre dağılımı belirlendikten sonra, yapılacak analizlerde hangi testlerin kullanılacağına karar verebilmek için en önemli unsurlardan biri normallik testidir. Verilerin normal dağılıp dağılmadığına bakılarak kullanılacak testler belirlenmektedir.

Tabachnick ve Fidell (2013)'e göre Çarpıklık (skewness) ve Basıklık (kurtosis) katsayıları -1,5 ile +1,5 arasında olduğunda verilerin dağılımı normaldir (Tabachnick ve Fidell, 2013).

Çizelge 4.22. Normallik testine göre verilerin dağılımı

Descriptives

			Statistic	Std. Error
Kullanım_sıklığı	Mean		,0000000	,04569117
	95%Confidence Interval for Mean	Lower Bound	-,0897804	
		Upper Bound	,0897804	
	5%Trimmed Mean		-,0019619	
	Median		,0590309	
	Variance		1,000	
	Std. Deviation		1,00000000	
	Minimum		-2,91976	
	Maximum		3,03724	
	Range		5,95700	
	Interquartile Range		1,31715	
	Skewness		-,026	,112
	Kurtosis		,031	,223

Kişisel_Bilgile-rin_Mahremiyeti	Mean		,0000000	,0456911 7
	95%Confidence Interval for Mean	Lower Bound	-,0897804	
		Upper Bound	,0897804	
	5%Trimmed Mean		,0653958	
	Median		,1973261	
	Variance		1,000	
	Std. Deviation		1,00000000	
	Minimum		-3,93590	
	Maximum		1,65215	
	Range		5,58805	
	Interquartile Range		1,26674	
	Skewness		-1,010	,112
	Kurtosis		1,150	,223
Gözetimin_Güven-lik_Amaçlı_Kulla-nımı	Mean		,0000000	,0456911 7
	95%Confidence Interval for Mean	Lower Bound	-,0897804	
		Upper Bound	,0897804	
	5%Trimmed Mean		-,0242246	
	Median		-,0414956	
	Variance		1,000	
	Std. Deviation		1,00000000	
	Minimum		-2,28455	
	Maximum		3,40880	
	Range		5,69334	
	Interquartile Range		1,28127	
	Skewness		,340	,112
	Kurtosis		,157	,223
İnternet_Kullanı-mından_Vaz-geçme_Eğilimi	Mean		,0000000	,0456911 7
		Lower Bound	-,0897804	

	95%Confidence Interval for Mean	Upper Bound	,0897804	
	5%Trimmed Mean		,0140604	
	Median		,0390940	
	Variance		1,000	
	Std. Deviation		1,00000000	
	Minimum		-3,37713	
	Maximum		2,88609	
	Range		6,26323	
	Interquartile Range		1,26018	
	Skewness		-,235	,112
				,223
	Kurtosis		,365	
Çevrimiçi_Gizli-lik_İhlalleri_Karşı-sında_Göster-i-len_Tutum	Mean		,0000000	,0456911 7
	95%Confidence Interval for Mean	Lower Bound	-,0897804	
		Upper Bound	,0897804	
	5%Trimmed Mean		,0378463	
	Median		,0262841	
	Variance		1,000	
	Std. Deviation		1,00000000	
	Minimum		-3,80481	
	Maximum		2,27192	
	Range		6,07673	
	Interquartile Range		1,21863	
	Skewness		-,558	,112
	Kurtosis		,825	,223

Yukarıdaki çizelgede görüldüğü üzere tüm faktörlerin Çarpıklık ve Basıklık katsayıları belirtilen aralığa (-1,5 ile +1,5) sahip olduğu için, verilerin normal dağılıma sahip oldukları ortaya çıkmaktadır. Bu durum bize, faktörleri incelerken normallik varsayımı isteyen Bağımsız T Testi ve ANOVA kullanabilme imkânını vermektedir.

4.4.4. Fark analizi

Faktör analiziyle oluşturulan faktörlerin sosyo-demografik özelliklere (cinsiyet, yaş, eğitim durumu, gelir durumu, medeni durum) göre farklılık gösterip göstermediğini ortaya koymak amacıyla parametrik testlerden iki bağımsız değişkeni olan demografik bilgiler (cinsiyet ve medeni durum) için Bağımsız T Testi ve ikiden fazla bağımsız değişkeni olan demografik bilgiler (yaş, eğitim durumu, gelir durumu, internete en çok girilen yer) ANOVA (Varyans) analizi uygulanmıştır. Uygulanan bu analizler sonucunda alt araştırma sorularımızın cevapları da ortaya çıkmıştır.

4.4.4.1. Bağımsız T testi

Cinsiyet (erkek, kadın) ve medeni durum (bekâr, evli) olma durumu demografik bilgileri iki değişkenli olduğundan, bu veriler Bağımsız T Testine tabi tutulacaktır.

4.4.4.1.1. Cinsiyet ve faktörler arasındaki fark

İki değişkene (erkek, kadın) sahip cinsiyet özelliği ve soru faktörleri üzerinde Bağımsız T Testi uygulanmıştır. Aşağıdaki çizelgelerde bu testin sonuçları yer almaktadır.

Çizelge 4.23. Cinsiyet Özelliğinin Betimsel İstatistik Çizelgesi

Group Statistics

Cinsiyetiniz			N	Mean	Std. Deviation	Std. Error Mean
Kullanım_sıklığı	dimension1	Erkek	263	-,1609838	1,02144344	,06298490
		Kadın	216	,1960127	,93889688	,06388384
Kişisel_Bilgilerin_Mahremiyeti	dimension1	Erkek	263	-,0010269	1,04450062	,06440667
		Kadın	216	,0012503	,94539820	,06432620
Gözetimin_Güvenlik_Amaçlı_Kullanımı	dimension1	Erkek	263	-,1039672	1,06455565	,06564331
		Kadın	216	,1265897	,90161811	,06134734
İnternet_Kullanımından_Vazgeçme_Eğilimi	dimension1	Erkek	263	-,1226472	1,02487293	,06319637
		Kadın	216	,1493343	,94998509	,06463830
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	dimension1	Erkek	263	-,1873313	1,05492604	,06504953
		Kadın	216	,2280933	,87858537	,05978016

Yukarıdaki çizelge Bağımsız T Testi yapıldığında ortaya çıkan ilk çizelgedir. Bu çizelgeye "betimsel istatistikler" çizelgesi adı verilmektedir. Bu çizelge hangi grupta kaç kişi bulunmaktadır ve her grubun ortalaması ve standart sapmasını göstermeye yarar (istatistik.gen.tr). Bu çizelge çalışmamızın sonraki kısımlarında medeni durum üzerinde uygulanacak Bağımsız T Testi ile yaş, eğitim durumu ve gelir durumu üzerine uygulanacak ANOVA Analizlerinde de ortaya çıkacaktır.

Çizelge 4.24. Cinsiyet Özelliği Üzerinde Uygulanan Bağımsız T Testi

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means			
		F	Sig.	t	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Kullanım_sıklığı	Equal variances assumed	3,785	,052	-3,947	,000	-,35699651	,09045664
	Equal variances not assumed			-3,979	,000	-,35699651	,08971200
Kişisel_Bilgilerin_Mahremiyeti	Equal variances assumed	5,382	,021	-,025	,980	-,00227716	,09192158
	Equal variances not assumed			-,025	,980	-,00227716	,09102790
Gözetimin_Güvenlik_Amaçlı_Kullanımı	Equal variances assumed	7,122	,008	-2,525	,012	-,23055689	,09131346
	Equal variances not assumed			-2,566	,011	-,23055689	,08984732
İnternet_Kullanımından_Vazgeçme_Eğilimi	Equal variances assumed	1,052	,306	-2,986	,003	-,27198145	,09107418
	Equal variances not assumed			-3,009	,003	-,27198145	,09039851
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	Equal variances assumed	4,831	,028	-4,619	,000	-,41542461	,08993214
	Equal variances not assumed			-4,702	,000	-,41542461	,08834653

Gerçekleştirilen Bağımsız T Testine göre Sig (2-Tailed) değerleri 0,05'den düşük olan Kullanım Sıklığı, Gözetimin Güvenlik Amaçlı Kullanımı, İnternet Kullanımından Vazgeçme Eğilimi ve Çevrimiçi Gizlilik İhlalleri Karşısında Gösterilen Tutum faktörlerinde yer alan sorulara verilen cevaplarda cinsiyet unsuruna göre anlamlı bir fark görülmüştür.

Araştırma Soru 1: Katılımcıların cinsiyetleri ile interneti kullanma sıklıkları arasında anlamlı bir fark var mıdır?

Çalışmamız kapsamında uygulanan anketteki 12, 20, 21, 22, 23, 24, 25 ve 27 numaralı sorular katılımcıların internet ve sosyal medya sitelerini hangi sıklıkla ve hangi amaçlarla ziyaret ettiğini ölçümlemek amacıyla sorulmuştur. Bu sorular faktör analizinde gruplandırılmış ve bu faktöre "kullanım sıklığı" faktörü adı verilmiştir.

Uygulanan Bağımsız T Testine göre (çizelge 4.24.) "interneti kullanım sıklığı" faktöründeki "Sig (2 Tailed)" değerinin 0,05'den küçük (0,00) olmasından dolayı interneti kullanma sıklığı ile cinsiyetler arasında anlamlı bir fark olduğu ortaya çıkmıştır.

İnterneti kullanım sıklığı ile cinsiyet özelliği arasında anlamlı bir fark bulunmasından dolayı anlam farkını tespit etmek amacıyla 4.23. numaralı çizelgede "kullanım sıklığı" faktöründeki mean (anlam) sütununa bakılır. Burada 0,1960127 değeriyle kadınların verdikleri cevapların anlam oranının erkeklerin -0,1609838 oranından daha yüksek olduğu gözlemlenmektir. Buna göre anketimize katılan internet kullanıcıları arasında kadınlar, erkeklere oranla interneti ve sosyal paylaşım sitelerini bilgi alma, iletişim, paylaşım, yer bildirimi, eğlence gibi amaçlarla daha çok ziyaret etmekte ve bu platformlarda daha çok içerik paylaşmaktadırlar. 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.

Araştırma Soru 2: Katılımcılarım cinsiyetleri ile yaşanan çevrimiçi gizlilik ihlalleri karşısında internetten vazgeçme eğilimleri arasında anlamlı bir fark var mıdır?

Çalışmamız kapsamında uyguladığımız anketteki 31, 32, 33 ve 38 numaralı sorular katılımcıların internet güvenliği ve çevrimiçi gizlilik alanlarındaki ihlaller karşısında internet kullanımından vazgeçme eğilimlerini ölçümleme amacıyla sorulmuştur. Bu sorular faktör analizi ile gruplandırılmış ve ortaya çıkan faktöre "internet kullanımından vazgeçme eğilimi" faktörü adı verilmiştir.

4.24. numaralı çizelgede yer alan Bağımsız T Testi sonucuna göre çalışmamız kapsamında uygulanan ankete katılan internet kullanıcılarının cinsiyetleri ile kullanıcıların internet üzerinde yaşanan çevrimiçi gizlilik ve internet güvenliği ihlallerine karşı internet kullanımından vazgeçme eğilimleri arasında anlamlı bir fark görülmüştür (Sig. 2-Tailed = 0,003, $p<0,05$)

Anlam farkını tespit etmek için 4.23. numaralı çizelge incelendiğinde "İnternet Kullanımından Vazgeçme Eğilimi" faktörüne ait mean (anlam) değerinin erkeklerde -0,1226472, kadınlarda ise 0,1493343 olmasından ötürü kadınların bu faktör grubunda yer alan sorulara verdiği cevaplarla, erkeklerin verdiği cevaplar arasında anlamlı bir fark bulunmaktadır. Bu bağlamda kadınların verdikleri cevaplar sonucunda çevrimiçi gizlilik ve internet güvenliğiyle ilgili alanlarda yaşananlar ihlaller karşısında kadınların internet kullanımından vazgeçme oranı, erkeklere oranla daha düşüktür. Anketimize katılan 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.

4.4.4.1.2. Medeni Durum ve faktörler arasındaki fark

İki değişkene (bekâr, evli) sahip medeni durum özelliği ve soru faktörleri üzerinde Bağımsız T Testi uygulanmıştır. Aşağıdaki çizelgelerde bu testin sonuçları yer almaktadır.

Çizelge 4.25. Medeni Durum Özelliğinin Betimsel İstatistik Çizelgesi

Group Statistics

	Medeni_Durum		N	Mean	Std. Deviation	Std. Error Mean
Kullanım_sıklığı	dimension1	Bekar	380	,0226961	1,01732205	,05218752
		Evli	99	-,0871165	,93026814	,09349547
Kişisel_Bilgilerin_Mahremiyeti	dimension1	Bekar	380	,0178789	1,00325153	,05146572
		Evli	99	-,0686261	,98945263	,09944373
Gözetimin_Güvenlik_Amaçlı_Kullanımı	dimension1	Bekar	380	-,0047788	,98547438	,05055377
		Evli	99	,0183430	1,05891968	,10642543
İnternet_Kullanımından_Vazgeçme_Eğilimi	dimension1	Bekar	380	-,0048195	1,01193929	,05191139
		Evli	99	,0184992	,95753342	,09623573
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	dimension1	Bekar	380	,0384524	1,02631380	,05264879
		Evli	99	-,1475951	,88105460	,08854932

Çizelge 4.26. Medeni Durum Özelliği Üzerinde Uygulanan Bağımsız T Testi

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means			
		F	Sig.	t	Sig. (2-tailed)	Mean Difference	Std. Error Difference
Kullanım_sıklığı	Equal variances assumed	1,107	,293	,973	,331	,10981261	,11284503
	Equal variances not assumed			1,026	,307	,10981261	,10707446
Kişisel_Bilgilerin_Mahremiyeti	Equal variances assumed	,162	,687	,766	,444	,08650498	,11288753
	Equal variances not assumed			,773	,441	,08650498	,11197221
Gözetimin_Güvenlik_Amaçlı_Kullanımı	Equal variances assumed	2,347	,126	-,205	,838	-,02312178	,11295203
	Equal variances not assumed			-,196	,845	-,02312178	,11782214
İnternet_Kullanımından_Vazgeçme_Eğilimi	Equal variances assumed	1,042	,308	-,206	,837	-,02331868	,11295195
	Equal variances not assumed			-,213	,831	-,02331868	,10934399
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	Equal variances assumed	3,081	,080	1,652	,099	,18604754	,11263533
	Equal variances not assumed			1,806	,073	,18604754	,10301882

Gerçekleştirilen Bağımsız T-Testine göre faktörlerin tümünün Sig (2-Tailed) değerleri 0,05'in üzerinde olduğundan,

katılımcıların medeni durumları ile sorulara yöneltilen cevaplar arasında anlamlı bir fark olmadığı gözlemlenmiştir. Bu bağlamda anlam değerlerinin incelenmesine gerek kalmamıştır.

4.4.4.2. ANOVA (Varyans) analizi

Yaş (14-17, 18-24, 25-34, 35-44, 45 ve üstü), eğitim durumu (ilköğretim, lise, lisans, lisansüstü), gelir durumu (0-999 TL, 1000-2999 TL, 3000-4999 TL, 5000 TL ve üzeri) demografik bilgileri ve internete girilen yer (ev, iş yeri, internet kafe, diğer) ikiden fazla değişkenli olduğundan, bu veriler ANOVA (Varyans) Analizine tabi tutulacaktır.

4.4.4.2.1. Yaş ve faktörler arasındaki fark

İkiden fazla değişkeni bulunan yaş özelliği (14-17, 18-24, 25-34, 35-44, 45 ve üstü) ile soru faktörleri üzerinde ANOVA Analizi uygulanmıştır. Aşağıdaki çizelgelerde bu analizin sonuçları yer almaktadır.

Çizelge 4.27. Yaş Özelliğinin Betimsel İstatistik Çizelgesi

Descriptives

		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
Kullanım_sıklığı	14-17	19	-,2335936	,84076089	,19288378	-1,33862	1,09209
	18-24	169	,0074679	1,03125610	,07932739	-2,50125	2,43800
	25-34	220	,0533039	,95739446	,06454752	-2,91976	3,03724
	35-44	50	-,0976262	,97014397	,13719908	-2,30627	1,98338
	45 ve üstü	21	-,1747303	1,35953956	,29667586	-2,36938	2,76421
	Total	479	,0000000	1,00000000	,04569117	-2,91976	3,03724
	14-17	19	-,1210032	1,17162960	,26879026	-3,15577	1,46510

Kişisel_Bilgilerin_Mahremiyeti	18-24	169	-,0025042	1,06310928	,08177764	-3,93590	1,65215
	25-34	220	,0292224	,93156087	,06280582	-3,46474	1,48622
	35-44	50	-,0534798	,96665156	,13670517	-3,22791	1,58768
	45 ve üstü	21	-,0491754	1,16018520	,25317317	-2,75029	1,28110
	Total	479	,0000000	1,00000000	,04569117	-3,93590	1,65215
Gözetimin_Güvenlik_Amaçlı_Kullanımı	14-17	19	,6483232	,90861151	,20844978	-1,23410	2,05536
	18-24	169	,1436431	,97717025	,07516694	-1,98236	3,06985
	25-34	220	-,1593539	,92900163	,06263328	-2,25010	3,07216
	35-44	50	-,0005160	1,01340806	,14331754	-2,28455	2,19213
	45 ve üstü	21	-,0719129	1,52028058	,33175242	-2,17028	3,40880
	Total	479	,0000000	1,00000000	,04569117	-2,28455	3,40880
İnternet_Kullanımından_Vazgeçme_Eğilimi	14-17	19	,1091911	,78706990	,18056622	-1,74285	1,26036
	18-24	169	-,1237004	,89686680	,06898975	-3,37713	2,27020
	25-34	220	,0854267	1,01302156	,06829790	-2,85107	2,88609
	35-44	50	-,1543711	1,25752937	,17784151	-3,14875	2,29777
	45 ve üstü	21	,3693054	1,02502027	,22367776	-2,31723	2,01882
	Total	479	,0000000	1,00000000	,04569117	-3,37713	2,88609
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	14-17	19	-,4143819	1,35174096	,31011064	-3,80481	1,99452
	18-24	169	,0369327	1,07309589	,08254584	-3,36902	2,27192
	25-34	220	,0647997	,91843024	,06192055	-3,32159	1,98921
	35-44	50	-,0448956	,97337984	,13765670	-2,60968	2,23356
	45 ve üstü	21	-,4942628	,73651651	,16072108	-2,76052	,64481
	Total	479	,0000000	1,00000000	,04569117	-3,80481	2,27192

Çizelge 4.28. Yaş Özelliği Üzerinde Uygulanan ANOVA Analizi

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Kullanım_sıklığı	Between Groups	2,789	4	,697	,695	,595
	Within Groups	475,211	474	1,003		
	Total	478,000	478			
Kişisel_Bilgilerin_Mahremiyeti	Between Groups	,661	4	,165	,164	,956
	Within Groups	477,339	474	1,007		
	Total	478,000	478			
Gözetimin_Güvenlik_Amaçlı_Kullanımı	Between Groups	17,168	4	4,292	4,415	,002
	Within Groups	460,832	474	,972		
	Total	478,000	478			
İnternet_Kullanımından_Vazgeçme_Eğilimi	Between Groups	8,474	4	2,118	2,139	,075
	Within Groups	469,526	474	,991		
	Total	478,000	478			
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	Between Groups	9,648	4	2,412	2,441	,046
	Within Groups	468,352	474	,988		
	Total	478,000	478			

Yaş özelliği üzerinde uygulanan ANOVA Analizine göre "Gözetimin Güvenlik Amaçlı Kullanımı" faktörünün Sig. değeri 0,002, "Çevrimiçi Gizlilik İhlalleri Karşısında Gösterilen

Tutum" faktörünün Sig. değeri ise 0,046'dır. Her iki faktörün de Sig. değerinin 0,05'ten küçük olması nedeniyle bu faktörlerde yer alan sorulara verilen cevaplar arasında anlamlı bir fark bulunmaktadır. Geriye kalan tüm faktörlerin Sig. değerlerinin 0,05'in üstünde olmasından dolayı bu faktörler ile verilen cevaplar arasında anlamlı bir fark yoktur.

Araştırma Sorusu 3: Katılımcıların yaşları ile gözetimin yalnızca güvenlik amaçlı kullanıldığı konusundaki görüş arasında anlamlı bir fark var mıdır?

Günümüzde özellikle ABD'nin başını çektiği bazı ülkelerde iktidardaki hükûmetler çeşitli gözetim sistemlerini kullandıklarını inkâr etmemekle birlikte ve bu gözetim sistemlerini teröre karşı halkın güvenliğini koruma amacıyla kullandıklarını ifade etmektedirler. Biz de bu bağlamda çalışmamız kapsamında uygulanan ankette 29, 36, 40, 41 ve 42 numaralı soruları katılımcıların gözetimin yalnızca güvenlik amaçlı kullanılıp kullanılmadığı konusundaki fikirlerini öğrenmek amacıyla onlara yönelttik. Bu soruları faktör analizinde gruplandırdık ve bu faktöre "gözetimin güvenlik amaçlı kullanımı" ismini verdik.

Önceki sayfada yer alan 4.28. numaralı çizelgedeki yaş özelliği üzerinde uygulanan ANOVA Analizine göre çalışmamız kapsamında gerçekleştirilen ankete katılan internet kullanıcılarının yaşları ile gözetimin yalnızca güvenlik amaçlı kullanıldığı görüşü arasında anlamlı bir ilişki vardır. Önceki sayfada "gözetimin güvenlik amaçlı kullanımı" faktörünün Sig. değerinin 0,002<0,05 olduğunu ve bu sebeple de yaş ile bu faktör arasında anlamlı bir fark bulunduğunu bahsetmiştik. Bu faktörde yer alan sorulara verilen cevaplar ile yaş grupları arasında anlamlı bir fark bulunmasından dolayı 4.27. numaralı çizelgede "gözetimin güvenlik amaçlı kullanımı" faktörü altında yer alan yaş gruplarının incelenmesi gerekir. İncelenen yaş grupları içerinde "14-17 yaş" grubunun mean

(anlam) değerinin 0,6483232 ile diğer yaş gruplarından daha yüksek olduğu görülür. Buna göre "14-17 yaş" grubunda yer alan katılımcılar gözetimin yalnızca güvenlik amaçlı yapıldığına dair görüşe sahiptirler. -0,1593539 anlam değerine sahip "25-34 yaş arası" katılımcılar ise bunun tam tersinde bir görüş benimsemişlerdir.

Yukarıdaki açıklamalara ve sonuca göre gözetimin yalnızca güvenlik amaçlı kullanıldığı konusundaki görüşü katılımcıların yaşlarına göre değişkenlik gösterdiği ortaya çıkmıştır.

4.4.4.2.2. Eğitim durumu ve faktörler arasındaki fark

İkiden fazla değişkeni bulunan eğitim durumu özelliği (ilköğretim, lise, lisans, lisansüstü) ile soru faktörleri üzerinde ANOVA Analizi uygulanmıştır. Aşağıdaki çizelgelerde bu analizin sonuçları yer almaktadır.

Çizelge 4.29. Eğitim Durumu Özelliğinin Betimsel İstatistik Çizelgesi

Descriptives

		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
Kullanım_sıklığı	İlköğretim	13	1,1961993	1,05720257	,29321524	-,50065	3,03724
	Lise	74	-,2072372	1,05979064	,12319816	-2,50125	2,49882
	Lisans	338	,0216876	,94982453	,05166364	-2,91976	2,63207
	Lisans Üstü	54	-,1397308	1,02399789	,13934846	-2,36938	1,91253
	Total	479	,0000000	1,00000000	,04569117	-2,91976	3,03724
Kişisel_Bilgilerin_ Mahremiyeti	İlköğretim	13	-,1164750	,75508331	,20942243	-1,49473	,80459
	Lise	74	-,0144921	,95649497	,11119028	-3,15577	1,49107
	Lisans	338	-,0092718	1,04460993	,05681929	-3,93590	1,65215
	Lisans Üstü	54	,1059345	,82195196	,11185349	-1,86060	1,58768
	Total	479	,0000000	1,00000000	,04569117	-3,93590	1,65215
Gözetimin_Güvenlik_ Amaçlı_Kullanımı	İlköğretim	13	1,7394210	,91677225	,25426687	,79743	3,40880
	Lise	74	,7446816	1,00407667	,11672154	-1,83217	3,07216
	Lisans	338	-,1128538	,85540737	,04652803	-2,28455	2,45520
	Lisans Üstü	54	-,7328580	,80154582	,10907657	-2,17028	1,42552
	Total	479	,0000000	1,00000000	,04569117	-2,28455	3,40880
İnternet_Kullanımından_ Vazgeçme_Eğilimi	İlköğretim	13	-,0608259	1,14898834	,31867203	-2,41496	1,26950
	Lise	74	,0396185	1,06594420	,12391350	-3,14875	2,17169
	Lisans	338	,0251753	,97227573	,05288483	-3,37713	2,88609
	Lisans Üstü	54	-,1972274	1,04755542	,14255424	-2,56934	2,26979
	Total	479	,0000000	1,00000000	,04569117	-3,37713	2,88609
Çevrimiçi_Gizlilik_İhlalleri_	İlköğretim	13	-1,1209851	1,13588668	,31503828	-2,76052	,85971
	Lise	74	-,3314605	1,20436813	,14000495	-3,80481	1,99452

Karşı-sında_Göste-rilen_ Tutum	Lisans	338	,0484323	,91404488	,04971749	-3,00143	2,27192
	Lisans Üstü	54	,4209403	,87142494	,11858591	-1,50734	2,23356
	Total	479	,0000000	1,00000000	,04569117	-3,80481	2,27192

Çizelge 4.30. Eğitim Durumu Özelliği Üzerinde Uygulanan ANOVA Analizi

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Kullanım_sıklığı	Between Groups	22,993	3	7,664	8,001	,000
	Within Groups	455,007	475	,958		
	Total	478,000	478			
Kişisel_Bilgilerin_ Mahremiyeti	Between Groups	,827	3	,276	,274	,844
	Within Groups	477,173	475	1,005		
	Total	478,000	478			
Gözetimin_Güven-lik_Amaçlı_ Kullanımı	Between Groups	113,676	3	37,892	49,403	,000
	Within Groups	364,324	475	,767		
	Total	478,000	478			
İnternet_Kullanımından_ Vazgeçme_Eğilimi	Between Groups	2,479	3	,826	,825	,480
	Within Groups	475,521	475	1,001		
	Total	478,000	478			
Çevrimiçi_Gizlilik_İhlalleri_ Karşısında_Gösterilen_ Tutum	Between Groups	34,827	3	11,609	12,443	,000
	Within Groups	443,173	475	,933		
	Total	478,000	478			

Yukarıdaki çizelgede yer alan ANOVA Analizi sonuçlarına göre eğitim durumu özelliği ile "kullanım sıklığı", "gözetimin güvenlik amaçlı kullanımı" ve "çevrimiçi gizlilik ihlalleri karşısında gösterilen tutum" faktörlerinde yer alan sorulara verilen cevaplar arasında anlamlı bir fark tespit edilmiştir. Anlamlı fark bulunan faktörlerin üstü sarı renkle belirginleştirilmiştir. Belirtilen bu üç faktörün de Sig. değeri 0,05'in altında olmasından dolayı bu faktörlerde yer alan sorulara verilen cevaplar eğitim durumuna göre farklılık göstermiştir.

"Kişisel bilgilerin mahremiyeti" ve "internet kullanımından vazgeçme eğilimi" faktörlerinde yer alan sorulara verilen cevaplar ise bu faktörlerin yapılan ANOVA Analizi sonucu Sig. değerlerinin 0,05'in üstünde çıkmasından dolayı eğitim durumu ile anlamlı bir fark oluşturmamıştır.

Araştırma Soru 4: Katılımcıların eğitim durumları ile çevrimiçi ortamda bulunan kişisel verilerin mahremiyetlerinin ihlal edildiğine dair görüşleri arasında anlamlı bir fark var mıdır?

Çalışmamız kapsamında uygulanan ankette yer alan 35, 37, 39 ve 43 numaralı sorular katılımcılara internet ve sosyal medyada bulunan kişisel bilgilerimizin mahremiyetinin devlet, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edilip edilmediği hakkındaki fikirlerini almak amacıyla yöneltilmiştir. Bu sorular faktör analizi ile gruplandırılmış ve ortaya çıkan faktöre "kişisel bilgilerin mahremiyeti" adı verilmiştir.

Yapılan ANOVA Analizi sonucunda katılımcıların eğitim durumları ile çevrimiçi ortamda bulunan kişisel verilen mahremiyetlerinin ihlal edildiğine dair görüşleri arasında anlamlı bir fark tespit edilememiştir.

Çizelge 4.30.'da yer alan ANOVA Analizi sonucunda göre "kişisel bilgilerin mahremiyeti" faktörüne verilen

cevaplar katılımcıların eğitim durumuna göre farklılık göstermemiştir. Çizelge incelendiğinde bu faktöre ait Sig. değerinin 0,05'in üstünde olduğu görülmektedir. Dolayısıyla anlamlı bir fark yoktur.

Ayrıca Çizelge 4.29.'da yer alan eğitim durumu özelliğinin betimsel istatistik çizelgesi incelendiğinde anlam değerlerinin tüm eğitim gruplarında birbirine yakın olduğu gözlemlenmektedir. Bu bağlamda farklı eğitim grubuna (ilköğretim, lise, lisans ve yüksek lisans) mensup kullanıcılar çevrimiçi ortamda yer alan kişisel verilerinin güvenliğinin ihlal edildiğine inanmaktadırlar. Bu görüşe en çok katılan grup 0,1059345 değerine sahip olan "lisansüstü" mezunu katılımcılarken; en az katılan grup -0,1164750 değer ile "ilköğretim" mezunlarıdır. Arada fark bulunmasına rağmen, ANOVA Analizi sonucundaki Sig. değerinin 0,844 olması, yani 0,05'ten büyük olması nedeniyle anlamlı bir fark yoktur.

4.4.4.2.3. Gelir durumu ve faktörler arasındaki fark

İkiden fazla değişkeni bulunan gelir durumu özelliği (0-999 TL, 1000-2999 TL, 3000-4999 TL, 5000 TL ve üzeri) ile soru faktörleri üzerinde ANOVA Analizi uygulanmıştır. Aşağıdaki çizelgelerde bu analizin sonuçları yer almaktadır.

Çizelge 4.31. Gelir Durumu Özelliğinin Betimsel İstatistik Çizelgesi

Descriptives

		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
Kullanım_sıklığı	0-999	185	-,0850436	,95707541	,07036558	-2,50125	3,03724
	1000-2999	217	,1105095	,97681551	,06631056	-2,91976	2,63207
	3000-4999	62	-,0970393	1,10838384	,14076489	-2,31595	2,49882
	5000 ve üzeri	15	-,1487371	1,29597382	,33461900	-2,36938	2,76421
	Total	479	,0000000	1,00000000	,04569117	-2,91976	3,03724
Kişisel_Bilgilerin_ Mahremiyeti	0-999	185	,0308339	1,02576843	,07541599	-3,93590	1,61869
	1000-2999	217	-,0551712	1,01217406	,06871085	-3,59851	1,49107
	3000-4999	62	,1194383	,92091126	,11695585	-3,46474	1,65215
	5000 ve üzeri	15	-,0758191	,82652500	,21340784	-1,86060	1,48622
	Total	479	,0000000	1,00000000	,04569117	-3,93590	1,65215
Gözetimin_Güvenlik_ Amaçlı_Kullanımı	0-999	185	,1210570	,96598513	,07102064	-1,98236	2,68801
	1000-2999	217	,0254425	,96745910	,06567540	-2,28455	3,06985
	3000-4999	62	-,4326797	1,07276277	,13624101	-2,09404	3,07216
	5000 ve üzeri	15	-,0726945	1,17702730	,30390714	-1,83217	3,40880
	Total	479	,0000000	1,00000000	,04569117	-2,28455	3,40880
İnternet_ Kullanımından_ Vazgeçme_Eğilimi	0-999	185	-,0534290	,88045420	,06473228	-2,41025	2,27020
	1000-2999	217	,1629547	1,04889635	,07120372	-3,37713	2,88609
	3000-4999	62	-,3171330	1,06073290	,13471321	-2,85107	2,26979

	5000 ve üzeri	15	-,3876374	1,01098773	,26103591	-2,31723	1,07496
	Total	479	,0000000	1,00000000	,04569117	-3,37713	2,88609
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	0-999	185	-,1033520	1,06983771	,07865603	-3,36902	1,99452
	1000-2999	217	,0626936	,95786104	,06502384	-3,80481	2,27192
	3000-4999	62	,0941961	,90640910	,11511407	-2,55238	2,23356
	5000 ve üzeri	15	-,0216374	1,05966278	,27360375	-2,76052	1,58322
	Total	479	,0000000	1,00000000	,04569117	-3,80481	2,27192

Çizelge 4.32. Gelir Durumu Özelliği Üzerinde Uygulanan ANOVA Analizi

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Kullanım_sıklığı	Between Groups	4,904	3	1,635	1,641	,179
	Within Groups	473,096	475	,996		
	Total	478,000	478			
Kişisel_Bilgilerin_Mahremiyeti	Between Groups	1,807	3	,602	,601	,615
	Within Groups	476,193	475	1,003		
	Total	478,000	478			
Gözetimin_Güvenlik_Amaçlı_Kullanımı	Between Groups	14,538	3	4,846	4,967	,002
	Within Groups	463,462	475	,976		
	Total	478,000	478			
İnternet_Kullanımından_Vazgeçme_Eğilimi	Between Groups	14,780	3	4,927	5,052	,002
	Within Groups	463,220	475	,975		
	Total	478,000	478			
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_Tutum	Between Groups	3,386	3	1,129	1,130	,337
	Within Groups	474,614	475	,999		
	Total	478,000	478			

Gelir durumu özelliği ile soru faktörleri üzerine ANOVA Analizi uygulanmıştır. Yukarıdaki çizelgelere göre katılımcıların gelir durumu ile "gözetimin güvenlik amaçlı kullanımı" ve "internet kullanımından vazgeçme eğilimi" faktörlerine ait sorulara katılımcıların verdiği cevaplar arasında anlamlı bir fark vardır. Bu iki faktörün de Sig. değerlerinin 0,02 olması; yani 0,05 değerinden daha küçük olması nedeniyle anlamlı fark tespit edilmiştir.

Sig. değerleri 0,05'ten büyük olan "kullanım sıklığı", "kişisel bilgilerin mahremiyeti" ve "çevrimiçi gizlilik ihlalleri karşısında gösterilen tutum" soru faktörleri ve bu faktörlerde yer alan sorulara verilen cevaplar ile katılımcıların gelir durumu arasında anlamlı bir fark söz konusu değildir.

Araştırma Soru 5: Katılımcıların gelir durumu ile gözetimin güvenlik amaçlı kullanıldığı konusundaki görüşleri arasında anlamlı bir fark var mıdır?

Önceden de belirttiğimiz gibi ABD'nin başını çektiği bazı ülkeler gözetim teknolojilerini kullandıklarını inkâr etmemekte; fakat bu teknolojileri yalnızca teröre karşı halkın güvenliğini korumak amacıyla kullandıklarını belirtmektedirler. Anketimize katılan internet ve sosyal medya kullanıcılarının bu fikre katılıp katılmadığını ölçümlemek amacıyla onlara 29, 36, 40, 41 ve 42 numaralı soruları yönelttik. Yine önceden belirttiğimiz gibi bu soruları faktör analizinde gruplandırdık ve bu faktöre "gözetimin güvenlik amaçlı kullanımı" ismini verdik.

Gelir durumu özelliği ile "gözetimin güvenlik amaçlı kullanımı" faktörü üzerinde uygulanan ANOVA Analizi sonucuna göre gözetimin yalnızca güvenlik amaçlı uygulandığıyla ilgili sorulara verilen cevaplar ile katılımcıların gelir durumu arasında anlamlı bir fark bulunmaktadır. Çizelge 4.32.'de bulunan gelir durumu özelliği ile soru faktörleri üzerine uygulanan ANOVA Analizi incelendiğinde "Gözetimin güvenlik

amaçlı kullanımı" soru faktörünün Sig. değeri 0,002'dir, yani bu değer 0,05'in altında olduğundan anlamlı bir fark söz konusudur. Bu bağlamda bu faktör grubunda yer alan sorulara katılımcıların gelir durumlarına göre farklı cevaplar verdikleri ortaya çıkmaktadır.

"Gözetimin güvenlik amaçlı kullanımı" soru faktörü ile farklı gelir grubuna mensup kullanıcıların cevapları arasında anlamlı bir fark bulunmasından dolayı çizelge 4.31.'de bulunan "gelir durumu özelliğinin betimsel istatistik çizelgesi"nin incelenmesi gerekmektedir. Bu çizelgede bulunan "gözetimin güvenlik amaçlı kullanımı" soru faktörünün yer aldığı satırdaki mean (anlam) değerleri incelendiğinde "3000-4999 TL" gelir grubu içinde bulunan katılımcıların cevaplarının -0,4326797'lik değer ile diğer gelir grubunda bulunan katılımcılara oranla anlamlı bir fark gösterdiği gözlemlenmektedir. Bu verilere göre "3000-4999 TL" gelir grubu içinde yer alan katılımcılara göre çevrimiçi ortamda gerçekleştirilen gözetim uygulamalarının yalnızca güvenlik amaçlı kullanıldığına diğer gelir grubunda bulunan kullanıcılara oranla daha az katılmaktadırlar. Bu görüşe en yakın duran diğer gelir grubu -0,0726945 anlam değeri ile aylık geliri "5000 TL ve üzeri" olan katılımcılardır. Gözetimin güvenlik amaçlı kullanımına en az katılan gelir grubu ise 0,1210570 anlam değeri ile aylık geliri 0-999 TL arasında olan katılımcılardır.

Araştırma Soru 6: Katılımcıların gelir durumu ile çevrimiçi gizlilik ihlalleri karşısında internetten vazgeçme eğilimleri arasında anlamlı bir ilişki var mıdır?

Çalışmamız kapsamında uyguladığımız anketteki 31, 32, 33 ve 38 numaralı sorular katılımcıların internet güvenliği ve çevrimiçi gizlilik alanlarında ihlaller karşısında internet kullanımından vazgeçme eğilimlerini ölçümleme amacıyla sorulmuştur. Bu sorular faktör analizi ile gruplandırılmış ve

ortaya çıkan faktöre "internet kullanımından vazgeçme eğilimi" faktörü adı verilmiştir.

Çizelge 4.32.'de gelir durumu ile soru faktörleri üzerinde uygulanan ANOVA Analizi sonuçları yer almaktadır. Bu çizelge incelendiğinde "internet kullanımından vazgeçme" eğilimi soru faktörünün Sig. değerinin 0,002 olduğu gözlemlenmektedir. Söz konusu 0,002 değeri 0,05'ten düşük olduğu için "internet kullanımından vazgeçme eğilimi" soru faktöründe yer alan sorular ile katılımcıların gelir durumu arasında anlamlı bir fark söz konusudur. "İnternetten vazgeçme eğilimi" soru faktöründe yer alan sorulara katılımcılar gelir durumlarına göre farklı cevaplar vermişledir.

Anlamın hangi gelir grupları arasında değişkenlik gösterdiğinin tespit edilmesi için Çizelge 4.31.'de yer alan "Gelir durumu özelliğinin betimsel istatistik çizelgesi" incelenmeli "internet kullanımından vazgeçme eğilimi" soru faktöründeki gelir grupları ve anlam oranı arasındaki farklar dikkate alınmalıdır. Bu bağlamda 0,1629547 anlam değerine sahip 1000-2999 TL gelir durumuna sahip katılımcıların bu soru faktörüne vermiş olduğu cevaplar diğer gelir gruplarına mensup olan katılımcıların verdiği cevaplarla değişkenlik göstermiştir. 1000-2999 TL gelir grubundaki katılımcıların anlam değerinin 0,1629547 ile diğer gelir gruplarından daha yüksek olması nedeniyle bu gelir grubuna mensup katılımcılar internet güvenliği ve çevrimiçi gizlilik alanlarında yaşanan ihlaller karşısında bu ortamlarda var olmaya devam etmeyi, diğer gelir grubundaki katılımcılara oranla daha fazla istemedirler. 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 -0,3876374 anlam değeri ile ayda 5000 TL ve üzeri kazanan katılımcılar

oluşturmaktadır. Bu katılımcılara göre internet ve sosyal medyada var olmak kişisel güvenlikten daha önemli değildir. Bu bağlamda bu katılımcıların internet güvenliği ve çevrimiçi ihlaller karşısında internet kullanımından vazgeçme eğilimi diğer gelir grubundaki katılımcılara oranla daha yüksektir.

4.4.4.2.4. İnternete en sık girilen yer ve faktörler arasındaki fark

İkiden fazla değişkeni bulunan internete en çok girilen yer (ev, işyeri, internet kafe ve diğer) ile soru faktörleri üzerinde ANOVA Analizi uygulanmıştır. Aşağıdaki çizelgelerde bu analizin sonuçları yer almaktadır.

Çizelge 4.33. İnternete En Sık Girilen Yer Betimsel İstatistik Çizelgesi

Descriptives

		N	Mean	Std. Deviation	Std. Error	Minimum	Maximum
Kullanım_sıklığı	Ev	369	-,0674036	,96510477	,05024135	-2,91976	2,43800
	İş yeri	82	,1564554	1,01771527	,11238785	-2,36938	2,63207
	İnternet kafe	2	,2289714	3,58536839	2,53523830	-2,30627	2,76421
	Diğer	26	,4455630	1,08691125	,21316083	-1,99425	3,03724
	Total	479	,0000000	1,00000000	,04569117	-2,91976	3,03724
Kişisel_Bilgilerin_ Mahremiyeti	Ev	369	-,0162099	1,02727533	,05347782	-3,93590	1,61869
	İş yeri	82	,0573069	,83298242	,09198752	-3,22791	1,48622
	İnternet kafe	2	-,4250139	1,24394382	,87960111	-1,30461	,45459
	Diğer	26	,0820122	1,11353755	,21838268	-3,09418	1,65215
	Total	479	,0000000	1,00000000	,04569117	-3,93590	1,65215
Gözetimin_Güvenlik_ Amaçlı_ Kullanımı	Ev	369	-,0468668	,94702782	,04930030	-2,28455	2,68801
	İş yeri	82	,0601240	1,18642115	,13101830	-2,17028	3,07216
	İnternet kafe	2	1,9275731	2,09476461	1,48122226	,44635	3,40880
	Diğer	26	,3272512	,85391388	,16746629	-1,09861	2,45520
	Total	479	,0000000	1,00000000	,04569117	-2,28455	3,40880
İnternet_Kullanımından_ Vazgeçme_Eğilimi	Ev	369	,0201563	,98673756	,05136751	-3,37713	2,88609
	İş yeri	82	,0283505	1,06340376	,11743330	-2,82193	2,17169
	İnternet kafe	2	-1,0445885	1,79979286	1,27264573	-2,31723	,22806
	Diğer	26	-,2951251	,89883070	,17627520	-2,07313	1,06961
	Total	479	,0000000	1,00000000	,04569117	-3,37713	2,88609
Çevrimiçi_Gizlilik_İhlalleri_ Karşısında_Gösterilen_ Tutum	Ev	369	,0429197	,98293513	,05116956	-3,80481	2,27192
	İş yeri	82	-,1864264	,93944915	,10374480	-2,59268	1,53313
	İnternet kafe	2	-1,2023778	2,20354747	1,55814336	-2,76052	,35577
	Diğer	26	,0713207	1,25786978	,24668856	-2,69677	1,80008
	Total	479	,0000000	1,00000000	,04569117	-3,80481	2,27192

Çizelge 4.34. İnternete En Sık Girilen Yer Özelliği Üzerinde Uygulanan ANOVA Analizi

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Kullanım_sıklığı	Between Groups	8,950	3	2,983	3,021	,029
	Within Groups	469,050	475	,987		
	Total	478,000	478			
Kişisel_Bilgilerin_Mahremiyeti	Between Groups	,902	3	,301	,299	,826
	Within Groups	477,098	475	1,004		
	Total	478,000	478			
Gözetimin_Güvenlik_Amaçlı_Kullanımı	Between Groups	11,322	3	3,774	3,841	,010
	Within Groups	466,678	475	,982		
	Total	478,000	478			
İnternet_Kullanımından_Vazgeçme_Eğilimi	Between Groups	4,663	3	1,554	1,560	,198
	Within Groups	473,337	475	,996		
	Total	478,000	478			
Çevrimiçi_Gizlilik_İhlalleri_Karşısında_Gösterilen_ Tutum	Between Groups	6,553	3	2,184	2,201	,087
	Within Groups	471,447	475	,993		
	Total	478,000	478			

İnternete en sık girilen yer ile soru faktörleri üzerinde ANOVA Analizi uygulanmıştır. Yukarıdaki çizelgelere göre katılımcıların internete en sık girdiği yer ile "kullanım sıklığı" ve "gözetimin güvenlik amaçlı kullanımı" faktörlerine ait

sorulara katılımcıların verdiği cevaplar arasında anlamlı bir fark vardır. "Kullanım sıklığı" faktörünün Sig. değeri 0,029, "gözetimin güvenlik amaçlı kullanımı" faktörünün Sig. değeri ise 0,010'dur. Her iki değerin de 0,05'ten küçük olması sebebiyle anlamlı bir fark söz konusudur.

Diğer faktörlerin Sig. değerlerinin 0,05'ten yüksek olmasından dolayı, bu faktörlerde yer alan sorulara katılımcıların verdikleri cevaplar ile internete en sık girilen yer arasında anlamlı bir fark söz konusu değildir.

"Kullanım sıklığı" faktöründeki sorulara verilen cevaplar ile anlamlı farklılık gösteren internete en sık girilen yer 0,4455630'lık değer ile "diğer" grubudur. "Gözetimin güvenlik amaçlı kullanımı" faktörü ile anlamlı farklılık gösteren yer ise -0.468668 anlam değeri ile "ev" grubudur.

5. SONUÇ VE ÖNERİLER

21. yüzyıla girilmesiyle birlikte dünyada ve ülkemizde teknoloji alanında önemli gelişmeler gerçekleşmiştir. Özellikle geniş bant internet bağlantısının ortaya çıkmasıyla internete kullanım ücretleri ucuzlamış ve bunun sonucunda internet kullanımı çok yüksek oranlara ulaşmıştır. Diğer yandan bilgisayar teknolojilerinde yaşanan gelişmeler de bilgisayar fiyatlarının ucuzlamasını sağlamış ve bilgisayar satışlarında önemli artışlar yaşanmıştır. Mobil telefonların akıllılaşmasıyla birlikte internet kullanımı cep telefonlarına da taşınmıştır. Birçok markadan yüzlerce model cep telefonu kısa sürede üretilmeye başlanmış ve düşük fiyatlara rağmen çok iyi performanslar veren cihazlar ortaya çıkmıştır. Akıllı telefonlar sayesinde bireyler bilgisayarların hantallığından kurtulmuşlardır. İnsanlar artık internete ev, iş yeri, internet kafe ve okul gibi sabit mekânlar dışında GSM operatörlerinin kapsama alanlarının bulunduğu her yerden internete bağlanma şansı bulmaya başlamışlardır. Bilişim teknolojilerinde yaşanan evrim yalnızca donanım alanında sınırlı kalmamış; mobil telefonlarda kullanılabilecek Android ve IOS gibi gelişmiş işletim sistemlerinin ortaya çıkmasıyla birlikte mobil telefon yazılımcığının da gelişmesi sayesinde tüm akıllı telefonlar birer küçük bilgisayara dönüşmüştür.

Facebook, Twitter, Instagram ve Google Plus gibi sosyal ağların ortaya çıkması insanlara sosyalleşebilecekleri yeni iletişim ortamları yaratmıştır. Bu sosyal ağlara katılım ve kullanım oranları, internet kullanım oranlarına paralel olarak çok hızlı bir şekilde yükselmiştir. Nitekim günümüzde istatistikler, internet kullanan hemen hemen herkesin bu sosyal

ağların en az birinde bir hesabı bulunduğunu ortaya koymaktadır. İnternet ve sosyal medya kullanımın bu denli yüksek oranlara ulaşmış olması beraberinde internet ortamında inanılmaz büyüklükte bir veri dolaşımını da getirmiştir. İnsanlar internet ve sosyal medya sitelerine üye olduklarında kişisel bilgilerini de bu sitelere girmektedirler. Kişiler kendileriyle ilgili genel ya da özel hemen hemen tüm verilerini bu siteler üzerinde paylaşmakta; hatta bu sitelerde ilgi alanlarını ve beğenileri de belirtmektedirler. Bu verilerin dışında kullanıcılar internet ve sosyal medya sitelerinde kendileriyle ilgili fotoğraf, video, yer bildirimi vb. birçok içeriği de paylaşmaktadırlar.

İnternet ve sosyal medya siteleri üzerinde gidip gelen bu denli büyük veri akışı sonucunda oluşan enformasyon yığınını kontrol etmek ya da sahip olmak isteyen bazı unsurlar birbirleriyle adeta yarışa girmektedir. Devletler ve devletleri yöneten hükûmetler toplumsal denetim amacıyla internet üzerinde çeşitli gözetim faaliyetleri gerçekleştirmektedirler. Bu amaçla internet üzerindeki her türlü kişisel veri devlet kurumları tarafından toplanmakta ve veritabanlarında saklanmaktadır. Daha sonra toplanan bu veriler işlenmekte ve kişilerin profilleri çıkarılmaktadır. Pazarlama şirketleri ise internet üzerindeki kişisel verileri gizli bir şekilde toplayarak bu verileri çevrimiçi davranışsal reklamcılık için kullanmaktadırlar. Diğer yandan bilgisayar korsanları ise çeşitli sahtecilik ve dolandırıcılık işleri için kullanıcıların bilgisayarlarına ve mobil telefonlarına çeşitli teknikler kullanarak sızmakta, kullanıcılara zarar vermektedirler. Böylece internet güvenliği ve çevrimiçi gizliliğimizin sürekli tehdit altında olması kaçınılmazdır.

Çalışmamızda devlet, pazarlama şirketleri ve bilgisayar korsanlarının internet güvenliği ve çevrimiçi alanda gerçekleştirdikleri ihlalleri detaylı olarak ele aldık. Bunu

gerçekleştirirken özellikle bilişim basınında kendine önemli yer edinen ve gündemde uzun süre kalan haberlerden yararlandık. Yaptığımız literatür taramasında sosyal teori içinde gözetim olgusuyla ilgilenmiş olan önemli kuramcıların görüşlerine yer verdik. Gözetim teknolojileri ve kişisel veri toplama araçlarıyla ilgili teknik terimlere, kavramlara bilişim sektörünün uzmanları sayesinde açıklık getirdik.

Ülkemizde yaşanan internet güvenliği ile çevrimiçi gizlilik ihlalleriyle ilgili internet kullanıcılarının kanaatlerini ve farkındalık düzeylerini ortaya koymak amacıyla bir anket çalışması gerçekleştirdik. Anket çalışması sonucunda elde ettiğimiz verilere çeşitli analizler uyguladık ve analizlerden çıkan bulguları yorumladık. Çalışmada örneklem olarak ülkemizde internet sitelerini ve sosyal ağları aktif olarak 14 yaş ve üstü kullanıcıları seçtik.

Çalışmada katılımcıların demografik özellikleri açısından internet güvenliği ve çevrimiçi gizlilik ihlalleri ile ilgili farkındalıkları arasındaki farklılıklar; internet ve sosyal medya sitelerinin demografik özelliklere göre kullanım amacı ve sıklıkları; internet güvenliği ve çevrimiçi gizlilik alanındaki ihlallerin güvenlik hedefli gerçekleştirilmesi karşısında katılımcıların tutumları; ihlallere karşı katılımcıların özgürlük hassasiyetleri; internet ve sosyal medya sitelerinin katılımcılar tarafından ne ölçüde güvenilir buldukları; ihlaller karşısında katılımcıların internet kullanımından vazgeçme eğilimleri analiz edilmiştir.

Çalışmaya ilişkin demografik bulgular şu şekildedir: 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 eğitimli

bireyler olduğu görülmektedir. Katılımcıların %82'si düşük ve orta gelir grubunda yer almıştır. Katılımcıların %79'u ile çoğunluğu bekârdır.

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.

Katılımcıların internet siteleri ve sosyal ağlardaki davranışlarıyla ilgili bulgular şu şekildedir: Bugün internet mobil telefonlar ve tabletler sayesinde hemen hemen her yerde kullanılabilse 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.

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

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 sağdığına 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 bulundurulan bir yazılımın varlığını katılımcıların %74'lük bir bölümü düşünmektedir ve bu oran oldukça yüksek bir orandır.

İktidarı elinde bulunduran 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.

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 ANAVOA 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.

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 içerisindedir. Bireyler medyadan ve diğer kaynaklardan bu gereksinimlerini gidermek için bir takım beklentilere giderler. 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 etmesinden dolayı, anonimdik ve özgürlük karşısında siber âlemde var olmak katılımcılara daha cazip gelmektedir.

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 kavramlar yavan kalmakta, anket çalışmamızda elde ettiğimiz bulgulara göre pek de önemli şeyler ifade etmemektedir.

Çalışmamızda çıkan sonuçların önceki çalışmalarla paralellik gösterdiği söylenebilir. Fakat daha önce de ifade ettiğimiz gibi çalışmamızı diğer çalışmalardan ayıran unsur, bu çalışmada mahremiyet ihlali gerçekleştiren yalnızca tek unsur yerine tüm unsurların aynı çalışmada ele alınmasıdır. Ülkemizde gözetimle ilgili birçok çalışma bulunsa da bilgisayar korsanları ve pazarlama şirketlerinin gerçekleştirdiği mahremiyet ihlalleriyle ilgili çok az çalışma bulunmaktadır. Çalışmamızın bu alanlarda yapılacak yeni çalışmalara farklı bir soluk getireceğini ummaktayız.

Son olarak; devlet, pazarlama şirketleri ve bilgisayar korsanlarının gerçekleştirdikleri internet güvenliği ile çevrimiçi gizlilik ihlallerine karşı internet kullanıcıları asla savunmasız değildir. Kendilerini korumak; daha fazla anonim kalmak isteyen internet ve sosyal medya kullanıcılarına önerilerimiz olacak. Bu öneriler ünlü güvenlik uzmanlarının yazdığı makale ve kitaplardan derlendi. Bu önerileri şu şekilde sıralayabiliriz: Kullandığınız bilgisayar ve cep telefonlarında bir antivirüs yazılımı bulundurmanız sizi virüslere ve bilgisayar korsanlarına karşı koruyacaktır. Windows ve IOS gibi işletim sistemlerine bağımlı kalmaktansa Linux gibi özgür ve açık kaynak kodlu işletim sistemlerine yönelmek, popüler işletim sistemlerindeki açık kapılara maruz kalmayı ortadan kaldıracaktır. Whatsapp gibi popüler sohbet yazılımları yerine Telegram ve Jabber gibi açık kaynak kodlu sohbet yazılımlarının kullanılması kişisel bilgilerin ve sohbetlerin ifşa edilmemesi açısından önemlidir. Hotmail, Gmail ve Yahoo gibi hemen hemen herkesin kullandığı e-posta hesaplarından kaçınılması gerekmektedir. Bu e-posta hesapları yerine gizliliğe daha çok veren e-posta hesaplarını tercih edebilir. Unutulmaması gereken bir şey var ki Gmail ve Hotmail gibi e-posta hesapları Google ve Microsoft'a bağlıdır ve bu şirketler çevrimiçi davranışsal reklamcılık faaliyetleri için kişisel bilgileri toplamaktadırlar. İnternette daha özgürce dolaşmak ve verilerinizi

toplayan hükûmetlere karşı kendinizi korumak istiyorsanız Google Chrome, Internet Explorer, Apple Safari, İnternet Explorer gibi internet tarayıcılarının aksine, çok katmanlı şifrelenmiş bağlantı sunan Tor Browser isimli internet tarayıcısı tercih edilebilir.

Bir diğer hatırlatma ise parola sorunsalı ile ilgilidir. İnternet sitelerinde ve sosyal ağ platformlarında "123456" veya "0000" gibi tahmin edilmesi çok kolay parolalar kullanılmamalıdır. Bu parolalar yerine aynı anda büyük harf, küçük harf, rakam ve özel karakterlerden oluşan uzun parolalar türetilmelidir. Kullanılan bir parola birden çok internet sitesinde, sosyal ağ platformunda ya da eposta hesabında kullanılmamalıdır. Parolalar belirli aralıklarla yenilenmelidir. Gizli soruların cevabını "tuttuğunuz takım" gibi son derece kolay tahmin edilebilecek bir şekilde ayarlamaması kullanıcının lehine olacaktır. Birçok farklı sitede farklı parola ve gizli soru kullanmak elbette kullanıcının kafasını fazlasıyla karıştıracaktır; fakat bu kafa karışıklığı küçük bir not defteri kullanılabilir. Geleneksel yöntemler işe yaramaya devam etmektedir. Yalnız bu not defterinin çaldırılmamasına özen gösterilmelidir. Kullanıcılar ceplerindeki cüzdanı nasıl çaldırmak istemiyorlarsa; parola ve gizli sorularına da aynı muameleyi yapmalıdır.

Akıllı telefonlara ve tabletlere indirilecek yazılımlara dikkat edilmeli ve her türlü sahte uygulamayı indirmekten kaçınılmalıdır. Uygulama izinlerini kontrol edilmelidir. Birçok akıllı telefon uygulamasının içerisinde kişisel verileri toplayan ve veritabanlarına gönderen arka kapılar mevcuttur. En son olarak dünyadaki en zayıf güvenlik unsurunun insan olduğu unutulmamalıdır. Siz siz olun, size bedava şeyler ve promosyonlar sağlayacağını iddia eden insanlardan uzak durun. Toplum mühendisliği dünyanın en kaliteli güvenlik yazılımının bile üstesinden gelemeyeceği kadar güçlü bir

silahtır. Bizi avlamaya çalışan toplum mühendislerine karşı sürekli uyanık olmalı ve çevremizi bu konuda bilinçlendirmeliyiz. Bu konuda bilinçlenmediğimiz takdirde hem kendimizin hem de en yakınlarımızın başı belaya girebilir; dolandırılabilir veya önemi bilgilerimizi çaldırabiliriz.

KAYNAKLAR

Akar, E. (2010). Sanal Toplulukların Bir Türü Olarak Sosyal Ağ Siteleri – Bir Pazarlama İletişimi Kanalı Olarak İşleyişi, *Anadolu Üniversitesi Sosyal Bilimler Dergisi,* 10 (1), 107-122.

Aksoy, H. C. (2008). *Kişisel Verilerin Korunması*, Yayımlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Aksoy, Ş. (2013). *Hasta Haklarında Mahremiyet ve Özel Hayatın Gizliliği*, Yayınlanmamış Yüksek Lisans Tezi, Beykent Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Akyıldız, M. A. (2013). *Siber Güvenlik Açısından Sızma Testlerinin Uygulamalar İle Değerlendirilmesi*, Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü, Isparta, 35.

Alikılıç, Ö. (2011). *Halkla İlişkiler 2.0 Sosyal Medyada Yeni Paydaşlar, Yeni Teknikler*. Ankara: Efil Yayınevi, 13.

Arslan, M. (2013). *Arama Motoru Reklamcılığının Etkinliği Üzerine Bir Araştırma: Google Adwords Uygulaması*, Yayınlanmamış Yüksek Lisans Tezi, Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Mersin, 50.

Başer, A. (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, 36.

Bauman, Z. ve Lyon D. (2013). *Akışkan Gözetim* (çev. Elçin Yılmaz). İstanbul: Ayrıntı Yayınları. (Eserin orijinali 2013 yılında yayımlandı), 66-71.

Bıçakçı, S. (2013). *21. Yüzyılda Siber Güvenlik*. İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 5-11.

Bigo, D. (2006). *Globalized (insecurity): the field and the ban- opticon*. Hong Kong: Hong Kong University Press.

Bozkurt, V. (2000). Gözetim ve İnternet: Özel Yaşamın Sonu mu?, *Birikim Dergisi,* 136, 69.

Brauch, H. G. (2008). Güvenliği Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü, *Uluslararası İlişkiler Dergisi,* 18, 3-5.

Canbek, G. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, *Politeknik Dergisi,* 9 (3), 168.

Chen, A. (2014). Anonymous No More: The Celebrated Hackers Represent the Worst of Techno-utopianism, *The Nation Journal,* 299 (22-23), 20-25.

Corwin, E. H. (2011). Deep Packet Inspection: Shaping the Internet and the Implications on Privacy and Security, *Information Security Journal,* 20 (6), 311-316.

Cox, J. T. and Cline, K. M. (2012). Parsing The Demographic: The Challenge Of Balancing Online Behavioral Advertising and Consumer Considerations, *Journal Of Internet Law,* 3, 3.

Crowley, D. ve Heyer, P. (2010). *İletişim Tarihi: Teknoloji, Kültür, Toplum* (çev. Berkay Ersöz). Ankara: Phoenix Yayınevi. (Eserin orijinali 2007 yılında yayımlandı), 461-462.

Çakar, Y. (2013). *Hacker Sırları 1*. Elektronik Baskı, 6-37.

Dolgun, U. (2005). *Enformasyon Toplumundan Gözetim Toplumuna: 21. Yüzyılda Gözetim, Toplumsal Denetim ve İktidar İlişkileri*. Bursa: Ekin Kitabevi, 27-56.

Elbahadır, E. (2014). *Hacking Interface*. İstanbul: Kodlab Yayın ve Dağıtım, 8-45.

Eriş, U. (2009). *Türkiye'de Kırıcı (Hacker) Kültürü*, Yayımlanmamış Doktora Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Flaherty, D. (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, M. (1992). *Deliliğin Tarihi* (çev. Mehmet Ali Kılıçbay). Ankara: İmge Kitabevi. (Eserin orijinali 1972 yılında yayımlandı), 90.

Foucault, M. (2012). *İktidarın Gözü – Seçme Yazılar 4* (çev. Işık Ergüden). İstanbul: Ayrıntı Yayınları. (Eserin orijinali 1994 yılında yayımlandı), 26-157.

Foucault, M. (2015). *Büyük Kapatılma – Seçme Yazılar 3* (çev. Ferda Keskin ve Işık Ergüden). İstanbul: Ayrıntı Yayınları. (Eserin orijinali 1994 yılında yayımlandı), 11.

Giddens, A. (1995). *A Contemporary Critique of Historical Materialism*. (İkinci Baskı). Amerika Birleşik Devletleri: Stanford University Press, 169.

Göle, N. (2001). *Modern Mahrem*. (Yedinci Baskı). İstanbul: Metis Yayınları, 128.

Haşıloğlu, S. B., Sezgin, M., ve Bardakçı, A. (2008). Hizmet Sektöründeki Veritabanlı Pazarlama Araştırmalarının Değerlendirilmesi, *Karamanoğlu Mehmetbey Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 14, 3.

İnternetsiz ülkenin 'hacker' askerleri. (2014, 21 Aralık). Milliyet Gazetesi.

Kakırman, Y. A. (2012). Sosyal Paylaşım Sitelerinin Dijital Yerlilerin Bilgi Edinme ve Mahremiyet Anlayışına Etkisi, *Bilgi Dünyası,* 13 (2), 529-542.

Kang, H. and McAllister M. P. (2011). Selling You and Your Clicks: Examining the Audience of Google, *TripleC.,* 9 (2), 141-153.

Kara, M. (2013). *Siber Saldırılar – Siber Savaşlar ve Etkileri*, Yayınlanmamış Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul, 11.

Kara, Y. ve Coşkun, A. (2012). Sosyal Ağların Pazarlama Aracı Olarak Kullanımı: Türkiye'deki Hazır Giyim Firmaları Örneği, *Afyon Kocatepe Üniversitesi İktisadi Ve İdari Bilimler Dergisi,* 14 (2), 73-89.

Karakaya, A. (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.

Kazancıoğlu, İ., Üstünoğlu, E. ve Baybars, M. (2012). Tüketicilerin Sosyal Ağ Sitelerindeki Reklamlara Yönelik Tutumlarının Satın Alma Davranışları Üzerine Etkisi: Facebook Örneği, *Uluslararası İktisadi ve İdari İncelemeler Dergisi,* 8, 159-182.

Karlıdağ, M. ve Fidaner, I. B. (2011). *Derin Veri Analizi: İnternet'teki Temel Gözetim Aracı*, 13. Akademik Bilişim Konferansında Sunulmuş Bildiri, İnönü Üniversitesi, Malatya.

Levy, S. (2014). *Hackerlar: Bilgisayar Devriminin Kahramanları* (çev. Emel Aslan). Ankara: ODTÜ Yayıncılık. (Eserin orijinali 2010 yılında yayımlandı), 481.

Maslow. A. H. (1943). *A Theory of Human Motivation. Psychological Review,* 50, 370-396.

Mathiesen, T. (1997). The Viewer Society: Michel Foucault's "Panopticon Revisited", *Theoretical Criminology,* 215.

Mitnick, K. D. ve Simon, W. L. (2015). *Aldatma Sanatı* (çev. Nejat Eralp Tezcan). Ankara: ODTÜ Yayıncılık. (Eserin orijinali 2002 yılında yayımlandı), 85.

Mitnick, K. D. ve Simon, W. L. (2015). *Sızma Sanatı* (çev. Emel Aslan). Ankara: ODTÜ Yayıncılık. (Eserin orijinali 2005 yılında yayımlandı), 257.

NSA Collecting Phone Records of millons of Verizon Customers Daily. (2013, June 6). *The Guardian.*

NSA Collects Millons of Email Address Books Globally. (2013, October 13). *The Washington Post*.

NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. (2013, October 30). The Telegraphy.

Nude Jennifer Lawrence photos leaked by hacker who claims to have 'private pictures of 100 A-listers'. (2013, September 1). The *Washington Post.*

Opm hack: China blamed for massive breach of US government data. (2015, June 5). *The Guardian.*

Öztürk, S. (2012). *Mekân ve İktidar*. Ankara: Phoenix Yayınevi, 138.

Öztürk, S. (2013). Filmlerle Görünürlüğün Dönüşümü: Panoptikon, Süperpanoptikon, Sinoptikon, *İletişim Kuramları ve Araştırmaları Dergisi,* 36, 133-151.

Pekşen, A. (2011). İnternet ve Hacktivizm: Yeni Toplumsal Muhalefet Biçimleri, *İzinsiz Gösteri Serbest Fikir Mecrası,* 299.

Pimenta, E. (2010). *Low Power Society, Continuous Hyperconsumption And The End Of The Medium Class In A Hyperurban Planet*. (Üçüncü Baskı). Londra: Elektronik Baskı, 272.

Singer, P. W. ve Friedman, A. (2015). *Siber Güvenlik ve Siber Savaş* (çev. Ali Atav). Ankara: Buzdağı Yayınevi. (Eserin orijinali 2014 yılında yayımlandı), 28-86.

Sucu, İ. (2011). Gözetim Toplumunun Karşı Ütopya Yüzü: İktidar Güçleri ve Ötekiler, *Atatürk İletişim Dergisi,* 2, 127.

Sweeney, L. (2013). Discrimination in Online Ad Delivery, *Communications of the ACM,* 56 (5), 47-48.

Tabachnick, B. G. and Fidell, L. S. (2013). *Using Multivariate Statistics*. (Sixth Edition). Boston: Pearson.

Tanılır, M. N. (2002). *İnternet Suçları ve Bireysel Mahremiyet*. Ankara: Liberte Yayınları, 42-45.

Tokgöz, C. (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.

Tümurtürkan, M. (2010). Gündelik Hayatın Gözetimi: Panoptik Toplumu, *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar,* 3 (2), 5.

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

Uçkan, Ö. (2014). Dijital aktivizmin sınır boyunda hacktivizm: Anonymous ve Redhack örnekleri. A. Keleş ve Y. Sal. (Editörler). *Hack Kültürü ve Hacktivizm.* İstanbul: Alternatif Bilişim Yayınları, 17.

Vural, Z. B. A. ve Bat, M. (2010). Yeni Bir İletişim Ortamı Olarak Sosyal Medya: Ege Üniversitesi İletişim Fakültesine Yönelik Bir Araştırma, *Journal of Yaşar University,* 20 (5), 3348-3382.

Yalçın, E. (2009). Hizmet Referanslı Güvenlik Anlayışında Meşruiyet ve Hesap Verilebilirlik, *Polis Bilimleri Dergisi,* 6, 3.

Yaylagül, L. (2008). *Kitle İletişim Kuramları: Egemen ve Eleştirel Yaklaşımlar*. Ankara: Dipnot Yayınları, 63.

Yılmaz, S. ve Salcan O. (2008). *Siber Uzay'da Güvenlik ve Türkiye*. İstanbul: Milenyum Yayınları, 35-37.

Yüksel, M. (2003). Modernleşme ve Mahremiyet. *Kültür ve İletişim*, 6 (1), 78.

Zukina, J. (2015). Accountability in a Smoke-Filled Room: The Inadequacy of Self Regulation Within the Internet Behavioral Advertising Industry, *Brooklyn Journal of Coporate, Financial and Commerical Law,* 7 (1), 282.

İnternet: Good, O. S. (August, 2014). PlayStation Network is down; hackers claim they did it. *Polygon Video Game Related News, Culture and Videos,* Web: http://www.polygon.com/2014/8/24/6062499/playstation-network-hack-attack adresinden 1 Eylül 2015'te alınmıştır.

İnternet: ABD'nin internetteki gözü PRISM nedir?. (2013, Haziran). *Terra Medusa Proaktif Bilgi Güvenliği Çözümleri İnternet Sitesinde Yayınlanmış Makale,* Web: http://www.terramedusa.com/abdnin-internetteki-gozu-prism-nedir/ adresinden 13 Ağustos 2015'te alınmıştır.

İnternet: Bayram, M. (Haziran, 2014). DNS Nedir? DNS Değiştirmek Ne İşe Yarar?. *Technopat Teknoloji Portalı*, Web: https://www.technopat.net/2014/06/26/dns-nedir-dns-degistirmek-ne-ise-yarar/ adresinden 22 Ağustos 2015'te alınmıştır.

İnternet: Bekir, E. K. (Ağustos). *TTNET ve Phorm Bizi (Hala) Fişliyor mu?* Web: https://www.facebook.com/notes/efe-kerem-bekir/ttnet-ve-phorm-bizi-hala-fi%C5%9Fliyor-mu/10152704495430786 adresinden 25 Eylül 2015'te alınmıştır.

İnternet: Bicchierai, L. F. (October, 2014). 98,000 Hacked Snapchat Photos and Videos Posted Online. *Mashable Digital Media Portal,* Web: http://mashable.com/2014/10/13/the-snappening-photos-videos-posted/ adresinden 30 Ağustos 2015'te alınmıştır.

İnternet: Bicchierai, L. F. (September, 2013). NSA Becomes Household Name After Snowden Leaks. *Mashable Digital Media Portal,* Web: http://mashable.com/2013/09/04/infographic-shows-how-nsa-became-household-name-after-snowden-leaks/ adresinden 12 Ağustos 2015'te alınmıştır.

İnternet: Clarke, R. (June, 2005). Have We Learnt To Love Big Brother?. *Roger Clarke'ın Kişisel İnternet Sitesinde Yayınlanmış Makale,* Web: http://www.rogerclarke.com/DV/DV2005.html adresinden 6 Ağustos 2015'te alınmıştır.

İnternet: Crecente, Brian. (December, 2014). Obama says Sony shouldn't have pulled The Interview, promises 'response' to North Korea. *Polygon Video Game Related News, Culture and Videos,* Web:

http://www.polygon.com/2014/12/19/7423179/obama-says-sony-shouldnt-have-pulled-the-interview-promises-response adresinden 1 Eylül 2015'te alınmıştır.

İnternet: Çamoğlu, K. (Ocak, 2009). Geçmişten Günümüze Pazarlama Dilleri. *Chip Online Dergisi,* Web: http://www.chip.com.tr/blog/kadircamoglu/Gecmisten-Gunumuze-Programlama-Dilleri_1846.html adresinden 3 Ağustos 2015'te alınmıştır.

İnternet: Edward Snowden kimdir, PRISM nedir?. (2013, Temmuz). *BT Teknoloji ve Haber Portalı,* Web: http://www.btnet.com.tr/84417-edward-snowden-ile-prism-nedir.html adresinden 12 Ağustos 2015'te alınmıştır.

İnternet: Farivar, C. (October, 2013). Yep, the NSA is grabbing your address book, contact lists too. *ARS Technica Technology News and Information Portal,* Web: http://arstechnica.com/tech-policy/2013/10/yep-the-nsa-is-grabbing-your-address-book-contact-lists-too/ adresinden 14 Ağustos 2015'te alınmıştır.

İnternet: Gallagher, R. (May, 2015). NSA Planned to Hijack Google App Store to Hack Smartphones. *The Intercept: A Firstlook Media Publication,* Web: https://firstlook.org/theintercept/2015/05/21/nsa-five-eyes-google-samsung-app-stores-spyware/ adresinden 15 Ağustos 2015'te alınmıştır.

İnternet: Gallagher, S. (May, 2014). Photos of an NSA "upgrade" factory show Cisco router getting implant. *ARS Technica Technology News and Information Portal,* Web: http://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant adresinden 15 Ağustos 2015'te alınmıştır.

İnternet: Gülyaşar, E. (Ağustos, 2014). İnternet üzerindeki her şeyi ABD için toplayan araç: XKeyscore. *BT Teknoloji ve Haber Portalı,* Web: http://www.btnet.com.tr/84750-internet-uzerindeki-her-seyi-abd-icin-toplayan-arac-xkeyscore.html adresinden 13 Ağustos 2015'te alınmıştır.

İnternet: Güngör, A. (Kasım, 2014). HSBC Türkiye Hacklendi!. *Technopat Teknoloji Portalı*, Web: https://www.technopat.net/2014/11/12/hsbc-turkiye-hacklendi/ adresinden 7 Eylül 2015'te alınmıştır.

İnternet: Hamburger, E. (Febuary, 2015). *Why Telegram has become the hottest messaging app in the World.* Web: http://www.theverge.com/2014/2/25/5445864/telegram-messenger-hottest-app-in-the-world adresinden 25 Eylül 2015'te alınmıştır.

İnternet: Jaycox, M. (January, 2014). Polls Continue to Show Majority of Americans Against NSA Spying. *Electronic Frontier Foundation,* Web: https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying adresinden12 Ağustos 2015'te alınmıştır.

İnternet: Keizer, G. (June, 2015). Founder of Kaspersky Lab struggles to come up with reason for attack that makes sense given the risk of discovery. *Computer World Digital Magazine About Computer and Technology Business,* Web: http://www.computerworld.com/article/2934398/cybercrime-hacking/duqu-20-hackers-may-have-cracked-kaspersky-to-recon-research.html/ adresinden 4 Eylül 2015'te alınmıştır.

İnternet: Kemp, S. (January, 2015). Digital, Social and Mobile Worldwide in 2015. *We are Social Digital Marketing Agency,* Web: http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/ adresinden 30 Temmuz 2015'te alınmıştır.

İnternet: Kızılkoyun, Fevzi. (Kasım, 2014). Ankara'da vatandaşların tapu bilgileri çalındı. *Hürriyet Gazetesi,* Web: http://www.hurriyet.com.tr/gundem/27662013.asp adresinden 6 Eylül 2015'te alınmıştır.

İnternet: Knight, D. (April, 2014). Personel Computer History: The First 25 Years. *Low End Mac,* Web: http://lowendmac.com/2014/personal-computer-history-the-first-25-years/ adresinden 3 Ağustos 2015'te alınmıştır.

İnternet: Kuzuloğlu, M. S. (Ekim, 2012). *Nedir bu Phorm meselesi.* Web: http://www.radikal.com.tr/yazarlar/m-serdar-kuzuloglu/nedir-bu-phorm-meselesi-1104210/ adresinden 25 Eylül 2015'te alınmıştır.

İnternet: Malware is not only abour viruses – companies preinstall it all the time, Richard Stallman. *The Guardian*, Web:

http://www.theguardian.com/technology/2015/may/22/malware-viruses-companies-preinstall adresinden 27 Eylül 2015'te alınmıştır.

İnternet: McCormick, R. (December, 2014). Sony threatens Twitter with legal action if it doesn't ban users linking to leaks. *The Verge Technology and Media News,* Web: http://www.theverge.com/2014/12/22/7438287/sony-threatens-twitter-legal-action-ban-users-leaks adresinden 1 Eylül 2015'te alınmıştır.

İnternet: Savov, V. (December, 2014). Sony Pictures hacked: the full story. *The Verge Technology and Media News,* Web: http://www.nbcnews.com/news/world/north-korea-behind-sony-hack-u-s-officials-n270451 adresinden 31 Ağustos 2015'te alınmıştır.

İnternet: Whittaker, Z. (October, 2013). Merkel wasn't alone: NSA tapped calls of 35 world leaders. *ZDnet Business Technology News Website*, Web: http://www.zdnet.com/article/merkel-wasnt-alone-nsa-tapped-calls-of-35-world-leaders adresinden 14 Ağustos 2015'te alınmıştır.

İnternet: Williams, O. (November, 2014). Sony Pictures hacked, entire computer system reportedly unusable. *The Next Web Tech News,* Web: http://thenextweb.com/insider/2014/11/24/sony-pictures-hacked-employee-computers-offline/ adresinden 31 Ağustos 2015'te alınmıştır.

İnternet: Zetter, K. (Febuary, 2015). Gemalto Confirms It Was Hacked But Insists the NSA Didn't Get Its Crypto Keys. *Wired Magazine,* Web: http://www.wired.com/2015/02/gemalto-confirms-hacked-insists-nsa-didnt-get-crypto-keys/ adresinden 14 Ağustos 2015'te alınmıştır.

İnternet: Zetter, K. (Febuary, 2015). Snowden: Spy Agencies 'Screwed All of Us' in Hacking Crypto Keys. *Wired Magazine,* Web: http://www.wired.com/2015/02/snowden-spy-agencies-screwed-us-hacking-crypto-keys/ adresinden 14 Ağustos 2015'te alınmıştır.

İnternet: http://gundem.milliyet.com.tr/-redhack-davasinda-bilirkisi-bulunamadi/gundem/gundemdetay/26.02.2013/1673461/default.htm, 12 Eylül 2015'te alınmıştır.

İnternet: http://bianet.org/bianet/bianet/137088-redhack-orgutunden-yedi-tutuklama, 12 Eylül 2015'te alınmıştır.

İnternet: http://bianet.org/bianet/siyaset/146995-reyhanli-belgelerinobet-saatine-denk-geldi-diye-tutuklandi, 12 Eylül 2015'te alınmıştır.

İnternet: http://bilgicagi.com/memleketce-fisleniyor-muyuz, 16 Ağustos 2015'te alınmıştır.

İnternet: http://bilisimtarihi.com/bilisim-tarihi/, 3 Ağustos 2015'te alınmıştır.

İnternet: http://blog.saklansana.com/vpn-mi-tor-mu-en-anonimi-en-guvenlisi-hangisi/, 28 Eylül 2015'te alınmıştır.

İnternet: http://dictionary.cambridge.org/dictionary/turkish/hacker, 18 Ağustos 2015'te alınmıştır.

İnternet: http://dictionary.cambridge.org/dictionary/turkish/hack, 18 Ağustos 2015'te alınmıştır.

İnternet: http://e-bergi.com/y/c-ve-unix-tarihi, 24 Ağustos 2015'te alınmıştır.

İnternet: http://e-bergi.com/y/Toplum-Muhendisligi, 23 Ağustos 2015'te alınmıştır.

İnternet: http://edition.cnn.com/SPECIALS/1999/mitnick.background/, 25 Ağustos 2015'te alınmıştır.

İnternet: http://en.wikipedia.org/wiki/Internet_privacy, 5 Ağustos 2015'te alınmıştır.

İnternet: http://enphormasyon.org/, 25 Eylül 2015'te alınmıştır.

İnternet: http://home.web.cern.ch/topics/birth-web, 4 Ağustos 2015'te alınmıştır.

İnternet: http://istatistik.gen.tr/t-testi-nin-spss-ile-uygulanmas-ve-yorumlanmas/, 10 Ekim 2015'te alınmıştır.

İnternet: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html, 3 Eylül 2015'te alınmıştır.

İnternet: http://siberbulten.com/strateji-guvenlik/stuxnetin-perde-arkasi-hedef-alinan-iranli-sirketler-1/, 27 Ağustos 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/%C3%96zg%C3%BCr_yaz%C4%B1l%C4%B1m, 27 Eylül 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/Edward_Snowden, 10 Ağustos 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/RedHack, 12 Eylül 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/Richard_Stallman, 27 Eylül 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/Tor_%28anonim_a%C4%9F%29, 27 Eylül 2015'te alınmıştır.

İnternet: http://tr.wikipedia.org/wiki/XMPP, 28 Eylül 2015'te alınmıştır.

İnternet: http://webrazzi.com/2014/12/18/sony-hack/, 31 Ağustos 2015'te alınmıştır.

İnternet: http://www.armaweb.com.tr/internetintarihcesi.htm, 4 Ağustos 2015'te alınmıştır.

İnternet: http://www.bilgiustam.com/dunyanin-ilk-bilgisayari-ve-bilgisayarin-tarihcesi/, 3 Ağustos 2015'te alınmıştır.

İnternet: http://www.businessinsider.com/nude-photo-leak-2014-9, 29 Ağustos 2015'te alınmıştır.

İnternet: http://www.chip.com.tr/haber/vpn-nedir-ne-ise-yarar_45313.html, 26 Eylül 2015'te alınmıştır.

İnternet: http://www.commodore.ca/commodore-products/commodore-pet-the-worlds-first-personal-computer/, 3 Ağustos 2015'te alınmıştır.

İnternet: http://www.cumhuriyet.com.tr/?hn=370420, 12 Eylül 2015'te alınmıştır.

İnternet: http://www.dunyabulteni.net/haber/264686/prizmadan-daha-buyugu-ortaya-cikti-tempora, 13 Ağustos 2015'te alınmıştır.

İnternet: http://www.gazetevatan.com/iste-son-zamanlarin-en-kotu-virusleri-314472-teknoloji/, 26 Ağustos 2015'te alınmıştır.

İnternet: http://www.gnu.org/philosophy/free-sw.tr.html, 27 Eylül 2015'te alınmıştır.

İnternet: http://www.haberler.com/yuz-binlerce-liselinin-bilgileri-internete-sizdi-4959738-haberi/, 5 Eylül 2015'te alınmıştır.

İnternet: http://www.haberturk.com/gundem/haber/797773-red-hack-davasinda-karar, 12 Eylül 2015'te alınmıştır.

İnternet: http://www.hurriyet.com.tr/gundem/23242468.asp, 12 Eylül 2015'te alınmıştır

İnternet: http://www.iphonedo.net/applein-icloud-hack-aciklamasi/, 29 Ağustos 2015'te alınmıştır.

İnternet: http://www.meful.net/bilgisayarin-tarihcesi/, 3 Ağustos 2015'te alınmıştır.

İnternet: http://www.memurlar.net/haber/422457/, 5 Eylül 2015'te alınmıştır.

İnternet: http://www.merriam-webster.com/dictionary/hack, 18 Ağustos 2015'te alınmıştır.

İnternet: http://www.merriam-webster.com/dictionary/hacker, 18 Ağustos 2015'te alınmıştır.

İnternet: http://www.muhasebetr.com/2015-asgari-ucret.html, 15 Temmuz 2015'te alınmıştır.

İnternet: http://www.ntv.com.tr/arsiv/id/25322046/, 11 Eylül 2015'te alınmıştır.

İnternet: http://www.pcworld.com.tr/nasil-yapilir/vpn-nedir-nasil-kullanilir/, 26 Eylül 2015'te alınmıştır.

İnternet: http://www.reuters.com/article/2013/10/29/us-adobe-cyberattack-idUSBRE99S1DJ20131029, 28 Ağustos 2015'te alınmıştır.

İnternet: http://www.siberguvenlik.org.tr/2012/12/siber-savaslar-baslangc.html, 5 Ağustos 2015'te alınmıştır.

İnternet: http://www.sondakika.com/haber/haber-meb-veri-tabaninda-bilgi-hirsizligi-6878336/, 5 Eylül 2015'te alınmıştır.

İnternet: http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=, 2 Ağustos 2015'te alınmıştır.

İnternet: http://www.techopedia.com/definition/24954/internet-privacy, 5 Ağustos 2015'te alınmıştır.

İnternet: http://www.teknokulis.com/Haberler/Guncel/2014/04/11/heartbleed-yuzune-hangi-sifrelerinizi-degistirmeniz-gerekli, 3 Eylül 2015'te alınmıştır.

İnternet: http://www.telegraph.co.uk/news/celebritynews/11067182/Nude-Jennifer-Lawrence-photos-leaked-by-hacker-who-claims-to-have-private-pictures-of-100-A-listers.html, 28 Ağustos 2015'te alınmıştır.

İnternet: http://www.theage.com.au/articles/2004/05/11/1084041382316.html, 25 Ağustos 2015'te alınmıştır.

İnternet: http://www.theverge.com/2014/12/8/7352581/sony-pictures-hacked-storystream, 31 Ağustos 2015'te alınmıştır.

İnternet: http://www.tomshardware.com/reviews/fifteen-greatest-hacking-exploits,1790-12.html, 27 Ağustos 2015'te alınmıştır.

İnternet: http://www.trendmicro.com.tr/guvenlik-istihbarati/arastirma/heartbleed/, 3 Eylül 2015'te alınmıştır.

İnternet: http://www.turk-internet.com/portal/yazigoster.php?yaziid=50153, 4 Eylül 2015'te alınmıştır.

İnternet: http://www.webopedia.com/TERM/K/keylogger.html, 22 Ağustos 2015'te alınmıştır.

İnternet: http://xmpp.org/xmpp-software/clients/, 29 Eylül 2015'te alınmıştır.

İnternet: https://edwardsnowden.com/frequently-asked-questions/, 11 Ağustos 2015'te alınmıştır.

İnternet: https://en.wikipedia.org/wiki/AdWords, 11 Ekim 2015'te alınmıştır.

İnternet: https://en.wikipedia.org/wiki/John_Draper, 24 Ağustos 2015'te alınmıştır.

İnternet: https://en.wikipedia.org/wiki/Phreaking, 21 Ağustos 2015'te alınmıştır.

İnternet: https://fr.wikipedia.org/wiki/Surveillance, 6 Ağustos 2015'te alınmıştır.

İnternet: https://news.spotify.com/tr/2014/05/27/important-notice-to-our-users/, 2 Eylül 2015'te alınmıştır.

İnternet: https://optin.stopwatching.us/, 15 Ağustos 2015'te alınmıştır.

İnternet: https://support.google.com/adsense/answer/9712?hl=tr, 12 Ekim 2015'te alınmıştır.

İnternet: https://tools.ietf.org/html/rfc1392, 20 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/%C3%96rnekleme#Kartopu_.C3.B6rneklemesi, 20 Eylül 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/%C4%B0%C5%9Fletim_sistemi, 3 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Anonymous_%28hacker_grubu%29, 29 Eylül 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Bilgisayar, 3 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Denial-of-service_attack, 22 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Script_kiddie, 21 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Siber, 4 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Watch_Dogs, 9 Ağustos 2015'te alınmıştır.

İnternet: https://tr.wikipedia.org/wiki/Whois, 21 Ağustos 2015'te alınmıştır.

İnternet: https://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-ve-onemsenmeyen-veriler-2.html, 23 Ağustos 2015'te alınmıştır.

İnternet: https://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/guncel-cryptolocker-saldirisina-dikkat.html, 8 Eylül 2015'te alınmıştır.

İnternet: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html, 23 Ağustos 2015'te alınmıştır.

İnternet: https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html, 14 Ağustos 2015'te alınmıştır.

İnternet: https://www.yahoo.com/tech/spotify-hacked-some-and-roid-owners-urged-to-reboot-87002789889.html, 2 Eylül 2015'te alınmıştır.

İnternet: https://yenimedya.wordpress.com/2013/07/23/3001/, 13 Ağustos 2015'te alınmıştır.

EKLER

EK-1 Anket Formu

İnternet Güvenliği ve Çevrimiçi Gizlilik Anketi

Gazi Üniversitesi - Sosyal Bilimler Enstitüsü - Radyo, Televizyon ve Sinema Anabilim Dalı Yüksek Lisans Tezi Araştırması

Doç. Dr. M. Sezai TÜRK danışmanlığında hazırlamakta olduğum Yüksek Lisans tezimin araştırması için oluşturduğum ankete 10 dakikanızı ayırıp, soruları yanıtlamanız çalışmama çok büyük katkı sağlayacaktır.

Lütfen desteğinizi esirgemeyin.

Saygılarımla,

Malik ASLANYÜREK

1. Cinsiyetiniz? *

o Kadın

o Erkek

2. Yaşınız? *

o 14-17

o 18-24

o 25-34

o 35-44

o 45 ve üstü

3. Eğitim Durumu *

o İlköğretim

o Lise

o Lisans

o Lisans Üstü

4. Geliriniz *

o 0-999

o 1000-2999

o 3000-4999

o 5000 ve üzeri

5. Medeni Durum *

o Evli

o Bekâr

6. İnternete en çok nerede giriyorsunuz? *

o Ev

o İş yeri

o İnternet kafe

o Kafe, okul vb. diğer mekânlar

7. İnterneti bilgi almak amacıyla kullanırım *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

8. İnterneti iletişim kurmak amacıyla kullanırım *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

9. İnterneti alışveriş amacıyla kullanırım *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

10. İnterneti bankacılık işlemlerini yapmak amacıyla kullanırım *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

11. İnterneti eğlence (müzik, film, oyun, vb.) amaçlı kullanırım *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

12. Hangi sıklıkla sosyal paylaşım sitelerini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

13. Hangi sıklıkla FACEBOOK sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

14. Hangi sıklıkla TWITTER sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

15. Hangi sıklıkla LINKEDIN sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

16. Hangi sıklıkla GOOGLE PLUS sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

17. Hangi sıklıkla INSTAGRAM sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

18. Hangi sıklıkla PINTEREST sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

19. Hangi sıklıkla FOURSQUARE sosyal paylaşım sitesini ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

20. Hangi sıklıkla sosyal paylaşım sitelerini Bilgi amacıyla (haber, köşe yazısı vb.) ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

21. Hangi sıklıkla sosyal paylaşım sitelerini Paylaşım amacıyla (Durum, fotoğraf, video, müzik, vb.) ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

22. Hangi sıklıkla sosyal paylaşım sitelerini İletişim amacıyla (Sohbet, beğeni, vb.) ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

23. Hangi sıklıkla sosyal paylaşım sitelerini Eğlence amacıyla (Oyun, vb.) ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

24. Hangi sıklıkla sosyal paylaşım sitelerini İş amacıyla ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

25. Hangi sıklıkla sosyal paylaşım sitelerini Yer bildirimi amacıyla ziyaret ediyorsunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

26. İnternet siteleri ve sosyal paylaşım ağlarına kayıt olurken kullanım şartları ve gizlilik politikasını okur musunuz? *

o Her zaman

o Sıkça

o Arada sırada

o Nadiren

o Hiçbir zaman

27. Sosyal paylaşım ağlarında hangi sıklıkta içerik paylaşırsınız? *

o Her gün

o Gün aşırı

o Üç günde bir

o Haftada bir

o Bir haftadan daha fazla

28. Sosyal paylaşım ağlarında bilginiz dışında sizinle ilgili ne tür içeriklerin yer alması sizi rahatsız eder? *

o Fotoğraf

o Video

o Yer bildirimi

o Durum bildirimi

o Ayarlarım bir başkasının benimle ilgili herhangi bir içerik paylaşılmasına kapalı durumdadır

29. İnternet ve sosyal paylaşım siteleri kullanıcısına güvenilir bir iletişim ortamı sağlamaktadır *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

30. İnternet ve sosyal paylaşım sitelerinde bireylerin mahremiyetleri hükûmetler, pazarlama şirketleri ve bilgisayar korsanları tarafından ihlal edilmektedir*

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

31. İnternet ve sosyal paylaşım sitelerinde kişisel güvenliğin ihlal edildiğini bilsem de varlığını sürdürmeye devam ederim *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

32. İnternet ve sosyal paylaşım sitelerinde var olmak, kişisel güvenlikten daha önemlidir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

33. İnternet ve sosyal paylaşım ağlarında daha kendimi özgür hissediyorum *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

34. Sosyal paylaşım sitelerinde gerçek profil yerine sahte profil oluşturmak daha güvenilirdir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

35. İnternet ve sosyal paylaşım sitelerinde bütün bilgileri tutan; hükûmet, pazarlama şirketleri ve bilgisayar korsanları tarafından kullanılan bir yazılım vardır*

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

36. Sosyal paylaşım sitelerinde devamlı yer bildirimi yapıldığında çevrenin bu bilgiye sahip olması rahatsız edicidir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

37. Bireylerin evlerinde yer bildirimi yapmaları, tüm adresin açıkça yer alması sebebiyle, güvenlik açısından doğru değildir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

38. Bireylerin çeşitli mekânlarda yer bildirimi yapmaları, sosyalleşmek için faydalıdır *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

39. Amaç her ne olursa olsun kişisel veriler izinsiz toplanmamalıdır *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

40. Suç oranının yüksek olduğu yerlerde toplumsal güvenlik için her birey mahremiyetinden taviz verebilmelidir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

41. Devlet ve devlete bağlı kurumlar gözetim teknolojilerini sadece toplumun güvenliği için kullanır *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

42. Güvenli bir ortam için kişisel alanı daraltmaya razı olunabilir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

43. Güvenlik hedefli de olsa kişisel veriler bireyin haberi olmadan elde ediliyorsa bu mahremiyet ihlalidir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum

44. Sosyal paylaşım sitelerindeki profilim kendi kimliğimden farklı bilgiler içermektedir *

o Kesinlikle katılıyorum

o Katılıyorum

o Kararsızım

o Katılmıyorum

o Kesinlikle katılmıyorum