AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Ömür TALAY

# MOBİL ORTAM REKLAMLARINDA DİJİTAL GÖZETİM ALGISI: DİJİTAL GÖÇMENLER VE DİJİTAL YERLİLERİN KARŞILAŞTIRMALI ANALİZİ

Halkla İlişkiler ve Tanıtım Ana Bilim Dalı
Yüksek Lisans Tezi

Antalya, 2018

AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

Ömür TALAY

# MOBİL ORTAM REKLAMLARINDA DİJİTAL GÖZETİM ALGISI: DİJİTAL GÖÇMENLER VE DİJİTAL YERLİLERİN KARŞILAŞTIRMALI ANALİZİ

Danışman
Doç. Dr. Merih TAŞKAYA

Halkla İlişkiler ve Tanıtım Ana Bilim Dalı
Yüksek Lisans Tezi

Antalya, 2018

**Akdeniz Üniversitesi**

**Sosyal Bilimler Enstitüsü Müdürlüğüne,**

Ömür TALAY'ın bu çalışması, jürimiz tarafından Halkla İlişkiler ve Tanıtım Ana Bilim Dalı Yüksek Lisans Programı tezi olarak kabul edilmiştir.

| | | |
|---|---|---|
| Başkan | : Doç.Dr. Burak ÖZÇETİN | (İmza) |
| Üye (Danışmanı) | : Doç.Dr. Merih TAŞKAYA | (İmza) |
| Üye | : Dr. Öğr. Üyesi Murad KARADUMAN | (İmza) |

| | |
|---|---|
| Tez Başlığı: | Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi |

Onay : Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

Tez Savunma Tarihi : 27/06/2018
Mezuniyet Tarihi : 09/07/2018

(İmza)
Prof. Dr. İhsan BULUT
Müdür

## AKADEMİK BEYAN

Yüksek Lisans Tezi olarak sunduğum “Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımca yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

**Ömür TALAY**

**T.C.**
**AKDENİZ ÜNİVERSİTESİ**
**SOSYAL BİLİMLER ENSTİTÜSÜ**
**TEZ ÇALIŞMASI ORİJİNALLİK RAPORU**
**BEYAN BELGESİ**

**SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE**

| **ÖĞRENCİ BİLGİLERİ** | |
|---|---|
| **Adı-Soyadı** | **Ömür TALAY** |
| **Öğrenci Numarası** | **20155220003** |
| **Enstitü Ana Bilim Dalı** | **Halkla İlişkiler ve Tanıtım** |
| **Programı** | **Tezli Yüksek Lisans** |
| **Programın Türü** | **(X) Tezli Yüksek Lisans ( ) Doktora ( ) Tezsiz Yüksek Lisans** |
| **Danışmanının Unvanı, Adı-Soyadı** | **Doç. Dr. Merih TAŞKAYA** |
| **Tez Başlığı** | **Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi** |
| **Turnitin Ödev Numarası** | **980360205** |

Yukarıda başlığı belirtilen tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 139 sayfalık kısmına ilişkin olarak, 04/07/2018 tarihinde tarafımdan Turnitin adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nda belirlenen filtrelemeler uygulanarak alınmış olan ve ekte sunulan rapora göre, tezin/dönem projesinin benzerlik oranı;

alıntılar hariç % 12

alıntılar dahil % 17'dir.

Danışman tarafından uygun olan seçenek işaretlenmelidir:

( ) Benzerlik oranları belirlenen limitleri aşmıyor ise;
Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylarım.

( ) Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise;

Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporu'nun doğruluğunu onaylar ve Uygulama Esasları'nda öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.

**Gerekçe:**

Benzerlik taraması yukarıda verilen ölçütlerin ışığı altında tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim.

04/07/2018
(imza)
Doç. Dr. Merih TAŞKAYA

# İ Ç İ N D E K İ L E R

## İKİNCİ BÖLÜM
## REKLAMA KRİTİK GÜNCELLEME: KİŞİSELLEŞTİRİLMİŞ REKLAMLAR VE MOBİL ORTAM REKLAMLARINDA DİJİTAL GÖZETİM



## ÜÇÜNCÜ BÖLÜM
## DİJİTAL GÖÇMENLER VE DİJİTAL YERLİLERİN KARŞILAŞTIRMALI ANALİZİ

# TABLOLAR LİSTESİ

# KISALTMALAR LİSTESİ

| | |
|---|---|
| AB: | Avrupa Birliği |
| ABD: | Amerika Birleşik Devletleri |
| AK: | Avrupa Konseyi |
| AP: | Avrupa Parlamentosu |
| API: | Application Programming Interface (Uygulama Programlama Arayüzü) |
| BM: | Birleşmiş Milletler |
| BİMER: | Başbakanlık İletişim Merkezi |
| ÇDR: | Çevrimiçi Davranışsal Reklam |
| DPI: | Deep Packet Inspection (Derin Veri Analizi) |
| GPS: | Global Positioning System (Küresel Konumlama Sistemi) |
| IDS: | Internet Detection System (Kötü Amaçlı Saldırıları Tespit Sistemi) |
| IMEI: | International Mobile Equipment Identity (Uluslararası Mobil Cihaz Kodu) |
| IP: | Internet Protocol Address (İnternet Protokol Adresi) |
| ISP: | Internet Service Provider (İnternet Servis Sağlayıcı) |
| KVKK: | Kişisel Verileri Koruma Kanunu |
| OECD: | Ekonomik İşbirliği ve Kalkınma Teşkilatı |
| OEEC: | Avrupa Ekonomik İşbirliği Teşkilatı |
| SGK: | Sosyal Güvenlik Kurumu |
| SIM: | Subscriber Identity Module (Abone Kimlik Modülü) |
| TBD: | Türkiye Bilişim Derneği |
| TCK: | Türk Ceza Kanunu |
| TDK: | Türk Dil Kurumu |
| URL: | Uniform Resource Locator |
| Vb.: | Ve Benzeri |
| Vd.: | Ve Diğerleri |
| VPN: | Virtual Private Network (Sanal Özel Ağ) |
| WI-FI: | Kablosuz Ağ Bağlantısı |
| WWW: | World Wide Web |
| 2FA: | Two Factor Authentication (İki Faktörlü Doğrulama) |

# ÖZET

Bilgi ve iletişim teknolojilerindeki gelişmelerin insan hayatını hızla değişime uğratması, reklamcılık alanında da kanal, yöntem, strateji açısından araçsal ve içeriksel dönüşüme neden olmuştur. Özellikle dijital iletişim uygulamaları geniş kitlelere ulaşmış ve buna bağlı olarak dijital reklam da hareket alanını genişletmiştir. Dijital ortam ve araçların insan hayatına yaygın biçimde dahil oluşu, dijital bir kültür oluşması sonucunu doğurmuştur. Dijital teknolojiler kültürü dönüştürürken, gözetimi de dijitalleştirip kültürel bir form haline getirmiştir. Bunun ötesinde gözetimin dijitalleşmesi, yönetsel ve tecimsel alanlarda, mahremiyetin göz ardı edildiği çok sayıda vakanın ortaya çıkmasının zeminini hazırlamıştır.

Şirketlerin ya da reklam verenlerin, kullanıcıların internette geçirdikleri zamanlarda bıraktığı dijital izlerle ya da çeşitli mobil uygulamalarca sızdırılan kişisel verileri kullanarak müşteri profili oluşturması ve kullanıcıların mobil ortamlarda ilgilendikleri konuların belirlenmesiyle yaratılan "kişiselleştirme", etik sorunları ve mahremiyet endişelerini beraberinde getirmektedir.

Kişiselleştirme sürecinde/sonrasında elde edilen kişisel verilerin, kişinin rızası ya da bilgisi dışında kullanımının yaratabileceği etik ve mahremiyet ihlallerine ilişkin farkındalığın dijital göçmenlere ve dijital yerlilere göre farklılık gösterdiği halde aynı yasal koruyuculuk çerçevesinde bulunmaları çalışmamız kapsamında araştırma sorunsalı olarak oluşturulmuştur.

Araştırmanın amacı, özel hayatın gizliliği temelinde, dijital gözetim ve dijital iz takibinin yol açabileceği mahremiyet ihlalleri ve bu bağlamdaki etik sorunlara ilişkin farkındalık düzeyinin kuşaklar arası farklılığının yol açabileceği sorunlara bilimsel yöntemlerle işaret etmek ve çözüm önerileri sunmaktır. Bu amacı gerçekleştirmek için, dijital göçmen ve dijital yerlilerin dijital gözetime ilişkin farkındalık ve algıları, mobil ortamlarda yayınlanan reklamların izlenme, fark edilme, kullanılma durumları ve mobil ortam reklamlarında gözetim olgusu kapsamında yüz yüze anket tekniği ile elde edilen verilerden hareketle, karşılaştırmalı olarak analiz edilip değerlendirilmiştir.

**Anahtar Kelimeler:** Mobil Reklam, Dijital Gözetim, Veri Gözetimi, Dijital Göçmenler, Dijital Yerliler.

## SUMMARY

## AWARENESS OF SURVEILLANCE THROUGH MOBILE MEDIA ADS: A COMPARATIVE ANALYSIS OF DIGITAL NATIVES AND DIGITAL IMMIGRANTS

Developments in information and communication technologies have rapidly changed human life, and this has also led to instrumental and content-related transformations in terms of channel, method, and strategies in the field of advertising. Especially digital communication applications have reached great masses, and digital advertising has expanded its playground accordingly. The inclusion of digital media and tools in human life has led to the formation of a digital culture. Digital technologies are transforming the culture, he has won the digitalized surveillance and oversight has become a cultural forms. Furthermore, the digitalization of surveillance has paved the way for the occurrence of a multitude of cases, in which privacy is ignored in administrative and commercial areas.

The "personalized database customer profile" that companies or advertisers create by following the digital footprints that users leave on the Internet, and the "personalization" they create by identifying what users are interested in on the mobile environment bring about ethical issues and privacy concerns.

While digital migrants and digital natives differ in terms of the level of awareness of ethical and privacy violations resulting from the use of personal data obtained during the personalization process without the knowledge and consent of the person being tracked, the fact that both digital migrants and digital natives are within the scope of the same legal security is identified as the problematic of this study.

The aim of this research is to point out the privacy violations that the digital surveillance and the tracking of digital footprints can cause on the basis of the right of privacy, and the problems that may arise from the differences of the generations in terms of their level of awareness of the ethical problems accordingly by scientific methods, and to propose solutions. In order to achieve this goal, awareness and perceptions of digital immigrants and digital natives about digital surveillance, within the framework of ad-views, ad awareness, ad usage and the phenomenon of surveillance on mobile settings, have been analyzed and evaluated comparatively on the basis of face-to-face survey data.


**Keywords:** Mobile Advertising, Digital Surveillance, Data Surveillance, Digital Immigrant, Digital Native.

# ÖNSÖZ

Bilgi iletişim teknolojileri gündelik hayatın hemen her alanında var olarak, kişilerin dünyasında oldukça merkezi bir noktada konumlandırılmış durumdadır. Dijital dünya ise giderek genişlemekte, kişiler de bu dünyada hızla yerlerini almaktadır. Dijitalleşmenin insan hayatında yarattığı dönüşümle birlikte artan hareketlilik, mobil cihazları kişisel bir alana dönüştürürken, mobil ortamları da en gözde reklam ortamı haline getirmiştir. Şirketlerin her an kişilerin yanında olan bu kişisel alanla ilgilenmesi de beklenen bir sonuçtur. Mobil ortam reklamlarındaki kişiselleştirmenin en önemli ham maddesi olan kişisel veriler ise kilit bir noktada durmakta, bu alandaki ciddi reklam gelirleri kişisel verileri daha da cazip hale getirmektedir. Böylelikle kişisel veriler şirketler için çok daha önem kazanmakta, reklam verenler için de daha fazla arzulanan bir değer biçimini almaktadır.

Bu bağlamda günümüzde gözetim daha çok internet tabanlı teknolojiler aracılığıyla gerçekleşir olmuştur. Geleneksel internet teknolojilerinin yerini alan mobil teknolojiler, bu ortamlardaki gözetimi de daha yoğun ve etkin hale getirmiştir. Kişisel verilerin şirketler ve reklam verenler tarafından elde edilme çabası da mobil ortamlarda gerçekleşen dijital gözetim ve dijital iz takibinin yaygınlaşmasıyla sonuçlanmıştır. Kişiler, mobil ortamlarda özel alanlarını korumakta güçlük çekmekte, özel hayatın gizliliği yitirilmekte, mahrem bilgiler daha şeffaf hale gelmektedir.

Bu duruma paralel olarak kişisel verilerin korunmasıyla ilgili ulusal ve uluslararası düzeyde birçok düzenleme yapılmış ve yapılmaya devam etmektedir. Çalışmanın ilerleyen bölümlerinde değinilecek olan bu düzenlemelerin kişilerin özel hayatındaki gizliliği ve mahremiyeti ne kadar koruduğu ise tartışmalıdır. Veri gözetimine ilişkin düzenlemeler şirketler ve reklam verenlerin lehine; kişilerin aleyhine gelişmektedir. Bu alandaki yasal düzenlemeler ve devletin koruyucu gücünün kişilerin lehine olması beklenirken, şirketlere tanınan ayrıcalıklarla birlikte bu düzenlemeler kişilerin aleyhine konumlanmakta ve böylelikle devletin koruyuculuğunu gölgede bırakmaktadır.

Mobil ortamlar ve mobil ortam reklamlarında gerçekleşen dijital gözetimin kişiler tarafından nasıl algılandığının araştırıldığı bu çalışmada konuya internet kullanıcıları perspektifinden yaklaşılmış olması çalışmayı önemli kılmaktadır. Bununla beraber dijital gözetime ilişkin farkındalık düzeyinde yaşanan farklılığın kuşaklar temelinde değerlendirilmesi, dijital haklar ve yasal düzenlemeler konusunda bilgi sahibi olma durumlarının yine kuşaklar arası karşılaştırma ile ortaya konması, alana özgü yapılacak sonraki çalışmalara da katkıda bulunacaktır. Tüm bunların bilimsel yöntemler eşliğinde açığa

çıkarılması ile birlikte kişilerin özel hayatını ve mahremiyetini koruma iddiasında bulunan yasal düzenleme ve koruyucu mekanizmalar sorgulanabilecek, kişilerin lehine olabilecek çözüm önerileri getirilebilecektir.

**Ömür TALAY**

**Antalya, 2018**

# GİRİŞ

Bilgi ve iletişim teknolojilerindeki gelişmelerin insan hayatını hızla değişime uğratması, reklamcılık alanında da kanal, yöntem ve strateji açısından araçsal ve içeriksel dönüşüme neden olmuştur. Bu dönüşüm, reklam verenin hedef kitleye ulaşmasını kolaylaştırıcı olanaklar sunduğu ticari alanda geniş kabul görmekte, reklam içeriği ve hedef kitle buluşmasını daha steril hale getirmeye yönelik teknolojik uygulamalar ve yazılımların gelişmesi de ivme kazanmaktadır. İnternetin yükselişi ile birlikte teknolojik araçlar adeta gündelik yaşamın önemli bir parçası haline gelmiş, bilgiye erişimi hızlı ve ulaşılabilir kılmış, zaman ve mekan sınırlarını inceltmiştir. Kişiler zamanla pasif okuyucu-dinleyici olmaktan çıkmış, aktif kullanıcı hatta içerik yaratıcısı haline dönüşerek neredeyse hayatın her alanında dijital ortamlarda vakit geçirmeye başlamıştır.

Dijital dünya; dijital ortam ve dijital ortam araçlarının etkin kullanımıyla beraber giderek zenginleşmektedir. İletişim biçimlerinin çeşitlenmesiyle beraber tüm iletişim ortamları dijital bir üst metinde birleşmiş, etkileşimli çoklu medyanın ciddi derecede gelişmesini sağlamıştır (Castells, 2008: 401). Dijital iletişim uygulamaları ise geniş kitlelere ulaşmış ve buna bağlı olarak dijital reklam da hareket alanını genişletmiştir. Dijital ortamın gücünün farkında olan şirketler müşterilerine dijital olarak ulaşmayı zorunlu görmenin yanı sıra daha hızlı ve daha az maliyetli olduğu için dijital reklamı tercih etmektedir. Dijital ortam ve araçların kullanımı da, dijital bir kültür oluşması sonucunu doğurmaktadır.

> Dijital kültür, dijital medya araçlarıyla meydana getirilen yaratıcı bir süreç ve bir dizi üründür. Bu kültürün, modern kültürü bir bütün olarak giderek artan biçimde şekillendiren pek çok özelliği vardır. Hız ve ekranların her an her yerde kullanıldığı bir kültür yaratır. Önceden programlanmış ve kullanıcıların ürettiği içeriklerin; parçaları ve kolajların bir kombinasyonudur. En göze çarpan özelliklerinden biri de dijital kültürün ürettiği kaynak ve mesajların niceliğinin katlanarak artmasıdır. Bu durum kolaylıkla enformasyon ve iletişim yüklenmesiyle sonuçlanmaktadır (Dijk, 2016: 323).

Enformasyonun hızla yaygınlaşması, dijital kültüre ilişkin yaklaşımların farklılaşmasını da beraberinde getirmiştir. Bilgi akışının kesintisizliğinin yarattığı faydalara odaklanan yaklaşımların yanı sıra, bireysel düzlemde kişisel verilerin elden ele dolaşması ve dolayısıyla gözetimin yaygınlaşmasını temel sorunsal olarak ele alan yaklaşımlar da literatürde geniş yer bulmuştur. Bu yaklaşımlara göre dijital teknolojiler kültürü dönüştürürken, gözetimi de dijitalleştirip kültürel bir form haline getirmiştir. Bunun ötesinde gözetimin dijitalleşmesi,

yönetsel ve tecimsel alanlarda, mahremiyetin göz ardı edildiği çok sayıda vakanın ortaya çıkmasının zeminini hazırlamıştır.

Günümüz koşullarında gözetimin giderek yaygın hale gelmesi, dijital gözetim kavramını ortaya çıkartırken, hayatımızın pek çok alanında çevremizi kuşatmış olan mobil teknolojilerin özel alanlarımız için ne ölçüde kontrol ve denetim mekanizması olarak kullanıldığı sorusunu da akıllara getirmektedir. Buna paralel olarak, internet kullanıcılarının bilgiye erişimini sağlayan mobil araçların, kullanıcının dijital izlerinin takip edildiği platformlar olarak değerlendirilmesi karşısında, ağ teknolojilerinin giderek gözetleme sistemlerine dönüştürüldüğü yönündeki yaklaşımların varlığı da söz konusudur. Şirketlerin ya da reklam verenlerin, kullanıcıların internette geçirdikleri zamanlarda bıraktığı dijital izlerle ya da çeşitli mobil uygulamalarca sızdırılan kişisel verileri kullanarak müşteri profili oluşturması ve kullanıcıların mobil ortamlarda ilgilendikleri konular çerçevesinde belirlenmesiyle yaratılan "kişiselleştirme", etik sorunları ve mahremiyet ihlali endişelerini de beraberinde getirmektedir.

Dijital iletişim kanallarını kullanma ve dijital iletişim kanallarının istenmeyen etkilerinden korunma becerisinin, kullanıcıların dijital teknolojiyle tanışma ya da bu teknolojilerin içinde doğma durumlarına göre değişiklik gösterdiği düşünülmektedir. Bu noktada, kuşak –generation- kavramı bu çalışmanın sürekli gündeminde olması gereken bir kavramdır. Dijital kültüre eklemlenme ya da dijital kültürün içine doğma durumlarına göre farklılaşan kuşaklar, dijital dünya söz konusu olduğunda yeniden tanımlanmaya ihtiyaç göstermiştir. Marc Prensky, çalışmalarında kuşakları yaş ve teknoloji kullanımlarına göre kategorilendirmiştir. Bu kategorileri ise 1980 yılından önce doğan, teknoloji ile sonradan tanışan "Dijital Göçmenler" ve 1980 yılından sonra doğan, teknoloji ile iç içe olan "Dijital Yerliler" olarak sınıflandırmıştır (Prensky, 2001a, 2001b). Dijital yerliler, teknolojinin içine doğan, ana dili dijital dil olan teknolojik araçları etkin bir biçimde kullanabilen ve bu araçlardan yoksun bir hayat süremeyecek olanlar kişiler olarak tanımlanabilmektedir. Dijital göçmenler ise teknolojiyle sonradan tanışan, dijital dili anlamaya ve anlamlandırmaya çalışan, teknolojik araçları kullanma becerisine sahip ancak dijital yerlilere göre nispeten uyum süreci uzun olan kişilerdir. Prensky'ye göre dijital yerliler ve dijital göçmenlerin düşünsel yapıları farklı olup, bilgiyi işleme şekilleri de farklılık göstermektedir (akt. Tonta, 2009: 746).

"Sosyologların kuşakları; X,Y,Z olarak bölümlendirmesiyle birlikte aslında bu bölümlendirmenin iletişim araçlarının etkileşimliliğine göre yapıldığı kanısı da giderek güçlenmektedir" (Karahisar, 2013: 71). Bu etkileşimin X ve Y kuşaklarında Z kuşağına göre düşük olduğu, Z kuşağının etkileşimli dijital ortamları tercih ettiği görülmektedir. Bu noktada söz konusu kuşak bölümlenmesindeki farklılıkların, gözetim algısına yansıyacağı

varsayımından hareketle, kuşaklar arasındaki gözetim algısındaki farklılıkların ortaya konularak irdelenmesi önem arz etmektedir.

**Çalışmanın Sorunsalı**

Mobil ortamlarda yayınlanan reklam içeriklerinin, internet kullanıcılarının web siteleri, arama motorları, mobil uygulamalar ya da sosyal medyada ilgilendikleri konular çerçevesinde belirlenmesiyle yaratılan kişiselleştirmenin yol açtığı etik sorunlar ve gizlilik ihlali endişeleri çerçevesinde belirlenen sorunsal, birbiriyle bağlantılı pek çok boyutta ele alınmıştır. Kişiselleştirme sürecinde/sonrasında elde edilen kişisel verilerin, kişinin rızası ya da bilgisi dışında kullanımının yaratabileceği etik ihlallere ve mahremiyet ihlallerine ilişkin farkındalığın dijital göçmenler ile dijital yerliler arasında farklılık gösterdiği halde aynı yasal koruyuculuk çerçevesinde bulunmaları, çalışmamız kapsamında araştırma sorunsalı olarak oluşturulmuştur.

**Çalışmanın Amacı**

İnternet kullanıcılarının bilgiye erişimini sağlayan mobil araçların, kullanıcının dijital izlerinin takip edildiği platformlar olarak değerlendirilmesi, ağ teknolojilerinin giderek gözetleme sistemlerine dönüştürüldüğü yönündeki yaklaşımların argümanlarını güçlendirmektedir. Araştırmanın amacı, özel hayatın gizliliği temelinde, dijital gözetim ve dijital iz takibinin yol açabileceği mahremiyet ihlalleri ve bu bağlamdaki etik sorunlara ilişkin farkındalık düzeyinin kuşaklar arası farklılığının, -özellikle dijital göçmenler kategorisine giren kitlenin hayatında- yol açabileceği sorunlara bilimsel yöntemlerle işaret etmek ve çözüm önerileri sunmak oluşturmaktadır. Bu amacı gerçekleştirmek için, dijital göçmen ve dijital yerlilerin dijital gözetime ilişkin farkındalık ve algıları, mobil ortamlarda yayınlanan reklamların izlenme, fark edilme, kullanılma durumları mobil ortam reklamlarında gözetim olgusu kapsamında karşılaştırmalı olarak analiz edilip değerlendirilecektir.

**Bu amaç doğrultusunda aşağıdaki sorulara çalışma boyunca yanıt aranmaya çalışılmıştır:**

Dijital göçmenler ve dijital yerliler, mobil ortam reklamlarında gerçekleşen dijital gözetimin farkında mıdır?

Dijital göçmenler ve dijital Yerliler, mobil ortamlarda hangi bilgilerini paylaşmaktadır?

Kişiler, mobil uygulamaların kişisel bilgileri üçüncü kişilerle paylaşabileceğini biliyorlar mı?

Kişiler çerezler konusunda bilgi sahibi midir?

Dijital göçmenler ve dijital yerliler, mobil uygulama yüklemeden önce uygulamaların erişim izinlerine dikkat ediyorlar mı?

Dijital göçmenler ve dijital yerliler mobil ortam reklamlarını engellemek için herhangi bir engelleme programı kullanıyorlar mı?

Kişiler mahremiyetin ihlaline karşı devletin koruyuculuğuna inanıyorlar mı?

Dijital göçmenler ve dijital yerliler, dijital haklarını biliyorlar mı?

Kişiler KVKK hakkında bilgi sahibi midir?

**Bu araştırma sorularının dayandığı varsayımlar şu şekildedir:**

Kişisel verilerin kullanıcıların izni olmadan kullanıldığı durumlar vardır.

Mobil ortam reklamlarında dijital gözetim bulunmaktadır.

**Araştırmanın hipotezleri de aşağıdaki gibidir:**

Dijital göçmenlerle dijital yerlilerin dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır.

Kadınlar ve erkekler arasında dijital gözetim algı-farkındalık düzeyleri açısından anlamlı bir farklılık bulunmaktadır.

Eğitim durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmaktadır.

Çalışma durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmaktadır.

Mobil ortam reklamlarında kullanılan kişiselleştirme, dijital gözetim bağlamında mahremiyet ihlaline ilişkin endişeleri artırmaktadır.

Dijital göçmenler ve dijital yerliler arasında arama yaptıkları ürünler ve hizmetlerle ilgili reklama maruz bırakılmaları sonucunda duydukları gizlilik ihlali endişesi düzeylerinde anlamlı bir farklılık vardır.

**Çalışmanın Önemi**

Dijitalleşmenin toplumda hızlı bir şekilde yayılması dijital kültür kavramının doğmasına neden olmuştur. Kitlelerin internet tabanlı mobil cihazlar aracılığı ile enformasyona anında ve kolay ulaşımı, bireyleri olduğu kadar şirketleri de cezbetmekte, adeta bu cihazları, bilgi dolaşımının yanında, cebimizde taşıdığımız bir reklam mecrasına dönüştürmektedir. Bu durum 'mobil ortam' tamlaması ile kavramsallaştırılmış, giderek gelişen mobil teknoloji ve mobil internet olanaklarıyla birlikte 'mobil reklamlar' yerini 'internet tabanlı mobil ortam reklamları'na bırakmaya başlamıştır. Türkçe literatürde, mobil iletişim ortamlarının reklam mecrası olarak kullanılması sırasında gerçekleşen dijital gözetime ilişkin yapılmış alan araştırmasına yönelik herhangi bir bilimsel çalışmaya rastlanmamıştır. Bu noktada çalışmamız, konu üzerine yapılacak çalışmalar için yol gösterici ve veri sağlayıcı bir karakter taşıması nedeniyle önemlidir. Yurtdışında yapılan araştırmalarda da doğrudan bu konuya odaklı yapılan

çalışmalar sınırlıdır. Daha önce yapılmış çalışmalar incelendiğinde, iletişim ortamlarında gözetim, internette gözetim, sosyal ağlar üzerinde gözetim gibi konulara değinilmiş olup mobil ortam reklamlarındaki gözetim boyutuna ilişkin algılar ve değerlendirmelerin ihmal edildiği görülmüştür. Çalışma kapsamında elde edilen bilgiler bilişim alanındaki uygulamaların etik boyutuna ilişkin yaklaşımların ve yasal mevzuatın geliştirilmesine hizmet edebilecektir. Çalışma, sosyal bilimler literatürüne yöntem ve kuram açısından da katkı sunacaktır.

Çalışmanın disiplinlerarası bir noktadan hareket ediyor olması, çalışmada kullanılan kavramların açıklanmasını zorunlu kılmıştır. Bu kavramlardan bazıları operasyonel olarak tanımlanmış ve aşağıda belirtilmiştir.

**Kavramsal Çerçeve**

Teknoloji, insanlık tarihi boyunca var olmuş, hemen hemen her dönemde insanoğlunun ellerinde değişik formlar almış, varoluşundan günümüze dek sürekli gelişim göstermeye devam etmiştir. Ahmet İnam (2005: 57, 58)'a göre "teknoloji yalnızca bir ürün değildir. Teknoloji amaçsal bir etkinlik, bilgi ve üründür. Bir insan etkinliğidir; yapan, eyleyen, üreten insandır". Teknolojinin kendisine içkin otonom tarihsel karakteri insan hayatına yeni bir düzenleme getirirken bu düzenlemenin deneyim ile bilgiyi kopartan maddi bir düzenleme olduğu görülmektedir. Bu sistemin maddi yapısının temelini de kişilerin bilgiyi oluşturma ve kullanma süreci göstermektedir (Gülenç ve Arıtürk, 2014: 119).

Sanayi toplumundan bilgi toplumuna geçilmesi, bilgiye kolay ve hızlı bir şekilde ulaşılması, teknolojinin de hızlı bir ivme kazanarak büyümesi sonucunu doğurmuştur. Bilgi toplumunun en temel özelliklerinden biri de teknoloji ve bilgi bağımlılığıdır. Bu bağımlılığa paralel olarak yaratılan teknoloji ihtiyacı ve bu ihtiyacın bir sonucu olan dijitalleşmenin yaygınlaşması, yeni teknolojik araç ve gereçlerin yoğun bir şekilde kullanılmasına neden olmuştur. Teknolojik araçlar, kapitalist sistemin yeniden üretimi için adeta hayatımızın merkezine konumlandırılmıştır. Teknolojinin belirleyiciliği gün geçtikçe insan hayatı için merkezi bir hal almaktadır:

> Teknoloji ile toplumun ilişkisi açısından vurgulanması gereken şey, devletin teknolojik yenilikleri gerek başlatarak, gerek yasaklayarak, gerek onların öncüllüğünü üstlenerek yüklendiği rolün, belli bir mekân ve zamanda hâkim olan toplumsal ve kültürel güçleri ifade edip örgütlediğinden dolayı, sürecin tamamı açısından belirleyici olduğudur. Teknoloji, büyük ölçüde bir toplumun kendini, devlet de dâhil toplumun kurumları üzerinden teknolojik üstünlüğe sevk etme kapasitesini ifade eder. Üretim güçlerinin bu gelişiminin gerçekleşmiş olduğu tarihi süreç, teknolojinin ve onun dokunduğu toplumsal ilişkiler ağının özelliklerine damgasını vurur (Castells, 2013: 15).

Teknoloji, ilk bakışta tarafsız olarak algılanmakta ve bütün toplumlara hizmet eder gibi görünmektedir. Ancak bu tarafsızlık irdelendiğinde, arka planda mülkiyet, üretim, dağıtım ve erişim gibi sorunların olduğu da görülmektedir (Çakır, 2015: 16). Anthony Giddens (2001: 58)'a göre "hiçbir teknoloji dâhil olduğu toplumsal çerçevelerden ayrı olarak yeterli biçimde incelenemez. Batı toplumlarında bu çerçeveler, her şeyden önce, kapitalist nitelik taşımaya devam etmektedir". Karl Marx (2012: 25) kapitalist toplumu, "*emek gücünün bir meta olarak özgürce alınıp satılabildiği bir toplum çeşidi*" olarak tanımlamaktadır. Marx, teknolojinin değer değil, meta yaratmak için kullanılan bir araç olduğunu ileri sürer (akt. Fuchs, 2015: 194). Teknolojinin salt kamusal fayda odaklı üretildiği ve yayıldığı görüşüne yönelik eleştiriler, güçlü argümanlarla sunulmaktadır. George Bassala'nın, teknolojinin insan ihtiyaçları öncelikli karakterinin meta odaklı bir yapıya dönüştüğüne ilişkin görüşleri, bu eleştiriler kapsamında önemli vurgular taşımaktadır:

> Teknolojiyi öncelikle insan ihtiyaçlarına hizmet etmesi için geliştirme özgürlüğü, endüstrileşmenin yayılması ve iletişim, ulaşım, güç üretimi ve imalat alanlarında modern mega-teknik sistemlerinin geliştirilmesiyle birlikte yitirilmiştir. Muazzam, karmaşık ve birbiriyle ilişkili bu teknolojik sistemler, insani değerleri baştanbaşa istila ederek insan kontrolünü hiçe saymaktadır. Bu sistemlerde değişiklik, yalnızca verimlilik veya büyük ölçekli bütünleşme gibi öncelikli teknik değerlerle çatışmadığı sürece mümkün olabilmektedir. Bu yüzden, yaşama, çalışma ve oyun oynama biçimlerimiz, modern endüstriyel toplumu yöneten tek parça teknolojik düzen tarafından yapılanmaktadır (Bassala, 2013: 316).

Günümüz toplumları teknolojiyle ciddi derecede kaynaşmış, toplumun tüm dinamiklerinin değişmezi haline gelerek, geniş kitleler için neredeyse vazgeçilmez bir parça olmuştur. Gelinen noktada teknoloji öylesine insan hayatına nüfuz etmiştir ki en yeni teknolojileri kullanmayan/kullanamayan kişiler çoğunlukla teknoloji yoksunu olarak görülmektedir. Çakır (2015: 17)'a göre teknolojik kullanımlar adeta başarının, verimliliğin, güncelliğin, toplumsal bilgi düzeyine erişimin göstergesi haline gelmiştir. Ona sahip olma ve kullanma becerisi mülkiyete ve bilgiye ilişkin sosyal bir statü sembolü gibi işlev görmekte ve bu şekilde her şeyi kuşatmaktadır.

İletişime sosyolojik bakış, kitle iletişim araçlarının en çarpıcı özelliğinin, zaman ve uzay içinde ve çok sayıda tekrarlanabilen mesajları geniş topluluklara iletebilme becerisi olduğunu ileri sürmektedir (Geray, 2003: 17). Toplumsal örgütlenme ve kültürel yapının doğrudan iletişim teknolojilerindeki değişime bağlı olduğunu öne süren yaklaşım da "Teknolojik Determinizm" olarak adlandırılmaktadır (Aktaş ve Çaycı, 2013: 2). Ancak belirtmek gerekir ki, teknolojik determinizm çoğunlukla, teknolojik üstünlüğün ardında yatan ekonomik, politik ve kültürel dinamikler üzerinde yeterince yoğunlaşılmadığında açıklayıcı olmaktan

uzaklaşmaktadır. Timisi (2016: 18)'ye göre "Teknolojik Determinizm, teknolojiyi toplumsal yaşamın merkezine koyan bir düşünce biçimi olarak gelişme, ilerleme, modernlik, demokrasi gibi temel kavram ve süreçlerin de belirleyicisi, taşıyıcısı, bir nevi motoru olarak ele alır". Söz konusu olan bilişim ve iletişim teknolojileri olduğunda bu görüş kendisine daha geniş bir kabul alanı bulabilmektedir. Özellikle bu gelişmelerin bir sonucu olan internetin, toplumun tüm dinamiklerine olan etkisi birçok araştırmaya konu olmuştur.

İnternet, temel anlamda yazılım ve donanımın bir birleşimi olan birtakım yönlendiriciler tarafından bağlamış sanal bir ağ kümesidir. Dünyadaki tüm iletişim süreçlerini etkileyen global bir role sahip olan internet, bilgisayar aracılığıyla kurulan iletişimin belkemiğidir: Bilgisayarların birbirleriyle haberleşmesini sağlayan ağdır (Çakır, 2015: 39; Castells, 2013: 463). İnternetin günümüzde bir "demokratikleşme" aracı olduğu iddiaları da literatürde yer almaktadır (Briggs ve Burke, 2004: 11). Öte yandan, bu yeni teknolojilerin, daha etkili bir denetim ve toplumsal kohezyon biçimlerini yaratmaya hizmet ettiği yönündeki görüşler de kabul görmektedir. Hatta baskıcı bir egemenlikte, bilişim teknolojileri tarafından yaratıldığı iddia edilen özgürlükler bile güçlü bir denetleme aracına dönüştürülebilmektedir (Marcuse, 2010: 14, 24). Çakır (2015: 51) da, interneti etkileşim, ifade özgürlüğü, paylaşım, bilgiye kolay erişim, gibi özelliklerin yanında; denetim ve gözetimi de kolaylaştıran global bir ağ olarak tanımlamaktadır. Bu ağlar o denli genişlemiştir ki internete anında erişim olanaklarıyla beraber 'medya'[1] da dönüşüme uğramış, daha etkileşimli bir yapı olan 'dijital medya' kavramı doğmuştur. Dijital medyanın taşıyıcısı ise bilgisayarları birbirine bağlayan ağlar arası geçişi mümkün kılan World Wide Web (WWW) isimli yazılımlardır (Wayne, 2006: 58). Mikroişlemcilerin bulunmasından sonra, yazılımlar da hızla katlanarak artmıştır. Yazılımlar teknolojinin 'yaratıcı yönünü' temsil etmektedir. İletişim sisteminin fiziksel bileşenleri için kullanılan 'hardware' (donanım) sözcüğünün karşıtı olan 'software' (yazılım) artık çok daha yeni anlamlar kazanmaya başlamıştır (Briggs ve Burke, 2004: 308).

Dijitalleşme, iletişim alanında köklü değişikliklere yol açmıştır: İletişim kitleselliğini artırmış, maliyeti ucuzlatmış, çevrimiçi olanakları genişletmiş ve interaktiviteyi sağlamıştır. "İletişimin dijitalleşmesi, ürünler ve süreçlerin aynı global/yerel ağ içinde bir içerik ve medya ifadeleri çeşitliliğini destekleyen farklı platformlarda geliştirildiği, teknolojik olarak bütünleşmiş bir medya sisteminin yayılmasını da teşvik etmiştir" (Castells, 2016: 109). Bu bütünleşmeyi "Birbirine Yaklaşma" kavramıyla açıklamak mümkündür: "Dijital teknolojinin

[1] İnsanların "medya" sözcüğünü kullanmaya başlamaları Oxford İngilizce Sözlüğü'ne göre 1920'lerde başlamış, 1950'lerde ise bir "iletişim devrimi"nden söz edilmeye başlanmıştır (Briggs ve Burke, 2004: 7).

gelişimine, metinlerin, sayıların, görüntülerin ve sesin birleşmesine, medyadaki farklı öğelerin bir araya gelmesine bağlı olarak özellikle medya ve telekomünikasyon endüstrilerinin bir arada bulunmasıdır" (Briggs ve Burke, 2004: 289).

Dijitalleşme, iletişimin globalleşmesini sağlarken, enformasyon işleme, depolama gibi yöntemlerden yararlanılmasına öncülük etmiştir. Böylece sürekli artan enformasyonu verimli ve hızlıca uzak mesafelere iletme olanağına kavuşulmuş, elektromanyetik dalgalarla iletilen mesajlar, bu sinyallere erişilebilen ortamda bulunan ve onları alacak donanıma sahip olan herkes tarafından erişilebilir hale gelmiştir (Mutlu, 2005: 121, 125). İşaya Üşür, (2001: 19) teknolojinin, globalleşmenin temel bileşenlerinden birisi olduğunu ve teknolojinin bir bileşen olmanın ötesinde globalleşmeyi olanaklı kılan ve globalleşmenin kaçınılmazlığını ortaya koyan bir amaç haline geldiğinden bahsetmektedir.

"Globalleşme, zaman ve uzam ufuklarının sıkıştırılmasını, anlık ve derinliği olmayan bir dünyanın yaratılmasını ifade etmektedir. Global uzam, bir akışlar uzamıdır, elektronik bir uzamdır, merkezi yoktur" (Morley ve Robins, 2011: 160). Paul Virilio (2003: 17)'da globalleşmenin iki tamamlayıcı görünümüne dikkat çekmektedir. Bunlar, haberleşmenin ve ulaşımın zamansal sıkışması nedeniyle mesafelerin aşırı ölçüde kısalması ve tele-gözetimin giderek yaygınlaşmasıdır. Araştırma konumuz kapsamında önemli bir tanımlama ise James R. Beniger tarafından ortaya atılmıştır. Beniger (2009) bilgi iletişim teknolojilerinin ortaya çıkışını ve yaygınlaşmasını "kontrol devrimi" olarak adlandırmaktadır. İletişim teknolojilerinin dijitalleşerek global hale gelmesi, dijital gözetimi olanaklı kılarken bunun yanında kültürel yapının da değişime uğramasına neden olmuştur.

İletişimin dijitalleşmesi ve dolayısıyla global hale gelmesiyle birlikte genel anlamda medya, kültürel kodların hızla yayılmasında etkin bir konuma gelmiştir. Böylelikle global düzlemde bu kültürel kodlar, çeşitli imaj ve simgeler aracılığıyla çeşitli kültürel karışımların ve kültürün melez formlarının ortaya çıkmasına öncülük etmiştir. Ortak simge ve kodların bu şekilde yaygınlaşmış olması ortaya büyük bir dijital ağın çıkışının da nedenidir (Çaycı ve Karagülle 2016: 579). Ağlar dijitalleştikçe toplumlar da birer online ağ toplumu haline dönüşmektedir. Manuel Castells (2016: 59) ağ toplumunu, toplumsal yapısı mikroelektroniğe dayalı, dijital olarak işlenen enformasyon ve iletişim teknolojilerinin harekete geçirdiği ağlar etrafında örgütlenmiş bir toplum olarak adlandırmaktadır. Bu durum pek çok kültürel kodun da globalleşmesini beraberinde getirmiştir. Bu globalleşmiş kodlar da ağların daha hızlı ve yaygın biçimde bütünleşmesi sonucunu doğurmuştur. Bu da dijital kültürün güçlü bir ivmeyle geniş bir yaşam alanı bulduğunun kanıtı sayılabilir. Dijital kültüre dahil olmak, internetin sağladığı iletişimde, özellikle sosyal ağlar aracılığı ile etkin bir aktör olmak sosyalleşmenin göstergesi

haline gelmiş, bu ortamlarda oluşturulan yeni kültürel kodlar ve bunların ifade biçimleri gündelik hayatta global biçimde yaygınlaşmıştır.

Türk Dil Kurumu'na[2] göre kültür, "toplumsal gelişme süreci içinde yaratılan bütün maddi ve manevi değerler ile bunları yaratmada, sonraki nesillere iletmede kullanılan, insanın doğal ve toplumsal çevresine egemenliğinin ölçüsünü gösteren araçların bütünü" olarak tanımlanmaktadır. Castells (2016: 70)'e göre toplumlar kültürel yapılardır ve insanların davranışlarını yönlendiren değerler ve inançların bütünüdür. John Fiske (2012: 35)'ye göre de kültür, "yaşayan, canlı bir süreçtir". Kültür, insanların günlük hayatındaki değerler ve yaşam tarzlarından doğmaktadır. Global kültürün kökeni ise kapitalizme dayanmaktadır. Yükselen global kültürün en görünür biçimde dışa vurulma aracı da popüler kültürdür ve bu kültür ekonomik ve politik düzlemde çok uluslu şirketler tarafından yayılmaktadır (Berger ve Huntington, 2003: 15).

"Kültür, iletişim, düşünce değiş tokuşu, geri bildirim sistemleri, veri analizi vb.'nin üretim sürecinde gittikçe artan öneminin yanında kaçınılmaz şekilde kültürel üretime, özellikle de dijital medyaya yöneltilen sermaye miktarının artmasıyla bağlantılıdır" (Wayne, 2006: 64). Bu kültürel üretim enformasyon toplumunda farklı, ağ toplumunda farklı şekilde gerçekleşmekte, Jan Van Dijk (2016: 41) bu farkı şu şekilde açıklamaktadır: Enformasyon toplumu kavramında faaliyet ve süreçlerin değişen özüne vurgu yapılmakta iken, ağ toplumu kavramında dikkat ve ilgi bu toplumların değişen örgütlenme biçimleri ve yapılarındadır. "Ağ toplumu globaldir, dünyada her bölgenin tarihi ve coğrafyasıyla bağlantılı bir kültürler çoğulluğunu işler ve bütünleştirir" (Castells, 2016: 70).

Gündelik yaşam kültürü, kapitalizmin sağladığı kaynakların yaratıcı ve beğeniye dayalı kullanımında hayat bulmaktadır (Fiske, 2016: 40). Gündelik hayat pratiklerinin teknolojik hale gelmesiyle birlikte deneyim ile bilgi arasındaki ilişki parçalanmakta ve ikili arasındaki boşluğun yeni ilkelerle doldurulmakta olduğu görülmektedir. Bu ilkeler, teknolojinin kendisinin üretmekte olduğu hayat tarzına işaret etmektedir; çünkü bu ilkeler gündelik hayatı belirlerken, kişilerin hareket alanlarını da biçimlendirmektedir (Gülenç ve Arıtürk, 2014: 118). Max Horkheimer, geç kapitalist toplumda teknolojinin bireyin silinişine sebep olan süreçlerden biri olduğunu ileri sürer (akt. Gülenç ve Arıtürk, 2014: 114). Teknoloji, insan hayatının her alanına nüfuz ederek farklılıkları ortadan kaldırmıştır.

Bilgi ve iletişim teknolojilerinde yaşanan gelişmelerin öncesinde kolektif yaşam ve kültürünün inşasında kullanılan ana mekanizma televizyonken, (Morley ve Robins, 2011: 160) internet bireyselleşmeyi tetiklemektedir. İnternetin artık kitle iletişimi için yaygın kullanıldığı

[2] http://www.tdk.gov.tr (erişim tarihi: 05.03.2018).

düşünüldüğünde bu teknolojinin insanları ağlarla birbirine bağlarken bir yandan da bireysellikte yarattığı keskinlik nedeniyle yalıtılmışlığı artırdığı da göz ardı edilmemelidir. Zygmunt Bauman (2016: 26)'a göre zamansal/mekansal mesafelerin ortadan kalkmasıyla beraber, insanlık durumu homojenleşmemiş aksine kutuplaşmıştır. Siber mekanda bedenlerin önemi yokken, bedenlerin hayatında siber mekanın kesin ve vazgeçilmez bir önemi bulunmaktadır. Bauman'ın vurguladığı kutuplaşma ve kimlik meselesi, bir taraftan da insanların bireysel kimlikleri konusunda daha keskin bir bakış açısına sahip olmalarına neden olmaktadır. "Kimlik edinme, globalleşme ve bireyselleşmenin birlikte yarattıkları baskı ve gerilimlerin yan etkisi ve yan ürünüdür" (Bauman, 2005: 189). Bireysel kimlik kazanma ihtiyacı, tüketim ve yaşam tarzı kalıplarını şekillendirmede rol oynamaktadır (Harvey, 2006: 145). Bu noktada kişiselleştirmenin reklam açısından da kritik bir önem taşıdığı görülmektedir: Kişiselleştirilmiş reklamlar bireye öznelik atfetmektedir. "Rasyonelleştirme ve sınıflandırma arzusu ise, kitlelerin bireyselleştirilmesi ve buna uygun sahiplenici bireycilik kültürü ile beraber, modernitenin temelini oluşturmaktadır" (Lyon, 2013: 13).

Bauman (2005: 178)'a göre "bireyselleşme insan 'kimliği'nin bir 'veri'den bir 'görev'e dönüştürülmesinden ve aktörlere bu görevi yerine getirmenin ve bunun yaratacağı sonuçların sorumluluğunun yüklenmesinden ibarettir". Diğer taraftan, bireyselleşme giderek kimlik meselesine entegre biçimde 'kişisellik' kavramı ile karşılanmaya başlamıştır.

İnternetin ortaya çıktığı ilk dönemlerde kullanılan web 1.0 yalnızca bilgi alma amaçlıyken, web 2.0 kullanıcıların içerik üretmesine, yorum yapmasına ve katkıda bulunmasına olanak tanımıştır. Web 2.0 etkileşim temelli olduğundan sosyal ağların da yaygınlaştığı dönemdir. Şu an içinde bulunduğumuz döneme ise web 3.0 hakim olmaya başlamıştır ve kullanıcıya özel, kişiselleştirilmiş bir dönem olarak adlandırılmaktadır. "Günümüzde, çoğu insanın varsayılan günlük davranışlarından birinin en azından bir kişiselleştirilmiş medya türüne bağlanmak olduğu, tarihte ilk defa söylenebilmektedir" (Chatfield, 2013: 38). İnternet üzerinde daha fazla medya ürünü dağıtılıp tüketildikçe, sosyal ağlar ya da diğer ortamlarda kullanıcıların ürettiği içeriklerle iç içe geçtikçe, kullanıcı davranışına göre yapılan reklamlar da odak noktası haline gelmektedir (Castells, 2016: 134). Kişiselleştirilmiş reklam mesajlarının taşıdığı anlam, hedefteki kişinin reklamı yapılan ürünleri satın alıp almamasının çok ötesindedir. Artık reklamlar ve indirimler, kişinin statüsünün göstergeleri haline gelmektedir (Turow, 2015: 19). Önceleri toplu üretim ve toplu ticaret söz konusuyken günümüzde bunlar bireysel hale gelmiştir. Artık tüketicinin satın alma davranışlarına göre ayarlı, hedeflenmiş ve bireyselleştirilmiş teknikler kullanılmaktadır (Lyon, 2006: 87). Tecimsel alanda kişiselleştirmenin asıl amacı, kullanıcıların dikkatini çekmek ve onların satın alma

motivasyonunu artırmaktır. Reklamın ona/kişiye özel olarak hazırlandığı ve yönlendirildiği illüzyonu yaratılmaktadır.

Kişiselleştirilmiş içerikler, web sitelerini ziyaret edenleri ya da mobil ortamları kullanan kişileri bu platformlarda daha uzun kalmaya ikna etmenin yanı sıra (bu şekilde reklamlarla etkileşim kurma olasılıklarını yükseltmek) reklamın içerdiği ticari mesajı da pekiştirmektedir (Turow, 2015: 274). Oscar Gandy Jr.'a göre şirketler, kişisel bilgileri kullanıcıların özelliklerine göre sınıflandırarak ürünlerini bu sınıflandırmaya göre pazarlama yoluna gitmektedir (akt. Arslantaş-Toktaş vd., 2012: 56). Dijital profilleme ve kişiselleştirme, sosyal ayrımları ve gizlilik ile ilgili sorunları yansıtan yeni bir jargon yaratmakta, pazarlamacılar ya da reklam verenler kullanıcı profillerini çıkarırken insanları hedef ve çöp olarak sınıflandırmaktadır (Turow, 2015: 21). Çeşitli arama motorlarıyla yapılan aramalarda farklı sonuçların elde edilmesi de bu durumla bağlantılıdır. Profilleme sonucunda çıkan verilere göre de düşük gelirli kişilere farklı, geliri yüksek kişilere farklı reklamlar gösterilebilmektedir. Bu sınıflandırma ise çeşitli yöntemlerle yapılmakta olup çoğunlukla çerezler (cookies) aracılığı ile gerçekleştirilmektedir. Temelde kullanıcıların web sayfası ziyaretlerini hızlandırmak amacıyla kullanılan çerezler bu işlevinin dışında kullanıcı profili oluşturmak, belirli kullanıcıların ilgileri ve zevklerine göre reklam içeriği oluşturmak, kullanıcı tarafından incelenen son reklamalar hakkında bilgi sahibi olmak için de kullanılmaktadır (Özdilek, 2002: 199).

> Çerezler, web sitelerinin kullanıcının daha önce siteye girip girmediğini öğrenmek için site her ziyaret edildiğinde diski okurlar. Tüketiciye sağladığını iddia ettikleri avantaj, bireysel ihtiyaçlara göre düzenlenmiş tüketici reklamlarının sadece doğru olan hedeflere yöneltilmesidir. Şirketin avantajı ise piyasanın bireyselleşmiş bir düzeyde bilinebilmesidir (Lyon, 2006: 208).

Tüm bu yöntemlerin kullanılması (ister kullanıcı profili çıkarmak olsun ister ticari bir mesajı pekiştirmek ya da buna benzer yöntemler) demografik bilgiler temelde olmak üzere, edinilen tüm bilgilerin şirketlerin yararına kullanılacağı gerçeğidir. Şirketlerin özellikle kuşaklar arasındaki farkları tespit ederek, bu farklara göre kişiselleştirilmiş reklam sunması, kuşakların zevk ve tercihlerinin belirlenerek tüm tüketim alışkanlıklarının haritalarının çıkarılması kuşak kavramının da açıklanmasını gerekli kılmaktadır.

"Her dönemin hakim değerleri, kültürel kodları ve bunların şekillendirdiği düşünce ve davranış kalıpları vardır. Bunları anlamak ve öngörülerde bulunabilmek için; bu dönemlerin kuşaklar üzerinden ele alınması daha gerçekçi sonuçlara ulaşabilmek için gereklidir" (Altuntuğ, 2012: 203). Kuşak; insan hayatındaki farklı evreler için tanımlanan, sosyal rollerin kazanıldığı ve insanın yaşamının aşamaları olan çocukluk, yetişkinlik ve yaşlılık süreleri boyunca, beraber

yaşamış insan topluluğu olarak da tanımlanabilir (Strauss ve Howe, 1991). Her kuşak kendi içinde farklı özellikleri barındırmakta, genellikle bireyler kendi kuşağının davranışlarına benzer özellikler sergilerken, diğer kuşak grubunun davranışlarından farklı özellikler de gösterebilmektedir.

Dijital kültür sürecini oluşturan bireyler dijital yerliler ve dijital göçmenler ifadelendirmeleriyle, iki uç grup olarak karşımıza çıksa da bu iki uç grubun yanı sıra "melez" olarak adlandırılan bir grubun varlığından da bahsedilmektedir (Karabulut, 2015: 11). Literatürde "dijital melezler" hakkında yeteri kadar bilgi ve düşünce olmasa da 'dijital melezler' diye adlandırılan farklı bir gruptan da söz edilebilir. Bu grup bazen göçmenlerin bazen de yerlilerin özelliklerini almaktadır (Karabulut, 2015: 20). Dijital melezler, göçmenlere göre dijital imkanların kullanımına daha fazla hakim olsalar da, bu imkanları dijital yerliler kadar iyi ve etkin biçimde kullanamamaktadırlar. Dijital melezler bilgi taramalarında öncelikle yazılı kaynakları tercih etmekte daha sonra dijital ortamları tercih etmektedir. Bu durumda ise dijital melezler, dijital göçmenlerin özelliklerini almaktadır. Buradan hareketle melez grup bir geçiş grubu olarak adlandırılabilir. Ancak 'dijital bölünme' ya da 'dijital uçurum' kavramları söz konusu olduğunda bu durum daha da farklı bir hal almaktadır. 'Dijital bölünme' bilgi iletişim teknolojileri ve internet kullanımında gelişmiş ülkeler ile gelişmekte olan ülkeler arasındaki mevcut farklılığı vurgulamak üzere kullanılmaktadır. Bu kavram globalleşmeyle beraber 'dijital uçurum' (digital abyss) haline dönüşmüştür (Kılıç, 2011: 84). Aslında dijital bölünme kavramı, bu noktada ülkeler arasındaki farkları vurgulamanın ötesinde bir toplumdaki katmanlar arasındaki farkları da belirtmektedir. Kimi durumlarda melez gruplar diğer grupların özelliklerini alsa da, bu grup gelişmiş toplumlarda yok denecek kadar az olabilir. Aynı şekilde, yerlilik, göçmenlik ve melezlik durumunun yaş ile belirlenmesi her zaman doğru bir çerçeve sunmayabilir. Teknoloji kullanımlarındaki yoğunluk değiştikçe yaş aralığının önemi de değişebilmektedir. Teknolojik olanaklara sınırlı şekilde sahip toplumlar tamamen dışa bağımlıdır ve teknolojiyi üreten toplumlar tarafından ne kadar istenirse o kadar teknolojiye sahip olabilmektelerdir ki "hiçbir toplum, en azından teknolojisinin bazı yönlerini dışarıdaki bir kaynaktan ödünç almayacak denli yalıtılmış ve kendine yeterli değildir" (Bassala, 2013: 124).

**Kuramsal Çerçeve**

Günlük hayatımızda farkında olalım ya da olmayalım izleniyor ve denetleniyoruz. Bu izleme ve denetleme de, bilişim teknolojilerini kullanan toplumlarda çoğunlukla bilgisayar sistemleri aracılığı ile gerçekleşiyor. İletişim ortamlarındaki gözetim ise o kadar yaygın hale gelmeye başlamıştır ki mahremiyet ihlallerinin denetimi ve yaptırımları yasal düzenlemelere rağmen neredeyse mümkün olmamaktadır. Teknolojinin varlığı hayatımızın birçok noktasında

kendini hissettirmekte, günlük kullanımda kişilere birçok kolaylık sağlamaktadır. Ancak bu durum kişisel verilerimizi şirketlere ve devletlere altın tepside sunduğumuz gerçeğini de değiştirmemektedir. Kişilerin ilgi alanı, dini, inançları, davranışları ve tüm aktiviteleri dijital gözetim altında tutulmakta ve bu bilgiler ekonomik, sosyal ve kültürel olarak kullanılmakta, kontrol edilmekte ve yönlendirilmektedir. İletişim teknolojilerindeki gözetimin yaygınlaşmasıyla beraber gözetim ile ilgili bilimsel çalışmalar da artış göstermiş ve "gözetim çalışmaları" adı altında bir çalışma alanı da ortaya çıkmıştır.

Fransızcada "surveiller" kelimesi izlemek, gözlemek anlamına gelmektedir. "Gözetleme, hakkında veri toplananları etkileme veya idare etme amacıyla tanımlanmış ya da tanımlanmamış herhangi bir kişisel veri toplanması ve işlenmesidir" (Lyon, 2006: 13). Gözetim, insanlar ve kurumlar hakkındaki bilgilerin gözlenmesi, bireysel ve toplumsal davranışların düzenlenmesi, denetlenmesi, kaydedilmesi ve kategorize edilmesini içeren bir süreçtir (Ball ve Webster, 2003: 1; Hier ve Greenberg, 2007). Gözetim kavramı sosyal ilişkilerin ortaya çıkışından itibaren var olan bir kavramdır (Güven, 2011: 173). David Lyon (1997: 39)'a göre gözetim yeni değildir. Eskiden beri insanlar, yapılanları kontrol etmek, kaydedilen ilerlemeyi izlemek, örgütlemek veya korumak/korunmak için diğerlerine 'bakmışlardır'. Devletler de yurttaşlarını kayıt altına alıp gözetlemekte, her şeyi hesaplanabilir ve okunabilir kılmak istemektedir (Arslantaş-Toktaş vd., 2012: 25). William Bogard (1996)'a göre bir şeyi gözlemek, aslında onu izlemek veya korumak demektir. Devletler için gözetimi meşru kılmanın en kestirme ve kolay yolu da Bogard'ın bahsetmiş olduğu 'koruma' adı altında terör önlemleri ve güvenlik söylemleridir:

> Güvenliği amaçlayan sistemin asıl amacı vatandaşların değil, sistemin güvenliğini sağlamaktır. Güvenlik ve gözetim mantığı, gizliliğin devletlerin ve şirketlerin hakkı olduğunu öne sürer (devlet ve şirket sırları). Vatandaşlardan ise gündelik yaşamlarında, haberleşmelerinde, ilişkilerinde şeffaflık talep eder. Mahrem ile kamusal; açık ile gizli olan arasındaki ilişkinin tepetaklak edildiği bir tahayyüldür bu.[3]

Gözetim toplumu ifadesi, gözetim kavramını yönetim ilişkisi olmanın ötesine yerleştiren bir mantığı temsil etmekte, gündelik hayatın içerisinde olağanlaştırılan ve insanlar tarafından gündelik kullanım biçimi haline gelen gözetim uygulamalarının sorunsallaştırılmasıyla ortaya çıkmaktadır (Baştürk, 2016: 206). "Gözetlenen toplumları belirleyen günlük hayatın izlenmesi, çok uzun yollar kat edebilen her çeşit veri akımları üretir. Bu izlemede önemli olan nokta, bilgisayara uyarlanmış sınıflandırma işleminde kelimeleri ve aktiviteleri kategorize etmek ve belirlemektedir" (Lyon, 2006: 180).

[3] http://ayrintidergi.com.tr/sokak-internet-muhalefet/ (erişim tarihi: 23.05.2018).

Gözetime eleştirel yaklaşımların yanı sıra yönetsel (olumlayan) perspektifler de literatürde yer almaktadır. Yönetsel yaklaşımların bir kısmı, gözetimin toplumsal alanı düzenleme etkisi odağından hareket etmekte ve gözetime tarafsız bir bakış açısına sahip oldukları iddia edilmektedir. Gözetim ve denetime tarafsız yaklaşanlara göre denetim, verilerin sistematik olarak toplanması ve kaydedilmesidir. Öte yandan tarafsız yaklaşımlar denetimin, tüm toplumların karakteristik bir özelliği olduğundan bahsetmektedir. Bu yaklaşımlar bilgi depolama, işleme ve kullanmanın tüm biçimlerinin de, internet denetiminin bir türü olduğunu ileri sürer. Gözetimin olumlu yönleri olduğunu düşünen yaklaşımların üzerinde durduğu nokta ise nüfusun organizasyonudur. Giddens (1984: 183)'a göre denetim, nüfusların yönetimi ile ilgili olarak, onların yöneticiler tarafından doğrudan kontrol edilmesi ve böylece bilginin kodlanmasıdır. Tüm kuruluş biçimleri, çalışmak için bu denetime ihtiyaç duyarlar. Ayrıca Giddens (1987: 27) gözetimin bilgi toplamadaki temel bir süreç olduğunu belirtirken, tüm modern toplumları bilgi toplumu olarak görmektedir. Gary T. Marx (2005)[4] gözetime iyimser yaklaşanların; gözetimin, verimliliğin ve risklerin yönetilmesindeki en önemli unsur olduğunu ve teknoloji gücünün gözetimin temel noktasını oluşturduğunu belirtmektedir. Michel Foucault, "hastalıkların ve salgınların tıbbi olarak gözetim altında tutulmaları, burada bir dizi başka denetimle dayanışma içindedir" değerlendirmesinde bulunmuştur. Askeri denetim, vergi denetimi, ölümler, danışıklı dövüşler üzerinde idari denetim olduğunu ileri sürmüştür (Foucault, 1992: 178). Gözetime eleştirel yaklaşımlar ise denetimi, denetim altındaki kişinin iradesine karşın, 'belirli amaçlar' doğrultusunda sistematik olarak bilgi toplama biçimi olarak görmektedirler. Foucault (1992: 183, 230)'ya göre denetim, bir disiplin gücü biçimidir. Disiplinler, hakimiyetin genel formülleridir; kuşatırlar, normalleştirirler, cezalandırırlar, hiyerarşikleştirirler, homojenleştirirler, farklılaştırırlar ve dışlarlar. Bu nedenle denetim, Foucault'a göre tamamen bir baskı tekniğidir. "Normalleştirici bir bakış; nitelemeye, tasnif etmeye ve cezalandırmaya izin veren bir gözetimdir. Bireylerin üzerinde, farklılaştırdıkları bir görünebilirlik kurmaktadır" (Foucault 1992: 247, 257). Yine eleştirel yaklaşımda teknolojinin insan hayatına dayatma ile dahil edildiğini, gözetimin de insanlık dışı, özgürlüklerden uzak ve güvenilmez olduğu dile getirilmektedir (G.T. Marx, 2005). Ayrıca gözetimin toplumların karakteristik bir özelliği olduğu savına da şiddetle karşı çıkmakta ve gözetimin, şiddet ve zorlama içerdiğini, bilgi toplamanın özgürlüklerin ve egemenliğin sınırlanmasıyla ilişkilendirilen negatif bir kavram olduğunu iddia etmektedirler.

Karl Marx'a göre "gözetim, emek ve sermaye arasındaki mücadelenin bir unsurudur" (akt. Bozkurt, 2000: 136). Yine Marx'a göre ekonomik ve politik bir kavram olan gözetim,

[4] http://web.mit.edu/gtmarx/www/surandsoc.html (erişim tarihi: 01.09.2017).

kapitalist ekonominin temel bileşenlerinden olup işçileri kontrol ve disipline etmek için kullanılan zorlayıcı bir yöntemdir (akt. Fuchs, 2012a, 2012b). Gilles Deleuze'e göre sömürü, denetim ve gözetim giderek daha da incelmekte, yayılmakta daha da moleküler bir hale gelmektedir.[5] Deleuze'in "gözetimin daha da moleküler hale gelmesi" derken bahsettiği şey de internetle beraber dijital medya aracılığıyla gözetimin daha merkezsiz bir hale gelmesidir. Alexis de Tocqueville'e göre de modern toplumlar gözetime bağımlıdır (akt. Lyon, 1997: 43, 45). Antonio Negri (1990) anında iletişim yoluyla çalışan "kontrol toplumları"na doğru ilerlendiğinden bahsetmiştir.[6] Gözetim devleti tarafından sindirilen insanın toplumla uyumlu hale getirilme çabasını 1984 adlı romanda aktaran Orwell ise teknolojinin gücünü "Büyük Birader"[7] le bir araya getirmiş ve devletin sosyal denetim mekanizmasını gözler önüne sermiştir (Orwell, 2015). Fiske ve Hancock (2016: 242) gözetimin totaliter bir güç olduğunu belirtmişlerdir. Herbert Marcuse (2010: 20) da "teknolojik temelinin örgütleniş yolu nedeniyle, çağdaş işleyim toplumunun totaliter olma eğiliminde olduğunu" ileri sürer.

Gözetim çalışmaları literatürüne bakıldığında gözetimin kronolojik olarak üç aşamadan oluştuğu görülmektedir. Birinci aşama "Panoptik" dönem ile başlamıştır, çoğunlukla mimari gözetim ve disiplin mekanizmalarını içeren bir yapıdadır. İkinci aşama disiplinden gözetleme ve kontrol aşamasına evrilme söz konusudur. Bu aşama fiziksel olmayıp dijital altyapıya odaklı, kişilerin her an her yerde gözetime tabi tutulmakta olduğu "Süperpanoptik" dönemdir. Üçüncü ve son aşama ise ilk iki aşamadaki çerçeve üzerine inşa edilen yine dijital tabanlı ancak "Veri Gözetimi"nin öne çıktığı, kendi kendine gözetim ve gönüllü paylaşım kavramlarının yer aldığı herkesin herkesi gözetlediği aşamadır. Günümüzde ikinci ve üçüncü aşamadaki gözetim daha çok güncel tartışmaların konusu halindedir.

Araştırmanın temel probleminden hareketle çalışmanın kuramsal çerçevesi Fouacult'un "gözetim toplumu" yaklaşımı etrafında şekillendirilmiştir. Çalışmanın odağında ise veri gözetimi bulunduğu için araştırma problematiği bu yaklaşımın yol göstericiliğinde "dijital gözetim" kavramı ile formüle edilmiştir. Bu nedenle literatürde yer alan gözetim biçimleri arasından Panoptikon ve Süperpanoptikon, çalışmanın tamamı boyunca temel kavramlar olarak çalışmaya eşlik etmiştir. Michel Foucault, Jeremy Bentham'ın hapishane modeli olan Panopticon'u, kontrol ve disiplinin metaforu olarak görmektedir ve modern iktidarın yapısını bu modele benzetmektedir. Foucault, Panopticon'un mahkumların düşünce ve davranışlarını kontrol altında tutan bir mekanizma olduğunu ileri sürer. Panoptikon, merkezi bir denetleneme

[5] http://www.cafrande.org/gilles-deleuze-kapitalizmin-yayilmasiyla-somuru-denetim-ve-gozetim-giderek-daha-da-incelmekte/ (erişim tarihi: 01.05.2018).
[6] https://www.uib.no/sites/w3.uib.no/files/attachments/6._deleuze-control_and_becoming.pdf (05.11.2017)
[7] Mutlak kontrolü amaçlayan merkezi bir otoriter güç.

kulesidir; ancak özünde bir disiplin mekanıdır. Amaç, görünmeyen gözler ile gözetlenen mahkumların itaat etmelerini sağlamaktır. Sosyal disiplinin bir uygulama aracı olarak kullanılan bu hapishane modeli, yerleşim biçiminden hücrelere, aydınlatma sisteminden gözetleme kulesine kadar, itaatin ve teslimiyetin mimarisidir. Foucault (1992: 10, 16)'ya göre fiziki cezalandırma 19. yüzyılın başlarında seyirlik bir unsur olmaktan çıkarak ceza sisteminin gizli bir parçası haline gelmeye başlamıştır. İktidar düzenine göre gözetlemenin cezalandırmadan daha etkili ve verimli olduğu anlaşılmıştır. (Fouacult, 2003: 23). Bedeni gözaltında tutacak bir denetim teknolojisinin kurulması gerekmiş, (Fouacult, 2007: 95) böylece hapishaneler cezanın etrafını çevreleyen bir denetim merkezi haline gelmiştir. Faucault (1992: 171) disiplinin, bağımlı, itaatkar bedenler imal ettiğini ve iktidar ile ilişkili olduğunu belirtmektedir. Foucault, Panoptikon ile modernite arasındaki ilişkiselliği vurgulamakta, modern toplumu, sürekli bir gerilim ve mücadele alanı yaratan disipliner özelliğinden bahsetmektedir (akt. Dolgun, 2008: 106). Disiplinsel iktidar, yalnızca analitik ve 'hücresel' değildir, aynı zamanda doğal ve 'organik' olan bireysellikle iç içedir. Hiyerarşik, sürekli ve işlevsel gözetim ise kendisiyle birlikte taşıdığı yeni iktidar mekanizması sayesinde yaygınlaşmaktadır (Foucault 1992: 194, 222). "Gözetim, aynı anda hem üretim aygıtının bir iç parçası; hem de disiplinsel iktidarın uzmanlaşmış bir çarkı olduğu ölçüde, belirleyici bir ekonomik işlemci haline gelmektedir" (Foucault, 1992: 220). Gözetim altında tutma sürekli olarak bir kayıt sisteminden destek alırken, insanların tutumları üzerinde etkin olmakta ve kişiler üzerinde daha fazla nüfuz olanağı sağlamaktadır (Foucault 1992: 247, 257). Ayrıca Panoptikon, iktidar düzeneklerini toplumun bütününe yaymaktadır. İktidar yalnızca üstyapı da değil, altyapıda da işlemektedir (Çığ, 2016: 106). Bu durum; insan ilişkilerinde, bireyler arasında, aile bünyesinde, eğitim ilişkisinde ve siyasi yapıda etkili olabilecek bir iktidar ilişkileri ağının var olduğunun göstergesidir (Foucault, 2005: 224).

Tarihteki kapatma, baskı, disiplin ya da devamlı gözetim gibi ilkelerden farklı olarak Panoptikon, sistematik gözetim sayesinde herhangi bir baskıya gerek duymadan gözetlenen kişinin zihninde öğrenilmiş çaresizlik halini almakta, hapishane metaforu sürekli görünür olmanın yarattığı baskıyla iktidarı zihinlerde pekiştirmekte, kişiler iktidarın normlarına uygun şekilde hareket etmekte, iktidarın gözünü içselleştirerek ona göre davranmakta ve normalizasyon sürecini tamamlamaktadır (Akan, 2017: 788; Çaycı, 2017: 45; Çığ, 2016: 105). Panoptikon, iktidarın otomatik işleyişini sağlayan bilinçli ve sürekli bir görülebilirlik halini yaratmaktadır. Gözetim altında tutma, eylemi itibariyle kesintili olsa bile, sonuçları itibariyle süreklidir (Foucault 1992: 247, 257). Bauman (1999: 59)'a göre "Panoptikon, gücün ve kontrolün modernleşmesinin hayati öneme sahip yönlerinin mükemmele yakın bir

metaforudur". Uğur Dolgun (2008: 105)'a göre de "Panoptikon, mimari bir yapıyı ifade etmekten öte, bir sistemin mantığını ve toplumsal denetime yönelik işleyiş mekanizmalarını ortaya koyar. Bu iç dinamikleri ile tüm toplumu dönüştüren ve bireyleri sürekli gözetim altında tutan disipliner bir mekanizmadır".

Lyon, (1997; 2001; 2003) gözetim çalışmalarında Foucault'un önemli bir yere sahip olduğunu kabul etmiş ancak günümüzde gerçekleşen gözetimde tüketim ve bilişim teknolojileri gibi konuların dışarıda bırakılamayacağını söylemiştir. Ayrıca gözetimin giderek merkezsiz bir hale gelmesiyle Foucault'un teorisinin güncelliğini yitirdiğini ileri sürmektedir.

Lyon'un kişisel verilerin toplanıp işlenmesinin "verilerin toplandığı kişileri etkilemek ve yönetmek" amacıyla yapıldığı iddiası, çalışmanın bu boyutta ele alınması gerektiği kanısını güçlendirmektedir. Günümüz toplumlarını yalnızca Panoptikon kavramı ile anlamak artık olanaksız hale gelmiştir. Süperpanoptikon ve Sinoptikon, Panoptikona eşlik etmektedir (Öztürk, 2013: 133). Deleuze, modern kapitalizmde disiplinci iktidarın, insanların gitgide dışsal bir şiddet olmadan kendi kendilerini disipline ettikleri bir biçime dönüştüğünü ileri sürmekte, böylece toplumların 'özdenetim toplumu' haline dönüştüklerini söylemektedir (akt. Fuchs, 2015: 190). Önceleri gözetime daha çok disiplin açısından yaklaşılmış olsa da günümüz koşullarında gelişen teknoloji ve internetle birlikte bu disiplin mekanizması, rızaya dayalı bir karaktere büründürülmüştür. Böylece denetim esnek bir görünüme kavuşmuş, denetimin yarattığı baskı görünmez hale getirilmiş; denetlenenin de denetim karşısında tepkisi zayıflatılmıştır. Bütün bunlar denetimin dijitalleşmesinin yarattığı dönüşümlerle olanaklı hale gelmiştir. Bu dönüşümün en önemli nedeni de insanların gönüllü olarak gözetime katılmasıyla beraber, bedenlerin dijital olarak denetlenmesini ve gözetimin evrensel bir denetim mekanizması haline dönüşmesini sağlamaktır. Günümüzde gözetim, teknolojik gelişimle birlikte mimariden teknolojik aygıtlara doğru bir kayma yaşamış, mimari gözetimin yerini elektronik gözetim almış, "teknolojik panoptikon" ya da "post panoptikon" denilen dönemi başlatmıştır (Çoban, 2016: 111).

Baştürk (2016: 133, 135)'e göre post panoptikon, gözetimin yeni ve niteliksel olarak dönüşüme uğramış bir boyutunu temsil etmekte, gözetim teknikleri ve kültüründe yeni dönüşümleri betimlemek için kullanılmaktadır. Günümüz gözetim teknolojilerine ek olarak, bireyler hemen her gün kullandıkları enformasyon teknolojileri aracılığıyla, incelikli bir gözetime maruz kalmaktadırlar. Böylece bireyler kişisel bilgilerinin gizliliğini yitirmekte ve bu bilgilerin gönüllü dağıtıcısı konumuna gelmektedir (Güven, 2011: 173).

> Post panoptikon evresinde mekân düşüncesi genellikle soyut alanlar olarak tasavvur edilmiştir. Dijital ortamla, bireylere dair verilerin tutulduğu alanlar olarak yeni bir mekân düşüncesinin somutluğunu

> yansıtırlar. Ancak bu soyut mekânı panoptik mekandan ayıran en temel farklılık, bu dijital ortamların beden içermemesi, başka bir deyişle bireyin fiziksel varoluşunun ikincil plana atılarak inşa edilmesidir. Tercihler, zevkler, alışverişler, harcamalar, görüşmeler, konuşmalar, bulunulan yerler, vb. gibi bir dizi yaşamsal aktivite veri haline getirilerek dosyalanmakta ve bireye ait tanımlayıcı alan haline gelmektedir (Baştürk, 2016: 134).

Panoptikon'dan Süperpanoptikon'a geçiş, gözetim pratiklerinin değişerek genişlediğini ve gönüllü olarak gözetime dahil olan kişilerin gözetimin nesnesi ve sürecin lokomotifi haline geldiğini göstermektedir (Karakaya, 2014: 84). Günümüz teknolojisi, elektronik olarak, Panoptikon'un temel özelliklerinin yerini almakta ve Süperpanoptikon'u yaratmaktadır (Lyon, 1997: 265). Mark Poster tarafından ortaya atılan Süperpanoptikon kavramı, Foucault'nun panoptik modelinin eskisi kadar disipline olmaktan çıkması ile beraber bireylerin rızası ile gerçekleşmesi, herhangi bir sınırının bulunmaması ve her yerdeliği gibi özellikleri nedeniyle kabul görmüştür. Poster (1990)'a göre Süperpanoptikon, enformasyon teknolojileri ile bireylerin rızasını alarak gözetim altına almakta, bedenler siberuzamda hapsolmaktadır. Ancak rıza üretimi sadece enformasyon teknolojilerinin ürettiği bir durum değildir. İnsanların zihinsel olarak yönlendirilmesinde başka unsurlar da bulunmaktadır. Enformasyon teknolojileri, hali hazırda rıza üretimi ile yönlendirilen zihinlerin daha hızla ve yaygın biçimde ele geçirilmesine aracı olmuştur. Sayıları giderek artan elektronik cihaz ve yazılımlar, birbirleriyle ilişki kurmalarını sağlayacak kimlik numaraları taşımaktadır. Bu, üretimin talebe göre nasıl şekillendirilmesi gerektiğini önceden belirleyen, "tüketici gözetimi" için büyük avantaj sağlamaktadır (Lyon, 2006: 88). Tüketici gözetimi açısından değerlendirildiğinde de bilişim teknolojileri ile yapılan her türlü gözetleme ve kişilerin tüm hareketlerin izlenmesi, Süperpanoptikon modelini işaret etmektedir (Sönmez, 2016: 268).

Süperpanoptikon ile beraber gözetim pratikleri değişirken, kitle iletişim araçlarının etkili olduğu Sinoptikon dönemi karşımıza çıkmaktadır. Sinoptikon kavramını ise ilk kullanan Thomas Mathiesen'dir. Sinoptikon (Synoptic) 'Syn' ve 'optikon' eşzamanlı ve görme anlamına gelen kelimelerin bir araya gelmesiyle türetilmiştir ve Sinoptikonu gözetimcisi olmayan gözetim olarak nitelenmektedir (Mathiesen, 1997: 218, 220, 223). Panoptikon da azınlık çoğunluğu izlerken sinoptikon da çoğunluk azınlığı izlemektedir ve bu da kitle iletişim araçları ile mümkün olmaktadır. "Çoğunluğun azınlığı izleyerek kendi biçimlerini oluşturduğu bir toplumsallık biçimi olarak 'synopticon', görmenin ve görüntünün egemen olduğu bir iletişim dünyasının sonucudur" (Baştürk, 2016: 220). Sinoptikonda gözetim, disiplin ve iktidar uygulaması olmaktan çıkarak gündelik hayata nüfuz etmekte ve sürekli hale gelmektedir. Mathiesen medya ile gözetim arasında sıkı bir bağ bulunduğunu ileri sürerken çoğunluğun kitle

iletişim araçları ile azınlığı izleyerek bir hayran kültürü oluşturduğundan söz etmektedir. İnsanların ruh ve bedenleri bu yolla denetim altına alınmakta ve sindirilmektedir (Mathiesen 2004: 99). Mathiesen bu mekanizmayı "sessizce sessizleştirme" olarak tanımlamakta ve bu mekanizmanın bireyleri silikleştirdiğinden bahsetmektedir. Sinoptikon kavramında bedenlerin, insanların oturdukları yerde, yerellikten kopartılmayarak, siber mekana çekilerek, başkalarının hayatını gözetlediği bir gözetim süreci söz konusuyken, günümüzde internetin yaygınlaşmasıyla birlikte, Sinoptikondan "Omnioptikon"a geçilmiştir. Artık çoğunluğun 'birbirini izlediği' bir gözetim süreci söz konusudur (Arslantaş-Toktaş vd., 2012: 33).

Omnioptikon, Panoptikondan beri ortaya atılan görüşlerin daha çok sentezlenmiş ve günümüz şartlarına uyarlanmış olan hali olarak betimlenebilir. Emanuel Pimenta gözetimden bahsederken gözetleyen ve gözetlenen olarak ayrım yapmamış herkesin herkesi kontrol etmesinden bahsetmiştir. Pimenta'nın vurguladığı şey bireylerin gözetimdeki konumudur. Bireyler gözetim aygıtlarını ve mekanizmalarını gönüllüce kullanmakta, kendi bilgilerini paylaşmaktan çekinmemekte, başkalarını gözetleyerek onlar hakkındaki bilgileri de paylaşabilmekte böylece gözetim sistemine dahil olmaktadırlar (Karakaya, 2014: 99).

Gözetime ilişkin diğer bir kavram olan Ban-opticon'da bir profilleme söz konusudur. Didier Bigo (2006: 34) Ban-optikon'u, Jean Luc Nancy'nin Giorgio Agamben tarafından düzenlendiği şekliyle 'ban' (yasak) terimini Foucault tarafından kullanılan 'optikon' kavramıyla birleştirerek oluşturmuştur. Bigo (2006)'ya göre Ban-optikon, yanlış davranışı yakalamak için bireyleri veya grupları izlemek yerine tüm kötü olanları önlemeyi amaçlamaktadır. Ban-optikonun işlevi ise Panoptikon'nun tersine içeride tutmak değil dışarıda tutulacak olanların belirlenmesidir. Günümüzde mülteci meseleleri Ban-optikon'a örnek olabilmektedir; "zira mülteci kampları bir yandan mültecilerin ya da sığınmacıların içeri girmesini yasaklarken diğer yandan da bu 'yabancı' bedenleri tahakküm altına alan bir gözetim sistemidir" (Tekin, 2012: 76).

"Modernite içinde teknik gözetime ilk olarak, kapitalist sistem içindeki fabrika ve atölyelerde işçilerin sermaye adına disipline edilmeleri yoluyla rastlanmaktadır" (Dolgun, 2008: 77). Gözetime tarihsel bir çerçeveden bakıldığında da, modernitenin temel boyutlarından biri olarak görülmektedir. Bauman ve Lyon (2013: 13)'a göre modernite olduğu yerde durmamaktadır, bu nedenle de ne tür bir moderniteden bahsedildiği sorusu da sorulmalıdır. Bauman ve Lyon (2016: 13) bugünkü durumu ise geç modernite, postmodernite ya da akışkan modernite olarak tanımlamaktadır. Modernizm, aydınlanma projesi olarak tanımlanmakta ve insanın özgürleşmesi olarak çerçevelendirilmektedir. Modernizmde insanın özgürleşmesini sağlayacak temel araçlar bilim ve kuram olarak konumlandırılırken, çoklukla geçmişten kopuşu

ya da başka bir deyişle zaman sürecinde kırılmayı ifade edecek içerikle kullanılan postmodernizmde ise odaklanılan durum kaos ve süreksizliktir. Bu durumda belirleyici bir toplum kuramı olanaksızdır. Gerçekten de bugün yeni bir sosyokültürel durumla, yeni kuram ve olgularla, yeni bilgi ve kuram anlayışıyla karşı karşıya kalındığı söylenmektedir (Şaylan, 2002: 225, 232). Her şeyin pazar için piyasanın belirleyiciliği doğrultusunda kurgulandığı içinde yaşadığımız dönemde, tüketim asıl odak haline gelmiştir. Fredric Jameson da postmodern kültürü İkinci Dünya Savaşı sonrasındaki geç kapitalizm aşamasının, tüketim toplumunun kültürü olarak görmektedir (akt. Featherstone 2005: 40). Kitle iletişim araçları da gerek içerik gerekse kullanım yaygınlığını sağlayacak teknolojik gelişmelerle bu kültüre hizmet eden bir noktadadır. Dan Schiller (2000) yeni medyayı kapitalizmin dijitalleşmesi olarak görmektedir ve dijital ağların, kapitalist ekonomiyi global düzleme de yaydığını öne sürer. Kapitalizm giderek dijital kapitalizm halini almaktadır:

> Giderek zenginleşen kapitalist toplumda insanlar, daha önceleri başka insanlar ile yoğun iletişim içindeyken yeni, zengin tüketim toplumunda artık metalaşmış nesneler tarafından kuşatılmış bulunmaktadırlar. Böylece insanlar bir metalaşma ve nesneleşme dönüşümü içine girmişlerdir. Bireyler, tek bir meta almaya değil nesneler sistemi almaya özendirilmekte; böylece birey tüketim yoluyla kendini diğer bireylerden farklı kıldığını sandığı bir tanınma sürecine girmekte ama aynı zamanda tüketim toplumunun uyumlu bir parçası olarak onunla bütünleşmektedir (Şaylan, 2002: 238).

Yirminci yüzyılın son yıllarından itibaren tüketici gözetimi için gözetim teknolojilerinin yaygın bir şekilde kullanıldığına tanık olunmaktadır (Özarslan, 2016: 148). Dolgun (2004: 3)'a göre de *"yeni ekonomi tüketicilerin gözetimi üzerinde yükselmektedir"* ve tüketim toplumundaki en önemli amaç, ihtiyaçların, arzu ve isteklerin tatmin edilmesinden ziyade tüketicinin metalaştırılmasıdır, *"tüketiciler satılabilir mal statüsünde yükseltilmektedir"* (Bauman ve Lyon, 2013: 46). Tüketici gözetimi, tüketme düzeyine dayanan sosyal bölümlenmeleri yansıtmakta ve pekiştirmekte, bu durumun sonucu olarak da kişilerin tüketiminin sadece gelirine değil, birlikte yaşadığı, iletişim kurduğu sosyal çevresine bağlı olduğunu göstermektedir (Lyon, 1997: 217; Kıray, 2005: 15, 20). Tüketici gözetimi, zorlayıcı olmamakla birlikte kişilere tüketici becerilerini öğretme ve tüketme davranışı aşılamaktadır. Böylece toplumda gözetimin kitlesel boyuta ulaşmasını sağlamakta, teknolojik ilerlemeler de sürekli olarak gözetim kapasitesini artırmaktadır (Lyon, 1997: 217, 218). Tüketicilerin gözetlenmesinde önemli bir yer tutan gönüllü bilgi paylaşımı, kişinin gözetimine neden olmakta ve özel alanın metalaşmasını sağlamaktadır. Bu da şirketlerin ekonomik anlamda kendilerini biçimlendirmelerine yol açmaktadır. Çünkü gözetim teknolojilerine sahip olan şirketlerin

piyasada başarılı olma şansı daha fazladır. Kısacası farklı iktidarların gözleri artık her an herkesin üzerindedir (Özarslan, 2016: 148).

"Bireyi toplumuna bağlayan düzeneğin kendisi değişmiş ve toplumsal denetim ürettiği yeni gereksinimlerde demir atmıştır" (Marcuse, 2010: 28). Tüketim ise bir özgürlük alanı olarak düşünülmekte ve sınırsız seçim modern piyasanın özü haline gelmektedir. Kişileri yeni mallar almak için ayartmaya çalışan, insanların kişisel bilgilerini dur durak bilmeden eleyip dokuyanların amansız gözü, bir zamanlar kutsal olarak kabul edilen ve en mahrem yer olan evlere bile sızmaktadır (Lyon, 1997: 250, 252). İnternet aracılığı ile gerçekleşen bu 'sızma'nın sonucu olarak web 2.0'ın da bir pazarlama ideolojisi olduğu, web 2.0'ın altında yatan katılımcılık kavramının yalnızca sahte-katılımcılık olduğu, web 2.0'a büyük kuruluşlar ve ticari çıkarlar tarafından hükmedildiği, onun bir reklamcılık makinesi olduğu eleştirileri de getirilmektedir (Fuchs, 2011: 137).

Tüketici kültürü düşüncesinin itici gücü kitlesel pazarlamadır ve bu gücün arkasında ise kitlesel reklamcılık vardır (Chaney, 1999: 27). "Kapitalist sistem, tüketim üzerinden beslendiği için reklamlar aracılığıyla yaratılan yapay ihtiyaçlar, sistemin çarklarının dönmesine katkıda bulunmaktadır" (Taşkaya, 2009: 119). Reklamlar, bir yandan belli bir ürün ya da hizmetin satın alınmasını teşvik ederken, hem kapitalizmin ekonomik yeniden üretimine hizmet etmekte hem de sahip oldukları içerikleriyle kapitalizmin toplumsal yeniden üretimine hizmet eden bir toplumsallaşma işlevi görmektedir (Dağtaş, 2009: 19). Reklamlar, ürünleri sembolize eden işaretlere içkin anlamları düzenlerken bazen bir ideoloji kadar önem kazanmaktadır. Bu metanın ideolojisidir (Taşkaya, 2013: 30; Lefebvre, 2016: 121). "Reklam, sadece bir tüketim ideolojisi sumakla kalmaz; tüketici kimliğiyle doyuma ulaşan, kendini edimler yoluyla gerçekleştiren ve kendi imgesiyle (veya idealiyle) örtüşen tüketici 'ben'in bir tasarımını sunar" (Lefebvre, 2016: 104). Bireysel zevkler bir tutku haline getirilerek ortaklık duygusu zayıflatılırken yabancılaşma kuvvetlendirilir. Böylece reklam yol gösterici bir araçtan daha farklı bir hal almakta, günlük yaşamı denetim altına alıp toplumsal ilişkilere egemen olmaktadır (Berger, 1993: 57). "Tüketim ekseninde yeni anlamlar yaratma işlevini yerine getiren reklamcılık, tüketicilerin tutumları üzerinde gerçekleştirilen manipülasyonların en önemli aracı konumundadır" (Taşkaya, 2009: 104).

Tüketici, medya içeriği tüketirken bile tüketim emeği ortaya koymaktadır. İzleyici emeği kavramı da kitle iletişim araçlarında reklamcılık bağlamında ortaya çıkmıştır (Fisher, 2015: 52). Dallas Smythe, bu yüzden medyayı sermaye birikim zincirinde yaşamsal bir bileşen olarak konumlandırmıştır. Smythe, kitle iletişim araçlarında devam eden şeyin öncelikle medya içeriğinin izleyici tarafından tüketilmesi değil, izleyicilerin ilgisinin reklam verenlere satılması

olduğunu ve kişilerin ‘izleyici metalarına’ dönüştürüldüğünü ileri sürmektedir. (Fisher, 2015: 54; Arvidsson ve Bonini, 2015: 160). Son yıllarda Smythe’nin çalışmaları yeniden gündeme gelmiştir; çünkü günümüzde Facebook ve Google gibi ticari şirketler, kullanıcıların karşılığı ödenmemiş emeklerinden yararlanmaktadırlar (Fuchs, 2015: 115). Çalışmanın odak noktalarından birini oluşturan bir diğer konu da şirketlerin, kullanıcıların yalnızca internette geçirdiği zamanla değil, onların ilgili alanlarıyla, çevrimiçi davranışlarıyla, dijital izleriyle ve demografik verileri ile ilgilendiğidir. Çünkü tüm bu veriler de büyük şirketler tarafından kullanılmakta veya reklam verenlere birer meta olarak satılmaktadır.

**Çalışmanın Bölümleri**

Çalışma üç bölüm olarak tasarlanmış olup birinci bölümde kişisel verilerin korunmasıyla ilgili ulusal ve uluslararası düzenlemeler çerçevesinde bu kanunlara neden ihtiyaç duyulduğu, önemi ve gerekçeleri değerlendirilmiştir.

İkinci bölümde reklam, mobil ortam reklamları, kişiselleştirilmiş reklamlar, bu reklamlardaki kişiselleştirmenin nedenleri ve mobil ortam reklamlarındaki dijital gözetim algısına ilişkin yaklaşım, görüş ve değerlendirmeler ilgili literatür kapsamında ele alınmıştır.

Üçüncü bölümde ise mobil cihaz kullanan ve internete bu cihazlar ile erişen dijital göçmenler ve dijital yerliler, iki ayrı grup olarak belirlenmiş ve yüz yüze anket tekniği uygulanarak, toplamda 832 katılımcıya 45 adet soru yöneltilmiş ve bu iki grubun reklamlarındaki dijital gözetime ilişkin algı ve farkındalık düzeyleri karşılaştırmalı olarak analiz edilmiştir. Daha sonra araştırma bulgularına yer verilmiş, araştırma sonucu elde edilen bulgular, ilgili literatür bağlamında açıklanmış, sonuç bölümünde ise öneriler sunularak araştırma tamamlanmıştır.

# BİRİNCİ BÖLÜM
# ÖZEL HAYATIN GİZLİLİĞİ VE MAHREMİYET KAVRAMI BAĞLAMINDA KİŞİSEL VERİLERİN KORUNMASI İLE İLGİLİ ULUSAL, ULUSLARARASI DÜZENLEMELER VE 6698 SAYILI KİŞİSEL VERİLERİN KORUNMASI KANUNUNUN DEĞERLENDİRİLMESİ

Bilişim teknolojilerinde yaşanan gelişmeler doğrultusunda 'bilgi'nin 'güce' dönüşmesi, güç ilişkileri üzerine tartışmalara yeni boyutlar eklemiştir. Her türlü bilginin 'veri' haline dönüştürülerek dijital ortamlara aktarılmasıyla, kişiler kendilerine ait kişisel alanları korumakta güçlük çekmeye ve kişisel verilerin dijital ortamlara kişinin rızası dışında aktarılması, depolanması ve işlenmesinde yaşanan kontrolü kaybetmeye başlamıştır. Buradan hareketle 'kişisel veri' ile ilgili kavramlar etik, özel hayatın gizliliği ve mahremiyet bağlamında kişisel verilerin korunması ile ilgili ulusal ve uluslararası yasal düzenlemeler etrafında değerlendirilmiştir.

## 1.1. Özel Hayatın Gizliliği ve Mahremiyet Kavramı

Temelde insani bir hak olan özel hayatın gizliliği, günümüzde önem kazanan ve sürekli gündemde olan bir konudur. Gizliliği ve mahremiyeti ortadan kaldıran gözetim, kişileri toplumsal sınıflandırmaya tabi tutmakta, kişisel verilerin bu sınıflandırmada kullanılması ise dijital ortamda hak ihlallerine ve etik sorunlara yol açmaktadır. Özellikle de özel hayatın gizliliği ve mahremiyet hakkının ihlal edilmesi, dijital ortamların güvenilirliğinin sorgulanmasının da temel nedenlerindendir.

TDK'ya[8] göre özel hayat, "Kişinin kendine özgü yaşayışı, yaşama tarzı, kendisini ilgilendiren tutum ve davranışı, özel yaşamı" olarak tanımlanmaktadır. 4721 sayılı Türk Medeni Kanunu'nda[9] kişilik kavramına yer verilmekte, kişiliğin, kişiye bağlı ve hukukça korunan bedenini, manevi hukuki nitelikteki varlıklarını ifade etmekte, kişinin toplumda yer edinebilmesi ve kişiliğini serbestçe geliştirebilmesi için tüm maddi ve manevi değerler üzerindeki hak olarak tanımlanmaktadır (Civelek, 2011: 14). Hak kavramı ise bir kişi, kurum veya bir şey üzerindeki gerekçelendirilmiş bir iddia ve talebi ifade etmektedir (Ersoy, 2009: 4). Günümüz demokratik hukuk devletlerinde, kişi bir bütün olarak kabul edilmekte ve özel hayat da bu bütünün önemli bir parçası olarak kabul görmektedir (Kılınç, 2012: 1099).

[8] http://www.tdk.gov.tr/ (erişim tarihi: 01.03.2018).
[9] https://www.tbmm.gov.tr/kanunlar/k4721.html (erişim tarihi: 01.04.2018).

Özel hayatı ifade etmek üzere birçok terim kullanılmaktadır. Özel hayat kavramı ile ilgili terim farklılıkları, daha ziyade kişinin özel hayatını koruma altına alan temel hakkını ifade edilmesi ile ilgilidir. Özel hayat, gizlilik ekseninde mahrem alanı, bir başka deyişle yaşam alanını ifade etmek üzere de kullanılabilmektedir (Korkmaz, 2014: 100).

Gizlilik, mahremiyetin sınırlarını çizmektedir. Mahremiyet ise bir kimsenin kendi alanıdır ve özerkliğin göstergesidir (Bauman ve Lyon, 2016: 41). Mahremiyet, "kişinin herkesle paylaşamayacağı veya herhangi bir kimse ile paylaşmamak hakkının bulunduğu olay, inanç ve duygularının, isteği üzerine o kişiyle paylaşılması" durumunu ifade eden "intimacy" deyiminin karşılığı olarak kullanılmaktadır (Küzeci, 2010: 14).

Özel hayatın gizliliği de "bir bireyin kendisini diğerlerine açıp açmayacağına ve bunu yapacaksa ne ölçüde yapacağına karar verme hakkıdır" (Dijk, 2016: 172). Özel hayatın gizliliği, tüm demokratik hukuk devletlerince benimsenmiş olup bir anayasa hukuku ilkesidir (Kılınç, 2012: 1099).

Özel hayatın gizliliği ve mahremiyetin daha iyi anlaşılabilmesi açısından bu kavramlara aşağıda daha detaylı bir şekilde yer verilmiştir. Ayrıca özel hayata ilişkin düzenlemelerin konuyla ilgili kısımları bu başlık altında toplanarak alandaki karışıklık giderilmeye çalışılmıştır.

### 1.1.1. Özel Hayatın Gizliliği ve Yasal Düzenlemeler

Herkesin aleni yaşantısının yanında, kendi maddi ve manevi varlığının geliştirebilmesi ve uygun gördüğü şekilde yaşayabilmesi için başkasının denetim ve gözetiminden uzak, kendi tarzına göre yaşayabildiği bir özel hayatı olmalıdır[10]. Özel hayatın gizliliği tüm demokratik toplumlarda yasalarca korunmakta, gizliliğin ihlali halinde cezai yaptırımlar uygulanmaktadır. Ülkemizde de özel hayatın gizliliği anayasal bir haktır ve kanunla korunmaktadır.

Türkiye Cumhuriyeti Anayasası'nın[11] 20. maddesi, "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." ifadesiyle özel hayatın gizliliğine net bir şekilde dikkat çekmektedir. Türk Ceza Kanunu'nun[12] 9. Bölümü de **"**Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" için ayrılmıştır.

Avrupa Konseyi tarafından 4 Kasım 1950'de imzalanan ve 3 Eylül 1953'te yürürlüğe konulan temel hak ve özgürlükleri korumayı amaçlayan Avrupa İnsan Hakları Sözleşmesi'nin[13] 8. maddesinin 1. fıkrasında özel hayatın gizliliği ile ilgili olarak "Herkes özel ve aile hayatına,

[10] http://eski.barobirlik.org.tr /yayinlar/kitaplar/OzelYasaminGizliligi.pdf (erişim tarihi: 05.03.2018).
[11] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf (erişim tarihi: 01.04.2018).
[12] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (erişim tarihi: 01.04.2018).
[13] https://www.echr.coe.int/Documents/Convention_TUR.pdf (erişim tarihi: 01.04.2018).

konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir" hükmü bulunmaktadır. 2. fıkrada ise "Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli tedbir olması durumunda söz konusu olabilir" ibaresi yer almaktadır.

Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'nin 12. maddesinde "Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır" hükmü bulunmaktadır.[14]

BM'nin, özel hayatın korunmasına ilişkin teklifi 19 Aralık 1968 tarihinde "İnsan Hakları ve Bilimsel ve Teknolojik Gelişmeler"[15] başlığı altında genel kurula sunulduktan sonra 1970'te rapor haline getirilmiştir. Ayrıca 23 Mart 1976'da yayınlanan "Medeni ve Siyasi Haklar Uluslararası Sözleşmesi"[16] adlı ikinci bir rapor, özel hayatın gizliliği ve mahremiyeti açısından İnsan Hakları Evrensel Beyannamesinin 12. maddesine benzer şekilde düzenlenmiş uluslararası bir metindir. Bu raporun 17. maddesinde yine günümüz düzenlemelerine temel kaynak olan "Hiç kimsenin özel hayatına, ailesine, evine ya da yazışmalarına keyfi ya da kanuna aykırı şekilde müdahale edilemeyeceği gibi şerefine ve itibarına da yasa dışı saldırılarda bulunulamaz" hükmü yer almaktadır.

Avrupa Birliği Temel Haklar Şartı[17] Avrupa Birliği tarafından 7-8 Aralık 2000 tarihlerinde Fransa'nın Nice kentindeki zirvede onaylanmıştır. Metnin "Özgürlükler" başlığı altındaki 7. maddesi "Herkes, özel ve aile hayatına, evine ve iletişimine saygı gösterilmesi hakkına sahiptir.", 8. maddesinin 1. fıkrasında "Herkes, kendisi ile ilgili kişisel verilerin koruması hakkına sahiptir", 2. fıkrasında "Bu veriler, belirli amaçlar için ilgili kişinin rızasına veya kanunlarda düzenlenmiş meşru bir temele dayanarak işlenebilir. Herkesin kendisi ile ilgili toplanan verilere erişme ve düzeltme hakkı vardır", 3. fıkrasında ise "Bu kurallara uyma, bağımsız bir otoritenin denetimine tabidir" hükümleri mevcuttur.

Görüldüğü üzere hem ulusal hem de uluslararası düzenlemelerde özel hayatın gizliliğinin *temel bir hak* olduğu görülmektedir. Bunun yanı sıra kişinin kendisi ve çevresi ile ilgili hükümler de ulusal ve uluslararası düzenlemelerde yer almaktadır. Aile, konut

---

[14] http://www.un.org/en/universal-declaration-human-rights/ç (erişim tarihi: 02.04.2018).
[15] https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/244/10/IMG/NR024410.pdf?OpenElement (erişim tarihi: 01.04.2018).
[16] https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (erişim tarihi: 01.04.2018).
[17] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (erişim tarihi: 05.04.2018).

dokunulmazlığı ve haberleşme gibi temel konular vurgulanmıştır. Son olarak kişisel verilerin de özel hayatın gizliliği kapsamında değerlendirilmesiyle beraber kişisel verilerin korunmasının önemi de artmıştır.

Özel hayatın gizliliği kapsamında fiziksel bir alan olarak korunan konut yanında bilgisayar sistemlerinin kullanılmaya başlanması ile birlikte konutun düşünsel olarak genişlediği ifade edilmekte, düşünsel bir alanın varlığı da vurgulanmaktadır. Örneğin İtalyan Ceza Kanununda 'siber alan' konutla eş değer tutulmaktadır. Siber alan kişiye ait bir alan olarak kabul edilmiştir (Ketizmen, 2008: 87).

#### 1.1.1.1. Özel Hayatın Gizliliği Hakkı ve Özel Hayata İlişkin Yaklaşımlar

Özel hayatın gizliliği hakkı kişinin kendisi ile ilgili tüm bilgilerin gizli kalmasını istemesi, bu bilgilerin kaydedilmemesi ve kullanılmamasını talep etmesi hakkıdır. Oya Araslı, özel hayatın gizliliği hakkının "insanın insan olmasından doğan yüksek değeri" olduğunu belirtmektedir (akt. Akgül, 2013: 69). Sultan Üzeltürk'e göre de özel hayatın gizliliği hakkının korunması iki temel nedene dayandırılmaktadır: İlki, çağdaş toplumun artık moral değerlerle kontrol edilemeyen, bireysel hassasiyetleri güçlü ve buna saygı bekleyen, doğrudan insan ilişkileri zayıf olduğu için de başkalarının özelini, mahremini merak eden bir kitleden oluşmasıdır. İkincisi, teknolojinin gelişmesiyle beraber bireyin özel hayatına müdahale edebilecek gözetim araçların hızla yayılmasıdır (akt. Ersoy, 2009:11).

Eren Sözüer (2017: 51, 54)'e göre özel hayata ilişkin ileri sürülen dört adet yaklaşım vardır ve bu yaklaşımlar şöyledir:

1. **Yalnız bırakılma hakkı:** "Yalnız bırakılma hakkı"[18] ilk kez Samuel D. Warren ve Louis D. Brandeis tarafından kullanılmıştır. Yalnız bırakılma hakkı bireyin hayatını, müdahale edilemeden sürdürebilmesini ifade etmektedir. Bu yaklaşımda özel hayat bir tür inziva olarak görülmekte, özel yaşamın altında yatan değerin "kişiliğin dokunulmazlığı" olduğunu savunulmaktadır.
2. **Kişiye sınırlı ulaşım:** Üç unsurdan oluşmaktadır: Gizlilik, (başkalarının kişiyi ne kadar tanıdığı). Tek başına olma durumu (başkalarının kişiye fiziksel olarak ne kadar ulaşabildiği). Anonimlik (kişinin başkalarının ilgisinde ne kadar maruz kaldığı). Bireyin özel hayatın korunmasındaki menfaati bu unsurlarla ilişkilidir.
3. **Yakınlık (intimacy):** Özel hayatı, bireysel gelişimin yanında bireyler arası ilişkilerin geliştirilmesine dayanmaktadır. Bu teori özel hayatı, bireyin kurduğu ilişkileri yakınlık ve uzaklık derecelerine göre şekillendirir.

[18] http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (erişim tarihi: 08.04.2018).

4. **Bireyin kişisel bilgileri üzerindeki kontrolü:** Bu yaklaşım, kişisel bilginin korunmasına hukuki zemin oluşturması bakımından önem taşımakta, bireyin kendisine ait tüm bilgileri açıklayıp/açıklamama ya da paylaşıp/paylaşmama tercihi özel hayatı kapsamında korunmaktadır.

### 1.1.1.2. Unutulma Hakkı

Unutulma hakkı en sade haliyle, "bireyin geçmişte hukuka uygun olarak yayılmış ve doğru nitelikteki bilgilerinin, zamanın geçmesine bağlı olarak erişimden kaldırılmasını ya da gündeme getirilmemesini talep edebilmesidir" (Sözüer, 2017: 8). Kişisel verilerin korunmasında bireyin kişisel verilerine yönelik sildirme hakkı bulunmaktadır; ancak bu her zaman olanaklı olmamaktadır. Her türlü kişisel verinin sınırsız biçimde kayıt altına alındığı ve sonrasında hızlı ve geniş bir şekilde paylaşımı nedeniyle ortadan kaldırılmasının oldukça zor ve karmaşık olduğu göz önünde bulundurulduğunda; bireyin gözetimden kaçınma ve dolayısıyla yaşamını özgür bir şekilde sürdürebilme isteği, unutulma hakkına olan ihtiyacı ön plana çıkarmaktadır (Akgül, 2015: 15). Unutulma hakkı, özel hayat kapsamında korunan bir hukuki taleptir ve özel hayata ilişkin yaklaşımların ele alınması, unutulma hakkının özel hayat ile ilişkisinin ortaya konulması bakımından elzemdir. Unutulma hakkı bireyi, dijital ortamlarda süresiz olarak varlığını devam ettiren (İnternet ortamında kalıcı olarak saklanan) tüm bilgilerin zararlı etkilerinden korumaktadır (Sözüer, 2017: 16, 17, 50). Bu bağlamda, unutulma hakkının, bireyin geçmişi ile geleceğini serbestçe şekillendirmesi, dolayısıyla dijital ortamda kişisel verilerini özgürce kullanma veya diğer kimselere kullandırmama isteğinin doğal bir sonucu olduğu belirtebilir (Akgül, 2015: 17). Kişilerin İnternete aktardığı tüm bilgilerin yanı sıra farkında olarak ya da olmayarak bıraktığı tüm dijital izlerin ne zaman hangi şekillerde karşısına çıkacağı bilinmediğinden bu hakkın talep edilmesi hayati bir nitelik taşımaktadır. İnternet'in günümüzün en yaygın başvurulan bilgi kaynağı olduğu göz önünde bulundurulduğunda, unutulma hakkının önemi daha iyi anlaşılacaktır (Sözüer, 2017: 16, 17).

### 1.1.1.3. Mahremiyet Hakkı ve Mahremiyetin Dönüşümü

Bilgi bağlamında mahremiyet hakkı, bireye ait tüm bilginin onun "rızası olmaksızın açıklanması, yayılması ve bu bilgilere başkalarının ulaşamamasıdır" (Öncü, 2011: 182). Mahremiyet Komitesi Raporu'na[19] göre mahremiyet hakkının iki yönü bulunmaktadır. Bunlardan ilki, bireyin kendisi ve çevresine izinsiz dahil olunmaması özgürlüğü, ikincisi ise bilgi mahremiyeti, yani kendisiyle ilgili bilgilerin başkalarına nasıl ve ne ölçüde aktarılacağına

[19] https://onlinelibrary.wiley.com/doi/full/10.1111/j.1467-923X.1972.tb02068.x (erişim tarihi: 10.04.2018).

kendisi için karar verme hakkıdır. Mahremiyet gözetimin karşısındadır; ancak mahremiyetin korunması günümüz teknolojilerin gözetimin en önemli aracı olması sebebiyle pek olanaklı görülmemektedir. "Mahremiyet, gözetimle birlikte kesintiye uğramakta, gizliliğini ve anlamını yitirmektedir" (Çakır, 2015: 11).

Irwin Altman (1975)'a göre mahremiyet, insanların keşfettiği veya aldığı bilgileri kontrol etmek suretiyle yaşamda herhangi bir durumda arzu edilen mahremiyet seviyesine ulaşma girişiminde bulundukları bir süreçtir. Yani, insanlar süregelen açıklama ve saklama eylemleri aracılığıyla sır saklarlar, kendilerini ve sırlarını düzenlerler. Altman mahremiyeti çevre ve sosyal davranış çalışmasının merkezi olan dört ana kavramdan birisi olarak kavramsallaştırır: mahremiyet, kişisel alan, bölgeselcilik ve dışlama. Altman kişisel alan ve bölgeselci davranışı, insanların mahremiyet amaçları hizmetlerinde kişiler arası sınırları ve çevresel faktörleri düzenlemek için kullandıkları mekanizmalar olarak açıklar. Kişisel alan, "bir kişinin çevresindeki bir sınır ve genelde rahatsız edici ve genelde onaylanmamış olan şeye davetsiz bir giriş" olarak kavramsallaştırılmıştır. Kişisel alana davetsiz girişler veya saldırılar, gizlilik ihlalini yansıtır ve endişeden, mesafeyi büyütüp etkileşimi azaltmak üzere tasarlanmış eylemlere kadar tepki çeşitliliğiyle sonuçlanabilir. Bölgesel davranış, diğer bir sosyal düzenleme mekanizması türüdür. Altman'a göre hayvanlar beslenme ya da çiftleşme alanları konusunda nasıl bölgeciler ise, insanlar da belirli yerler ve nesneleri kişisel veya öncelikli bölge olarak varsayarlar. Öncelikli bölge, sahipliğin bir kişiselleştirme biçimi üzerinden edinildiği, belirli ihtiyaçları veya dürtüleri karşılayan bir alan, bir yer veya bir nesneyi ifade eder. Başka bir insanın öncelikli alanına girme, yalnızca izinle gerçekleştirilebilir ve izinsiz girme, yoğun duygusal tepki ve fiziksel eylem oluşturabilen bir istila olarak görülmektedir (akt. Shklovski vd., 2014: 2348).

Mahremiyetin yitirilişinin başlangıcı 1960'ların ortasına denk gelmektedir. "Mahremiyetin Ölümü" olarak adlandırılan bu dönemde, mahremiyetin yitirilişi giderek çeşitlenen tartışma ve yayınlarla öne çıkarılmıştır. Myron Brenton'ın 1964'te yayınlanan Mahremiyet İstilacıları,[20] [The Privacy Invaders] kişisel bilginin kontrolü ile ilgili tedbirlere dikkat çekmekte, aynı yıl Vance Packard'ın Çıplak Toplum'unda[21] [The Naked Society], "tek tek vatandaşlara uygulanan gözetlemenin muazzam ölçüde yoğunlaşmasından ve insanların mahremiyetleri üzerindeki büyük istila"yı tanımlamaktaydı. 1969'da "Şu anda" diye yazan Jerry Rosenberg, "bireyler ve örgütlerin birçok faaliyetini içeren bilgiyi, onlardan habersiz saklayacak, birleştirecek ve tek bir düğmeye dokunarak sınırsız erişim imkanına kavuşacak bir

[20] Brenton, M. (1964). The Privacy Invaders. New York: Coward-McCann.
[21] Packard, V. (1964). The Naked Society'McKay. New York.

ulusal bilgisayar sistemi planlanıyor"[22] diyerek günümüz teknolojilerinin ulaşacağı boyutları çok önceden belirtmiştir. Ulusal Sivil Haklar Konseyi'nin sponsor olduğu ve dijital veri bankalarının neden olacağı olumlu/olumsuz muhtemel sonuçlarıyla ilgili yayınlanan Gizlilik ve İnsan Hakları[23] [Privacy and Human Right] adlı makalede ise "toplum(un) uçurumun eşiğinde" olduğu sonucuna varılıyordu. 1970'lere gelindiğinde Arthur R. Miller, "toplumu şeffaf bir dünyaya dönüştürecek bir izleme sistemi"nden[24] bahsediyordu (Vincent, 2016: 178, 179).

1980'lerde İsveç'te nüfus sayımıyla ilgili yeni bir yöntem kullanılmasıyla ilgili kaygılar gün yüzüne çıkmaya başlamıştı (Lyon, 1997: 153). 1990'larda Mahremiyetin Sonu: Toplam İzleme Nasıl Gerçeğe Dönüşüyor[25] [The End of Privacy: How Total Surveillance Is Becoming a Reality], Veritabanı Ulusu: 21. Yüzyılda Mahremiyetin Ölümü[26] [Database Nation: The Death of Privacy in the 21st Century] gibi eserlerde mahremiyete ilişkin yazılardandı. 2000 yılında Micheal Fromkin "Hükümetler ve Şirketler Tarafından Mahremiyeti Ortadan Kaldıran Teknolojilerin Benimsenmesi"[27] başlıklı bir yazı kaleme aldı; 2006 yılında ise David Holtzman, Mahremiyetin Kaybı[28] [Privacy Lost] adlı çalışmasında, "Mahremiyetimiz kutuplardaki buzullardan daha hızlı ilerliyor; teknoloji onu hukuk sisteminin koruyabileceğinden daha hızlı eritiyor" ifadeleriyle konuya ilişkin düşüncelerini anlatmıştı. 2014'te Jacob Morgan "Şüphesiz öyle görünüyor ve bizler, onu bilmeden öldürenlerdeniz"[29] diyerek mahremiyetin yok oluşuna başka bir boyuttan bakmıştır (Vincent, 2016: 180, 181).

Günümüzde ise mahremiyetin ölümünden bahsetmektense mahremiyet anlayışının değiştiğinden bahsetmek daha doğru olacaktır. Bauman ve Lyon (2016: 35)'a göre "Mahrem olan her şey artık potansiyel olarak kamusal alanda yapılıyor ve kamunun tüketimine açık halde. Bunun nedeni de insanların neyin kamusal neyin mahrem olması gerektiği konusundaki anlayışlarının değişmesidir". İnternetin yaygınlaşmasıyla beraber, ev içindeki ilişkiler daha yalıtık ve daha bireysel haline gelirken, aile bireyleriyle bile paylaşılmaktan imtina edinilen özel ve mahrem bilgiler dijital ortamlarda yayınlanmakta ve adeta bir teşhir atmosferine neden olmaktadır (Çakır, 2015: 49). Sosyal medya kullanımının yaygınlaşmasıyla birlikte teşhirci mahremiyetin yükselişine tanık olunmaktadır (Vincent, 2016: 212). Sosyal medyada ortaya dökülen mahremiyet aslında paraya dönüşmektedir: "Facebook'ta da gördüğünüz gibi her bir

[22] Rosenberg, J. M. (1969). The Death of Privacy. Random House.
[23] Robertson, A. H. (1973). Privacy and Human Rights. University Press.
[24] Miller, A. R. (1971). Assault on Privacy.
[25] Whitaker, R. (1999). The End of Privacy: How Total Surveillance Is Becoming a Reality
[26] Garfinkel, S. (2000). Database Nation: The Death of Privacy in the 21st Century. " O'Reilly Media, Inc.".
[27] Froomkin, A. M. (2000). The Death of Privacy?. Stanford Law Review, 1461-1543.
[28] Holtzman, D. H. (2006). Privacy Lost. How Technology Is Endangering Your Privacy, Jossey-BassSan Francisco.
[29] https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#9c487031a77c (erişim tarihi: 10.04.2018).

sayfa reklamlarla dolu vaziyettedir". Bu ortamlardaki profiller ciddi bir piyasa değeri taşımaktadır (Uyanık, 2013: 9). Sosyal medyanın yanında, e-postalar, cep telefonu görüşmeleri ve bu ortamlardaki kişisel verilerin mahrem ilişkilerle ilgili daha zengin bir bilgi kaynağı sunduğu anlaşılmaktadır (Vincent, 2016: 213).

### 1.1.2. Haberleşmenin Gizliliği İle İlgili Düzenlemeler

Uluslararası düzeyde 12 Temmuz 2002 de kabul edilen Avrupa Parlamentosu ve Avrupa Konseyi tarafından "Kişisel verilerin işlenmesi ve Elektronik Haberleşme sektöründeki gizlilik ve mahremiyetin korunması 2002/58/EC Sayılı Direktifi"[30] önceki düzenlemelere göre daha güncel ve ayrıntılıdır. Daha önce yapılan düzenlemelere ek olarak elektronik haberleşme sektöründeki düzenlemeleri içermesi de diğer düzenlemelerden ayrılmaktadır. En göze çarpan madde ise 22. maddededir: "Kullanıcının rızası dışında internet trafik bilgilerinin saklanmasının yasaklanmasını, bilgilerinin gerekenden uzun sürede saklanmadığı ve gizliliğin garanti altına alındığı sürece yasaklamayı" hedeflememektedir. Bu maddede belirtildiği üzere kullanıcıların trafik bilgilerinin rızası dışında kaydedilmesi kaçınılmaz olacaktır. Trafik bilgileri kişinin hangi sitelere girdiğini, hangi işlemleri yaptığını veya hangi konumlarda bulunduğu vb. gibi verilerdir ve adeta kişiyi bir haritalandırmaya tabi tutmaktadır. Bu bağlamda trafik bilgisinin bir kişisel veri olduğu da açıktır. Burada yine şirketlerin lehine bir durum söz konusudur. Şirketler gizliliğin garanti altına alındığını ve bu bilgilerin uzun sürelerde saklanmadığını iddia ederek bu bilgilere istediği kadar erişme, işleme hakkını elde edebileceklerdir.

Direktifin 25. Maddesinde 'cookies' olarak adlandırılan çerezler'den "web sitesi trafiği ve online reklamcılığın etkinliğinin analiz edilmesinde ve kullanıcı kimliğinin doğrulanmasında meşru ve faydalı bir araç" olarak bahsedilmektedir. Kullanıcılara da "cookie ya da benzeri terminal ekipmanlarının saklanmasını reddetme fırsatı verilmelidir" denilmektedir. Bu maddede çerez'lerin faydalı bir araç olduğundan bahsedilmektedir. Ancak gerçek şudur ki bu fayda kişiler açısından değil şirketler açısından söz konusudur. Kullanıcılara bu araçların saklanmasını reddetme fırsatı verilmesi ise neredeyse imkansızdır. Çerezler ya otomatik olarak cihazlara kaydedilmektedir ya da gizlilik politikası ile hizmeti kullanan kişilere "bu hizmeti kullandığınızda çerezler'e izin vermiş olursunuz" uyarısı ile dayatılmaktadır. Kullanıcıların çerez'leri reddetmesi durumunda da verilen hizmeti kullanabilmeleri engellenmektedir. Çerez kullanımındaki sorunlardan biri de kullanıcının sabit diskinde kendisiyle ilgili yazılmış olan

[30] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (erişim tarihi: 01.04.2018).

bilgiye sahip olmayı ve bu bilgiye sonraki kullanım için tekrar ulaşabilmeyi isteyip istemediğidir (Özdilek, 2002: 186).

35. maddede ise "dijital mobil şebekelerde mobil kullanıcının coğrafi konum verileri haberleşmenin sağlanması için işlenir" hükmü yer almaktadır. Kişisel trafik verilerinin işlenmesi ise tamamen abonenin rızasıyla mümkün olmalıdır. Abonelerin rızası olsa bile istediğinde reddedebilmeleri gerekmektedir". Direktifte ayrıca "şirketlerin pazarlama faaliyetlerinde kişisel verileri koruma kurallarına riayet etmesi şartıyla bu verilerin kullanılmasının uygun olduğuna" işaret etmektedir. Özellikle son paragraf kişisel verilerin kullanımının kötüye kullanılabilmesi sonucunu doğurmaktadır: "Kişisel verileri koruma kurallarına riayet etmesi şartı" bu verilerin hangi amaçlarla kullanılabileceğini kapsamadığından önemli bir sorun teşkil etmektedir. Verilerin şirketin "pazarlama faaliyetleri" adı altında kendi çıkarına mı yoksa başka bir şirket ya da kuruluşun çıkarına mı kullanacağı açık değildir. Daha da açmak gerekirse, "Şirketin bu verileri pazarlama faaliyeti olarak başka bir şirkete pazarladığında da bu verilerin kullanılması uygun olacak mıdır?", sorusu akıllara gelmektedir.

#### 1.1.2.1. İnternet ve Haberleşmenin Gizliliği

İnternet'in bireysel anlamda kullanımı haberleşmenin gizliliği kapsamında değerlendirilmektedir. Bir haberleşme aracı olarak internetin kullanımı, Anayasanın 22. maddesine göre, ("Herkes, haberleşme hürriyetine sahiptir. Haberleşmenin gizliliği esastır.") haberleşme hürriyeti kapsamındadır (Ketizmen, 2008: 23).

5369 sayılı Evrensel Hizmetin Sağlanması ve Bazı Kanunlarda Değişiklik Yapılması Hakkında Kanun'un[31] 2. maddesinde internet, elektronik haberleşme hizmetini ifade etmektedir. Ayrıca 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun[32] bu alandaki ilk genel kanun olma özelliğini taşımaktadır.

### 1.2. Kişisel Veri Kavramı

Veri, işlenmemiş sistematik ham bir bilgidir. TDK'ya[33] göre veri, 'bilgi', 'data' olarak tanımlanmaktadır. Türkçe'de enformasyon ve bilgi kavramları karıştırılmakta olduğundan, bu kavramların da kısaca açıklanmasında fayda bulunmaktadır. Temel olarak veri (data),

[31] http://www.resmigazete.gov.tr/eskiler/2005/06/20050625-2.htm (erişim tarihi: 01.04.2018).
[32] http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (erişim tarihi: 10.04.2018).
[33] http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5accc689371c27.27581172 (erişim tarihi: 01.03.2018).

işlenmemiş (ham) enformasyon parçacıkları, Enformasyon (information) organize edilmiş bir veri seti, bilgi ise (knowledge) anlamlı enformasyonlardır (Akgün ve Keskin, 2003: 176). Kişisel veri ise kişiye ilişkin ayırt edici, tıpkı parmak izi gibi ona dair izler taşıyan ve tanımlayan her türlü bilgidir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda[34] da kişisel veri, "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" olarak tanımlanmıştır. Doğrudan veya dolaylı olarak kişilerin ırkını ve etnik kökenini, siyasi eğilimi, dini inançlarını, sağlık ve cinsel yaşamını ortaya çıkaran verilere de hassas veri denmektedir (Kaya, 2011: 318). 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 6. maddesinde ise hassas veriler, özel nitelikli veriler olarak geçmektedir.

Kişisel veri kavramına verilebilecek örnekler en sade hali ile kişilerin adı-soyadı, kimlik numarası, iletişim bilgileri ve benzeridir. Ancak günümüzde kişisel veriler dijital ortamlarda farkında olunmadan dijital iz olarak bırakılmakta, depolanmakta ve üçüncü kişilerle paylaşılabilmektedir. Dijital iz, dijital ortamlarda yaptığımız günlük aktivitelerimizde arkamızda bıraktığımız elektronik işaretlerdir. Bu izlere verilebilecek örnekler görseller, yazılar, sosyal medyadaki etiketler, kredi kartı bilgileri, şifreler, IP adresleri, interneti kullanım alışkanlıkları, alışveriş tercihleri, davranışları gibi daha da çok detaylandırılabilecek bilgilerdir. Kişisel veriler hem elle hem de dijital olarak işlenebilmektedir. Günümüzde neredeyse tüm veriler dijital bilgi olarak dijital ortamlara aktarılmaktadır. "Dijital bilgi, mikro işlemcilerden 'bit'lere[35], çeşitli devrelerce elektronik sinyallere dönüştürülmüş verilerdir" (Wayne, 2006: 57). Verilerin aktarılması da veri iletişimi terimiyle açıklanabilir ve bir kablo, radyo dalgası ya da ışık demeti gibi fiziksel bir iletişim aracı boyunca bilgi göndermek için yapılan düşük seviyeli mekanizmaları ve teknolojileri üzerinde yapılan çalışmaları ifade eder (Comer, 2016: 3).

Literatürde kişisel verinin belirli bir kişiyle ilgili olduğu, bilgi kaynağı belirsizse; yani anonimse koruma altına alınmadığından bahsedilmektedir. Ancak teknolojik uygulamalarla bu anonim bilgiden bile kişisel birtakım izler bulunabilmektedir. Örneğin takip edilemeyen bir tarayıcı kullanan ya da VPN[36] gibi uygulamalar ile internete bağlanan bir kullanıcının hangi internet sitelerine girdiği, hangi dosyayı indirdiği veya hangi haberleri hangi saatlerde okuduğu istatistiksel olarak hesaplanabilmekte ve bu bilgiler daha önce hangi IP adresinden, hangi konumdan, hangi tarayıcıdan işlem yapıldıysa bu bilgiler ile eşlenebilmektedir. Buna örnek verilmesi gerekirse; kişi anonim olarak gezindiği sırada Google şirketinin 'Gmail' hizmetini kullanmış olsun. Burada oturum açtığında kişinin anonim olarak internete girmediği zamanlarda nerelerden bu hizmete erişildiği bilinmekte, hangi haber sitelerine girdiği veya

[34] www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (erişim tarihi: 01.04.2018).
[35] Data Birimi.
[36] Sanal Özel Ağ.

hangi medyayı takip ettiği daha önce kaydedilmiş olduğundan, kullanıcının bu tarz uygulamaları kullandığında anonim olarak gezinmesinin pek bir şey ifade etmediği görülmektedir. Gelinen noktada dijital ortamlarda bıraktığımız dijital izlerin korunması gerekmekte, bu izlerin de kişisel veri kapsamında değerlendirilmesi önem taşımaktadır.

Veri, günümüzde ekonomik değer biçimi yaratmak için kullanılan bir hammadde, ekonomik girdi halini almıştır (Schönberger-Mayer ve Cukier, 2013: 13). Dijital ortamlara aktarılan kişisel verilerin denetimi ve kullanılması, şirketlerin ekonomik amaçlarına hizmet eden ana aktiviteler haline gelmiştir. Gözetleme şu anda sadece geçmişin hareketlerini izlemekle kalmamakta, aynı zamanda gelecekteki olayları da tahmin etmeye çalışmaktadır (Lyon, 2006: 181). Örneğin uçak seyahatlerinde koridordaki koltukları tercih eden insanların başkalarına yardım etme, hayır işleri söz konusu olduğunda daha bonkör olduğu bilinmesi kişisel verilerden çıkan anlamlar sayesindedir. Hatta bireylerin kredi kartı kullanım alışkanlıklarına bakılarak ve bu izlerin takip edilerek, ertesi gün nerede olacaklarının bile tahmin edilebileceği iddia edilmektedir (Türkoğlu, 2010: 7).

Veri, 21. yüzyılın petrolüdür ve çevrimiçi izleme de davranış, hareketler ve tercihlerden üretilen bu petrolü çıkarmak için gereken ana teknolojilerden biri çerezlerdir.[37] Kişiler ağlara bağlandığı anda çerezler, davranışlarla ilgili bilgi toplanmakta, depolanmakta ve farklı amaçlara hizmet eden sayısız algoritma[38] tarafından analiz edilmektedir. Davranışlar, ilgi alanları ve tercihler ilgili veriler de şüphesiz oradaki en değerli veri setidir.[39]

OECD Genel Sekreteri Angel Gurría'nın, "İnternet Ekonomisinin Geleceği Üzerine"[40] konulu toplantıda kişisel verilerin önemini vurgularken bu verileri internet ekonomisinin "para birimi"ne benzetmiştir. Çevrimiçi depolanan kişisel verilerin birikmiş mali değerinin ise 2020'ye kadar yıllık 1 trilyon Euro'ya ulaşabileceği tahmin edilmektedir.[41] Tüm bu nedenlerden ötürü küresel şirketlerin çoğu, satabileceği veya kullanabileceği belirli bir kişisel veri miktarı içeriğini sağlama anlayışı için stratejiler geliştirmekte ve iş modellerini değiştirmektedir.[42]

Kişisel verilerin para birimi olarak konumlandırılması, kişisel verileri korumanın ne kadar önemli olduğunu gözler önüne sermektedir. Kişisel veri konusunun daha iyi

---

[37] https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).
[38] Bir sorunu çözmek veya belirlenmiş bir amaca ulaşmak için tasarlanan yola, takip edilen işlem basamakları.
[39] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).
[40] http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinternetecono my.htm (erişim tarihi: 01.04.2018).
[41] http://www.ft.com/cms/s/0/5fd7d8a8-28e5-11e2-b92c-00144feabdc0.html (erişim tarihi: 20.05.2018).
[42] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

anlaşılabilmesi açısından "büyük veri" ve "veri madenciliği" kavramlarının açıklanmasını gerekli kıldığından bu kavramlara aşağıda yer verilmiştir.

### 1.2.1. Büyük Veri (Big Data) ve Üst Veri (Meta Data) Kavramları

Veritabanları, dijital teknolojilerin gelişmesiyle birlikte giderek önem kazanmaktadır. Veritabanı, birbiriyle ilişkisi olan verilerin tutulduğu, veriler topluluğunun mantıksal ve fiziksel olarak tanımlarının yer aldığı bilgi depolarıdır (Şentürk, 2006: 4). Analog dönemde verilerin toplanması ve analiz edilmesi giderek daha zorlaşmış, sayısallaştırma büyük veriye geçişi sağlamak için önemli hale gelmiş, bilgisayar sistemlerinin kişisel verileri kaydetme ve işleme kapasitesi giderek artmıştır. Bilgisayar sistemleri bünyesinde yer alan kişisel veriler öyle büyük bir ölçeğe ulaşmıştır ki kavranması olanaksız hale gelmiştir (Alternatif Bilişim Derneği, 2013: 12; Mayer-Schönberger ve Cukier, 2013: 22, 23). Günümüzde Google, Facebook, Microsoft vb. gibi büyük şirketler birer veri tabanı haline dönüşmüştür. Çünkü bu şirketler çok büyük ölçeklere ulaşan veriyi devamlı olarak kaydedebilme ve işleyebilme potansiyeline sahiptir. Endüstri analisti John Battelle, 2005 yılında yaptığı çalışmada Google'ı "niyetler veritabanı", "her tür amaç için keşfedilebilen, mahkeme çağrısı oluşturabilen, arşivlenebilen, takip edilebilen ve istismar edilebilen arzu, ihtiyaç, istek ve tercihleri içeren çok büyük bir tıklama veritabanı" olarak tanımlamıştır[43].

Büyük Veri; kullanıcıların internetteki tüm aktivitelerinden toplanan veridir ve anlamlı hale getirilerek işlenmektedir. Büyük Veri, tek bir sunucu veya sınırlı sayıda bilgisayarla yönetilemeyen veya analiz edilemeyen ve çok yüksek miktarda belirli ya da belirsiz kaynaktan gelen veri kitlelerini ifade etmek için kullanılmaktadır (Alternatif Bilişim Derneği, 2013: 11). Başka bir tanıma göre Büyük Veri; sosyal medya paylaşımları, mobil cihazlarla gerçekleştirilen arama kayıtları, her türlü fotoğraf, video, doküman, parmak izi, dijital sertifika, ağ konumu, sosyal medya verileri vb. gibi farklı kaynaklardan elde edilen verilerin anlamlı ve işlenebilir hale dönüştürülmüş biçimidir (Eyüpoğlu vd., 2017: 177).

Üst veri ise kısaca, belirli bir veri hakkındaki bilgilerdir. Belirli bir veri seti ya da kaynak hakkında nasıl, ne zaman ve kim tarafından oluşturulduğu hakkında tanımlayıcı bilgiler içermektedir. Üst veriyi örneklendirmek gerekirse; saat kaçta, nereden, hangi baz istasyonunu kullanarak arama yapıldığı, arama yapılan IMEI numarası, ne kadar süre konuşulduğu gibi bilgileri içerir**.** Herhangi bir e-posta gönderildiğinde postaya nereden ve ne zaman erişildiği, IP adresi, yazı karakter kodu, sunucu transfer bilgisi gibi detaylı bilgileri içermektedir.[44] Üst veri,

---

[43] http://networkcultures.org/query/wp-content/uploads/sites/4/2014/06/1.Kylie_Jarrett.pdf (erişim tarihi: 20.05.2018).

[44] https://network23.org/kame/2014/03/19/tib-ve-metadata/ (erişim tarihi: 04.05.2018).

tek bir veri ya da belirli bir dijital varlık hakkında ayrıntılı bilgi sağlarken, büyük veri, tüm verilerdeki detaylı bilgilerin yanı sıra, kişilerin tüketim kalıpları ve eğilimlerini keşfetme olanağı vermektedir. Büyük veri, çok büyük bir veri yığınıdır ve standart teknoloji araçlarıyla incelenemezken üst veriyi incelemek daha kolay olabilmektedir: "Üst veri iğne ise, büyük veri samanlıktır".[45] 2014 yılında Edward Snowden şöyle bir açıklama yapmıştır:

> Üst veri, olağanüstü bir biçimde müdahalecidir. Bir analizci olarak içerik yerine üst veriye bakmayı tercih ederim, çünkü o daha hızlı ve kolay, ayrıca yalan da söylemiyor… Eğer telefon konuşmanızı dinliyorsam, öylesine konuşuyormuş gibi yapabilirsiniz, kodlar kullanabilirsiniz. Fakat eğer üst verinize bakıyorsam, hangi numaranın hangi numarayı aradığını biliyor olurum. Hangi bilgisayarın hangi bilgisayarla konuştuğunu biliyor olurum.[46]

Amerika Birleşik Devletleri Ulusal Güvenlik Teşkilatında Genel Danışman olan Stewart Baker şöyle demiştir: "*Üst veri kesinlikle bir insanın yaşamı hakkında her şeyi söylüyor. Eğer yeterli üst veriniz varsa, içeriğe ihtiyacınız kalmaz*".[47]

Şirketler, büyük verilerde yer alan kişisel verilerin güvenliğini ve kişilerin mahremiyetini sağlamak için çeşitli kimliksizleştirme (anonim hale getirme) yöntemleri kullanmaktadır. Ayrıca güvenliği ve mahremiyeti garanti altına almak için en yaygın çözüm ise yazılı taahhütler olmaktadır. Fakat bu çözümün de çok başarılı olduğu söylenememektedir. Şifreler, denetimli erişim ve iki-faktörlü kimlik doğrulama (2FA)[48]; veri dinamik ve dağıtık veri sistemlerinde paylaşıldığı ve bir araya getirildiğinde güvenliği ve gizliliği sağlamak için düzenli olarak kullanılan teknik çözümler olsa da yeterli değildir (Eyüpoğlu vd., 2017: 177).

### 1.2.2. Veri Madenciliği

Veri madenciliği, birçok araştırmacı tarafından "özbilgi keşfi" ile eşdeğer olarak kullanılmakta, bazı araştırmacılar tarafından da veri tabanlarındaki özbilgi keşif ve analiz süreci olarak değerlendirilmektedir (Şentürk, 2006: 2; Karacan ve Yeşilbudak, 2010: 18).

Oded Maimon ve Lior Rokach'a göre veri madenciliği, veri yığınları arasından istatistik ve matematik teknikleri kullanılarak verilerdeki gizli örüntüleri çözmeye yarayan, fark edilmesi güç ilişkileri açığa çıkaran, ileriye yönelik tahminler yapılmasını sağlayan ve bu alanda kurallar üreten veri tabanı teknolojisi ve tekniklerin uygulanmasını ifade etmektedir (akt. Çuhadar, 2011: 1449). Toplanan verilerin niceliksel artışı, bunların içerisinden kullanışlı olanların

[45] https://www.linkedin.com/pulse/big-data-vs-metadata-whats-difference-toby-martin (erişim tarihi: 04.05.2018).
[46] https://labs.rs/en/invisible-infrastructures-data-flow/ (erişim tarihi: 15.12.2017).
[47] https://labs.rs/en/invisible-infrastructures-data-flow/ (erişim tarihi: 15.12.2017).
[48] İki Faktörlü Doğrulama.

bulunmasını zorlaştırmaktadır. Bu zorluğun "veri madenciliği" (data mining) ile aşıldığı görülmektedir (Küzeci, 2010: 29). Sahip olunan çok büyük miktardaki veriden, karar vericinin etkin bir şekilde ve daha fazla bilgiye dayalı karar vermesinde kullanılabilmesi amacıyla gizli, örtük, ilişkili, bağıntı veya trendlerin otomatik ya da yarı otomatik bir biçimde ortaya çıkarılmasıdır (Şentürk, 2006: 4). Kısaca veri madenciliği, veri tabanlarından elde edilen bilgiyi yapılandırarak, bilgi keşfedilmesini sağlayan araçlar ve teknikler olarak nitelendirilebilir (Civelek, 2011: 42). Veri madenciliği ile ilgili tüm bu tanımlamalar göstermektedir ki hiç durmadan artan bu veri yığınlarının işlenmesinin gün geçtikçe zorlaşacağı öngörülmekte, veri madenciliğinin öneminin de ileride daha iyi anlaşılacağı ve konu ile ilgili yapılan çalışmaların da artış göstereceği düşünülmektedir.

### 1.2.3. Kişisel Verilerin Korunması ve Önemi

Bilgi güvenliği elektronik ortamdaki verilerin gizliliğinin ve bütünlüğünün teknik olanaklar vasıtasıyla korunması ve sadece yetkili kişilerce kullanımının sağlanmasını ifade etmektedir. Kavramdan genellikle sadece bilginin gizliliği ve şifrelenmesi anlaşılsa da, bilgi güvenliği bu verilere erişim kontrolü ve verilerin değiştirilmesinin önlenmesini de içermektedir (Ersoy, 2009: 23).

Veri, ilk bakışta kişisel bilgi olarak görünmemekte; ancak büyük veri süreciyle geriye doğru iz takibi yapılarak kişiye ulaşılabilmekte, kişinin hayatıyla ilgili gizli ayrıntılar ortaya çıkarılabilmektedir: Büyük Veri, mahremiyeti yok etmekte, özgürlüğü tehdit etmektedir (Mayer-Schönberger ve Cukier, 2013: 159, 170).

> Kişisel verilerin korunması verinin korunması değil, kişiyle ilgili verilerin işlenmesi nedeniyle bireyin özgürlüğünün korunmasıdır; bir başka deyişle veri güvenliği sorunu değil, bir özgürlük sorunudur. Bu nedenle kişisel verilerin korunması konusunun, genel olarak bilişim ile ilgili konular arasında yer almakla birlikte, asıl olarak bir üst kavram olan "gözetim"in bir parçası olarak ele alınması ve incelenmesi gerekir. Aksi halde konu, verinin korunması yani güvenlik ve gizlilik konusuna sıkışır ki, bu da temel sorunun gözden kaçırılması sonucuna yol açabilir. Bu haliyle, gözetime bir tepki olarak kişisel verilerin korunması, bireylerin özgürlüklerinin korunması ve bunun karsısında da kurum ve kuruluşların kişisel veriler konusunda sorumluluk ve yükümlülüklerinin belirlenmesi anlamına gelmektedir (Türkiye Bilişim Derneği, 2008: 5).

Gelinen noktada kişisel verileri korumanın, özel hayatın gizliliği ve mahremiyeti korumayla eşdeğer olduğu görülmektedir. Kişisel verilerin korunmasıyla ilgili uluslararası ve ulusal düzenlemelere de aşağıda yer verilmiş ve değerlendirmeler sunulmuştur.

## 1.3. Kişisel Verilerin Korunmasıyla İlgili Düzenlemeler

Verinin korunması ile ilgili dünyada ilk yasal düzenleme 1970 yılında Federal Almanya'nın Hesseb eyaletinde yapılmıştır. Bu düzenleme ilk veri koruma otoritesi olan Veri Güvenlik Ofisi (Datenschutzbeauftragter) tarafından kurulmuştur (Civelek, 2011: 9). Uluslararası ve ulusal kaynaklarda, temel hak ve özgürlükler arasında, kişisel verilerin korunması, bireylerin özel hayatlarındaki gizliliğin bir parçası olarak görülmekte, bireylerin kişisel verileri üzerindeki kontrolü sağlamasının önemi vurgulanmaktadır (Korkmaz, 2016: 149).

### 1.3.1. Uluslararası Düzenlemeler

Genel olarak uluslararası düzenlemeler hem kişisel verilerin korunması hakkının temel garantilerini hem de kişisel verilerin işlenmesinin temel ilkelerini ortaya koymaktadır (Şimşek, 2008: 218). Avrupa düzenlemelerinden ayrı olarak ABD, veri koruma mevzuatı yaklaşımından ziyade, sektörel ve ilgili mevzuattan oluşan karma bir mevzuat tercih etmektedir. AB yasalarına göre, kişisel verilerin korunması temel bir hak olarak kabul edilmekte ve bu alandaki yasal düzenlemeler bireylerin çıkarlarını, işletmelerin meşru ihtiyaçlarıyla müşteri verilerinden değer elde etmesini dengelemeye çalışmaktadır. ABD'de ise hükümet, özellikle ifade söz konusu olduğunda anayasal olarak özel sektöre müdahale etmemektedir. Dolayısıyla sistem, kişisel bilgilerin korunmasına daha az önem göstermektedir (Cleff, 2008: 424).

#### 1.3.1.1. Avrupa Konseyi

Avrupa Konseyi, insan hakları, hukukun üstünlüğü ve çoğulcu demokrasi ilkelerini korumak ve güçlendirmek üzere 5 Mayıs 1949 tarihinde kurulmuş uluslararası bir örgüttür.[49]AK, kişisel verilerin korunmasıyla ilgili 28 Ocak 1981 tarihli "Kişisel Verilerin Otomatik İşlenmesi ile İlgili Bireylerin Korunması Sözleşmesi"[50] kişisel verilerin toplanması, kaydedilmesi ve işlenmesinde kötüye kullanımlara karşı bireyi koruyan ilk bağlayıcı uluslararası sözleşmedir. Bu sözleşmede kişisel verilerin toplanması ve işlenmesi ile ilgili hassas verilerin kaydedilmesinin uygun olmadığı durumlarda engellenmesi gerektiği; ancak çıkarların gözetilmesi durumunda (güvenlik ve savunma) mümkün olacağına dikkat çekilmektedir. Ayrıca sözleşme gerektiği kadar verinin saklanması, verilere yetkisiz erişimin engellenerek veri güvenliğinin sağlanması, kişilerin, verilerinin saklandığını ya da işlendiğini bilmesinin sağlanması, kişilerin gerektiğinde bu verilerin silinmesini talep etme ya da düzeltilmesi hakkının bulunması gerektiğini içermektedir.

---

[49] http://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa (erişim tarihi: 04.04.2018).
[50] https://rm.coe.int/1680078b37 (erişim tarihi: 04.04.2018).

### 1.3.1.2. Avrupa Birliği

7 Şubat 1992 tarihinde imzalanan Maastricht Antlaşması ile kurulan AB 28 üye ülkeden oluşmaktadır. 24 Ekim 1995 tarih ve 95/46/EC sayılı Kişisel Verilerin İşlenmesi ve Bu Verilerin Dolaşımı Konusunda Bireylerin Korunması Direktifi'nin[51] amacı AB üye ülkelerinin mevzuatlarının düzenlenerek, uyumlu hale getirilmesi ve kişisel verilerin bu doğrultuda korunmasının sağlanmasıdır.

Direktifte, gelişen teknolojiyle kişisel verilerin işlenmesine sıklıkla başvurulmakta, sınır ötesi akışın telekomünikasyon ağları ile kolaylaştığından bahsedilmektedir. Kişilerin uyruğu ne olursa olsun temel hak ve hürriyetlerin gözetilmesi, özellikle mahremiyetine saygı gösterilmesi vurgulanmıştır.

### 1.3.1.3. OECD

Dünya halklarının refahını ve ekonomik kalkınmasını sağlamayı amaçlayan OEEC'in[52] devamı niteliğinde 30 Eylül 1961 yılında kurulan ve bugün 34 üyesi bulunan Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD)'na üye ülkeler tarafından yürütülen çalışmalar sonucu 23 Eylül 1982 tarihinde "Kişisel Verilerin Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeler"[53] başlığı ile yayınlanan metne göre; kişisel verilerin toplanmasına sınırlamalar getirilmeli ve bu tür veriler uygun, adil araçlarla kişinin bilgisi ve rızası dahilinde alınmalıdır. Kişisel veriler kullanım amaçlarıyla ilgili olmalı, başka amaçlar için kullanılmamalı ya da kullandırılmamalıdır. Kişisel verilere erişim, değiştirme, yasadışı kullanma gibi durumlara karşı her türlü güvenlik önlemlerinin alınması gerekmektedir. Kişisel verilere ilişkin uygulamalar ve politikalar açıkça belirtilmelidir.

### 1.3.1.4. Birleşmiş Milletler

Birleşmiş Milletler 24 Ekim 1945 tarihinde dünya barışını ve güvenliğini korumak amacıyla kurulan uluslararası bir örgüttür. BM tarafından hazırlanan ve 14 Aralık 1990 tarih ve 45/95 sayılı genel kurul kararıyla kabul edilen "Dijital Ortama Aktarılmış Kişisel Veri Dosyalarının Düzenlenmesine İlişkin İlkeler"[54] adlı belgede 10 maddede kişisel verilerin korunması, verilerin toplanması ve işlenmesinde adaletli olunması ve yasalara uygun olması

---

[51] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (erişim tarihi: 04.04.2018).
[52] https://www.britannica.com/topic/Organisation-for-European-Economic-Co-operation (erişim tarihi: 27.05.2018).
[53] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (erişim tarihi: 01.04.2018).
[54] http://www.refworld.org/pdfid/3ddcafaac.pdfß (erişim tarihi: 04.04.2018).

konusuna vurgu yapılmıştır. Gizliliğin korunması, kötüye kullanımın engellenmesi, denetim ve yaptırımlardan sorumlu makamların kurulması gerekliliğine dikkat çekilmiştir.

BM'nin bu düzenlemelerinin hukuki açıdan bağlayıcılığı bulunmasa da bir tavsiye niteliği taşımaktadır ve uluslararası düzeyde birtakım ideallere hizmet etmesi bakımından da uluslararası alanda öneme sahiptir (Özdemir, 2009: 18).

### 1.3.2. Ulusal Düzenlemeler

Günümüze dek uluslararası düzeyde birçok düzenleme ile koruma altına alınan kişisel veriler teknolojinin gelişmesiyle daha da önemli hale gelmiş, ülkemizde de bu alandaki boşluk hem Türkiye Cumhuriyeti Anayasası'na eklenen ek maddeyle hem de 6698 sayılı Kişisel Verilerin Korunması Kanunu[55] ile doldurulmuştur. Kişisel verilerin kaydedilmesi, işlenmesi ve aktarılmasıyla ilgili düzenlemelerle bu veriler koruma altına alınmıştır. Ayrıca diğer ulusal düzenlemelere de aşağıda yer verilmiştir.

#### 1.3.2.1. Anayasal Düzenlemeler

Anayasanın 20. maddesine ek olarak 2010 yılında kişisel verilerin korunmasıyla ilgili ek fıkra eklenmiştir: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" hükmüne yer verilmiştir.

#### 1.3.2.2. 5237 Sayılı Türk Ceza Kanunu

5237 sayılı Türk Ceza Kanunu'nun 135. maddesi kişisel verilerin kaydedilmesi ve hassas verilerle ilgili cezalara ayrılmıştır. TCK'nın 136. maddesinde ise kişisel verileri hukuka aykırı olarak ele geçiren ve yayan kişilerle ilgili cezalar yer almakta, 138. maddede ise veri sorumlularının verileri yok etmemesi halinde veri sorumlularına verilecek olan cezalar bulunmaktadır. Bu maddeler aşağıda belirtilmiştir:

TCK'nın 135. maddesinin 1. fıkrasına göre hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.

TCK'nın 135. maddesinin 2. fıkrasına göre kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına,

[55] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (erişim tarihi: 01.04.2018).

sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.

TCK'nın 136. maddesinin 1. bölümünde kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört yıla kadar hapis cezası ile cezalandırılır.

TCK'nın 138. maddesinin 1. bölümünde kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.

### 1.3.2.3. 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Değerlendirilmesi

6698 Sayılı Kişisel Verilerin Korunması Kanunu 24/03/2016 tarihinde kabul edilmiş ve 07/04/2016 tarihinde resmi gazetede yayımlanmıştır.

Kanunun 1. bölümünde amaç, kapsam ve tanımlara yer verilmiştir ve uluslararası kaynaklarla benzerlik taşımaktadır. KVKK da temel amaç kişisel verilerin işlenmesinde özel hayatın gizliliği çerçevesinde temel hak ve özgürlükleri korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin uyacakları usul ve esasları düzenlemektir.

Kanunun 2. bölümünde kişisel verilerin işlenmesine ayrılmıştır. Kişisel verilerin bu kanunda ve diğer kanunlardaki usul ve esaslara göre işlenebileceği yer almıştır.

**KVKK'nın 4. maddesine göre kişisel verilerin işlenmesindeki ilkeler:**

**1.** Kişisel veriler, ancak bu kanunda ve diğer kanunlarda öngörülen usul ve esaslara uygun olarak işlenebilir.

**2.** Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:

**a)** Hukuka ve dürüstlük kurallarına uygun olma.

**b)** Doğru ve gerektiğinde güncel olma.

**c)** Belirli, açık ve meşru amaçlar için işlenme.

**d)** İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

**e)** İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Kişisel verilerin işlenmesindeki ilkelerde "belirli, açık ve meşru amaçlar için işlenme" ilkesi günümüzdeki uygulamalarca gerçekleştirilen veri işleme politikalarıyla uyuşmamaktadır. Konuyla ilgili birçok ihlal bulunmakta, kişisel verilerin hangi şekilde işlendiği açık olsa bile bu konu suistimal edilebilmektedir. Ayrıca yurtdışı merkezli hizmet veren şirketlerin bu konuda nasıl bir sorumluluklarının olduğu da bilinmemektedir. "İşlendikleri amaçlar bağlantılı, sınırlı ve ölçülü olma" ilkesinde ise örneğin Facebook, reklam amacıyla kişisel verileri işlediğini

belirtse de Cambridge Analytica şirketine sağladığı bu veriler farklı amaçlar için kullanılmıştır. Cambridge Analytica'nın bu verileri ABD başkanlık seçiminde kullandığı iddiası gündeme gelmiştir. Ülkemizde ise yaklaşık 234 bin kullanıcı bu durumundan etkilenmiştir.

Kullanıcıların psikolojik profil detaylarına sahip olduğu 50 milyon kişilik potansiyel seçmen datasını ayrıca elinde bulundurduğu verilerle birleştiren Cambridge Analytica, birçok farklı başkan adayının kampanyasında bu dataları reklam hedeflemesi amacıyla kullanmıştır. ABD seçimleriyle de sınırlı kalmayan Cambridge Analytica'nın Brexit[56] sürecinde de oldukça etkili olduğu sanılmaktadır.[57]

**KVKK'nın 5. maddesine göre kişisel verilerin işlenme şartları:**

**1.** Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

**2.** Aşağıdaki şartlardan birinin varlığı halinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

**a)** Kanunlarda açıkça öngörülmesi.

**b)** Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

**c)** Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

**d)** Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması.

**e)** İlgili kişinin kendisi tarafından alenileştirilmiş olması.

**f)** Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

**g)** İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması.

Kişisel verilerin işlenme şartlarında belirtilen "ilgili kişinin açık rızası olmaksızın işlenemez" hükmü kişisel verilerin korunmasında hayati önem taşımaktadır. Kişiyle ilgili verilerin kaydedilmesi, işlenmesi ve aktarılmasında yaşanan etik sorunlar en çok bu maddenin ihlali ile mümkün olmaktadır. Dijital ortamlarda kişisel verilerin işlenmesiyle ilgili olarak bilgilendirme yapılması artık zorunludur. Birçok şirket de politikalarını güncelleyerek bu bilgilendirmeyi yapmaktadır. Ancak kullanıcıların karşısına çıkan "Bu siteyi kullanarak kişisel

[56] http://t24.com.tr/haber/10-soruda-brexit-nedir-ingiltere-abden-ne-istiyor,345754 (erişim tarihi: 25.04.2018).
[57] https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri (erişim tarihi 22.03.2018)

veri politikamızı kabul etmiş olursunuz" ya da "Bu uygulamayı kullanarak çerez politikamızı kabul etmiş olursunuz" gibi bazı uyarılar kişisel rızayı ortadan kaldırmakta, kişiyi adeta mecbur kılmaktadır. Bu durumda kullanıcı gizlilik politikalarını okumadan hizmeti kullanmakta ya da o hizmeti hiç kullanamama durumu ile karşı karşıya kalmaktadır. Ayrıca kişinin rızası hangi bilgilerini paylaşıp hangi bilgilerini paylaşmayacağını açıkça karşılamamaktadır. Örneğin e-posta bilgilerini paylaşmak isteyen kullanıcı, konum bilgilerini paylaşmaktan imtina edebilmektedir. Bu durumda da kişinin rızası tam olarak mümkün olmayacaktır.

**KVKK'nın 6. maddesine göre özel nitelikli kişisel verilerin işlenme şartları:**

**1.** Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir.

**2.** Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır.

**3.** Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hallerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir.

**4.** Özel nitelikli kişisel verilerin işlenmesinde, ayrıca kurul tarafından belirlenen yeterli önlemlerin alınması şarttır.

Yukarıda görüldüğü üzere KVKK da hassas veriler özel nitelikli kişisel veriler olarak düzenlenmiştir. Bu verilerin işlenmesinde yine kişinin rızasının alınması zorunludur ancak bilindiği üzere özel nitelikteki veriler kişinin rızası olmadan da işlenebilmektedir. Bu verilerin işlenmesinde yaşanabilecek bir kötüye kullanım telafi edilemeyen sonuçlar doğurabilecektir. Ülkemizde 2013 yılında meydana gelen bir olay "SGK'nın kişilerin sağlık verilerini sızdırması"[58] sonucu yaşanan gizlilik ve mahremiyet ihlali, bu alandaki ciddi açığı gündeme getirmiştir. Bu durum devletin, kişilere ait tüm hassas verileri kanunlarla açık şekilde korunmasını, devletin gizlilik ve mahremiyet ihlali halinde ciddi yaptırımlar uygulanması gerekliliğini açıkça ortaya koymaktadır.

[58] http://t24.com.tr/yazarlar/fusun-sarp-nebil/danistayin-satilamaz-dedigi-saglik-verilerinin-sgk-tarafindan-65-bin-liraya-satildigi-onaylandi,19165 (erişim tarihi: 25.05.2018).

**KVKK'nın 7. maddesine göre kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesi:**

**1.** Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması halinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hale getirilir.

**2.** Kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesine ilişkin diğer kanunlarda yer alan hükümler saklıdır.

**3.** Kişisel verilerin silinmesine, yok edilmesine veya anonim hale getirilmesine ilişkin usul ve esaslar yönetmelikle düzenlenir.

7. maddede kişisel verilerin yok edilmesi konusu önem arz eden konuların başında gelmektedir. Toplanan bilgilerin sınırlı sürelerde depolanması ve gerektiğinde bu verilerin yok edilmesi gerekmektedir. Gizlilik politikalarında ise bu sürenin açıkça belirtilmesi gerekmektedir. Bu maddedeki eksiklikler 28.10.2017 tarihinde resmi gazetede yayınlanan "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik"[59] ile giderilmeye çalışılmıştır. Özellikle kişisel verilerin silinmesi, yok edilmesi ve anonim hale getirilmesiyle ilgili yapılan işlemlerin kayıt altına alınması ve saklama süreleri ile ilgili yönetmeliğin 7. maddesinin 3. fıkrasında belirtilmiştir. Bu maddeye göre söz konusu kayıtlar 3 yıl boyunca saklanmaktadır. 7. maddenin 5. fıkrasında ise kişisel verileri silme, yok etme ve anonim hale getirme yöntemlerini seçme hakkı "veri sorumlusu"na[60] tanınmıştır. Veri sorumlusu ile ilgili detaylı bilgi aşağıda açıklanacaktır. Aynı maddenin son cümlesinde "İlgili kişinin talebi halinde uygun yöntemi gerekçesini açıklayarak seçer" ifadesine yer verilmiştir.

**KVKK'nın 8. maddesine göre kişisel verilerin aktarılması:**

**1.** Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz.

**2.** Kişisel veriler;

**a)** 5.maddenin 2. fıkrasında,

**b)** Yeterli önlemler alınmak kaydıyla, 6. maddenin 3. fıkrasında, belirtilen şartlardan birinin bulunması halinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir.

**3.** Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

**4.** Kişisel verilerin yurt dışına aktarılması.

---

[59] http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm (erişim tarihi: 10.04.2018).

[60] KVKK'nın tanımlar bölümünün 3. maddesinde veri sorumlusu: Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişi olarak tanımlanmaktadır.

**KVKK'nın 9. maddesine göre kişisel verilerin yurt dışına aktarılması:**

**1.** Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

**2.** Kişisel veriler, 5. maddenin 2. fıkrası ile 6. maddenin 3. fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede;

**a)** Yeterli korumanın bulunması,

**b)** Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

**3.** Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir.

**4.** Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve 2. fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine;

**a)** Türkiye'nin taraf olduğu uluslararası sözleşmeleri,

**b)** Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu,

**c)** Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini,

**ç)** Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını,

**d)** Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması halinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

**5.** Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir.

**6.** Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.

9. maddede kişisel verilerin yurtdışına aktarılmasıyla ilgili maddelere yer verilmiştir. İlgili kişinin rızası yine göze çarpmakta; ancak yine kişinin rızası dışında verilerin aktarılabilmesiyle ilgili madde de yer almaktadır. Kişisel verilerin yurtdışı merkezli şirketlere aktarılmasında yaşanabilecek etik ihlallere karşı, kişisel veriler bu kapsamda koruma altına alınmıştır. Ancak halen dijital ortamlardaki web site ve bazı uygulamaların bu konuyla ilgili yükümlülükleri yerine getirmediği de görülmektedir. Özellikle mobil uygulamaların kişilerin

rızası dışında kişisel verilerini sızdırdığı göz önüne alınırsa buradaki boşluk daha da net anlaşılacaktır.

Kanunun 3. Bölümü Haklar ve Yükümlülükler ile ilgilidir.

**KVKK'nın 10. maddesine göre veri sorumlusunun aydınlatma yükümlülüğü:**

**1.** Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere;

**a)** Veri sorumlusunun ve varsa temsilcisinin kimliği,

**b)** Kişisel verilerin hangi amaçla işleneceği,

**c)** İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,

**ç)** Kişisel veri toplamanın yöntemi ve hukuki sebebi,

**d)** 11. maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür.

**KVKK'nın 11. Maddesine göre ilgili kişinin hakları:**

**1.** Herkes, veri sorumlusuna başvurarak kendisiyle ilgili;

**a)** Kişisel veri işlenip işlenmediğini öğrenme,

**b)** Kişisel verileri işlenmişse buna ilişkin bilgi talep etme,

**c)** Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme,

**ç)** Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme,

**d)** Kişisel verilerin eksik veya yanlış işlenmiş olması halinde bunların düzeltilmesini isteme,

**e)** 7. maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme,

**f)** (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme,

**g)** İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme,

**ğ)** Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması halinde zararın giderilmesini talep etme, haklarına sahiptir.

Bu bölümde haklar ve yükümlülüklere yer verilmiş olup özellikle kişinin veriler üzerindeki kontrolü üzerinde durulmuştur. Ancak yine burada kişilere büyük sorumluluklar yüklenmiştir. Kişilerin verinin işlenip işlenmediğini öğrenebilmesi ve buna ilişkin bilgi talep

etmesi zaman alıcı bir işlem olabilmektedir. Kişinin bu verilerin amacına uygun olarak işlenip işlenmediğini öğrenmesi için öncelikle tüm bu konulara hakim olması gerekmektedir. Kişi tüm bunları bilmiyorsa ve mevzuata hakim değilse, kendisine gelen zararı da tam olarak kavrayamayacaktır. Bu nedenle öncelikle devletin bu konuyla ilgili tüm koruma mekanizmalarını devreye sokması gerekmekte, bu mekanizmaların tükendiği noktada kişiler yükümlü olmalıdır.

**KVKK'nın 12. maddesine göre veri güvenliğine ilişkin yükümlülükler:**

**1.** Veri sorumlusu;

**a)** Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

**b)** Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

**c)** Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

**2.** Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi halinde, 1. fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

**3.** Veri sorumlusu, kendi kurum veya kuruluşunda, bu kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

**4.** Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

**5.** İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir.

KVKK'nın 12. maddesinin 3. fıkrasında belirtildiği üzere denetim, kanunun hükümlerinin uygulanmasını sağlamak amacıyla veri sorumlusu tarafından kendi kurum ve kuruluşunda gerçekleştirilmektedir. Kanuna göre şirketler veri sorumlusu olmaktadır. Ancak denetimin yalnızca veri sorumlusunun kontrolünde olması, kişisel verilerin ne ölçüde korunacağı konusunu havada bırakmaktadır. 11.04.2018 tarihinde BİMER[61] üzerinden Kişisel Verileri Koruma Kurumu'na iletilmek üzere "Veri sorumlusu üzerinde bağımsız bir üst kurulun bulunup bulunmadığı" ile ilgili soruya cevaben, 16.04.2018 tarihinde yanıtlanan yazıda

[61] Başbakanlık İletişim Merkezi.

"Bağımsız bir üst kurulun bulunmadığı" anlaşılmış olup, bu durumun kanundaki en büyük eksikliklerden biri olduğu görülmüştür.

KVKK'nın 12. maddesinin 5. Fıkrasında belirtildiği üzere, "işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve kurula bildirir. Kurul, gerekmesi halinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir" hükmü ile veri ihlalleriyle ilgili kişiler bilgilendirmekte; ancak bu bilgilendirme 'yetkisiz erişim ilanı'[62] olmaktan öteye geçememektedir.

Kanunun 4. bölümü başvuru, şikayet ve veri sorumluları ile ilgilidir. Bu bölümde ilgili kişinin şikayet ve başvurularının hangi şekillerde yapılacağı belirtilmektedir. Kanunun 5. bölümü suçlar ve kabahatleri düzenlemektedir. TCK'nın ilgili maddeleri yukarıda verildiğinden, bu bölümün hükümlerine değinilmemiştir. Kanunun 6. bölümü kişisel verileri koruma kurumu ve teşkilatın yapısı ile ilgilidir. Kanunun 7. bölümünde çeşitli hükümler (istisnalar) yer almaktadır ki yine yukarıda değinilen milli savunma, kamu güvenliği gibi nedenlerle kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla kişisel verilerin işlenebilmesi, bu verilerin anonim hale getirilerek araştırma, planlama ve istatistik vb. amaçlarla işlenmesi gibi hükümlere yer verilmektedir.

[62] https://www.kvkk.gov.tr/Icerik/4219/Kamuoyu-Duyurusu-Ihlal-Bildirimi (erişim tarihi: 04.05.2018).

# İKİNCİ BÖLÜM
# REKLAMA KRİTİK GÜNCELLEME: KİŞİSELLEŞTİRİLMİŞ REKLAMLAR VE MOBİL ORTAM REKLAMLARINDA DİJİTAL GÖZETİM

Bu bölümde mobil ortam reklamlarında gerçekleşen dijital gözetimin irdelenebilmesi için öncelikle bireyin gözetimi ve internette gerçekleşen gözetim konusuna değinilmiş, daha sonra da reklam, mobilite ve mobil ortamlar ile ilgili konulardan bahsedilmiştir. Ayrıca, mobil ortamda gerçekleştirilen dijital gözetimin yaygın olarak gerçekleştirildiği reklam türleri olarak kişiselleştirilmiş reklam, çevrimiçi davranışsal reklam (hedefli reklam) ve mobil reklam ile ilgili literatür taramalarına yer verilerek, konuya ilişkin çeşitli bakış açıları ortaya konulmuş ve mobil ortamlarda ve mobil ortam reklamlarında gerçekleşen gözetim açıklanmıştır.

## 2.1. Bireyin Gözetimi ve İnternette Gözetim

Gözetim pratikleri bir kişinin diğer bir kişi üzerinde ona göz kulak olduğu ya da incelediği yönünde bir izlenim bırakabilmek için sergilediği ilkel izleme edimleriyle başlamaktadır (Lyon, 2013: 14, 15). Kutsal olarak bilinen eski metinlerde de gözetlemenin zaman zaman denetleyen, zaman zaman da koruyan kollayan olarak kullanıldığı görülmektedir (Çakır, 2015: 195). Ancak günümüzde evlerin dışarıdan gelecek olan şiddet ya da baskılara karşı bir sığınak olduğu hayali, elektronik cihazların evlere sokulmasıyla beraber kişilerin bazen farkında olduğu ya da bazen de haberi bile olmadan içeriden dışarı veya dışarıdan içeri veri göndermesiyle alt üst edilmiştir (Lyon, 2006: 37).

Gözetim, devletler veya şirketlerin belirli grupların davranışlarını önleme amaçlı olarak veri toplama, biriktirme, analiz etme, değerlendirme ve kullanma yollarını uyguladığı; potansiyel olarak fiziksel, ideolojik ya da yapısal şiddeti içeren ve insanları belirli davranışlara yöneltmeye çalışsan bir süreçtir. Dijital gözetim bireyler arasında ayrım yapmamakta, herkesi gözetim altına alarak 'toplu gözetim' durumu yaratmaktadır. Bu ise, şüpheli/şüpheli olmayan ayrımını ortadan kaldırmakta ve herkesi potansiyel şüpheli konumuna getirmektedir. Gözetlenenlerin çoğunun farkında olmadıkları toplu gözetimin temel gerekçeleri de üç noktada toplanmaktadır: Güvenlik, terörizmle mücadele ve suçu önceden önleme (Çakır: 2015: 248, 317). Julian Assange vd. (2016: 15)'ye göre:

> Devletler zorlayıcı şiddet gücünün durmaksızın nerede ve nasıl uygulanacağını tespit eden sistemlerdir. Devletlerin gitgide internetle bütünleştiği, uygarlığın geleceğinin internetin geleceğine bağlı olduğunu,

buna bağlı olarak güç ilişkilerini tanımlamamız gerektiğini, eğer bu tanımlamayı yapmazsak da insanlığı devasa bir kitlesel gözetim ve denetim hapishanesine çevireceğini ileri sürmektedir.

Modern devlet verimliliği artırmak ve hedeflerini gerçekleştirmek için kişisel verilere ihtiyaç duymaktadır. Bunun için geliştirilen çeşitli sistemler ve araçlar, beraberinde gözetim, denetim, disiplin ve yönlendirme gibi toplumun tamamı üzerinde bir değişim yaratabilecek etkileri de getirmektedir (Küzeci, 2010: 26). Kontrol edilmek istenen nesneyi, bireyi ya da toplumu bilmek, onu gözetlemekten geçmektedir. Bu nedenle iktidarlar toplumu kontrol etmek için onu daha çok tanımak ve bilmek ihtiyacı içindedirler (Karahekya, 2009: 334).

Gözetim çoğu zaman devletler tarafından gerçekleştirilse de günümüzde büyük şirketler gözetim sürecine dahil olmuştur. Ekonomik yaşamın olağan ilişkileri olan üretim ve tüketim gibi unsurlar artık çok daha fazla gözetimin konusu haline gelmiştir. Gözetim, disipline edici bir pratik olmaktan çıkarak ekonomik yaşamın gözetimiyle gündelik hayata tecimsel kaygılarla sızmıştır. İnsanların tercihleri üzerinden özel profiller çıkartılmakta, üretim şablonu buna göre dizayn edilmekte ve bu durum şirketler vasıtasıyla açığa çıkmaktadır (Baştürk, 2016: 213). Yaşam Modeli Analizleriyle kişilerin alışkanlıkları belirlenmekte, profiller bu alışkanlıklar ve davranışlara göre belirlenmektedir. Yaşam Modeli Analizi özellikle öznenin alışkanlıklarını belgelemek veya anlamak için kullanılan, öznenin geçmiş davranışını saptayan, mevcut davranışlarını tespit eden ve gelecekteki davranışlarını öngören bir bilgisayarlı veri derlemesi ve analiz yöntemidir.[63]

Tüketimcilik, toplumsal denetimin bir aracı olarak görülse de, toplumsal denetimin diğer tiplerinden farklıdır. Doğrudan pazarlamanın ve isme gönderilen reklamların hedefi olanlar, bir davranışı yönlendirme girişiminin nesneleridir (Lyon, 1997: 90). Bilgi toplama eyleminin odağında önceden belirli bir birey varken artık bireylerle birlikte kişilerin ilgi alanlarına dayalı eğilimler ve kategoriler izlenir olmuştur (İsmayılov ve Sunal, 2012: 37). Kişiler gözetleyebilen, depolayabilen ve kullanıcılarla ilgili bilgiyi dağıtabilen teknolojilere gitgide daha fazla güvendikçe, yığınsal veri toplama gündelik hayata bağlı olarak 'tasarlanır' hale gelmiştir (Shklovski vd., 2014: 2347).

### 2.1.1. Bireyin Gözetimi

Bireyin gözetimi, temel anlamda onu tanımaya yönelmekte; daha çok bireyin kim olduğu sorusuyla ilgilenmektedir. Bireylerin kim olduğu sorusu da kimlik belirleme ile ilişkilidir. Bu noktada gözetim aracı olarak kullanılan kişisel veri, kişilerin doğal ya da sonradan

[63] https://labs.rs/en/metadata/ (erişim tarihi: 15.12.17).

kazanılmış bazı özelliklerinin, alışkanlıklarının ya da eğilimlerinin öğrenilmesi ve bunlara göre kişilerin sınıflandırılması olanağını sunmaktadır (Türkiye Bilişim Derneği, 2008: 15). Bilişim teknolojileri aracılığıyla şekillenen dijital toplumda kişiler, güvenlik ve özgürlük arasında seçim yapmaya zorlanmakta; bu araçlar bireylere özgürlük vaadi sunarken mahremiyeti ihlal etmektedir (Çalık ve Toker 2016: 9). Kişiye yönelik gözetimin boyutları Alan Westin, tarafından üç ayrı düzlemde açıklanmıştır:

"Fiziksel gözetim", "psikolojik gözetim" ve "veri gözetimi". Westin, bunları şu şekilde tanımlamaktadır:

1. **Fiziksel Gözetim:** Kişinin bulunduğu yerin, hareketlerinin, konuşmalarının ya da özel yazışmalarının kişinin bilgisi veya rızası dışında çeşitli araçlarla gözetlenmesi. Konum takibi, fiziksel gözetime verilebilecek en iyi örnek olmakla birlikte çeşitli mobil uygulamalarca yazışmaların denetlenmesi de bu gözetim boyutuna atıfta bulunmaktadır.
2. **Psikolojik Gözetim:** Yazılı ve sözlü testlerin, araçların veya maddelerin kullanılması suretiyle, kişinin isteyerek vermediği bilgileri enformasyonu elde etme veya kişinin kendisinin özel hayatı ve kişiliği bakımından önemli olabilecek hususları farkında olmadan açığa çıkarma. Panoptikon, ilk bakışta fiziksel bir gözetim gibi gözükse de psikolojik bir yanı da bulunmaktadır. Kişilerin, sürekli olarak görünmeyen bir göz tarafından gözetlendiği hissi bu psikolojik boyuta işaret etmektedir.
3. **Veri Gözetimi:** Veri işleme araçları aracılığıyla kişi veya gruplar hakkındaki bilginin, enformasyonun toplanması, işlenmesi, değişimi ve kullanımı. Bugün gelinen noktada dijital ortamlarda tüm bu gözetim durumlarıyla karşı karşıya kalınmaktadır (akt. Ketizmen, 2008: 193, 194).

Bu doğrultuda incelendiğinde, özellikle günümüz toplumları açısından bireyin gözetimine ilişkin en etkin ve kolay yolun veri gözetimi şeklinde gerçekleştirildiği görülmektedir. Fiziksel gözetim ve psikolojik gözetime ilişkin bilgi ya da enformasyonun, bilişim sistemleri aracılığıyla işlenebilmesi olanağı, veri gözetiminin sınırlarını ortadan kaldırabilecek nitelikte bir gözetim boyutu olduğunun da göstergesidir (Türkiye Bilişim Derneği, 2008: 16). Şirketlerin veya reklam verenlerin, görünürde kişilerin hayatını kolaylaştırması ya da iyi vakit geçirebilmesi için tasarladığı, gerçekte bireyin gözetimi için kullanılan bu teknolojilerin, kişilerde hangi tepkilere yol açtığı konusunda açıklayıcı bir sınıflama Gary Gumpert ve Susan J. Drucker tarafından yapılmıştır.

Gumpert ve Drucker'a göre gözetlenmeye karşı gösterilecek olan tepkilerin biçimlenmesinde, kişilerin gözetlendiklerinin farkında olup olmamaları etkili olmaktadır. Bu bağlamda gözetlemeye karşı oluşan tepkileri aşağıdaki şekilde kategorilendirmişlerdir:

- **Gözetleme teknolojilerinin farkında olmama:** Gözetleme teknolojilerinin var olup olmadığını bilmeyen kişilerde bu teknolojiler davranış değişikliğine yol açmamaktadır.
- **Gözetleme teknolojilerinin farkında olmakla birlikte kullanım amacını bilmeme:** Kişiler gözetleme teknolojilerinin var olduğundan haberdar olabilir ve gözetim altında olduklarını bir ihtimal olarak görebilirler.
- **Gözetleme yapıldığının tam farkında olma:** Kişiler bulundukları ortamlarda gözetleme yapıldığını bilmekte ve bu gözetleme onların davranış biçimlerini belirlemekte büyük rol oynamaktadır. Kişiler, gözetlemenin nasıl ve ne şekilde gerçekleştiğini öğrenmeye çalışmaktadır. Gözetime ilişkin farkındalık, kişilerin 3 farklı davranış biçimi sergilemesine neden olabilmektedir (akt. Güven, 2011: 189).

Gumper ve Drucker'a göre, bireyler gözetlemenin farkında oldukları zaman aşağıdaki davranış biçimlerini sergileyebilirler:

- **Tepkisel Davranış:** Gözetleme teknolojisine sahip olanlara karşı davranış biçimi. Bu davranış biçimi gözetim teknolojilerine sahip şirketlerin sorgulanmasına neden olabilir.
- **Farkında olmayı ihmal etme:** Sanki gözetleme yokmuş gibi davranma biçimi. Bu davranış biçiminde ise kişiler gözetlendiğini bilse de bu teknolojileri kullanmayı sürdürmekte, gözetimin varlığını inkar edebilmektedir.
- **Gözetlemeye tepki vermeme:** Gözetimin bir kültürel ya da teknolojik norm (çalışmanın giriş kısmında bahsedilen ve gözetime yönetsel yaklaşanların, gözetimin toplumların karakteristik bir özelliği olduğu yönündeki iddiası) olduğu varsayımı üzerine kurulu davranış biçimi (akt. Güven, 2011: 190). Bu davranış biçiminde ise kişiler gözetimi kabullenmekte, bu durum kendileri için bir sorun yaratmadığı sürece gözetime tepki vermemektedirler.

Bireyin gözetimi yukarıda da bahsedildiği üzere devletler ve büyük şirketler tarafından gerçekleştirilmektedir. Günümüz koşullarında gözetimin en fazla gerçekleştirildiği yer şüphesiz internettir ve internette gerçekleşen gözetimin açıklanmasını gerekli kılmaktadır.

### 2.1.2. İnternette Gözetim

Gözetlenme sistemleri gitgide daha az belirgin, gittikçe daha çok sistematik ve zekice olmaktadır (Lyon 2006: 12). Günümüzde ise halen en önemli gözetim aracının toplanan verilerin saklanması, eşlenmesi, geri getirilmesi, işlenmesi ve pazarlanmasına olanak tanıyan bilgisayarlar olduğu söylenebilir (Küzeci, 2010: 31). Bilişim teknolojilerindeki gelişmeler, insanların hayatlarında daha önce var olmayan dönüşümlere yol açmıştır. Kişilerin hayatı "çevrimiçi" ve "çevrimdışı" olmak üzere iki evrene bölünmüş ve iki merkezli hale gelmiştir

(Bauman ve Lyon, 2013: 51). Gözetimin daha yoğun, belirsiz hatta pek çok durumda rızaya dayalı olarak yapıldığı alanın, çevrimiçi evren olduğu görüşü geniş kabul görmektedir. Bu durumun yaratacağı tehlikeler de aynı yoğunlukta dile getirilmektedir:

> Elimizdeki en önemli özgürleşme aracı olan internet, totaliterliğin bugüne dek görülmedik düzeyde tehlikeli bir yöntemi haline geldi. Bu dönüşüm sessiz sedasız gerçekleşiyor, zira olup bitenden haberdar olan kişiler küresel gözetim endüstrisinde istihdam edilmiş oldukları için, gerçekleri dile getirmek çıkarlarına ters düşüyor. Kendi gidişatına bırakılacak olursa birkaç yıl içinde dünya uygarlığı izlemeye, gözetlemeye dayalı postmodern bir kara ütopyaya dönüşecek ve internet konusunda olağanüstü hünerli bireyler dışında kimsenin bundan kaçması mümkün olmayacak (Assange vd., 2016: 11).

Bilgisayarların ve mobil cihazların neredeyse her yerde olması bu alandaki güvenlik açıklarını da beraberinde getirmektedir. Güvenlik açıklarının önlenmesi için oluşturulan sistemler ise adeta gözetimin bir parçası haline gelmektedir.

İnternet alanında artan güvenlik ihlalleri nedeniyle verileri korumayı amaçlayan çeşitli türlerde güvenlik yazılımları geliştirilmiştir. Bu bağlamda 'Kötü Amaçlı Saldırıları Tespit Sistemi' (Intrusion Detection System - IDS*)* ortaya çıkmıştır. IDS, sunucu ve ağlardaki saldırıları algılayıp engellemeyi amaçlarken, sunucu veya ağdaki etkinlikleri sürekli izleyerek, ya bilindik zararlı yazılım imzalarıyla karşılaştırmakta ya da sistemdeki bozuklukları algılamaya çalışmaktadır. IDS'ler ağdan akan verilerin içeriğini de incelediğinden mahremiyeti ve gizliliği ihlal etmektedir. İnternet'in sürekli artan önemi, kısmen IDS'den ilham alan, 'Derin Veri Analizi' (Deep Packet Inspection - DPI) adında yeni bir kavramın gelişimini hazırlamıştır. DPI süreci, internetteki tüm iletişim süreçlerini incelemektedir. Bu nedenle DPI uygulamasının özel yaşam ve bilgi güvenliği açısından ciddi sonuçları bulunmaktadır. Ayrıca, belirli bir organizasyonu ilgilendiren IDS'nin aksine, DPI sistemleri 'İnternet Servis Sağlayıcılar' (Internet Service Provider - ISP) tarafından uygulanmakta ve ISP'leri kullanan kişilerin tamamını olası özel hayatın gizliliği ve mahremiyet ihlallerine açık hale getirmektedir (Kırlıdoğ ve Fidaner, 2013: 1015). Çoğu ülkedeki servis sağlayıcıları yasal olarak üst veriyi depolamaya tabidir. Servis sağlayıcılar, üst veriyi depolayarak ve analiz ederek, verilerin kaynağını, varış yerini, tarihini, zamanını, süresini ve iletişim türünü tespit edebilir ve tanımlayabilir.[64]

DPI kullanımının temel üç alanı aşağıdaki gibidir:

1. **Ağ İzleme:** Buradaki amaç, bir ağdaki kullanıcıların tamamı, bir kesimi veya tekil olarak kullanıcılar tarafından nasıl kullanıldığını anlamaktır.

[64] https://labs.rs/en/invisible-infrastructures-data-flow/ (erişim tarihi: 15.12.17).

2. **Hedefli Reklamcılık:** Reklam veren birçok şirket hedefli reklam kullanmaktadır. Hedef, ilgi alanları, arama sözcükleri ve ziyaret ettikleri web sitelerine göre belirlenmektedir. Hedefli reklam için DPI kullanıldığında ise daha 'derin' ve daha anlamlı verilerle daha isabetli hedefleme yapılabilir. Bu hedefleme için gereken verilerin toplanması, genellikle kişilerin cihazlarına kaydedilen çerezler ile yapılmaktadır. Tüm kullanıcılara kimlik numaraları atanmakta ve kullanıcıların ilgi alanlarını belirlemek için bütün etkinlikler kaydedilmektedir. Kullanıcılar teorik olarak bilgilerinin toplanmasını engelleyebilir veya o hizmeti kullanmayı bırakabilir; ama daha karmaşık sistemler, kullanıcılar çerezler silindiğinde dahi kullanıcı hakkında bilgi toplamayı sürdürebilmektedirler.
3. **Gözetim ve Sansür:** Devletlerce yasal veya yasadışı yapılan gözetim ve sansür, çocuk pornografisi gibi genel kabul görmüş suçların engellenmesinden, ülkedeki muhalif hareketlerin baskılanması gibi baskıcı eylemlere kadar farklı biçimler alabilmektedir. Genelde amaç ikincisi olsa da ilki DPI kurulumunu gerekçelendirmek için kullanılmaktadır. Devletler DPI gözetimi için ISP'lerin rıza ve işbirliğine ihtiyaç duymaktadırlar. ISP'ler çalışabilmek için devlet iznine tabi olduklarından bu duruma zorluk çıkarmamaktadırlar. Sonuçta DPI sistemi sınırsız bir gözetim için kullanılmakta ve kullanıcıların özel yaşamı ve mahremiyeti ihlal edilmektedir (Kırlıdoğ ve Fidaner, 2013: 1016, 1017).

Gelinen noktada internet alanındaki güvenlik ihlallerini önlemek amacıyla geliştirilen araçlar ve yazılımların gözetime hizmet ettiği görülmekte, bu sistemlerin amacının dışında kullanılmakta olduğu anlaşılmakta, kişilerin gözetimi için devletlerin ve şirketlerin amaçlarına hizmet eden bir mekanizma olduğu sonucu ortaya çıkmaktadır.

## 2.2. Bir Kitle İletişim Biçimi: Reklam

Kitle iletişimi, tek bir kaynak aracılığıyla çok sayıda insanla iletişim kurmak anlamına gelmektedir. Yavuz Odabaşı ve Mine Oyman'a göre kaynak ile hedef kitle arasındaki kanallar da kitle iletişim araçları olarak adlandırılmaktadır (akt. Elden, 2013: 27). Reklamcılığın asıl gelişimi de reklamın biçimsel bir öğesi olan iletişim araçlarıyla ilgili olan teknolojik gelişmelerle bağlantılı bir şekilde gerçekleşmiştir (Avşar vd., 2011: 182). Reklam bir iletişim biçimidir ve kendi içerisinde bir iletişim süreci vardır. Bu iletişim sürecini ise şu şekilde açıklamak mümkündür: Reklam, bir iletişim süreci olarak değerlendirilirse, süreci başlatan bir reklam verenin belli bir ürün ya da hizmeti hedef kitlesinde istediği yönde olumlu bir algı oluşturmak için iletisini çeşitli işitsel, görsel göstergeler yoluyla kodlayarak, hedef kitleye en

doğru zamanda ve en doğru kanal aracılığıyla iletmesidir (Elden, 2013: 24). Reklam iletişiminde hedef kitlenin önemini vurgulayan kavram ise, 'seçici algı' olarak bilinen tutumdur. Seçici algı aracılığıyla olası hedef kitle, reklam iletisinde aktarılmak istenen bilgileri alımlamakta, içselleştirmekte ve iletişim bu anlamda gerçekleşmiş sayılmaktadır (Sarı, 2009: 10).

Sanayi devriminin getirdiği kitlesel üretim olgusu, satıcı-alıcı ilişkisinde değişikliklere neden olurken, önceleri yüz yüze kurulabilen iletişim, kitlesel üretime geçilmesi ile beraber sona ermiş, tüketicilerle iletişim kurabilmek için onları kendilerinden ve ürünlerinden haberdar etmek isteyen üreticileri, kaçınılmaz olarak bir kitle iletişimi biçimi olan reklama yöneltmiştir (Avşar vd., 2011: 46). Jean Baudrillard'ın aşağıda verilen görüşü reklamın kitle iletişi işlevini net bir şekilde yansıtmaktadır:

> Reklam belki de çağımızın en dikkate değer kitle iletişim aracıdır. Reklamın kitle iletişim işlevi daha çok reklamın özerkleşmiş, yani gerçek nesnelere, gerçek bir dünyaya, bir göndergesele değil, bir göstergeden diğerine, bir nesneden diğerin, bir tüketiciden diğerine gönderme yapan araç mantığından kaynaklanmaktadır (Baudrillard, 2008: 57).

Reklamların toplumsal yaşamla bu denli iç içe geçmesi, reklam verenin hedef kitle ile daha yoğun iletişim kurma çabasının bir sonucudur (Elden, 2013: 214). Bu sonucun ortaya çıkması ise daha eskilere dayanmaktadır. Reklamcılık ve uygulamalarının ilk izleri Ortaçağ'da görülmüş, Ortaçağ'ın ekonomik ve toplumsal yapısının bir sonucu olarak reklamlar, üretimden elde edilen artılar için pazar bulma ve malı satabilme endişesi ile ortaya çıkmıştır (Avşar vd., 2011: 182). İçinde yaşadığımız dönemde de aynı temel motivasyonla hareket eden reklamcılar, piyasa ekonomisi koşulları altında pazar bulma ve ürün/hizmet satışını artırmak ve hızlandırmak niyeti ile hedef kitlelerini manipüle edecek çok çeşitli illüzyonlara başvurmaktadır.

Reklamlar, üretici ile tüketici arasındaki iletişimi sağlamasının yanı sıra günümüzün bilgi ve iletişim çağında toplumu etkileyen sosyal ve kültürel bir olgudur. Aslında reklamın ilk işlevi aynı kategorideki ürünler arasında bir farklılık yaratmaktır. Bunu da ürüne bir "imge" vererek yapmaktadır (Williamson, 2011: 24).

> Yaşadığımız kentlerde hepimiz her gün yüzlerce reklam imgesi görürüz. Karşımıza bu denli sık çıkan başka hiçbir imge yoktur. Tarihte başka hiçbir toplum böylesine kalabalık imgeler yığını, böylesine yoğun bir mesaj yağmuru görmemiştir. Bu imgelerin bize seslenip durmasına öylesine alışmışızdır ki üzerimizde yaptıkları etkinin tümüne pek dikkat etmeyiz. Belli bir imge ya da mesaj içimizden birinin dikkatini

> bugünlük çekebilir çünkü o kişi o özel şeye ilgi duymaktadır. Oysa hepimiz reklam imgelerinin tümünü bir iklim özelliği gibi doğal kabul ederiz (Berger, 2008: 129,130).

Reklamlar kültürel sistemleri biçimlendirirken, reklamlarla sunulan mitler ve sembollerle de farkında olunmaksızın kültürel yaşamı düzenlemektedir. Reklam, kültürel alana daha fazla nüfuz etmekte, giderek çok güçlü bir ideolojik güç haline gelmektedir (Hackley 2002: 219). Tüm bunların bir sonucu olarak reklam, tatminsizlikler yaratmakta, tüketim kültürünü ve anamalcı toplum düzenlerinde var olan yabancılaşmayı körüklemektedir (Berger, 1997: 56).

### 2.2.1. Reklamda Mobilite ve Mobil Reklam

Bir kitle iletişim biçimi olan reklam, giderek artan hareketliliğin ve mobil cihazların kişisel bir alan olarak değerlendirmesinin bir sonucu olarak kişiselleştirilmeye ve bireysel bir hale gelmeye başlamıştır. Mobil cihazların kolay taşınabilmesi ve her an ulaşabilir olması, kişilerin sabit olduğu durumlarda bile çok sık kullanılmasını sağlamaktadır. Kişilere mobil cihazlarında kullandıkları mobil ortamlar üzerinden ulaşmanın önemi de şirketler tarafından fark edilmiş, mobil ortam reklam yatırımları giderek artmıştır. Mobil teknolojiler geliştikçe, akıllı telefonlar pahalı bir merak olmaktan çıkıp, kullanıcılarının günlük yaşamlarına derin bir şekilde karışan ürünler haline gelmiştir. Bu cihazların sergilediği işlevler, yalnızca hayatı kolaylaştırma, eğlence ya da sosyalliğe elverişli uzantılarla ilgili değildir, aynı zamanda benliği yansıtma ve oluşturmayla ilgilidir (Shklovski vd., 2014: 2348).

Mobil cihazlar telefon olmanın ötesine geçerek çok işlevli araçlar haline gelmiş, artık çok daha etkileşimli bir yapıya bürünmüştür (Turow, 2015: 19). Etkileşim, iletişim teknolojilerinin en önemli özelliklerinden biridir. Etkileşim, sürecin kaynak ve alıcıyı iletişim sürecinde etkin kılması ve bu işlemlerin aynı iletişim kanalı üzerinde gerçekleşiyor olmasıdır (Başaran, 2010: 268). Medya yakınsamasıyla (convergance) birlikte bütünleşen ekranlar ve etkileşimli mobil iletişimle beraber mobil cihazlar birer mecra haline dönüşmüştür. Bu dönüşüm, geleneksel medyaya duyulan ilgiyi dijital medyaya kanalize etmekte, böylelikle medya tüketim eğilimleri teknolojik gelişmeler paralelinde değişime uğramaktadır (Çaycı ve Karagülle, 2016: 573). Van Dijk'ın bilgi ve iletişim ağlarındaki yöndeşme ile ilgili aşağıdaki açıklaması oldukça değerlidir:

> Ağ toplumunun temel karakteristik özellikleri mikro-elektronik ve dijitalleşme, bu temellerin yanında ise güncel eğilimler: bilgi ve iletişim ağlarının yöndeşmesi; dijital medya cihazlarının mintyatürleşmesi, bu

> gibi iletişim araçlarının günlük hayatın içine katılması ve birleşmesi; mobil, kablosuz ve geniş banta geçiş ve son olarak da bulut bilişimin[65] yükselişidir (Dijk, 2016: 77)

Kişilerin hareketi, mobil cihazların her yerdeliği ve kullanıcılara anında iletişim olanağı, reklam verenlerin 'mobil reklam'ları etkin bir şekilde kullanmasıyla sonuçlanmıştır. Mobil reklam, mobil tabanlı reklam iletilerinin yayıncılar ve reklam verenler tarafından kişilere iletilen reklamlardır. Mobil reklamcılık ise mobil araçlar üzerinden sürdürülen reklam faaliyeti olarak tanımlanabilir. Mobil reklamlar, tüketiciye diğer geleneksel reklam araçlarına göre daha hızlı ulaşmakta ve kişiselleştirilmiş mesajlar sunma imkanı sunmaktadır. Geleneksel reklam ortamında, reklam mesajında yapılacak bir hatanın düzeltilmesi yüksek maliyetleri beraberinde getirirken, mobil reklamda düzeltme ise tekrar mesaj gönderme kadar kolay olmaktadır (Özgüven, 2013: 9). Mobil reklamcılık, tüm bu kolaylıklarının yanı sıra özgürlüklere müdahalelerle ve mahremiyet ihlalleriyle de anılır olmuştur. Mobil reklamcılık, samimi bir kişisel alan içerisinde son derece müdahaleci bir uygulama haline gelebileceğinden, tüketicilerin kişisel verilerinin korunması konusundaki artan kaygılar da gündeme gelmektedir (Cleff, 2008: 423).

Jonna Häkkilä ve Craip Chatfield'in 2005 yılında yapmış olduğu bir araştırmada kullanıcıların cep telefonları ve kişisel verilerine fiziksel erişim izni verme kararlarını ve insanların telefonlarını oldukça kişisel bulduklarını, bunu diğerleriyle paylaşma konusunda isteksiz olduklarını ve yakın arkadaşlarla paylaşırken bile kendilerini huzursuz hissettiklerini belirtmişlerdir. Araştırma ayrıca cep telefonu kullanıcılarının uygulamaların cihazlarındaki veriye, bilgileri olmadan eriştiğini gördüklerinde, şaşırdıklarını ve kişisel alanlarının ihlal edildiği hissine kapıldıklarını göstermiştir (akt. Shklovski vd., 2014: 2348, 2349).

Google tarafından sunulan mobil reklamların, kullanıcının hem ilgi alanlarına hem de demografik bilgisine odaklanarak, mobil reklamların oldukça kişiselleştirilmiş hale getirildiğini göstermektedir. Ayrıca bilgilerin hiçbirisi kişiselleştirme için kullanılmayacak olsa da, kullanıcının gelir, politik görüş ve medeni hal gibi diğer bilgileri rastlantısal tahminlerden daha yüksek bir oranda tahmin edilebilmektedir (Meng vd., 2016: 2). Bir kullanıcının aygıtından toplanan bir reklam dizisi, hassas verilerin de dahil olması potansiyeliyle birlikte, o kullanıcının gerçek kişisel bilgisinin kesin bir temsili olarak görülebilir. Buradan hareketle kullanıcının demografik bilgisini, kişiselleştirilmiş mobil reklamlardan elde etmek mümkün olmaktadır. Cinsiyet, yaş ve ebeveynlik durumu ise Google'ın mevcut reklam ürününde sunulan üç hedefleme seçeneğidir. Dolayısıyla, bu kategorilerde gördükleri reklama dayalı olarak da

[65] Bulut bilişim, kullanıcının bilgisayarında sahip olduğu sistemlere göre daha ucuz ve daha büyük depolama alanı, işlem ve veri saklama hizmetlerini gerçekleştirebileceği sistemlere denilmektedir (Comer, 2016: 23).

kullanıcının demografik bilgisi elde edilebilmektedir. Wei Meng vd. (2016: 10, 11)'nin 2016 yılında mobil uygulamalar ile ilgili yapmış oldukları çalışmanın bulguları, Google'ın reklamcılara önerdiği vaadi sunabileceğini, belirtilen demografik gruplara reklamları doğru bir şekilde iletebileceğini doğrulamaktadır.

Mobil reklamların büyük bir bölümü; kullanıcı konumuna, günün saatine ve gerçek kullanıcılar etrafında oluşturulmuş profillere dayalı olarak hedeflenmektedir. AdMob[66] kütüphanesi, Android işletim sistemi tabanlı reklamlarının en büyük kaynağını temsil etmektedir. Diğer reklamcılık kütüphanelerinin ve işletim sistemlerinin de benzer davranışları gösterdiğine inanılmaktadır. Sonuç olarak mobil reklamların kullanıcıların hedeflenmesi ile ilgili verilerin toplanmasında önemli bir etkisi olduğu açıkça görülmektedir (Book ve Wallach, 2015: 13).

## 2.3. Kişiselleştirilmiş Reklamlar

Yukarıda da bahsedildiği üzere mobil teknolojilerdeki tüm bu gelişmeler reklam verenlerin odak noktasını, geleneksel kitlesel reklamcılıktan kişiselleştirilmiş reklamcılığa kaydırmasına olanak tanımıştır. Kişiselleştirilmiş reklamlar birbirini destekleyen üç gelişmeden doğmuştur: Reklamcıların kullanıcılardan kişisel veri toplama arzusu, bu verileri erişilebilir şekilde sunabilen şirketlerin ortaya çıkması ve kişilere sunulan reklamların seçilebilmesini sağlayan teknolojilerin geliştirilmesi (Turow, 2015: 138). Mobil cihazların kişisel alanlar haline gelmesi kişiselleştirilmiş reklamları da mobil ortamlar için daha önemli hale getirmiştir. Tüm kullanıcılara aynı iletilerin gönderilmesindense iletilerin kişiselleştirilerek gönderilmesi reklamların etkinliğini de artırmaktadır. Kullanıcı profilleri sayesinde ilgi alanı, marka tercihi ve konum odaklı reklamlar daha öz bir hedef kitleye yönlendirilebilmektedir. Dijital ortamlardaki reklamların ölçülmesi de gelişmiş yazılımlar sayesinde çok kolay bir hale gelmiştir. Geleneksel medyaya oranla hata payı düşük, hızlı ve sistemlidir. Ayrıca kişiselleştirilmiş reklamcılığın geleneksel reklamcılığa göre daha fazla artı değer ürettiği ile ilgili Fuchs'un aşağıdaki değerlendirmesi önemlidir:

> Hedefli reklamcılık, internet şirketlerinin kullanıcılara tek seferde sadece tek bir reklam değil, sayısız reklam sunmasını sağlar ve bu şekilde kullanıcılara metalar sunan daha fazla toplam reklam zamanı üretilmiş olur. Göreli artı değer üretimi, aynı zaman periyodunda eskisinden daha fazla artı değer oluşturulduğu anlamına gelir. Hedefli internet reklamcılığı, hedefi olmayan reklamlardan daha fazla artı değer (başka bir deyişle, reklam şirketinin kullanıcı-tarafından-oluşturulan içerik ve işlem verisi oluşturan

[66] Google'ın mobil uygulama geliştiricilerinin kendi mobil uygulamalarında ya da iş ortağı olduğu uygulamalarda reklam yayınlayabilmesi için sunduğu reklamcılık hizmeti.

ücretli çalışanların ve kullanıcıların daha fazla karşılığı ödenmeyen emek zamanını) içermektedir (Fuchs, 2015: 151).

Kişiselleştirme, İngilizcede "Personalization" kelimesine karşılık gelmektedir. Kişiselleştirme, her bir alıcıya atıfta bulunan; isim, cinsiyet, ikamet, meslek ve geçmiş davranışlar gibi alıcının kişisel özelliklerine dayanan bir mesaja elemanları dahil etmeyi içeren bir iletişim stratejisi olarak tanımlanabilir (Maslowska vd., 2016: 74).

Kişiselleştirilebilirlik web ortamında yükselen bir değer haline gelmiştir. Web üzerinde kimliklerin ve kullanıcı alışkanlıklarının giderek belirginleşmesi ile birlikte, görünümler de kişiye göre şekillendirilebilir kılınmıştır (Emiroğlu, 2009: 151). Kişiselleştirme yalnızca web ortamında değil, sosyal medyada ve mobil uygulamalarda da kullanılmaya başlanmıştır. Surprenant ve Solomon (1987) hizmet sağlayıcılarının müşterilere daha iyi hizmet sunma konusunda kişisel bilgiler edinmek ve müşterilerin ihtiyaçlarını ve tercihlerini analiz etmek için müşteriyle etkileşim kurmaları gerektiğini; böylece bu ihtiyaç ve tercihleri karşılayan hizmetler sağlayabileceğini belirtmişlerdir. Cliff Allen, 1999 yılındaki çalışmasında tüketicilerin değişen yaşam tarzına dikkat çekmiş, servis sağlayıcıların farklı müşterilere kişiselleştirilmiş mal ve hizmetler sağlamaya yönelttiğini; bu sebeple içerik ve medyanın farklı hedef gruplar veya kişiler için özelleştirilmesi gerektiğini vurgulamıştır.[67] Tae Hyun Baek ve Mariko Morimoto (2012: 59) kişiselleştirilmiş reklamcılığın kişisel bilgilere dayalı ücretli medya aracılığıyla her bir bireysel tüketiciye sunulan özelleştirilmiş promosyon mesajlarının bir formu olarak tanımlamaktadır.

Kişiselleştirilmiş iletişimin etkili bir ikna stratejisi olduğu düşünülmektedir. Kişiselleştirilmiş reklamcılığın da dikkat, algılama ve mesaja karşı tutum üzerindeki etkilere aracılık ettiği doğrulanmıştır. Ayrıca reklamların, alıcının adını da içerecek şekilde kişiselleştirilmesi, hem pozitif hem de negatif olarak değer kazandıran bilişsel tepkilere de yol açabilmektedir (Maslowska vd., 2016: 74). 2006 yılında yapılan bir çalışma ise insanların ilgi alanlarına giren reklamlara olumlu tepki verdiğini gösterilmiştir (De Castro ve Shimakawa, 2016: 91).

Kişilerin mobil reklamcılığa karşı tutumlarını etkileyen faktörlere odaklanan birçok davranış araştırması, kişiselleştirmenin mobil reklamcılıktaki önemini ortaya koymuştur (Wang vd., 2007: 17). Kişiselleştirme, diğer reklam türleriyle karşılaştırıldığında mobil reklamlarda daha önemli bir faktördür. Bu faktör, mobil ortamın geleneksel medyadan daha fazla ayrılmasına yardımcı olmaktadır (Xu vd., 2008: 714). Leppaniemi ve Karjaluoto (2005:

[67] https://www.clickz.com/personalization-vs-customization-2/82921/ (erişim tarihi: 08.05.2018).

213)'nun "mobil reklamcılıkta tüketici kabulü" ile ilgili araştırması, kişiselleştirilmiş mobil reklamlarda zamana ve yere odaklanmanın da önemli bir faktör olduğunu belirtmiştir. Dongsong Zhang (2003: 13)'ın "Kişiselleştirilmiş ve uyarlanabilir içeriği mobil cihazlara nasıl sunacağına" ilişkin araştırması arka plan bilgisi, tercihleri ve ilgi alanlarının dikkate alınması gerektiğini bildirmektedir. Ramin Vatanparast (2007: 19)'ın "Mobil reklamcılık" ile ilgili çalışması da mobil reklamcılıktaki kişiselleştirilmiş hizmetlerin; konum, zaman, arka plan bilgisi, tercihler, arama geçmişi ve sanal toplulukların özelliklerini dikkate alması gerektiğini belirtmektedir.

İnternet'in yüksek penetrasyon oranı ve etkileşimli yapısı göz önüne alındığında, yalnızca reklam mesajları almak yerine, tüketiciler artık gerekli reklam bilgilerini proaktif bir şekilde arayabilmektedirler. Şirketler, tüketiciler için kişiselleştirilmiş reklamlar tasarlarken, onların güvenini kazanmak için gizliliklerini ve güvenliğini korumalıdır. Böylelikle tüketiciler, kendilerine özel olarak hazırlanan reklam içeriğini düzgün bir şekilde alabilir ve görüntüleyebilirlerse, tüketicide iyi bir izlenim bırakabileceği ve ürünü satın alma arzusunu da artırabileceği iddia edilmektedir (Chen ve Hsieh, 2012: 543, 555).

Çevrimiçi bir video sağlayıcısı olan Eyeview'in 2011 yılında yaptığı araştırmada[68], çevrimiçi video reklamlarda kişiselleştirme ve alaka düzeyinin, satın alma niyetinde % 37'lik bir artış, marka tercihlerinde % 100 artış ve marka sadakatinde % 73'lük artış ile sonuçlandığı bulunmuştur. 2007 yılında yapılan bir çalışmanın sonuçlarına göre de Facebook reklamlarının kişiselleştirilmiş olmasının ve tıklama niyeti üzerindeki olumlu etkisinin, Facebook'a yönelik daha olumlu tutumları olan katılımcılar için daha güçlü olduğu ortaya konulmuştur (Keyzer vd., 2015: 124). Burada kişiselleştirmenin yanı sıra bu reklamların hangi ortamda yayınlandığı da önem kazanmaktadır: Kişiselleştirme, reklam verenler için cazip olsa da, kişisel verilerin izinsiz şekilde kullanılarak yapılan hedeflemenin tüketicilerin ilgili ürün ya da markalara olan güveni üzerinde önemli ölçüde etkili olduğu düşünülmektedir (Bleier ve Eisenbeiss, 2015: 390).

Meng vd. (2016: 3)'nin yapmış olduğu araştırmada büyük reklam ağlarının (örneğin; Google) reklamcılara hedef nüfusunu belirlemeleri için sağladığı ara yüz incelenmiş ve reklam ağlarının genellikle şu üç tür hedeflemeyi sağladıkları sonucuna varılmıştır:

- **Konu Hedefleme.** Konu hedefleme, reklamcıların mobil uygulama içinde sundukları reklamlarını, içerikle bağlantılı uygulamaların içerisine yerleştirmelerini sağlar. Reklamcılar, reklam ağı ara yüzü aracılığıyla bir ya da birden fazla konu seçerek, reklam ağının konuyla ilgili uygulamalara gönderim yapmasını sağlayabilirler. Örneğin;

[68] https://www.emarketer.com/Article/Personalized-Online-Video-Ads-Boost-Branding/1008655 (erişim tarihi: 13/09/2017).

reklamcılar ‘Otomobiller & Araçlar’ konusunu hedef alarak, arabalar ya da diğer otomobil tema içeriğine sahip olan uygulamalara, otomobillerle alakalı reklamların iletilmesini sağlayabilirler. Ayrıca ‘Kamyonlar & Arazi Araçları’ gibi daha belirli alt başlıklar da, daha etkili konu hedefleme sağlanması için, ‘Otomobiller & Araçlar’ genel başlığı altında bulunmaktadır.

- **İlgi Alanı Hedefleme.** İlgi alanı hedefleme, kullanıcılar reklamı yapılan ürünle ya da servisle doğrudan bağlantılı olmayan uygulamaları kullanıyor olsa bile, reklamcıların sunduğuna benzeyen ürünler ya da servislerle ilgilenen kullanıcılara ulaşmayı içermektedir. Kullanıcıların ilgi alanı profilleri, kullanıcının mobil aygıttaki kullanım şablonlarına, daha önce tıkladığı reklam kategorilerine ve daha fazlasına bağlı olarak, reklam ağı tarafından yeniden oluşturulabilir. Ayrıca, aynı kullanıcıyı bilgisayar ve mobil aygıtlar üzerinden bulmak istendiğinde de, ilgi alanı profiline çapraz platform birleşiminin yapılması gerekli olabilir. Reklam ağı, reklamcıların ilgi alanı kategorilerini seçmesini sağlayarak, profillerinde daha önce aynı kategorilere ilgi duymuş olan kişilere reklam hizmeti sağlayabilir.
- **Demografik Hedefleme.** Reklamcılar, seçilmiş bir demografi grubu içerisindeki kullanıcılara reklam sunmak için, demografik hedeflemeyi kullanırlar. Örneğin; reklamı yapılan iş belirli bir yaş aralığındaki kullanıcı grubunun ihtiyacını karşılıyorsa, (örneğin; daha genç insanlar spor arabaları daha çok severler) bu insan grubu için hedeflenen reklamlar, diğerlerinden daha etkilidir.

Meng vd. (2016: 7)’nin analizi, mobil reklamların kullanıcının ilgi alanlarına bağlı olarak yüksek ölçüde kişiselleştirildiğini göstermektedir. 100 adet reklam izleniminin gözleminden elde edilen reklam ilgi alanı profillerinin, yüksek bir kesinlik ve anımsama ile kullanıcıların gerçek ilgi alanı profillerine oldukça yakın olduğu görülmüştür. Reklam ilgi alanı profillerindeki kategorilerin %83’ünden fazlası kullanıcıların %11’i için doğrudur ve gerçek kullanıcı ilgi alanı kategorilerinin %50’sinden fazlası, kullanıcıların %60’ı için reklam ilgi alanı profillerinde saklanmıştır. Daha sonra mobil reklamların büyük bir bölümünün, gerçek kullanıcı ilgi alanlarıyla uyuştuğu fark edilmiştir. Kullanıcıların %41’i için reklam izlenimlerinin %57’sinden fazlası, kullanıcıların gerçek ilgi alanlarına uymaktadır. Ayrıca istatistiksel testleri kullanarak demografiye dayalı kişiselleştirilmiş reklamlar da tespit edilmiştir. Kişiselleştirilmiş reklamlarda yüksek sayıda gözlenen demografik kategorinin, cinsiyet olduğu görülmüştür. Kişiselleştirme, reklamcılar tarafından ifade edilen belirgin bir hedefleme seçeneği olabilmekte (yaş, cinsiyet ve ebeveynlik durumu) veya kişiselleştirme, bir reklam ağının patentli kişiselleştirme algoritmalarının bir sonucu olabilmektedir (gelir, din,

vb.). Ayrıca mobil reklamcılıkta demografiye dayalı kişiselleştirmenin, uygulamada da geçerli olduğu saptanmıştır. Bazı demografik kategorilerle bağlantılı olan, özel olmayan reklamlarla birlikte bu reklamlar da gerçek kullanıcının demografik profilinin iyi bir temsili olabilmektedir. Bu durum şirketlere ve reklam verenlere gerçek kullanıcıların özel kişisel bilgilerini öğrenmeleri için büyük bir fırsat sunmaktadır. Yukarıda belirtilen çalışmalardan anlaşılacağı üzere kişiselleştirilmiş reklamların, mobil ortamlar ve mobil cihazlardaki kişisel veri sızıntısına bir kanal olarak hizmet ettiği, bu verilerden elde edilen bilgilerin reklam oluşturma sürecinde kullanıldığı ve gizlilik ihlali endişelerine neden olabilecek unsurları içerdiği sonucuna ulaşılmaktadır.

## 2.4. Çevrimiçi Davranışsal Reklam (Hedefli Reklam)

Davranışsal hedefleme; yanıt geçmişi, konum odaklı veri, sosyal-ekonomik veri, hava durumu verisi veya mevcut herhangi bir veriyi birleştiren algoritmalar tarafından gerçekleştirilen gelişmiş hedefleme yöntemidir. Mobil Uygulamalar ve web platformları, giyilebilir teknoloji aracılığıyla biyometrik veriler, otomobillerdeki gezi verisi, akıllı evler, akıllı şehirler ve son olarak da ücretsiz internet sağlayan bir uydu sistemi ile dünyanın yörüngesinin ele geçirilmesi ile birlikte, fiziksel alana kadar genişlemektedir.[69]

Çevrimiçi davranışsal reklam (ÇDR), hedefli reklam olarak da bilinmekte, bireyin çevrimiçi etkinlikleriyle ilgili toplanan verilerden oluşturulmaktadır (McDonald ve Cranor, 2009: 1). Daha önce çevrimiçi olarak arama yapılan, görüntülenen veya tıklanan belirli ürünlerin/hizmetlerin ya da daha önce ziyaret edilmiş çevrimiçi mağazaların belirli markaların ya da ürünlerinin öne çıkarılarak yeniden gösterilmesi yöntemleri ile uygulanmakta olan çevrimiçi davranışsal reklamcılık; popülerliği, artan kullanımı ve 'tıklanma' sayısı ile ölçülebilmesi nedeniyle reklam verenlerin sıklıkla kullandığı bir reklamcılık stratejisidir (Karabıyık ve Armağan, 2017: 212). Çevrimiçi trafiğin takip edilmesiyle beraber kişinin ilgi alanları saptanmakta ve buna göre reklam gösterilmektedir (Kararslan vd., 2014).

Bu noktada sorulması gereken soru şudur: Google ve Facebook, ücretsiz hizmet sunan şirketler olmalarına rağmen nasıl oluyor da yüz milyarlarca dolar değere sahip olabiliyorlar? Cevabı açıktır: Profil çıkarma ve kullanıcı hedefleme hizmetini satmakta ve belirli bir kullanıcı grubuna reklam hizmeti vermesini sağlamaktadırlar.[70] Böylelikle ücretsiz sunulan hizmetlerin aslında ücretsiz olmadığı, ücretsiz hizmetin bedelinin kişisel verilerle ödendiği anlaşılmaktadır.

---

[69] https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).
[70] https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).

Gandy, panoptik bir sınıflandırmadan bahsetmektedir. Bu panoptik bakış, kişilerin ölçümlenerek belirli bir kategori ve sınıflandırmaya tabi tutulduğu bir gözetim biçimidir. Çevrimiçi davranışsal reklamcılık mekanizması da tam da bu şekilde çalışmaktadır (akt. Fuchs, 2015: 154).

Joseph Turow (2015: 135)'a göre şirketler, kullanıcıları hedeflenmesi gereken kullanıcı ve hedeflenmemesi gerek "çöp" kullanıcı olarak iki kategori olarak sınıflandırmaktadır. Çöp kategorisine girenler yok sayılmakta ya da bulundukları düzeyde daha uygun olduğu düşünülen başka ürünlere yönlendirilmektedir. Hedef kategorisine girenlerse, haklarında toplanan bilgilere ve demografik profillerine, inançlarına ve yaşam stillerine göre tekrar tekrar değerlendirilmekte, daha sonra bu kişilere, elde edilen sonuçlara uygun mesajlar ve indirimler gönderilmektedir. Buna örnek verilmesi gerekirse Google'da arama yapan kullanıcılar farklı sonuçlara ulaşmaktadırlar. Bunun nedeni de Google'ın daha önce yapılan aramalarla oluşturulan profillere göre uygun sonuçlar çıkartmasıdır. Yani bir kullanıcı hedef olarak belirlenmişse farklı, çöp olarak belirlenmişse farklı sonuçlar, reklamlar ve içerikler almaktadır.

Çevrimiçi davranışsal reklamlara yönelik yapılan çalışmalara bakıldığında farklı sonuçlar ortaya konulduğu görülmektedir. Bu çalışmalarda genellikle ÇDR'lerin satın alma davranışı üzerine olan etkisi incelenmiş olup ÇDR'lerin mobil ortamlarda sıkça başvurulan bir reklam stratejisi olduğu düşünüldüğünde, gözetime ilişkin boyutu ihmal edildiği anlaşılmaktadır. Yapılan araştırmalarda nadir olarak gizlilik ve mahremiyet ile ilgili konulara değinildiği görülmüştür.

Çevrimiçi davranışsal reklamlarla ilgili olarak ABD'de Aleecia M. McDonald Lorrie Faith Cranor (2010: 63) tarafından ÇDR ve internet reklamları ile ilgili bilgileri ve algıları hakkında derinlemesine görüşme ve anket tekniği kullanılarak yapılan bir çalışmaya göre, katılımcıların yaklaşık % 20'si ÇDR avantajlarından yararlanmak istemektedir. Katılımcıların % 64'ü ise bu fikri rahatsız edici bulmaktadır. McDonald ve Cranor (2010: 27)'un yine aynı yıl yapılan başka bir çalışmasında 314 katılımcının yer aldığı ve ÇDR'nin nasıl anlaşıldığı ile ilgili olarak katılımcıların çoğunluğu, reklamları görmezden gelmeye çalışmış ve reklam verenlere veri sağlama konusunda hiçbir istek göstermemiştir. Ayrıca kullanıcılar bu reklamcılık mekanizması hakkında yeterli bilgiye sahip değillerdir. Kullanıcıların çoğu, çerezlerin bilgisayarlarında veri depoladığını, uyarlanmış reklamları etkinleştirdiğini ve sitelerin genelinde izlemeye izin verdiğinin farkındadır. ÇDR'de kullanılan çerezlerin diğer verilerle birleştirilip birleştirilmeyeceği, çerezlerin hangi verileri sakladığını, çerezleri engellemenin coğrafi konum gizliliğini koruduğu ve özellikle yasalar ve yasaların uygulanması konusunda özellikle belirsiz olduğu gibi önemli detayların da açık olmadığı sonucuna varılmıştır. Yine

ABD'de 2012 yılında 48 katılımcı ile yarı yapılandırılmış görüşme tekniği kullanılarak yapılan bir çalışmaya göre: Genel olarak katılımcılar, çevrimiçi davranışsal reklamcılığın tüketicilere faydalar sağladığına; ancak ve bunun gizlilik risklerine neden olduğuna inanmaktadır. Katılımcılar, çoğunlukla reklam şirketlerine güvenmemektedir. Katılımcılar, davranışsal reklamcılığın bazen yararlı bazen de zararlı olduğunu belirtmişlerdir. Katılımcılar, şirketlerin kullanıcıları profillemek için kullanılan teknolojilerini algılamakta güçlük çekmektedir. Bununla birlikte, güncel uyarı ve gizlilik politikası mekanizmalarını etkisiz bulmuştur (Ur vd., 2012: 4, 11).

Ithaca Collage'in[71] yapmış olduğu bir araştırmada kişilerin webde gezinme alışkanlıklarına ve diğer kişisel bilgilerine dayanarak kullanıcıları hedefleyen çevrimiçi reklamların kişinin ürünü satın alma niyetini olumsuz yönde etkilediğini öne sürmektedir. Kullanıcılar bu tür bir reklam uygulamasını 'ürkütücü' bulmaktadır.

Türkiye'de ise 2016 yılında 446 katılımcı ile gerçekleştirilen yüksek lisans tez çalışmasında internet kullanıcılarının ÇDR'ye bakışı, ilgi ve farkındalıkları daha sonrasında da satın almaya yönelik davranışları incelenmiş, kullanıcıların % 63,7'sinin ilgilendiği ve incelediği ürünleri daha sonra reklam olarak gördüğü tespit edilmiştir. Katılımcıların % 51'i bu reklamlardan rahatsız olduğunu, % 15,7'i rahatsız olmadığını beyan etmiştir. Ayrıca katılımcıların % 67,7'si bu reklamlardan sonra satın alma davranışı göstermemiş, % 13,7'si ise satın alma davranışı göstermiştir (Aydın, 2016: 164, 167, 168). Yine Türkiye'de 2017 de yayınlanan bir "Tüketicinin Çevrimiçi Davranışsal Reklamlara Tıklama Kararını Etkileyen Faktörler" başlıklı makalede ise ÇDR'lere dair bilgilerin, tüketicilerin mahremiyet ihlali endişeleri üzerindeki etkisi ve ÇDR'lere olan güven duygusunun tüketicilerdeki mahremiyet ihlali endişelerine nasıl etki ettiği incelenmiştir. Çalışmada mahremiyeti korumaya dair kaygıların reklama tıklama kararının verilmesi ile ilişkili olmadığı bulunmuştur. İnternet tarama geçmişi bilgilerinin (dijital ayak izi) kullanılması ile tüketicilerde oluşan özel hayata müdahale edilmişlik duygusu ve bu duygunun meydana getirdiği endişeye sahip olmanın, bireylerin çevrimiçi davranışsal reklamları tıklama kararı almalarında etkili olmadığı sonucuna ulaşılmıştır. Çevrimiçi davranışsal reklam içeriğinin tüketiciye hitap etmesi, tüketicinin reklama tıklama kararı almasına etki etmektedir. Çevrimiçi reklamcılık uygulamalarına güven duyuldukça mahremiyet ihlali endişelerinde azalma görülmüştür. Tüketicilerin söz konusu reklamcılık hakkında doğru ve yeterli bilgiye sahip olmaları da, tüketicilerin mahremiyet ihlali endişesi taşımalarına etki etmemektedir (Karabıyık ve Armağan, 2017: 213).

[71] https://www.ithaca.edu/ic-news/releases/online-creep:-targeted-ads-may-have-opposite-effect-of-marketers-intent-39546/#.V-tiPiiLSHv (erişim tarihi: 13.09.2017).

## 2.5. Mobil Ortam Reklamlarında Dijital Gözetim

Çevrimiçi ortamda neredeyse her hareket, yüzlerce farklı görünmez takipçi, varlıklarına dair bir iz bulunmayan ve çevrimiçi hareketleri hakkında bilgi toplayan gizli ve sessiz 'sensörler' ağı tarafından takip edilmekte ve kayıt altına alınmaktadır.[72] Kullanımı gittikçe artan ve yaygınlaşan mobil ortamlar hayatımızda daha çok yer edinmekte ve bu ortamlarda iş ve işlemlerin daha çok yapılmasını kaçınılmaz kılmaktadır (Sağıroğlu ve Mohammed, 2009: 146). Özellikle Android işletim sistemi kullanan mobil cihazların Windows işletim sistemini kullanan (hem mobil hem masaüstü) cihazlara karşı üstünlük kurması[73] ve mobil cihaz kullanımının masaüstü bilgisayar kullanımını geçmesiyle birlikte[74] internete bağlı mobil ortamlar daha fazla tercih edilmeye başlanmış, buna bağlı olarak bu ortamlarda yayınlanan reklamların sayısında da dikkate değer bir artış meydana gelmiştir.

### 2.5.1. Reklam Ortamları

Reklamlar, bir mal, hizmet, fikir, kişi ya da kurumla ilgili mesajların, kaynaktan hedef kitleye taşınmasına hizmet etmektedir. Reklamların bu işlevi ise çeşitli reklam ortamları kullanılarak gerçekleştirilmektedir (Elden, 2013: 213). Günümüzde dijitalleşmenin önem kazanması, reklamcılık alanında dijital ortamların yoğun olarak kullanılmasını beraberinde getirmiştir. Dijital ortam, bilgiyi dijital bir formatta yayacak olan elektronik ortamlara atıfta bulunmaktadır. Bunlar, bilgisayarlar, cep telefonları, akıllı telefonlar veya dijital dış mekan tabelaları ve ekranlar gibi dijital cihazlardır (Smith, 2011: 490). "Reklam ortamları da reklamların hedef kitleyle buluştuğu yerlerdir ve bu ortamların reklam kampanyalarının üzerinde önemli etkileri bulunmaktadır" (Elden, 2013: 213). Bu tanıma bakılarak reklam ortamlarını, reklamların hayat bulduğu ve varlığını sürdürdüğü mecralar olarak değerlendirmek mümkündür. Elden, "Reklam Ortamlarını": yayın yapan reklam ortamları (radyo-televizyon), basılı reklam ortamları (gazete, dergi, doğrudan postalama ve diğer basılı reklam materyalleri) açıkhava reklam ortamları, transit reklam ortamları, internet, satış yeri reklam uygulamaları ve sinema olarak tanımlamıştır. (Elden, 2013: 216). Günümüzde reklam ortamlarının değişime uğramasıyla beraber, reklam okuryazarlığı da dijital okuryazarlığın en önemli bileşeni haline gelmiştir (Taşkaya, 2016: 201).

---

[72] https://labs.rs/en/metadata/ (erişim tarihi: 15.12.2017).
[73] http://gs.statcounter.com/press/android-challenges-windows-as-worlds-most-popular-operating-system (erişim tarihi: 13/09/2017).
[74] http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide (erişim tarihi: 13/09/2017).

### 2.5.2. İnternet Tabanlı Mobil Ortam Reklamlarının Tanımlanması

Mobil ortam reklamları, internet tabanlı olmakla birlikte web ortamı, arama motorları, sosyal medya ve mobil uygulamalarda yayınlanan reklamladır. Bu reklamcılığın kullanıcılara reklam sunma metotları arasında ise reklam bantları (web-banner), geçiş reklamları (video-mobil uygulama içi), teklif reklamları (bir ürün ya da uygulamaya yönlendiren) ve bildirim reklamları (push) bulunmaktadır.[75]

Literatüre bakıldığında dijital reklamın geniş bir reklam ortamını kapsadığı görülmektedir. Bunlar genelde; radyo-televizyon, internet, açık hava, sinema ve dijital tabela[76] gibi dijital olan ortamlardır ve dijital reklamlar da bu ortamlarda yayınlanan reklamlar olarak değerlendirilmektedir. Mobil reklam kavramı ise mobil dijital cihazları kapsadığı gibi dijital olmayan reklamları da içermektedir. Mobilden kasıt hareketli olmak ise motorlu bir aracın arkasından çekilen reklam panosu ya da gezici halde anons yaparak reklam yapan mobil satıcıların reklamları da mobil reklam içerisinde yer bulabilir. Bu durumda bu ortamlarda birer mobil reklam ortamı olacaktır. Ancak 'internet tabanlı mobil ortam reklamları' yalnızca dijital cihazlar üzerinden ve internet aracılığıyla gerçekleştirilen reklamları kapsamaktadır. İnternet tabanlı mobil ortam reklamları tüm bu yönleriyle mobil reklamdan ayrılmaktadır. Bunun yanı sıra internet reklamcılığı tüm cihazlarda (masaüstü, mobil ve diğer ortamlar) gerçekleşmekteyken, internet tabanlı mobil ortam reklamları yalnızca mobil cihazlar üzerinden gerçekleştirilmektedir. Kuşkusuz internet tabanlı mobil ortam reklamları bir dijital reklamdır; ayrıca mobil reklamdan mobil olma özelliğini, internet reklamından ise internete bağlı olma özelliğini almakta ve mobil reklamlar ya da internet reklamları gibi tanımlanmaya ihtiyaç duymaktadır. IAB Türkiye'nin[77] yapmış olduğu bir araştırmaya göre sektördeki gelişmelere paralel olarak 2016 yılının veri analizinde değişikliğe gidilmiş ve 'mobil'in format olmaktan çıkarılarak 'platform' (ortam) olarak konumlandırıldığı belirtilmiştir. Sonuç olarak internete bağlı haldeki mobil cihaza gönderilen, bu ortamlarda yayınlanan ve kullanıcı tarafından alınan reklam türüne 'internet tabanlı mobil ortam reklamları' denilmesi gerekmektedir. Ancak internet olanaklarının giderek artması ve neredeyse her alanda kullanılır olması 'internet tabanlı' ibaresinin kullanılmasını gerekli kılmamaktadır. Bu nedenle bu reklamların 'mobil ortam reklamları' olarak anılmasının daha uygun olacağı kanaatine varılmıştır.

---

[75] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).
[76] Digital Signage.
[77] http://www.iabturkiye.org/iab-turkiye-2016-dijital-reklam-yatirimlarini-acikladi (erişim tarihi: 20.05.2018).

### 2.5.3. Mobil Ortamlarda ve Mobil Ortam Reklamlarında Gözetim

Yukarıda bahsedildiği üzere internet tabanlı mobil ortamlar: Web ortamı, arama motorları, sosyal medya ve mobil uygulamalar olmak üzere dört başlık altında toplanabilmektedir. Kullanıcılar web ortamında gezinirken, arama yaparken ya da herhangi bir sosyal medya ortamını kullanırken, bu ortamlara ya bir tarayıcı üzerinden (tarayıcılarda aslında birer mobil uygulamadır) ya da bir mobil uygulama üzerinden erişmektedirler. Bu duruma bakıldığında yukarıdaki tüm ortamlar mobil uygulama ortamı gibi gözükmektedir. Ancak özellikle sosyal medyanın aktif ve etkileşimli bir ortam olması ve milyonlarca kullanıcısının bulunması, sosyal medyanın başlıca bir ortam olarak değerlendirilmesini gerektirmektedir. Örneğin kullanıcılara anlık bir fayda sağlayan bir el feneri mobil uygulamasıyla, günde binlerce konunun gündeme taşındığı/tartışıldığı Twitter aynı konumda durmamaktadır. Ayrıca arama motorlarının çok yüksek oranlarda kullanımı, kullanıcılar için adeta vazgeçilmez oluşu (son dönemde widget'ler[78] aracılığı ile de arama motorlarına erişilebilmektedir) arama motorlarını da başlı başına bir ortam haline getirmiştir.

Web ortamı internetin ortaya çıkışından itibaren var olan, hangi araçla bağlanılırsa bağlanılsın (ister tarayıcı ister mobil uygulama veya herhangi bir widget) başlı başına bir ortamdır ve internetteki gözetimin en baştan beri temelini oluşturmaktadır. Ayrıca tüm bu ortamların kendilerine ait bir reklam ekosisteminin bulunması da ayrı birer ortam olarak değerlendirilme durumlarını güçlendirmektedir. Mobil uygulamalar ise web, arama motoru ve sosyal medya ortamlarından farklı olarak, hali hazırda gerçekleştirilen gözetimin, dijital iz takibi ve kişisel veri sızıntılarının en yoğun olduğu ortamlardan biridir. Günümüzde çok çeşitli mobil uygulamalar bir taraftan kişilerin günlük yaşamlarını kolaylaştırmakta diğer taraftan ise bu uygulamaların kullanımı, pek çok kişisel verinin toplanmasına da zemin hazırlamaktadır.

#### 2.5.3.1. Web Ortamı

Web ortamı, internetin ortaya çıkışından itibaren bu alandaki en temel ortam olmakla birlikte halen varlığını güçlü bir şekilde sürdürmektedir. İnternetin ilk uygulamalarından biri olan web, internet kapsamında dijital gözetimin de başlangıç noktası sayılabilmektedir. Özellikle bu alana özgü olarak yaratılan dijital iz takibi ve profilleme için kullanılan çerezler bu ortamın en önemli gözetim araçlarındandır:

[78] Mobil uygulamalarda kullanıcıların bir hizmete erişmesini sağlayan uygulama veya arabirimin bir bileşeni. (Örn: Hava Durumu, Goolge Arama, Saat, Takvim vb.).

> Web ne yeni bir şeydir, ne de 10 yıl önceki haliyle aynıdır. Çoğu çağdaş web platformunun bir önemli karakteristiği, yüksek miktarda kişisel bilgi ve kullanıcı davranış verisini depoluyor, işleme koyuyor, onlara erişim sağlıyor ve onları satıyor olmasıdır (Fuchs, 2011: 137).

1994 yılında geliştirilen çerezler, iletişim ağının ticarileştirilmesi ve gelir kaynağı haline getirilmesinde önemli bir araç haline gelmiştir. Günümüzde çoğu büyük şirketin ana gelir kaynağı olan kullanıcı hedefli iş modellerinin gelişmesini sağlamıştır.[79] 1990'ların ortasından itibaren elektronik ticaretin gelişmesi, hali hazırda bulunan müşteri gözetleme katmanlarına bir başkasını eklemiştir. Şirketler, fareyi (mouse) her kullandıklarında bıraktıkları izden, müşterilerin isteklerini takip etmelerine izin veren çerezler ya da benzer araçlar kullanmaya başlamışlardır. Çerezler, bilgisayar kullanıcısının sabit diskinde, internette hangi siteleri ziyaret ettiğine dair verileri kaydetmenin bir yoludur. Bunlar, firmaların reklam amacıyla, kişisel bilgisayarlardan veri toplayarak, kullanıcı hedeflerini belirlemelerine izin vermektedir (Lyon, 2006: 88).

Davranışsal hedefleme ile kullanıcıların dijital hizmetlerde arkalarında bıraktıkları veri olan dijital ayak izleri istismar edilmekte, çoğu kişisel veri 'sahibinin bilgisi olmadan'[80] toplanmaktadır. Dijital ayak izleri farklı türlerde bilgiler içerebilir: Bunlar kimi zaman IP adresi, ziyaret edilen web siteleri, ziyaretin uzunluğu ve zamanı, cihaz türü, arama sorguları, konum bilgisi olmakta, kimi zaman cinsiyet ve yaş, cinsel tercih, ya da satın alınan kitaplar olabilmektedir. Tüm bu bilgiler bir araya geldiğinde, kullanıcı profili oluşturulmasını, oluşturma sürecinin gerçekleşmesini ve hesaplanmış veri analizi tarafından oluşturulan profillerin kullanılmasını sağlar ve kullanıcılar hakkında büyük miktarda veri içerisinde biçimlerin ve ilişkilerin keşfedilmesine izin verir:

> Web ile etkileşim daha doğal hale geldikçe ve web, diğerleriyle etkileşimde aracı oldukça; web tarama davranışları, bilinçdışı davranış biçimleri aracılığıyla, kim olduğumuzu eşsiz biçimde karakterize edecek kadar zengin hale gelmektedir.[81]

Çerezler kullanıcıların hangi sitelerde gezindiği, hangi reklamlara tıkladığını, daha da önemlisi hangi ürünlere/hizmetlere ya da konulara eğilimli olduklarını belirlemekte ve bunları kayıt altına almaktadır. Ayrıca 'log' denilen bir dosyalama sistemi ile yapılan aktiviteler, cihazlara kaydedilmektedir. İnternet sitelerinde bulunan web böcekleri ise görünmeyecek kadar

---

[79] https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).
[80] Pasif dijital ayak izi
[81] https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).

küçük bir boyutta olup kullanıcılara banner, iletişim formu şeklinde ya da elektronik posta olarak, hatta bazı web sitelerinin boş sayfalarına yerleştirilerek gönderilebilmektedir. Örneğin kullanıcılar, web sayfasında boş bir yere tıklandığında bir anket şirketinin pop-up reklamı ile karşılaşabilir ve bu siteye yönlendirilebilir. Bu böcekler, kişilerin aktivitelerini kaydettiği gibi, tıklanılan reklamları, ziyaret sayıları gibi bilgileri de elde edebilmektedir.

Kullanıcıların e-postalara web ortamından erişimi sırasında Google açısından dikkat çekici bir konu bulunmaktadır. Bu hizmet kapsamında kullanıcıların e-postalarının içeriğini otomatik olarak inceleyen, kaydeden ve e-postanın yanına içeriğine uygun reklamlar ekleyen bir sistem bulunmaktadır (Küzeci, 2010: 35). E-posta hizmetleriyle ilgili söylenebilecek başka bir durum da okundu bilgisidir: E-posta hizmeti sağlayıcılarının, şirketlere tanıdığı mükemmel bir gözetim aracıdır. Şirketler gönderdiği postaların hangi saatlerde okunduğunu, hangisinin okunup okunmadığını bu yolla öğrenebilmekte, kullanıcı ya da müşterisi hakkında bu verilerden de işine yarayacak sonuçlar çıkarabilmektedir.

Web ortamında anahtar kelime/konu aramanın en temel yazılım parçası ise tarayıcılardır. Temelde, kullanıcının komutlarını (çoğunlukla URL olarak), sunucuların anlayabileceği taleplere çeviren ve daha sonra sunucunun yanıtını kullanıcının anlayabileceği bir biçimde sunan yazılımlardır. Dolayısıyla, bu yapboz içerisinde tarayıcı, kullanıcının tarama alışkanlıkları hakkındaki verilerin tamamına sahip olan bir parçadır. Çoğu modern tarayıcı, kullanıcıların profil oluşturmalarına, giriş yapmalarına olanak sağlar ve kullandıkları tüm cihazlarda aynı ayarlara, yer imlerine ve geçmişe sahip olurlar. Bu da, o tarayıcıyı oluşturmuş olan şirket/kuruluşun sahibi olduğu bir merkez noktasına verilerini gönderdikleri anlamına gelmektedir.[82] Web ortamındaki reklamcılıkta tarayıcı içinde sunulan reklamlar, genellikle doğrudan bilgi iletim birimi içerisinde, reklam ağlarından kullanıcılara sunulmaktadır. Böylece, reklam ağlarının kişisel bilgilerini elde ettiği kullanıcılar, toplanan kişisel bilgilerine bağlı olarak reklam ağlarının kişiselleştirdiği reklam içeriğini görebilmektedirler (Meng vd., 2016: 3). Web ortamında reklam ağları kişilerin verilerine ulaşabilirken, mobil ortamlarda durum biraz farklıdır: Reklam servisi veren herhangi bir uygulama, kullanıcıya gösterilen kişiselleştirilmiş reklamları gözlemleyebilmektedir. Google, kullanıcı profillerini uygulama geliştiricilerle ve muhtemelen diğer reklam ağlarıyla büyük ölçüde paylaşmaktadır ve Google bu paylaşılan/sızdırılan bilginin nasıl kullanıldığını belirleyememektedir (Meng vd., 2016: 12). Bu konuya ‘mobil uygulamalar’ başlıklı bölümde detaylı olarak yer verilmiştir.

[82] https://labs.rs/en/metadata/ (erişim tarihi: 15.12.2017).

### 2.5.3.2. Arama Motorları

Erken dönemde arama motorları, basitçe aranan kelimeleri içeren belgeler dizisi ile ilişkili bir kelime dizisi oluşturmakta, bunu da kelimenin metnin içinde ya da herhangi bir yerinde geçip geçmemesine göre derecelendirilmesini esas alarak yapmaktaydı (Dreyfus, 2016: 29). Bugün ise arama motorları erken dönemdeki aranan kelimeleri aramaktan daha fazlasını yapar hale gelmiştir. Arama motorlarına yazılan her kelime o arama motorunun veri tabanlarında saklanmakta, kişilerin dijital izleri kabul edilen bu aramaları sınıflandırarak kişilerin profilini oluşturmakta, kullanıcılara bu aramalara özgü kişiselleştirilmiş reklam göstermektedir. Ayrıca kullanıcıların web ortamında karşılaştığı kişiselleştirilmiş reklamların büyük çoğunluğu bu aramalardan elde edilmektedir. Arama motorlarında aranan bir ürün/hizmet çok kısa bir süre içerisinde kullanıcılara bant reklam olarak iş ortaklığı bulunan web sitelerinde reklam olarak gösterilebilmektedir. Bazı arama motorları kendi ortaklık programları (Adwords[83] vb.) kapsamında, kişiselleştirilmiş reklamların dışında da reklam hizmeti sunmaktadır. Ürün, hizmet, web sitesi ya da çeşitli mobil uygulamaların reklamları, kişilerin yapmış olduğu aramalara göre üst kısımlarda sıralanmaktadır.

Günümüzde anahtar kelimelerin önemi de giderek artmaktadır. Arama motorlarında yalnızca birkaç anahtar kelime yazarak istenilen sonuçlara ulaşılabilmektedir. Bu anahtar kelimeler Google'ın Adwords ortaklık programında reklam verenlere öneri olarak sunduğu bir hizmettir. Ürün/hizmet ile ilgili anahtar kelimeler girilerek hedefe daha yakın sonuçlar elde edilmektedir. Anahtar kelimelerin tüm bu özellikleri bu ortamdaki gözetim için kilit rol oynamaktadır. Örneğin Google her yıl Google arama motorunda en çok aranan kelimeleri yayınlamaktadır.[84] Tüm bunlardan anlaşılacağı üzere kullanıcıların yapmış olduğu ürün/hizmet arama ya da ilgilendiği tüm konular arama motorlarına sahip şirketlerin elinde bulunmakta, şirkelerin çıkarlarına hizmet eden bir mekanizma olarak çalışmaktadır.

Anahtar kelime ve aramalar yalnızca arama motorlarında değil, çeşitli mobil uygulamalar ve araçlarla da gerçekleştirilmektedir. Mobil uygulamalar başlığı altında bu konuya değinilecek olsa da konunun daha iyi anlaşılabilmesi açısından birkaç örnek verilmesi uygun görülmüştür. Örneğin, Cloud Natural Language API[85] (Bulut Doğal Dil) adlı (Google'a göre öğrenim platformuna bağlı olan) bu araç; metin belgelerinde, haber makalelerinde veya web günlüklerinde adı geçen insanlar, yerler, olaylar ve daha fazlası hakkında *bilgi almak* için kullanılabilir. Yine buna benzer bir mobil uygulama olan klavye uygulamalarına örnek verilecek olursa; kullanıcının standart klavyesinin yerini alan bu uygulamalar, kullanıcılara

[83] Google'ın reklamcılık hizmeti.
[84] http://t24.com.tr/haber/iste-2017de-googleda-en-cok-arananlar,525250 (erişim tarihi: 18.05.2018).
[85] Cloud Natural Language API https://cloud.google.com/natural-language/ (erişim tarihi: 17.05.2018).

‘kişiselleştirme imkanı’ sunma adı altında yapılan aramaları ve sohbet esnasında konuşulanları bir anahtar kelime setine dönüştürerek kaydetmektedir. Ücretsiz olan bu uygulamalar bazı televizyonlarda bile reklam vermektedir. Burada yine “nasıl oluyor da?” sorusu sorulmalıdır. Sorunun cevabı yine çok açıktır: Kullanıcıların mobil ortamlarda ilgilendiği konular, kişisel veriler ve dijital izler bu uygulamalarca şirketlere ve reklam verenlere sızdırılmaktadır. Ayrıca bu klavyelerde ‘öğrenme’ özelliği mevcuttur. Bu uygulamalar kullanıcıların daha önce ne yazdıklarını öğrenmekte, herhangi bir yazım hatasında kelimeyi otomatik olarak düzeltme imkanı tanımaktadır. Bu durum tamamen gözetimle ilgilidir; çünkü kullanıcıların neler yazdığını, hangi konularla ilgilendiğini bilmek onu tanımanın en iyi yolu yoludur.

#### 2.5.3.3. Sosyal Medya

Sosyal medyadaki gözetim web ve arama motoru ortamlarına oranla daha detaylı ve kapsamlı olmaktadır. Web ortamında ve arama motorlarında genelde tarama geçmişi ve aranılan kelimeler ön plana çıkarken, sosyal medya tüm bunları içermekte, ayrıca kişilere ait daha detaylı bilgileri barındırdığından gözetim kapasitesini de daha geniş alanlara yaymaktadır. Başlıca sosyal medya ortamları ise Facebook, Instagram, Twitter, Google+, Whatsapp, Youtube ve benzeridir. Facebook, Instagram, Twitter ve Google+ çok yüksek oranda kullanımı olan, ciddi derecede kayıtlı kullanıcıya sahip sosyal medya ortamları olarak öne çıkmaktadır. Whatsapp ise anlık konuşma mobil uygulaması olarak ortaya çıksa da son güncellemeleriyle (fotoğraf ve durum paylaşımı, yorum yapma etkileşimi gibi) kişinin telefon rehberinde kayıtlı olan kişilerle sınırlı bir sosyal medya ortamı haline dönüşmüştür. YouTube ise video odaklı bir sosyal medya ortamıdır ve reklam verenler için özellikle son yıllarda daha da tercih edilir olmuştur.

“Sosyal medyanın varlığı kullanıcıların izlenmesine ve edinilen bilgilerin diğerlerine satılmasına bağlıdır” (Bauman ve Lyon, 2013: 18). “Bir milyar insanın dörtte üçünden fazlası, kendilerine dair en mahrem şeyleri, halka açılmasının ardından geçen beş yılda isteyerek Facebook’a yüklemişlerdir” (Chatfield, 2013: 30). Sosyal medya kullanımı, gündelik yaşam pratiklerince içselleştirilmiştir. Bu durum da gözetimi bir hiperkontrole dönüştürmüştür. Sosyal medya şirketlerinin kullanıcıları sürekli olarak kişisel bilgi ve görsellerini paylaşmaya yönlendirmeleri, hikaye ya da durum paylaşmaları için mesajlarla uyarmaları da teşhir, gözetim ve röntgenciliğe katılım çağrısı niteliği taşımaktadır (Çakır: 2015: 332, 374).

> Ticari sosyal medya üzerindeki gözetim, dinamik ve daimi olarak kullanıcı tarafından oluşturulan içeriği yaratıp paylaşan, profillere ve verilere göz atan, başkalarıyla etkileşime giren, toplulukları yaratan, katılan

> ve inşa eden ve enformasyonu yeniden yaratan üretüketiciler[86] üzerindeki gözetimdir. Facebook'ta fotoğraf ve başka görseller yükleyen, duvar iletileri ve yorumlar yazan, kişi listesine e-posta gönderen, arkadaş biriktiren veya başkalarının profillerine göz atan kullanıcılar, reklamcılara satılan izleyici metasını tesis ederler. Geleneksel kitle medyasındaki izleyici metasıyla internetteki izleyici metası arasındaki fark, ikincisindeki kullanıcıların aynı zamanda içerik üreticisi olmaları, burada kullanıcı tarafından oluşturulan içeriklerin olması ve kullanıcıların sürekli olarak yaratıcı faaliyette, iletişimde, topluluk inşasında ve içerik üretiminde bulunmasıdır (Fuchs, 2015: 152, 153).

Sosyal ağ siteleri özellikle hedefli reklamcılığa uygundur; çünkü yüksek miktarda kullanıcı beğenisi ve antipatisini depolamakta ve iletmektedir. Dolayısıyla bu verilerin ekonomik amaçlarla denetlenmesi ve kullanıcıların hangi ürünü satın alma eğilimi olduğunu bulmak mümkün hale gelmektedir. Bu durum, hedefli reklamcılığın neden çoğu kar-odaklı sosyal ağ sitelerinin gelirinin ana kaynağı ve iş modeli olduğunu açıklamaktadır. Facebook, kitle denetimi kullanmaktadır; birbirinden farklı milyonlarca kullanıcının kişisel verisini ve kullanım davranışlarını depolamakta, kıyaslamakta, onlara rahatça erişebilmekte ve onları satmaktadır. Fakat, bu kitle denetimi aynı zamanda kişiselleştirilmiş ve bireyselleştirilmiştir, çünkü her kullanıcının ilgi alanları ve göz atma davranışlarının detaylı analizi ve çevrimiçi davranışlarla diğer kullanıcıların ilgi alanlarının kıyaslanması, kullanıcıların tüketici ilgi gruplarına göre ayrılmalarını ve her kullanıcı bireye hedeflenmiş reklamlar sunulmasını sağlamaktadır. Bunun altında yatan varsayım, algoritmik seçim ve kıyaslama mekanizmalarının, kullanıcıların tüketimsel ilgi alanlarını hesaplayabildiğidir. Dolayısıyla, kişiselleştirilmiş reklamcılıkla birleştirilen büyük bir kullanıcı kitlesinin ekonomik denetim kombinasyonu, bir kişisel kitle veri denetimi türü olarak karakterize edilebilir. Hedefli reklamcılık ve ekonomik denetim kullanımı, Facebook'un gizlilik ilkesi tarafından da resmi olarak garanti altına alınmaktadır:

"Reklamcıların, reklamlarını görecek olan kullanıcı özelliklerini seçmelerine izin veriyoruz ve bu reklamlar için uygun seyirciyi seçmek amacıyla, topladığımız şahsi olmayacak şekilde teşhis edilebilen niteliklerin herhangi birisini kullanabiliriz (doğum yılınız veya diğer hassas kişisel bilgiler veya tercihler gibi, diğer kullanıcılara göstermek istemediğiniz bilgiler de dahil olmak üzere)" (Facebook Gizlilik İlkeleri, 15 Eylül 2010'da erişilmiştir). Ayrıca Facebook, kendi kullanıcılarının Facebook ile ekonomik ortaklığı olan diğer web platformlarındaki kullanıcı davranışı hakkında verileri almakta, depolamakta ve işleme koymaktadır:

[86] Alvin Toffler tarafından üretici-tüketici sözcüklerinin bir araya getirilerek internet ortamındaki üretici ve tüketici arasındaki sınırın bulanıklaştığını ifade ettiği kavramdır (Toffler, 2008).

"Bizlerle bilgi paylaşan diğer web siteleri ve reklamcılık ortakları ile program kurabiliriz. […] Bazı reklamların etkililiğini ölçmek amacıyla, diğer sitelerde belirli reklamları görüp görmediğinize veya etkileşime geçip geçmediğinize dair bilgi alabiliriz" (Facebook Gizlilik İlkeleri, 15 Eylül 2010'da erişilmiştir). Yukarıda verilen bilgi, şu anlama gelmektedir; kullanıcı eğer bir web sitesindeki reklama tıklarsa veya çevrimiçi bir mağazadan alışveriş yaparsa ve Facebook'un, siteyi yöneten şirket ile bir iş ortaklığı varsa, bu verilerin Facebook'a verildiğini ve kişiselleştirilmiş reklamlar üzerinden kullanıcıları hedeflemek için kullanıldığı sonucunu ortaya koymaktadır (Fuchs, 2011: 138, 139).

Facebook, herkesi kapsayan bir sınıflandırma makinesidir. Öncelikle kullanıcılardan üyelik için, ilgi gruplarıyla, arkadaşlarıyla sohbet edebilmesi için ve kişisel kullanıcı tarafından oluşturulmuş içerik yükleyebilmesi için kişisel veri yüklemelerini talep ederek, kullanıcıların ilgi alanlarını *tanımlar*. Kullanıcılar, örneğin Facebook'ta, sıklıkla yer bilgisi, durum ve ruh hali mesajları, aktivite mesajları, diğer profillere yorumlar, videolar ve görüntüler yayınlamaktadırlar. Bu durumda kullanıcılar, iletişimde oldukça aktif öznelerdir. Bu kalıcı, yaratıcı çevrimiçi aktivite ise, denetimin nesnesi haline gelmektedir. Facebook, kullanıcıların anında ticarileştirilen kalıcı aktif yaratıcılıklarını savunmaktadır; dolayısıyla Facebook, insan yaratıcılığını ve iletişimini tamamen ticarileştiren bir makinedir (Fuchs, 2011: 139, 140).

Gözetleme artık yalnızca devletler ve şirketler tarafından değil çevremizi kuşatan sosyal ağ kullanıcıları tarafından da gerçekleşmektedir. Kullanıcılar izinli/izinsiz ya da izin verdiği ölçüde herkes tarafından gözetlenip takip edilmektedir. Yani kişiler kendi gözetimlerine gönüllü olarak katılmaktadır. Yüz yüze iletişimde kişisel bilgilerini başkalarıyla paylaşmaktan imtina eden kişiler, sosyal medyada mahrem olan birçok şeyi paylaşma eğilimindelerdir. Facebook birçok sosyal ağ sitesine göre kullanıcılarına daha fazla gizlilik kontrolü imkanı tanığını iddia etse de Facebook'un ekosistemi görme, gösterme ve gözetle(n)meye yönelik bir iletişim biçimi oluşturmaktadır (Korkmaz, 2013: 120). Ayrıca Cambridge Analytica'ya sızdırılan kişisel verilerle birlikte kullanıcılarına daha fazla gizlilik kontrolü imkanı tanıdığı savı yerle bir olmuştur.[87]

Bir insanın tarama geçmişinin ardındaki gerçek ismini bulmak için ise veri setlerine bakmak yeterlidir. Yalnızca Facebook trafiğini, örneğin ziyaret ettiği profil sayfalarını sınıflandırarak, gerçek kişiler tespit edilebilir. Facebook "gerçek isim ilkesi" uyguladığı için, bir insanın tarama geçmişini gerçek ismiyle bağdaştırmak çok kolay bir yoldur.[88]

---

[87] https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri (erişim tarihi 22.03.2018).
[88] https://labs.rs/en/metadata/ (erişim tarihi: 15.12.2017).

Sosyal medya şirketlerinin kullandıkları algoritmalar artık o kadar gelişmiştir ki bu ortamlarda yer alıp gözetlenmemek mümkün değildir. Bu ortamlara kaydolurken başta kullanıcının telefon numarasının istenmesi ve akabinde neredeyse tüm bilgilerin profillerine eklenmesiyle birlikte kişiler, adeta sosyal medyaya kendilerini teslim etmektedirler. Bu şirketlerin de kendilerine ait bir reklam ekosistemi bulunmaktadır ve bu ortamlarda yer alan reklamlar yine kullanıcılarının ilgi alanları ve profillerine göre kişiselleştirilerek oluşturulmaktadır. Örnek verilecek olursa; Facebook'taki 'beğen' ya da Twitter'daki 'retweet' hangi ürünler ya da hangi konuyla ilgilendiğimizi belirleyebilmektedir. Bir başka örnek vermek gerekirse YouTube'da herhangi bir video izlendiğinde bu video ile bağlantılı reklamlar kullanıcılara gösterilmektedir. Örneğin bir yemek tarifi videosu izleyen kişiye herhangi bir restoranın reklamı gösterilebilmektedir. Youtube aynı zamanda kullanıcıların 'ilgilerini çekebilecek' videolarda önermektedir. Böylelikle ilgiye dayalı daha değişik videoları izlettirmekte, bu videolarla bağlantılı reklamları da göstermektedir. Kısacası bu ortamlar bir süre sonra kullanıcıları tanımaya başlamaktadır. Bu ortamlarda paylaşılan hikayeler, her türlü kişisel veri, fotoğraflar ya da yorumların şirketlerce kullanılması ya da başka şirketler ve reklam verenlerle paylaşılması, kullanıcılara bu bilgilerin korunmasıyla ilgili güçlü bir taahhüt verilememesi nedenleriyle bu alandaki gizlilik ve mahremiyet ihlalleri de gündemdeki yerini korumaya devam edecektir.

#### 2.5.3.4. Mobil Uygulamalar

Yukarıda bahsedildiği üzere mobil uygulamalar günümüzde gerçekleşen gözetimin, dijital iz takibi ve kişisel veri sızıntılarının en yoğun olduğu ortamlardan birisidir. Mobil cihazların etkin kullanımı mobil uygulamalara olan ilgiyi de artırmakta, bu duruma paralel olarak reklamlar için de çok iyi bir ortam oluşturmaktadır.

Uygulama içi reklamcılık, ücretsiz mobil uygulama ekosisteminin temel bir parçasıdır. Bu durum uygulama geliştiricilerinin kullanıcılarını ücrete tabi tutmadan, işlerinden fayda sağlayabildikleri bir 'çift taraflı kazanç' üretmektedir. Ancak web ortamındaki reklamcılıkta da olduğu gibi, uygulama içi reklamcılığın ardındaki reklam ağları, reklam yerleştirmelerinin etkililiğini/karlılığını geliştirmek için, kişiselleştirme kullanmaktadırlar. Kişiselleştirilmiş reklam sunma ihtiyacı duyan reklam ağları, kullanıcılar hakkında veri toplamaya ve onların profillerini oluşturmaya sevk edilmektedir. Mobil uygulama geliştiricileri ise çalışmalarını ücretsiz olarak yayınlayarak, uygulama içi reklamcılık sayesinde bir gelir oluşturabilirler. Geleneksel web reklamcılığında da olduğu gibi, kişiselleştirme, uygulama içi reklamcılığın etkililiğini geliştirir (ve böylelikle, uygulama geliştiricilerinin kazandığı geliri de arttırır). Bu

tür bir kişiselleştirmenin yalnızca reklam hizmeti veren tarafın belirli bir kullanıcı bilgisine (örneğin; ilgi alanları, demografik bilgiler) erişim sağlayabildiği zaman gerçekleştirilebildiği ve bundan dolayı veri sızıntısının daima bir sorun haline geldiği anlaşılmaktadır (Meng vd., 2016: 1).

Ipsos Otx[89] tarafından Nisan 2010 tarihinde ABD'de gerçekleştirilen 5000 mobil kullanıcılı bir ankette, katılımcıların %82'si akıllı telefonlarda reklamları fark ettiklerini ve %49'u da bu reklamlara bağlı olarak harekete geçtiklerini belirtmişlerdir. Uygulamalardaki reklamlar, kullanıcılarda ve onların satın alma biçimlerinde önemli bir etkiye sahiptir. Küresel mobil reklamcılık pazarına 2012 yılında ortalama 5,3 milyon dolar değer biçilmiştir, bu da reklamcıların kullanıcı biçimlerine ve kişisel veriye erişim sağlamasının ne kadar değerli olduğunu göstermektedir.[90]

Android gibi başlıca platformlarda çoğu kullanıcı, aygıtlarını kullanmadan önce Google hesaplarına giriş yaptığı için, bu hesaplardan daha fazla kişisel bilgi toplanabilir. Bir reklam ağı, bilgi toplama amaçlı tüm potansiyel yollarla kullanıcı profilleri yaratmak/güncellemek için, bu kişisel özellikleri kullanabilir ve hedef kullanıcılara uygulama içinde kişiselleştirilmiş reklamlar sunabilir. Uygulama içi reklamcılık, uygulamalarla aynı yetki düzeyindeki süreçlerde yayınlanan reklamları hedeflemektedir. Uygulama geliştiricileri de kullanıcıların gerçek ilgi alanlarını ve demografik bilgilerini, uygulama içerisindeki kullanıcıların kişiselleştirilmiş reklamlarına erişim sağlayarak öğrenebilmektedir (Meng vd., 2016: 3). Kullanıcılara mobil uygulamalara erişimden sonraki kayıt sürecinde bazı büyük şirketler tarafından entegre şekilde kolay kayıt olma seçeneği de sunulmaktadır. Örneğin, bir mobil uygulamaya giriş yapılacağı zaman e-posta ve şifre haricinde "Facebook ile bağlan" ya da "Google+ ile devam et" seçenekleri sunulmaktadır. Bu durum genelde mobil uygulama ile bu şirketler arasındaki ortaklık bağına işaret etmektedir.

Yapılan araştırmalar kullanıcının hassas kişisel bilgisinin, mobil uygulama içinde sunulan kişiselleştirilmiş reklamlar aracılığıyla, üçüncü taraf uygulama geliştiricilerine sızma olasılığını göstermiştir (Meng vd., 2016: 11). "Veri sızıntısı" bir açıdan, belki yanlış bir adlandırmadır – uygulamanın olanak sağladığı veri akışları, genellikle tesadüfi dikkatsizlikler veya kasıtsız sonuçlar değildir; fakat uygulamayı her şeyden önce mümkün kılan iş modelinin merkezidir. "Kasıtlı veri dağıtımı" daha uygun bir terimdir (Shklovski vd., 2014: 2350).

[89] (https://www.thinkwithgoogle.com/advertising-channels/mobile/the-mobile-movement/ (erişim tarihi: 17.05.2018).
[90] (https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011 (erişim tarihi: 17.05.2018).

Buradan mobil uygulamaların veri sızdırmada ana bir mekanizma olduğu, bilinçli olarak veri dağıtımı yapıldığı sonucu çıkarılmaktadır.

Sunucu uygulamalar, herhangi bir ek izne gerek duymadan tüm kişiselleştirilmiş reklamları gözlemleyebilmektedirler. Kişiselleştirme özü itibariyle kullanıcının kişisel bilgisine dayalı olarak yapıldığından, reklam ağı, kullanıcıya hangi reklamın gösterildiğini sunucu uygulamaya göstererek, topladığı kullanıcı bilgilerinden bazılarını uygulama geliştiricisine kasıtsız olarak da sızdırabilmektedir. Çalışmalar, bu tür sızdırılan bilginin, kullanıcının demografik bilgisini kesin olarak elde etmek için kullanılabileceğini göstermektedir. Bu durum özellikle hedeflemede kullanıldığı bilinen cinsiyet, yaş ve ebeveynlik durumu gibi bilgiler için doğrudur. Ek olarak, reklam ağlarının açık bir şekilde toplamıyor ya da kullanmıyor olabileceği bazı bilgiler de ayrıca uygulama geliştiricisine sızdırılabilir. Rastgele tahmin üzerinden, bir kullanıcıya servis edilen kişiselleştirilmiş reklamları gözlemleyerek bir kullanıcının gelirinin, politik yanlılığının ve medeni durumunun tahmin edilebileceği gösterilmiştir. Bu şekilde elde edilen bilgi daha sonra fiyat ayrımcılığı için kullanılabilir. Örneğin aynı ürün, farklı gelir gruplarındaki kullanıcılara farklı fiyatlarda satılabilir. Üstelik kişisel bilgi de üçüncü taraflara satılabilir ya da aktarılabilir. Uygulama içinde sunulan kişiselleştirilmiş reklamlardaki gizlilik ihlallerine karşı bir savunma oluşturmak için, daha fazla koruma oluşturulması gerekmektedir (Meng vd., 2016: 13, 14).

Tüm bunlara önlem olarak Android üzerinde kişisel kullanıcı verilerinin (kişiselleştirilmiş reklamların), yetkisiz taraflardan (uygulama geliştiricilerinden) korunması gerekliliğinin altı çizilmelidir. Aynı zamanda reklam ağının gizli bilgisinden veri alınırken sunucu uygulamanın, reklam kütüphanesinin verilerini okuması da engellenmelidir. Bunun yanında reklam ağları, mobil uygulama içi reklamcılık ekosisteminin özü olarak kullanıcının gizliliğinin korunmasından sorumludur. Reklam sağlayıcılar ürünlerinin içerisine kullanıcının gizliliğini korumak için savunma mekanizmaları yerleştirmelidirler. Çevrimiçi aramalarda gizliliği koruma kapsamı için kullanıcının arama geçmişine engeller eklenebilir ve bu teknik, karşı tarafın kişisel kullanıcı bilgisini öğrenmesini ve gizlilik tehdidinin (tamamını olmasa bile) bir kısmının azaltabilmesini sağlayabilir. Reklam ağları, kişiselleştirilmiş reklamlara engel koymanın yanı sıra, reklamcılar için daha yüzeysel oluşturulmuş hedefleme seçenekleri sunabilirler. Örneğin; reklamcıların 26 yaşındaki kullanıcıları açık olarak hedeflemelerini sağlamaktansa, hedefleme için bir yelpaze (örneğin; 25-34 yaş arası) sağlayabilirler. Bu tür yaklaşımlar, karşı tarafın erişebildiği kişisel bilginin daha yüzeysel boyutlarda olmasını sağlayabilir ve gizlilik ihlallerinin şiddetini azaltabilir. Google AdMob hali hazırda yalnızca yüzeysel boyutlarda yaş gruplarını hedeflemektedir; diğer reklam ağlarını da hedefleme

yöntemlerinde benzer bir modeli benimsemeye teşvik edilebilir. Tüm bu tedbirlerin ardındaki fikir, bu tür reklamlar aracılığıyla gerçekleştirilen gizlilik ihlalinin seviyesini kısıtlamak amacıyla, reklamdaki kişiselleştirmenin niteliğini dengelemektir. Her reklam ağının bu tür bir yaklaşımı benimsemesinin beklenmesi zor gözükmektedir. Çünkü daha az kişiselleştirilmiş reklam, reklam gelirinde ciddi kayıplara neden olabilmektedir (Meng vd., 2016: 13, 14).

Android reklam kütüphaneleri hakkında Theodore Book ve Chris Bronk tarafından 2016 yılında yapılan bir araştırma[91], bazı durumlarda mobil reklamların bir kullanıcının yerini ve kişilerini toplayabileceğini ve hatta mikrofonla ve kamera ile kişileri dinleyip izleyebileceğini göstermiştir. Prensipte, kullanıcılar (muhtemelen okuyucu da dahil), bu verilerin toplanması, paylaşılması ve işlenmesi için başvuruyla birlikte verilen bir gizlilik politikasını kabul ederek onay vermiş sayılmaktadır. Bilgilerinin bu şekilde toplanmasını istemeyen kullanıcılar ise söz konusu uygulamayı yüklememeyi seçebilirler. Bununla birlikte, mobil cihazların (dolayısıyla mobil uygulamalar ve reklamlar) çok önemli bir araç haline geldiği göz önüne alındığında, mobil dünyada bu şekilde seçim yapmak çoğu kullanıcı için çok zor olacaktır. Mobil cihazlardaki reklamlar genellikle bir uygulama içinde çalışan küçük bir program olan bir reklam kütüphanesi tarafından verilir. Kütüphane, reklam talep eder, görüntüler ve bir kullanıcı bunları tıkladığında tepki verir. Diğer programlarla aynı şeyleri yapar ve genellikle bir reklam istendiğinde mobil cihazdan iletilen bazı verileri toplarlar. Cihazların kullanım düzenlerini belirlemek de nispeten kolaydır. Reklam şirketi, kullanıcının sabahın erken saatlerinde hava durumunu kontrol ettiğini, belirli saatlerde trafiği kontrol ettiğini, hangi sosyal medya ortamını takip ettiğini ve akşamları hangi haberleri okuduğunu biliyor olabilir. Şirket, telefonun geceleri belirli bir mahalle içindeki bir ev ağında, belirli bir şirketin kurumsal ağında gün boyunca olduğunu veya akşamları bir kafede göründüğünü öğrenebilir. Bu verilerin tümü, kullanıcı alışkanlıklarının ayrıntılı bir profilini sağlayabilir. Ayrıca kullanıcının tüm verileri, onunla etkileşime geçen diğer kullanıcı verileriyle de bir araya getirilebilmektedir. Ancak hepsi bu kadarla da sınırlı değildir. Mobil reklam kitaplıklarını kullanan bir reklamcılık şirketi, birçok kullanıcı hakkında bilgi toplayabilir, iş yeri veya ev ağı verilerinden kimlerin aile üyeleri olabileceğini çıkarabilir. Sosyal bağlantılar, Wi-Fi erişim noktalarına ya da mobil internet şebekelerine erişimden toplanabilir. Ayrıca, iş arkadaşlarını tanımlamak ve kullanıcının en çok zaman harcadığı insanları haritaya koymak kolaylaşmakta ve büyük bir doğrulukla anlaşılabilmektedir.[92] Şirketler bizim nerede, ne zaman, kimlerle ne yaptığımızı merak etmekte, mobil uygulamaların veri sızdırma mekanizmalarını da bunlara göre ayarlanmaktadır. Örneğin

[91] http://journals.uic.edu/ojs/index.php/fm/article/view/6154/5215 (erişim tarihi: 22.05.2017).
[92] http://journals.uic.edu/ojs/index.php/fm/article/view/6154/5215 (erişim tarihi: 22.05.2017).

konum bilgisi açık, sosyal medya ortamlarından herhangi birini kullanan bir kişiden, bir fotoğraf çektiğinde öncelikle arkadaşlarını etiketlemesini daha sonra fotoğrafın hangi konumda olduğunun anlaşılabilmesi için herhangi bir yerle ilişkilendirilmesini (bu büyük ihtimalle Google Haritalar olacaktır), fotoğrafı sosyal medyada paylaşacaksa duyguları veya fotoğrafın konusunun (hashtag) eklemesini isteyecektir. Görüldüğü üzere mobil uygulamalar, kişilerin etrafını yukarıda bahsedilenleri öğrenebilmek için adeta çevrelemiş durumdadır. Konum bilgileri ile ilgili bazı araştırmalar göstermektedir ki, reklam kütüphanelerinin ağırlıklı erişim yüzdelerinde konum bilgisi yüzde 49.6 ile ilk sıradadır.[93]

Mobil taşıyıcılar, operatörün hizmet verdiği alana coğrafik olarak dağıtılan bir baz istasyonu altyapısına sahiplerdir. Baz istasyonları, mobil altyapının tamamının bel kemiğini oluşturmaktadır. Tüm taşıyıcıların arşivlediği genel bir üst veri seti vardır. Bu set içerisinde arayanın numarası, arananın numarası, IMEI, baz istasyon detayları, çağrının tarihi ve zamanı, çağrının süresi, internet veri miktarı, hizmet türü, her iki tarafın da kimlikleri hakkında detaylar, mevcut cihazda kullanılmış tüm SIM kartların listesi bulunmaktadır.[94]

Günümüzde Google Haritalar gibi coğrafi bilgi sistemlerinden kaçınmak genelde zordur. Fiziksel katmanı, mobil telefonlardan gelen konum verisiyle zenginleştirilmiş çoklu bilgi katmanlarıyla birleştirerek, kendilerini fiziksel alanı, büyük şehirlerin karmaşık toplu ulaşım sistemlerini, ticari ve sosyal hizmetleri, tarihsel bilgiyi ya da eğitim merkezlerini içeren esaslı bir araç olarak kabul ettirmektedirler. Otomatik pilotla fiziksel alanlarda hareket edilmesini sağlamaktadırlar. Fakat bu coğrafi bilgi sistemleri, yalnızca çevrimiçi davranış verilerimizi değil, aynı zamanda fiziksel alanlarla nasıl etkileşime geçtiğimizin bilgisini de toplayan hizmetler sağlamaktadır.[95] Bugün bazı aileler çeşitli mobil uygulamalarla birbirlerini takip edebilmektedir. Kişilerin cihazlarındaki GPS özelliği sayesinde onların nerede oldukları, hangi konumlarda daha sık bulundukları izlenebilmektedir. Hedef noktalar belirlenmişse ve takip edilen cihaz bu hedef noktalara varırsa takip eden kişiler bir mesajla ya da bildirimle uyarılabilmektedir. Hatta takip edilen cihazların anlık şarj durumları bile görüntülenebilmektedir.

Irina Shklovski vd. (2014: 2354)'nin çalışmasında akıllı telefon kullanıcıları, fazla ayrıcalıklı uygulamalarının tamamını silmek istememektedirler. Bunun, "ücretsiz" bir şey almanın bedeli olduğunu söylemekte ve olumsuz bir şey olmadığı sürece bu bedeli ödemede herhangi bir sorun görmemektedirler. Araştırmada bir katılımcının söyledikleri ise çok

[93] http://journals.uic.edu/ojs/index.php/fm/article/view/6154/5215 (erişim tarihi: 22.05.2017).
[94] https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/ (erişim tarihi: 15.12.2017).
[95] https://labs.rs/en/metadata/ (erişim tarihi: 15.12.2017).

çarpıcıdır: *"Şu atasözüne inanıyorum: "Bedavadan bir öğlen yemeği aldığınız zaman; aslında siz bir başkasına servis ediliyorsunuzdur. Ücretsiz eğlencenin değiş-tokuşu budur"*. Buradan anlaşılacağı üzere ücretsiz mobil uygulamalar, kullanıcıların kişisel verilerini sızdırarak hizmetin bedelini yine kullanıcılara ödettirmektedir. Dolayısıyla ortada ücretsiz olan bir durum yoktur. Ücretsiz olarak görünen; ama arka planda verileri sızdıran uygulamalar vardır. Shklovski vd.'nin araştırmasında bahsi geçen "olumsuz bir şey olmadığı sürece bedel ödeme" durumunun nasıl anlaşılacağı da bilinmemektedir. Kimi kullanıcı için bu veriler mahremken, kimileri için sıradan bir veridir. Sonuç olarak mobil cihazlar artık kişisel, mahrem alanlar olarak değerlendirilmektedir. Bu alanlarda yaşanabilecek her türlü mahremiyet ihlali ciddi sonuçlar doğurabilecek nitelikte olacaktır.

Altman, öncelikli (mahrem) bir bölgeye tekrarlanan saldırıların, bir insanın öz-kimliği üzerinde ciddi sonuçlar doğurabileceğini ve erişimi düzenleyememenin de uzun süreçte öz-saygı eksikliğine neden olabileceğini belirtmektedir. Bir insanın gizliliğine saldırmak, o insanın yaşam kontrolünü elinden almaktan daha önemlidir ve bu, bir bireyin bağımsızlığını ve itibarını ciddi şekilde etkileyebilir. Altman'a göre bu, "kontrolü ciddi şekilde başkalarına vermektir, yalnızca bilginin ifşası değildir". Bir insanın mahrem bölgesine tekrarlanan saldırılar ve çözümün var olmadığı inancı, insanlara kendilerini savunabilecekleri yollar gösterildiğinde bile saldırılara tepki vermeyi bıraktıkları zaman öğrenilmiş çaresizlikle sonuçlanabilmektedir. Öğrenilmiş çaresizlik genel olarak; kişiler bir durumun değiştirilemez veya kaçınılmaz olduğuna inandığında ve bir çözüm yolu ortaya çıksa bile o duruma dair nedenler oluşturduklarında gerçekleşmektedir (akt. Shklovski vd., 2014: 2354).

Shklovski vd. (2014: 2354, 2355)'nin çalışmasında bir katılımcının şu sözü dikkate değerdir: *"Sessizce kabul ediyorum. Bunu düşünmemi sağladığınızda, bunu aslında sevmedim, fakat muhtemelen indireceğim bir sonraki uygulamada bunları tamamen unutmuş olacağım"*. Diğer bir katılımcı ise: *"Bu noktada bu, bir kötülükmüş gibi görünüyor. Çünkü çok yaygın, sanırım bu durum hiçbir zaman yok olmayacak"* demiştir. Her iki durumda da, katılımcının durumu değiştirmek için yapabileceği hiçbir şey olmadığı ve devam etmek istiyorsa, bunu kabul etmek zorunda olduğu konusunda üstü kapalı bir kabulleniş bulunmaktadır. Çalışmada katılımcıların akıllı telefonlarındaki belirli uygulamaların bilgi paylaşımı eylemleri hakkında bilgilendiklerinde, çoğunlukla şaşkınlık ve hatta öfke ifadelerinde bulunmakta; fakat akıllı telefonlarını tekrar kullanmaya başladıklarında, işlerine olduğu şekilde devam ettikleri görülmektedir. Bu durum reklamcılık endüstrisi için iyi bir haber olabilir, çünkü tüketiciler bilgi paylaşımını protesto etseler de, işin derinliğinde davranışlarını değiştirecek kadar bu konuyla ilgilenmemektedirler.

#### 2.5.3.4.1. Gizlilik Politikaları

Neredeyse tüm kullanıcılar, cihazlarına yükledikleri uygulamalar aracılığıyla bağlı oldukları Hizmet Kullanım Şartları, Gizlilik Politikaları ve diğer yasal belgelerin önemini görmezden gelmektedirler. Diğer yandan bu uygulamaları ücretsiz olarak satan/sunan şirketler, bu belgeleri kullanıcının uygulamanın çalışmak için talep ettiği minimum izinden daha fazlasını vermesini sağlayacak bir biçimde düzenlemektedirler.[96]

Kullanıcılar akıllı telefonları üzerinden her ay ortalama 27 uygulamaya aktif biçimde erişmektedir. Aylık kullanılan uygulama sayısı hızla yükselmese de (2011 yılında 23,2 uygulamadan 2013 yılında 26,8 uygulamaya), Hizmet Kullanım Şartları ve Gizlilik İlkelerinin okunmaması sorunu, uygulama kullanımında ortak bir sorun olmaya devam etmektedir[97]. Ancak, android kullanıcıları için yüklenen uygulama sayısı, yıllık ortalama 95'tir[98]. Analizler, bir Gizlilik Politikasının ortalama 2.518 kelime uzunluğunda olduğunu ve 10 dakika okunma süresinin olduğunu göstermektedir ki, bu da, kullanıcının yüklediği uygulamaların Gizlilik İlkelerini okumak için kabaca 950 dakika (15,83 saat veya 2 iş günü) harcaması gerektiği anlamına gelmektedir.[99] Bu tür koşullar ve ilkeler genellikle çok uzundur ve karmaşık, hukuki bir dille yazılmıştır. Dolayısıyla her kullanıcının detayları okuduğu ve tüm kuralları gerçekten kabul ettiğinden şüphe duyulabilir. Facebook'un gizlilik ilkelerinin mevcut İngilizce versiyonu (5 Ekim 2010'dan alınan versiyon) 35,553 karakter bulundurmaktadır, bu da ortalama 11 sayfa tek boşluklu metin anlamına gelmektedir. Mevcut Facebook kullanım koşullarında 23,540 karakter bulunmaktadır (4 Ekim 2010'da erişildi) bu da ortalama sekiz sayfaya denk gelmektedir. Yüz milyonlarca Facebook kullanıcısının bu kuralları baştan sona, tamamen incelemesi ve tüm detayları anlayarak tamamını kabul etmesi imkansızdır (Fuchs, 2011: 142).

Önemli olan bu kafa karıştırıcı, karmaşık ve zamanı sömüren Gizlilik İlkeleri ve Hizmet Kullanım Şartlarının ardındaki hikayeyi anlamaktır. Hizmet Kullanım Şartları ve Gizlilik Politikalarının, ortalama bir kullanıcının anlaması için uzun, karmaşık ve zor düzenlenmesinin birçok nedeni olabilir. Birincisi, uygulama üreten veya dağıtımı yapan şirketlerin, itibarlarını pahalıya mal olacak biçimde zedeleyebilecek hukuki sonuçları önlemek ve kullanıcıdan gelebilecek herhangi bir potansiyel iddiadan kendilerini korumak istemeleri, ikinci olası neden ise, kullanıcının cihazındaki kişisel bilgiye erişimi mümkün kılmaktır[100]. Tüm bunların yanında

---

[96] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).
[97] http://techcrunch.com/2014/07/01/an-upper-limit-for-apps-new-data-suggests-consumers-only-use-around-two-dozen-apps-per-month/ (erişim tarihi: 19.05.2018).
[98] http://thenextweb.com/apps/2014/08/26/android-users-average-95-apps-installed-phones-according-yahoo-aviate-data/ (erişim tarihi: 19.05.2018).
[99] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).
[100] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

birçok Gizlilik Politikası ya da Hizmet Kullanım Koşulları ile hiç karşılaşılmayabilir. Bu duruma örnek verirsek, herhangi bir cihaz aldığımızda içerisindeki işletim sistemleri ve birçok uygulama yüklü haldedir. Android işletim sistemi veya Windows işletim sistemi en baştan cihaza kurulduğunda hem gizlilik sözleşmesi hem de kullanıcı sözleşmeleri kişilerin onayına sunulmaktadır. Hatta Windows tabanlı cihazlarda kişiselleştirmenin devre dışı bırakılabilme seçeneği bile bulunmaktadır. Ayrıca birçok mobil uygulama bu cihazlarda yüklü haldedir. Bunlarda başlıca Google uygulamaları, hava durumu, müzik ya da sohbet uygulamalarıdır. Kişiler 'uygulama yöneticisi' bölümünü kontrol etmediği sürece (herhangi bir güncelleştirme aldığında da fark edebilir) bu uygulamalarla karşılaşmamaktadırlar. Başlı başına bu durum bile bir gizlilik ihlalidir ve bu durumun önlenebilmesi için cihazlardaki varsayılan ayarlarında kişiselleştirmelerin kapalı, gizlilik veya hizmet sözleşmelerinin kullanıcının iznine tabi olması gerekmektedir. Sistem ayarları dışında herhangi bir mobil uygulamanın yüklü olmaması, eğer yüklü ise kullanıcı uygulamayı çalıştırana kadar devre dışı olması ve gereken mobil izinlerin kullanıcı tarafından verilmesi gerekmektedir.

#### 2.5.3.4.3. Mobil İzinler

Mobil izinler, günümüz uygulama marketlerinden indirilen ve mobil cihazlarda sıklıkla kullanılan birçok popüler uygulama tarafından kullanıcının cihazına erişim için hem teknik açıdan (mobil uygulamanın cihazda sağlıklı olarak çalışabilmesi için gereken izinler) hem de kişisel verileri sızdırması için kullanılan bir yöntemdir. Örnek vermek gerekirse Instagram uygulamasına 'fotoğraf ve video çekme' izni verilmezse kullanıcı teknik olarak fotoğrafını paylaşamayacaktır. Ancak aynı uygulamanın 'cihazın uyumasını engelleme' izni teknik bir durumdan daha farklı bir durumdur. Cihazın uyuması kullanıcının kontrolündeyken Instagram uygulaması bunu bile değiştirebilecek izni elde etmektedir.

Mobil uygulamaların sıklıkla kullandığı mobil izinler aşağıda belirtilmiştir:

- **Telefon görüşmesi yapma:** Bu izin, uygulamaların telefon görüşmesi yapmalarına izin vermektedir. Uygulamalar telefon ekranını başlatabilir ve numarayı yazabilirler, fakat kullanıcıyı arama tuşuna basmaya teşvik etmesi gerekmektedir; bu izin uygulamaların tüm süreci arka planda yürütmesini sağlamaktadır.
- **Kısa mesaj veya çoklu ortam mesajı gönderme:** Bu izin, uygulamanın kullanıcı adına kısa mesaj veya çoklu ortam mesajı göndermesine izin vermektedir.
- **Dijital hafıza kartı içeriğini değiştirme/silme:** Bu izin, uygulamaların dijital hafıza kartında depolanmış herhangi bir şeyi okuma, yazma ve silmesine izin vermektedir.

Birçok kullanıcı, uygulamaların hafıza kartına veri yazmasını istediği için, bu izni isteme konusunda da birçok meşru neden vardır.

- **Kişileri okuma:** Eğer uygulama, kişi detaylarına erişmek için doğrudan belirli bir özellik sunmuyorsa, bu izni istemesinin de herhangi bir nedeni yoktur. Telefonda depolanan her kişiye erişim sağlayabilir.
- **Kişi verisi yazma:** Hızlı arama için kullanılan uygulamalar ve belirli sosyal ağ uygulamaları düzenli işlemler için bu izni isterler, aksi takdirde bu iznin istenmesi gerekçesizdir.
- **Takvim verisini okuma:** Takvim verisi genelde kişiler ve yer bilgilerini içerir, bu durum da onu belirli bir hassas veri türü haline getirmektedir.
- **Tarayıcı geçmişi ve yer imleri okuma:** Tarayıcı geçmişi ve yer imleri, kullanıcı hakkında oldukça fazla şeyi ortaya çıkarmaktadır, dolayısıyla bunlara erişim sağlanması da belirli bir seviyede gizlilik ihlali uygulaması haline gelmektedir.
- **Hassas kayıtları okuma:** Kayıtlar, mantıksal olarak haritaya dökülebilecek veriler içermektedir ve kullanıcı eylemlerini açığa çıkarmaktadır. Bazı uygulamalar, kullanıcı adları ve şifreler gibi verileri kaydetmektedir.
- **Global sistem ayarlarını değiştirme:** Global sistem ayalarını değiştirmek, değişimler diğer türden kullanıcı verisini ortaya çıkarıyorsa, müdahaleci işlem sayılabilir (Konum ayarlarını açma ve kapatma).
- **Çalışan uygulamalara erişme:** Çalışan uygulamalar listesi, görev yöneticisi gibi uygulamalar için yerinde bir kaynaktır. Fakat aynı zamanda kullanıcının tercihleri ve kullanılan hizmetler hakkında bilgileri de açığa çıkarmaktadır.
- **Sistem düzeyi bildirimlerini gösterme:** Bu iznin suiistimali, açılır reklam miktarının artmasına neden olabilir.
- **Fotoğraf ve video çekme:** Bu izin, uygulamanın daha ileri bir teşvik olmaksızın, fotoğraf ve video çekmesine müsaade eder.
- **Ekstra konum komutlarına erişim:** Bu izne sahip olan uygulamalar, kullanıcın coğrafi konumu hakkında detaylı bilgiye sahip olmaktadırlar.
- **Yapılandırmayı değiştirme:** Bu iznin ne sağladığı konusunda, dil ve bölgesel ayarları değiştirme haricinde net bir bilgi yoktur.
- **Arka plan işlemlerini etkisiz hale getirme:** Anti-virüs ve benzeri uygulamaların işlemlerini etkisiz hale getirdiği takdirde, riskli olma potansiyeli taşıyan bir izindir.

- **Giden çağrıları yönlendirme:** Bu izin, giden çağrıyla bağlantılı üst veriye erişim sağlamaktadır, bu durumda bu izin yalnızca internet üzerinden sesli iletişim uygulamalarına verilmelidir.
- **Oturum başlatma protokolü kullanma:** Oturum başlatma protokolü, internet üzerinden sesli iletişim servisleri için kullanılmaktadır, bu durumda, "telefon görüşmesi yapma" izni ile benzer özelliklere sahiptir.
- **Güvenlik ayarları yazma:** Bu izin, sistem uygulamaları için ayrılmalıdır.
- **Profil okuma:** Bu izin, uygulamanın telefonda depolanmış olan kullanıcının kişisel hesap detaylarını okumasına müsaade eder.
- **Kısa mesaj okuma:** Bu iznin verildiği uygulamalar, kısa mesajlara erişebilir ve onları okuyabilir, bu da ciddi bir gizlilik ihlalidir.
- **Çağrı kaydı yazma:** Bu izin, kötücül davranışı saklamak için suistimal edilebilir.
- **Profil yazma:** Bu izne sahip uygulamalar, kullanıcı profiline veri yazabilirler.
- **Sosyal akışı okuma:** Bu izin, uygulamaların Facebook ve Twitter gibi sosyal ağlardaki güncellemelere erişmesini sağlar. Bu yalnızca kullanıcının kendi güncellemelerini değil, aynı zamanda kullanıcıların kendi ağlarının güncellemelerini de içerir.
- **Hesapları onaylama:** Bu izin, uygulamaların şifreler gibi kimlik bilgilerini onaylamalarına müsaade eder ve bu izin, genelde kimlik hırsızlığı için kullanılsa da, kullanıcı onayı talep eden uygulamalar için meşrudur, o uygulamalar için ayrılmalıdır.
- **E-posta eklerini okuma:** E-posta ekleri genelde hassas içerikten oluşur, dolayısıyla özel olmalıdır. Bu izin, e-posta müşterisi uygulamaları için ayrılmalıdır.
- **Kısa mesaj/çoklu ortam mesajları alma:** Bu izin, uygulamanın gelen kısa mesajı/çoklu ortam mesajını denetlemesini, onları kaydetmesini veya işlemi önceden şekillendirmesini sağlar.
- **Sistem servisi ekleme:** Bu izin yalnızca sistem uygulamaları için kullanılmalıdır.
- **Anlık iletileri (IM) okuma:** Bu izni talep eden uygulamalar, Facebook Messenger ve benzeri uygulamalardaki anlık iletileri okuyabilirler.[101]

  **Bazı mobil uygulamaların verdiği izinler de aşağıdaki tablodaki gibidir:**

**Tablo 2.1 Whatsapp - Gmail Uygulamalarının Erişim İzinleri[102]**

| | |
|---|---|
| **Whatsapp**:<br>o Uygulama içi satın alımlar:<br>▪ Uygulama içi satın alımlar | **Gmail:**<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi |

[101] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).
[102] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

| | |
|---|---|
| o Cihaz & uygulama geçmişi:<br>▪ Çalışan uygulamaları görmek<br>o Kimlik:<br>▪ Cihazdaki hesapları bulma<br>▪ Hesap ekleme veya silme<br>▪ Kişi kartınızı okuma<br>o Kişiler / Takvim:<br>▪ Kişilerinizi okuma<br>▪ Kişilerinizi düzenleme<br>o Konum:<br>▪ (Ağa dayalı) Yaklaşık konum<br>▪ Kesin konum (GPS ve ağa dayalı)<br>o Kısa Mesaj:<br>▪ Mesaj alma (Kısa mesaj)<br>▪ Kısa mesaj gönderme<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi<br>▪ USB deponuzun içeriklerini düzenleme veya silme<br>o Kamera / Mikrofon:<br>▪ Fotoğraf veya video çekme<br>▪ Ses kaydetme<br>o Kablosuz Ağ Bağlantı Bilgisi:<br>▪ Kablosuz Ağ bağlantılarını görüntüleme<br>o Cihaz ID & Arama Bilgisi:<br>▪ Telefon durumunu ve kimliğini okuma<br>o Diğer:<br>▪ Bildirimsiz dosya indirme<br>▪ Başlangıçta çalışma<br>▪ Cihazın uyumasını engelleme<br>▪ Ağ bağlantıları görüntüleme<br>▪ Kısa yol oluşturma<br>▪ Pil istatistiklerini okuma<br>▪ Ses ayarlarını değiştirme<br>▪ Google hizmet kurulumunu okuma<br>▪ Diğer uygulamalar üzerine yazma<br>▪ Tam ağ erişimi<br>▪ Senkronizasyon ayarlarını okuma<br>▪ Titreşimi kontrol etme<br>▪ Ağ bağlanabilirliğini değiştirme | ▪ USB deponuzun içeriklerini düzenleme veya silme<br>o Telefon:<br>▪ Arama kayıtlarını okuma<br>▪ Arama kaydı yazma<br>o Kişiler / Takvim:<br>▪ Kişilerinizi okuma<br>▪ Kişilerinizi düzenleme<br>o Kimlik:<br>▪ Hesap ekleme veya silme<br>▪ Kişi kartınızı okuma<br>o Diğer:<br>▪ Titreşimi kontrol etme<br>▪ Senkronizasyon ayarlarını okuma<br>▪ Tam ağ erişimi<br>▪ Google hizmet kurulumunu okuma<br>▪ Cihazdaki hesapları kullanma<br>▪ Yakın Saha İletişimini kontrol etme<br>▪ Cihazın uyumasını engelleme<br>▪ Ağ bağlantılarını görüntüleme<br>▪ Başlangıçta çalışma<br>▪ Bildirimsiz dosya indirme<br>▪ Abonelik bilgileri yazma<br>▪ Gmail okuma<br>▪ Abonelik bilgileri okuma<br>▪ Gmail'i düzenleme<br>▪ Yapılandırılmış hesapları görüntüleme<br>▪ Gmail gönderme |

Anlık mesajlaşma olarak piyasaya çıkan ancak sonrasında bir sosyal medya uygulaması olarak devam eden Whattsapp ve bir Google hizmeti olan e-posta uygulaması Gmail'in mobil izinleri karşılaştırıldığında Whatsapp'ın Gmail'e göre daha çok mobil izin talep ettiği görülmektedir. Ancak Gmail, bir e-posta uygulaması olmasına rağmen arama kaydı okuma-yazma, kişi kartı okuma, hesap ekleme-silme izni talep etmektedir. Gmail, 'kişi kartı okuma' iznini kişinin rehberindeki kişiye e-posta göndermek için kullanmak istiyor olabilir; ancak yine de diğer izinleri (hesap-ekleme silme) elde etmesinde hiçbir gerekçe bulunmamaktadır.

**Tablo 2.2 Google Chrome - DuckDuck Go Tarayıcılarının Erişim İzinleri[103]**

| **Chrome:** | **DuckDuck Go:** |
|---|---|
| o Kişiler / Takvim:<br>▪ Takvim etkinliklerini ve özel bilgi okuma<br>▪ Sahibin bilgisi olmadan takvim etkinliği ekleme/düzenleme ve misafirlere e-posta gönderme<br>▪ Kişilerinizi okuma<br>▪ Kişilerinizi düzenleme<br>o Kimlik:<br>▪ Cihazdaki hesapları bulma<br>▪ Hesap ekleme veya silme<br>▪ Kişi kartınızı okuma<br>o Cihaz & uygulama geçmişi:<br>▪ Web yer imlerini ve geçmişini okumak<br>▪ Çalışan uygulamaları görme<br>o Cihaz & uygulama geçmişi:<br>▪ Web yer imlerini ve geçmişini okumak<br>o Kablosuz Ağ Bağlantı Bilgisi:<br>▪ Kablosuz Ağ bağlantılarını görme<br>o Kamera / Mikrofon:<br>▪ Fotoğraf ve video çekme<br>▪ Ses kaydetme<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi<br>▪ USB deponuzun içeriklerini düzenleme veya silme<br>o Konum:<br>▪ (Ağa dayalı) Yaklaşık konum<br>▪ Kesin konum (GPS ve ağa dayalı)<br>o Kimlik:<br>▪ Cihazdaki hesapları bulma<br>▪ Hesap ekleme veya silme<br>o Diğer:<br>▪ Titreşimi kontrol etme<br>▪ Senkronizasyon ayarlarını okuma<br>▪ Tam ağ erişimi<br>▪ Senkronizasyonu açma ve kapama<br>▪ Ses ayarlarını değiştirme<br>▪ Cihazdaki hesapları kullanma<br>▪ Kısa yollar oluşturma<br>▪ Yakın Saha İletişimini kontrol etme<br>▪ Cihazın uyumasını engelleme<br>▪ Ağ bağlantılarını görüntüleme<br>▪ Senkronizasyon istatistiklerini okuma<br>▪ Web yer imlerini ve geçmişini okumak | o Diğer:<br>▪ Tam ağ erişimi<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi<br>▪ USB deponuzun içeriklerini düzenleme veya silme |

Tablo 2.2'de görüldüğü üzere tamamen reklam üzerine kurulu Google Chrome tarayıcısı ile herhangi bir kişisel veriyi, dijital izi takip edip kaydetmediğini ve sızdırmadığını iddia eden

[103] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

DuckDuck Go tarayıcısı karşılaştırılmıştır. DuckDuck Go yalnızca uygulamanın çalışabilmesi için gerekli olan izinleri talep ederken, Google Chrome, neredeyse tüm izinleri talep etmekte, adeta bir gözetim makinesi olarak çalışmaktadır.

**Tablo 2.3 Facebook - Instagram Uygulamalarının Erişim İzinleri**[104]

| **Facebook:** | **Instagram:** |
|---|---|
| o Konum:<br>▪ (Ağa dayalı) Yaklaşık konum<br>▪ Kesin konum (GPS ve ağa dayalı)<br>o Kısa Mesaj:<br>▪ Mesajlarınızı okuma (Kısa mesaj veya çoklu ortam mesajı)<br>o Telefon:<br>▪ Arama kaydı yazma<br>▪ Arama kayıtlarını okuma<br>▪ Telefon numaralarını doğrudan arama<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi<br>▪ USB deponuzun içeriklerini düzenleme veya silme<br>o Kamera / Mikrofon:<br>▪ Fotoğraf ve video çekme<br>▪ Ses kaydetme<br>o Cihaz ID & Arama Bilgisi:<br>▪ Telefon durumu ve kimliği okuma<br>o Kablosuz Ağ Bağlantı Bilgisi:<br>▪ Kablosuz Ağ bağlantılarını görme<br>o Cihaz & uygulama geçmişi:<br>▪ Çalışan uygulamaları görmek<br>o Kimlik:<br>▪ Cihazdaki hesapları bulma<br>▪ Hesap ekleme veya silme<br>▪ Kişi kartınızı okuma<br>o Kişiler & Takvim:<br>▪ Kişilerinizi okuma<br>▪ Cihazdaki hesapları bağlama<br>▪ Kişilerinizi düzenleme<br>o Diğer:<br>▪ Bildirimsiz dosya indirme<br>▪ Duvar kâğıdı boyutunu ayarlama<br>▪ Hesaplar oluşturma ve şifre belirleme<br>▪ Başlangıçta çalışma<br>▪ Cihazın uyumasını engelleme<br>▪ Ağ bağlantılarını görüntüleme<br>▪ Ses ayarlarını değiştirme<br>▪ Senkronizasyonu açma ve kapama<br>▪ Diğer uygulamalar üzerine yazma<br>▪ Durum çubuğunu yok etme/genişletme<br>▪ Ağ bağlanılabilirliğini değiştirme | o Cihaz & uygulama geçmişi:<br>▪ Çalışan uygulamaları görmek<br>o Kimlik:<br>▪ Cihazdaki hesapları bulma<br>▪ Hesap ekleme veya silme<br>o Kişiler & Takvim:<br>▪ Kişilerinizi okuma<br>o Konum:<br>▪ Kesin konum (GPS ve ağa dayalı)<br>o Fotoğraflar / Medya Dosyaları:<br>▪ Korumalı hafızaya erişim denemesi<br>▪ USB deponuzun içeriklerini düzenleme veya silme<br>o Kamera / Mikrofon:<br>▪ Fotoğraf ve video çekme<br>▪ Ses kaydetme<br>o Diğer:<br>▪ Ekran oryantasyonunu değiştirme<br>▪ İnternetten veri alma<br>▪ Geçici belleği okuma<br>▪ Pil istatistiklerini okuma<br>▪ Cihazın uyumasını engelleme<br>▪ Ağ bağlantılarını görüntüleme |

[104] https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

| | |
|---|---|
| ▪ Duvar kâğıdı ayarlama<br>▪ İstek dışı yayın gönderme<br>▪ Pil istatistiklerini okuma<br>▪ Çalışan uygulamaları yeniden sıralama<br>▪ Kablosuz ağa bağlanma/bağlanmama<br>▪ Senkronizasyon ayarlarını okuma<br>▪ Titreşimi kontrol etme | |

Tablo 2.3'te görüldüğü üzere yine kişisel verilerin elde edilmesine hizmet eden ve reklam üzerine kurulu bir sosyal medya uygulaması olan Facebook ve ona nazaran daha az erişim izni talep eden Instagram sosyal medya uygulaması karşılaştırılmıştır. Burada Facebook'un neredeyse tüm erişim izinlerini talep ettiği görülmektedir. Özellikle 'bildirimsiz dosya indirme' izni ile ne gibi bir işlem yapacağı sorusu da akılları kurcalamaktadır. Instagram uygulamasının ise daha çok teknik erişimden yararlandığı anlaşılmaktadır.

Tüm bu tablolardan da anlaşılacağı üzere, mobil uygulama geliştiricileri 'mobil izinler' aracılığıyla kullanıcıların cihazlarına erişmekte, kişilere ait özel alanları işgal etmekte, cihaz ayar ve araçlarını istediğinde değiştirebilecek imkanı ellerinde bulundurmaktadır. Tüm bunların sonucu olarak da kullanıcıların kişisel verileri kaydedilmekte, işlenmekte, aktarılmakta ve kişilerin mahremiyeti açıkça ihlal edilmektedir.

# ÜÇÜNCÜ BÖLÜM
# DİJİTAL GÖÇMENLER VE DİJİTAL YERLİLERİN KARŞILAŞTIRMALI ANALİZİ

## 3.1. Araştırmanın Tasarımı

Araştırma, Ankara ilinin üç büyük ilçesinde[105] gerçekleştirilmiştir. Ankara ilinin seçilme nedenlerinin başında, metropol ve kozmopolit karakterinin yanı sıra, başkent olması, emekli nüfusunun fazla olması[106], kamu çalışanının fazla olması[107], teknoloji ve bilişim ile ilgili kamu kurumlarına olan yakınlık, Kişisel Verileri Koruma Kurumu'nun merkezinin bulunması gibi faktörler yer almaktadır.

Çalışmamızda kuşaklar arası değerlendirme söz konusu olduğu için, dijital teknolojiyle tanışma yaşı araştırma kapsamında önemlidir. Dijital olanakların kullanımının öncelikle bu olanaklara görece daha yoğun sahiplik gösteren devlet kurumlarında başlamış olduğu bilinmektedir. Günümüzde kişilerin büyük bölümü çalışma hayatları içinde internet kullanımını öğrenmeye başlamaktadırlar (Becerikli, 2013: 25). Dijital olanaklarla iş yerlerinde tanışan dijital göçmenlerin durumu da dijital beceri açısından araştırma için önem arz etmektedir. Daha önce yapılan çoğu çalışma, iş yerinde bilgisayar tecrübesi edinmenin, belirli hobilere sahip olmanın ve okula giden çocuklarla bir aile sahibi olmanın da yetişkinlerde dijital beceri kazanımında belirleyici olduğunu ortaya koymaktadır (Dijk ve Hacker, 2003: 319). Bu nedenle Ankara ilindeki kamu çalışanlarının da yüksek oranda olması dijital yatkınlık açısından değerlidir. Dijital yerliler dijital göçmenlere göre teknoloji kullanımında daha etkindir. Dijital yerlilerin dijital olanaklarla evlerinde ve okullarında tanışmış olması, çeşitli çevresel faktörler nedeniyle de dijital göçmenlere oranla dijital becerilere daha yatkın oldukları sonucunu doğurmaktadır.

Araştırmanın evrenini Ankara ilinin üç büyük ilçesinde bulunan kişiler oluşturmaktadır. Araştırmanın örneklemini ise mobil cihaz kullanan ve internete bu cihazlar ile erişen 18-72 yaş aralığındaki kişiler oluşturmaktadır. Araştırmanın kapsamında ise yalnızca mobil ortam reklamlarında gerçekleşen dijital gözetim bulunmaktadır. Mobil olmayan ortamlarla internete bağlanan kişiler ve mobil olmayan ortamlardaki reklamlar kapsam dışı bırakılmıştır. Araştırmaya dahil edilen katılımcılar 18-72 yaş aralığı ile sınırlandırılmıştır. Yaş kriteri olarak

---

[105] https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu (erişim tarihi: 25.05.2018).
[106] http://www.haberturk.com/ekonomi/is-yasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi (erişim tarihi: 25.05.2018).
[107] http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012 (erişim tarihi: 25.05.2018).

bu sınır 1946-2000 yılları arası doğumlu kişilerdir. Alt sınır olarak belirlenen 2000 yılı doğumlu katılımcıların yaşı -ebeveyn izni olmaksızın ankette görüşmeci olma yaşı 18 olduğundan- daha alt yaşlar tercih edilmemiştir. Üst sınır olarak da 'Baby Boomers'[108] olarak adlandırılan kuşak 1946-1964 yılları arasında doğan kişiler olarak belirlenmiştir. Araştırmada kota örnekleme tercih edilerek 18-37 yaş arası dijital yerliler 38-72 yaş arası dijital göçmenler olarak iki gruba ayrılmış ve katılımcılar bu iki gruptan rastlantısal olarak seçilmiştir. Örneklem büyüklüğü nedeniyle p ve q değerleri 0,05 alınarak, %5'lik hata payı ise α= 0,05 kabul edilerek 384 olarak hesaplanmıştır. Bu nedenle 384 kişinin üzerinde katılımcıya ulaşılmıştır.

Araştırmada nicel araştırma yöntemi kapsamında yüz yüze anket tekniği kullanılmış olup, dijital göçmeler ve dijital yerlilere toplam 45 adet soru yöneltilmiştir. İki grubun karşılaştırılacak olması sebebiyle eşit sayıda, 384 üstü katılımcıya ulaşılması gerekmiş ve uygulanan anket sayısı toplamda 832 olmuştur. Dijital göçmenlerle yüz yüze görüşülerek toplamda 412 sağlıklı anket sonucu elde edilmiştir. Dijital yerlilerle de yüz yüze görüşülerek 420 anket sonucuna ulaşılmış, bu sayı dijital göçmenler ile eşitlenerek 412 sonuç değerlendirmeye alınmış olup toplamda 824 anket araştırmaya dahil edilmiştir. Araştırma sırasında katılımcılara mobil internet kullanım durumları ve sosyal medya kullanıp kullanmadıkları sorulmuş, yüz yüze anket uygulamasına mobil internet kullananlarla devam edilmiştir. Bununla birlikte alan gözlemleri doğrultusunda, mobil internet ve sosyal medya kullanmayanların sayısının dikkate alınmayacak kadar az olduğu söylenebilir.

## 3.2. Güvenilirlik Analizi:

Araştırma öncesinde Ankara ilindeki üç büyük ilçede yapılan pilot çalışmada soruların anlaşılabilir olduğu, çelişkide kalınan herhangi bir sorunun olmadığı görülmüştür. 40 dijital göçmen ve 40 dijital yerli olmak üzere toplamda 80 anket uygulanıp araştırmaya dahil edilmiştir. Veriler güvenirlik analizine tabi tutulmuş, Cronbach's Alpha değerinin 0,8'in üzerinde bir değerde bulunduğu anlaşılmış ve verilerin yüksek güvenilirlikte olduğu sonucuna ulaşılmıştır.

**Tablo 3.1 Güvenilirlik Analizi**

| Cronbach's Alpha | N of Items |
|---|---|
| ,806 | 34 |

[108] https://www.academia.edu/19706219/Dijital_Ku%C5%9Faklar_Dijital_Ku%C5%9Faklar%C4%B1_Nas%C4%B1l_%C3%87al%C4%B1%C5%9Fmal%C4%B1?auto=download (erişim tarihi: 20.05.2018).

## 3.3. Araştırma Verilerinin Analizi

Araştırma verilerinin analizinde öncelikle demografik bulgulara, mobil internet kullanımına, sosyal medya ortamı kullanımına, mobil ortamlarda reklam görme durumuna, gizlilik ve mahremiyet ihlallerine ilişkin algı ve tutumlarla ilgili bulgulara yer verilmiş, daha sonra da araştırma soruları analiz edilmiş ve hipotezler sınanarak açıklanmıştır.

### 3.3.1. Demografik Bulgular

Katılımcıların demografik bulgularına ilişkin frekans dağılımları aşağıda verilmiştir:

**Tablo 3.2 Katılımcıların Cinsiyet Bilgilerine Ait Dağılım**

| | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|
| Kadın | 418 | 50,7 | 50,7 | 50,7 |
| Erkek | 406 | 49,3 | 49,3 | 100,0 |
| Total | 824 | 100,0 | 100,0 | |

Araştırma bulgularına göre katılımcıların cinsiyet oranları birbirine yakındır. Katılımcıların %50,7 si kadınlardan, %49,3'ü ise erkeklerden oluşmaktadır.

**Tablo 3.3 Katılımcıların Yaş Ortalamaları**

| N | Minimum | Maksimum | Ortalama | Standart Sapma |
|---|---|---|---|---|
| 824 | 18,00 | 68,00 | 36,4114 | 13,97209 |
| 824 | | | | |

Katılımcıların yaş ortalaması en küçük yaş 18, en büyük yaş 68 olmak üzere 36,4'tür.

**Tablo 3.4 Katılımcıların Medeni Durumuna İlişkin Dağılım**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Evli | 415 | 50,4 | 50,7 | 50,7 |
| | Bekar | 404 | 49,0 | 49,3 | 100,0 |
| | Total | 819 | 99,4 | 100,0 | |
| Kayıp Veri | Sistem | 5 | ,6 | | |
| | Toplam | 824 | 100,0 | | |

Katılımcıların medeni durumu da yüzde olarak birbirine yakındır. 415 katılımcı evli, 404 katılımcı ise bekardır.

**Tablo 3.5 Katılımcıların Çalışma Durumuna İlişkin Dağılım**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Özel Sektörde Ücretli Çalışan | 211 | 25,6 | 25,9 | 25,9 |
| | Kamu Çalışanı | 184 | 22,3 | 22,6 | 48,5 |
| | Emekli | 75 | 9,1 | 9,2 | 57,7 |
| | Serbest Meslek | 56 | 6,8 | 6,9 | 64,6 |
| | Ev Kadını | 20 | 2,4 | 2,5 | 67,1 |
| | Öğrenci | 252 | 30,6 | 31,0 | 98,0 |
| | Çalışmıyor | 14 | 1,7 | 1,7 | 99,8 |
| | Diğer | 2 | ,2 | ,2 | 100,0 |
| | Total | 814 | 98,8 | 100,0 | |
| Kayıp Veri | Sistem | 10 | 1,2 | | |
| | Toplam | 824 | 100,0 | | |

Tablo 3.5'e göre katılımcıların çalışma durumları ise çeşitlidir. Sırasıyla 252 katılımcı öğrenci, 211 katılımcı özel sektörde ücretli çalışan, 184 katılımcı kamu çalışanı, 75 katılımcı da emeklidir. Çalışma durumlarını ev kadını ve çalışmıyor olarak belirten kişilerin ise azınlıkta olduğu görülmektedir.

**Tablo 3.6 Katılımcıların Eğitim Durumuna Göre Dağılımı**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Okur-Yazar | 4 | ,5 | ,5 | ,5 |
| | İlköğretim | 64 | 7,8 | 7,8 | 8,3 |
| | Lise | 245 | 29,7 | 29,8 | 38,1 |
| | Önlisans | 119 | 14,4 | 14,5 | 52,6 |
| | Lisans | 331 | 40,2 | 40,3 | 92,8 |
| | Lisansüstü | 59 | 7,2 | 7,2 | 100,0 |
| | Total | 822 | 99,8 | 100,0 | |
| Kayıp Veri | Sistem | 2 | ,2 | | |
| | Toplam | 824 | 100,0 | | |

Katılımcıların eğitim durumuna ilişkin dağılımını gösteren Tablo 3.6'da görüldüğü üzere, eğitim durumu lisans olan katılımcı sayısı 331 olup toplam katılımcıların %40,2'sini oluşturmaktadır. Burada dikkat çeken bulgu, eğitim durumu ilköğretim ve lise olanların yüzdeleridir ve bu noktada dijital göçmen/dijital yerli olarak hangi grubun içerisinde

konumlandıklarının açıklanması gerekliliği doğmuştur. Tablo 3.7'de katılımcıların eğitim durumlarına göre hangi kuşak grubunda yer aldıklarına dair bulgular yer almaktadır.

**Tablo 3.7 Eğitim Durumunun Kuşaklara Göre Dağılımı**

| | | | Kuşak | | |
|---|---|---|---|---|---|
| | | | **Göçmen** | **Yerli** | **Toplam** |
| Eğitim Durumu | Okur-Yazar | N | 3 | 1 | 4 |
| | | % | %0,7 | %0,2 | %0,5 |
| | İlköğretim | N | 56 | 8 | 64 |
| | | % | %13,6 | %1,9 | %7,8 |
| | Lise | N | 155 | 90 | 245 |
| | | % | %37,7 | %21,9 | %29,8 |
| | Önlisans | N | 87 | 32 | 119 |
| | | % | %21,2 | %7,8 | %14,5 |
| | Lisans | N | 83 | 248 | 331 |
| | | % | %20,2 | %60,3 | %40,3 |
| | Lisansüstü | N | 27 | 32 | 59 |
| | | % | %6,6 | %7,8 | %7,2 |
| | Toplam | N | 411 | 411 | 822 |
| | | % | %100,0 | %100,0 | %100,0 |

Tablo 3.7'de görüldüğü üzere eğitim durumu ilköğretim olanların %13,6'sı ve eğitim durumu lise olanların %37,7'si dijital göçmenler grubunun içerisinde yer almaktadır. Dijital yerlilerin ise %60,3'ünün eğitim durumu lisanstır.

### 3.3.2. Mobil İnternet Erişimi İle İlgili Bulgular

Kişilerin, mobil internete erişimini hangi cihazlar ile gerçekleştirdiğini öğrenmek için yöneltilen soru doğrultusunda aşağıdaki bulgulara ulaşılmıştır.

**Tablo 3.8 Mobil İnternet Erişimine İlişkin Dağılım**

| | | **Frekans** | **Yüzde** | **Geçerli Yüzde** | **Kümülatif Yüzde** |
|---|---|---|---|---|---|
| Geçerli Veri | Mobil Telefon | **706** | **85,7** | **86,8** | **86,8** |
| | Tablet / iPad | 28 | 3,4 | 3,4 | 90,3 |
| | Taşınabilir Bilgisayar | 78 | 9,5 | 9,6 | 99,9 |
| | Giyilebilir Teknolojiler | 1 | ,1 | ,1 | 100,0 |
| | Total | 813 | 98,7 | 100,0 | |

| | | | |
|---|---|---|---|
| Kayıp Veri | Sistem | 11 | 1,3 |
| | Toplam | 824 | 100,0 |

Katılımcıların mobil internet erişimlerini ortaya koyan tablo 3.8'de görüldüğü üzere mobil telefon ile mobil internete erişim %85,7 ile ilk sırada yer almıştır. Buradan anlaşılacağı gibi katılımcılar çok yüksek oranda mobil telefon kullanmakta, mobil telefonu sırasıyla %9,5 ile taşınabilir bilgisayar ve %3,4 ile tablet/ipad izlemektedir. Mobil telefonların bu denli fazla kullanılıyor olması, bilgisayarların yapmış olduğu birçok işlemi mobil telefonların da yapıyor olmasıdır. Ayrıca mobil telefonların ergonomik yapısı ve mobil telefonların her an her yerde kullanılabilir olması da kullanıcıları bu cihazlara yöneltmektedir.

### 3.3.3. Sosyal Medya Ortamı Kullanımı İle İlgili Bulgular

Katılımcıların en çok hangi sosyal medya ortamını kullandıkları araştırma kapsamında önemli olup sosyal medya kullanımına ilişkin frekans dağılımları aşağıda sunulmuştur.

**Tablo 3.9 Mobil Ortamlarda Sosyal Medya Kullanımına İlişkin Dağılım**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Facebook | **235** | **28,5** | **29,8** | **29,8** |
| | Twitter | 74 | 9,0 | 9,4 | 39,2 |
| | Instagram | **366** | **44,4** | **46,4** | **85,6** |
| | Google+ | 73 | 8,9 | 9,3 | 94,8 |
| | Whatsapp | 41 | 5,0 | 5,2 | 100,0 |
| | Total | 789 | 95,8 | 100,0 | |
| Kayıp Veri | Sistem | 35 | 4,2 | | |
| | Toplam | 824 | 100,0 | | |

Tablo 3.9'da görüldüğü üzere sosyal medya kullanımında iki sosyal medya ortamının daha çok kullanıldığı görülmektedir. Katılımcıların %44'ü Instagram kullanırken, %28,5'i Facebook kullanmaktadır. Daha sonra sırasıyla Twitter, Google+ ve Whatsapp gelmektedir. Aslında Whatsapp katılımcılara yöneltilen sorularda bulunmamaktadır. Diğer olarak açılan seçeneğe 41 kişi tarafından yazılmıştır. Yukarıda daha önce bahsedildiği üzere Whatsapp'ın anlık görüşme uygulaması olmaktan çıkarak sosyal medya platformuna evrildiği de anlaşılmaktadır. Görülmektedir ki kişiler sosyal medyada çokça vakit geçirmekte ve bu ortamları yoğun olarak kullanmaktadır. Böylece sosyal medya kullanımı, gündelik yaşam pratiklerince içselleştirilmekte, mobil ortamlardaki gözetimi bir hiperkontrole

dönüştürmektedir (Çakır, 2015: 332). Tablo 3.9'dan elde edilen bulguların kuşak ve cinsiyet açısından da değerlendirilmesi doğru olacaktır.

**Tablo 3.10 Mobil Ortamlarda Sosyal Medya Kullanımının Cinsiyete Göre Dağılımı**

| Kullanılan sosyal medya platformu | | Cinsiyetiniz | | |
|---|---|---|---|---|
| | | **Kadın** | **Erkek** | **Toplam** |
| Facebook | N | **87** | **148** | **235** |
| | % | **%21,6** | **%38,2** | **%29,8** |
| Twitter | N | 39 | 35 | 74 |
| | % | %9,7 | %9,0 | %9,4 |
| Instagram | N | **235** | **131** | **366** |
| | % | **%58,5** | **%33,9** | **%46,4** |
| Google+ | N | 26 | 47 | 73 |
| | % | %6,5 | %12,1 | %9,3 |
| Whatsapp | N | 15 | 26 | 41 |
| | % | %3,7 | %6,7 | %5,2 |
| Toplam | N | 402 | 387 | 789 |
| | % | 100,0 | 100,0 | 100,0 |

Tablo 3.10'da görüldüğü gibi Instagram kullanan katılımcıların 235'i kadın, 131'i erkektir. Bu sosyal medya platformunu kullanan kadınlar erkeklere üstünlük kurmaktadır. Facebook kullanımında ise tam tersi bir sonuç bulunmaktadır. Facebook kullanan katılımcıların 148'i erkek, 87'si ise kadındır.

**Tablo 3.11 Mobil Ortamlarda Sosyal Medya Kullanımının Kuşaklara Göre Dağılımı**

| Kullanılan sosyal medya platformu | | Kuşak | | |
|---|---|---|---|---|
| | | **Göçmen** | **Yerli** | **Total** |
| Facebook | N | **195** | **40** | **235** |
| | % | **%49,1** | **%10,2** | **%29,8** |
| Twitter | N | 32 | 42 | 74 |
| | % | %8,1 | %10,7 | %9,4 |
| Instagram | N | **99** | **267** | **366** |
| | % | **%24,9** | **%68,1** | **%46,4** |
| Google+ | N | 45 | 28 | 73 |
| | % | %11,3 | %7,1 | %9,3 |
| Whatsapp | N | 26 | 15 | 41 |
| | % | %6,5 | %3,8 | %5,2 |
| Toplam | N | 397 | 392 | 789 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | % | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 |

Tablo 3.11'de görüldüğü üzere Instagram kullanıcıları 267 kişiyle dijital yerlilerden oluşmakta, Facebook kullanıcıları ise 195 kişiyle dijital göçmenlerden oluşmaktadır. Tablo 3.10 ve 3.11'den hareketle sosyal medya kullanımında kadın dijital yerlilerin çoğunlukla Instagram'ı, erkek dijital göçmenlerin de çoğunlukla Facebook'u tercih ettiği anlaşılmaktadır. "Bireysel seviyede ağ oluşturma, ilişki kurmak ve sosyal ilişkileri geliştirmek için kullanılan sistematik bir yöntemdir. Giderek kişiselleşen toplumda ağ oluşturma bariz bir sosyal ihtiyaç haline gelirken, ağlar kişiselleşmenin sosyal emsalleri olarak görülmektedir" (Dijk, 2016: 56). Dijital yerlilerin sosyal medyayı hem kendini ifade etme hem bilgi paylaşımı hem de sosyalleşmek için ideal bir ortam olarak gördüğü ve dijital yerlilerin sosyal medya ortamına bu anlamı yüklemesiyle onların gittikçe bireyselleşip insansız iletişime geçtiğini göstermektedir (Yıldız, 2012: 541). Dijital göçmenlerse sosyal medya ortamlarını daha çok "merak ve takip" üzerine kurulu bilgi alma ve paylaşımı olarak kullandıkları anlaşılmakta, bireysellik durumunda ise dijital yerlilerden ayrıldıkları görülmektedir.

**Tablo 3.12 Mobil Ortamlarda Sosyal Medya Kullanımının Eğitim Durumuna Göre Dağılımı**

| | | Eğitim Durumu | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Okur-Yazar** | **İlköğretim** | **Lise** | **Önlisans** | **Lisans** | **Lisansüstü** | **Toplam** |
| Facebook | N | 2 | 44 | 123 | 20 | 39 | 6 | 234 |
| | % | %50,0 | %72,1 | %51,2 | %17,9 | %12,5 | %10,3 | %29,7 |
| Twitter | N | 0 | 2 | 10 | 11 | 35 | 16 | 74 |
| | % | %0,0 | %3,3 | %4,2 | %9,8 | %11,2 | %27,6 | %9,4 |
| Instagram | N | 1 | 9 | 72 | 60 | 193 | 30 | 365 |
| | % | %25,0 | %14,8 | %30,0 | %53,6 | %61,9 | %51,7 | %46,4 |
| Google+ | N | 1 | 1 | 19 | 15 | 32 | 5 | 73 |
| | % | %25,0 | %1,6 | %7,9 | %13,4 | %10,3 | %8,6 | %9,3 |
| Whatsapp | N | 0 | 5 | 16 | 6 | 13 | 1 | 41 |
| | % | %0,0 | %8,2 | %6,7 | %5,4 | %4,2 | %1,7 | %5,2 |
| Toplam | N | 4 | 61 | 240 | 112 | 312 | 58 | 787 |
| | % | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 | %100,0 |

Tablo 3.12'den anlaşılacağı üzere eğitim durumu lisans ve lisansüstü olan katılımcılar en çok sosyal medya kullanımında Instagram'ı tercih ederken, eğitim durumu lise olan katılımcılar Facebook'u tercih etmektedir. Eğitim durumu ilköğretim olan katılımcıların ise en çok Facebook'u tercih ettiği görülmektedir. Twitter kullanımına bakıldığında, katılımcıların eğitim durumunun artmasıyla Twitter kullanım oranının arttığı göze çarpmaktadır.

### 3.3.4. Mobil Ortamlarda Yayınlanan Reklamların Farkındalık Durumu İle İlgili Bulgular

Araştırma kapsamında "Daha önce arama yapılan ürünler/hizmetlerle ilgili daha sonra mobil ortamlarda reklam görme durumu"nun bilinmesi, bu reklamların fark edilip edilmediğinin ölçülmesi araştırma açısından önemlidir.

**Tablo 3.13 Daha Önce Arama Yapılan Ürünler/Hizmetlerle İlgili Daha Sonra Mobil Ortamlarda Reklam Görme Durumuna İlişkin Dağılım**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Evet | **765** | **92,8** | **93,5** | **93,5** |
| | Hayır | 53 | 6,4 | 6,5 | 100,0 |
| | Total | 818 | 99,3 | 100,0 | |
| Kayıp Veri | Sistem | 6 | ,7 | | |
| | Toplam | 824 | 100,0 | | |

Katılımcıların %92,8'i daha önce yaptığı ürünler/hizmetlerle ilgili daha sonra mobil ortamlarda yayınlanan reklamları fark ettiklerini ifade etmişlerdir. Mobil ortamlarda reklam görmediğini belirten katılımcıların oranı ise %6,4'tür. Dolayısıyla bu ortamlarda yayınlanan reklamların fark edilme durumunun oldukça yüksek olduğu ortaya konulmuştur.

**Tablo 3.14 Daha Önce Arama Yapılan Ürünler/Hizmetlerle İlgili Mobil Ortam Reklamlarının Görülme Sıklığının, Sosyal Medya Türüne Göre Dağılımı**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Sosyal Medya | **558** | **67,7** | **68,5** | **68,5** |
| | Arama Motoru | 109 | 13,2 | 13,4 | 81,8 |
| | Mobil Uygulama İçi | 58 | 7,0 | 7,1 | 89,0 |
| | Web (Banner) | 90 | 10,9 | 11,0 | 100,0 |
| | Total | 815 | 98,9 | 100,0 | |
| Kayıp Veri | Sistem | 9 | 1,1 | | |
| | Toplam | 824 | 100,0 | | |

Tablo 3.14'e göre ise katılımcılar en çok %67,7 ile sosyal medya ortamında reklam görmektedir. Sosyal medya ortamından sonra %13,2 ile arama motoru ikinci sırada yer almaktadır. Kişilerin daha çok sosyal medya ortamlarında vakit geçirdiği düşünüldüğünde,

kullanıcıların bu ortamlarda reklam görmesi de açıklanabilir bir durumdur. Bu durum aynı zamanda internette okuryazarlık becerisini gerektirmektedir. Reklam okuryazarlığı açısından internette yer alan enformasyonun içeriğinin reklam olup olmadığı konusu da başka bir zorluktur. Bu sorunla baş edebilmek için medya okuryazarlığı adı altında çalışmalar yaygınlık kazanmıştır. Ancak pek çok eğitimci ve akademisyene göre bu çalışmaların mevcut haliyle kişilerin medyanın olumsuz etkilerinden korunabileceği iddiaları sorunludur. Bu noktada sorun, Türkiye için mevcut pedagojik yaklaşım sorunudur. Eğitimin, eleştirel perspektiften yoksun sistematiği, medya okuryazarlığı çalışmalarını da sekteye uğratan temel nedendir (Taşkaya, 2016: 199, 224).

### 3.3.5 Gizlilik ve Mahremiyet İhlallerindeki Algı ve Tutumlara İlişkin Bulgular

Mobil ortamlarda gizlilik ve mahremiyet ihlallerindeki algı ve tutumlarla ilgili bulgular aşağıda yer almaktadır.

**Tablo 3.15 Daha Önce Arama Yapılan Ürünler/Hizmetlerle İlgili Daha Sonra Mobil Ortamlarda Reklam Görme Durumuna İlişkin Gizlilik Endişeleri Dağılımı**

| | | Frekans | Yüzde | Geçerli Yüzde | Kümülatif Yüzde |
|---|---|---|---|---|---|
| Geçerli Veri | Evet | 584 | 70,9 | **71,2** | 71,2 |
| | Hayır | 236 | 28,6 | **28,8** | 100,0 |
| | Total | 820 | 99,5 | 100,0 | |
| Kayıp Veri | Sistem | 4 | ,5 | | |
| | Toplam | 824 | 100,0 | | |

Tablo 3.15'teki bulgulara göre daha önce arama yapılan ürün/hizmetlerle ilgili daha sonra reklam görmek, katılımcıların %71,2'sinde gizlilik ihlali endişesi yaratmaktadır. Gizlilik ihlali endişesi yaratmayan katılımcı oranı da %28,8'dir.

**Tablo 3.16 Daha Önce Arama Yapılan Ürünler/Hizmetlerle İlgili Daha Sonra Mobil Ortamlarda Reklam Görme Durumunun Yarattığı Gizlilik Endişelerine İlişkin Bulguların Kuşaklara Göre Dağılımı**

| | | | Kuşak | | |
|---|---|---|---|---|---|
| Gizlilik endişelerine ilişkin yanıtlar | | | Göçmen | Yerli | Toplam |
| | Evet | N | **332** | 252 | 584 |
| | | % | **%81,0** | %61,5 | %71,2 |
| | Hayır | N | 78 | **158** | 236 |
| | | % | %19,0 | **%38,5** | %28,8 |

| | | | | |
|---|---|---|---|---|
| Toplam | N | 410 | 410 | 820 |
| | % | %100,0 | %100,0 | %100,0 |

Gizlilik ihlali endişeleri kuşaklara göre incelendiğinde ise ortaya çarpıcı sonuçlar çıkmaktadır. Tablo 3.15'e göre dijital göçmenlerin %81'i gizlilik ihlali endişesi bildirirken yalnızca %19'u gizlilik ihlali endişesi bildirmemiştir. Dijital yerlilerde ise makas daha dardır ve gizlilik ihlali endişesi bildiren dijital yerlilerin oranı %61,5, gizlilik ihlali endişesi bildirmeyen dijital yerlilerin oranı %35,5'tir. Buradan çıkarılacak sonuç ise dijital göçmenler dijital yerlilere oranla daha fazla gizlilik ihlali endişesi taşımakta ve mahremiyet ihlallerinden daha fazla korkmaktadırlar.

**Tablo 3.17 İnternette Mahremiyetin Korunmasının Olanaklı Bulunup Bulunmadığına İlişkin Yanıtların Dağılımı**

| | | **Frekans** | **Yüzde** | **Geçerli Yüzde** | **Kümülatif Yüzde** |
|---|---|---|---|---|---|
| Geçerli Veri | Olanaklı | 208 | 25,2 | 25,4 | 25,4 |
| | Olanaksız | **612** | **74,3** | **74,6** | **100,0** |
| | Total | 820 | 99,5 | 100,0 | |
| Kayıp Veri | Sistem | 4 | ,5 | | |
| | Toplam | 824 | 100,0 | | |

Tablo 3.17'deki bulgular ile tablo 3.15'teki gizlilik ihlali endişeleri bulgularına paralel bir sonuç barındırmaktadır. Katılımcıların %74,3'ü internette mahremiyeti korumanın olanaklı olmadığını belirtmiştir. İnternette mahremiyeti korumanın olanaklı olduğunu düşünen kısımda ise %25,2'lik bir orandadır. Burada gizlilik ve mahremiyet ihlali endişelerinin benzer sonuçlar ortaya koyduğu görülmekte, bu alanla ilgili çalışmaların da genişletilmesi gerekliliğini göstermektedir.

**Tablo 3.18 İnternette Mahremiyetin Korunmasının Olanaklı Bulunup Bulunmadığına İlişkin Yanıtların Kuşaklara Göre Dağılımı Dağılım**

| **Mahremiyet düşüncelerine ilişkin yanıtlar** | | **Kuşak** | | |
|---|---|---|---|---|
| | | **Göçmen** | **Yerli** | **Total** |
| Olanaklı | N | 83 | 125 | 208 |
| | % | %20,3 | %30,4 | %25,4 |
| **Olanaksız** | **N** | **326** | **286** | **612** |
| | **%** | **%79,7** | **%69,6** | **%74,6** |
| Toplam | N | 409 | 411 | 820 |

| | | | | |
|---|---|---|---|---|
| | % | %100,0 | %100,0 | %100,0 |

İnternette mahremiyeti korumanın olanaklı olup olmadığı ile ilgili soru kuşaklar arası değerlendirildiğinde dijital göçmenlerin %79,7'si internette mahremiyeti korumanın olanaklı olmadığını bildirmiş, yalnızca %20,3'lük bir kısım olanaklı olduğunu belirtmiştir. Dijital yerlilerde ise %69,6'lık bir bölüm internette mahremiyeti korumanın olanaklı olmadığını savunurken %30,4 internette mahremiyeti korumanın olanaklı olduğunu düşünmektedir. Buradan çıkarılacak sonuç ise dijital göçmenlerin dijital yerlilere göre daha umutsuz olduğudur. Toplamda ise yine katılımcıların üçte ikilik kısmı internette mahremiyeti korumanın olanaklı olmadığını düşünmektedir.

## 3.4. Dijital Gözetime İlişkin Algı-Tutum ve Farkındalıklara İlişkin Bulgular

Aşağıdaki bulgular araştırma soruları kapsamında değerlendirilmiştir:

**Dijital göçmenler ve dijital yerliler, mobil ortam reklamlarında gerçekleşen dijital gözetimin farkında mıdır?**

Mobil ortam reklamları kişilerin dijital ortamlarda bıraktığı dijital izler ile yaratılmaktadır. Katılımcılara konu hakkında bilgi verilmiş olup gözetim ile ilgili sorular yöneltilmiş ve mobil ortam reklamlarıyla gerçekleşen dijital gözetimin farkındalığı ölçülmüştür.

**Tablo 3.19 Kuşaklara Göre Mobil Ortamlarda Dijital Gözetim Farkındalığı**

| **Katılımcıların mobil ortamlardaki dijital gözetimin farkında olup olmadıklarına ilişkin yanıtları** | | **Kuşak** | | |
|---|---|---|---|---|
| | | **Göçmen** | **Yerli** | **Toplam** |
| Katılıyorum | N | **314** | **271** | **585** |
| | % | **%78,3** | **%67,1** | **%72,7** |
| Kararsızım | N | 42 | 61 | 103 |
| | % | %10,5 | %15,1 | %12,8 |
| Katılmıyorum | N | 29 | 61 | 90 |
| | % | %7,2 | %15,1 | %11,2 |
| Bilgim Yok | N | 16 | 11 | 27 |
| | % | %4,0 | %2,7 | %3,4 |
| Toplam | N | 401 | 404 | 805 |
| | % | %100,0 | %100,0 | %100,0 |

Tablo 3.19'dan anlaşılacağı üzere dijital göçmenlerin %78,3'ü dijital yerlilerin %67,1'i mobil ortam reklamlarındaki gözetimin farkındalardır. Toplam katılımcıların ise %72,7'si farkında, %12,8'lik bir kısmı kararsız olup çok az bir oranda da (%11,2) farkında değillerdir.

Katılımcıların %3,4'ü de bilgilerinin olmadığını belirtmiştir. Sonuç olarak hem dijital göçmenler hem de dijital yerliler mobil ortamlarda gözetlendikleri hissini taşımaktadır.

**Kişiler, mobil ortamlarda hangi bilgilerini paylaşmaktadır?**

Tablo 3.20, 3.21 ve 3.22'de görüldüğü üzere katılımcılara mobil ortamlarda hangi kişisel bilgilerini paylaştıkları sorulmuştur.

**Tablo 3.20 Kuşaklara Göre Mobil Ortamlarda Telefon Numarası Paylaşımı**

| Katılımcıların kişisel bilgi paylaşımına ilişkin yanıtları | | | Kuşak | | |
|---|---|---|---|---|---|
| | | | Göçmen | Yerli | Toplam |
| | Katılıyorum | N | 32 | 74 | 106 |
| | | % | %7,9 | %18,3 | %13,1 |
| | Kararsızım | N | 25 | 98 | 123 |
| | | % | %6,1 | %24,2 | %15,1 |
| | Katılmıyorum | N | 340 | 227 | 567 |
| | | % | %83,5 | %56,0 | %69,8 |
| | Bilgim Yok | N | 10 | 6 | 16 |
| | | % | %2,5 | %1,5 | %2,0 |
| | Toplam | N | 407 | 405 | 812 |
| | | % | %100,0 | %100,0 | %100,0 |

**Tablo 3.21 Kuşaklara Göre Mobil Ortamlarda İkamet / İş Adresi Bilgisi Paylaşımı**

| Adres bilgisi paylaşma durumuna ilişkin yanıtlar | | | Kuşak | | |
|---|---|---|---|---|---|
| | | | Göçmen | Yerli | Toplam |
| | Katılıyorum (paylaşırım)? | N | 32 | 68 | 100 |
| | | % | %7,8 | %16,7 | %12,2 |
| | Kararsızım | N | 20 | 84 | 104 |
| | | % | %4,9 | %20,6 | %12,7 |
| | Katılmıyorum (paylaşmam)? | N | 347 | 246 | 593 |
| | | % | %84,8 | %60,3 | %72,6 |
| | Bilgim Yok | N | 10 | 10 | 20 |
| | | % | %2,4 | %2,5 | %2,4 |
| | Toplam | N | 409 | 408 | 817 |
| | | % | %100,0 | %100,0 | %100,0 |

**Tablo 3.22 Kuşaklara Göre Mobil Ortamlarda E-Posta Bilgisi Paylaşımı**

| Katılımcıların kişisel bilgi paylaşımına ilişkin yanıtları | | | Kuşak | | |
|---|---|---|---|---|---|
| | | | Göçmen | Yerli | Toplam |
| | Katılıyorum | N | 124 | 225 | 349 |

| | | | | |
|---|---|---|---|---|
| | % | %30,4 | %55,6 | %42,9 |
| Kararsızım | N | 30 | 73 | 103 |
| | % | %7,4 | %18,0 | %12,7 |
| Katılmıyorum | N | 243 | 104 | 347 |
| | % | %59,6 | %25,7 | %42,7 |
| Bilgim Yok | N | 11 | 3 | 14 |
| | % | %2,7 | %0,7 | %1,7 |
| Toplam | N | 408 | 405 | 813 |
| | % | %100,0 | %100,0 | %100,0 |

Elde edilen bulgulara göre dijital göçmenlerin, telefon numarası ve ikamet/iş adresi bilgilerini paylaşmaktan çekindiği, dijital yerlilerin ise göçmenlere göre daha fazla bu bilgileri paylaştıkları görülmektedir. Ayrıca kararsızların oranlarına bakıldığında dijital yerlilerin bu bilgilerin paylaşılmasında daha kararsız olduğu görülmekte, göçmenlerin ise bilgilerini paylaşmakta daha keskin bir biçimde isteksiz olduğu anlaşılmaktadır. Mobil ortamlarda e-posta adreslerinin paylaşımı ise dikkat çekicidir. Dijital yerliler e-posta bilgilerini dijital göçmenlere göre daha fazla paylaşmaktadır. Ayrıca dijital göçmenler de e-posta bilgilerini, telefon numarası ve ikamet/iş adresi bilgilerine göre daha fazla paylaşmaktadır. Bu duruma da e-posta bilgilerinin diğer bilgilere oranla daha sanal bir nitelik taşıması, kişisel veri olarak daha az riskli görülmesinin neden olduğu düşünülmektedir. Sonuç olarak kullanıcıların mobil ortamlarda paylaşmış olduğu bilgiler farklılık göstermekte, kullanıcıların kişisel bilgilere olan bakış açılarında da bir farklılık olduğu görülmektedir.

**Kişiler, mobil uygulamaların kişisel bilgileri üçüncü kişilerle paylaşabileceğini bilmekte midir?**

Mobil uygulamaların kişisel verileri sızdırmasıyla ilgili bilgilere çalışmanın ikinci bölümünde değinilmiştir. Buradan hareketle katılımcılara veri sızıntıları ile ilgili bilgilerinin olup olmadığı sorulmuş Tablo 3.23'de görüldüğü üzere dijital göçmenler ve dijital yerlilerde yaklaşık sonuçlar elde edilmiştir.

**Tablo 3.23 Mobil Uygulamaların Kullanıcıların Kişisel Bilgilerini Üçüncü Kişilerle Paylaşabileceği Bilgisinin Kuşaklara Göre Bilinirlik Durumu**

| Katılımcıların mobil ortamlarda kişisel bilgi paylaşımına ilişkin yanıtları | | Kuşak | | |
|---|---|---|---|---|
| | | Göçmen | Yerli | Total |
| Katılıyorum | N | 245 | 244 | 489 |
| | % | %60,3 | %60,4 | %60,4 |
| Kararsızım | N | 53 | 75 | 128 |
| | % | %13,1 | %18,6 | %15,8 |

| | | | | |
|---|---|---|---|---|
| Katılmıyorum | N | 43 | 54 | 97 |
| | % | %10,6 | %13,4 | %12,0 |
| Bilgim Yok | N | 65 | 31 | 96 |
| | % | %16,0 | %7,7 | %11,9 |
| Total | N | 406 | 404 | 810 |
| | % | %100,0 | %100,0 | %100,0 |

Her iki grup da yaklaşık olarak %60'lık bir farkındalık göstermiştir. Ancak dijital göçmenlerin %16'lık oranda 'bilgim yok' cevabının, dijital yerlilere oranla (%7,7) yüksek olduğu görülürken, dijital yerlilerin dijital göçmenlere göre bu duruma daha hakim olduğu anlaşılmaktadır. Kararsızların oranına bakıldığında da dijital yerlilerin dijital göçmenlere göre daha kararsız oldukları görülmektedir.

**Kişiler, çerezler konusunda bilgi sahibi midir?**

**Tablo 3.24 Kuşaklara Göre Çerezler (cookies) Hakkında Bilgi Sahibi Olma Durumu**

| | | | Kuşak | | |
|---|---|---|---|---|---|
| Çerezlerin bilinirliğine ilişkin yanıtlar | | | Göçmen | Yerli | Toplam |
| Katılıyorum | N | | 91 | 153 | 244 |
| | % | | %22,4 | %37,5 | %30,0 |
| Kararsızım | N | | 51 | 93 | 144 |
| | % | | %12,6 | %22,8 | %17,7 |
| Katılmıyorum | N | | 53 | 72 | 125 |
| | % | | %13,1 | %17,6 | %15,4 |
| Bilgim Yok | N | | **211** | 90 | 301 |
| | % | | **%52,0** | %22,1 | %37,0 |
| Toplam | N | | 406 | 408 | 814 |
| | % | | %100,0 | %100,0 | %100,0 |

Tablo 3.24'ten anlaşılacağı üzere özellikle web ortamında dijital gözetim için kullanılan çerezlerin bilinirliği sorgulanmış, dijital göçmenlerin konuyla ilgili çok az bilgiye sahip oldukları görülmüştür. Dijital göçmenlerin %52'si çerezler hakkında bilgi sahibi değilken, dijital yerlilerin %37,5'i çerezler hakkında bilgi sahibidirler. Genel olarak bakıldığında ise çerezler konusunda (%37,0) bilgi eksikliği olduğu anlaşılmaktadır. Çerez'ler çeşitli web siteleri ya da mobil tabanlı uygulamalarda standart bir biçimde açık olarak ayarlıdır. Kullanıcılar uygulamayı yüklediğinde ya da web hizmetini kullandığında çerez'lere otomatik olarak izin vermiş olmaktadır. Kullanıcılar yazılım ayarlarından bu seçeneği değiştirmediği sürece çerez'ler veri kaydetmeyi sürdürmektedir. Bu durum kullanıcının haberi olmadan verilerin

kaydedilmesine gizliliğin ve mahremiyetin ihlal edilmesine neden olmaktadır. Şirketlerin, web sitelerinin ya da mobil uygulamaların kullanıcıları yeteri kadar bilgilendirmediği de araştırmada elde edilen bulgular arasındandır. Özellikle web sitelerinin altında bant şeklinde çıkan çerez politikasına ilişkin uyarılar kullanıcılar tarafından dikkate alınmamakta, bu politikalara dikkat edilse de çerez politikalarının uzun ve karmaşık olması bu metinleri anlaşılır kılmamaktadır. Bu doğrultuda yeteri kadar ve daha anlaşılabilir bilgilendirmelerin, kuşaklar arası farklılıkların da dikkate alınarak oluşturulması gerektiği sonucuna ulaşılmaktadır.

**Dijital göçmenler ve dijital yerliler, mobil uygulama yüklemeden önce uygulamaların erişim izinlerine dikkat ediyorlar mı?**

**Tablo 3.25 Kuşaklara Göre Mobil Uygulama Kullanımında Erişim İzinlerindeki Dikkatlere İlişkin Bulgular**

| | | | Kuşak | | |
|---|---|---|---|---|---|
| **Mobil Uygulamaların erişim izinlerine ilişkin yanıtlar** | | | **Göçmen** | **Yerli** | **Toplam** |
| | Katılıyorum | N | **325** | **308** | **633** |
| | | % | **%79,7** | **%75,5** | **%77,6** |
| | Kararsızım | N | 28 | 50 | 78 |
| | | % | %6,9 | %12,3 | %9,6 |
| | Katılmıyorum | N | 31 | 40 | 71 |
| | | % | %7,6 | %9,8 | %8,7 |
| | Bilgim Yok | N | 24 | 10 | 34 |
| | | % | %5,9 | %2,5 | %4,2 |
| | Toplam | N | 408 | 408 | 816 |
| | | % | %100,0 | %100,0 | %100,0 |

Mobil uygulamaların erişim izinleri, bu ortamlarda gerçekleşen veri sızıntılarında başroldedir. Tablo 3.25'te görüldüğü üzere katılımcıların büyük çoğunluğu yani %77,6'sı erişim izinlerine dikkat etmektedir. Mobil uygulama erişim izinlerine dikkat eden dijital göçmenler ve dijital yerliler arasında büyük bir fark bulunmamaktadır. Bulgulara göre dijital yerliler dijital göçmenlere göre erişim izinlerine daha az dikkat etmektedir. Alan gözlemleri doğrultusunda ise kullanıcıların bazılarının erişim izinleriyle karşılaşmadığı görülmüştür. Bu kullanıcıların IOS işletim sistemine sahip cihazlar kullandığı anlaşılmış olup uygulama marketlerinden uygulama yüklerken erişim izinlerini göremediği, ilgili yayıncının bu durumu kısıtladığı sonucuna ulaşılmıştır. Kullanıcılar ancak uygulamaları kullanırken uygulama tarafından erişim izni talep edildiğinde bu izinlerin ne olduğunu öğrenebilmektedirler. Daha mobil uygulamayı indirirken karşılaşılan bu durum gizlilik ve mahremiyet ihlali endişelerinin haklılığını açıkça göstermektedir.

**Dijital göçmenler ve dijital yerliler mobil ortam reklamlarını engellemek için herhangi bir engelleme programları kullanıyorlar mı?**

**Tablo 3.26 Kuşaklara Göre Mobil Ortam Reklamlarında Engelleme Programlarının Kullanımı**

| Engelleme programları kullanımına ilişkin yanıtlar | | Kuşak | | |
|---|---|---|---|---|
| | | Göçmen | Yerli | Toplam |
| Katılıyorum | N | 95 | 128 | 223 |
| | % | %23,4 | %31,5 | %27,5 |
| Kararsızım | N | 14 | 80 | 94 |
| | % | %3,4 | %19,7 | %11,6 |
| Katılmıyorum | N | 80 | 150 | 230 |
| | % | %19,7 | %36,9 | %28,3 |
| Bilgim Yok | N | **217** | 48 | 265 |
| | % | **%53,4** | %11,8 | %32,6 |
| Toplam | N | 406 | 406 | 812 |
| | % | 100,0 | 100,0 | 100,0 |

Mobil ortam reklamlarını ya da açılır pencereleri engellemek için herhangi bir engelleme programı kullanıp kullanmadıkları sorusuna katılımcıların verdiği yanıtlar yine çerezler hakkındaki bilgilere paralel bir sonucu ortaya koymaktadır. Dijital göçmenlerin %53,4'ü bu programlar hakkında herhangi bir bilgilerinin olmadığını belirtmişlerdir. Dijital yerlilerin %31,5'inin bu programları kullandığı, %36,9'unun ise bu programları bildiği ancak kullanmadığı tespit edilmiştir. Bilgim yok cevabı veren dijital göçmen sayısı 217 iken dijital yerlilerin sayısı 48'dir. Tüm kullanıcılar mükemmel internet becerilerine ya da yazılım tekniklerine sahip değildir, bu durum dijital eşitsizliğin bir yönü olarak görülmektedir (Fuchs 2011: 142). Dolayısıyla bu becerilere ve teknik konulara hakim olanların internet ortamındaki gizliliğini koruyabilmesi ya da mobil ortam reklamlarından kaçınabilmesi, dijital becerilere sahip olmayanlara göre daha kolay ve olanaklı olacaktır.

**Kişiler mahremiyetin ihlaline karşı devletin koruyuculuğuna inanıyorlar mı?**

**Tablo 3.27 Kuşaklara Göre Mahremiyetin İhlaline Karşı Devletin Koruyuculuğuna İlişkin Bulgular**

| Devletin koruyuculuğuna ilişkin yanıtlar | | Kuşak | | |
|---|---|---|---|---|
| | | Göçmen | Yerli | Toplam |
| Katılıyorum | N | 38 | 67 | 105 |
| | % | %9,3 | %16,8 | %13,0 |
| Kararsızım | N | 69 | 123 | 192 |

| | | | | |
|---|---|---|---|---|
| | % | %16,9 | %30,8 | %23,7 |
| Katılmıyorum | N | **272** | **192** | **464** |
| | % | **%66,5** | **%48,0** | **%57,4** |
| Bilgim Yok | N | 30 | 18 | 48 |
| | % | %7,3 | %4,5 | %5,9 |
| Toplam | N | 409 | 400 | 809 |
| | % | %100,0 | %100,0 | %100,0 |

Devletin koruyuculuğunun katılımcılar tarafından güvenilir bulunup bulunmadığı sorusuna verilen yanıtlar çarpıcıdır. Dijital göçmenler (%66,5) dijital yerlilere oranla (%48) devletin koruyuculuğuna inanmamaktadır. Dijital yerlilerin ise %30.8'le kararsız olması şaşırtıcıdır. Toplam katılımcıların da %13'ü devletin koruyuculuğuna inanmaktadır ki bu oldukça düşük bir orandır. Gary T. Marx (2005)'ın gözetimin özgürlüklerden uzak ve güvenilmez olduğu sonucunu ortaya koyması buradaki bulgularla da örtüşmektedir. Kişiler, devletler ve şirketler tarafından gerçekleştirilen dijital gözetimin çoğunlukla farkındadır. Bilişim ve internet teknolojilerine güvenme durumu da kişilere sorulmuş, kişilerin internet ve bilişim teknolojilerine güvenmediği ortaya çıkmıştır. Sonuç olarak kişilerin mobil ortamlarda kişisel alanlarını korumakta güçlük çektiği, devletin koruyucu gücüne inanmadığı görülmektedir.

**Dijital göçmenler ve dijital yerliler, dijital haklarını biliyorlar mı?**

**Tablo 3.28 Kuşaklara Göre Dijital Hakların Bilinirliği**

| | | **Kuşak** | | |
|---|---|---|---|---|
| **Dijital hakların bilinirliğine ilişkin yanıtlar** | | **Göçmen** | **Yerli** | **Toplam** |
| Katılıyorum | N | 92 | 161 | 253 |
| | % | %22,4 | %40,3 | %31,2 |
| Kararsızım | N | 80 | 126 | 206 |
| | % | %19,5 | %31,5 | %25,4 |
| Katılmıyorum | N | 48 | 56 | 104 |
| | % | %11,7 | %14,0 | %12,8 |
| Bilgim Yok | N | **190** | 57 | 247 |
| | % | **%46,3** | %14,2 | %30,5 |
| Toplam | N | 410 | 400 | 810 |
| | % | %100,0 | %100,0 | %100,0 |

Tablo 3.28'de görüldüğü üzere dijital haklar konusunda dijital göçmenler ve dijital yerliler arasında büyük bir uçurum bulunmaktadır. Dijital haklarımı biliyorum diyen dijital göçmenlerin oranı %22,4 iken dijital yerlilerin %40,3'lük bir kısmı dijital haklarını

bilmektedir. Ayrıca kararsızların dağılımında da iki grup arasında dijital yerliler daha yüksek kararsızlık durumu içindedir. Dijital göçmenlerin %46,3'ü dijital haklar hakkında bilgim yok cevabını seçerek çok çarpıcı bir sonuca imza atmışlardır. Dijital yerlilerin ise bilgim yok cevabı %14,2'dir ve çok düşük bir orandadır.

**Kişiler KVKK hakkında bilgi sahibi midir?**

**Tablo 3.29 Kuşaklara Göre Kişisel Verilerin Korunması Kanunu'nun Bilinirliği**

| KVKK'nın bilinirliğine ilişkin yanıtlar | | Kuşak | | |
|---|---|---|---|---|
| | | **Göçmen** | **Yerli** | **Toplam** |
| Katılıyorum | N | 64 | 126 | 190 |
| | % | %15,6 | %31,5 | %23,5 |
| Kararsızım | N | 32 | 128 | 160 |
| | % | %7,8 | %32,0 | %19,8 |
| Katılmıyorum | N | 69 | 73 | 142 |
| | % | %16,9 | %18,3 | %17,6 |
| Bilgim Yok | N | **244** | 73 | 317 |
| | % | **%59,7** | %18,3 | %39,2 |
| Toplam | N | 409 | 400 | 809 |
| | % | %100,0 | %100,0 | %100,0 |

Kişisel Verilerin Korunması Kanunu hakkında bilgi sahibi olan katılımcıların toplam oranı %23,5 iken KVKK hakkında bilgisi olmayan katılımcı oranı %39,2'dir. Ancak kuşaklararası fark göze çarpmakta, dijital yerlilerin %31,5'i KVKK hakkında bilgi sahibiyken, dijital göçmenlerin yalnızca %15,6'sının bilgi sahibi olduğu görülmüştür. Dijital göçmenlerin %59,7'lik bir kısmı KVKK hakkında bilgi sahibi değilken dijital yerlilerin %18,3'ü KVKK hakkında bilgi sahibi değildir. Bu bulgulara göre KVKK'nın özellikle dijital göçmenler tarafından az biliniyor oluşu sorgulanmalıdır. Sonuç olarak kişisel verilerin korunmasıyla ilgili mevcut düzenlemelerin kuşaklar arası farklara göre yeniden değerlendirilmesi ve bundan sonra yapılacak olan düzenlemelerin ve kanunların kuşaklar arası farkları gözeterek yapılması gerekliliği anlaşılmakta olup bu düzenlemelerin kişiler için anlaşılabilir olması gerekliliğini de göstermektedir.

## 3.5. Hipotezler

Araştırma kapsamında belirlenen hipotezleri sınamak üzere uygun analiz türünün belirlenebilmesi için araştırma verilerinin normal dağılımına uygunluğu test edilmiş,

demografik veriler ve ilk grupta sorulan sorular haricindeki 34 soru normallik testine tabi tutulmuştur.

**Tablo 3.30 Normallik Testi**

| | Kolmogorov-Smirnov[a] | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Statistic | df | Sig. | Statistic | df | Sig. |
| Soru 12 | ,301 | 709 | ,000 | ,744 | 709 | ,000 |
| Soru 13 | ,467 | 709 | ,000 | ,565 | 709 | ,000 |
| Soru 14 | ,464 | 709 | ,000 | ,574 | 709 | ,000 |
| Soru 15 | ,439 | 709 | ,000 | ,600 | 709 | ,000 |
| Soru 16 | ,447 | 709 | ,000 | ,581 | 709 | ,000 |
| Soru 17 | ,427 | 709 | ,000 | ,625 | 709 | ,000 |
| Soru 18 | ,444 | 709 | ,000 | ,612 | 709 | ,000 |
| Soru 19 | ,426 | 709 | ,000 | ,645 | 709 | ,000 |
| Soru 20 | ,324 | 709 | ,000 | ,750 | 709 | ,000 |
| Soru 21 | ,446 | 709 | ,000 | ,580 | 709 | ,000 |
| Soru 22 | ,519 | 709 | ,000 | ,368 | 709 | ,000 |
| Soru 23 | ,346 | 709 | ,000 | ,726 | 709 | ,000 |
| Soru 24 | ,292 | 709 | ,000 | ,806 | 709 | ,000 |
| Soru 25 | ,434 | 709 | ,000 | ,638 | 709 | ,000 |
| Soru 26 | ,449 | 709 | ,000 | ,614 | 709 | ,000 |
| Soru 27 | ,466 | 709 | ,000 | ,533 | 709 | ,000 |
| Soru 28 | ,383 | 709 | ,000 | ,692 | 709 | ,000 |
| Soru 29 | ,436 | 709 | ,000 | ,634 | 709 | ,000 |
| Soru 30 | ,444 | 709 | ,000 | ,618 | 709 | ,000 |
| Soru 31 | ,297 | 709 | ,000 | ,734 | 709 | ,000 |
| Soru 32 | ,443 | 709 | ,000 | ,618 | 709 | ,000 |
| Soru 33 | ,392 | 709 | ,000 | ,710 | 709 | ,000 |
| Soru 34 | ,372 | 709 | ,000 | ,687 | 709 | ,000 |
| Soru 35 | ,425 | 709 | ,000 | ,626 | 709 | ,000 |
| Soru 36 | ,222 | 709 | ,000 | ,839 | 709 | ,000 |
| Soru 37 | ,244 | 709 | ,000 | ,792 | 709 | ,000 |
| Soru 38 | ,306 | 709 | ,000 | ,821 | 709 | ,000 |
| Soru 39 | ,241 | 709 | ,000 | ,801 | 709 | ,000 |
| Soru 40 | ,224 | 709 | ,000 | ,805 | 709 | ,000 |
| Soru 41 | ,365 | 709 | ,000 | ,752 | 709 | ,000 |
| Soru 42 | ,217 | 709 | ,000 | ,815 | 709 | ,000 |
| Soru 43 | ,258 | 709 | ,000 | ,803 | 709 | ,000 |
| Soru 44 | ,348 | 709 | ,000 | ,791 | 709 | ,000 |
| Soru 45 | ,222 | 709 | ,000 | ,858 | 709 | ,000 |

Kolmogorov-Smirnov Testi ve Shapiro-Wilk testi sonuçlarına göre (Tablo 3.30 normallik testi: sig, 000) soruların normal dağılım göstermediği tespit edilmiştir. Bu nedenle

hipotezleri sınamak üzere uygun analiz yöntemi olarak parametrik olmayan Mann-Whitney U Testi, Ki-Kare Testi ve Sperman's Korelasyon Analizi testleri kullanılmıştır.

### 3.5.1. Dijital Göçmenlerle Dijital Yerlilerin Dijital Gözetime İlişkin Algı-Farkındalık Düzeyleri

Dijital göçmenlerle dijital yerlilerin dijital gözetime ilişkin algı-farkındalık düzeylerini ölçmek amacıyla parametrik olmayan bir analiz yöntemi olan Mann-Whitney U testi uygulanmıştır.

**Tablo 3.31 Mann-Whitney U Testi – Kuşaklara Göre Dijital Gözetim Algıları**

| | Dijital gözetime ilişkin algı-farkındalık |
|---|---|
| Mann-Whitney U | 72098,500 |
| Wilcoxon W | 152699,500 |
| Z | -3,448 |
| Asymp. Sig. (2-tailed) | ,001 |

$H_{0:}$ Dijital göçmenlerle dijital yerlilerin dijital gözetime ilişkin algı-farkındalık düzeyleri arasında anlamlı bir farklılık bulunmamaktadır.

$H_{1:}$ Dijital göçmenlerle dijital yerlilerin dijital gözetime ilişkin algı-farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır.

Tablo 3.31'de görüldüğü üzere Asymp. Sig. (2-tailed) değerinin ',001' olarak ölçüldüğü görülmekte ve bu değerin '0,05'ten küçük olması nedeniyle $H_0$ hipotezi reddedilmektedir. Yani dijital göçmenlerle dijital yerlilerin dijital gözetime ilişkin algı-farkındalık düzeyleri arasında anlamlı bir farklılık bulunmaktadır. Dijital göçmenlerin dijital gözetim algı ve farkındalık düzeylerinin dijital yerlilere göre daha yüksek olduğu ölçülmüştür.

#### 3.5.1.1. Cinsiyete Göre Dijital Gözetim Algı-Farkındalık Düzeyleri

Cinsiyete göre dijital gözetim algı-farkındalık düzeylerini ölçmek amacıyla Mann-Whitney U testi uygulanmıştır.

**Tablo 3.32 Mann-Whitney U Testi – Cinsiyete Göre Dijital Gözetim Algıları**

| | Dijital gözetime ilişkin algı-farkındalık |
|---|---|
| Mann-Whitney U | 75293,000 |
| Wilcoxon W | 160371,000 |
| Z | -2,195 |

| | |
|---|---|
| Asymp. Sig. (2-tailed) | ,028 |

$H_{0:}$ Kadınlar ve erkekler arasında dijital gözetime ilişkin algı-farkındalık düzeyleri açısından anlamlı bir farklılık bulunmamaktadır.

$H_{1:}$ Kadınlar ve erkekler arasında dijital gözetime ilişkin algı-farkındalık düzeyleri açısından anlamlı bir farklılık bulunmaktadır.

Tablo 3.32'de görüldüğü üzere Asymp. Sig. (2-tailed) değerinin ',028' olarak ölçüldüğü görülmekte ve bu değerin '0,05'ten küçük olması nedeniyle $H_0$ hipotezi reddedilmektedir. Yani kadınlar ve erkekler arasında gözetime ilişkin algı-farkındalık düzeyleri açısından anlamlı bir farklılık bulunmaktadır. Kadınların algı ve farkındalık düzeylerinin erkeklere göre daha yüksek olduğu ölçülmüştür.

### 3.5.1.2. Eğitim Durumuna Göre Dijital Gözetim Algı-Farkındalık Düzeyleri

Eğitim durumu ile dijital gözetim arasında anlamlı bir ilişkinin bulup bulunmadığının ölçmek amacıyla parametrik olmayan bir analiz yöntemi olan Ki-Kare testi uygulanmıştır.

**Tablo 3.33 Ki-Kare Testi – Eğitim Durumuna Göre Gözetim Algıları**

| | Value | df | Asymp.Sig.(2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 47,191[a] | 15 | ,000 |
| Likelihood Ratio | 42,340 | 15 | ,000 |
| Linear-by-Linear Association | 7,077 | 1 | ,008 |
| N of Valid Cases | 803 | | |

$H_{0:}$ Eğitim durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmamaktadır.

$H_{1:}$ Eğitim durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmaktadır.

Tablo 3.33'te görüldüğü üzere Asymp. Sig. (2-sided) anlamlılık değerinin ',000' olarak ölçüldüğü görülmekte ve bu değerin '0,05'ten küçük olması nedeniyle $H_0$ hipotezi reddedilmektedir. Yani eğitim durumu ile dijital gözetim algı-farkındalık arasında anlamlı bir ilişki bulunmaktadır.

### 3.5.1.3. Çalışma Durumuna Göre Dijital Gözetim Algı-Farkındalık Düzeyleri

Çalışma durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişkinin bulup bulunmadığının ölçmek amacıyla Ki-Kare testi uygulanmıştır.

**Tablo 3.34 Ki-Kare Testi – Çalışma Durumuna Göre Gözetim Algıları**

| | Value | df | Asymptotic Significance (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 63,041[a] | 21 | ,000 |
| Likelihood Ratio | 63,364 | 21 | ,000 |
| Linear-by-Linear Association | 8,706 | 1 | ,003 |
| N of Valid Cases | 796 | | |

$H_{0:}$ Çalışma durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmamaktadır.

$H_{1:}$ Çalışma durumu ile dijital gözetim algı-farkındalık düzeyleri arasında anlamlı bir ilişki bulunmaktadır.

Tablo 3.34'te görüldüğü üzere Asymp. Sig. (2-sided) anlamlılık değerinin ',000' olarak ölçüldüğü görülmekte ve bu değerin '0,05'ten küçük olması nedeniyle $H_0$ hipotezi reddedilmektedir. Yani çalışma durumu ile dijital gözetim algısı arasında anlamlı bir ilişki bulunmaktadır.

## 3.5.2. Kişiselleştirme-Mahremiyet İhlaline İlişkin Endişe Düzeyleri

Kişiselleştirmenin ile mahremiyet ihlaline ilişkin endişeleri artırıp artırmadığını ölçmek amacıyla parametrik olmayan bir analiz yöntemi olan Spearman's Korelasyonu testi uygulanmıştır.

**Tablo 3.35 Sperman's Korelasyon Analizi – Kişiselleştirme-Mahremiyet İhlali Endişe Düzeyleri**

| | | | Kişiselleştirme | Mahremiyet İhlali Endişe Düzeyi |
|---|---|---|---|---|
| Spearman's rho | **Kişiselleştirme** | Correlation Coefficient | 1,000 | ,302** |
| | | Sig. (2-tailed) | . | ,000 |
| | | N | 817 | 804 |
| | **Mahremiyet İhlali Endişe Düzeyi** | Correlation Coefficient | ,302** | 1,000 |
| | | Sig. (2-tailed) | ,000 | . |
| | | N | 804 | 811 |

**. Correlation is significant at the 0.01 level (2-tailed).

$H_{0:}$ Mobil ortam reklamlarında kullanılan kişiselleştirme, dijital gözetim bağlamında mahremiyet ihlaline ilişkin endişeleri artırmamaktadır.

$H_{1:}$ Mobil ortam reklamlarında kullanılan kişiselleştirme, dijital gözetim bağlamında mahremiyet ihlaline ilişkin endişeleri artırmaktadır.

Tablo 3.35'de görüldüğü üzere correlation anlamlılık değerinin ',302**' olarak ölçüldüğü görülmekte, pozitif yönde bir ilişki söz konusu olmakta ve $H_0$ hipotezi reddedilmektedir. Yani mobil ortam reklamlarında kullanılan kişiselleştirme, dijital gözetim bağlamında mahremiyet ihlaline ilişkin endişeleri artırmaktadır.

### 3.5.3. Dijital Göçmenler ve Dijital Yerlilerin Gizlilik Endişesi Düzeyleri

Dijital göçmenler ve dijital yerlilerin gizlilik ihlali endişesi düzeylerini ölçmek amacıyla Mann-Whitney U testi uygulanmıştır.

**Tablo 3.36 Mann-Whitney U Testi – Gizlilik Endişeleri**

| | **Gizlilik Endişeleri** |
|---|---|
| Mann-Whitney U | 67650,000 |
| Wilcoxon W | 151905,000 |
| Z | -6,167 |
| Asymp. Sig. (2-tailed) | ,000 |

$H_{0:}$ Dijital göçmenler ve dijital yerliler arasında arama yaptıkları ürünler ve hizmetlerle ilgili reklama maruz bırakılmaları sonucunda duydukları gizlilik ihlali endişesi düzeylerinde anlamlı bir farklılık bulunmamaktadır.

$H_{1:}$ Dijital göçmenler ve dijital yerliler arasında arama yaptıkları ürünler ve hizmetlerle ilgili reklama maruz bırakılmaları sonucunda duydukları gizlilik ihlali endişesi düzeylerinde anlamlı bir farklılık bulunmaktadır.

Tablo 3.36'da görüldüğü üzere Asymp. Sig. (2-tailed) değerinin ',000' olarak ölçüldüğü görülmekte ve bu değerin '0,05'ten küçük olması nedeniyle $H_0$ hipotezi reddedilmektedir. Yani dijital göçmenler ve dijital yerliler arasında arama yaptıkları ürünler ve hizmetlerle ilgili reklama maruz bırakılmaları sonucunda duydukları gizlilik ihlali endişesi düzeylerinde farklılık bulunmaktadır.

# SONUÇ

Mobil ortamlarda bireylerin gözetimi çeşitli uygulamalarla giderek kolaylaşmış, internetteki gözetim ise daha da meşru hale gelmiştir. David Lyon (2006: 180)'un bahsetmiş olduğu "gündelik hayatın izlenmesi" çabası kişilerin tüm aktivitelerinin takip edilmesiyle sonuçlanmış, böylelikle sürekli ve gözetleyen için pek çok açıdan işlevsel olan gözetim giderek yaygınlaşmıştır. Michel Foucault (1992: 222)'un deyişiyle "sürekli gözetim altında tutma" kişiler üzerine daha fazla nüfuz etmiş ve gündelik hayatı da etkisi altına almıştır. Öyle ki şirketler ve devletlerin gözetimi dışında bireyler de birbirlerini gözetleyerek, mobil ortamlardaki gözetime dahil olmuştur. Çalışmanın kuramsal kısmında bahsedilen 'belirli amaçlar doğrultusunda sistematik bilgi toplama' ve 'verilerin toplandığı kişileri etkileme' konuları araştırmanın veri gözetimine odaklanmasını sağlamış, bilişim teknolojileri aracılığı ile gerçekleştirilen ve görünürde rızaya dayalı olan dijital gözetimin Süperpanoptikon kavramı ile açıklanması nedeniyle mobil ortamlardaki dijital gözetim bu yönüyle değerlendirilmiştir.

Mobil ortam reklamlarında gerçekleşen gözetim ise 'kişiselleştirme' yoluyla yapılmakta ve kişisel verilerin kişilerin rızası dışında kullanılmasına neden olmaktadır. Mobil ortamlardaki gizlilik ve mahremiyet ihlalleri son yıllarda artış göstermiş, bu ortamlar kullanıcıların kişisel alanı olarak kabul edilen mobil cihazlar aracılığıyla gerçekleşen veri sızıntılarının merkezi haline gelmiştir. Araştırma sürecinde yapılan gözlemlere dayanılarak ve araştırma sonucunda elde edilen bulgular ışığında, mobil ortamlardaki gözetimin kişiselleştirme için kişisel verilerin elde edilmesi çabası sonucu gerçekleştiği anlaşılmıştır. İlgili literatür de bu sonucu desteklemektedir. Bu ortamlarda gerçekleşen gözetimin farkında olma ve etkilerinden korunma durumlarının ise kişilerin yaş, cinsiyet, eğitim durumu, çalışma durumu ve kullanıcıların dijital becerilerine göre değişiklik gösterdiği araştırmanın önemli bulguları arasındadır. Bulgulara göre dijital göçmenler mobil ortamlarda gerçekleşen gözetimin daha fazla farkındadır. Ayrıca kadın katılımcıların gözetime ilişkin farkındalıkları daha yüksektir. Gözetimin etkilerinden korunma durumunun da dijital beceri ve eğitimle ilişkili olduğu görülmektedir. Eğitim seviyesi arttıkça dijital beceri de artmakta, dolayısıyla gözetimden korunma durumu da buna paralel olarak artmaktadır.

Dijital göçmenlerin dijital gözetim algılarının dijital yerlilere göre yüksek olmasına karşın, teknolojiye ve uygulamalara dijital yerliler kadar hakim olmadıkları beklenilen bir sonuç olarak elde edilmiştir. Bununla birlikte dijital göçmenlerin mahremiyet ihlaline ilişkin endişe düzeylerinin dijital yerlilere göre daha yüksek olduğu görülmektedir. Bu bulgular dijital göçmenlerin dijital dünyadan ve internet ortamından korktuklarını ortaya koymuştur. Yine bu

endişelere paralel olarak dijital göçmenlerin, mahremiyetin korunması konusunda dijital yerlilere göre daha umutsuz oldukları anlaşılmıştır. Bu umutsuzluğun, öğrenilmiş çaresizlik durumunu da beraberinde getirdiği, dijital göçmenlerde gizliliği ve mahremiyeti korumanın olanaklı olamayacağı düşüncesinin de kalıplaşmış bir düşünce haline geldiği görülmüştür.

Kişiler, mobil ortamlardaki dijital gözetimin farkında olmalarına rağmen bu durumu sorgulamamaktadır. İnternette mahremiyeti korumanın olanaklı olmadığını düşünen kişiler çoğunlukta olmasına rağmen, internet ortamında kişisel bilgilerini paylaşmaktan çekinmemekte ve bu ortamlarda vakit geçirmekten vazgeçmemektedirler. Literatüre bakıldığında da benzer sonuçların olduğu görülmektedir. Veri toplama ve takibe karşı kişiler genelde bunu *ürpertici* bulmakta, gözetime olumsuz yaklaşmaktadır. Ancak kişiler gözetime karşı olumsuz yaklaşsalar da veri toplamayı içeren teknolojileri ve uygulamaları kullanmaya devam etmektedir (Shklovski vd., 2014: 2347).

Kişilerin gözetime karşı verdiği reaksiyon da büyük çoğunlukla tepkisizlik hali olmaktadır. Gözetimin farkında olan kişiler gözetime tepki vermemekte, kendisinin bu durumdan etkilenmeyeceğini düşünmektedir. Buna ilaveten kişiler gözetimin hep var olduğunu ve bundan sonra da var olacağını düşünmekte ve kabullenmektedir. Bu durum yine Panoptikon kavramını işaret etmekte, gözetimin kişilerde öğrenilmiş çaresizlik durumunu yaratan bir eylem olduğunu göstermektedir. Kişiler, kişisel bilgileri tanımlamakta da zorluk çekmektedirler. Kişiler, kişisel bilgi olarak tanımladıkları bilgileri (bunlar genelde kimlik numaraları, telefon numaraları ve iş/ev adresi ile sınırlı bilgileridir) paylaşmaktan çekinmekte, bu bilgileri daha mahrem bilgiler olarak görmektedirler. E-posta bilgileri ise ikamet/iş adresi bilgilerine göre daha sanal bir nitelik taşıdığından daha çok paylaşılmaktadır. Ancak kullanıcılar bu duruma dikkat etse de bir süre sonra kişisel verileri üzerindeki kontrolü kaybetmektedir. Özellikle mobil uygulamalarda gerçekleşen veri sızıntıları hesaba katıldığında kişiler mobil ortamlarda bu bilgilerini paylaşsa da paylaşmasa da, çeşitli mobil uygulamalarca bu bilgiler üçüncü kişilere sızdırılmaktadır. Ayrıca kullanıcılara ücretsiz olarak sunulduğu iddia edilen ve ücretsiz olarak kullanıldığı sanılan mobil uygulamaların bedelinin, kişisel ve mahrem bilgilerin kaybedilişiyle kişiler tarafından ödendiği görülmektedir. Aynı şekilde sosyal medya ve web ortamında çerez ve gizlilik politikaları okunmadan verilen izinler, kişisel verileri şirketlerin ve reklam verenlerin kullanımına daha açık hale getirmektedir. Araştırma bulgularına göre kişiler genel olarak çerezler hakkında bilgi sahibi değillerdir. Araştırma kapsamında şirketlerin ya da mobil uygulamaların çerezler konusunda kişileri yeteri kadar bilgilendirmediği de ortaya konulmuştur. Mobil uygulamalardaki veri sızıntılarının en önemli aracı olan erişim izinleri konusunda da kullanıcılar mobil uygulamaların erişim izinlerine genelde dikkat etse de, yine

bu uygulamaları kullanmaktan vazgeçmemektedir. Literatüre bakıldığında kullanıcıların erişim izinlerine dikkat ettiği halde popüler uygulamalardan vazgeçmediği ortaya konulmuştur. Buradan hareketle kullanıcıların mobil uygulamaların erişim izinlerine bağlı olarak mobil uygulamayı kullanıp kullanmama durumlarının mobil alandaki çalışmalar açısından önemli olduğu anlaşılmaktadır. Ülkemizde de bu durumla ilgili olarak yapılacak çalışmalara ihtiyaç duyulduğu ön görülmekte, kullanıcıların uygulamalara ilişkin eylemlerinin ölçülmesinin yararlı olacağı düşünülmektedir.

Mobil ortamlarda var olan ve bu ortamlarda yayınlanan reklamlarla gerçekleştirilen dijital gözetimden korunma sorumluluğunun ilgili yasal düzenlemeler çerçevesinde kişilere/kullanıcılara bırakılmış olduğu anlaşılmıştır. Buradan hareketle medya okuryazarlığı konusu üzerinde daha fazla durulması gerekmekte ve reklamları eleştirel bakış açısı ile okuyabilmek için genel eğitim yapısının; dolayısıyla medya okuryazarlığı eğitimine yönelik müfredatın içeriğinin eleştirel yaklaşımla hazırlanması ve uygulanması gerekmektedir (Taşkaya, 2016: 227). Araştırma sonucunda, dijital gözetim ve kullanıcıların kişisel verilerinin korunmasıyla ilgili, devletin denetim mekanizmalarının yetersiz bulunduğu ve kişilerin devletin koruyuculuğuna inanmadığı sonucu ortaya konulmuştur. Kişilerin genel olarak dijital haklarını bilmediği ve KVKK hakkında bilgi sahibi olmadığı görülmüştür. Ayrıca dijital gözetimin farkında olma durumunun dijital göçmenlere ve dijital yerlilere göre farklılık gösterdiği halde aynı yasal koruyuculuk çerçevesinde bulunmaları da tartışılmış, kişisel verilerin korunması, tüketicinin korunması ya da bu alandaki düzenlemelerin, -özellikle cezai yaptırımlar kapsamında- kuşakların yaş, eğitim durumu, dijital olanaklar ve dijital becerilerine göre değerlendirilerek düzenlenmesi gerekliliği de ortaya konulmuştur. Gelinen noktada, gözetimin etkilerinden korunmak ve mahremiyeti korumak bireysel düzlemde mümkün görünmemektedir. Gelecekte yaşanabilecek en önemli insan hakkı ihlallerinin, bu sistemlerin sunduğu imkanlar ve meşru kıldığı düzen sayesinde olacağı da uzak bir ihtimal değildir (Yanık, 2017: 796). Bu bağlamda mevcut yasal düzenlemelerin ve yeni yapılacak olan kanunların, dijital gözetime ilişkin kuşaklar arası algı ve farkındalık düzeylerine odaklanılarak revize ve inşa edilmesi gerekmektedir.

Bundan sonra yapılacak araştırmalarda, mobil ortamlar ve mobil ortam reklamlarında gerçekleşen dijital gözetim ile ilgili nitel araştırmalarla da elde edilecek sonuçlara dayanılarak dijital alanda yapılacak çalışmaların genişletilmesi bu alandaki ihtiyacın karşılanması için oldukça önemlidir.

# KAYNAKÇA


Akgül, A. (2013). *Kişisel Verilerin Korunması Açısından İdarenin Hukuki Sorumluluğu ve Yargısal Denetimi.* Doktora Tezi. Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü.

Akgül, A. (2015). ‘‘Kişisel Verilerin Korunmasında Yeni Bir Hak: ‘‘Unutulma Hakkı’’ ve AB Adalet Divanı’nın ‘‘Google Kararı’’, *TBB Dergisi,* (116): 11-38.

Akgün, A. E. ve Keskin, H. (2003). “Sosyal Bir Etkileşim Süreci Olarak Bilgi Yönetimi ve Bilgi Yönetimi Süreci”. *İktisadi ve İdari Bilimler Fakültesi Dergisi*, 5(1): 175-188.

Aktaş, C. ve Çaycı, B. (2013). “Yeni Enformasyon ve İletişim Teknolojilerinin Sosyal Hayattaki Rolü”. https://www.academia.edu/5175989/Yeni_Enformasyon_ve_%C4%B0leti%C5%9Fim_Teknolojilerinin_Sosyal_Hayattaki_Rol%C3%BC_The_Role_of_New_Information_and_Communication_Technologies_in_Social_Life (erişim tarihi: 17.05.2018)

Alternatif Bilişim Derneği (2013). Veri Korumaya Giriş [Broşür] https://ekitap.alternatifbilisim.org/files/veri_korumaya_giris_edri_paper_06_tr.pdf (Erişim Tarihi: 22.12.2017).

Altuntuğ, N. (2012). “Kuşaktan Kuşağa Tüketim Olgusu ve Geleceğin Tüketici Profili”. *Organizasyon ve Yönetim Bilimleri Dergisi*, 4(1): 203-212.

Arslantaş-Toktaş, S., Binark, M., Dikmen, E. Ş., Küzeci, E., ve Özaygen, A. (2012). *Türkiye’de Dijital Gözetim: TC Kimlik Kartlarından E Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi.* Alternatif Bilişim Derneği, İstanbul.

Arvidsson, A. ve Bonini, T. (2015). “Valuing Audience Passions: From Smythe to Tarde”.*European Journal of Cultural Studies*, 18(2): 158-173.

Assange, J., Appelbaum, J., Müller-Maguhn, A. ve Zimmermann, J. (2013). *Şifrepunk: Özgürlük ve İnternetin Geleceği Üzerine Bir Tartışma*. (Çev. A. D. Temiz). Metis Yayınları, İstanbul.

Avşar Z., Elden M., Çaydere O. ve Bakır, U. (2011). *Reklam ve Hukuksal Düzenlemeleri*. Geçit Yayınları, İstanbul.

Aydın. S. (2016). *Gelişen Web Teknolojileri İle Şekillenen İnternet Reklamcılığının Tüketici Davranışlarına Etkisi, Çevrimiçi Davranışsal Reklamcılık Üzerine Bir Araştırma.* Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Baek, T. H. ve Morimoto, M. (2012). Stay Away From Me. *Journal of Advertising*, 41(1): 59-76.

Ball, K. ve Webster, F. (2003). *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Age*. Pluto Press.

Basalla, G. (2013). *Teknolojinin Evrimi*. (Çev. C. Soydemir), Doğu Batı Yayınları, Ankara.

Başaran, F. (2010). "Yeni İletişim Teknolojileri, Alternatif İletişim Olanakları". *Mülkiye Dergisi*, 34(269): 255-270.

Baştürk, E. (2016) *Gözetimin Soykütüğü: Faucault'dan Deleuze'e Postmodern Bir Arkeoloji*. Kalkedon Yayıncılık, İstanbul.

Baudrillard, J. (2008). *Tüketim Toplumu*, (Çev. H. Deliceçaylı ve F.Keskin), Ayrıntı Yayınları, İstanbul.

Bauman, Z. (2005). *Bireyselleşmiş Toplum*. (Çev. Y. Alogan), Ayrıntı Yayınları, İstanbul.

Bauman, Z. ve Lyon, D. (2013). *Akışkan Gözetim*. (Çev. E. Yılmaz), Ayrıntı Yayınları, İstanbul.

Bauman, Z. (2016). *Küreselleşme.* (Çev. A. Yılmaz), Ayrıntı Yayınları, İstanbul.

Becerikli, S. Y. (2013). Kuşaklararası İletişim Açısından Yeni İletişim Teknolojilerinin Kullanımı: İleri Yas Grubu Üzerine Bir Değerlendirme. *İstanbul Üniversitesi İletişim Fakültesi Dergisi*, (44), 19-31.

Beniger, J. (2009). *The control revolution: Technological and Economic Origins of the Information Society*. Harvard University Press.

Berger A. A., N. Ulutak ve A. Tunç (ed.). (1993). *Kitle İletişiminde Çözümleme Yöntemleri*. Anadolu Üniversitesi Yayınları, Eskişehir.

Berger, J. (2008). *Görme Biçimleri*. (Çev. Y. Salman), Metis Yayınları, İstanbul.

Berger, L. ve Huntington, S. (2003). *Bir Küre Bin Bir Küreselleşme*. Kitap Yayınevi, İstanbul.

Bigo, D. ( 2006) '*Security, Exception, Ban and Surveillance*', D. Lyon (ed.) *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton :Willan Publishing, 46-68.

Bleier, A. ve Eisenbeiss, M. (2015). "The Importance of Trust for Personalized OnlineAdvertising". *Journal of Retailing*, 91(3): 390-409.

Bogard, W. (1996). *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. Cambridge University Press.

Book T. ve Wallach D. S. (2015). "An Empirical Study of Mobile Ad Targeting," *Arxiv Preprint Arxiv:1502.06577*,1-14.https://arxiv.org/pdf/1502.06577.pdf (erişim tarihi: 01.02.2017)

Bozkurt, V. (2000). "Gözetim ve İnternet: Özel Yaşamın Sonu Mu?". *Birikim Dergisi*, (136): 75-81.

Briggs, A. ve Burke, P. (2004). *Medyanın Toplumsal Tarihi: Gutenberg'den İnternete*. (Çev.İ. Şener), İzdüşüm Yayınları, İstanbul.

Castells, M. (2008). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür: Kimliğin Gücü*. Bilgi Üniversitesi Yayınları, İstanbul.

Castells, M. (2013). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür: Ağ Toplumunun Yükselişi*. (Çev. E. Kılıç), Bilgi Üniversitesi Yayınları, İstanbul.

Castells, M. (2016). *İletişim Gücü* (Çev. E. Kılıç), Bilgi Üniversitesi Yayınları, İstanbul.

Chaney, D. (1999). *Yaşam Tarzları,* (Çev. İ. Kutluk). Dost Yayınları, Ankara.

Chatfield, T. (2013). *Dijital Çağa Nasıl Uyum Sağlarız.* (Çev. L. Konca), Sel Yayıncılık, İstanbul.

Chen, P. T. ve Hsieh, H. P. (2012). "Personalized Mobile Advertising: Its Key Attributes, Trends, And Social Impact". *Technological Forecasting and Social Change*, 79(3): 543-557.

Civelek, D. Y. (2011). *Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi.* Uzmanlık Tezi, TC Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı.

Cleff, E. B. (2008). "Regulating Mobile Advertising in the European Union and the United States". Computer Law & Security Review, 24(5): 421-436.

Çalık, D. ve Toker, G. (2016). "Ekran Çağı İnsanı ve Dijital Toplum", *XXI. Yüzyılda Türkiye'de İnternet Konferansı*, 03-05 Kasım 2016, Ankara: TED Üniversitesi.

Çakır, M. (2015). *İnternette Gösteri ve Gözetim. Eleştirel Bir Okuma*. Ütopya Yayınevi, Ankara.

Çaycı, B. ve Karagülle, A. E. (2016). "İletişimin Dijitalleşmesi ve Kültürel Melezleşme" *Global Media Journal: Turkish Edition*, 6(12): 570-586.

Çaycı, A. E. ve Çaycı, B. (2017). "Dijital İletişim Çağında Teknolojinin Açığa Çıkardıkları: Gözetim ve Mahremiyet". *İnönü Üniversitesi İletişim Fakültesi Elektronik Dergisi (İNİF E Dergi)*, 1(2): 157-169.

Çığ, E. Ç. (2016). "Dijital Çağda Bakışın Politikası: Panoptikon ve Aleniyet İlkesi". *Toplum ve Demokrasi Dergisi*, 10(21): 91-113.

Çoban, B. (2016). "Gözün İktidarı Üzerine", (Çev. ve hzl. B. Çoban ve Z. Özarslan), *Panoptikon: Gözün İktidarı. Su Yayınları*, İstanbul, 111-138.

Çuhadar M. (2013). "Turizmde Veri Madenciliği Alanında Yapılan Akademik Çalışmaların İncelenmesi: Türkiye ve Dünya Karşılaştırması". 14. Ulusal Turizm Kongresi, 5-8 Aralık 2013, Kayseri: 1448-1466.

Dağtaş, B. (2009). *Reklam Kültür Toplum*. Ütopya Yayınevi, Ankara.

De Castro, J. E. ve Shimakawa, H. (2006). "Mobile Advertisement System Utilizing User's Contextual Information". *In Mobile Data Management, MDM 2006. 7th International Conference on*, 91-91.

De Keyzer, F., Dens, N., ve De Pelsmacker, P. (2015). "Is This For Me? How Consumers Respond To Personalized Advertising On Social Network Sites". *Journal of Interactive Advertising*, 15(2): 124-134.

Dolgun, U. (2004). "Gözetim Toplumunun Yükselişi: Enformasyon Toplumundan Gözetim Toplumuna". *Yönetim Bilimleri Dergisi (1: 3)*

Dolgun, U. (2008). *Şeffaf Hapishane Yahut Gözetim Toplumu*. Ötüken Neşriyat, İstanbul.

Emiroğlu, B.G. (2009). "Semantik Web (Anlamsal Ağ) Yapıları ve Yansımaları". XI. Akademik Bilişim Konferansı'nda sunulan bildiri. 11-13 Şubat 2009. Şanlıurfa.

Ersoy, U. (2009**)**. *Bir İnsan Hakları Kavramı Olarak "Kişisel Verilerin Korunması".* Yüksek Lisans Tezi. Gazi Üniversitesi Sosyal Bilimler Enstitüsü.

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H., ve Öneş. O. (2017). "Büyük Veride Kişi Mahremiyetinin Korunması". *International Journal Of Informatics Technologies*, 10(2): 177-184.

Featherstone, M. (2005). *Postmodernizm ve Tüketim Kültürü*. (Çev. M. Küçük), Ayrıntı Yayınları, İstanbul.

Fisher, E. (2015). "'You Media': Audiencing as Marketing in Social Media". *Media, Culture & Society*, 37(1): 50-67.

Fiske, J. (2012). *Popüler Kültürü Anlamak*. Parşömen Yayınları, İstanbul.

Fiske, J. ve Hancock, B. H. (2016). *Media Matters: Race & Gender in US Politics*. Routledge.

Foucault, M. (1992). *Hapishanenin Doğuşu*. (Çev. M. A. Kılıçbay), İmge Kitabevi, Ankara.

Foucault, M. (2003). *İktidarın Gözü.* (Çev. I. Ergüden), Ayrıntı Yayınları, İstanbul.

Foucault, M. (2005). *Özne ve İktidar*. (Çev. I. Ergüden ve O. Akınay), Ayrıntı Yayınları, İstanbul.

Foucault, M. (2007). *Cinselliğin Tarihi*. (Çev. H. U. Tanrıöver), Ayrıntı Yayınları, İstanbul.

Fuchs, C. (2011). "New Media, Web 2.0 and Surveillance". *Sociology compass*, 5(2): 134-147.

Fuchs, C. (2012a). "Political Economy and Surveillance Theory". *Critical Sociology*, 39(5): 671-687.

Fuchs, C. (2012b). "Critique, Democracy and Philosophy in 21st Century Information Society. Towards Critical Theories of Social Media". *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, 10(1): 114-121.

Fuchs, C. (2015). *Dijital Emek ve Karl Marx.* (Çev. T. E. Kalaycı ve S. Oğuz), Nota Bene Yayınları, İstanbul.

Geray, H. (2003). *İletişim ve Teknoloji*. Ütopya Yayınevi, Ankara.

Giddens, A. (1984). *The Constitution of Society: Outline of the Structuration Theory.* Cambridge Polity Press.

Giddens, A. (1987). *Social Theory and Modern Sociology*. Stanford University Press.

Giddens, A. (2001). *Sosyoloji: Eleştirel Bir Giriş*. (Çev. Ü. Yıldız), Phoenix Yayınevi, Ankara.

Gülenç, K. ve Arıtürk, M. H. (2014). "Teknoloji Çağında Rasyonalite, Deneyim ve Bilgi: Sorunlar & Eleştiriler". *Uludağ Üniversitesi Fen-Edebiyat Fakültesi Felsefe Dergisi*, (22): 113-131.

Güven, S. K. (2011). "Gözetimin Toplumsal Meşruiyeti" H, Köse, (Ed.). *Medya Mahrem Medyada Mahremiyet Olgusu ve Transparan Bir Yaşamdan Parçalar*. Ayrıntı Yayınları, İstanbul, 173-198.

Hackley, C. (2002). "The Panoptic Role Of Advertising Agencies In The Production Of Consumer Culture". *Consumption, Markets and Culture*, 5(3): 211-229.

Harvey, D. (1997). *Postmodernliğin Durumu*. (Çev. S. Savran), Metis Yayınları, İstanbul.

Herbert, M. (2010). *Tek Boyutlu İnsan*. (Çev. A.Yıldırımlı), İdea Yayınları, İstanbul.

Hier, S. ve Greenberg, J. (2007). *The Surveillance Studies Reader*. McGraw-Hill Education.

İnam, A. (1999). *Teknoloji Benim Neyim Oluyor?* Metu Press Odtü Geliştirme Vakfı Yayıncılık, Ankara.

İsmayılov, E. K. ve Sunal, G. (2012). "Gözetlenen ve Gözetleyen Bir Toplumda, Beden ve Mahremiyet İlişkisi: Facebook Örneği". *Akdeniz İletişim Dergisi*, (18): 21-41.

Karaarslan, E., Eren, M. B., ve Koç, S. (2014). "Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi". Türkiye'de İnternet Konferansı, İzmir.

Karabıyık, B. K. ve Armağan, E. (2017). "Tüketicinin Çevrimiçi Davranışsal Reklamlara Tıklama Kararını Etkileyen Faktörler". *Journal of Yaşar University*, 12(47): 212-215.

Karabulut, B. (2015). "Bilgi Toplumu Çağında Dijital Yerliler, Göçmenler ve Melezler". *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (21): 11-23.

Karacan, H. ve Yeşilbudak, M. (2010). "Kullanıcı Merkezli İnteraktif Veri Madenciliği: Bir Literatür Taraması". *International Journal Of Informatics Technologies*, 3(1): 17-22.

Karakaya, A. (2014). *Yeni İletişim Ortamları İle Sömürgeciliğin Dönüşümü Gözetim Olgusu ve Bireylerin Farkındalık ve Teslimiyetleri Üzerine Bir Araştırma.* Yüksek Lisans Tezi. Marmara Üniversitesi Sosyal Bilimler Enstitüsü.

Karakehya, H. (2009). "Gözetim ve Suçla Mücadele: Gözetimin Tarihsel Gelişimi İle Yakın Dönemde Gerçekleştirilen Hukuki Düzenleme ve Uygulamalar Bağlamında Bir Değerlendirme". *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 58(2): 319-357.

Karahisar, T. (2013). "Dijital Nesil, Dijital İletişim ve Dijitalleşen (!) Türkçe". *AJIT-e: Online Academic Journal of Information Technology,* 4(12): 71-83.

Kaya, C. (2011). "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi". *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası,* 69(1-2): 317-334.

Ketizmen, M. (2008). *Türk Ceza Hukukunda Bilişim Suçları: Bilişim Alanında Suçlar, Kişisel Verilerin Korunması*. Adalet Yayınevi, Ankara.

Kılıç, Ç. (2011). "Küreselleşen Dünyada Dijital Bölünme Sorunu". *Erzincan Üniversitesi Eğitim Fakültesi Dergisi,* 13(1): 81-91.

Kılınç, D. (2012). "Anayasal Bir Hak Olarak Kişisel Verilerin Korunması". *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61(3): 1089-1169.

Kıray, M. B. ve Bayazıt, N. (2005). *Tüketim Normları Üzerine Karşılaştırmalı Bir Araştırma*. Bağlam Yayıncılık, İstanbul.

Kırlıdoğ, M ve Fidaner, I. B. (2013). "Derin Veri Analizi: İnternet'teki Temel Gözetim Aracı". *Akademik Bilişim Konferansı 2013*, Antalya.

Korkmaz, İ. (2016). "Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme". *TBB Dergisi*, 124: 81-152.

Korkmaz, İ. (2013). "Facebook ve Mahremiyet: Görmek ve Gözetle(N)Mek". *Yalova Üniversitesi Sosyal Bilimler Dergisi*, 3(5): 107-122.

Korkmaz, A. (2014). "İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması". *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi* 16(1): 99-103.

Küzeci, E. (2010). *Kişisel Verilerin Korunması*. Turhan Kitabevi, Ankara.

Leppaniemi, M. ve Karjaluoto, H. (2005). "Factors İnfluencing Consumers' Willingness To Accept Mobile Advertising: A Conceptual Model". *International Journal of Mobile Communications,* 3(3), 197-213.

Lefebvre. H. (2016). *Modern Dünyada Gündelik Hayat*. (Çev. I. Gürbüz), Metis Yayınları, İstanbul.

Lyon, D. (1997). *Elektronik Göz*. (Çev. D. Hattatoğlu), Sarmal Yayınevi, İstanbul.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. McGraw-Hill Education.

Lyon, D. (2003). *Surveillance After September 11*. Polity Press.

Lyon, D. (2006). *Gözetlenen Toplum: Günlük Hayatı Kontrol Etmek.* (Çev. G. Soykan), Kalkedon Yayıncılık, İstanbul.

Lyon, D. (2013). *Gözetim Çalışmaları.* (Çev. A. Toprak), Kalkedon Yayıncılık, İstanbul.

Marx, K. (2012). *Grundrisse: Ekonomi Politiğin Eleştirisi İçin Ön Çalışma*. (Çev. S. Nişanyan), Birikim Yayınları, İstanbul.

Maslowska, E., Smit, E. G. ve Van Den Putte, B. (2016). "It Is All in the Name: A Study of Consumers' Responses to Personalized Communication". *Journal of Interactive Advertising*, 16(1), 74-85.

Mathiesen, T. (1997). "The Viewer Society: Michel Foucault's Panoptikon Revisited" *Theoretical Criminology,* 1:215-234.

Mathiesen, T. (2004). *Silently Silenced: Essays On The Creation Of Acquiescence in Modern Society*. Waterside Press.

Mayer-Schönberger V. ve Cukier S. K. (2013) *Büyük Veri: Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim.* (Çev. B. Erol), *Paloma Yayınevi, İstanbul.*

McDonald, A. ve Cranor, L. F. (2010). "Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising,". *Research Conference on Communication, Information and Internet Policy*, (30): 1-31

Meng, W. Ding R., Chung S. P., Han S., ve Lee W. (2016:) "The Price Of Free: Privacy Leakage In Personalized Mobile In-Apps Ads," *23nd Annual Network and Distributed System Security Symposium, NDSS, San Diego, California, USA*, February, 1-15.

Morley, D. ve Robins, K. (2011). *Kimlik Mekânları: Küresel Medya, Elektronik Ortamlar ve Kültürel Sınırlar*. (Çev. E. Zeybekoğlu), Ayrıntı Yayınları, İstanbul.

Mutlu, E. (2005). *Globalleşme, Popüler Kültür ve Medya*. Ütopya Yayınevi, Ankara.

Orwell, G. (2015). *1984*. (Çev. C. Üster), Can Sanat Yayınları, İstanbul.

Öncü, G. A. (2011). *Avrupa İnsan Hakları Sözleşmesinde Özel Yaşamın Korunması Hakkı*, Beta Yayınevi, İstanbul.

Özarslan, Z. (2016). "Gözün İktidarı: Elektronik Gözetim Sistemleri", *Panoptikon: Gözün İktidarı.* (Çev. ve hzl. B. Çoban ve Z. Özarslan), *Su Yayınları*, İstanbul, 139-153.

Özdemir, H. (2009). "*Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması"*. Seçkin Yayıncılık, Ankara.

Özdilek, A. O. (2002). *İnternet ve Hukuk*. Papatya Yayıncılık, İstanbul.

Özgüven, N. (2013). "Tüketicilerin Mobil Reklamcılığı Kabullenmelerinde Etkili Olan Faktörler Üzerine Bir Uygulama", *Yönetim Bilimleri Dergisi*, 11(21): 7-28.

Öztürk, S. (2013). "Filmlerle Görünürlüğün Dönüşümü: Panoptikon, Süperpanoptikon, Sinoptikon". *İletişim Kuram ve Araştırma Dergisi*, (36): 132-151.

Prensky, M. (2001b). *"Digital Natives, Digital İmmigrants, Part II: Do They Really Think Differently? On the Horizon"* 9(6): 1-6: http://d.scribd.com/docs/25yfw2gwramobinjk3vt.pdf. (erişim tarihi: 15.12.2017).

Prensky, M. (2001a). *"Digital Natives, Digital İmmigrants. On the Horizon"* 9(5): 1-6. https://www.marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf (erişim tarihi: 15.12.2017).

Sağıroğlu Ş. ve Mohammed M. (2009). "Mobil Ortamlara Yapılan Saldırılar Üzerine Bir İnceleme". *Tübav Bilim Dergisi* 2(2):138-147.

Sarı S. N. (2009). *Sınır Tanımayan Reklam Ortamı Açıkhava Reklamcılığı*. Beta Yayınları, İstanbul.

Schiller, D. (2000). *Digital Capitalism: Networking the Global Market System*. MIT Press.

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., ve Borgthorsson, H. (2014). "Leakiness And Creepiness in App Space: Perceptions Of Privacy And Mobile App Use". *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2347-2356.

Smith, K. T. (2011). "Digital Marketing Strategies That Millennials Find Appealing, Motivating, Or Just Annoying". *Journal of Strategic Marketing*, 19(6): 489-499.

Sönmez, B. (2016). "Gözetim Toplumunun Gümümüz Tüketim Dinamikleri Bağlamında Yeniden Yorumlanmasına İlişkin Bir İnceleme". *Selçuk Üniversitesi İletişim Fakültesi Akademik Dergisi*, 9(2): 262-284.

Sözüer, E. (2017). *Unutulma Hakkı.* On İki Levha Yayıncılık, İstanbul.

Strauss, W. ve Howe, N. (1991). *Generations: The History of America's Future, 1584 to 2069*. New York.

Surprenant, C. F. ve Solomon, M. R. (1987). "Predictability And Personalization In The Service Encounter". *The Journal of Marketing*, 86-96.

Şaylan, G. (2002). *Postmodernizm*. İmge Kitabevi, Ankara.

Şentürk, A. (2006). *Veri Madenciliği: Kavram ve Teknikler.* Ekin Yayınevi, Bursa.

Şimşek, O. (2008). *Anayasa Hukukunda Kişisel Verilerin Korunması*. Beta Yayın, İstanbul.

Taşkaya, M. (2009). "Beden Politikaları ve Reklamda Kadın". *2. Uluslararası Suç ve Ceza Film Festivali*, 103-108.

Taşkaya, M. (2013). "Reklamda Nostaljik Unsurlar: Kimlik Vaadi ve Anlamın Tüketimi". *Ethos Felsefe ve Toplumsal Bilimlerde Diyaloglar Dergisi*, 6(1): 1-37.

Taşkaya, M. (2016). "Eleştirel Reklam Okuryazarlığı". E. Küçük Durur (Ed.). *Medya Okuryazarlığı*. Siyasal Kitabevi, Ankara, 189-230.

TBD-Kamu-BİB, Kamu Bilişim Platformu X. "Kişisel Verilerin Korunması." (2008). II. Çalışma Gurubu 1. Bölüm "Kişisel Verilerin Korunması ya da Kişisel Verilerin İşlenmesi Karşılığında Bireyin Korunması" 13-22.

Tekin F. (2012). *Sosyolojik Açıdan Sınır: Hakkâri Örneği. Doktora Tezi.* Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Timisi, N. (hzl.). (2016). *Dijital Kavramlar, Olanaklar, Deneyimler.* Kalkedon Yayınları, İstanbul.

Toffler, A. (2008). *Üçüncü Dalga: Bir Fütürist Ekonomi Analizi Klasiği*. (Çev. S. Yeniçeri), Koridor Yayıncılık, İstanbul.

Tonta, Y. (2009). "Dijital Yerliler, Sosyal Ağlar ve Kütüphanelerin Geleceği". *Türk Kütüphaneciliği*, 23(4): 742-768.

Turow, J. (2015). *İzleniyoruz*. (Çev. M. Benveniste), Hil Yayın, İstanbul.

Türkoğlu, T. (2010). *Dijital Kültür*. Beyaz Yayınları, İstanbul.

Ur B., Leon P. G., Cranor L. F., Shay R., ve Wang Y. (2012). "Smart, Useful, Scary, Creepy: Perceptions Of Online Behavioral Advertising," *In Proceedings of the Eighth Symposium on Usable Privacy and Security, Ser.* Soups'12. New York, USA: ACM, (4:1): 4:15.

Uyanık F. (2013). "Sosyal Medya: Kurgusallık ve Mahremiyet". *Kocaeli Üniversitesi Yeni Medya Kongresi*. 7 Mayıs 2013, Kocaeli: 1-17.

Üşür, İ. (2001). "Teknoloji Felsefesi Üzerine ya da Tarihin Tanrısı Teknoloji Midir?". *Mülkiye Dergisi*, 25(230): 7-26.

Van Dijk, J. ve Hacker, K. (2003). The Digital Divide as a Complex and Dynamic Phenomenon. *The Information Society*, 19(4): 315-326.

Van Dijk, J. (2016). *Ağ Toplumu.* Kafka Yayınevi, İstanbul.

Vatanparast, R. (2007). "Piercing The Fog Of Mobile Advertising". *Management of Mobile Business, 2007. International Conference on the IEEE*, 19-19.

Vincent, D. (2016). *Mahremiyet Kısa Bir Tarih*. (Çev. D. C. Başaraner), Epos Yayınları, İstanbul.

Virilio, P. (2003). *Enformasyon Bombası,* (Çev. K. Şahin), Metis Yayınları, İstanbul.

Wang, M. C., Liao, S., Zhu, R. S., Xu, D. J., Chen, H., ve Wang, W. (2007). Evaluation on a Personalized Mobile Advertising System: a Comparative Approach". *Pacis 2007 Proceedings* (139): 10-18.

Wayne, M. (2009). *Marksizm ve Medya Araştırmaları: Anahtar Kavramlar, Çağdaş Eğilimler.* (Çev. B. Cezar), Yordam Kitap, İstanbul.

Williamson, J. (2011). *Reklamların Dili* (Çev. A. Fethi), Ütopya Yayınevi, Ankara.

Yanık, A. (2017). "Bir Süperpanoptikon Olarak Yeni Medya: Yeni Medya Işığında Gözetimin Eleştirisi". *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 5(2): 784-800.

Zhang, D. (2003). "Delivery Of Personalized And Adaptive Content to Mobile Devices: A Framework And Enabling Technology". *Communications of the Association for Information Systems*, 12(1): 13.

Xu, D. J., Liao, S. S., ve Li, Q. (2008). "Combining Empirical Experimentation AndModeling Techniques: A Design Research Approach For Personalized Mobile Advertising Applications". *Decision Support Systems*, 44(3): 710-724.

**İnternet Kaynakları**

http://www.tdk.gov.tr (erişim tarihi: 05.03.2018).

"Sokak, İnternet, Muhalefet", http://ayrintidergi.com.tr/sokak-internet-muhalefet/ (erişim tarihi: 23.05.2018).

"Deleuze: Kapitalizmin yayılmasıyla sömürü, denetim ve gözetim giderek daha da incelmekte" 26.09.2016, https://www.cafrande.org/gilles-deleuze-kapitalizmin-yayilmasiyla-somuru-denetim-ve-gozetim-giderek-daha-da-incelmekte/ (erişim tarihi: 01.05.2018).

"10 soruda 'Brexit' nedir, İngiltere AB'den ne istiyor", 17.06.2016, http://t24.com.tr/haber/10-soruda-brexit-nedir-ingiltere-abden-ne-istiyor,345754 (erişim tarihi: 25.04.2018).

https://www.tbmm.gov.tr/kanunlar/k4721.html (erişim tarihi: 01.04.2018).

http://eski.barobirlik.org.tr/yayinlar/kitaplar/OzelYasaminGizliligi.pdf (erişim tarihi: 05.03.2018).

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2709.pdf (erişim tarihi: 01.04.2018).

"IAB Türkiye 2016 Dijital Reklam Yatırımlarını Açıkladı", 05.07.2017, http://www.iabturkiye.org/iab-turkiye-2016-dijital-reklam-yatirimlarini-acikladi (erişim tarihi: 20.05.2018).

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf (erişim tarihi: 01.04.2018).

https://www.echr.coe.int/Documents/Convention_TUR.pdf (erişim tarihi: 01.04.2018).

http://www.un.org/en/universal-declaration-human-rights/ (erişim tarihi: 02.04.2018).

"Hangi şehirde kaç memur çalışıyor"? http://trend.mynet.com/hangi-sehirde-kac-memur-yasiyor-1036012 (erişim tarihi: 25.05.2018).

https://documentsddsny.un.org/doc/RESOLUTION/GEN/NR0/244/10/IMG/NR024410.pdf?OpenElement (erişim tarihi: 01.04.2018).

https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/ (erişim tarihi: 15.12.2017).

https://labs.rs/en/metadata/ (erişim tarihi: 15.12.17).

https://labs.rs/en/invisible-infrastructures-online-trackers/ (erişim tarihi: 15.12.2017).

https://labs.rs/en/invisible-infrastructures-mobile-permissions/ (erişim tarihi: 15.12.2017).

https://labs.rs/en/invisible-infrastructures-data-flow/ (erişim tarihi: 15.12.2017).

https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (erişim tarihi: 01.04.2018).

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT (erişim tarihi: 05.04.2018).

http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf (erişim tarihi: 08.04.2018).

"İşte 2017'de Google'da en çok arananlar", 01.01.2018, http://t24.com.tr/haber/iste2017degoogleda-en-cok-arananlar,525250 (erişim tarihi: 18.05.2018).

https://onlinelibrary.wiley.com/doi/full/10.1111/j.1467-923X.1972.tb02068.x (erişim tarihi: 10.04.2018).

https://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/#9c487031a77c (erişim tarihi: 10.04.2018).

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (erişim tarihi: 01.04.2018).

http://www.resmigazete.gov.tr/eskiler/2005/06/20050625-2.htm (erişim tarihi: 01.04.2018).

"Türkiye'nin emekli haritası çıkartıldı", 07.06.2017, http://www.haberturk.com/ekonomi/isyasam/haber/1544055-turkiye-nin-emekli-haritasi-cikartildi (erişim tarihi: 25.05.2018).

http://www.resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm (erişim tarihi: 10.04.2018).

www.mevzuat.gov.tr/MevzuatMetin/1.5.6698.pdf (erişim tarihi: 01.04.2018).

http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinterneteconomy.htm (erişim tarihi: 01.04.2018).

http://www.ft.com/cms/s/0/5fd7d8a8-28e5-11e2-b92c-00144feabdc0.html (erişim tarihi: 20.05.2018).

http://networkcultures.org/query/wp-content/uploads/sites/4/2014/06/1.Kylie_Jarrett.pdf (erişim tarihi: 20.05.2018).

https://www.linkedin.com/pulse/big-data-vs-metadata-whats-difference-toby-martin (erişim tarihi: 04.05.2018).

https://network23.org/kame/2014/03/19/tib-ve-metadata/ (erişim tarihi: 04.05.2018).

https://www.britannica.com/topic/Organisation-for-European-Economic-Co-operation (erişim tarihi: 27.05.2018).

https://rm.coe.int/1680078b37 (erişim tarihi: 04.04.2018).

http://www.mfa.gov.tr/avrupa-konseyi_.tr.mfa (erişim tarihi: 04.04.2018).

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (erişim tarihi: 01.04.2018).

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML (erişim tarihi: 04.04.2018).

http://www.refworld.org/pdfid/3ddcafaac.pdfß (erişim tarihi: 04.04.2018).

https://www.academia.edu/19706219/Dijital_Ku%C5%9Faklar_Dijital_Ku%C5%9Faklar%4%B1_Nas%C4%B1l_%C3%87al%C4%B1%C5%9Fmal%C4%B1?auto=download (erişim tarihi: 20.05.2018)

https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri (erişim tarihi 22.03.2018)

"Danıştay'ın 'Satılamaz' dediği sağlık verilerinin SGK tarafından 65 bin liraya satıldığı onaylandı", 18.02.2018, http://t24.com.tr/yazarlar/fusun-sarp-nebil/danistayin-satilamaz-dedigi-saglik-verilerinin-sgk-tarafindan-65-bin-liraya-satildigi-onaylandi,19165 (erişim tarihi: 25.05.2018).

http://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm (erişim tarihi: 10.04.2018).

https://www.kvkk.gov.tr/Icerik/4219/Kamuoyu-Duyurusu-Ihlal-Bildirimi (erişim tarihi: 04.05.2018).

https://www.clickz.com/personalization-vs-customization-2/82921/ (erişim tarihi: 08.05.2018).

https://www.emarketer.com/Article/Personalized-Online-Video-Ads-BoostBranding/1008655 (erişim tarihi: 13/09/2017).

https://www.ithaca.edu/ic-news/releases/online-creep:-targeted-ads-may-have-opposite-effect-of-marketers-intent-39546/#.V-tiPiiLSHv (erişim tarihi: 13.09.2017).

http://gs.statcounter.com/press/android-challenges-windows-as-worlds-most-popular-operating-system (erişim tarihi: 13/09/2017).

http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide (erişim tarihi: 13/09/2017).

https://cloud.google.com/natural-language/ (erişim tarihi: 17.05.2018).

https://webrazzi.com/2018/03/22/cambridge-analytica-hikayesi-facebook-ve-buyuk-veri (erişim tarihi 22.03.2018).

https://www.thinkwithgoogle.com/advertising-channels/mobile/the-mobile-movement/ (erişim tarihi: 17.05.2018).

https://www.gsma.com/publicpolicy/user-perspectives-on-mobile-privacy-september-2011 (erişim tarihi: 17.05.2018).

http://journals.uic.edu/ojs/index.php/fm/article/view/6154/5215 (erişim tarihi: 22.05.2017).

http://techcrunch.com/2014/07/01/an-upper-limit-for-apps-new-data-suggests-consumers-only-use-around-two-dozen-apps-per-month/ (erişim tarihi: 19.05.2018).

http://thenextweb.com/apps/2014/08/26/android-users-average-95-apps-installed-phones-according-yahoo-aviate-data/ (erişim tarihi: 19.05.2018).

https://www.nufusu.com/ilceleri/ankara-ilceleri-nufusu (erişim tarihi: 25.05.2018).

**EK 1- ANKET FORMU**

Bu anket, "İnternet Tabanlı Mobil Ortam Reklamlarında Dijital Gözetim Algısı; Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi" başlıklı yüksek lisans tez çalışması için yürütülmektedir. Anket genelinde hiçbir şekilde kimlik bilgisi istenmemektedir. Anket sonuçları hiçbir şekilde ticari amaçla kullanılmayacaktır. Katılımınız için şimdiden teşekkür ederim.

Bilgi için: Ömür TALAY
omurtalay@akdeniz.edu.tr

**1. Cinsiyetiniz:**

a) Kadın b) Erkek

**2. Yaşınız:**

……..

**3. Medeni Durumunuz:**

a) Evli b) Bekar

**4. Çalışma Durumunuz:**

a) Özel Sektörde Ücretli Çalışan b) Kamu Çalışanı c) Emekli d) Serbest Meslek

e) Ev Kadını f) Öğrenci g) Çalışmıyor h) Diğer …….

**5. Eğitim Durumunuz:**

a) Okur-Yazar b) İlköğretim c) Lise d) Önlisans e) Lisans f) Lisansüstü

**6. Mobil internet erişiminizi en çok aşağıdakilerden hangisiyle gerçekleştiriyorsunuz?**

a) Mobil Telefon b) Tablet / iPad c) Taşınabilir Bilgisayar d) Giyilebilir Teknolojiler

**7. Mobil ortamlarda en çok hangi sosyal medya platformunu kullanıyorsunuz?**

a) Facebook b) Twitter c) Instagram d) Google+ e) Diğer …….

**8. Daha önce arama yaptığınız ürünler / hizmetlerle ilgili daha sonra mobil ortamlarda reklam görüyor musunuz?**

a) Evet b) Hayır

**9. Daha önce arama yaptığınız ürünler / hizmetlerle ilgili en sık hangi mobil ortamlarda reklam görüyorsunuz?**

a) Sosyal Medya b) Arama Motoru c) Mobil Uygulama İçi d) Web (Banner)

**10. Daha önce arama yaptığınız ürünler, hizmetlerle ilgili daha sonra reklam almanız sizde herhangi bir gizlilik endişesi yaratıyor mu?**

a) Evet b) Hayır

**11. İnternette mahremiyeti korunmanın olanaklı olduğunu düşünüyor musunuz?**

a) Evet b) Hayır

| Aşağıda **mobil ortam reklamları, teknoloji kullanımı, kişisel veriler, mahremiyet ve gizlilik endişelerine** yönelik bazı ifadeler verilmiştir. Kendinize en yakın olan seçeneği işaretleyiniz. | | **Katılıyorum** | **Kararsızım** | **Katılmıyorum** | **Bilgim Yok** |
|---|---|---|---|---|---|
| **12.** | Sosyal medyada yer alan reklamlar dikkatimi çeker. | | | | |
| **13.** | Web sayfalarında yer alan banner reklamları tıklarım. | | | | |
| **14.** | Arama motorlarında yer alan reklamları tıklarım. | | | | |
| **15.** | Mobil uygulama içinde yer alan reklamları okumam hemen kapatırım. | | | | |
| **16.** | Mobil ortam reklamları rahatsız edicidir. | | | | |
| **17.** | Kişiselleştirilmiş (size özel) reklam görmek beni rahatsız eder. | | | | |
| **18.** | Bana özel kampanya veya indirim tanımlanacaksa kişisel bilgilerimi paylaşırım. | | | | |
| **19.** | Bana özel kampanya veya indirim tanımlanacaksa kişiselleştirilmiş reklam almak isterim. | | | | |
| **20.** | Kişisel bilgilerimi almak istediğim ürün ya da hizmete göre paylaşırım. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **21.** | Mobil ortamlarda bıraktığım dijital izlerin kaydedilmesi ve işlenmesiyle yaratılan reklamlar gözetlendiğim hissini yaratıyor. | | | | |
| **22.** | Kişisel bilgilerimin haberim veya iznim olmaksınız kullanılmasını doğru bulmuyorum. | | | | |
| **23.** | Kişiselleştirilmiş reklamları kapatabileceğimi biliyorum. | | | | |
| **24.** | Bilişim teknolojilerine güvenirim. | | | | |
| **25.** | Ücretsiz mobil uygulamaları kullanmak için kişisel bilgilerimi paylaşırım. | | | | |
| **26.** | Mobil uygulamalarda reklam görmemek için ücretli mobil uygulama satın alırım. | | | | |
| **27.** | Mobil uygulama yüklemeden önce veya kullanırken uygulamaların erişim izinlerine dikkat ederim. | | | | |
| **28.** | Mobil ortamlarda kredi kartı bilgilerimi kullanmaktan endişe duyuruyorum. | | | | |
| **29.** | Mobil ortamlarda (web, sosyal medya, mobil uygulama) telefon numaramı paylaşırım. | | | | |
| **30.** | Mobil uygulama ya da sosyal medya platformlarını kullanırken ikamet / iş adresi bilgilerimi paylaşırım. | | | | |
| **31.** | Mobil uygulama ya da sosyal medya platformlarını kullanırken e-posta bilgilerimi paylaşırım. | | | | |
| **32.** | Konum bilgim her zaman açıktır. | | | | |
| **33.** | Konum bilgilerimi paylaşmamın gizlilik ve mahremiyet açısından sorun teşkil etmeyeceğini düşünüyorum. | | | | |
| **34.** | Mobil uygulamaların kişisel bilgilerimi üçüncü kişilerle paylaşabileceğini biliyorum. | | | | |
| **35.** | Mobil ortam reklamlarının mahremiyetimi ihlal ettiğin düşünüyorum. | | | | |
| **36.** | Teknoloji her zaman faydalıdır. | | | | |
| **37.** | Çerezler (cookies) hakkında bilgi sahibiyim. | | | | |
| **38.** | Web sitelerinin kullanıcıları çerezler hakkında yeteri kadar bilgilendirdiğini düşünüyorum. | | | | |
| **39.** | Mobil cihazımdan çerezleri düzenli olarak temizlerim. | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **40.** | Pop-up (açılır pencere) ya da diğer mobil ortam reklamlarını engellemek için adblock gibi engelleme programları kullanırım. | | | | |
| **41** | İnternetin güvenilir olduğuna inanıyorum. | | | | |
| **42.** | Dijital haklarımı bilirim. | | | | |
| **43.** | "Kişisel Verilerin Korunması Kanunu" hakkında bilgi sahibiyim. | | | | |
| **44.** | Mahremiyetin ihlaline karşı devletin koruyuculuğuna inanıyorum. | | | | |
| **45.** | Gözetimle baş edebilirim çünkü konuya ya da uygulamalara hakimim. | | | | |

# EK 2- KVKK BİLGİ EDİNME BAŞVURUSU





**Başbakanlık**

Başbakanlık İletişim Merkezi (BİMER) Başvuru Sorgulama

Başvuru Bilgileri

| | |
|---|---|
| **Başvuru Sayısı** | 1800631067 |
| **Başvuru Zamanı** | 11/04/2018 10:45:14 |
| **Başvuru Tipi** | Bilgi Edinme |
| **Başvuru Durumu** | Başvuru Yapıldı |
| **Başvuru Metni** | KİŞİSEL VERİLERİ KORUMA KURUMU BAŞKANLIĞINA İLETİLMEK ÜZERE,<br><br>6698 sayılı Kişisel Verilerin Koruması Kanunu'nun 12. Maddesinin 3. Fıkrasında "Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır." hükmü bulunmaktadır. Veri sorumlusundan başka bir bağımsız üst denetim mekanizması bulunmakta mıdır? Kişisel Verileri Koruma Kurulu bir üst denetim mekanizmasını mı oluşturmaktadır yoksa yalnızca şikayet konu olduğunda mı gerekli denetim ve incelemeyi yapmaktadır.<br><br>Gereğini bilgilerinize arz ederim. |
| **Başvuru Yolu** | BİMER Sayfası |

Cevaplar

| Cevap Zamanı | Cevap | Kurum Birim Adı |
|---|---|---|
| 16/04/2018 15:39:44 | Sayın Başvuru Sahibi,<br>Başvurunuzda yer verilen 6698 sayılı Kişisel Verilerin Korunması Kanununun (Kanun) 12 nci maddesinin (3) numaralı fıkrası uyarınca veri sorumluları tarafından Kanun hükümlerinin uygulanmasının sağlanması amacıyla gerçekleştirilecek olan denetimlerin doğrudan veri sorumlusunun kendisi tarafından yapılması mümkün olduğu gibi dış hizmet alımı yoluyla da gerçekleştirilmesi mümkün bulunmaktadır. Bununla birlikte söz konusu denetimleri gerçekleştirilmek üzere Kişisel Verileri Koruma Kurulunca (Kurul) yetkilendirilmiş herhangi bir bağımsız denetim kuruluşu bulunmadığı gibi, Kanunda bu anlamda yetkilendirme yapılmasına ilişkin emredici herhangi bir hüküm yer almadığından bu aşamada böyle bir yetkilendirme de gündemde bulunmamaktadır.<br>Diğer taraftan, Kanunun 15 inci maddesinin (1) numaralı fıkrası hükmü uyarınca Kurul, şikayet üzerine veya ihlal iddiasını öğrenmesi durumunda resen, görev alanına giren konularda gerekli incelemeyi yapmakta olup, veri sorumlularının periyodik bazda denetime tabi tutulmaları söz konusu değildir.<br>Bilgilerinize sunulur. | KİŞİSEL VERİLERİ KORUMA KURUMU BAŞKANLIĞI |

# Ö Z G E Ç M İ Ş

| | |
|---|---|
| **Adı ve SOYADI** | Ömür TALAY |
| **Doğum Yeri - Tarihi** | Ankara – 02.10.1982 |
| **EĞİTİM DURUMU** | |
| **Mezun Olduğu Lise** | Dikmen Lisesi / Ankara |
| **Lisans Diploması** | Akdeniz Üniversitesi İletişim Fakültesi Halkla İlişkiler ve Tanıtım |
| **Tez/ Dönem Projesi Konusu** | Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi |
| **Yabancı Dil** | İngilizce |
| **İŞ DENEYİMİ** | |
| **Çalıştığı Kurumlar** | Akdeniz Üniversitesi İletişim Fakültesi |
| **E-Posta** | omurtalay@akdeniz.edu.tr |