

T.C
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
HALKLA İLİŞKİLER ve TANITIM ANABİLİM DALI
DOKTORA TEZİ

**GÖZETİM KAPİTALİZMİNDE KİŞİSEL
VERİLERİN KULLANIMI: ETİK WEB
ÇERÇEVESİNDE WEB SİTELERİ VE MOBİL
UYGULAMALAR ÜZERİNE BİR ARAŞTIRMA**

Murat ULUK
2502180121

TEZ DANIŞMANI
Doç. Dr. Nilnur TANDAÇGÜNEŞ KAHRAMAN

İstanbul - 2022

ÖZ

GÖZETİM KAPİTALİZMİNDE KİŞİSEL VERİLERİN KULLANIMI: ETİK WEB ÇERÇEVESİNDE WEB SİTELERİ VE MOBİL UYGULAMALAR ÜZERİNE BİR ARAŞTIRMA MURAT ULUK

Gözetim kapitalizmi kavramı, gözetleme ve kapitalizm olgularının birbirini beslediği ve geliştirdiği bir sistemi vurgulamaktadır. Gözetlemeyi bir iş modeli olarak tercih eden platformlar her türlü insan deneyimini toplamakta, işlemekte ve alınıp satılır ürünlere dönüştürmektedir. Gözetim kapitalizmi bir bilinmezliğe sahiptir ve sistemin işleyiş biçimi ve yarattığı sorunlar web'i etik bağlamda sorunlu hâle getirmektedir. Çalışma iki genel amaç doğrultusunda gerçekleştirilmiştir. Birinci amaç gözetim kapitalizminin izini sürerek aktörleri ve gözetleme yöntemlerini ortaya çıkarmaktır. İkinci amaç ise gözetim kapitalizmine bütüncül bir bakış açısıyla yaklaşarak sistemde yarattığı sorunları tespit etmek ve etik bir web'in tahsis edilmesi için nelerin gerekli olduğuna dair bir yol haritası çıkarmaktır. İki genel amaç doğrultusunda on araştırma sorusuna cevap aranmıştır. Çalışmada iki genel amaca ve araştırma sorularına cevap bulmaya yönelik olarak nicel ve nitel yöntemlerin bir arada kullanıldığı karma yöntem tercih edilmiştir. Nicel araştırma kapsamında incelenen web sitelerinin %79'unda, mobil uygulamaların %76'sında üçüncü taraf şirketlerin izleme yazılımları tespit edilmiştir. Web sitelerinin %92'si siteye girerken üçüncü taraf çerezleri reddetmek veya çerez kullanımını özelleştirmek için kullanıcılara hiçbir seçenek sunmamaktadır. Nitel araştırmada katılımcılara uzmanlık alanlarına göre yarı yapılandırılmış sorular sorulmuştur. Cevaplar belirli ana ve alt temalara ayrılarak gözetim kapitalizmi geniş bir perspektifle irdelenmiş ve etik bir web için nelerin olması gerektiği tartışılmıştır. Çalışma, çevrim içi gözetimin web siteleri ve mobil uygulamalar aracılığıyla pratikte nasıl gerçekleştiğini ortaya çıkarması bakımından alana katkı sağlamaktadır. Gözetim kapitalizminin derinlemesine irdelenmesinin gözetim çalışmalarına ve etik web yaklaşımının ise ilgili yerli literatüre katkı sağlaması beklenmektedir.

Anahtar Kelimeler: gözetim, gözetim kapitalizmi, etik web, kişisel veri, çerez

ABSTRACT

USAGE OF PERSONAL DATA IN SURVEILLANCE CAPITALISM: A RESEARCH ON WEBSITES AND MOBILE APPS WITHIN THE FRAME OF ETHICAL WEB

MURAT ULUK

Surveillance capitalism emphasizes a system in which surveillance and capitalism feed and develop each other. Platforms that prefer surveillance as a business model collect all kinds of human experiences, process them and convert them into commodities. Surveillance capitalism is unknowable to us and the way its operations and the problems it creates make the web problematic within the context of ethics. This study is carried out in parallel with two general purposes. The first purpose is to trace the surveillance capitalism and to reveal the surveillance actors and their surveillance methods. The second purpose is to identify the problems surveillance capitalism created in the system by approaching it from a holistic point of view and to determine a road map for what is necessary for the allocation of an ethical web. In the line with two general purposes, answers to ten questions have been sought. In the study, a mixed-method in which quantitative and qualitative methods were used together, was preferred to find answers to both two general objectives and research questions. Within the scope of quantitative research, third-party companies trackers were detected in 79% of the websites and 76% of mobile applications. 92% of websites offer users no choice to reject third-party cookies or customize the use of cookies in the first place when entering the site. In the qualitative study, participants were asked semi-structured questions according to their field of expertise. The answers are divided into specific main and sub-themes, surveillance capitalism has been examined from a broad perspective and what should be for an ethical web has been discussed. The study contributes to the communication literature in terms of revealing how online surveillance takes place in practice through websites and mobile apps. It is expected that the in-depth examination of surveillance capitalism will contribute to surveillance studies and the ethical web approach will contribute relevant works in literature.

Key Words: surveillance, surveillance capitalism, ethical web, personal data, cookie

ÖNSÖZ

Bilgi ve tecrübelerini benimle paylaşan, yol gösteren ve desteğini esirgemeyen tez danışmanım, değerli hocam Sayın Doç. Dr. Nilnur TANDAÇGÜNEŞ KAHRAMAN'a içten dileklerle teşekkür ederim. Tez izleme komitesinde olan, çalışmaya kıymetli katkılar sağlayan, tavsiye ve önerileriyle ufkumu genişleten değerli hocalarım Sayın Prof. Dr. Süleyman İRVAN ve Sayın Doç. Dr. Betül ÖNAY DOĞAN'a teşekkürlerimi sunarım.

Hayatımın her bir aşamasında bulunan ve tüm kazanımlarımın arkasında yeri olan anneme ve ablama teşekkür ederim. Tez çalışmamın başından sonuna kadar yanımda olan ve her konuda desteğini hissettiğim sevgili Hande'ye teşekkür ederim.

Nitel araştırma kapsamında görüşme yapmayı kabul eden, değerli vakitlerini bana ayıran, düşünce ve deneyimlerini benimle paylaşarak bu çalışmanın ortaya çıkmasına katkı sağlayan tüm katılımcılara teşekkür ederim.

İSTANBUL, 2022

MURAT ULUK

İÇİNDEKİLER

ÖZ.....	ii
ABSTRACT	iii
ÖNSÖZ.....	iv
ŞEKİLLER LİSTESİ.....	ix
TABLolar LİSTESİ.....	x
GRAFİKLER LİSTESİ.....	xiii
KISALTMALAR LİSTESİ.....	xiv
GİRİŞ	1

BİRİNCİ BÖLÜM

GEÇMİŞTEN GÜNÜMÜZE KAPİTALİZM, GÖZETİM ve BİLGİ TOPLUMU

1.1. Kapitalizm Olgusu: Kavramsal ve Tarihsel Bir Bakış	6
1.1.1. Ticari Kapitalizm.....	11
1.1.2. Sanayi Kapitalizmi	14
1.1.3. Bilişsel Kapitalizm	16
1.1. Gözetim Olgusu: Kuramsal ve Tarihsel Bir Bakış	20
1.2.1. Erken Modern Dönemde Gözetim Çalışmaları	25
1.2.2. Modern Dönemde Gözetim Çalışmaları.....	28
1.2.3. Postmodern Bilgisayar Destekli Gözetim Çalışmaları	33
1.2.3.1. Erken Dönem Veri Gözetimi ve Veri Tabanı Pazarlaması.....	38
1.3. Bilgi / Enformasyon Toplumu.....	43

İKİNCİ BÖLÜM

ÇEVİRİM İÇİ GÖZETİM, KULLANICILAR ve REKLAM

2.1. İnternet ve Gözetim.....	56
2.1.1. Web Siteleri ve Gözetim	59
2.1.1.1. Çerezler ve Çerez Türleri	61
2.1.1.2. İzleme Pikselleri	65
2.1.1.3. Çerezsiz Dünya ve İzleme Teknolojilerinin Geleceği	66
2.1.2. Sosyal Medya Platformları ve Gözetim	70

2.1.3. Mobil Uygulamalar ve Gözetim	74
2.1.4. Nesnelerin İnterneti (IoT) ve Gözetim	80
2.2. İletişim Teknolojilerinin Kullanıcı Emeği ve Metalaşma Süreciyle İlişkisi	84
2.2.1. Medya Çalışmalarında İzleyici Emeği ve İzleyici Metası.....	85
2.2.2. Dijital Emek ve Kullanıcı Metası: Prosumer'dan Produser'a Tüketici/Kullanıcının Dönüşümü	88
2.3. Dijital Ekonomide Veri, Platformlar ve Reklam.....	94
2.3.1. Dijital Ekonomi Kavramı	94
2.3.2. Platformlar ve Yeni Birikim Modelleri	97
2.3.3. Veri Şirketleri ve Gözetleme Araçları	99
2.3.4. Veriye Dayalı Reklamcılık ve Çevrim İçi Reklam Endüstrisi	103
2.3.4.1. Çevrim İçi Reklam ve Reklam Platformları	107
2.4. Gözetim Kapitalizmi: Gözetim Temelli Dijital Ekonomiye Eleştirel Bir Bakış 111	

ÜÇÜNCÜ BÖLÜM

DİJİTAL VERİ BAĞLAMINDA MAHREMİYET ve ETİK WEB

3.1. Büyük Veri Kavramı	119
3.2. Kişisel Veri Kavramı.....	122
3.2.1. Türlerine Göre Kişisel Veri	124
3.2.2. Kişisel Veri Ekosistemi	129
3.2.3. Kişisel Verilerin Korunması Üzerine Uluslararası Düzenlemeler	133
3.2.3.1. Dünyadaki Yasal Düzenlemeler	135
3.2.3.2. Türkiye'deki Yasal Düzenlemeler.....	139
3.3. Veri Gizliliği ve Güvenliği.....	141
3.3.1. Veri Güvenliğinin Temel İlkeleri	144
3.3.2. Veri Gizliliği ve Mahremiyet	147
3.3.3. Üçüncü Taraf İzlemeler	153
3.3.4. Gizlilik Sözleşmeleri ile Gözetimin Sıradanlaşması	156
3. 4. Etik Web Tasarım ve Geliştirme	160
3.4.1. Yönlendirici Tasarımlar: Çerez Onay Kutu Tasarımları ve Açık Rızaya Etkileri	164

DÖRDÜNCÜ BÖLÜM
GÖZETİM KAPİTALİZMİ, ÇEVİRİM İÇİ KULLANICI GÖZETİMİ ve ETİK
WEB ÜZERİNE KARMA BİR ARAŞTIRMA

4.1. Araştırmaya Giriş	172
4.1.1. Araştırmanın Amacı	173
4.1.2. Araştırmanın Önemi	175
4.1.3. Araştırma Soruları	175
4.2. Araştırmanın Yöntemi.....	177
4.2.1. Evren ve Örneklem.....	178
4.2.2. Araştırmanın Sınırlılıkları	179
4.2.3. Verilerin Toplanması, Analizi ve Çözümlemesi	180
4.3. Araştırmanın Bulguları.....	180
4.3.1. Nicel Araştırma	180
4.3.1.1. Web Sitelerindeki Üçüncü Taraf İzleyiciler	181
4.3.1.2. Mobil Uygulamalardaki Üçüncü Taraf İzleyiciler	194
4.3.1.3. Web Sitelerinin Açık Rıza Alma Biçimleri.....	204
4.3.1.4. Web Sitelerinin Çerez Politikaları ve Gizlilik Sözleşmelerinin İçerik Analizi	209
4.3.1.4.1. Çerez Politikası ve Gizlilik Sözleşmeleriyle İlgili Genel İzlenimlerin Oluşturduğu Bulgular	216
4.3.2. Nitel Araştırma	223
4.3.2.1. Gözetim Kapitalizmi.....	224
4.3.2.1.1. Sorun Gözetim Mi? Kapitalizm Mi?	224
4.3.2.1.2. Gözetim Kapitalistleri: Google, Facebook ve Diğerleri	227
4.3.2.1.3. Sahipliğin Sorgulanması: Kullandığımız Cihazlar Kimin?	232
4.3.2.2. Kişisel Veriye Dayalı Çevrim İçi Reklamcılık.....	233
4.3.2.3. Kişisel Verilerin Korunmasına Yönelik Yasal Düzenlemeler.....	239
4.3.2.3.1. KVK Kanunu Çerezleri ve Açık Rızayı Nasıl Değerlendiriyor?..	240
4.3.2.3.2. Türkiye’de Web Siteleri Yasal Açıdan Ne Derece Sorunlu?	242
4.3.2.3.3. Yasaların Uygulanabilirliği ve Cezaların Caydırıcılığı	244
4.3.2.4. Veri / Gözetim Farkındalığı ve Mahremiyet	246
4.3.2.4.1. Mahremiyet Tartışması	246
4.3.2.4.2. “İstemiyorsan Kullanmamakta Özgürsün”	249

4.3.2.4.3. “Verilerimin Toplanması Umrumda Değil”	252
4.3.2.4.4. Veri Farkındalığı / Bilinci	256
4.3.2.5. Etik Bir Web’in İnşası	259
4.3.2.5.1. Mevcut Sistemdeki Problem	260
4.3.2.5.2. Verilerin Kontrolünü Kullanıcılara Vermek	264
4.3.2.5.3. Hizmetlerin Ücretli Olması Neyi Değİştirir?	268
4.3.2.5.4. Etik Bir Web’i Nasıl Sağlarız?	271
4.4. Araştırma Bulgularının Yorumlanması ve Tartışma	278
SONUÇ	308
KAYNAKÇA	316
EKLER	345
ÖZ GEÇMİŞ	346

ŞEKİLLER LİSTESİ

Şekil 3.1: Nudging Tekniğiyle Tasarlanmış Bir Açık Rıza Onay Kutusu.....	165
Şekil 3.2: Karanlık Desen Örneği.....	166
Şekil 3.3: Karanlık Desen Örneği.....	167
Şekil 3.4: Karanlık Desen Örneği.....	167
Şekil 3.5: Hurriyet.com.tr Adresinde Rıza Onay Kutusunda Yer Alan Seçenekler Aktif Olarak Kullanıcıya Sunulması.....	168
Şekil 3.6: Web Sitelerinin Çerez Onay Kutularına Ait Farklı Tasarım ve Rıza Talep Örnekleri.....	169
Şekil 3.7: Yasal ve Etik Zemine Uygun Olarak Tasarlanmış Bir Açık Rıza Onay Kutusu Tasarımı.....	171

TABLÖLAR LİSTESİ

Tablo 1.1: Modernitenin Kurumsal Boyutları.....	10
Tablo 1.2: Gözetim Kuramlarının Temelleri.....	24
Tablo 1.3: Gözetimin Boyutları	35
Tablo 1.4: Postmodern Dönemdeki Başlıca Gözetim Çalışmaları.....	38
Tablo 1.5: Enformasyon Toplumunun Temel Kategorileri, Ölçülebilirliği ve Metaforları.....	46
Tablo 1.6: Bilgiye Dayalı Toplumun Temel Birimleri	47
Tablo 1.7: Daniel Bell'e Göre Enformasyon Toplumunun Boyutları.....	49
Tablo 2.1: İnternet Gözetiminin Boyutları ve Nitelikleri.....	58
Tablo 2.2: Hurriyet.com.tr'yi Ziyaret Eden Bir Kullanıcının Sitedeki Gezinimlerini Takip Eden Üçüncü Taraf Şirketler	60
Tablo 2.3: RV AppStudios Tarafından Geliştirilen El Feneri (Flashlight - Torch LED Light) Mobil Uygulamasında Yer Alan İzleme Kodları ve Uygulamanın Cihazdan Talep Ettiği Erişim İzinleri.	78
Tablo 2.4: Literatür Taraması Sonucu Ortaya Çıkan Dijital Ekonomi Tablosunun Özeti.	96
Tablo 2.5: Çevrim İçi Davranışsal Reklam Süreci.....	106
Tablo 3.1: Kişisel Veri Kategorileri.....	127
Tablo 3.2: Information Accountability Foundation, Dünya Ekonomik Forumu	127
Tablo 3.3: Veri Oluşumundan Veri Tüketimine Kişisel Veri Ekosistemi	130
Tablo 3.4: Acxiom ve Oracle'ın Sahip Olduğu Tüketicilere İlişkin Veri Örnekleri	133
Tablo 4.1: Sitelerde Tespit Edilen Çerezlerin Tür ve Amaçlarına Göre Dağılımı..	181
Tablo 4.2: En Çok Çerez Yerleştiren 15 Şirket ve Çerez Sayıları.	182
Tablo 4.3: 48 Site ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışveriş Ağı. .	183
Tablo 4.4: 16 Haber Sitesi ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışveriş Ağı.....	184

Tablo 4.5: 6 E-Ticaret Sitesi ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışveriş Ağı.	185
Tablo 4.6: 100 ve Üzeri Üçüncü Taraf Çerez Yerleştiren 11 Web Sitesi.	186
Tablo 4.7: 48 Web Sitesinde Bulunan Google Reklam Ürünlerine Ait Çerezlerin Sayısı ve Alan Adı Uzantıları.	187
Tablo 4.8: 48 Web Sitesinde Bulunan Diğer Google Çerezlerine Ait Alan Adı Uzantıları.	187
Tablo 4.9: 48 Web Sitesinde Bulunan Facebook Çerezlerine Ait Alan Adı Uzantıları.	188
Tablo 4.10: 72 Mobil Uygulamadaki Tespit Edilen İzleyicilerin Kullanım Amaçları.	195
Tablo 4.11: 72 Mobil Uygulamada En Çok Yer Verilen Üçüncü Taraf İzleyiciler.	196
Tablo 4.12: En Çok Üçüncü Taraf İzleyiciye Sahip 15 Mobil Uygulama.	198
Tablo 4.13: 72 Mobil Uygulamada Tespit Edilen Üçüncü Taraf İzleyicilerin Ağ Haritası.	200
Tablo 4.14: En Çok Üçüncü Taraf İzleyiciye Sahip Uygulamaların Kimlere Veri Sağladığını Gösteren Ağ Haritası.	201
Tablo 4.15: Üçüncü Taraf Reklam İzleyicilere Sahip Uygulamalar ile Veri Paylaştığı Reklam Şirketlerinin Ağ Haritası.	202
Tablo 4.16: Büyük Teknoloji Şirketlerinin Üçüncü Taraf Olarak Uygulamalarda Hangi Amaçlar ve Ürünler Yer Aldığını Gösteren Diyagram.	203
Tablo 4.17: 48 Sitenin Çerez Kullanım Bildirimi ve Açık Rıza Taleplerinin Türleri.	204
Tablo 4.18: Hangi Verilerin Toplandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.	210
Tablo 4.19: Verilerin Hangi Amaçla Toplandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.	211
Tablo 4.20: Verilerin Nasıl İşlendiği Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.	211
Tablo 4.21: Verilerin Hangi Üçüncü Taraf Şirket veya Sektörlerle Paylaşıldığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.	212

Tablo 4.22: Çerezlerin Ne Kadar Süreyle Saklandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.....	213
Tablo 4.23: Çerezlerin veya Kişisel Verilerin Silinmesi İçin Bir İletişim Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.....	214
Tablo 4.24: Sitesinde Üçüncü Tarafların Sözleşmelerine Sorumluluk Verme Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.....	215
Tablo 4.25: Görüşmecilerin Listesi ve Meslekleri.....	223
Tablo 4.26: Nitel Araştırma Sonucu Çıkarılan Ana ve Alt Temalar.....	224



GRAFİKLER LİSTESİ

Grafik 3.1: İhtiyaçların Etik Hiyerarşisi	161
Grafik 4.1: Seçeneksiz Çerez Bildirimi Örneği.	205
Grafik 4.2: Onaylama Bildirim Mantığı ve “Okudum” Butonu (Ntv.Com.Tr).....	205
Grafik 4.3: Mynet.com Adresini Türkiye’den Ziyaret Eden Bir Kullanıcının Karşılaştığı Onaylama Bildirim Kutusu.....	206
Grafik 4.4: Mynet.com Adresini Yurt Dışından Ziyaret Eden Bir Kullanıcının Karşılaştığı Onaylama Bildirim Kutuları.	206
Grafik 4.5: Çerez Kategorilerinin Hazır Seçili Olarak Sunulmasına Bir Örnek. ...	207
Grafik 4.6: Çerez Kategorilerinin Listelenmesi.....	208
Grafik 4.7: Çerez Kategorilerinin Pasif Olarak Sunulmasına Bir Örnek.	209
Grafik 4.8: Haberturk.com’un Çerez Politikasında Yer Alan Üçüncü Taraf Şirketlerin Listesi.	212
Grafik 4.9: Doviz.com’un Çerez Politikasında Yer Alan Çerez Listesi.	213
Grafik 4.10: EDAA (Avrupa İnteraktif Dijital Reklam Birliği) Tarafından Oluşturulan Youronlinechoices Web Sitesinde Yer Alan Şirketler ve Kullanıcıya Sunduğu Seçenekler.	215
Grafik 4.11: Eksisozluk.com’un Kullanıcıya Sunduğu Çerez Bildirim Kutusu.....	219
Grafik 4.12: Ntv.com.tr’nin Çerez Politikasında Yer Alan Çerezlere İlişkin Detaylı Bilgilerden Bir Kısmı.....	221

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AWS	: Amazon Web Services
BM	: Birleşmiş Milletler
CalOPPA	: California Online Privacy Protection Act
CNAME	: A Canonical Name (Kanonik Ad)
CNIL	: Commission Nationale Informatique & Libertés (Fransa Veri Koruma Kurumu)
COPPA	: Children's Online Privacy Protection Rule (Çocukların Çevrim İçi Gizliliğini Koruma Yasası)
CPC	: Cost Per Click (Tıklama Başına Maliyet)
CPM	: Cost Per Mile (Bin Başına Maliyet)
DSP	: Demand Side Platform (Talep Yönlü Platform)
EDRi	: European Digital Rights (Avrupa Dijital Haklar Ağı)
FCRA	: Fair Credit Reporting Act (Adil Kredi Raporlama Kanunu)
FLoC	: Federated Learning of Cohorts
FOIA	: Freedom of Information Act (Bilgi Edinme Özgürlüğü Yasası)
GDPR	: General Data Protection Regulation (Genel Veri Koruma Yönetmeliği)
GLBA	: The Gramm-Leach-Bliley Act (Gramm Leach Bliley Kanunu)
IAB	: Interactive Advertising Bureau
IOT	: Internet of Things (Nesnelerin İnterneti)
KTB	: Kişisel Tanımlanabilir Bilgiler
KVKK	: Kişisel Verilerin Korunması Kanunu
MÖ	: Millattan Önce

OECD	:Organisation for Economic Co-operation and Development (Ekonomik Kalkınma ve İşbirliği Örgütü)
SDK	: Software Development Kit (Yazılım Geliştirme Kiti)
SSP	: Supply Side Platform (Arz Yönlü Platform)
UNCTAD	: United Nations Conference on Trade and Development (Birleşmiş Milletler Ticaret ve Kalkınma Konferansı)
URL	: Uniform Resource Locator (Birörnek Kaynak Konumlayıcı)



GİRİŞ

Gözetim, bilgi birikimine; kapitalizm, servet artışına vurgu yapmaktadır. Gözetim ve kapitalizm kavramları tarih boyunca hiçbir zaman şimdiki kadar içiçe geçmemiştir. Bugünün baskın dijital kapitalizm anlayışı gözetlemeye dayalı gerçekleşmektedir. Gözetleme faaliyetleri ile milyarlarca insan hakkında veri toplanmakta, bu verilerin işlenmesiyle oluşturulan ürünlerin satışıyla servet artışı yaşanmaktadır. Şirketler, her yıl artan gelirleri ile gözetlemeye daha fazla bütçe ayırarak gözetleme araçlarını geliştirmekte ve bu durum daha da zenginleşmeye yol açmaktadır. Birbirini destekleyen bu döngü ile gözetim her yere yayılarak daha da derinleşmektedir. Gözetim kapitalizmi, insan davranışlarını ve iletişim faaliyetlerini hammadde olarak görmekte ve el koymaktadır. Topladıkları hammaddeleri makine öğrenimi yoluyla insanların geleceğini öngören ürünler hâline getirmekte ve yeni nesil piyasalarda alınıp satılır metalar olarak satışa sunmaktadır (Zuboff, 2019: 8).

Gözetime dayalı iş modelleri web teknolojilerinin, platformların ve şirketlerin hâkim gelir yöntemlerinden birisi hâline gelmiştir. Sosyal ağlar, teknoloji şirketleri, web siteleri, mobil uygulamalar, reklam ve analitik şirketleri gibi çevrim içi platformlara sahip tüm sistemler gerek birinci taraf olarak gerekse üçüncü taraf olarak kullanıcıları sürekli olarak gözetleme altında tutmaktadır. Web'e erişen kişi sayısı ve web'te geçirilen süre dikkate alındığında milyarlarca insanın farklı platformlardaki her bir çevrim içi hareketi daha önce hiç duyulmamış yüzlerce şirket tarafından izlenmektedir. Toplanan veriler onların uzak sunucularında saklanmakta, onların algoritmalarıyla işlenmekte ve onlar için hizmet etmektedir. Bu sarmal gözetim kapitalizminin bilinmezlik üzerine inşa edilmesinden kaynaklanmaktadır.

Kişisel verilerin korunmasına yönelik dünyada ve Türkiye'de yasal düzenlemeler geliştirilmiştir. Bu düzenlemeler bir yanıyla çevrim içi gözetleme faaliyetlerinin kullanım amacı kapsamında, açık rıza alarak ve şeffaf bir şekilde yürütülmesi gerekliliğini ortaya koymaktadır. Diğer yandan birçok web sitesi ve uygulama, gelir modelini reklama göre inşa ettiği ve reklam şirketleriyle işbirliği yaptığı için kullanıcı verileri üçüncü taraf şirketlere aktarılmaktadır. Dolayısıyla

çevrim içi platformların bu yasal zorunluluğu nasıl karşıladığına yönelik bir bilgi eksikliği söz konusudur.

Gözetim kapitalizmi koşulları ve mevcut web teknolojisinin insana yaklaşımı, web'in ortaya çıkış amaçlarıyla çelişmektedir. Web, tüm insanlar için şeffaf, erişilebilir, mahremiyete önem veren, ifade özgürlüğünü savunan, verilerin sahipliği, kontrolü ve yönetiminin kullanıcıda olduğu ve en önemlisi tekelleşmenin olmadığı bir ideal üzerine inşa edilmiştir. Web bugün geldiği noktada ise insan haklarının zedelendiği, tekelleşmiş şirketlerin çoğunluğu gözetlediği, haklarında çıkarımlarda bulunduğu, belirli azınlık grupların çıkarına çalışan, mahremiyetin ortadan kalktığı, manipülasyonun normalleştiği merkezî bir sistem hâline dönüşmüştür. Bu koşullar altında ve bu koşullara rağmen etik bir web'in inşası tüm web kullanıcılarının haklarını korumak ve onlara web'in kuruluş amacına uygun bir web deneyimi sağlamak için gereklidir.

Çalışma, yukarıda değinilenleri göz önünde bulundurarak iki temel amaç taşımaktadır. Bunların ilki gözetim kapitalizminin izini sürmektir. Buna bağlı olarak ilk amaç, kullanıcıları gözetleyenlerin kimler olduklarını ortaya çıkarmak ve nasıl gözetlediklerini tespit etmektir. Ayrıca, gözetimin gerçekleştiği platformların gözetlemeye ilişkin yasal düzenlemelere bağlı kalıp kalmadıkları da ortaya konulmaktadır. İkinci temel amaç, gözetimin izinden elde edilen bulguları da hesaba katarak gözetim kapitalizminin yarattığı sorunları bütüncül bir bakış açısıyla ele almak ve etik bir web'in inşasını sağlamadaki gerekli unsurları ortaya çıkarmaktır.

Gözetleme üzerine yapılan çalışmalar genellikle devlet gözetimi, sosyal medya gözetimi, gözetim toplumu, gözetim farkındalığı, elektronik gözetim, bireyin bireyi gözetlemesi (dikizleme), denetim ve disiplin gibi kavramlar üzerine yoğunlaşmaktadır. Bu çalışma, teknoloji şirketlerinin gözetiminin yaygınlığını ve nereye kadar erişebildiğini ortaya çıkarması bakımından gözetim çalışmaları alanına katkı sağlamaktadır. Buna ek olarak etik web üzerine yapılan tartışmalar ve geliştirilen yaklaşımların, hem akademik hem de sosyal alanda etik web çalışmalarının yaygınlaşmasına ve yeni tartışmaların yürütülmesine yardımcı olması beklenmektedir.

Çalışmada iki genel amaç doğrultusunda, içerisindeki alt amaçları da içine alarak, aşağıdaki araştırma sorularına cevap aranmıştır:

- 1) Hangi platform ve şirketler, web siteleri ve mobil uygulamalar aracılığıyla veri toplamaktadır?
- 2) Hangi tür gözetleme araçları ve teknolojiler hangi amaçlara dayalı olarak kullanıcı verilerini toplamaktadır?
- 3) Web siteleri, üçüncü tarafların izleme teknolojilerini kullanması için kullanıcılardan nasıl izin almaktadır?
- 4) Web sitelerinin çerez politikaları ve gizlilik sözleşmeleri kullanıcı faaliyetlerinin çevrim içi gözetlenmesini nasıl ele almaktadır?
- 5) Teknoloji şirketleri ve gözetleme faaliyetleri arasında nasıl bir ilişki söz konusudur?
- 6) Kişisel verilerin korunmasına ilişkin yasal düzenlemeler, kullanıcı gözetimini azaltmaya yönelik nasıl bir katkı sunmaktadır?
- 7) Çevrim içi reklam endüstrisinde gözetim faaliyetleri nasıl ele alınmaktadır?
- 8) Gözetim ve mahremiyet arasındaki ilişki kişisel verilerin korunması ve kişisel veri farkındalığının artmasıyla nasıl bir değişime uğramaktadır?
- 9) Gözetim kapitalizmini etik hâle getirmek ne derece mümkündür? Sistemdeki değişiklikler, gözetim kapitalizminin olumsuz etkilediği alanların azaltılmasında bir rol oynayabilir mi?
- 10) Etik web'in oluşumunda hangi yolların izlenmesi gerekmektedir?

Çalışmanın amaçları doğrultusunda ve araştırma sorularının cevaplarını bulmak için hem nicel hem de nitel yöntemin bir arada olduğu karma araştırma yöntemi tercih edilmiştir. Nicel araştırma Ekim ve Kasım 2021 tarihlerinde gerçekleşmiş olup, nitel araştırma Aralık 2021'de yürütülmüştür.

Çalışmanın ilk ayağını nicel araştırma oluşturmaktadır. Özellikle ilk dört araştırma sorusunun cevabını bulmak için Türkiye'nin en çok ziyaret edilen ilk 50 web sitesi ve en çok indirilen ilk 50 mobil uygulaması incelenmiştir. Bu platformlar aracılığıyla üçüncü taraf izleme teknolojileri, bu teknolojilerin sahipleri, şirketlerin platformlar arası gözetleme ilişkisi ve izlemelerin hangi amaçlarla gerçekleştiği gibi bilgiler ortaya konulmuştur. Buna ek olarak 50 web sitesinin üçüncü taraflara veri aktarırken kullanıcılardan açık rıza alıp almadığı araştırılmış; veri politikaları ile gizlilik sözleşmeleri içerik analizi yöntemiyle incelenmiştir. Nicel araştırma, söz konusu örneklem dâhilinde gözetim kapitalizmi aktörlerinin kimler olduklarını ve platformlardaki yaygınlığını tespit etmek üzere gerçekleşmekte; ayrıca veri alışverişinin yasal düzenlemelere ne kadar uygun olduğunu irdelemektedir.

Karma yöntemin ikinci ayağını nitel araştırma oluşturmaktadır. Yoruma ihtiyaç duyulan nicel araştırma bulgularını tartışmak ve diğer araştırma sorularının cevaplarını bulmak için teknoloji, iletişim, reklam, tasarım ve hukuk alanında uzman kişilerle yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Her görüşmeciye hem genel hem de uzmanlık alanına göre özelleştirilmiş sorular sorulmuştur. Görüşmelerin bulguları belirli ana temalara ve buna bağlı olarak oluşturulan alt temalara ayrılarak paylaşılmıştır.

Araştırma sorularına, nicel ve nitel araştırma bulgularının yorumlanması ve tartışılması ile cevap aranmıştır. Araştırma bulgularının yorumlanması ve tartışılması başlığında her bir araştırma sorusu paylaşılarak ona ait bulgulara yer verilmiş ve tartışmalar yürütülmüştür.

Tez çalışmasının literatürü gözetim, kapitalizm, mahremiyet, web, dijital ekonomi, reklam, büyük veri ve kişisel verilerin korunması gibi başlıklar hakkında yerli ve yabancı kaynakların taranması, incelenmesi ve güncel çalışmaların bulgularına yer verilmesiyle hazırlanmıştır. Bu bağlamda tez dört bölümden oluşmaktadır. İlk bölümde kapitalizm ve kapitalizmin tarihsel sürecine; gözetim olgusu ve günümüze kadarki gelişim ve değişimine ve bilgi / enformasyon toplumuna dair egemen ve eleştirel bakış açılarına yer verilmiştir.

İkinci bölüm daha yakın dönemi ele alarak, İnternette gözetleme unsurlarının ortaya çıkışı, platformların kullanıcıları gözetlemesi, kullanıcı emeğinin ve iletişimsel faaliyetlerinin metalaşması, dijital ekonomide verinin önemi ve sahipliği, kişisel veriye dayalı reklamcılık endüstrisi, reklam şirketleri ve gözetim kapitalizmi konularını işlemektedir.

Üçüncü bölümde ise büyük veri ve kişisel veri ekosisteminin çalışma prensiplerine, kişisel verilerin korunmasına yönelik ulusal ve uluslararası yasal düzenlemelere, veri gizliliği ve mahremiyet üzerine yaklaşımlara, üçüncü taraf şirketlerin izleme yöntemlerine, gizlilik sözleşmeleri üzerine çalışmalara, manipülatif tasarım üretimine ve etik web kavramına değinilmiştir.

Dördüncü bölümde tez çerçevesinde çevrim içi kullanıcı gözetimi ve etik web üzerine karma bir araştırma gerçekleştirilmiştir. Bu bölümde araştırmanın konusu, yöntemi, bulguları ve bulguların yorumlanması ve tartışılması başlıkları yer almaktadır.

BİRİNCİ BÖLÜM

GEÇMİŞTEN GÜNÜMÜZE KAPİTALİZM, GÖZETİM ve BİLGİ TOPLUMU

1.1. Kapitalizm Olgusu: Kavramsal ve Tarihsel Bir Bakış

Kapitalizm, özel mülkiyete ve ücretli emeğe dayalı, sermaye sahibinin daha çok sermaye biriktirme amacı taşıdığı ekonomik bir sistemdir. Kapitalizm, “kapital” sözcüğünden türemiştir. Kapitalizmde anahtar bir yeri olan sermaye ise *birikmiş zenginlik* şeklinde ifade edilmektedir (Wallerstein, 2016: 15). Giddens ve Sutton kapitalizmi “*ticari büyüme ve yatırım odaklı kâr üretimiyle, piyasa mübadelesine dayanan batı kökenli ekonomik sistem*” olarak tanımlamaktadır (2018: 142). Dobb’a göre kapitalizm “... sermayenin, ağırlıklı olarak özel ya da kişisel mülkiyette olması” demektir (1990: 12). Zira kapitalizm öncesi toplumlarda üretim araçları sermaye sahiplerine değil, malı üreten zanaatkârlara ait olan işyeri, kullanılan makineler ve hammaddelelerden oluşmuştur (Fulcher, 2004: 14). Marx kapitalizmi “*Kapitalist üretimin itici gücü ve belirleyici amacı, mümkün olduğu kadar sermayenin kendini değerlendirmesi, yani mümkün olduğunca artı değer üretmesi, dolayısıyla emek gücünün kapitalist tarafından mümkün olduğu kadar çok sömürülmesidir*” şeklinde nitelemektedir (Fuchs, 2014: 141). Bu nitelemeyle paralel olarak kapitalizmi yalnızca meta üretim sistemi olarak değil, işgücünün kendisinin de meta olarak alışveriş nesnesi olduğu bir sistem olarak görmektedir (Güçlü, 2019: 208). Wallerstein (2016: 39), kapitalist sistemin daha çok sermaye üretmek için sermaye ürettiğini belirtmektedir. Bu bağlamda sınırsız sermaye birikimini “*kapitalist uygarlığın var olma nedeni ve temel etkinliği*” olarak ifade etmektedir (2016: 122). Kerov (2014: 9) kapitalizmi tanımlarken onun bir yandan mülkten ya tamamen ya da neredeyse yoksun kitleleri

“ücretlilere¹” dönüştürdüğünü, diğer yandan da üretim araçlarının az sayıdaki zümrede bulunduğu bir toplum düzeni olduğunu vurgulamaktadır.

Kapitalizm, meta üretim sistemidir ve her meta “kullanım değeri” ve “değişim değeri”ne sahiptir. Kullanım değeri, tüketim sürecinde ortaya çıkan değerdir, sağladığı faydadır. Bir ürünü meta olarak tanımlamak için mutlaka bir kullanım değeri olması gerekir. Değişim değeri “*bir ürünün başka ürünlerle değiştirilmek için arz edildiğinde sahip olduğu değer*” olarak ifade edilir. Değişim değeri, ekonomik ilişkiyi gerektirir ve malların mübadele edildiği piyasadan ayrı olarak düşünülemez (Giddens, 2010: 91-92).

Kapitalist adı verilen kişi, kurum ve kuruluşlar sermayeyi elinde tutan ve durmaksızın daha çok sermaye birikimini amaçlayan ve hedefe odaklı gruplardır (Wallerstein, 2016: 16). Buna bağlı olarak kapitalist sistem varlığını sürdürmek için daima sermaye birikimine ihtiyaç duymaktadır. Sermaye ise paraya dönüştürülebilen ödenmemiş emeğin işçilerden çıkarılmasıyla arttırılabilmektedir (Fuchs, 2014: 141). Kapitalizmde değer, metada nesneleşerek maddi bir form kazanan soyut insan emegidir (Harvey, 2012: 33). İşçilerin “*emek-gücüne eşit bir değer yaratması için gerekenden daha uzun bir süre çalışmış olması*” kapitalistin artı-değer elde etmesindeki başlıca unsurdur (Kerov, 2014: 16). Diğer bir ifadeyle, işçinin geçimini sağlamaya yetecek değerden daha fazlasını üretmesiyle “artı-değer” oluşur. Sözü edilen değer, kapitalist tarafından el konudan artı üretimdir. Bu noktada artı değer, kârın ana kaynağıdır, somut çıktısıdır (Giddens, 2010: 96). İşçiye ödeme yapılmadan el konulan bu artı-değer, kapitalist sömürünün temelini oluşturmaktadır. Marx da kapitalizmi tanımlayan belirleyici özelliğin “*işçi sınıfını sömüren üretim sermayesi sahipleri*” olduğunu gösterme çabası içinde olmuştur. Sınıflı toplumun temeli olarak görülen “artık” oluşumu, sömürgeye dayalı gelişim ve kapitalist büyümeyle gerçekleşmiştir (Turner, 2014: 347).

¹ Ücret, “*işçi tarafından satılan emek için işveren tarafından ödenen fiyattır.*” (Fulcher, 2004: 14).

Kapitalizmde işi yapmaya zorlanacak veya aklı çelinerek işin yapılması sağlanacak bir grup “işçi” gerekmektedir. İşçilerin bulunması ve malların üretilmesiyle söz konusu malların sahada pazarlanması ihtiyacı doğmaktadır. Bu ihtiyacın karşılanması için dağıtım ağına ve malları almaya istekli ve aynı zamanda alım gücüne de sahip olan insanlar gerekmektedir. Malların, satıcıya olan maliyetinden daha yüksek bedelle satılması ve aradaki farkın satıcının kendi geçimini idame ettirmek için ihtiyaç duyduğundan daha fazlası olması, yani kâr sağlaması lazımdır. Kâr sağlayan grup, uygun zaman ve koşullarda yeni yatırımlar yaparak bu döngüyü yenileyip daha fazla kâr elde etmenin yollarını bulabilmektedir (Wallerstein, 2016: 17).

Kapitalist toplumlarda proleterler² ve burjuvalar birbirleriyle sıkı bir bağ içindedir. İşçi, kapitalistin yanında çalışmadan hayatını idame ettiremez; kapitalist, işçi olmadan ve onu sömürmeden zenginleşemez. Birbiriyle bağlı bu iki olgu aynı zamanda birbirinin de karşıtıdır. Bu bağlılık ve karşıtlık, kapitalist toplumun en önemli toplumsal çelişkisidir (Kerov, 2014: 21).

İşçiler özgürdür, kimse için çalışmak zorunda değildir. Fakat üretim araçlarına sahip olmadıklarından kendisinin ve ailesinin geçimini sağlamak için çalışmak zorundadır. En başta işçi, iş boyunca sarf ettiği emeği ve harcadığı enerjiyi geri yerine getirmek için gıda, giyim ve barınma gibi temel ihtiyaçlarını karşılamak zorundadır (Giddens, 2010: 95). Kerov, işçi ve kapitalist arasındaki ilişkiyi şu sözlerle açıklamaktadır:

“İşçi, işçi olarak kapitalistin yanında çalışmak zorundadır, çünkü yiyeceği yoktur; kapitalist, yani üretim araçlarının sahibi ise, üretime başlamak için işçiye muhtaçtır. İşçi, her insan gibi, emek-gücüne, yani çalışma yeteneğine sahiptir. Bütün üretim biçiminin temel ögesi olan emek-gücü de kapitalist toplumda bir meta hâline gelir; meta üretimi genelleşir.” (Kerov, 2014: 12)

Fulcher (2004: 15), işçinin ücretli emeğinin hem özgür olduğunu hem de olmadığını belirtmektedir. Ona göre sahipleri tarafından çalışmaya zorlanan kölelerin

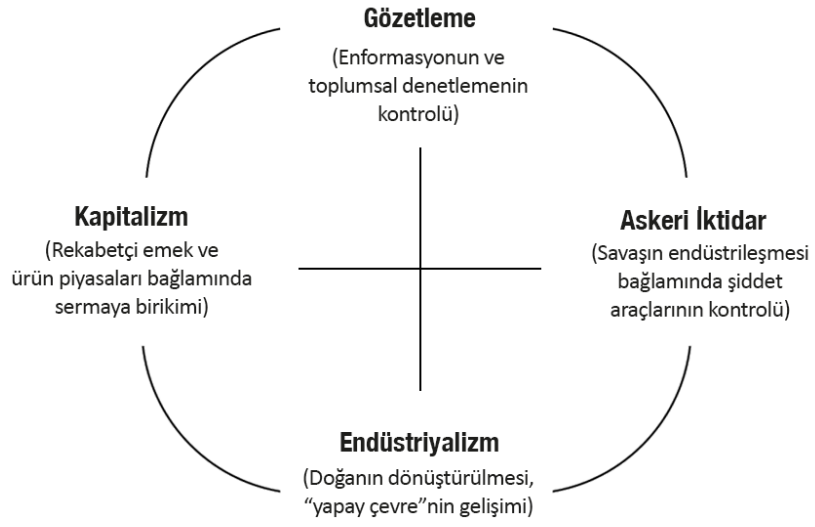
² Proleter, emeğini satan insanlardır (Wallerstein, 2016: 24).

veya feodal toplumlarda efendilerinin topraklarına bağı olan serflerin aksine, ücreti karşılığında emeğini satan kişiler nerede ve kimin için çalışıp çalışmama özgürlüğüne sahiptir. Fakat tüm bunlara rağmen yanıltıcı bir durum söz konusudur; kapitalist toplumlarda ücretli iş olmadan hayatta kalmak neredeyse imkânsızdır. Ayrıca iş ve işveren seçenekleri de sınırlıdır. Emeğini satan işçiler de köle ve serfler gibi çeşitli disiplin uygulamalarıyla sıkı denetim altına çalışırlar. Marx'ın ifadesiyle ücretli işçiler “ücretli köleler” hâline dönüşmüştür.

İnsanın fiziksel enerji harcamasını gerektiren emek gücü piyasada alınıp satılan bir metadır (Giddens, 2010: 95). Tüm metaların ortak özelliği üretimlerinde cisimleşen insan emeğinin taşıyıcıları olmalarıdır; dolayısıyla metalara insan emeğinin ürünleri denilebilir (Harvey, 2012: 32). Bu metalar, sermaye sahiplerinin kârlılığını garanti altına almada kilit bir rol oynar. Öteki taraftan bakıldığında *kâr sağlamak*, işçinin kendi emeğinin sahipliğine ve emeğinin çıktılara, yani ürünlerine, yabancılaştıran bir sömürüden ibarettir (Turner, 2014: 348). Marx, işçinin kendi ürününe yabancılaşmasını temel zeminde şu boyutlarıyla tartışır: (1) Piyasa ekonomisinin ana prensibi malların mübadele amacıyla üretilmesidir ve kapitalist üretim sürecinde malların değişimi ve dağılımı serbest piyasanın kontrolü altındadır. Piyasada alınıp – satılır bir meta olan işçi ise ürettiği mal üzerinde söz sahibi değildir. Piyasa, kapitalistin çıkarlarını işçinin çıkarların aksi yönünde arttıracak biçimde işlemeye devam eder. (2) İşçi yaptığı işe yabancılaşır; zira yapılan iş, bilişsel ve zihinsel bir doyum sağlayan özgür bir emekle değil, dış koşulların dayatmasıyla gerçekleşen bir emekle gerçekleşir. İş, bir amacın aracı olmaktan çıkarak bizzat bir amaç hâline dönüşmüştür. (3) Emeğin yabancılaşması toplumsal sonuçlar doğurur; toplumsal ilişkiler piyasa güçlerine indirgenme eğilimi gösterir. (4) Yabancılaşmış emek insanın doğayla ilişkisini farklı bir bağlama taşır; insanın üretici etkinlikleri doğaya hâkim olmak yerine doğaya ayak uydurmaya indirgenir (Giddens, 2010: 42-44).

Kapitalizm; endüstriyalizm, gözetim ve askeri iktidar ile birlikte modernitenin dört kurumsal boyutundan birisidir (Giddens, 1994: 54 - 60). Kapitalizm, “*özel sermaye mülkiyeti ile mülksüz ücretli emek arasındaki ilişki*” temeline odaklanan meta üretimi sistemidir. Söz konusu ikili ilişki, sınıf sistemini de oluşturan ana bileşendir.

Endüstriyalizm, diğer ifadeyle sanayileşme, makine gibi cansız güç kaynaklarının mal üretiminde söz sahibi olmasını kapsar. Endüstriyalizm, yalnızca büyük fabrika ve iş alanlarını değil, hizmet, ulaşım, iletişim ve gündelik ev hayatını da etkiler. Gözetim, gözetlenen toplulukların siyasal zemindeki aktivitelerini kontrolü ve denetimini içerir. Denetim doğrudan olabildiği gibi bir o kadar da dolaylıdır ve enformasyon kontrolüne dayalıdır. Dördüncü ve son kurumsal boyut ise askeri güçtür. Askeri güç, savaşın endüstriyel hâle gelmesiyle savaşın niteliğindeki değişimini imler.



Tablo 1.1: Modernitenin Kurumsal Boyutları (Giddens, 1994).

Birbiriyle bağlantılı dört boyut arasındaki ilişki tablodaki çizgileri takip ederek ortaya konulabilir. Giddens bu noktada şu örneği verir; gözetim, fabrika ve iş yerlerinde yönetimin gücünü sağlamlaştırabilir ve endüstriyalizmin gelişimine katkı sağlayabilir. Böylece, farklı modern kurumların birbirleriyle bağlı ve etkileşime hazır bir ağ içinde oldukları ifade edilebilir.

Robinson (2004), kapitalizmi dört döneme ayırmaktadır. Ona göre kapitalizm Kolomb'un Amerika'yı keşfiyle ilk olarak Feodal Avrupa'da ortaya çıkmaya başlamıştır. Kapitalizmin ikinci dönemi sanayi devrimiyle ortaya çıkan sanayi kapitalizmi, üçüncü dönem küreselleşmeyle ve serbest piyasa ekonomisinin oluşmasıyla yaygınlaşan kurumsal kapitalizmdir. Bilgi ve iletişim teknolojilerinin öne çıktığı günümüz enformasyon çağını ise kapitalizmin dördüncü dönemi olarak kabul

etmektedir. Her bir dönemin özünde, sermaye-emek ve kapitalist üretim ilişkileri şeklinde adlandırılan belirli toplumsal etkileşim biçimleri aracılığıyla gerçekleşen üretim vardır (Gray, 2004). Bir başka yazar Moulier–Boutang (2012: 49), “*Cognitive Capitalism*” adlı eserinde kapitalizmi üç temel başlıkta incelemektedir. Birincisi, tüccar ve finans birikim mekanizmalarının hegemonyasına dayanan ve 16. yy’de başlayıp ile 17. yy’nin sonuna kadar devam eden ticari kapitalizmdir. İkincisi, fiziksel sermaye birikimine ve “Manchester tarzı”³ fabrikaların itici güç olduğu tek tip metaların seri üretimine dayalı sanayi kapitalizmidir. Üçüncüsü, maddi olmayan sermaye birikimi ve bilgi ve enformasyon ekonomisinin öncülüğünde kurulan bilişsel kapitalizmdir. Çalışmada kapitalizmin tarihsel seyri, Moulier-Boutang’ın bu üç temel kapitalizm kategorilendirmesiyle incelenmekte olup ilerleyen bölümlerde Zuboff’un (2019) bugün bilgi kapitalizminin baskın biçimi olarak nitelediği ve insan deneyimlerini öngörü ürünlerine dönüştürerek artı değer yaratan gözetim kapitalizmi sistemi detaylıca ele alınmaktadır.

1.1.1. Ticari Kapitalizm

Sermaye, “*daha fazla para kazanmak için yatırım yapılan para*” anlamı taşımaktadır. Kolaylıkla paraya dönüşebilecek maddi bir varlık da, yatırım için hazır bulunan nakit para da sermaye olabilmektedir. Kapitalist olarak nitelenen kişi ve gruplar ise, kapitalizmin bugün kabul görmüş tanımından çok daha önce tarih sahnesinde yerini almıştır. Eski zamanlarda özellikle tüccarlar, üstüne kâr koyarak sattıkları mallara daha fazla yatırım yaparak daha fazla kâr sağlama yoluna gitmiştir (Fulcher, 2004: 13-14). Bu tür bir ticari kapitalizm, diğer bir ifadeyle tüccar kapitalizmi, alışverişe dayalı, metanın ucuz bir sahadan alınıp pahalı bir sahada satılmasıyla ortaya çıkmıştır.

Thier (2020: 18-19), kapitalizmin geçmişini tarım devrimine kadar götürmektedir. On iki bin yıl önce tarımla birlikte yerleşik hayata geçen insanlar,

³ 19. yy’nin başlarında İngiltere’de sanayinin ve sanayi işçilerinin en çok olduğu şehir olan Manchester; uzun çalışma saatleri, güvencesiz iş ortamı, erkek – kadın ve çocukların zor şartlarda çalıştığı sert bir düzen içermektedir. Kapitalist sistemin en sert koşullarını betimlemek için yazar burada “Manchester tarzı” ifadesini kullanmıştır.

gelecekteki olası ihtiyaları iin o an ihtiya duyduklarından daha fazlasını retme imkânına eriřmiřlerdir. Grece daha yakın bir gemiřte ise tccarların daha fazla kâr elde etmek iin yerel pazarlardan bařka pazarlara giderek rnlerini satma arzusu ticari ve tarımsal kapitalist sistemin (her ne kadar o zaman adı yle olmasa da) geliřmesine nayak olmuřtur. Fakat mnferit ve kk lekli ticari faaliyetlerden ziyade kapitalizmin (ve ticari kapitalizmin) iktisadi bir sistem olarak var olması coğrafi keřiflerle ve smrgeci yayılma hareketleriyle baėdařtırılmaktadır.

Kapitalist bir dnya ekonomisi olarak nitelenen modern dnya sistemi, on altıncı yzyıl boyunca Amerika ile Avrupa kıtalarının belirli blgelerinde oluřmaya bařlamıř ve zamanla tm dnyayı etkisi altına alacak biimde geniřlemiřtir (Wallerstein, 2016: 99). Coğrafi keřifler aėı, Avrupalı gl devletlerin dnyanın byk bir blmn gerek ticari bakımdan gerekse řiddet uygulayarak boyun eėdirme aėı olarak da tanımlanmaktadır. 1487 yılında Portekizli denizci Bartolomeu Dias mit Burnu’nu, 1492’de Kristof Kolomb Amerika’yı keřfetmiř; 1498’de Vasco de Gama Afrika’yı dolařarak Hindistan’a ulařmıřtır. Tm bu keřifler beraberinde zenginlik avını getirmiřtir (Beaud, 2016: 21). Portekizliler ve İspanyollar Gney Amerika yerli imparatorlukları yaėmalamıř, Afrika’nın gney ucunda birok liman inřa ederek oraları Avrupa slerine dnřtrmř ve Asya’ya giden deniz yolunun kontroln ellerine almıřlardır. Hollanda, 17. yy’de Gneydoėu Asya’da smrge imparatorluėu kurmuř ve Kuzey Amerika ve Afrika’yı etkisi altına almak iin İngilizler ve Fransızlarla mcadele iine girmiřtir. İngilizler, Hollandalılarla yaptıkları savařlardan galip gelmiř; sonrasında Fransız ve İspanyollarla karřılařtıėı diėer savařlarda da stnlk saėlayarak 18.yy’de stn bir smrge gc olduėunu ispat etmiřtir. İngilizler, Kuzey Amerika’dan Hindistan’ın gneyine ve Avustralya’ya kadar byk bir alanda hkm srmř veya bu alanlarda etkisini hissettirmiř; ayrıca gl donanmasıyla yine bu rota zerinde byk ticari faaliyetler gerekleřtirmiřtir. Avrupalı glerin dnya topraklarının zerindeki etkisi ticari kapitalizmin etkin olduėu iki yzyılda olduka geniřlemiřtir: Avrupalı devletler 1500’l yıllarda dnyanın %7’sini kontrol edebiliyorken 1775 yılında bu oran %35 olarak gerekleřmiřtir (Kocka, 2016: 55).

Amerika'nın keşfiyle birlikte İnka ve Aztek uygarlıklarının değerli madenleri yağmalanarak Avrupa'ya taşınmıştır. Yüz yılı aşkın bir sürede binlerce ton gümüş ve yüzlerce ton altın İspanya'ya aktarılmış; değerli madenlerin ülkedeki arzının çoğalmasıyla bu süre zarfında fiyatlar üç-dört kat artış göstermiştir. Enflasyondan yalnızca İspanya nasibini almamış, İngiltere ve Fransa gibi ülkelerde de fiyat artışları gözlemlenmiştir (Beaud, 2016: 22-28). Halk yükselen fiyatlara isyan ederken bir grup bundan memnun olmuştur: tüccarlar. Artan fiyatlar aracılığıyla daha fazla kâr elde eden tüccarlar, sağladıkları kârları daha fazla kâr için üretime – manifaktürlere ve imalathanelere – yatırmışlardır.

16.yy'nin ortalarından 17.yy'nin ortalarına kadar geçen sürede Büyük Britanya sanayisinde kapitalist ilişkiler ortaya çıkmıştır. Bu tarihler arasında manüfaktürlerin⁴ büyümesi, üretimi hızlandırmıştır. Örneğin, 100 yılda yalnızca kömür üretimi 14 kat artarak yılda 3 milyon tona ulaşmıştır. Kurşun, kalay, bakır gibi maddelerin üretimi sekiz kat, demir madeni üretimi ise üç kat artış göstermiştir. Bununla birlikte tarım ve hayvancılıkta da radikal değişimler meydana gelmiştir. Soylular, koyun yetiştirme ve yün satımı gibi işlerin kârlı olduğunun farkına varmışlardır. Feodal beyler, köylülerin tarım alanlarına kapitalist faaliyetler amacıyla el koyarak onları mülklerinden etmiştir. Bu faaliyetlerin bir sonucu olarak ticaretin gelişmesi de Avrupa'da kapitalist ilişkilerin hızla ilerlemesine destek olmuştur (Kerov, 2014: 28-29).

Beaud'un (2016: 59-60) ifadeleriyle sonuç olarak, Yeni Dünya'ya ait hazine ve varlıkların yağmalanması ile Avrupa'ya aktarılan zenginlik ve Amerika'da şeker kamışı tarlalarında, maden sahalarında ve tarımsal üretimde zorla çalıştırılan Afrikalı köle emeği kapitalizmin gelişmesine zemin hazırlamıştır. Ayrıca Büyük Britanya'da olduğu gibi manüfaktürlerin, imalathanelerin kurulması, burjuvaların ve feodal beylerin tüccarlara dönüşerek zanaatkâr emekçilere kendi kurallarını dayatmaları ve üretim süreçlerini kontrol altına alma çalışmaları bugün kapitalist üretim tarzı olarak bildiğimiz üretimin doğmasına yol açmıştır.

⁴ Manu: El, Facture: Üretmek. "Elle yapılan üretim." (Dobb, 1990: 29).

1.1.2. Sanayi Kapitalizmi

Kapitalist sanayi, kapitalist manüfaktürlerde yaygın olan kol emeğinin yerini makinelerin alması anlamına gelmektedir. Dolayısıyla manüfaktürden makineli sanayiye geçiş sanayi devrimi olarak adlandırılmaktadır. Sanayi devrimi, makineleşmiş bir dizi teknik yeniliğin üretim sürecini ev ve zanaat atölyesinden fabrikaya taşıdığı, bir ya da birkaç kişinin el veya düşük profilli makinelerle yaptıkları üretimi yüzlerce işçinin ekip çalışmasıyla yaptığı, kapitalizmin yükselişindeki önemli bir dönüm noktasıdır (Dobb, 1990: 27). Sanayi devrimi, 18. yy ortalarında İngiltere’de başlamış ve 19.yy’de diğer ülkelere yayılmıştır. Sanayinin İngiltere’de hızla gelişmesi ve sanayi devriminin İngiltere’de ortaya çıkması; ülkede köleliğin erken tasfiyesi ve köylülerin mülksüzleştirilmesi ile doğrudan ilişkidir (Kerov, 2014: 47). Sanayi devrimi ile makine kullanımına geçişle sanayi işçisi topluluklarının oluşması, proletaryanın sınıflaşması ve köylülüğün sona ermesi / oldukça azalması gibi toplumsal değişimler meydana gelmiştir (a.e., s.51). Marx, *Kapital*’de ticari veya farklı kapitalizm türlerinden ziyade 19.yy’deki sanayi kapitalizmini analiz etmektedir ve onu “*gerçek kapitalist üretim tarzı*” olarak betimlemektedir (Beaud, 2016: 177).

19.yy’nin başlarında herkesin dikkatle ele aldığı olgular Fransız Devrimi ve Avrupa’da yaşanan savaşlarken, sanayileşme arka planda kalmış ve daha az dikkat çekmiş bir diğer olgu olarak karşımıza çıkmaktadır. Sanayileşme ile daha çok meta üretiminin ve daha çok işçi sömürsünün meydana gelmesi bir tarafta zenginliği inanılmaz seviyede arttırırken diğer tarafta yoksulluğun derinleşmesine neden olmuştur (Beaud, 2016: 117). Kocka (2016: 97), sanayileşmeyi “*özünde birbirine bağlı üç gelişmenin yer aldığı karmaşık ve geniş kapsamlı bir sosyoekonomik dönüşüm süreci.*” cümlesiyle tanımlamaktadır. Sözü edilen birbirine bağlı üç gelişme ise şunlardır: (1) 18. yy’deki buhar makinesinin gelişimi ve eğirme ve dokumanın makineleşmesinden 21. yy’nin başlarındaki üretimin ve iletişimin dijitalleşmesine kadar olan organizasyon ve teknolojik alandaki yenilikler. (2) İnsanlığın doğayla olan ilişkiyi kökünden değiştiren yeni enerji kaynaklarının büyük çapta sömürülmesi. (3) zanaat atölyelerinin yerine bir üretim tesisi olarak fabrikaların yaygınlaşması,

yönetim ve uygulamanın ayrışması. Tüm bu gelişmeler sermaye sahibinin zenginleşmesini sağlayan bir üretim yönetimi olarak sanayileşmeyi doğurmuştur.

Ticari kapitalizmde kârı sağlayan şey değerli maden ticaretiyken sanayi kapitalizmiyle birlikte kâr, üretimin verimliliği ile ilişkili bir hâle dönüşmüştür (Gençoğlu, 2020: 242). Makineleşme, güçler ilişkisini değiştirerek ticaret burjuvazisinin önemini kaybetmesine neden olmuş, sanayi burjuvazisini ise onun tahtına yerleştirmiştir (Kerov, 2014: 52). Sanayi kapitalizmi, ticari kapitalizmin “ucuza satın alıp pahalıya satma” anlayışını rafa kaldırmıştır. Bugün bilinen anlamıyla kapitalizmin ticari kapitalizmden en önemli farkı yalnızca ticaretin değil, üretimin de dâhil olduğu tüm ekonominin sermaye yatırımına muhtaç olmasıdır.

Sanayileşmenin kapitalizmi nasıl değiştirdiği dört adımda açıklanmaktadır (Kocka, 2016:101 - 103): (1) Ücret ile emek gücünün mübadelesiyle somutlaşan kapitalist meta biçimi ilk kez insan emeğine tamamen ve toplu olarak uygulanmıştır. Sözleşmeye dayalı ücretli emek kitlesel biçimde yaygınlaşmış ve çalışma ilişkileri kapitalist hâle gelmiştir. (2) Fabrikalar, madenler, yeni ulaşım sistemleri, üretim tesislerinin makineleşmesi ve yayılmasıyla sabit sermaye birikimi hiç olmadığı kadar büyük bir ölçeğe ulaşmıştır. (3) Örgütsel ve teknolojik yenilikler, sanayi öncesi kapitalizm türleriyle kıyaslanamayacak kadar önemli bir hâle gelmiştir. Fabrikalar ve makineleşme tekstildeki öncül imalat gereçlerinin, buharlı gemi yolları nehir ve kanalların, elektrikli ampul üreticileri gaz lambası üreticilerinin yerini almıştır (Günümüz örneğiyle daktilo üretici pazarının yerini bilgisayar üreticilerinin alması gibi). (4) Sanayileşmeyle birlikte ortaya çıkan krizler, kapitalizmin önceki türlerinde yaşanan krizlere göre farklılaşmaya başlamıştır. Sanayileşmeyle kapitalizm artık ekonominin egemen bir düzenleyicisi hâlini almış ve dolayısıyla yaşanan krizler toplumda, kültürde ve siyasette derin izler bırakmıştır.

Kapitalist üretim biçiminin her alana yayılmasıyla işçilerin sömürülmesi paralel biçimde ilerlemiştir. Makinenin üretimi basitleştirmesi ile makinenin bir uzantısı hâline gelen işçinin vasfı değersiz hâle gelmiştir. Bu nedenle kapitalist üretim belirli bir görevi yerine getirebilecek, çarkın dişlilerinden birisi olacak kadın, erkek, çocuk kim varsa ucuz emek olarak görüp kullanmaya başlamıştır (Kerov, 2014: 52).

Sanayi kapitalizmi yalnızca “iş” yaratmakla kalmamış, aynı zamanda modern bir kavram olan “boş zamanı” da yaratmıştır. Kapitalist üretimin yarattığı disiplinli çalışmanın bir sonucu olarak boş zaman; akşamları, hafta sonları, tatilleri, kısacası çalışma içermeyen tüm zamanı kapsamaktadır. Boş zaman, 19. yy’nin ortalarıyla birlikte ticarileşmeye başlamış ve yeni bir kapitalist üretim sahasına dönüşmüştür. İşçiler artık boş zamanlarını kapitalist işletmeler tarafından düzenlenen, ücretli etkinlik ve faaliyetlere katılmakla geçirmeye başlamıştır. Boş zamanı doldurmaya yönelik etkinlikler - at yarışları, spor müsabakaları, seyircili sporlar - çalışanların boş zamanlarını sömürmeye ve yeni gelir kaynakları oluşturma amaçlı yepyeni endüstrilerin doğmasını sağlamıştır (Fulcher, 2004: 8-9).

Sanayi kapitalizmi, 20. yüzyılın başlarında General Motors ve Ford Motor Company öncülüğünde seri üretime dayalı yeni bir sisteme doğru evrilmiştir. Henry Ford, Frederick Taylor’un “*Bilimsel Yönetim İlkeleri*”nden ilham alarak 1910’lu yıllarda Michigan Detroit’te motorlu taşıt fabrikasındaki montaj hattının kurulmasına önyak olmuştur. Belirli bir çalışma standardının, vasıfsız iş gücünün, düzenli ve sıkı bir iş bölümünün ve dakik çalışma saatlerinin yer aldığı “fordist” üretim biçimi ucuza ve kitlesel otomobil üretilmesini sağlamış; söz konusu üretim kitlesel tüketimi doğurmuştur (McGuigan, 2009: 102). Fordist üretim mantığı, rutinleşmiş emek sürecini, çok sayıda standartlaşmış ürünlerin üretimini ve kayda değer bir kârlılığı içermektedir (Pietrykowski, 1999). Fordizm, 20. yüzyılın ikinci yarısından itibaren değişen ekonomik koşullara ayak uyduramamış; etkisini ve yaygınlığını kaybetmeye başlayarak yerini monolitik olmayan, stokların olmadığı ve daha esnek bir yapıyı imleyen post-fordizme bırakmıştır.

1.1.3. Bilişsel Kapitalizm

Bilişsel kapitalizm, coğrafi keşiflerle ortaya çıkan ticari kapitalizm ve sanayi kapitalizmden sonra gelen üçüncü evre kapitalizm olarak adlandırılmaktadır. Bu evrede önemli olan nokta, birikim sürecinde maddi olmayan emeğin kullanımı ve simgesel mal ve deneyimlerin üretimini merkez alan yeni bir biçim olmasıdır (Bulut - Peters, 2014: 31). Bilişsel kapitalizm yaklaşımı, bilgiye dayalı ekonominin liberal

kuramlarının bir eleştirisi olarak ve aynı zamanda kapitalist gelişimdeki mevcut aşamaya ait yorumların yetersizliğine bir yanıt olarak gelişmiştir (Tsogas, 2012: 383). Moulier–Boutang (2012: 57) bilişsel kapitalizmi “*birikimin nesnesinin bilgiden oluştuğu, bilginin değerin temel kaynağı hâline geldiği ve değerlendirme sürecinde ana karakter olduğu bir birikim tarzı*” olarak tanımlamaktadır. Diğer kapitalizm türlerinin aksine bilişsel kapitalizmin altında servet yaratım süreci homojen ve standartlaşmış emek organizasyon şemasına dayanmamaktadır. Bu türde üretken etkinlik, hem dilsel hem de dilsel olmayan iletişimsel metaların gelişiminden yararlanan ağ şeklindeki yapıların baskın hâle geldiği yeni örgütsel modellere göre gerçekleştirilmektedir (Fumagalli - Lucarelli, 2007).

Tsogas (2012: 383), bilgiden türetilen bilişsel sınıfının günümüz kapitalizminde bilgi birikiminin merkezî bir yer tuttuğunun altının çizmek için kullanıldığını belirtmektedir. Bilgiye dayalı üretim organizasyonu ile kapitalist ekonomik üretim tarzının bir araya gelmesiyle oluşan bilişsel kapitalizm çağdaş toplumun genelini tanımlamaktadır. Zira Tsogas’a göre yakın dönemde sıkça tercih edilen bilgi ekonomisi terimi toplumun bir yönüne (ekonomik faaliyetlerine) vurgu yaparken, çağımız üretiminin *post-fordist* olarak adlandırılmasının yetersiz ve sınırlı bulunmaktadır. Moulier–Boutang, bilişsel kapitalizmin ayırt edici özelliklerini aşağıdaki gibi maddelendirmiştir (2012: 50-56):

- Maddi olmayanın ve maddi olmayanın üretimiyle bağlantılı hizmetlerin artan rolü, yani ekonominin sanallaştırılması, bilişsel kapitalizmin en ayırt edici özelliklerinden biridir.
- Maddi olmayanın etkisi, yeni bilgisayar teknolojilerinin ve dolayısıyla dijitalleşmiş verilerin sonucudur.
- Bilgi ve bilimin yeri sağlamlaşır; ürün ve hizmetler içerisinde kristalize olur. Kristalizasyonla birlikte maddi emek ortadan kalmasa da stratejik bir varlık olarak merkezî rolünü kaybeder.
- Üretim süreçlerindeki klasik iş bölümü ve çalışma prensibi anlayışı yerini “esnek üretim” veya “sıfır stoklu üretim” gibi üretilere bırakmıştır.

- Sermaye ile emek, vasıflı ile vasıfsız emek arasındaki geleneksel ayrımlar yok olmaya başlamıştır. “Beşeri sermaye“ ve “entelektüel sermaye” terimlerinin yaygın biçimde kullanılmaya başlaması bunun bir belirtisidir.
- Tutarlı bir dijitalleşme, programlama, elektronik sistemlerin düzenlenmesiyle ve internetin icadı ağ toplumunun oluşumu mümkün hâle gelmiştir.
- Dijitalleşmeyle birlikte “beyinler arasındaki iş birliğinin” hızla gelişmesi, endüstriyel emek ve emek gücüne ait kabul edilen paradigmalarda ve servet üretimindeki maddi malların payında bir düşüş meydana getirmiştir.
- Bilişsel kapitalizmde üretilen metaların maddi olmayan doğası öğrenme süreçleri, kullanımları, yıpranma payları ve zenginleşmeleri bakımından enformasyon-metaları / bilgi-metalarının güçlü bir özgüllüğü yansıtmaktadır.
- Sanayi kapitalizmi metalar aracılığıyla meta üretimini; bilişsel kapitalizm, bilgi aracılığıyla bilginin üretimini ifade etmektedir. Yeni bir bilgi, teknik malzemelere ihtiyaç duyulmadan ancak bir bilgi birikimi temelinde yapılabilir. Bu üretim ise birbirine bağlı dijital ağlarda harekete geçirilen “kolektif beyin aktivitesiyle” gerçekleştirilir.

Maddi olmayan emek kavramı bilişsel kapitalizmin temel yapı taşıdır. Bu çerçevede bilişsel kapitalizm “*maddi olmayan varlıkları temel alan yeni bir birikim rejimi*” olarak değerlendirilmektedir (Bulut - Peters, 2014: 40). Maurizio Lazzarato, “*metanın enformasyonel ve kültürel içeriğini üreten emeği*” anlatmak için maddi olmayan emek kavramını öne sürmüştür; Michael Hardt ve Antonio Negri ise bu kavramı daha tanınır hâle getirerek tanıma iletişim, bilgi, enformasyon, ilişki gibi “*maddi olmayan sonuçlar yaratan emek*” eklemesini yapmıştır (Fuchs, 2014: 145). Hardt ve Negri’ye göre (2004: 122) 20.yy’nin son yıllarına girerken sanayi emeği hegemonyası yerini bilgi, enformasyon, iletişim vb. maddi olmayan ürünlerin üretimine bırakmıştır. Maddi olmayan emek bir yandan “*fikirler, semboller, kodlar, metinler, dilsel figürler ve imajlar üretirken*” diğer yandan duygulanımsal emek bağlamında “*rahatlık, esenlik, tatmin, heyecan veya tutku*” gibi hislerin üretimiyle de bağlantılıdır. Günümüzde maddi olmayan emeği içeren birçok iş her iki türdeki emeği de içinde barındırır. Hardt ve Negri’nin önemle arz ettiği bir nokta ise maddi olmayanın *emek* değil, *emeğin ürünü* olmasıdır. Başka

ifadeyle, maddi olmayan üretimde beyin ve bedenin işlevi diğer emek türleriyle aynıdır. Dolayısıyla sarf edilen emek yine maddidir; üretim sonucu ortaya çıkan ürün maddi olmayandır (a.e., s.123).

Bilişsel kapitalizm kavramı dışında benzer bir bağlam çerçevesinde çeşitli kapitalizm kavramsallaştırmaları da yapılmıştır. Franco Berardi, enformasyon teknolojileri “*dilsel emeğin sermaye değerlemesi ile tam olarak bütünleştirdiğinde*” semiyo-kapitalizmin ortaya çıktığını söylemektedir (2009: 149). Berardi, özellikle dil ve ekonomi arasındaki ilişkinin altını çizerek bu tanıımı yapmaktadır. Semiyo-kapitalizmi ayrıca ruhun ve zihnin üretici bir güç olarak sömürülmesine dayandırır (2014: 160). Philip Graham (2000), kapitalizmin güncel versiyonu olarak belirttiği hiperkapitalizm terimi ile günümüz yeni medyasında değerli bilgi metalarının anında tüketiminin, üretiminin, dağıtımının ve alışverişlerinin kolaylaştığını paylaşmaktadır. Ritzer & Jurgenson (2010) ortaya attıkları üretketici kapitalizmi kavramını “maaş bordrosunun olmadığı bir sistem” şeklinde ifade ederek ücret bağlamında şu şekilde açıklığa kavuşturur: “*Kapitalist bakış açısına göre düşük ücretli bir işçiden (az vasıflı işçi) daha iyi olan tek şey, hiç ücret almadan çalışan (üretketici) birisidir. Marksist ifadeyle ise işçi büyük miktarda artı değer üretirken, üreten tüketici yalnızca artı değer üretir.*” (2010: 26). Fuchs, bilişsel kapitalizm yerine enformasyonel kapitalizm kavramını kullanır. Enformasyonel kapitalizmde sermaye birikiminin bir boyutu olan bilgi emeği; iletişim, enformasyon, toplumsal ilişkiler ile iletişim teknolojilerini hem üreten hem de dağıtan emektir. Piyasada meta olarak anılıp satılan yazılım, veri, danışmanlık, reklam, film, müzik, istatistik vb. bilgi ürün ve hizmetleri bilgi işçileri tarafından üretilir. Fakat enformasyonel kapitalizmde bilgi yalnızca meta olarak bilgi işçileri tarafından üretilen ürün ve hizmetlerden oluşmaz. Bilgi, çocuklarını yetiştiren ebeveynler ve gündelik hayatta politikayla uğraşan kişiler tarafından üretilebildiği gibi sermaye tarafından kendine mal edilen enformasyonel içerik üreten radyo programına katılan dinleyicileri, televizyon izleyicileri, program konukları ve sosyal ağ kullanıcıları tarafından da günlük yaşam içinde üretilir (Fuchs, 2014: 163-164).

Özellikle içinde bulunduğumuz yüzyılda maddi olmayan emeğin, emeğin ürününün ve bilgi üretiminin tarihte hiç olmadığı kadar yüksek olduğu dikkate

alındığında kapitalizmin egemen yansımaları, adı her ne olursa olsun, söz konusu kavramlarda görülebilmektedir. Bugün teknoloji şirketlerinin her yıl artan kârları sahip oldukları ağ teknolojilerinin tabana yayılmış olması ve bu sistemlerdeki aktiviteleri gözetleme becerilerinin bir sonucudur. Geleneksel kapitalizmde denetim ve disiplin mekanizması olan gözetim, bilişsel kapitalizmle birlikte farklı amaçlar ve yöntemlerle kullanılmaya başlanmıştır. Günümüzde daha fazla kâr elde etmenin bir yöntemine dönüşen gözetim olgusunu tüm yönleriyle ele alarak kapitalizmle ilişkisini daha sağlıklı resmetmek mümkündür.

1.1. Gözetim Olgusu: Kuramsal ve Tarihsel Bir Bakış

Gözetim olgusu modern zamanlardan bugüne farklı yaklaşımlarla sürekli tartışılmıştır. Dil bilgisel olarak gözetim Fransızca “*surveiller*” fiilinden türetilmiştir, aynı dilde “*bakarak olmak*” anlamına gelmektedir. Bu anlam etrafı öylece süzmekten ziyade belli insan davranışlarının dikkate alınması sürecini ifade eder (Lyon, 2013: 30). Latince gözetleme kulesi ve şehir duvarlarının ardındaki tehditkâr pusuları ima eden “*vigilāre*” kelimesiyle bağlantılıdır (Marx, 2015: 734) ve genel olarak “*etkileme, yönetme, koruma, yönlendirme gibi amaçlarla kişisel enformasyona dönük odaklı, sistemli ve düzenli ilgi*” şeklinde ifade edilebilir (Lyon, 2013: 31). Gözetimin yaygın nedenleri arasında devletin topraklarını savunması, suçun önlenmesi ve polislik faaliyetleri, trafik ve ulaşım yönetimi, göçmenlik yönetimi, asayiş yönetimi, çocuk koruma işlemleri, halk sağlığı gözetimi, özel mülkiyet koruma, müşteri ilişkileri ve pazarlama gibi durumlar yer almaktadır. Jenkins (2012: 162), bu yaygın nedenlerde gözetime yol açan iki unsuru şöyle açıklamaktadır : (1) ister az ister çok olsun, insanların korunması ve yönetimi. Korunma ve yönetim arasındaki bağ ince ve belirsizdir ve her ikisi de gerek özel sektörde gerekse devlet kanallarında modern yönetim zihniyetinin merkezinde yer almaktadır. (2) Gözetim tek taraflıdır; etkileşimli olmaktan ziyade gözlemseldir. Gözetleyen gözetlenene toplanan bilgiler hakkında paylaşımda bulunmaz, açıklama yapmaz. Gözetlenen gözetim hakkında soru soramaz.

Gözetim, önceleri kabilelerde, monarşilerde ve imparatorluklarda egemenliği sağlama işleviyle kendini göstermiştir (Dolgun, 2015:21). Erken dönem modernizmle

birlikte Karl Marx tarafından kapitalizmin ekonomi politiğinin bir parçası olarak görülmüştür. Marx, modern toplumların biricik özelliğinin en yoğun gözetim faaliyetlerini yürüten kapitalist ekonomik sistem olduğunu belirtir. Gözetim, idari denetim amacıyla işçilerin verimliliğini yüksek seviyede tutmak için araçsallaştırılır. Piyasa içi rekabeti güçlendirme ve en az maliyetle en çok üretim sağlamak için gözetim temel bir araç olarak görülür. Daha sonradan Weber tarafından bürokratik sistemin bir ürünü olarak ele alınmıştır (Lyon, 2013:15; Dolgun, 2015: 88-89). Jeremy Bentham, *Panoptikon* adlı eserinde gözetimi “bugüne kadar örneği olmayan, zihin üzerinde zihinsel iktidar elde eden yeni bir yöntem” olarak tanımlar (akt. Mattelart, 2012:13). Panoptikon, Bentham tarafından kardeşi Samuel’in işçileri denetim altına alma düşüncesine dayanarak geliştirilmiş; görünmeyen bir denetçinin olabildiğince çok insanı gözetlemesi şeklinde, her bir kurum için uyarlanabilecek ideal bir mimari yapıyı imlemektedir.

Foucault (2015), gözetimi panoptikon gibi kapalı alanlarda tahakküm ve kontrole geçiş süreciyle açıklamaktadır. Foucault, gözetim toplumu çerçevesinde enformasyon ve bilgiyi, enformasyon toplumu yaklaşımlarından farklı olarak denetim, disiplin ve eşitsizliklerin birincil kaynağı olarak ele almaktadır. Ona göre hâkim gözetim toplumu modeli panoptikon üzerine inşa edilmiştir (Laughey, 2010: 113). Panoptikon’un en büyük etkisi, iktidarın tutukluda sürekli olarak görünürlük sağlaması olmuştur. Tutuklu her an gözlenebildiğini düşündüğü kuleyi sürekli olarak görmektedir. Fakat kuleden bir gözcünün ona bakıp bakmadığını bilemez. Bu yapı iktidarı rutinleştirmek ve devamlılığını sağlamaktadır (Foucault, 2019: 297). Deleuze, gözetimin yalnızca kapalı alanlarda gerçekleşmediğini ve her yere yayıldığını ifade etmektedir. Deleuze’un denetim toplumu kavramsallaştırması, Foucault’un “kapalı ve özgün gözetim alanlarına dayalı disiplin toplumu” yaklaşımının artık “elektronik teknolojilerin gündelik hayatın çeşitli alanlarında sürekli ve hareketli gözetim olanağı sunduğu denetim toplumuna” dönüştüğü şeklinde açıklanmaktadır (Lyon, 2013: 284). Denetim toplumu duvarların arkasında değil her an her yerde gözetlenme, sürekli takip edilme ve belirsizlikle ilişkilendirilmektedir. Deleuze’a göre çağdaş kapitalizmde disiplin, dışarı kaynaklı herhangi bir baskı olmadan kendi kendini denetleyen ve kontrol eden bir sistem ile değişime uğramıştır (Çakır, 2014: 99). Anthony Giddens

(1994), daha önce kapitalizm başlığında yer verildiği gibi gözetimi modernitenin dört büyük kurumsal boyutundan birisi olarak kabul etmektedir. Hatta gözetimin örgütler için hayati bir önem taşıdığını, yönetimi kolaylaştırdığını ve modernitenin bir diğer boyutu olan endüstriyalizmi geliştireceğini öne sürmektedir.

Gözetim üzerine gerek geleneksel gerekse çağdaş yorum, tanım ve kavramların hepsi, toplumun “ağ”, “sanayi sonrası”, “küresel”, “enformasyon”, “bilgi”, “tüketim”, “risk” veya “akışkan” gibi sahip olduğu sıfatların yanında “gözetim” toplumu olduğunu da işaret eder ve bu terimlerin birbirlerini etkileyip dönüştürdüklerinin altını çizer. Gözetim toplumu, hayatımızın her anının gözetim ile kaplandığına, gözetimin her an her yerdeliğine, gözetimden kaçınılmaz olduğuna dikkat çeker ve gözetim aktivitelerinin devlet sınırlarını aşarak tüm sosyal kanallara yerleştiğini gösterir (Lyon, 2013: 45; 2018: 60-61). Ek olarak, gözetimin emniyet ve güvenlikle ilişkisinin yanı sıra çeşitli kurumlarca kişisel verilerin toplandığı ve birbiriyle ilişkilendirildiği bir bağlamda bütünsel bir anlamı ele almaktadır (Dolgun, 2015:27). Kavram ilk defa Gary T. Marx (1985) tarafından dile getirilmiştir. Marx, gözetim toplumunu açıklarken modern gözetim araçlarının her yerdeliğine vurgu yapar: “*günümüz gözetim toplumu fiziksel, sosyal ve kişisel alanlarda daha derinlere inebilir; fısıltıları duyar ve duvarlara, pencerelere, bulutlara ve karanlığa nüfuz eder*”. Oscar Gandy (1989: 62), modern gözetim teknolojisini, çevre hakkındaki bilgiyi algılama, ölçme, depolama, işleme aygıtlarını içeren entegre bir donanım ve yazılım sistemi olarak tanımlar. Yeni teknolojiler, gözetim aracılı veri arayışını eski yöntemlere nazaran daha verimli, kapsamlı ve göze batmayan hâle getirmiştir. Eski yöntemlerle gözetim toplumu ele alındığında baskı, disiplin ve düzene dayalı bir yapı tezahür edilirken; çağdaş gözetim toplumu insanın ve çevresinin en mikro düzeyde bilinebildiği, tanınabildiği ve en önemlisi ne yapacağının öngörülebildiği bir alana işaret eder. Bilgisayar ve ağ tabanlı gözetim araçları dijital anlamda gözetlenen toplumun oluşmasına önyak olmuştur.

Günlük yaşamda gözetimi ele alan çağdaş yaklaşımlar, Orwell’in 1984’ünden veya Foucault’nun Bentham’ın panoptikon metaforunu kullanımıyla ortaya çıkan imgelerden giderek uzaklaşmaktadır (Daems, 2019: 8). Deleuze, Foucault’cu kurumların ve onların disipline etme yollarının artık var olmadığını, ya da en azından

diğer gözetim türleriyle yer değiştirdiğini gözlemler (Galič vd., 2016:19). Haggery ve Ericson (2000), ağlarla bağlı gerçekleşen, insanı derinlemesine gözetleyen çağdaş gözetimin geçmiş gözetimden farklı olduğunu, dolayısıyla bugünü açıklarken panoptikonun uygun bir metafor olmadığını dile getirir. Orwell veya Foucault'nun kavramlarını günümüze uyarlamak yerine, çağdaş gözetimin özelliklerini keşfetmek ve açıklamak için farklı araçlar önerir. Benzer biçimde Lyon, gözetim tartışmalarında ilk akla gelen “*Büyük Birader*”in tüm vurgusunu araçlar ve zorbalara üzerine yoğunlaştırdığını; gözetime neden olan olayların, gözetimi geliştiren fikirlerin ve gözetimi sorgulayan veya ona itaat eden kişilerin görülmesini engellediğini belirtir (Bauman - Lyon, 2018: 19-20). Daems (2019: 8), bugünün dünyasında büyük verinin büyük biradere meydan okuduğunu iddia eder. Lyon, Foucault'nun özdisiplinli toplumların ortaya çıkışını panoptikon örneğiyle anlatmasının büyük önem taşıdığını; fakat gözetim çalışmalarında panoptikondan sürekli bahsedilmesinin bıkkınlık verdiğini söyler (Bauman - Lyon, 2018: 66-67). Ayrıca, Foucault'nun bilgisayarlar ve dijital gözetim hakkında herhangi bir fikir beyan etmemesine rağmen yeni yaklaşımlara esin kaynağı olmasını ironik bulduğunu (Lyon, 2018:31); günümüz gözetim toplumunda gücün değişik kanallar aracılığıyla aktığını ve toplumsal yaşamı yönlendiren bir gözcü kulesinin olmadığını ifade eder (a.e., s. 23).

Yukarıda da bahsedildiği gibi gözetim çalışmaları genellikle Foucault'un gözetim anlayışına göre sembolleştirdiği panoptikon üzerine inşa edilenler ve panoptikon üzerine inşa edilmeyenler olarak farklı yaklaşımlarla ele alınmaktadır. Foucault'un panoptikonu üzerine inşa edilen gözetim çalışmaları şu varsayımlardan birini veya birkaçını içermektedir: (1) Foucault'nun panoptikon kavramı günümüzde gözetimi incelemek için kullanışlıdır. (2) Gözetim olumsuz olarak tanımlanmalıdır. (3) Bu bakış açısı gözetimi dar bir tanım içinde kullanır. (4) Gözetleme; baskı, disiplin, güç ve tahakküm ile bağlantılıdır. (5) Güç merkezîdir ve toplum kontrollü olma eğilimindedir. Panoptikon üzerine inşa edilmeyen gözetim kuramlarında ise şu varsayımların bir ya da birden çoğu yer almaktadır: (1) Günümüz gözetimini analiz etmede panoptikon yeterli değildir. (2) Gözetime yaklaşım tarafsız olmalıdır. (3) Bu bakış açısı gözetimi geniş bir tanımda kullanmaktadır. (4) Veri toplama işleminin hem zorlayıcı hem de kolaylaştırıcı etkileri vardır. (5) Gözetim öncelikle çoğul ve teknik

bir süreç olarak kabul edilir. Thomas Allmer'ın (2012: 23-24) ana hatlarıyla yer verdiği bu ayrım gözetim üzerine analiz ve araştırma yapan yazarlar tarafından sıkça tartışılmalıdır. Allmer, panoptikona üzerine inşa edilen ve edilmeyen gözetim çalışmalarını ve yazarları şu şekilde tabloştürmüştür:

Gözetim Kuramlarının Temelleri		
	Tanım	Yazar
<i>Panoptikon üzerine inşa edilen gözetim kuramları</i>	Bu yaklaşımı benimseyen yazarlar gözetim faaliyetlerinin her zaman olumsuz olduğunu düşünür ve baskı, iktidar ve tahakkümle bağlantılı olduğunu vurgular. Bu yazarlara göre iktidar merkezî hâle gelerek toplumu baskı ve kontrol altında tutma eğilimi gösterir. Dar bir gözetim tanımına sahiptir.	Gilles Deleuze, Mark Poster, Oscar Gandy, Frank Webster, Thomas Mathiesen, Greg Elmer
<i>Panoptikon üzerine inşa edilmeyen gözetim kuramları</i>	Gözetim üzerine çalışmalar yapan birçok bilim insanı, yazar ve akademisyen gözetime tarafsız yaklaşır, genel ifadeler kullanır ve gözetimin panoptik olmayan unsurlarının altını çizer. Bu yaklaşımda geniş bir gözetim tanımı yer alır ve verilerin toplanmasına ilişkin olumlu ve olumsuz etkilerinin ikisi de paylaşılır. Gözetim genellikle çoğul, tarafsız ve teknik bir süreç olarak kabul edilir.	Anthony Giddens, Gary T. Marx, David Lyon, Roger Clarke, Jean Baudrillard, Kevin Haggerty, Richard Erickson, William Bogard, Christopher Dandeker

Tablo 1.2: Gözetim Kuramlarının Temelleri (Allmer, 2012: 40-41).

Gözetim tarihsel olarak ele alındığında modernite mihenk taşı olarak karşımıza çıkmaktadır. Modernite ana özelliklerine göre şu şekilde özetlenmektedir: (1) Fabrika ve makine temelli kapitalizmin ortaya çıkışıyla verimlilik, öngörülebilirlik, kontrol ve disiplin kavramlarına dayalı olarak sosyal yaşama dair rasyonel ve hesaplayıcı tutumların gelişimi. (2) İşbölümü ve mesleki uzmanlaşmanın ortaya çıkması. “Kamusal” ile “özel”, “ev” ile “iş” ayrımlarının toplumsal yaşamda giderek farklılaşması. (3) Devlet ve özel kurumların, bürokrasilerin ve şehir merkezlerinin gelişmesi / büyümesi. Ulaşım ve iletişim teknolojilerinin gelişimiyle iletişimin hızlanması. (4) Kendi çıkarları, duyarlılıkları ve kültürü ile görece orta ve üst sınıfların artışı. (5) Psikoloji, psikiyatri, sosyoloji, istatistik ve halk sağlığı gibi beşeri bilimlerin gelişimi. (6) Bilimsel bilginin, nesnel düşüncenin ve teknolojinin doğadan yararlanarak insan varlığını ve sosyal yaşamı iyi yönde değiştirebileceği fikrini oluşturan ilerleme inancının yerleşmesi (Staples, 2000). Gözetimin modernizmdeki işlevi her bir maddede kendini hissettirmektedir. Dolayısıyla tarihsel olarak gözetim üzerine bir inceleme yapmak gerektiğinde modernite tam merkezde yer almaktadır. Lyon da gözetimi teknikleri açısından üçe ayırırken moderniteyi tam ortada ele almaktadır: (1) Modern öncesi: yüz yüze gözetimin yer aldığı, şimdiki zamanda gerçekleşen gözetimdir. İşverenin işçileri gözetlemesi modern öncesi gözetim tekniğine örnek oluşturabilir. (2) Modern: dosyala dayalı, bugün ve geçmiş yönelimli, karmaşık; *“kapsayıcılığı, aynılığı, birörnekliği, tektürelliği özendirme eğilimdedir.”* (3) Postmodern: dijital aracılı, davranışsal modellere dayanan ve gelecek yönelimli gözetim tekniğidir. Hem bireyin kendisine hem de dünyaya odaklıdır (Lyon, 2013: 113). Bu çalışmada gözetime tarihsel olarak yer verilirken Lyon’un bu ayrımından faydalanılmıştır.

1.2.1. Erken Modern Dönemde Gözetim Çalışmaları

Gözetim olgusu düzenli olarak izleme, kayıt altına alma, saklama, denetleme, yönetme, sınıflandırma ile doğrudan ilişkilidir. Aynı zamanda sanayileşme ve kapitalizmle birlikte modernitenin tamamlayıcı bir parçası olarak kabul edilmektedir. Gözetleme faaliyetleri her ne kadar modern dönemle birlikte organize ve merkezî bir hâle gelse de modern öncesi dönemlerde farklı biçimlerde kendisini göstermiştir.

Dolayısıyla erken modern dönemi incelemeden önce gözetimin modern öncesi devlet ve kurumlarda nasıl gerçekleştiğini ele almak mümkündür. Lyon (2013: 115 -117), modern öncesi tarihlerde gizlice izlemenin yanı sıra dinlemenin de gözetim aracı olduğunun altını çizmekte; ayrıca gözetimin izleme, dinleme, casusluk ve röntgencilik şeklinde gerçekleşmesinin yanı sıra nüfus sayımı ve devlet ve kurumların kişisel bilgileri kayıt altına alma gibi durumları da kapsadığını vurgulamaktadır. Hintli yazar Çanakya M.Ö. 4. yüzyılda yazdığı *Arthashastra* adlı eserde insanlara ait bilgi toplamanın ne kadar önemli olduğunu o dönemlerde dikkat çekmiştir. Aynı şekilde Sun Tzu, *Savaş Sanatı* yapıtında düşman hakkında bilgi sahibi olmanın savaş stratejilerini oluşturmada etkisinin ve savaş sırasında yaratacağı avantajların altını çizmiştir. Antik Mısır'da nüfus sayımları yapıldığı tahmin edilirken bugüne kaydı kalan en eski nüfus sayım verileri yaklaşık iki bin yıl öncesine aittir ve Çin'in Han Hanedanlığı tarafından yaptırılmıştır. Benzer biçimde Roma İmparatorluğunda tüm yetişkin erkeklerin askerlik hizmetine uygun olup olmadıklarına ilişkin bilgiler tutulmuştur. 1086 yılında İngiltere'nin büyük bir kısmı ile Galler'in belirli bölgelerini içine alarak yapılan araştırma ile hazırlanan *Domesday Kitabı*, 13.000'den fazla içerdiği kayıtlarla devletin vatandaşlar hakkında organize bilgi toplamasının erken örneklerinden birisidir (Weller, 2012: 57-58). Modern öncesi bir başka örnek ise sağlık verilerine ilişkindir. Sağlık verilerine yönelik ilk gözetim faaliyetleri 1300'lü yılların başındaki bubonik (hıyarcıklı) veba hastalığına kadar dayanmaktadır. O dönem Venedik Cumhuriyeti yakınlarındaki limana yanaşan gemiler halk sağlığı yetkilileri tarafından veba benzeri hastalıkların tespiti için taranmış, kaydedilmiş ve buna göre muhtemel hastaların karaya çıkması engellenmiştir (Thacker, 2010). Görüldüğü üzere casusluk faaliyetlerinden nüfus sayımına halk sağlığı güvenliğinden kişisel veri toplamaya kadar çeşitli amaçlar doğrultusunda gözetim pratikleri modern öncesi dönemde de kendisine yer bulmuştur. Fakat bugün bilinen şekliyle gözetim, yani sosyal hayatın kurumsal olarak merkezî ve yaygın bir biçimde gözetlenmesi, modern zamanlarla birlikte ortaya çıkmıştır (Lyon, 1994: 24).

Erken modern olarak ifade edilen 16. yüzyılın başlangıcı ile beraber ordu, okul, fabrika ve devlet kurumlarında ortaya çıkan gözetim pratikleri zamanla gündelik hayatın tüm alanlarına yayılmıştır. Özellikle teknik gözetimin nasibini aldığı ilk

alanlardan olan atölye ve fabrikalar, kapitalist düzen içerisinde işçilerin sermaye sahipleri tarafından disiplin altına alınmasına dayanmaktadır (Dolgun, 2015: 77). Bununla birlikte Lyon, modern toplumların kalıcı özelliklerinden birinin beraberinde güçlü bir gözetimi de getiren kapitalist ekonomik sistem olduğunu ifade etmektedir (1994: 25). Paralel biçimde erken kapitalist dönemlerde evden ayrı bir işyeri sahasının oluşması ve ücretli işgücüyle birlikte emeğin bu sahada görünür olmaya başlaması, sermaye sahiplerinin işçileri denetleme arzusunun doğurmuştur. Çalışma sürelerinin verimliliğini denetlemek ve işçilerin potansiyel emek güçlerinin sonuna kadar kullandıklarından emin olmak isteyen kapitalistler, işyerlerine denetçiler olarak bu faaliyetleri yürütmüştür (Lyon, 2013: 117-118). Daha önceleri işçileri (serfleri, köleleri, köylüleri) disipline etmek ve itaatsizliklerle başa çıkmak için fiziksel güç ve şiddete maruz kalmış ve zor kullanılarak korkutulmuştur. Modernizm ve kapitalizmin erken dönemleriyle birlikte işyeri ve işçinin farklı anlamlar kazanarak dönüşmesi farklı ve daha yumuşak başa çıkma pratiklerinin doğmasına neden olmuştur. Gözetleme faaliyetlerinin işyeri ve fabrikalarda yer almaya başlamasıyla işi zamanında bitirme, işçiyi uygun işbölümüne yerleştirme, işçilerin çalışmalarının sınanması ve gözlemlenmesi gibi yöntemler bu alanlarda kendisine yer bulmuştur. Diğer bir ifadeyle, işçinin işin başında olup olmadığı ve işini ne kadar özverili yaptığı artık kolaylıkla izlenebilmekte; işçiler yeteneğine göre sınıflandırılabilen, birbirleriyle karşılaştırılabilen ve tüm üretim aşamaları gözlemlenebilmektedir (Dolgun, 2015: 78 - 83). Verimlilik artışı ile sermaye birikiminin doğrudan ilişkisi olduğu düşünüldüğünde gözetim olgusunun fabrika ve işyerlerinde hayati bir önem taşıdığı görülmektedir.

Foucault'un (2007) büyük kapatılma olarak nitelendirdiği toplumsal değişim ve disiplin süreçleri gözetimin erken modern dönemdeki en etkili yansımasını oluşturmaktadır. Kapatılma olgusu, 17. yüzyılın ortalarında Paris'te kurulan ve "Genel Hastane" olarak adlandırılan kurumda deliler, hastalar, aylaklar, hırsızlar, sakatlar, eşcinseller, evsizler gibi çeşitli öznelerin bir arada gözetime tabi tutulmasıyla başlamıştır. Bu kişilerin en büyük ortak yanları işsiz olmaları, çalışmak istememeleri veya evsiz olmalarıdır. Dolayısıyla kapatılmadan kurtulmak için bir meslek sahibi olmak veya az ücretli de olsa çalışmak gerekmiştir. O dönemde tımarhane, hastane,

hapishane gibi ayrı kurumlar olmadığı için hepsini tek bir çatıda buluşturan genel hastaneler, mahkemelerden bağımsız bir oluşum olarak yargı ve infaz gücüne sahip bir kurumdur. Yönetim bütünlüğünü elinde bulundurması, kapatılma olgusunun gözetim tabanlı bir iktidar görevi olarak icra edilmesini sağlamıştır. Kapatılmanın altında ahlaki ve dinsel nedenlerin yatmasının yanı sıra ön planda çıkan en büyük neden kapitalizm ve onun dönüştürdüğü sosyo-ekonomik unsurlardır. Köylerinden sürülen köylüler, kaçak askerler, hastalar, işsizler kısacası başıboş olan “aylak” ve “serseriler” belirli bir düzen içinde yabancı kalmış ve toplumsal çerçevede sorun teşkil etmişlerdir. Bu kesimdeki insanlar toplumsal bir huzursuzluk yaratarak düzeni bozmakla itham edilmektedir ve tehlikeli kabul edildikleri için daimi bir gözetim altında tutulmalı ve denetlenmelidir. Bu denetimden çıkış yolu veya denetime tabi olmama yolu ise çalışarak bir efendiye sahip olmaları ve onun denetimi altında olmalarıdır. Kapatılmanın kapitalizmle güçlü ilişkisi, onun köklerinin İngiltere’de, en sanayileşmiş şehirlerinde çıkmasıyla ortaya konulmuştur. Kapitalizmin ihtiyaç duyduğu emek gücünü üretmek için kapatılma olgusu aylaklığı azaltmak ve ucuz işgücü sağlamak gibi kilit işlevleri yerine getirmiştir. Bunların yanında bireylerin ve toplumun disiplin altına alınmasında da önemli katkılar sağlamıştır (Dolgun, 2015: 67-73).

1.2.2. Modern Dönemde Gözetim Çalışmaları

19. yüzyıl beraberinde geniş ölçekli bir sistematik gözetimi getirmiştir. Sistematik gözetim askeri örgütlenmenin, sanayi kasaba ve şehirlerin, hükümet idaresinin ve Avrupa ulus devletlerindeki kapitalist ticari girişimlerin büyümesiyle meydana gelmiştir (Lyon, 1994: 24). Kapitalist ekonomik sistem işçilerin fabrikalarda, işyeri ve atölyelerde tek bir çatı altında toplanarak gözetlenmesini beraberinde getirmiştir. Bugün sistem içinde yönetim olarak adlandırılan şey de çalışanları izlemek ve kontrol altında uyumlu biçimde çalıştıklarından emin olmak olarak nitelenebilir. Gözetimi bir olgu olarak ilk analiz edenlerden olan Max Weber’e göre gözetim bürokrasiye doğrudan bağlıdır. Buna göre modern dönemin merkezinde bürokratik örgütlenme yer almaktadır. Gözetim, sahip olduğu araçlarla bürokrasinin oluşmasındaki güçlü öğelerden birisidir. Weber, örgütlerin gelişiminin enformasyon akış süreçlerinin denetimine bağlı olduğunu ve bu aşamada enformasyonu yazıya

dökmenin ve saklamanın önemine dikkat çekmektedir (Giddens, 2008: 686). Lyon, modern dönem gözetim faaliyetlerinde bürokrasinin önemine vurgu yaparak onun için “adlandırma, kimliklendirme, sayım, sınıflandırma, kayıt tutma” vb. işlemlerin ne kadar önemli olduğunun üzerinde durmaktadır. Böylelikle bürokrasinin “denetleyiciliği ve enformasyon toplama kapasitesi” sayesinde temel bir gözetim biçimi olduğu söylenebilmektedir (Lyon, 2013: 119-120). Örgütler bürokratik gözetim süreçlerine çok yönlü olarak maruz kalmaktadır. Foucault, örgütlerin mimari yapısının bürokratik gözetimi etkilediğini ve gözetimi şekillendirdiğini ifade etmektedir. Bu bağlamda Giddens (2008: 694-695), örgüt gözetimini birkaç başlıkla ele almaktadır. İlki, astların çalışmasının üstler tarafından doğrudan izlenmesini içermektedir. İşyerleri, okullar ve benzer kurumların iç mekân tasarımları buna göre inşa edilmektedir. Örneğin, sınıflar öğrencinin öğretmeni doğrudan görebilecekleri biçimde tasarlanır; masa ve sıralar ona göre yerleştirilir. Bir diğeri, Weber’in de modern örgütler için ne denli önemli olduğunu vurguladığı dosyalama ve kayıt tutmayı kapsamaktadır. Çalışanların kişisel bilgilerinden oluşan kayıtlar onların davranışlarını düzenlemek ve örgütlerdeki geleceklerine karar vermek için kullanılmıştır. Son olarak bireyin başkaları tarafından gözetlendiğinin farkında olması ve ona göre davranışlarını düzenlemesi anlamına gelen öz-gözetim karşımıza çıkmaktadır. Örneğin, çağrı merkezi çalışanları görüşmelerin kayıt altına alındığını ve amirlerinin gözetiminde olduklarını bilerek görüşmelerini sürdürmektedir.

Michel Foucault, 20.yy’nin ikinci yarısında gözetimi bürokrasinin ve dolayısıyla örgütlerin ötesine taşıyarak toplumun genelinde disiplin bağlamında incelemektedir. Ona göre toplumun kendisi “*iktidar tekniklerinin ve stratejilerinin her zaman mevcut olduğu bir disiplin toplumu*” hâline gelmiştir. Daha önce de ifade edildiği gibi ordu, hapishane ve fabrika gibi kurumlarda gelişen gözetim uygulamaları yaşamın her zemininde kendini hissettirmeye başlamıştır. Modern toplumlarda insanlar daha fazla gözetlenmekte, faaliyetleri sınıflanmakta ve belgelenmektedir (Lyon, 1994: 26). Modern dönem zihni olduğu kadar bedeni de şekillendirmek için tasarlanmış bir dizi söylem, teknik ve uygulama doğurmuştur. Foucault’nun “disiplin iktidarı” olarak adlandırdığı kavram, toplumsal ve siyasi baskı biçimini içermektedir. Disiplin iktidarı doğrudan hükümetin veya üst düzey yöneticilerden kitlelere doğru

gerçekleşmez, çok farklı sayıda kurumsal ve örgütsel alanda ve gündelik rutinde çeşitli ortamlarda çeşitli insanlar tarafından geliştirilip uygulanabilmektedir. Bu özelliği onun sadece “yukarıdan aşağıya” biçiminde değil, büyük oranda sosyal bedenler arası dolaşan “çift yönlü” olarak görünmesini sağlamaktadır. Disiplin iktidarı, yalnızca birkaç kişinin elinde değil her zaman her yerdedir, parçalara bölünmüştür ve dağınıktır. Disiplin iktidarı sade bir baskı içerse, yani doğrudan yukarıdan aşağıya baskıcı bir biçimde gerçekleşse birçok direnç noktalarıyla karşılaşabilir ve sınırlı etkiler bırakır. Oysaki onun yerine disiplin teknikleri uygulanırken avantajları vurgulanmaktadır: gözetleme kameralarının kamu güvenliğini arttıracak gibi (Staples, 2000). Foucault, disiplin iktidarının ekseriyetle otomatik, anonim, sürekli ve kapsamlı biçimde meydana geldiğini ve toplumun en derinine inerek en arkadaki kişiye kadar uzanabildiğini ifade etmektedir. Toparlayacak olursak, gözetimi disiplin toplumu kavramıyla analiz eden Foucault, geçmişteki keyfi cezalandırmalar, işkenceler ve idamların aksine modern disiplin çağında insanlara doğrudan şiddet uygulamak yerine yumuşak güç kullanılarak disiplin altına alındığını, kontrol edildiğini dile getirmektedir. Panoptikon metaforu ise disiplin toplumunu açıklamada ideal bir sembol olarak betimlenmektedir.

1989 yılında Berlin Duvarı yıkılana kadar Doğu Almanya Devlet Güvenlik Bakanlığı (Stasi) yüzbinlerce çalışanıyla milyonlarca insanı gözetim altında tutmuştur. Onların mektuplarını okumuş, rutinlerini takip etmiş, caddelerde ve sokaklarda gözetlemiş, evlerine dinleme cihazları yerleştirmiş ve telefonlarını dinlemiştir. Tüm bunların sonucunda elde edilen bilgiler uç uca konulduğunda 140 kilometre uzunluğuna erişecek sayıda dosyalarda tutulmuştur. Bu bağlamda İkinci Dünya Savaşı bitimiyle Web’in ortaya çıkışına kadarki süre zarfında Doğu Almanya’nın en büyük gözetim devletlerinden birisi olduğun söylenebilir (Mayer-Schönberger - Cukier, 2013: 157).

Modern döneme ilişkin gözetim çalışmaları ve uygulamaları disiplin, iktidar ve yönetim bağlamında sıkça tartışılmalıdır. 19. yüzyılda icat edilen iletişim araçlarının birer gözetim nesnesi olarak o dönemki toplumsal ve siyasi zeminde nasıl karşılık bulduğuna yönelik çalışmalar nadiren ele alınmıştır. Bu soruna dikkat çeken

Josh Lauer, gözetimin moderniteyle birlikte anılmaya başlamasına rağmen gözetime yönelik araştırmaların genellikle 20. yüzyıldaki teknolojileri içerdiğini ve İkinci Dünya Savaşı öncesindeki gözetim faaliyetlerinin geri planda kaldığını ifade etmektedir. Bu bağlamda Lauer (2012: 571-577), 19.yüzyılın sonlarına ait üç modern gözetim aracının tarihine odaklanmaktadır: taşınabilir fotoğraf makineleri, fonograf ve telefon. 1839 yılında erken fotoğrafçılıkta kullanılan bir teknik olan dagerreyotipinin icadıyla fotoğraf kitlesel bir tanınırlık kazanmaya başlamıştır. 19.yy'nin sonlarına kadar kamera teknolojisinin sınırlı fiziksel ve teknik imkânları, kişileri gizli fotoğraflama amaçlı kullanımını kısıtlamıştır. Kameraların küçülmesiyle fotoğraflar kısa sürede şantaj ve gerilla aktivizmi aracı olarak kullanılmaya başlamış ve tehditkâr bir araç hâline gelmiştir. Kameralar, diğer yandan, dönemin ünlü yıldızlarından siyasetçilere ve hatta halk plajlarındaki insanlara kadar birçok kesimin peşinden gitmiş ve onları rahatsız ve ifşa edecek boyutlarda çekimler gerçekleştirilmesine aracı olmuştur. Örneğin, 1899 yılında New York'ta yaşayan genç bir kadın, yerli bir un şirketinin 25.000 adet basıp çeşitli yerlere dağıttığı bir broşürde fotoğrafının kullanıldığını gördükten sonra sinir krizi geçirmiştir (Mensel, 1991'den akt. Lauer, 2012). Lauer'in ikinci ele aldığı cihaz fonografıdır. Edison'un 1878 yılında icat ettiği fonograf, seslerin kayıt altına alındığı, süresiz olarak korunabildiği, sınırsız kopyalanabildiği ve yeniden üretilebildiği bir cihazdır. Edison'un iletişim hızlandırması amaçlı büyük umutlar beslediği fonograf sıklıkla "seslerin fotoğrafı" olarak tanımlanmıştır. Edison, fonografin *"söylediklerimize dikkat etmemizi öğreteceğini"* ve konuşmaları daha kibar ve doğrudan hâle getirerek topluma *"kesin bir ahlaki etki"* empoze edeceğini iddia etmiştir (Edison, 1888'den akt. Lauer, 2012). Edison, araca dair olumlu bir bakış açısına sahip olsa da fonograf dönemin gazetelerine göre genel olarak kadın-erkek ve aile içi ilişkilerdeki sadakat, aldatma ve yalanların tespitinde sıkça tercih edilmiştir. Lauer, son olarak telefonu incelemiştir. Graham Bell, 1876'da patentini aldığı telefonu halka açık platformlarda sunmaya başladığı zaman ilk tepkiler cihazın "gözetim aracı" olduğu yönünde olmuştur. Bazı yazarlar elektrik direklerine bağlanan telefon kablolarıyla yoldan geçenlerin konuşmalarının gizlice dinleneceğini aktarırken, bazıları telefonların toplulukların dedikodularını ve gizli toplumsal ilişkileri ifşa etmesi tehdidiyle karşı karşıya olduklarını yazarak gençleri *"telefonun mucidinin infazını ve eserinin yok edilmesini"* talep etmeye davet etmiştir.

1890'lı yıllara kadar doktor ve iş insanları tarafından sıkça tercih edilen telefonun gözetim aracına dönüşmesi santral teknolojisiyle birlikte olmuştur. Kadın telefon operatörleri tıpkı telgrafları yöneten erkekler gibi gizlilik yemini etse de gizli dinlemelerin ve suiistimallerin önüne geçilememiştir. Diğer yandan 20. yüzyıl ile birlikte özel hatların yanı sıra daha uygun fiyatlı bir alternatif sunan paylaşımlı hatların ortaya çıkması gizli dinlemeleri neredeyse kaçınılmaz hâle getirmiştir. Onlarca ailenin ortak hattı kullanmasını ve mahremiyet sorunlarını New York Times'tan bir yazar şu sözlerle ifade etmiştir: *“Diğer abonelere haber vermeden bir kişinin kız arkadaşıyla telefonda görüşme yapması mümkün değildir.”* (Lauer, 2012: 577). Artık evin tüm kapıları, pencereleri kapalı olsa ve kişi evde yalnız olsa bile telefon görüşmesinin başkası tarafından dinlenip dinlemediği bilinmez bir durum olmuştur. İlgili dönemlerde gözetleme araçları olarak bu üç cihazın bireysel ve toplumsal mahremiyet ve gizlilik üzerine etkilerinin incelenmesi, gözetim aracılı bu olguların yeni olmadığının birer göstergesi olması açısından değerli birer kaynak oluşturmuştur.

Modern dönemde teknolojik imkânların gelişmesi tüketicilerin ve tüketim alışkanlıklarının gözetimini de mümkün kılmıştır. Bakacak olursak ödeme ve finansal işlemlere ilişkin kayıtların tutulmaya başlamasını 19.yy'nin sonlarına kadar dayandırmaktadır. O tarihlerde büyük mağazalar, kredi veren kuruluşların yıllardır üzerine kafa yorduğu iki soruyla karşılaşmıştır: Kredi çekenlerin güvenilir olduğu nasıl tespit edilir? Borçlar nasıl tahsil edilir? Mağazalar bu sorulara muhasebe ve faturaların kaydını tutma ve yeni kredi kontrol sistemleriyle cevap bulmaya çalışmıştır. 20.yy'nin erken dönemlerinde söz konusu mağazalar artık bireysel alışveriş yapanları mağaza hesaplarıyla ilişkilendiren kredi jetonları vermeye başlamıştır. Bu jetonlar genellikle kazınmış isimlerden oluşan plakalar, anahtarlıklar ve kâğıt cüzdan kartlarından oluşmuştur. İlk kartlı ödeme sistemi olan bu jetonlar tüketici davranışlarına ait verilerin hızla birikmesinde öncü bir rol oynamıştır (Lauer, 2020:3).

Birinci Dünya Savaşı'ndan kısa bir zaman sonra büyük perakende mağazaları veresiye müşteriler için onları tanımlayan fişler vermeye başlamıştır. Bilinen ilk örnekleri mağazanın adı ve hesap numarasının basılı olduğu metal anahtarlıklar

olmuştur. Bu fişler sahiplerinin meşru olarak borçlu olduğunu göstermek ve hesap numarasını hatırlamak gibi temelde iki ana amaca hizmet etmiştir. Benzer basılı bir fiş mantığı, 1914'te bir telgraf şirketi olan Western Union'da da görülmektedir. Şirket müşterilerine isimleri, adresleri ve imzalarının yer aldığı kâğıt kartlar çıkartmaya başlamıştır. Tarihteki ilk tüketici kartları olarak kabul edilen bu kartlar sahiplerinin kimliğini doğrulamak ve telgraf çekmek için kullanılmıştır. 1920'li yılların sonunda tanımlama ve kayıt tutmayı bir araya getiren *Charga-Plate* adlı yeni bir ödeme teknolojisi geliştirilmiştir. Bu sistem müşteri adı, adresi ve hesap numarasının yer aldığı kabartmalı bir metal plakadan oluşuyordu. *Charga-Plate*'ten önce müşteriler krediyle alışveriş yapmak istediklerinde mağaza çalışanları her müşterinin adını, adresini ve hesap numarasını satış fişlerine elle yazarak kayıt tutmuştur. Kartla birlikte müşterilerin kartları bir baskı makinesine yerleştirilmekte ve kabartmalı metal kart ile satış fişi arasına karbon kâğıt koyularak kopya çıkarılmaktadır. Bu teknoloji yalnızca zamandan kazanım sağlamamış, aynı zamanda tüm işlem geçmişleri ile kart sahipleri arasındaki bağlantının somut biçimde kayıt altına alınmasını temin etmiştir (Lauer, 2020: 5).

1.2.3. Postmodern Bilgisayar Destekli Gözetim Çalışmaları

Postmodern döneme ilişkin gözetim çalışmalarında bilgisayar teknolojisi merkezde yer almaktadır. Gözetim, erken modernde tamamen modern dönemde ise kısmen fiziksel biçimde birinin diğerini / diğerlerini izlediği bir işlemken bilgisayar teknolojisinin hızlı gelişimiyle soyut bir zeminde gerçekleşmeye başlamıştır. Gary T. Marx (2002) bu kapsamda gözetimi unsurlarını geleneksel ve yeni olarak sınıflandırarak bir tablo ortaya koymuştur. Tabloda hem eski hem de yeni gözetim arasındaki temel farklılıklara genel hatlarıyla yer verilmiştir.

BOYUT	Geleneksel Gözetim	Yeni Gözetim
<i>Duyu</i>	Yardımsız duyu	Daha geniş duyular
<i>Görünürlük (Kimin, nereden gözetlediği)</i>	Görünür	Az görünür veya hiç görünmez

<i>Rıza</i>	Az düzeyde gönüllülük	Yüksek düzeyde gönüllülük
<i>Maliyet (Veri başına)</i>	Pahalı	Ucuz
<i>Veri toplayanın veya analizini yapanın konumu</i>	Olay mahallinde	Uzaktan
<i>Değer sistemi</i>	Sert (Daha çok baskı)	Yumuşak (Daha az baskı)
<i>Bütünleşme</i>	Farklı aktivitelerden veri toplama	Rutin aktivitelere yerleşmiş veri toplama
<i>Veri toplayıcılar</i>	İnsanlar, hayvanlar	Makineler (kısmen veya tamamen otomatiklemiş)
<i>Verinin ikameti</i>	Toplayanlarda, yerel alanlarda	Üçüncü partilerde, genellikle uzakta
<i>Zamanlama</i>	Belirli bir noktada veya aralıklı	Sürekli, durmaksızın
<i>Zaman Aralığı</i>	Bugün	Dün, bugün, yarın
<i>Veri geçerliliği</i>	Sık sık gecikmeli	Gerçek zamanlı mevcudiyet
<i>Teknolojinin kullanılabilirliği</i>	Seçkinlere ait	Daha demokratik, bazı türleri yaygın kullanımda
<i>Veri toplamamanın nesnesi</i>	Bireysel	Bireysel, ilgiye göre kategorilendirme
<i>Kapsam</i>	Tek ölçümleme	Çoklu ölçümleme
<i>Bağlam</i>	Bağlamsal	Bağlamsız
<i>Derinlik</i>	Az yoğun	Çok yoğun
<i>Mesafe</i>	Az yaygın	Çok yaygın
<i>Gözcünün bilgisini bilenlerin oranı</i>	Daha yüksek (gözetleyen kişinin bildiğini gözetlenen de biliyor)	Daha düşük (gözetleyen, gözetlenenin bilmediği şeyleri de biliyor)
<i>Gözetim nesnesinin tanımlanabilirliği</i>	Bilinen kişiler	Bilinen kişiler dışında bilinmeyenler ve kitleler
<i>Vurgu</i>	Bireyler	Bireyler, ağ sistemleri
<i>Gerçekçilik</i>	Doğrudan temsil	Doğrudan ve simülasyon

<i>Biçim</i>	Tek medya	Çoklu medya (video ve ses de dâhil)
<i>Veriyi kim toplar</i>	Uzmanlar	Uzmanlar, öz-izleme, görev dağılımı
<i>Veri analizi</i>	Veri toplama, saklama, analiz etme ve sınıflama daha zor	Veri toplama, saklama, analiz etme ve sınıflama daha kolay
<i>Veri birleştirme</i>	Ayrık birleştirilemez veriler (farklı formatlar veya konumları nedeniyle)	Görsel, işitsel, metinsel veya sayısal verilerin kolayca birleştirilir
<i>Veri iletişimi</i>	Göndermesi ve alması oldukça zor	Göndermesi ve alması kolay

Tablo 1.3: Gözetimin Boyutları (Marx, 2002).

Marx, özetleyecek olursak yeni gözetimde duyuların genişlediğini, veri toplamanın sistematik hâle geldiğini, insandan ziyade makineler aracılığıyla ve uzaktan yapıldığını, veri bedelinin ucuzladığını, verilerin anından toplanabildiğini, sürekli veri arzının sağlandığını, yalnızca şimdi ile değil geçmiş ve gelecekle de ilgilenildiğini ve geleneksel gözetime göre daha düşük görünürlüğe sahip olduğunu (veya görünmez olduğunun) altını çizmektedir.

Yakın tarihten günümüze gözetime yönelik çağdaş teorik yaklaşımlar, çoğunluğun azınlığı, çoğunluğun çoğunluğu, bireyin bireyi, bireyin cihazları, cihazların bireyleri izlemesi gibi merkezî olmayan farklı gözetim formlarının etrafında şekillenmeye başlamıştır. Roger Clarke (1988) tarafından ortaya atılan veri gözetimi (*dataveillance*) kavramı bilgisayar destekli kişisel verilerin gözetimini içerir. Kavram, Clarke tarafından “*bir veya daha fazla kişinin hareketlerinin veya iletişiminin araştırılması veya izlenmesinde kişisel veri sistemlerinin düzenli olarak kullanılması.*” şeklinde açıklanır (a.e., s. 499). Diana Gordon (1987), devletlerin ve ticari şirketlerin elinde bulundurduğu farklı kişisel veri tabanlarının birbirleriyle bağlantıda olduğunu ve tüm toplumun elektronik panoptikon altında yer aldığına dikkat çeker. Oscar Gandy (1993), küresel kapitalist sistemde kişisel verilerin ekonomi politiğini ele aldığı çalışmada, bireyleri politik ve ekonomik tahmini değerlere göre ayırtıran süreci

panoptik sıralama olarak adlandırır. Mark Poster (1995), bilgisayar veri tabanlarının özneleri gözetlemesi ve profillemesi üzerinden süper-panoptikon kavramını geliştirir; dünyamızı saran elektrik devreleri ve telefon kablolarının süper-panoptikon olarak tabir ettiği kavramın uç noktaları olduğunu söyler. Ona göre bilgisayar veri tabanları artık panoptikonu hapishanelerden dışarı çıkarmıştır (Lyon, 2018: 234).

Bauman, sürekli değişim için olan modern dünyada gözetimin ona ayak uydurduğunu ve sürekli değişen bir karaktere büründüğünü ifade eder ve günümüz dünyasını panoptik-sonrası olarak, akışkan gözetim şeklinde tanımlar (Bauman - Lyon, 2018: 8-15). Panoptik-sonrası iktidar ilişkilerinde yönetenler bizzat kontrol kulesinde veya yakınlarında olmak zorunda değildir; istenilen zamanda kimsenin ulaşamayacağı kadar uzaklarda olabilmek özgürlüğüne sahiplerdir (Bauman, 2017: 35). Thomas Mathiesen (1997), azınlığın çoğunluğu gözetlediği panoptikonun aksine, kitle iletişim araçları ve elektronik medyanın yaygınlaşmasıyla çoğunluğun azınlığı izlediği sinoptikon kavramını ortaya atar. Kavram, gözetlenenin gözetleyene dönüşmesinin önemine dikkat çeker. Jeffrey Rosen ise panoptikonun, herkesin her zaman her yerde gözetim altında olduğu omniptikona dönüştüğünü iddia eder (Sprague, 2007:2). Armstrong ve Norris'in (1999), güvenlik kameraları incelemeleri üzerinden geliştirdiği algoritmik gözetim kavramı, veri tabanları, kameralar ve tanıma sistemlerinin birbirine bağlanmasıyla akıllı görüntü izleme, yüz tanıma veya araç plakası tanıma gibi çoğunlukla otomatik gerçekleşen işlemleri ele alır. Boyne (2000) da Bauman gibi çoğun azı izlediği çağdaş batı toplumları için panoptikon sonrası kavramını kullanır.

Marx (2002:12), yeni gözetim olarak adlandırdığı kavramı *“kişisel verileri elde etmek veya oluşturmak için teknik araçların kullanılması”* olarak açıklar ve günlük yaşamdaki teknolojik olmayan gözetimi kavramın kapsamı dışında tutar. Pecora, (2002), *“Biri Bizi Gözetliyor”*, *“Survivor”* gibi televizyon programlarının gözetimin disipline edici, düzen sağlayıcı yapısını kırarak eğlenceli bir arzu nesnesi hâline dönüştürdüğünü; dolayısıyla gözetimi evcilleştirdiğini öne sürer. Lyon (2003:14-15), günümüze ait gözetimin sınıflandırma dürtüsünü vurguladığı *sosyal sınıflandırma* ile insan hayatının veri tabanlarında sosyal ve kişisel kategoriler hâline geldiğinin üstünde

durur. Gözetlemeye karşı bir kavram olarak çıkan ters gözetim (*Sousveillance*) ise, gözetimin toplumu tepeden izleyen anlayışının aksine insanların yönetim organlarını aşağıdan izlemesi anlamına gelmektedir; kameralar aracılığıyla izleyenleri izlemenin bir direniş biçimi hâlini almasıdır (Mann, 2004). Wood ve Graham (2003), Marx'ın yeni gözetimi bağlamında dijital teknoloji ve tekniklerin gelişimiyle ortaya çıkan dijital gözetimi toplumsal etkileri üzerinden inceler.

Siva Vaidhyanathan'ın (2011; 2018: 67) ortaya attığı kriptoptikon kavramı, devasa şirket ve devlet gözetiminin gizemli bir bilgi ekosistemini ifade eder ve Bentham'ın panoptikon kavramından ayrılır. Kriptoptikon tarayıcı çerezlerine, telekomünikasyon firmaları tarafından tutulan veri akışlarına, uydu görüntülerine, küresel konum sistemlerine, gizli ses kayıtlarına, mağaza indirim kartlarına ve mobil uygulamalara dayanmaktadır. Doucek vd (2018), insana değil nesnelerle ilgili verilere odaklanmış, sistematik ve rutin bir dikkat anlamına gelen Nesnelerin Gözetimi (SoT) kavramını geliştirir. Her biri veri toplama amacını maskenin ardında bırakmaktadır. Bentham'ın panoptikondaki mahkûmlarının aksine kullanıcılar izlendiklerinden veya profillerinin çıkartıldığından haberdar değildir. Son yıllarda kavramsallaşan bir başka gözetim yaklaşımı, bilgi kapitalizminin bir uzantısı olarak tanımlanan gözetim kapitalizmidir (Foster & McChesney, 2014; Zuboff, 2015; 2019). Gözetim kapitalizmi, her türlü insan deneyimini verilere; verileri ise kâra dönüştürme amacıyla yapılan gözetim faaliyetlerini içermektedir.

Gözetim Çalışmaları & Kavramlar	Yazarlar
Disiplin toplumu	Foucault (2015; 2019)
Gözetim toplumu	Marx (1985)
Elektronik panoptikon	Diana Gordon (1987)
Veri gözetimi	Roger Clarke (1988)
Denetim toplumu	Deleuze (1992)
Panoptik sıralama	Oscar Gandy (1993),
Süper-panoptikon	Mark Poster (1995)
Sinoptikon	Thomas Mathiesen (1997)

Omnitikon	Jeffrey Rosen (2004)
Algoritmik gözetim	Armstrong ve Norris (1999)
Gözetim topluluğu	Haggery ve Ericson (2000)
Panoptikon-sonrası	Boyne (2000), Bauman (2017)
Yeni gözetim	Marx (2002)
Sayısallaştırılmış gözetim	Wood ve Graham (2003)
Sosyal sıralama olarak gözetim	Lyon (2003)
Akışkan gözetim	Bauman & Lyon (2018)
Ters gözetim (<i>Sousveillance</i>)	Mann (2004)
Üretketici kapitalizmi	Ritzer & Jurgenson (2010)
Web 2.0 gözetimi	Fuchs (2011)
Gözetim kapitalizmi	Foster & McChesney (2014), Zuboff (2014; 2019)
Kriptoptikon	Vaidhyathan (2011; 2018)
Nesnelerin Gözetimi (SoT)	Doucek vd. (2018)
Elektronik izleme	Daems (2019)

Tablo 1.4: Postmodern Dönemdeki Başlıca Gözetim Çalışmaları
(Kaynak: Yazar).

1.2.3.1. Erken Dönem Veri Gözetimi ve Veri Tabanı Pazarlaması

Roger Clarke (1988: 499) veri gözetimi kavramını bireylerin veya grupların davranış veya iletişimlerinin takip edilmesi veya araştırılmasına kişisel veri sistemlerinin rutin olarak kullanılması olarak ifade etmektedir. Bu tanım şu ipuçlarını barındırmaktadır: (1) birey veya grupların hareketleri takip edilmektedir, (2) takip sonucu toplanan kişisel veriler, veri sistemlerinde (veri tabanlarında) saklanmaktadır ve (3) gerektiğinde veri sistemleri taranarak kişisel veriler gün yüzüne çıkarılmaktadır. Elektronik gözetim kişisel deneyimlerin, davranışların ve iletişimsel faaliyetlerin verilere dönüşmesini sağlamıştır. Bununla beraber geleneksel gözetimin “şimdi ve burada” gerçekleşmesi yerini “her an her yerdeliğe” bırakmıştır. Veri gözetimine kaynak sağlayan veri tabanları başta bilgisayar teknolojisinin gelişimi ve gözetimin

teknolojik ilerlemelere entegre olmasıyla büyük miktarda veriye sahip olmuştur. Bir şirketin bireysel tüketiciler, vatandaşlar ve müşteriler hakkındaki bilgileri veri tabanlarında kontrol altında tutabilmesi ve istediği zaman kullanabilmesi ona 80'li yıllara kadar petrol şirketlerinin sahip olduğu kaynak temelli güce benzer bir güç sağlamıştır (Lace, 2005: 17). Bugün veri tabanları birçok kaynaktan beslenerek büyümeye devam etmektedir. Ferguson bu kaynakları ve günümüz veri gözetim türlerini şu şekilde sıralamaktadır (2017:173-178):

(1) Perakende gözetimi: Müşterilerin satın alma alışkanlıklarını inceleyerek geleceği tahmin etmeye yöneliktir. Sadakat kartları bu alışkanlıkları izlemek ve başkalarının alışverişleriyle kıyaslayarak çıkarımda bulunmak için kullanışlı araçtır.

(2) İnternet gözetimi: Arama yapılan anahtar kelimeler, web gezinimleri, çevrimiçi alışverişler, fare hareketleri, klavyede yazılanlar, kaydırmalar, kaçınmalar, epostalar, yol tarifleri, uçak biletleri, otel rezervasyonları vb. tüm çevrimiçi hareketlerin izlenmesini içerir.

(3) Sosyal medya gözetimi: Facebook, Twitter ve Instagram vb. platformlarda üretilen içerikler, mesajlaşmalar, beğeniler, favoriler, kaydedilenler, yorumlar, tıklamalar, etiketlemeler, paylaşımlar ve yüklenen fotoğraflar gibi içeriklerin takibidir.

(4) Veri şirketleri: Yeni dijital ekonominin merkezinde yer alan veri şirketleri, çeşitli kamu ve özel kuruluşlardan topladıkları verilerle kategorilere ayrılmış büyük çapta insan profillerine sahiptirler. Bu verileri ticari bir öge olarak alıp satarlar.

(5) Sensör gözetimi: “Nesnelerin interneti” kavramını karşılayan tüm akıllı cihazlar sensör aracılı gözetimin araçlarıdır. Akıllı ev aletleri, televizyonlar, mikrodalga fırın, kol saati, araba vb. tüm araçlar günlük kişisel eylemleri kayıt altına alarak kişiler hakkında daha fazla bilgi toplamaktadır.

(6) Finansal gözetim: Finansal kredi derecelendirme raporlarını içeren finansal gözetim, şirketlerin bireysel kredi riskini azaltmaya yönelik topladıkları verileri oluşturur. İstihdam, net gelir, fatura ödeme alışkanlıkları vb. geleneksel yöntemlerin yanında örneğin “koltuğunun ayaklarının altına keçe koyanların” kredilerini düzenli ödeme eğilimlerinin daha iyi olacağı tahminleri de yürütmektedirler.

(7) Siyasi gözetim: Siyasi partiler ve liderler, özellikle seçim kampanyalarında çeşitli kategoriler belirleyerek o gruplara hedefli reklamlar çıkarmakta ve onlara özel kampanyalar üretmektedir. Veri toplama süreçlerinde birey ve ailelerin siyasi eğilimleri, ilgi alanları ve çevreyle ilişkilerine dikkat edilerek destek talep edilir.

Veri gözetimi, tüketici davranışını öngören ve yönlendiren sonuçları hedefler ve pazar ile tüketici ilişkisi için engin sonuçlar önerir (Ruckenstein - Granroth, 2019). Erken dönem veri gözetimini incelendiğinde tüketiciler hakkında bilgi toplamak ve onları belirli sınıflar altında kategorilendirmek karşımıza çıkmaktadır. Özellikle reklam ve pazarlama faaliyetlerinde tüketicilerin sınıflaması ve hedeflenmesi 20. yy’nin ikinci yarısından itibaren hız kazanmıştır. Bilgisayar teknolojisinin pazarlama endüstrisine girişi müşteri bilgilerinin kaydedildiği metal kart ve kalıpları (*Charga-Plate* örneğindeki gibi) ortadan kaldırmış; dahası istatistiksel modelleme, birleştirme, temizleme, kişiselleştirme, tarama gibi birçok yeniliği beraberinde getirmiştir (Peterson vd., 1993: 30). Teknolojinin reklam ve pazarlama alanına hızlı adaptasyonu ile “bireysel hedefleme” ve “ihtiyaca yönelik pazarlama” gibi kavramlar ortaya çıkmıştır. Bu durum tüketicilerin gündelik yaşamlarının baskı ve iktidar kurmaktan ziyade pazarlama ve ticari amaçlı izlenmesine yol açmıştır. Örneğin, 1970’li yıllara kadar kredi kartı şirketleri gerek teknik imkânsızlıklar gerekse ihtiyaç duyulmadığı için kart sahipleri hakkında neredeyse hiç işlem verisi tutmamıştır. Teknolojik gelişmelerin 1980’li yıllarda daha baskın biçimde kendini hissettirmesi ve kredi kartı işlem geçmişinin bir meta/varlık olarak kabul edilmesi birbiriyle paralel biçimde gerçekleşmiştir. American Express’in kredi kartı faturalama işlemlerini elektronik ortama taşıması ile kart sahiplerinin alışveriş verileri bir araya getirilmiş ve pazarlama

veri tabanların oluşmasına önayak olmuştur (Lauer, 2020). 1990’larla beraber ise özel sektöre ait kişisel veri tabanları hızla gelişerek kişisel veriler sektörleri arası alışveriş nesnesi hâline dönüşmüştür (Lyon, 2018: 90-91).

Bilgisayar ve veri tabanı teknolojisindeki gelişmelerin devamında ortaya çıkan veri tabanı pazarlaması pazarlama verimliliğini arttırmak için müşteri veri tabanlarının kullanılması olarak tanımlanmaktadır (Blattberg vd., 2008: 3). Veri tabanı pazarlaması bilgisayar destekli tüketici gözetiminin ilk aşaması olarak kabul edilmektedir (Lyon, 2013: 69). Veri tabanının yapı taşı müşteri bilgi dosyasıdır. Bu dosya müşterinin adı, adresi, telefon numarası, demografik özellikleri, yaşam tarzı, alışveriş geçmişi ve çevresindeki kişilerden elde edilebilecek her türlü veriyi içermektedir (Blattberg vd., 2008: 183). Bu noktada kişisel veri gözetimi devreye girmektedir. Veri tabanında bulunan veriler iki kaynak aracılığıyla toplanmaktadır: dâhili ve harici kaynaklar. Dâhili kaynaklar şirketlerin kendi müşterilerinden topladıkları verilerdir. Tutulan kayıtlar, faturalar, garanti formları, promosyon kodu kullanımı vb. verilerden oluşur. Bu bağlamda veri tabanı pazarlamasının özellikle çok sayıda müşteriyle içli dışlı olan ve onların işlem verisini kayıt altına alan perakende satış yapanlar, finansal hizmetler ve telekomünikasyon gibi sektörlerde başarılı olması beklenmektedir (Anić, 2015). Müşteri hakkında daha fazla veri toplamak isteyenler ile müşteriyle doğrudan teması olmayan şirketler harici kaynakları kullanmaktadır. Bunlar arasında ücretsiz ödül çekilişleri, yarışmalar, doldurulan formlar, garanti kayıtları, kredi kartı işlem verileri yer almaktadır. Sözü edilenlere ek olarak *“Yaşam tarzı veri tabanı”* olarak adlandırılan listeler şirketlere finans, eğlence ve paketli ürün gibi belirli sektörlerle ait mallardan satın almış kişilerin listelerini satmaktadır (Tapp vd., 2013: 38-39). 1980’li yıllarda İngiltere’de ortaya çıkan yaşam tarzı veri tabanlarında alışveriş alışkanlıklarından sağlığa araç kullanımından tatil tercihlerine kadar birden çok sorunun yer aldığı anketlerin cevapları saklanmaktadır (Harris, 1998). İnternet öncesi dönemde kişisel verilerin ve veri tabanlarının pazarlama faaliyetlerindeki önemi, sektörün tüm alanlardan veri elde etme ve yeni kaynaklar ortaya çıkarma yarışını hızlandırmıştır.

1990’lı yıllarda veri gözetimine ilişkin en yenilikçi çözümler arayan ve aktif biçimde veri talep eden gruplar arasında perakende satış yapan firmalar gelmiştir.

Özellikle gıda perakendecileri, müşteri verilerini toplamak için diğer perakende satış yapan firmalara nazaran ortalama iki kat daha fazla bütçe ayırmıştır. 1996 yılında KPGM'nin 10 ülkeden 140 perakendeciyle yaptığı ankette bu firmaların %61'inin müşteri veri tabanına sahip olduğu, kalanların ise en kısa sürede çalışmalara başlamaya niyetli oldukları tespit edilmiştir. Veri tabanına sahip olanların %86'sı, sistematik bir gözetim aracı olan sadakat kartlarını kullanarak müşteri alışveriş verilerinin kayıt altına alındığını belirtmiştir (Boyne, 2000: 296). Sadakat kartları aracılığıyla perakendeciler tüketicilerin geride bıraktıkları izlere dayanarak alışveriş alışkanlıklarını takip etmiş, onların "ihtiyaçlarını" karşılamak için geliştirmelerde bulunmuş ve stoklarını buna göre güncelleme imkânı bulmuştur (Smith - Sparks, 2003). Birleşik Krallık'ın en ünlü perakende market zincirlerinden Tesco'nun 1995 yılında piyasaya sürdüğü *Clubcard* isimli sadakat kartı, gerek yenilikçi fikirleri gerekse müşteri verilerini toplamadaki gücüyle büyük ses getirmiştir. Tesco, Clubcard aracılığıyla tek kalem bir ürüne kadar veri toplayabilmekte ve sonrasında her ürünü bireysel olarak her bir müşteriyle eşleştirebilmektedir. Ayrıca kart başvurusunda müşterinin hane içi bilgileri ve mesleği gibi kişisel verileri de toplamaktadır. Elde ettiği tüm veriler neticesinde büyük bir veri yığını inşa eden Tesco, müşterilerini sınıflandırmaya dahi yönelmiştir. "Bekâr yetişkinler", "emekliler", "şehirde çalışanlar" gibi demografik sınıfların yanı sıra "fiyat duyarlılığına sahip olanlar", "yemek meraklıları", "sadık olanlar" gibi alışkanlıklara yönelik sınıflandırmalar oluşturulmuştur (Tapp vd., 2013: 92). 2001 yılına gelindiğinde Clubcard sahibi tüketici sayısı yalnızca Birleşik Krallık'ta 10 milyondan fazlası aktif olmak üzere 20 milyonu bulmuştur (Law, 2008: 23). Kredi kartlarından sonra sadakat kartlarının da "plastik gözetim"⁵ aracı olarak kullanılmaya başlaması özel sektörün veri gözetimindeki yerini kuvvetlendirmiştir.

Kişisel veri gözetimi yalnızca perakende ürün satan firmaların, telekomünikasyon, banka veya finans sektörünün değil, teknoloji üreticilerinin de radarına girmiştir. Üstelik bu durum bizzat teknolojinin donanımına eklenen bir tür "casus parça" ile denenmiştir. Dolayısıyla bu yönüyle internet gözetiminden tamamen

⁵ (Lauer, 2020).

farklı bir gözetim yöntemi taşımaktadır. 1999'un başlarında Intel, kendi ürünü olan Pentium III işlemcisinin içine eşsiz bir kimliğe sahip bir çip yerleştirme planı yapmıştır (Lyon, 2018: 209). Bu çip yalnızca Intel'in kendi web sunucularında okunabilecek bir özelliğe sahip olacak biçimde tasarlanmıştır. Elektronik gözetime ilişkin yeni bir yaklaşım sunan işlemciye entegre edilmiş çipler, kişisel bilgisayarları sahipleriyle eşleştirerek onlar hakkında Intel'e veri transferi sağlama amacı taşımıştır (Jones, 1999). O dönem işlemci pazarının %75'inden fazlasını elinde bulunduran Intel'in tüm bilgisayarlara "casus" yerleştirme planları dönemin gizlilik hakları savunucularının tepkileri sonrası rafa kaldırılmıştır. Böylece Intel'in kişisel bilgisayarlardan mikroçip aracılığıyla çevrimiçi ve çevrimdışı veri toplama gayesi sonlanmıştır.

1.3. Bilgi / Enformasyon Toplumu

1956 yılında ABD'de beyaz yakalı çalışanların mavi yakalıları sayısal olarak ilk defa geçmesi yeni bir toplumun ortaya çıkmasına önayak olmuştur (Alakuş, 1991: 7). Buradan hareketle "bilgi işi", "bilgi işçisi", "bilgi ekonomisi" terimleri ve "bilgi toplumu" kavramı 1960'lı yılların sonunda Peter F. Drucker (1993: 16), "enformasyon toplumu" kavramı Fritz Machlup tarafından bilgi ve hizmet sektörünün yükselişini vurgulamak için kullanılmıştır. Enformasyon toplumu, *"bilginin ekonomik, sosyal, kültürel ve siyasi yaşamın her alanında yoğun bir biçimde kullanıldığı"* bir toplumdur (Moore, 1998: 274). Alvin Gouldner'a göre gelişmiş toplumlarda kültürel sermayesi yüksek, zihinsel bir beceriyle çalışarak hayatını idame ettiren ve yükseköğrenimli bir sosyal sınıfla birlikte ortaya çıkmıştır (Dura - Atik, 2002: 39). Masuda'ya göre ise enformasyona sahip olmanın, dönüşümün ve bireyin entelektüel yaratıcılığının gelişiminin kaynağı ve itici gücü olduğu yeni bir toplum türüdür (Z. Karvalics, 2007: 34). 1993'ün sonunda kurulan Bangemann Grubu, Avrupa Birliği Konseyine "Avrupa ve Küresel Enformasyon Toplumu" başlıklı bir rapor hazırlamıştır. Rapor, Avrupa Birliği ülkelerinin iletişim ve teknolojik gelişmelerde geride kalmaması adına bir dizi öneri içermektedir. Raporda enformasyon toplumuna ilişkin şu ifadeler yer almaktadır:

"Tüm dünyada bilgi ve iletişim teknolojileri, geçmişte olanlar kadar önemli ve geniş kapsamlı yeni bir endüstri devrimi yaratıyor. Bu, bilgiye dayanan bir devrimdir ve insan bilgisinin ifadesidir. Teknolojik ilerleme artık

enformasyonu sözlü, yazılı veya görsel olarak, mesafe, zaman ve hacim kısıtlamaları olmadan işlememize, depolamamıza, geri almamıza ve iletmemize olanak tanıyor. Bu devrim, insan zekâsının kapasitesini genişletiyor ve birlikte çalışma biçimimizi ve yaşama şeklimizi değiştiren bir kaynak sağlıyor.” (Bangemann Group, 1994).

Türkçe karşılıklarına bakıldığında bilgi toplumu “knowledge society”ye, enformasyon toplumu ise “information society”ye atıfta bulunmaktadır. Oysaki *information* kelimesinin Türkçe karşılığı alanyazında sıklıkla *bilgi* olarak karşımıza çıkmaktadır. Çakır (2018: 22), bilginin “işlenmiş, sınanmış, seçilmiş, tanımlanmış” bilgi gruplarını; enformasyonun ise “işlenmemiş bilgi, yorum, düşünce, yaklaşım, haberleri” nitelediğini ve içerdiğini ifade etmektedir. Diğer bir ifadeyle enformasyon, işlenmiş verilerin belirli bir bağlamda okunmasıyla ortaya çıkan değerdir. Bir düzen hâline getirilmiş verilerdir. Bilgi sözcüğü iki anlam taşımaktadır; ilki, bir konuyla ilgili fikir sahibi olmak ve konuyu anlamakla ilişkilidir. İkincisi, fikir ve durumları ortaya koyan, bir kişiden diğerine aktarılabilen veri ve belgelerdir (Alakuş, 1991: 5). Kısacası bilginin, öğrenme ve algılama yoluyla çeşitli fikir, düşünce ve problemler hakkında oluşan farkındalık ile oluştuğu söylenebilmektedir. Karar alma süreçlerinde öğrenme, içgörü, algı ve deneyim ön plandadır. Bilgi toplumu ve enformasyon toplumu kavramlarının ortak özelliği enformasyonun niteliğine yaptığı vurgudur. Her iki kavram da modern toplumda bilgi ve enformasyonun önemi üzerinde durmaktadır (Gezmen, 2019: 427). Bu başlık altında alıntı yapılan yazarların kendi çevirilerine, tanımlamalarına ve İngilizce çevirilerde kullanılan terimin birebir çevirisine özen gösterilerek “bilgi toplumu” ve “enformasyon toplumu” kavramları ayrı ayrı tercih edilmektedir.

Sanayi devriminden önce toplumların zenginliği sahip oldukları denizler, yeryüzü ve yer altı kaynakları ile ölçülmüştür. Sanayileşme ile birlikte doğadan elde edilen hammaddelerin fabrikalarda işlenmesi ekonomik gücün kaynağını belirgin olarak değiştirmiştir. Bilgi çağı olarak tabir edilen sanayi sonrası ise iletişim teknolojilerinin merkezde olduğu ve bilginin bizzat kendisinin toplumsal zenginliğe kaynak oluşturduğu bir döneme işaret etmektedir (Alakuş, 1991: 6-7). Drucker (1993: 17 - 18), temel ekonomik kaynağın ne sermayenin sahip olduğu üretim araçlarında, ne

doğal kaynaklarda ne de emekte olduğunu; servet yaratan faaliyetlerin kaynağının artık bilgi olduğunu ve bilgi olacağını ifade eder. Ona göre bilgi çalışanları kapitalist sistem tezahüründeki işçilerden farklı olarak “üretim araçlarını” ve “üretim olanaklarını” elinde bulunduracaktır. Bilgi toplumunda servet sahipleri çelik üreticilerinden değil, TV programcıları, bilgisayar üreticileri, yazılımcılar gibi enformasyona dayalı işler yürüten kurum ve şirketlerden oluşmaktadır. Yirminci yüzyılın ikinci yarısı boyunca ekonominin merkezinde yer alan sanayiler, malların üretimi ve dağıtımıyla ilgili değil, bilgi ve enformasyonun üretimi ve dağıtımıyla ilgilidir (Drucker, 1993: 254).

Z. Karvalics (2007), enformasyon ve bilgi toplumlarının oluşumuna ilişkin temel kategorileri, kategorilerin toplum içindeki olması gereken düzeyleri ve bunlara ait kavramsal metaforlara yer vermektedir.

Temel kategori	Ölçülebilirlik	Metafor
Üretim	Enformasyon sektörünün bir parçasını oluşturan ve diğer sektörlerle ilişkili olarak enformasyon ve bilgi ürünleri üreten işletmelerin miktarı	<i>Enformasyon toplumu, bilgi toplumu, bilgi ve enformasyon endüstrisi, enformasyon ekonomisi, bilgiye dayalı ekonomi</i>
İstihdam	Diğer sektörlerle ilişkili olarak bilgi ve enformasyon sektörlerindeki çalışanların sayısı ve oranı	<i>Beyaz yakalı işçiler, bilgi ve enformasyon işçileri, maddi olmayan işçiler, bilgi sınıfı aydınları</i>
Çalışma	Yapılan işin türüne göre kaç kişi ve ne ölçüde "meslek olarak" enformasyon faaliyetlerinde bulunmaktadır?	<i>Zekâ – beyin işçisi, zihin çalışanı</i>
Kaynak ve teknoloji	Bilgi ve enformasyon geleneksel yöntemlere ek olarak kaynak ve sermaye biçimleri olarak görülür.	<i>Entelektüel sermaye, insan sermayesi, enformasyon sermayesi, kurumsal bilgi ve enformasyon varlıkları</i>
Gelir ve refah	Olması gereken miktarla ilgili kabul edilmiş ortak bir değer olmamakla	<i>Bolluk ve refah devleti</i>

	birlikte ulusal düzeyde Gayri Safi Milli Hâsıla, bireysel düzeyde ise aylık gelirle ilişkilidir.	
Tüketim	Tüketici sepetinde yer alan enformasyon, kültürel ürün, araç ve hizmetler	<i>Tüketim toplumu, üretüketiciler, medyatik toplum</i>
Eğitim (Eğitim seviyesi)	Toplumda yükseköğrenim görmüş kişilerin oranı	<i>Öğrenen toplum, meritokrasi</i>
Kavrama	Kavrama yeteneğinin ölçülebilir boyutlardaki sonuçları; mikroskobik boyutlar, astronomik uzaklık ve ölçüler, keşfedilen gen kombinasyonlar, işaret işleme vb.	<i>Yaşam boyu öğrenme, bilimsel devrim, nano ölçeği, peta ölçeği</i>
Anlaşmazlık yönetim usulleri ve güç kullanma	Ekonomik çatışmaları iş zekâsı, yenilikçi rekabet anlayışı gibi bir enformasyon bağlamına taşıyarak geleneksel savaş türlerinin değişime uğraması.	<i>Enformasyon savaşı, siber savaşlar, ticari istihbarat, bürokrasi, risk toplumu</i>
Birbirine bağlılık	Karşılıklı bağlılık derecesi.	<i>Telematik toplum, kablolu toplum</i>
Dünya görüşü ve mantıksal çerçeve	Enerji merkezli dünya görüşünün yerini enformasyon merkezli dünya görüşünün alması, geleceğe yönelik çalışmaların temel bir özellik olması ve küresel sistem seviyelerinin ve uzay çağı anlayışının analiz ve yorumlar için temel bir çerçeve hâline gelmesi.	<i>Küresel köy, teknokültür, enformasyon uygarlığı</i>

Tablo 1.5: Enformasyon Toplumunun Temel Kategorileri, Ölçülebilirliği ve Metaforları (Z. Karvalics, 2007: 33-34).

Z. Karvalics, özellikle metaforlara dikkat çekerek enformasyon ve bilgi toplumu kavramının diğer kavramlarla çatışan değil, aksine onları da içine alan çatı bir kavram olduğunu ifade etmektedir.

Bilgi toplumu, enformasyon toplumunun gelişimi sonucunda ortaya çıkmıştır. Enformasyon toplumunun bilgi toplumuna dönüşümü teknolojik araçlar ve işlevsel araçlar olarak iki kategoride toplanmıştır (Filip, 2002'den akt. Steliac vd., 2012):

Teknolojik birimler	İşlevsel birimler
İnternet	Ekonomik araçlar için bilgi yönetimi
e-kitap teknolojisi	Küresel çapta bilginin ahlaki kullanımının yönetimi
Akıllı araçlar (Yapay zekâyla donatılmış sistemler)	Biyolojik ve genomik bilgi
Çevrenin insan faaliyetleri için akıllıca kullanımı	Sosyal ve bireysel düzeyde sağlık sistemi
	Çevreyi koruma ve sürdürülebilir bir toplum sağlama
	Varlık hakkında daha derin bir bilgi
	Yeni bir teknolojik bilgi üretme
	Yeni bir bilgi ve yenilik kültürü geliştirme
	e-Öğrenme sistemi geliştirme

Tablo 1.6: Bilgiye Dayalı Toplumun Temel Birimleri
(Filip, 2002’den akt. Steliac vd., 2012).

Moore (1998:271-272), enformasyon toplumlarının temel özelliklerini üçe ayırmaktadır. Buna göre enformasyonun ilk özelliği, ekonomik bir kaynak olarak kullanılmasıdır. Şirketler, kurum ve kuruluşlar yeniliği teşvik etmek, verimliliklerini / ürettikleri ürün veya hizmet kalitesini arttırmak ve rekabet ortamında avantaj sağlamak için enformasyonu daha fazla kullanırlar. İkinci özellik, toplumun enformasyonu eskiye göre daha fazla kullanmasıyla ilişkilidir. İnsanlar artık tüketim faaliyetlerinde enformasyona daha yoğun bir talepte bulunmaktadır. Farklı ürünler arasında bilinçli seçimler yapmak, çeşitli hizmetleri karşılaştırmak, vatandaşlığa bağlı hak ve sorumluluklarının farkına varmak; kısacası insanlar, kendi hayatlarında daha güçlü biçimde söz sahibi olmak için enformasyona başvururlar. Son özellikte ise ekonomi içinde gelişen bir enformasyon sektörünün altı çizilmektedir. Buradaki anlamıyla enformasyon sektörünün büyük bir kısmı telekomünikasyon ve bilgisayar ağları gibi teknolojik altyapılarla ilgilidir. Neredeyse tüm enformasyon toplumlarında enformasyon sektörü genel ekonomiden daha hızlı büyümektedir. Moore, bu

özelliklerle enformasyon toplumlarında bilginin hem şirketlerin hem de bireylerin kendilerini geliştirmesi, iyileştirmesi ve bilinçlenmesi için kullanıldığını ifade etmektedir. Ayrıca, ülke ekonomisindeki enformasyon sektörünün kayda değer yükselişinin “enformasyon toplumu” olmadaki önemine yer vermektedir.

Sanayi üretiminin azalması ve enformasyonun artması ile toplumların ekonomik ve sosyal bağlamda uğradığı dönüşümün ele alındığı ve Daniel Bell tarafından “Sanayi sonrası toplum” olarak nitelenen yeni toplumsal yapı, enformasyon toplumuyla paralel bir anlama sahiptir. Bell’e göre kol gücüne dayalı mavi yakalı sanayi sektörünün öneminin azalması ve enformasyona ve hizmete dayalı sektörlerin gelişimi ve artışı ekonomik ve toplumsal zeminde değişimler meydana getirmiştir. Sanayi sonrası toplum, hayat standartlarının üst seviyelere çıktığı, gelir adaletsizliklerinin azaldığı, verimliliğin arttığı, enformasyonun çoğaldığı ve akışının hızlandığı; geleneksel anlayışın temsil ettiği zaman ve mekân algısının değiştiği bir toplumu işaret etmektedir (Çakır, 2018: 26).

Daniel Bell (1976: 576), modern zamanlardan yüz yıl önce başlayan, tarımdan sanayiye, kırsaldan kente doğru gerçekleşen hareketleri ilk büyük değişim; içinde bulunan, sanayi toplumundan sanayi sonrası topluma geçişi ise ikinci büyük değişim olarak ele almaktadır. Küresel çapta örnekler vererek toplumları sosyo-ekonomik özelliklerine göre sanayi öncesi, sanayi ve sanayi sonrası olarak üç kategoride incelemektedir.

Boyutlar	Sanayi Öncesi	Sanayi	Sanayi Sonrası
<i>Üretim biçimi</i>	Doğal maddelerin işlenmesi	Fabrika	İşleme, yeniden işleme
<i>Ekonomi sektörü</i>	Tarım, madencilik, balıkçılık, kereste, gaz ve petrol	Meta üretimi, imalat, dayanıklı ve dayanıksız tüketim malları, inşaat sanayi	Hizmetler, taşımacılık, sigorta, gayrimenkul, sağlık, eğitim, araştırma
<i>Dönüştürülen kaynak</i>	Doğal rüzgâr – su gücü, çeki	Yaratılan enerji, elektrik, petrol,	Bilgi, bilgisayar ve veri iletim sistemleri

	hayvanları, insan gücü	gaz, kömür, nükleer güç	
<i>Stratejik kaynak</i>	Hammadde	Finansal sermaye	Bilgi
<i>Teknoloji</i>	El sanatları	Makine teknolojisi	Entelektüel teknoloji
<i>Temel beceri</i>	Zanaatçı, el işçisi, çiftçi	Yarı vasıflı işçi, mühendis	Bilim insanı, teknik ve profesyonel meslekler
<i>Yöntem</i>	Sağduyu, deneme-yanılma, tecrübe	Deneycilik	Soyut teoriler, modeller, simülasyonlar, analizler
<i>Zaman perspektifi</i>	Geçmişe yönelik	Geçici adaptasyon	Geleceğe yönelik: öngörü ve planlama
<i>Düzen</i>	Doğaya karşı oyun	Fabrikalaşmış doğaya karşı oyun	Bireyler arası oyun
<i>Eksen ilke</i>	Gelenekçilik	Ekonomik büyüme	Teorik bilginin kodlanması

Tablo 1.7: Daniel Bell'e Göre Enformasyon Toplunun Boyutları (Z. Karvalics, 2007: 35).

Sanayi öncesi toplumların işgücünün yarısından fazlası madencilik, balıkçılık, ormancılık ve tarım gibi sektörlerde çalışmaktadır. İş, kol gücüyle icra edilir ve kuşaktan kuşağa aktarılır. Bu toplumlarda geniş aile yapısı hâkimdir; çocuk, ekonomik bir değer olarak görülür. Sanayi toplumları somut bir mal üreten toplumlardır. Teknik ve makineleşme yaygındır. Enerji, üretkenliğin temeli olmuştur ve kas gücünün yerini almıştır. Sanayi sonrası toplum ise hizmete dayalıdır; önemli olan ne enerji ne de kas gücüdür; önemli olan enformasyondur (Bell, 1976: 576). Bell, sanayi sonrası toplumda eşitsizliklerin azaldığını ve refahın yükseldiğini, yetenekli mühendis ve teknisyen sınıfının yaratıldığını, kaynakların en az maliyet ve emekle kullanıldığını ve verimliliğin arttığını, birçok alanda küreselleşmenin etkisini gösterdiğini ve yüksek miktarda enformasyonun hızlı biçimde hareket etmesiyle uzay / zaman arasında bozulmalar yaşattığını dile getirerek iyimser bir bakış açısına sahip olmuştur (Laughey, 2010: 107-108).

Japonya’da bilgisayarların yaygınlaşmasında öncü isimlerden birisi olan Yoneji Masuda, 1980 yılında yayımlanan “*Sanayi Sonrası Toplum olarak Enformasyon Toplumu*” adlı eseriyle enformasyon toplumu kuramcılar arasında önemli bir yer edinmiştir. Masuda (1981: 29), sanayi toplumundan tamamen farklı yeni bir tür olarak tanımladığı enformasyon toplumunda, toplumun oluşumu ve gelişimindeki itici gücün “*maddi değerlerle değil, enformasyonel değerlerin üretilmesiyle olacağını*” söylemektedir. Yanı sıra, sanayi toplumlarındaki en önemli şey olan maddi tüketimin yerini enformasyon toplumlarında bireylerin bilişsel yaratıcılığına bırakacağını dile getirmektedir. Enformasyon toplumu ile küresel ve geleceğe odaklanan bir toplum yapısı oluşacak; sanayi toplumundaki maddi değer ve tüketimin önemi azalarak, enformasyonun değeri ve sermayesi ekonomide kayda değer bir yere sahip olacaktır. Masuda’nın “Computopia” adını verdiği ve teknolojinin / bilgisayarın merkezde konumlandığı bu toplum, kendi geleceği hakkında kararlar verebilecek, ihtimallerin peşinden gidebilecek, kendi gayesi doğrultusunda kendi geleceğini inşa edebilecektir (Masuda’dan akt. Çakır, 2018: 37).

Masuda’ya göre (1981: 32) sanayi toplumunun ekonomik yapısı (1) satış odaklı bir meta ekonomisi, (2) iş bölümlerini kullanarak üretimin uzmanlaşması, (3) işletmeler ve hane halkı arasında tam üretim ve tüketim bölümleri ile nitelenmektedir. Enformasyon toplumunda ise (1) sosyo-ekonomik kalkınmanın ekseni olan enformasyon, bilişim hizmeti ile üretilecek, (2) enformasyonun bireyler tarafından kendi kendilerine üretimi artacak ve enformasyon çoğalacak, (3) çoğalan enformasyon iş birliği şeklinde üretilerek ve ortak kullanılarak daha da genişleyecek ve (4) ekonomi, yapısal olarak mübadele (değişim) ekonomisinden işbirliği ekonomisine doğru değişim yaşayacaktır.

Enformasyon toplumuna ilişkin en etkili yaklaşımlardan bir diğeri enformasyon çağını “üçüncü dalga” olarak nitelendiren Alvin Toffler’dır (2008). Toffler, tarım toplumunu birinci dalga, sanayi toplumunu ikinci dalga olarak tanımlarken içinde bulunan enformasyon toplumunun üçüncü dalga olarak temsil edildiğini belirtmektedir. On bin yıl önceki insanlığın tarihini değiştiren tarımsal devrimin ve 18. yy’daki sanayi teknolojilerinin gelişimiyle yaşanan sanayi devriminin

birinci ve ikinci dalgayı ortaya çıkması gibi, bilgi ve iletişim teknolojilerinin yaygınlaşması ve kendini sürekli geliştirmesi üçüncü dalgayı yaratan itici güç olmuştur. Üçüncü dalgada yeni sanayilerin “bilgisayarlarla, elektroniğe, enformasyona, biyoteknolojiye ve bu gibi şeylere” dayalı olarak gelişeceğini söyleyen Toffler, üçüncü dalga ekonomisinin süper hızlı olduğunu ve tüm şirketlerin yeni teknolojilere yüksek miktarda yatırım yapması gerektiğini vurgulamaktadır (Toffler, 1992: 68-69). Toffler, ikinci dalgadaki egemen kitlesel sanayi üretiminin üçüncü dalgayla birlikte değişerek bireysel, yerel ve daha küçük parçalar hâlinde yapılan üretimlere dönüştüğünü belirtmektedir. Frankfurt Okulu’nun kültür endüstrisi ve standartlaşma üzerine düşüncelerinin üçüncü dalga toplumlarında geçerli olmadığını, söz konusu toplumda artık kültür ürünlerinin birörneklikten uzaklaştığına dikkat çekmektedir (Laughey, 2010: 106).

Castells, enformasyon toplumu kavramının enformasyonun toplum içindeki önemini vurguladığını söylerken onu kendi özgün ifadesiyle oluşturduğu *enformasyonel toplum* teriminden ayırmaktadır. Ona göre enformasyonel terimi, enformasyonun üretimi, işlenmesi ve iletimiyle ve bu dönemde ortaya çıkan yeni teknolojik gelişmelerle birlikte üretkenliğin ve gücün temel kaynağına dönüşmesiyle özel bir toplumsal örgütlenme türünün niteliklerine vurgu yapmaktadır. Diğer bir ifadeyle, enformasyonel terimi, bilgi ve enformasyonun toplumlar için olan öneminin dışına çıkarak neden olduğu dönüşümleri daha somut bir zeminde anlatmayı amaçlamaktadır (Castells, 2008: 25). Ağ toplumu ifadesi tam da bu noktada karşımıza çıkmaktadır. Ağ toplumu, mikro elektronik tabanlı enformasyon ve iletişim teknolojilerinin aracılığıyla ortaya çıkan ve sosyal ağlardan oluşan yeni bir sosyal yapıyı vurgulamak için kullanılmaktadır. Castells (2005), iletişim ağlarının sınırları aşabilmesi sayesinde ağ toplumunun küresel olduğunu, küresel ağlara dayandığını; tüm dünyaya yayıldığını ve sermaye, mal, hizmet, iletişim ve emek gibi tüm küresel ağlara nüfuz ettiğini belirtmektedir. Bu nedenle ağ toplumu bir anlamda da küreselleşmeye atıfta bulunmaktadır.

Jan van Dijk (2018), ağ toplumunu “sosyal ve medya ağlarından oluşan bir altyapının toplumun her seviyesindeki örgütlenme tarzını belirlediği modern bir

toplum türü” şeklinde tanımlamaktadır. Ona göre enformasyon toplumu daha çok içerik ve enformasyonun büyüklüğüyle ilişkiliyken ağ toplumu toplumsal biçim ve örgütlenmeye odaklanmaktadır. Dijk, 20. yüzyıl zarfında kitle toplumuna ait yapıların giderek ağ toplumu yapılarına dönüştüğünü ve 21. yüzyılın “ağlar çağı” olduğunu ifade etmektedir. Ona göre ağ toplumunun temel birimi ağlarla birbirine bağlanan bireylerdir. Ağlar, toplumun tüm tabakalarına hizmet etmekte ve onları birbirine bağlamaktadır.

Ağlar, ekonomik çerçevede oldukça önemli bir bağlayıcıdır. Castells, enformasyon toplumunun içinde bulunduğu ekonomik süreci geleneksel kapitalizmin farklı bir türü olarak “yeni ekonomi” şeklinde tanımlamaktadır (Castells, 2005: 7; Çakır, 2018: 39). Enformasyonun temel güç olduğu bu ekonomide firmalar, işletmeler, şirketler ve devletler sahip oldukları enformasyonla ve onu işleme ve yeniden üretme kapasiteleriyle ön plana çıkmaktadır. Küresel ekonominin yeni hâli, mevcut üretim süreçlerini içeren ekonomik etkinliklerin bir parçası olarak değil; aksine, tüm ekonomik faaliyetleri gelişmiş enformasyon teknolojilerinin üretkenlik potansiyellerinin agresif biçimde kullanılmasıyla yeniden yapılandırmaktadır (Stalder, 1998). Yeni ekonomiyi tamamen yeni olarak kabul etmekten ziyade eskisinin yeni bir versiyonu olarak kabul etmesi onu Toffler’den ayırmaktadır. Castells’in ifade etmeye çalıştığı şey, ağ toplumunun enformasyonel ekonomisinin, tarım ve sanayi ekonomilerinin yerini almadığı (yani üçüncü bir dalga söz konusu değildir), aksine onların içine işlediğidir (Laughey, 2010: 109). Enformasyona ait tüm bileşenler geleneksel kapitalist faaliyet ve iş kollarıyla örtüşerek iç içe geçmiştir.

Webster (2002; 2006), enformasyon toplumu kavramını belirli yaklaşımları ele alarak altı tanım üzerinden incelemektedir. Bunların ilk beşi sırasıyla teknolojik, mesleki, ekonomik, mekânsal ve kültürelidir. Bu tanımların ortak noktası bilgidaki niceliksel değişikliklerin, yükselişin, enformasyon toplumunu oluşturduğu fikrine dayanmasıdır. Altıncı tanım ise kendisine aittir; günümüzde enformasyonun çokluğuna değil, onun yaşama biçimini dönüştürmesiyle ilgilidir. Webster’ın incelediği beş niceliksel ve bir niteliksel tanımı sırasıyla aşağıdaki gibi ele alabiliriz (Webster, 2002: 23-26; 2006: 9-21):

- 1) **Teknolojik:** 1970’li yılların sonlarıyla birlikte ortaya çıkan uydu teknolojileri, kişisel bilgisayarlar, ağlar arası iletişim, işlemciler, çekirdekler ve CD-ROM gibi yeni teknolojiler enformasyon toplumunun gelişine zemin hazırlamıştır. Yeni teknolojiler kaynaklı enformasyon toplumuna geçişi iki döneme ayırmak mümkündür. İlki, 1980’li yıllarında başında devasa bilgisayarları kişisel bilgisayarlara dönüştürmeye olanak sağlayan mikro işlemcilerin toplumun yaşam tarzında yaşatacağı değişimlere odaklanmaktadır. İkincisi, 1990’lı yılların ortalarıyla beraber bilgisayar iletişim sistemlerinin (e-posta, veri iletişimi, çevrimiçi alışveriş, bireysel iletişim) sunduğu imkân ve olanaklarla ilgilidir.
- 2) **Mesleki:** Kol gücü (el emeği) ve makine kullanımının (el becerisi) yerini bilginin almasıyla bilgi işçiliğinin artışı, enformasyon toplumunun oluşmasına zemin hazırlamıştır. Enformasyon toplumunda kas gücü ile çalışanların sayısı hammadde enformasyon olan beyaz yakalı çalışanların sayısından daha az hâle gelmiştir. Diğer bir ifadeyle, imalat sektörü istihdamında düşüş ile hizmet sektörü istihdamında artış meydana gelmiştir. Mesleki değişim, Daniel Bell’in *sanayi sonrası toplum* kavramıyla doğrudan ilişkilidir.
- 3) **Ekonomik:** Bu tanım, genel ekonomide enformasyonun oynadığı rolün ağır basmaya başlamasına dayandırılmaktadır. Enformasyon toplumlarında bilgiye dayalı iş sektörlerinin Gayri Safi Milli Hâsıla içindeki yeri tarım veya imalat sanayilerine nazaran daha büyük bir paya sahiptir. Bu payın büyüklüğü “enformasyon ekonomisi” adıyla ekonominin yeni bir türünü ortaya çıkaracak kadar yer kaplamaktadır.
- 4) **Mekânsal:** Enformasyon toplumunun bu tanımındaki temel vurgu, mekânları birbirine bağlayan bilgi ağlarındadır. Bilgi ağları zaman ve mekânın üzerinde derin etkiler bırakmıştır ve zamanla sosyal örgütlenmenin belirgin bir özelliği hâlini dönüşmüştür. Enformasyon toplumların, farklı konumlar ve farklı mekânlar, uygun elektrik altyapısı ve teknolojik araçlara sahip olduğu takdirde

istenildiği zaman birbirine erişebilecek ve iletişime geçebilecek durumdadır. Castells'in *ağ toplumu* kavramıyla aynı anlayışa sahiptir.

5) Kültürel: Enformasyon toplumunun kültürel tanımı, içinde bulunan bilgi ortamı ve maruz kalınan bilgi akışının altını çizmektedir. Bugün günlük yaşam içerisinde dolaşan enformasyonların sayısında geçmişe kıyasla büyük bir artış söz konusudur. Televizyon, telefon, radyo, bilgisayar, internet, mobil cihazlar, uydu teknolojileri ve diğer birçok araç bilgi içerecek şekilde tasarlanmıştır. Tüm bu araçlar aracılığıyla insanlar sürekli olarak enformasyona maruz kalmakta; her bir mesajda yer alan semboller ve simgeler dünya çapında yeni bir kültürün oluşumuna önyak olmaktadır. Webster, sembol ve simgelerin çok farklı türlerde, hızla değişebilen ve tutarsız olabildiğini ifade ederek enformasyon bolluğunun yol açtığı anlam kaybını Baudrillard'a atıf yaparak açıklar: *“Daha çok bilginin ve daha az anlamın olduğu bir dünyada yaşıyoruz.”*

6) Yaşam biçimindeki değişim: Webster, ilk beş tanımda bilgideki niceliksel artışa vurgu yaparak enformasyon toplumunu dair bakış açılarına, altıncı tanımda bilginin insan yaşamında veya toplumda neden olduğu değişimlere yer vermektedir. Bu yönüyle altıncı tanım nicelikten öte niteliksel bağlamda ele alınmaktadır. Webster, enformasyon toplumu ve toplum nezdindeki değişimleri Daniel Bell, Anthony Giddens, Herbert Schiller, Mark Poster ve Manuel Castells gibi kuramcılarının fikir ve görüşlerini tartışarak açıklamıştır.

Frank Webster genel olarak ilk beş maddedeki nicel fetişizme yönelik eleştiriler sunmaktadır. Enformasyon toplumu tanımlarındaki beyaz yakalı çalışan sayısı, enformasyonun ekonomi içindeki büyüklüğü, teknolojik araç sahipliği, bilgi ağlarının kullanımı ve çokluğu gibi niceliksel birimlerin fazlalığı enformasyon toplumuna girildiğini varsaymaktadır. Oysaki enformasyondaki nicel fazlalık bir önceki toplum yapısının bittiğini ve yeni bir topluma, enformasyon toplumuna, geçildiğini söylemek için yeterli değildir. Webster bu ifadesini desteklemek için şu

örneği paylaşmaktadır: “*Bugün 1970 yılından daha fazla otomobile sahip olduğumuz için otomobil toplumu değiliz.*” (Webster, 2006: 22).

Bilgi ve enformasyon toplumuna ilişkin fikir ve düşüncelerin bulunduğu ortak nokta, endüstriye dayalı üretimin yerini bilgi / hizmet sektörüne bırakması ve enformasyonun ekonomide merkezî bir role sahip olduğunu vurgulamasıdır. Yeni bir toplum yapısını imleyen bu kavramların diğer bir yüzünde toplumun gözetim altında olduğu gerçeği yatmaktadır. Bilgi toplumları aynı zamanda gözetim toplumlarıdır. Belirleyici düzeyde bilgi ve iletişim teknolojilerine bağımlı olan yeni toplumsal yapıda kişisel veriler daha önceki zamanlara göre daha fazla sistematik ve yoğun bir gözetime maruz kalmaktadır (Lyon, 2018: 60). Bu durum enformasyon toplumu ile gözetim toplumu arasındaki sınırları giderek ortadan kaldırmaktadır (Dolgun, 2015:212).

İKİNCİ BÖLÜM

ÇEVİRİM İÇİ GÖZETİM, KULLANICILAR ve REKLAM

2.1. İnternet ve Gözetim

“İstihbarat teşkilatları ve kolluk kuvvetleri, (...), şirketlerin soyut kimliklerimizin haritasını çıkarmak için yaptıkları çalışmaların rüzgârından faydalaniyor.” (O’Shea, 2021: 56).

İlk web tarayıcılarının 1994 ve 1995’te piyasaya sürülmesi internetin panoptik bir hâle dönüşmesinde kilit bir rol oynamıştır (Elmer, 2003: 113). Geçen çeyrek asırlık süreden sonra bugün ağlara bağlı insanların düzenli olarak her gün, her dakika izlenmesi ve dijital ortamda kayıt altına alınması günlük yaşamın bir parçası hâline dönüşmüştür. Milyarlarca insanın internet erişimli cihazlarda gerçekleştirdiği eylemler (tıklama, beğenme, mesajlaşma, görüntüleme) izlenmektedir. Öte yandan IP adresleri, konumları, cihaz bilgileri ve cihazın bağlı olduğu WIFI adı gibi herhangi bir eyleme gereksinim duymadan zaten var olan durumların da takibi gözetim araçlarının radarına takılmaktadır. Gözetim, sosyal ağlarda ve web sitelerinde devam ettiği gibi internete bağlanabilen her bir cihazın kendisinde, sensörler aracılığıyla ve mobil cihaz ve uygulamalarda da devam etmektedir. Böylelikle sistematik olarak izleme faaliyetleri insanın her anını farklı kaynaklardan elde ettiği verilerle kayıt altına alarak onun hakkında oluşturulan profillerin zenginleşmesine katkı sağlar.

Fuchs vd. (2012: 16-19) interneti on dört boyutuyla el alarak, bu boyutları hem internetin temel niteliğindeki hem de internet gözetiminin niteliğindeki ilişkisine değinmektedir.

Boyut	İnternetin Niteliği	İnternet Gözetiminin Niteliği
(1) Mekân	Küresel iletişim	Küresel bir bilgi alanından belirli kişiler hakkında birçok veri nesnesinin toplanması ve birleştirilmesini kapsar. Söz

		konusu durum yalnızca tek bir noktadan değil, ağdaki tüm düğümlerden gözetim ile mümkündür.
(2) Zaman	Eşzamanlı ve eşzamansız küresel iletişim	Gerçek zamanlı iletişimin, gerçek zamanlı gözetimi. Daha sonra kullanılmak üzere depolanan eşzamansız iletişimin gözetimi.
(3) Hız	Yüksek hızda veri aktarımı	Gözetim, yüksek hızda veri aktarımıyla gerçekleşir.
(4) Boyut	Depolama kapasitelerinin artışı	Gözetim verilerinin artışı ve daha fazla bireye erişimle veriler, gözetim amacıyla kullanılan ve zamanla küçülen ve ucuzlayan depolama cihazlarında saklanabilir.
(5) Çoğalma	Veriler kolayca ve sonsuza kadar orijinaline zarar vermeden kopyalanabilir	Gözetim kolay ve ucuz hâle getirir; birden fazla veri kopyası mevcutsa, belirli verilerin bulunması daha kolaydır.
(6) Duyusal Modalite	Entegre bir ortamda metin, ses ve görüntünün dijital kombinasyonu	Çok algılı verilerin tek bir ortamda gözetimi.
(7) İletişim Akışı	Çoktan çoka iletişim	Sosyal ağ gözetimi: bireylerin kişisel ve profesyonel sosyal ağları görünür ve gözetlenebilir hâle geldi.
(8) Bilgi Yapısı	Ağ bağlantılı, birbiriyle bağlı, hiper metin bilgi yapısı	Kişilerarasındaki bağlantılar daha kolay izlenebilir.
(9) Alıcılar (İzleyiciler)	Alıcılar, bilgi üreticileri hâline dönüşür (Üretketici)	Yeni sermaye birikim stratejileri reklamverenlere emtia olarak satılan yaratıcı kullanıcılar ve kullanıcı tarafından oluşturulan içeriğin sürekli gözetimine

		dayanan hedefli reklamcılığa dayanır.
(10) Etkileşim ve Sosyalite Biçimi	Uzaktan işbirliği ile bilgi üretimi, uzaktan bilgi paylaşımı.	Paylaşım ve işbirliğinin, fikri mülkiyet haklarının gözetimini sağlayan yasalar.
(11) Bağlam	Bağlamdan arındırılmış bilgi ve anonimlik	Bağlamsızlaştırma, şüpheli ve öncelikle gözetimi geliştirir.
(12) Gerçeklik	Gerçeklik ve kurgu arasındaki çizginin bulanıklaşması	İnsanları riske atan ve gözetimi yoğunlaştıran gözetleyenler, kurgusal gerçeklik ile hakiki gerçekliği karıştırabilir.
(13) Kimlik ve Duygular	İnternet, kimlik inşasına ve Çevrim içi temsiliyete izin veren etkileyici bir ortamdır	Kişiselleştirilmiş gözetimle bireylerin oldukça kişisel özellikleri ve duygularının gözetimi mümkündür.
(14) Uygunluk	İnternet, günlük yaşamında her alanında yaygın olarak kullanılmaktadır.	İnternetin her yerdeliği, gözetiminin de her yerdeliğidir. Heteronom toplumlarda, ekonomik, politik, adli ve diğer amaçlar için internet bilgilerinin ve iletişimin sürekli ve derinlemesine gözetimi vardır.

Tablo 2.1: İnternet Gözetiminin Boyutları ve Nitelikleri
(Fuchs vd., 2012: 16-19; Fuchs, 2015: 399-401).

İnternet gözetimi, detaylı olarak tablo 2.1’de okunduğu gibi; he an, her yerde, ağa bağlı her cihazdan olabildiğince çok insan, insan etkinlikleri ve kullanım verisinin toplanması, saklanması ve ticaretini kapsamaktadır. Veriler binlerce kez kopyalanabilir, çoğaltılabilir, paylaşılabilir ve başka verilerle birleştirilebilir durumdadır. İnternetteki izleme faaliyetleri insanların Çevrim içi yaratıcı emeğinin, iletişimin ve benliğinin gözetimini de kapsayarak büyük bir gözetim ağının oluşmasına neden olur. Tüm çabalar neticesinde insanın dijital bir kimliği ortaya çıkarılır. Thomas Hemnes (akt. Ferguson, 2017: 174), Çevrim içi gözetim sonucu inşa edilen dijital kimliğin ne olduğunu şu şekilde aktarır:

“Bir bireyin dijital kimliğini noktacılık akımına ait bir resime benzeterek düşünebiliriz. Bir bireye ait temel gerçekler, hassas gerçekler, etkileşimsel gerçekler olarak adlandırdığımız şeyler dâhil binlerce küçük dijital bilgi, bireyin bir resmini oluşturmak için bir araya getirilebilir: sevdikleri, hoşlanmadıkları, eğilimleri, geliri. Aslına bakarsak, kişiliğinin İnternet ile bağlantısı olan her yönü resmi oluşturur. “

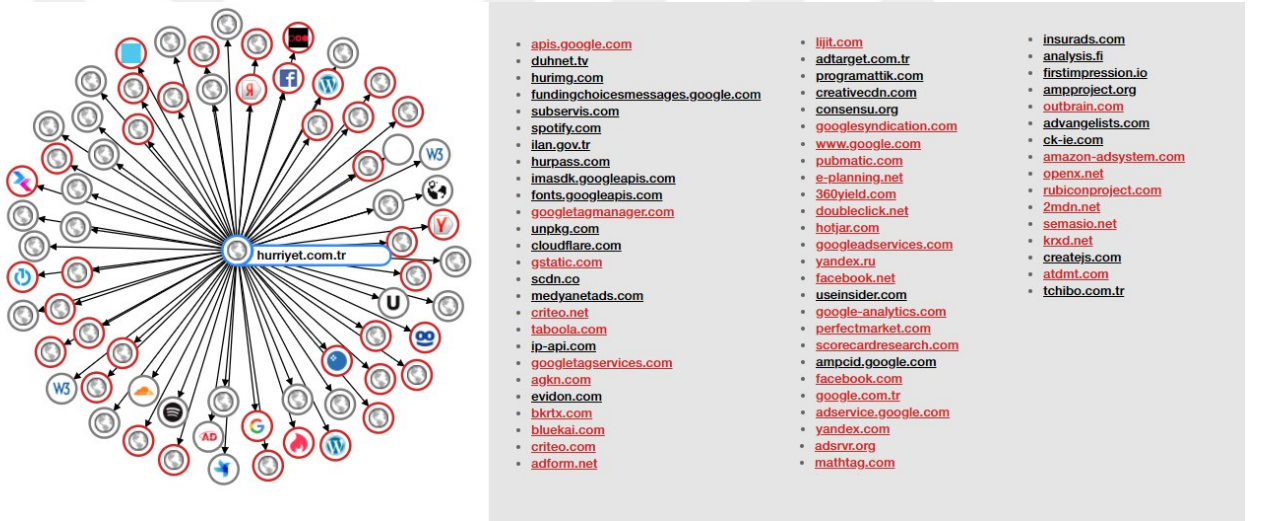
Andrews (2013: 23) bu kimliği dijital ikiz olarak tanımlar. Yani, çevrim içi izlemeden arda kalanlar bireyin sanal bir yorumunu inşa eder ve hakkında verilecek kararlar fiziksel bireyden ziyade dijital ikizi üzerinden belirlenir. Neticede, internet gözetimi arama yapılan kelimeler, web sitesi ziyaretleri, sosyal medya platformlarındaki gezinimler, yüklenen fotoğraflar, yapılan yorumlar, Çevrim içi alışverişler, fare hareketleri, kaydırmalar, kaçınmalar, klavyede basılan tuşlar, gönderilen ve alınan e-posta içerikleri, yol tarifleri, oynanan oyunlar, mobil uygulama kullanımları, otel rezervasyonları, uçak biletleri vb. tüm çevrim içi etkinliklerin izlenmesini içerir. Tüm çabalar insanı daha iyi tanıma, tanımlama ve geleceğini öngörme niyeti barındırır.

2.1.1. Web Siteleri ve Gözetim

Greg Elmer, interneti ağırlıklı olarak ekonomik gözetimin güçlü bir alanı olarak yorumlamakta ve 1997 yılında internet gözetiminin aşamalarını iki adımla açıklamaktadır: *“İnternet, ilk önce arama motorları tarafından dizinlendi; sonrasında kullanıcıların çevrim içi davranışını etkin bir biçimde izlemek, araştırmak ve daha sonra bunların profilini çıkarmak için ‘örümcekler’ ve ‘çerezler’ aracılığıyla tanımlanır hâle geldi.”* (Elmer, 1997’den akt. Allmer, 2012: 129). Elmer’in o dönemki ifadeleri hala geçerliliğini korumakta; web sitelerinin gözetimi hem gelişmiş hem de daha geniş bir alana yayılarak devam etmektedir. Bugün, ziyaret edilen web sitelerinden aramalara kadar internette gezinen kullanıcıların alışkanlıklarını ve davranışlarını izlemek; tercihleri, ilgi alanları, sorunları, sevdikleri veya sevmedikleri şeyler hakkında çeşitli ve geniş bilgiler toplamak için en yaygın yollardan biridir (Christl - Spiekermann, 2016: 43). Kullanıcılarının ağ üzerinde çevrim içi davranışlarını izleyen, ölçen ve kaydeden çok sayıda yöntemden söz edebiliriz.

Çerezler ve pikseller gibi izleme teknolojileri çevrim içi gözetim en sık kullanılan ve bilinen yöntemlerdir. Çerezler cihazlarda saklanırken, izleme pikselleri doğrudan sahibinin sunucusuyla iletişime geçerek bilgi alışverişinde bulunur.

Web sitesi ziyareti sırasında çerezler ve izleme pikselleri aracılığıyla kullanıcı gözetimi sınır tanımamaktadır. Örneğin, Türkiye'nin en çok ziyaret edilen haber sitelerinden birini ele alalım: *hurriyet.com.tr*. Tablo 2.2'de, 28 Kasım 2020 tarihinde Hürriyet Gazetesi web sitesinin içerisinde bulunan üçüncü taraf izleme kodlarının kimler olduğu yer almaktadır.



Tablo 2.2: hurriyet.com.tr'yi Ziyaret Eden Bir Kullanıcının Sitedeki Gezinimlerini Takip Eden Üçüncü Taraf Şirketler
(28 Kasım 2020 tarihinde Disconnect tarayıcı eklentisi aracılığıyla elde edilmiştir).

Tabloda verilen web sitelerinin hepsi üçüncü taraf platformlardan oluşmakta; gerek kitle analizi gerçekleştirmekte gerek kullanıcı davranış verilerini toplamakta gerekse kullanıcıya kişiselleştirilmiş reklam gösterimi sağlamaktadır. Kullanıcı hurriyet.com.tr'yi ziyaret ettiği ve sitede gezindiği sırada onu Google, Yandex ve Facebook gibi bilinen platformların yanı sıra Pubmatic, Criteo, Taboola gibi reklam teknoloji şirketleri, Türk Telekom'un reklam platformu Programattik ve BlueKai gibi veri şirketleri izlemeye, ilgi ve davranışlarını kayıt altına almaya başlamaktadır. Bu gözetim ağının günümüzde neredeyse her bir web sitesinde olduğu düşünüldüğünde, reklam servisleri, platformlar ve şirketler kullanıcıları siteler arası takip ederek onlar

hakkında daha zengin içgörüler elde edebilmektedir. Bu yönüyle web siteleri çevrim içi gözetimin başlıca kaynağı olarak kabul edilebilir.

2.1.1.1. Çerezler ve Çerez Türleri

Çerez (Cookie), bir sunucu ile bir bilgisayar arasında bilgilerin aktarılmasını sağlayan kod parçacıklarıdır. “*Kişiyi özel elektronik ayak izi*” şeklinde de ifade edilebilir (Lokke, 2018: 63). İlk ticari web tarayıcısı olan Netscape tarafından 1994 yılında geliştirilmiştir (Kristol, 2001). Ortaya çıkışından önce internet kullanıcılarının bilgisayarı ile uzak sunucular arasındaki veri alışverişi anonim olarak gerçekleşirken (Peacock, 2014); çerezlerin sabit diske kaydedilmesiyle birlikte sunucu ile kişisel bilgisayar arasında doğrudan bir iletişim sağlanmaya başlamıştır. Netscape’te çalışan programcı Lou Montulli, alışveriş sepetine eklenen ürünleri sepette tutabilme amacıyla daha sonradan adına “cookie” dediği küçük hatırlatıcı metin dosyalarını icat etmiştir. Bu yolla hem sepete eklenen ürünler sabit diske kaydedilerek aynı kullanıcının bir sonraki ziyaretinde hatırlanmış, hem de ziyaretçilerin kim olduğunun tespit edilememesi sorunu ortadan kalkmıştır. Sabit diske yerleştirilen çerezde kullanıcının kimlik kodu ve sitedeki gezinim sırasında gerçekleştirdiği davranışlar kayıt altına alınmaktaydı. Aynı kişi aynı bilgisayarı kullanarak siteyi ziyaret ettiğinde tarayıcıdaki etiketler çerezi tanıyacak; çerezdeki veriler incelenerek kullanıcının bir önceki ziyaretinden kayıt altına alınmış her şeyi görüntüleyebilecektir (Turow, 2016: 80).

Roger A. Clarke (akt. Elmer, 2003: 118), çerez teknolojisinin nasıl çalıştığını adım adım şu şekilde açıklamaktadır: (1) Bir web tarayıcısı bir web sunucusundan sayfa talep eder. (2) Web sunucusu, web tarayıcısına talep edilen sayfayı gönderir, aynı zamanda, kullanıcı bilgisayarının sabit diskine “çerez” kaydetmesi için talimat iletir. (3) Tarayıcı bir engel ile karşılaşmazsa bu işlemi uygular. (4) Kullanıcı bir web sayfasını her görüntülemek istediğinde, web tarayıcısı web sunucusunun talimatla iletme istediği çerezin hâlihazırda sabit diskte olup olmadığını kontrol eder. (5) Eğer çerez varsa, tarayıcı çerez kaydını web sayfası talebiyle birlikte sunucuya iletir. (6) Bir web sunucusu kendisiyle ilişkilendirilmiş bir çerez bilgisine sahip olarak sayfa görüntüleme talebi aldığı anda, sunucu kullanıcı hakkındaki şeyleri hatırlamak için

çerezde kaydı tutulan bilgileri kullanabilir. Netscape Navigator 1.1 tarayıcısıyla tanıtılan bu yenilik, sunucuların e-ticaret faaliyetlerini kolaylaştıracak şekilde kullanıcı davranışlarını izlemesini sağlamış; çok geçmeden ise hedefli reklamcılığın vazgeçilmezi hâline gelmiştir (West, 2019: 27). Oturum çerezlerinin süresi tarayıcı kapatıldığında dolarken, kalıcı çerezler uzun süre boyunca saklanabilir. Söz konusu çerezler günler, aylar veya yıllar sürecektir şekilde yapılandırılabilir ve hatta sonsuza kadar cihazda kalacak şekilde tasarlanabilir (Miyazaki, 2008).

Çerez dosyaları üç ögeyi içerir: (1) çerezi oluşturan platformun sunucu adını, (2) çerezin kullanım süresini, (3) çerez değerini. Çerez değeri, eşsiz bir birleşimden meydana gelen rakamlardan oluşur. Çerezler her kullanıcıya özel bir dizi benzersiz içeriğe sahiptir ve şifrelidir. Kişiyi temsil eden çerez içeriğine erişim yalnızca çerez sahibi tarafından yapılabilir, zira şifrenin anahtarı olmadan çerezde tutulan bilgiler anlamlı değildir (Wheeler, 2015:104). Örneğin, Google’a ait çerezler yalnızca Google tarafından görüntülenir ve okunur. Diğer çerez sahipleri, Google’ın kullanıcı hakkında sakladığı verilere erişemez. Dolayısıyla cihaza yerleştirilen her bir çerez rastgele sayı ve rakamlardan oluşan metin dosyaları gibi gözükse de içerisinde birden çok veri barındıran ve yalnızca çerez sahibi tarafından okunarak anlamlı hâle getirilebilen bir yapıdadır.

Çerez teknolojisinin yaygınlaşması bazı tartışmaları da beraberinde getirmiştir. Çerezlere olumlu yaklaşımlar genellikle web’i kişiselleştirme potansiyeline vurgu yapmıştır. Olası potansiyel etkilerini inceleyenler çerezlerin her yere yayılmasıyla insanların tek tek hedeflenebilir hâle geleceğini ve mahremiyet kaygılarını dile getirmiştir (West, 2019: 27). Zira Lou Montulli ve çerez teknolojisini icat ederken ona yardımcı olan John Giannadrea, çerezin cihaza yerleşirken kullanıcıdan izin alınmaması gerektiğini düşünmüştür. Montulli ve Giannadrea, çerezin kabul edilip edilmeyeceğini kullanıcıya sormayarak mahremiyet kaygılarının ortaya çıkmasına ve şeffaflık eksikliğinin meşrulaştırılmasına önayak olmuştur (Turow, 2016: 80-81). Gelineen noktada farklı türlere ve amaçlara sahip çerezler hem kullanıcı deneyimini geliştirmeye odaklanırken hem de web sitesi sahibine, platformlara ve şirketlere değerli kullanıcı verileri paylaşmaktadır.

Bugün birçok internet sitesi çeşitli amaçlar doğrultusunda çerezlere ihtiyaç duymaktadır. Bu çerezleri birinci taraf çerezler ve üçüncü taraf çerezler olarak ikiye ayırabiliriz. Birinci taraf çerezler, doğrudan ziyaret edilen web sitesine ait çerezlerdir. Üçüncü taraf ise web sitesinin kontrolü altında olmayan, ondan bağımsız olarak bilgi toplayan ve paylaşan tüzel kişi ve gruplardır (Wheeler, 2015:105). Bu bilgiler ışığında amaçlarına göre birinci taraf çerezleri zorunlu ve tercih çerezleri; üçüncü taraf çerezleri analitik ve pazarlama çerezleri olarak tanımlayabiliriz (GDPR, 2019).

- a) **Zorunlu çerezler:** Bu çerezler web sitesini ziyaret ederken ve onun çeşitli özelliklerini kullanırken gereklidir. Web sitesiyle ilişkili olduğu için birinci parti çerezler olarak adlandırılır. Bir alışveriş sitesinde sepete eklenen ürünün bir sonraki ziyarette sepette tutması bu çerez tipine örnek verilebilir.
- b) **Tercih çerezleri:** İşlevsel çerezler olarak da adlandırılan bu çerez türü, bir web sitesi ziyaretinizde daha önceden yaptığınız tercihleri saklamaya yararmaktadır. Kullanıcı adı - şifre bilgilerinin otomatik olarak doldurulması, varsayılan temalar, tercihler veya dil ayarları bu çerezlerin kullanımına örnek gösterilebilir.
- c) **Analitik çerezler:** Bir web sitesinin nasıl kullanıldığı; hangi sayfaların ziyaret edildiği, hangi bağlantıların tıklandığı ve oturum süresi gibi veriler hakkında bilgi toplayan çerezlerdir. Bu veriler kullanıcı tanımlamak niyetiyle değil istatistiksel veri olarak kaydedilir ve anonimdir. Kullanıcı ziyaretlerini kayıt altına almak ve web sayfasında gerçekleştirdikleri davranışları takip ederek analiz amaçlı bilgi toplamak oldukça yaygındır. En popüler analiz aracı, Google ürünü olan Google Analytics'tir. Builtwith (2020) verilerine göre dünyada en az 28 milyon web sitesi Google Analytics'e ait çerezi web sitesinde barındırmaktadır. Dünyanın en çok ziyaret edilen ilk 10 bin sitesinin %72'si; ilk 100 bin sitenin %65'i; ilk 1 milyon sitenin %53'ünde Analytics çerezi bulunmaktadır. Türkiye'de ise en az 100 bin web sitesinde yer aldığı belirtilmiştir.

d) Pazarlama çerezleri: Reklamverenlerin web sitesi aracılığıyla kullanıcılara reklam göstermesine yardımcı olan ve kullanıcıları izleyen çerezlerdir. Bu çerezler aracılığıyla kullanıcı verileri diğer veri şirketleriyle, kuruluşlarla, platformlarla ve/veya reklamverenlerle paylaşılabilir. Bu çerezler her zaman “üçüncü taraf çerez” olarak ifade edilir. Google Tag Manager, Facebook Connect, Criteo, Adobe Audience Manager gibi uygulamalar üçüncü taraf çerezlere örnek gösterilebilir. Dünya çapında en çok ziyaret edilen 1 milyon web sitesinin en az %30’u Google’ın reklam bağlantılı ürünü olan DoubleClick, en az %15’i Facebook Custom Audiences ve yine en az %15’inde Google Adsense uygulamalarına ait çerezler yer almaktadır. Builtwith’in Türkiye’de incelediği 100 bin web sitenin %33’ünde Google Adsense, %21’inde DoubleClick, %7’sinde Google Remarketing ve %4’ünde Facebook Custom Audiences uygulamalarına ait çerezler olduğu tespit edilmiştir.

Çerezlerin tüketiciye sağladığı varsayılan avantaj, kullanıcı deneyimini geliştirmesi ve kişisel ihtiyaçlara yönelik düzenlenmiş tüketici reklamlarının doğru hedeflere, yani kullanıcılara sunulmasıdır. Şirketlerin avantajı ise tüm pazarın en mikro düzeyde bireysel olarak bilinebilmesidir (Lyon, 2018:208). Yukarıda görüldüğü üzere tüketiciye sunulan avantajlar birinci taraf çerezlerle ilişkiliyken; şirketlerin, platformların ve reklamverenlerin bireysel hedeflemesine yardımcı olan çerezler üçüncü taraftır. Çerezlerin tarayıcılara dâhil edilmesi ve reklam endüstrisinin ihtiyaçlarına olumlu katkıları sonucu internet teknolojileri ticari gözetim için temel bir altyapı oluşturmuştur (West, 2019: 28). Lyon’un ifade ettiği gibi kitlenin bireysel olarak bilinebilmesinde önemli bir rol oynayan çerezler, gözetlemenin internetin iş modeli hâline gelmesine de zemin hazırlamıştır. Ayrıca çerezlerin tür ve amaçları ele alındığında internet sitesinin doğrudan kullanıcıyla ilişkili çerezleri dışında dış kaynaklı üçüncü taraf çerezlerin mahremiyet ve şeffaflık üzerine kaygıları tetiklediği de düşünülmektedir.

2.1.1.2. İzleme Pikselleri

İzleme pikselleri (Web işaretçisi olarak da bilinir), bir web sitesinin çeşitli alanlarına yerleştirilen 1x1 piksel boyutundaki şeffaf bir grafik dosyasıdır. Web sitesinin herhangi bir yerinde yer alan bu dosya kullanıcıların siteye ne zaman girdiğini ve sitede ne yaptıklarını izler ve kaydeder (Pedley, 2002: 46). Web sitelerinin HTML kaynak kodunda yer alan izleme pikselleri, sayfa görüntülediği zaman sunucusuyla iletişime geçer ve şu bilgileri gönderebilir: (1) Bilgisayarın IP adresini, (2) sayfa URL'sini, (3) grafiğin URL'sini, (4) görüntülenme zamanını, (5) tarayıcının ne olduğunu, (6) önceden yerleşmiş çerez değerini (Smith, 1999). Bu bilgilerin yanı sıra cihaz tipi (cep telefonu, tablet veya bilgisayar), cihazın işletim sistemi, ekran çözünürlüğü ve kullanıcının web sitesi kullanım hareketleri de gözetlenerek kayıt altına alınır. İzleme pikselleri, kullanıcı hakkında bilgi toplama konusunda çerezlere benzer fakat alternatif bir yöntem olarak karşımıza çıkar.

İzleme pikselleri, bir web sitesinde olduğu gibi bir e-posta içinde de görünmez biçimde yer alabilir. E-posta pazarlama (E-mailing) hizmeti veren firmalar, atılan toplu e-postaların kaçıcının okunduğunu ve alıcının e-posta ile nasıl etkileşime girdiğinin verisini bu grafikler aracılığıyla elde eder. Bazı durumlarda “casus yazılım” işlevi görerek kullanıcının Çevrim içi etkinliğini izleyebilir. Şüpheli e-postalar web işaretçisinden yararlanarak kullanıcı aktivitelerini izinsiz bir biçimde kaydeder.

İzleme pikselleri, reklam hizmeti sağlayan kurumlar tarafından sıkça kullanılır. Kurumlar, pikseller sayesinde sitede yayınlanan reklamlarla etkileşimi ölçerek kullanıcı davranış verilerini temin eder; bu noktada reklamın o kullanıcıya ne sıklıkla görüldüğü ve kullanıcının ne zaman tıkladığı gibi veriler üzerine bir profil oluşturulmasına yardımcı olur. 2000 yılında Inteltyics Inc. isimli bir güvenlik şirketi tarafından analiz edilen 51 milyon web sayfasının yaklaşık %30'unda en az bir adet üçüncü taraflarca yerleştirilmiş bir izleme pikseli olduğu tespit edilmiştir (Baruh, 2007: 195). California Üniversitesi'nde 2009'da yapılan bir çalışmada ise en çok ziyaret edilen 50 web sitesinde en az bir adet izleme pikseli olduğu ortaya konulmuştur. Hatta söz konusu izleme piksellerinin, çoğu sitede birden çok, bazılarında yüze yakın olduğu da vurgulanmıştır (Andrews, 2013).

İzleme pikselleri, tıpkı çerez teknolojisinde olduğu gibi, kullanıcı bilgisi dâhilinde olmadan onun hakkında kapsamlı bilgiler toplaması ve üçüncü taraflara iletmesi dolayısıyla tartışmalara sebep olmaktadır. Gözle görülmeyen grafikler aracılığıyla gerçekleşen kullanıcı gözetimi, genellikle açık rıza alınmadan gerçekleşir. Verilerin nerede saklandığı, kimlerle paylaşıldığı ve ne amaçla kullanıldığına ilişkin bir şeffaflık olmadığı gibi, rıza alınmadan girilen bu sistemden çıkış da söz konusu değildir.

2.1.1.3. Çerezsiz Dünya ve İzleme Teknolojilerinin Geleceği

Teknoloji ve reklam şirketlerinin mevcut izleme sistemleri gerek kullanıcılardaki veri bilincinin artmasından gerekse bu konudaki yasal düzenlemelerin ortaya çıkmasından etkilenmektedir. Bunun yanında birçok web tarayıcısı yeni güncellemelerinde üçüncü taraf çerezleri otomatik olarak engelleyen özellikleri bünyelerine katmıştır. Apple'ın Safari tarayıcısı varsayılan olarak üçüncü taraf çerezleri engellemiştir. Mozilla'nın Firefox tarayıcısı üçüncü taraf çerezleri, kullanıcıları siteler arası gözetlemesine sınır getirerek kısmen de olsa engelleme yoluna gitmiştir. Google'ın Chrome tarayıcısı 2023 yılı ortaları itibarıyla varsayılan olarak üçüncü taraf çerezleri engelleyeceğini beyan etmiştir. Tüm bu gelişmeler başta sosyal medya platformları olmak üzere diğer analitik ve reklam şirketlerinin kullanıcıları gözetleme adına yeni çözümler üretmesine yol açmıştır.

IAB France (2021), “Çerezsiz ve Rızasız 2022” adıyla hazırladığı kılavuzda üçüncü taraf çerezlere ilişkin engellemelerin yakın gelecekte yaygınlaşması ile reklam endüstrisinin kullanıcıları nasıl tanımlayacağı ve onlara kişiselleştirilmiş reklam göstereceği üzerine güncel çalışmaları paylaşmaktadır. 1) Birinci çerez: şirketlerin web sitesi, mobil uygulamaları veya müşteri ilişkileri yönetimi veri tabanları gibi kendi çevresel kaynaklarından elde ettiği kullanıcı / tüketici verileri üzerinden hedefleme yapılabilir. 2) Tek oturum açma (Single Sign-On / SSO): tek kullanıcı kimliği ile birden fazla oturum açma imkânının sağlanması ile kullanıcılar birden çok sitede takip edilebilir. 3) Benzersiz tanımlayıcı (Unique ID): Benzersiz tanımlayıcı, kişinin siteler arası ziyaretlerinin takip edilmesini sağlar. Birden çok değişkenin bir araya gelmesiyle

kiři eşsizleştirilir. 4) Reklam / cihaz kimlięi: mobil uygulama dünyasında reklam amaçlı sıkça kullanılan ve benzersiz harf ve sayı kombinasyonundan oluşan bir tanımlayıcıdır. 5) Parmak izi: Kullanıcıları belirlemek için üst verilerinin toplanmasını içerir. Üst veriler kullanılan cihazın işletim sistemi, tarayıcısı, pil seviyesi, dili vb. verilerden oluşur ve bunların bir araya gelmesiyle kullanıcının parmak izi oluşur. 6) Gruplama (Kohort): anonimleşmiş grupların hedeflemesi bireysel kullanıcı izlemenin yerine bir alternatif sunar. (7) IP adresi: IP adreslerinin doğrudan hedeflenmesiyle oluşur. Aynı IP adresini kullanan farklı kişiler aynı reklamlarla karşılaşabileceğinden dolayı çerez kadar etkili değildir. Fakat IAB France’a göre bu yöntem açık rızanın alınması zorunluluğunu yasal olarak aşabilmektedir. Bu izleme ve veri toplama yöntemleri çerezlere alternatif olarak sunulmuştur. Diğer yandan bazı baskın teknikler de hem Google hem de reklam şirketleri tarafından oluşturulmaya başlanmıştır.

Google, kendi ürünü olan Chrome tarayıcısında üçüncü taraf çerezleri engelleyeceğini ilan etmesi Google adına bir paradoks olarak karşımıza çıkmaktadır. Bunun anlamı, Google kendi sahip olduğu tarayıcıda kendisine ait başka sitelerdeki çerezleri engelleyecektir. Dünyadaki tüm web sitelerinde üçüncü taraf çerez olarak hizmetleri en çok tercih edilen Google, FLoC (Federated Learning of Cohorts) sistemini tanıtarak kullanıcı mahremiyetine saygı duyan bir sistem geliştirdiğini açıklamıştır (Roviaro, 2020) . FLoC, kişiselleştirilmiş reklam gösterimi için bireysel veri toplama ve kullanıcı profilleri oluşturma yerine yapay zekâya dayalı olarak kullanıcıların tarama geçmişleri üzerinden profiller oluşturulmasını önermektedir. Bu model kullanıcıların ziyaret ettikleri web sitelerini toplamakta, aynı siteleri ziyaret edenleri bir araya getirmekte ve bunları makine öğrenimi desteğiyle anlamlandırarak ilgi alanları vb. kategoriler hâline getirmektedir. Yani benzer tarama geçmişine sahip benzer insanlar benzer kategoriler altında toplanmaktadır. Reklamverenler bu kategorileri hedefleyerek kişiselleştirilmiş reklam gösterebilmektedir. Kullanıcılara bizzat bir çerez atanmadığı ve çerez kimliği tanımlanmadığı için bu sistemin kullanıcı mahremiyetine önem verdiği öne sürülmektedir. Öte yandan test aşamasındaki FLoC sistemi üzerine bir araştırma yapan Rescorla (2021), sistemin anonimliği net olarak sağlayamama ve çerezlere göre daha fazla bilgi toplama gibi dezavantajları olduğunu

tespit etmiştir. Rescorla'ya göre birkaç bin kişiden oluşan bir FLoC kategorisi, tarayıcı parmakizi aracılığıyla kategori içindeki kullanıcıları birkaç kişiye kadar filtreleme imkânına sahiptir. FLoC'a ait tanımlayıcılar kullanıcıların aktivitelerine göre her hafta değişmektedir. Dolayısıyla bir hafta aynı grup içinde olan kullanıcılar diğer hafta farklı gruplarda yer alabilir. Rescorla, tanımlayıcı kimlikleri haftalık değişimi, bireysel kullanıcıların tespitini kolaylaştırabileceğini ifade etmektedir. Son olarak FLoC teknolojisinin çerezlere nazaran daha fazla bilgi topladığı bilgisi paylaşılmaktadır. Çerezlerin bir kişiyi oldukça iyi tanıması için öncelikle birçok farklı platformdan o kişi hakkında veri toplayabilmesi ve başka şirketlerle veri alışverişi yaparak sahip olduğu veri setini zengileştirmesi gerekmektedir. FLoC'a ait tanımlayıcılar tüm sitelerde aynı olduğu için kullanıcının ziyaret ettiği tüm siteler görülebilmektedir. FLoC'un şu anda çeşitli ülkelerde test aşamasındayken, yürürlüğe giriş tarihi henüz net değildir (Goel, 2021).

Tarayıcılar tarafından üçüncü taraf çerezlerin kullanıcı verilerine erişiminin kısıtlanması şirketlerin kendilerini birinci taraf çerez yapma girişimlerinin doğmasına sebep olmuştur. Birinci taraf çerezler, web sitesinin kendi alan adı uzantısına ait çerezlerdir. Bu çerezler aracılığıyla üçüncü taraf çerezlerin topladıkları kadar kapsamlı kullanıcı verileri toplanmasa da sosyal medya platformları, reklam ve analitik şirketleri siteler izin verdiği sürece bu verilere erişebilecektir.

Reklam teknoloji şirketleri, üçüncü taraf çerez olarak yer aldığı sitelerin alan adlarına yeni bir CNAME kaydı oluşturarak kendilerini birinci taraf çerez gibi gösterebilmektedir. Bu teknik ile hem izleme faaliyetlerini devam ettirebilmekte hem de sitede birinci taraf çerez olarak yer aldığı için engelleme girişimlerini atlatabilmektedir. Web sitesinde CNAME kaydı olan izleyici şirketler, birinci taraf çerezlerin eriştiği her şeye bu şekilde erişebilir ve tarayıcılar tarafından meşru olarak görülür (Olejnik, 2021). CNAME tabanlı izleyiciler, birinci taraf hâline geldikleri için web sitesindeki hassas bilgilere de doğrudan erişmesi mümkündür. 2021 yılında yapılan bir araştırmaya göre, en çok ziyaret edilen on bin web sitesinin %9,98'inde en az bir adet CNAME tabanlı izleyici yer almaktadır (Dimova vd., 2021). Sonuç olarak üçüncü taraf çerezlere alternatif bir yöntem olarak karşımıza çıkan CNAME tabanlı

izleme hem tarayıcıları hem yasaları hem de kullanıcıları bir nevi kandırmakta ve izleme faaliyetini gizlemektedir.

Çerezlere alternatif bir başka kullanıcı izleme tekniği reklam teknoloji şirketi The Trade Desk (TTD) tarafından sunulan Unified ID 2.0 (UID 2.0) adlı yöntemdir (theTradeDesk, 2021). UID 2.0, tıpkı üçüncü taraf çerezler gibi kullanıcı verilerini toplamakta ve siteler arası takip edebilmekte olan bir sistemdir. Açık kaynaklı ve ücretsiz olan bu sistemde kullanıcılar UID 2.0'ın olduğu bir sitede e-posta adreslerini onayladıkları andan itibaren sisteme dâhil olurlar. Kullanıcı yalnızca tek bir onay vermesiyle UID 2.0 ağındaki tüm web siteleri ilgili kullanıcıya kişiselleştirilmiş reklam gösterme olanağına sahip olur. Bu aşamadan itibaren UID 2.0, kullanıcı için bir eşsiz ve şifreli bir tanımlayıcı üretir ve bu tanımlayıcı üçüncü taraf çerezlerin işlevini gerçekleştirir.

İzleme teknolojilerine bir başka alternatif, kullanıcıların kendi verilerini kendi istekleriyle paylaştıkları “sıfır taraf veriler” olarak adlandırılan bir yöntemdir. İlk defa 2018 yılında adı konulan sıfır taraf veri yöntemi, yayıncıların, markaların, analitik ve reklam şirketlerinin kullanıcılardan veri toplamasıyla değil doğrudan kullanıcıların kendi verilerini onlara sağlamasıyla ortaya çıkmaktadır (Khatibloo, 2018). Bu sistem bir yandan da araştırma şirketlerinin topladıkları verilere benzemektedir. Bir mağazadan kazak alacağınız zaman istediğiniz kazağın rengi, bedeni, yapısı, tarzı, bütçe gibi değişkenleri mağaza çalışanıyla paylaşmak sıfır taraf veri mantığının fiziksel dünyadaki yansıması olarak nitelendirilmektedir. Çevrim içi ortamda en sık tercih edilen veri toplama tekniği anketlerdir (Parr, 2021). Şirketler bu yolla kullanıcıları kendi paylaştıkları veriler doğrultusunda tanımlayabilmektedir.

Teknoloji şirketleri, reklam ve analitik hizmeti sağlayan şirketler ve diğer platformlar bir yandan üçüncü taraf çerezler dışında kullanıcıları izlemenin çeşitli alternatiflerini ararken diğer yandan icat ettikleri yeni izleme teknolojileri sayesinde de birbirleriyle rekabet etmektedir. Cihazların veya tarayıcıların üçüncü taraf çerezleri tamamen veya kısmen engellemesi söz konusu şirketlerin yeni yollar üretmesine yol açacaktır. Yakın gelecekte hizmete alınacak yeni izleme teknolojileri belki de çerezlerden daha aktif ve verimli çalışma potansiyeline sahip olacaktır. Dolayısıyla

üçüncü taraf çerez kullanımının önünün kapanması, kullanıcı gözetiminin ve iş modelinin önemli bir kısmı çerezlere bağlı olan şirketlerin sonunu getirmeyecek; aksine, gözetimin yeni alternatif yöntemler aracılığıyla devam etmesine neden olacaktır.

2.1.2. Sosyal Medya Platformları ve Gözetim

Sosyal medya platformları ve diğer Web 2.0 ile ortaya çıkan platformlar, ortak üretim ve paylaşım, topluluklara, bilgi alışverişine ve iletişime odaklanmaktadır (Çakır, 2014: 104). Odak noktasındaki süreçlere ait etkinliklerin dijitalleşmesi, elektronik gözetimin derinleşmesine ve devasa miktarda kişisel verinin toplanmasına sebep olmuştur. Daniel Trottier ve David Lyon (2012: 93-104), internette kişisel verilerin toplanmasındaki değişime dikkat çekerek sosyal medya platformlarının gözetim özelliklerini Facebook örneği üzerinden beş madde ile açıklamaktadır:

(1) Kullanıcılar diğer kullanıcılarla işbirliğine dayalı bir kimlik inşa eder. Profiller, hem kullanıcıların hem de arkadaşlarının kişi hakkında kişisel bilgiler ekleyebileceği alanlarla doludur. Tüm bu bilgiler arkadaş ağıyla paylaşılır. Yorumlar yazılır, fotoğraflar eklenir, fotoğraflara arkadaşlar etiketlenir. Hem kendisi hakkında ne yazıldığına bakar, hem de başkalarının profillerini gezerek onlar hakkında bilgi toplar. Eğer kullanıcı profilinde duvarını kapatır, fotoğraf eklemeyi veya arkadaşlarının fotoğraf etiketlemesine izin vermezse genellikle bir şey gizlediği kanısına varılır.

(2) Reklamcılar, işverenler ve diğer kurumsal gözetleyiciler zengin kullanıcı bilgisine erişebilir. Kullanıcılar profillerini oluştururken, yorum yazarken veya fotoğraf yüklerken bunu kimlerin göreceğini az çok tahmin ederler. Kafalarında belirli bir kitle vardır. Yine de bu kitle, örneğin arkadaş listesi, kullanıcı bilgisine erişimi olan insanların yalnızca küçük bir bölümünü oluşturur. Platformlar, kullanıcıların sosyal ağlarda izlenmesine yardımcı olur.

(3) Facebook gibi siteler sosyal bağlantıları görünür, ölçülebilir ve aranabilir içeriklere dönüştürür. Sosyal medya ile bireylerin profilini çıkarmak

sıradan bir özellik hâline gelir. Araştırmacılar, gerek kullanıcı gerekse arkadaşlarıyla ilgili verileri toplayarak çıkarımlar yapabilir.

(4) Sosyal medya platformlarının ara yüzü ve içeriği daima değişime uğrar. Eklenen yeni özellikler ile kullanıcılardan yeni bilgiler talep eder ve sürekli yeni bilgi toplayabileceği özelliklerin geliştirilmesini sağlar. Gizlilik ayarları daha şeffaf hâle geldikçe daha da karmaşık bir düzenleme sistemi ortaya çıkıyor.

(5) Sosyal medya içeriğin bağlamını kolayca değiştirir. Facebook’a yüklenen bir bilgi bağlamından giderek uzaklaşır. Sosyal medya gözetimi birçok bağlamdan toplanan verilerin bir araya getirilerek oluşmuş profillerin gözetimidir. Çağdaş gözetimin temellerinde olduğu gibi; belirli bir bağlamda ve ortamdaki toplanan veri, başka bir yerde incelenir ve inceleme sonuçları yine başka bir bağlamda ortaya çıkabilir.

Trottier ve Lyon, bu başlıklar altında sosyal medya platformlarında gerçekleşen aktivitelerin kullanıcıların kontrolünden nasıl çıktığını ve bu durumun gözetimdeki artan “akışkanlığı” daha da artırabildiğini tartışmaktadır (2012: 103).

Fuchs and Trottier (akt. Fuchs, 2015: 402), entegre olan ve yakınsayan gözetimin, sosyal medya gözetiminin belirli bir özelliği olduğunu ifade eder. Onlara göre, Facebook gibi sosyal medya platformlarında farklı sosyal rollerdeki (gelir düzeyi vb.) çeşitli sosyal etkinlikler (bilişsel, iletişimsel) ve yaşam dünyasına ait bilgiler (siyasi görüş, özel hayat) tek bir profile eşleştirilmiştir. Bu eşleştirme sürecinde sosyal roller içindeki sosyal etkinlikler hakkında veri üretimi söz konusudur. Bu durum, bir Facebook profilinin içerisinde şunların olduğuna işaret eder: (1) Kişisel veriler, (2) İletişimsel veriler, (3) Kişisel rollere (arkadaş, sevgili, baba, akraba), sivil rollere (aktivist, hayran, dernek üyesi) ve sistematik rollere (siyaset bağlamında politikacı, bürokrat, seçmen - ekonomi bağlamında: işçi, yönetici, iş sahibi, tüketici) ilişkin sosyal ağ ve topluluk verisi. Farklı sosyal roller ve etkinlikler sosyalleşmenin, yakın ilişkilerin ve boş zaman etkinliklerinin yürütüldüğü durumlarda yakınsama eğilimi gösterir. Tıpkı, büyük teknoloji şirketlerinin çalışma alanlarını oyun alanı hâline

dönüştürmesi ve iş ile oyunun birbirine entegre olması gibi. Bunun anlamı sosyal medya gözetiminin, yakınsayan, birbirine entegre bir gözetleme biçimi olduğudur.

Sosyal medyanın artık sosyal medya olmadığı belirten Vaidhyathan (2018:103), tüm medya şirketlerinin “sosyal” hâle gelmeye çalıştığını; bunun arkasında yatan nedenin ise “*sosyal bağların yapışkanlığı sayesinde kişinin dikkatini çekmeye çalışan başkalarını savuşturma*” olarak tanımlar. Medya şirketleri, hizmetlerini ne kadar “sosyalleştirir” ve insanları kendine ne kadar “bağlarsa”, diğer rakiplerinde daha az zaman geçiren kullanıcılar şirket için daha değerli bir meta hâline dönüşür. Kendi platformunda daha fazla zaman geçiren kullanıcı, hem daha fazla veri üretir hem de daha fazla reklam görüntüler. Aynı şekilde Fuchs da (2015: 399) zamanın, ticari sosyal platformlar için kilit bir role sahip olduğunu dile getirir. Böylelikle değer, Facebook gibi sosyal ağlarda, kullanıcının web sitesi veya mobil uygulama içinde geçirdiği ortalama zamanla oluşur (a.e., s. 374). Öte yandan bu platformlarda zaman geçirirken *kimsenin zorlayarak yaptırmadığı* fikir akıllara gelmektedir. Oysaki sosyal ağların kullanımında doğrudan değil dolaylı bir zorlayıcı unsur söz konusudur. Dolaylı zorlayıcı unsur, ağ platformlarının dışında kalındığında yaşanabilecek dezavantajları içerir: iş fırsatlarını kaçırma, kişisel temaslar uzak kalma, toplumsal ilişkileri yitirme gibi (Ekman, 2019:109). İçerde kalmanın maliyeti ise çevrim içi hareketlerimizin izlenmesine ve ticari amaçla satılmasına göz yummaktır.

Sosyal medya platformlarında haber kaynakları, yorumlar, fotoğraflar, günlük yaşam aktiviteleri ve ilgi alanları ticari avantajlar edinmek için veri noktalarına indirgenir. Platformda geçirilen süre, platforma sağlanan veri kaynağına dönüşür (Ferguson, 2017: 175). Bu şekilde sosyal medya platformları, geleneksel kitle medyasına göre insanlar hakkında daha keskin bilgilere erişir ve onları diledikleri biçimde sınıflandırabilir. Kitle medyası izleyicilerini yığınlar hâlinde ve daha soyut dilimler olarak bilirken, yeni medyada bireye inmek mümkündür (Fisher, 2019: 138). Platform içindeki etkinlikler kişinin daha iyi tanımlanmasını sağlar; böylece kişi, belirli kategorilerle ilgilenen şirketler / reklamverenler için değerli birer tüketici veri seti hâlini gelir. Dijitalleşen insan iletişimi ve deneyimleri, platformların kârlılığını garanti altına alan metalar olarak karşımıza çıkar.

Sosyal medya platformlarında gözetim yalnızca ağ sahipleri tarafından değil şirketler tarafından da kullanıcıların etkileşime girdiği her alanda gerçekleşmektedir. Örneğin, Coca Cola'nın soğuk çay markalarından biri olan Gold Peak, kullanıcıların Facebook, Instagram ve Twitter'da herkese açık olarak paylaştıkları fotoğrafları tarayarak kaydetmiş ve onlara paylaştığı fotoğraflara göre reklam gösterimi gerçekleştirmiştir (Dua, 2017). Gold Peak, hazırladığı özel görüntü yazılım motoruyla rakipleri olan Snapple, Honest Tea, Lipton vb. markaların kutularını veya bardaklarını paylaşan kullanıcıları bulur. Sonrasında bahsi geçen kullanıcıları hedefler ve kendi reklamlarını gösterir. Yani, bir kullanıcı Instagram'da Lipton soğuk çayın olduğu bir masadan fotoğraf paylaştığı anda yazılım motorunun ağına takılır. Gold Peak, kullanıcıyı potansiyel müşteri olarak hedefler ve kullanıcı birkaç saat sonra girdiği bir haber sitesinde veya sosyal medya platformunda Gold Peak reklamıyla karşılaşabilir.

Fuchs, *“Gözetim toplumunda sosyal ağ siteleri”* başlıklı araştırmasında katılımcılara Facebook ve diğer ticari sosyal medya platformlarında üretilen emek, kişisel veri metalaşması ve platformların ücretsiz hizmetleri ile emeğin mübadelesini kabul edip etmediklerini soran bir araştırma gerçekleştirmiştir. Araştırma sonucunda katılımcıların %82,1'inin (n=3558), web sitelerinde kişiselleştirilmiş reklam görmek istemedikleri tespit edilmiştir (Fuchs, 2015: 424). PewResearch'in ABD'de yaptığı bir araştırmada ise halkın %81'i, şirketler tarafından toplanan veriler nedeniyle karşılaştıkları potansiyel risklerin onlar için sağlanacağı faydalardan daha ağır bastığını söylemiştir. Aynı zamanda ankete katılanların %79'u verilerinin şirketler tarafından nasıl kullanıldığına ilişkin endişe duyduğunu dile getirmiştir (Auxier vd., 2019). PewResearch'in bu sefer Facebook üzerine yaptığı bir başka araştırmada, kullanıcıların %74'ü Facebook'un ilgi alanlarına göre kategorilendirdiği listeyi bilmediğini söylemiştir. Araştırmaya katılanların yarısı, Facebook'un ilgi alanlarına göre insanları kategorilere ayırmasından rahatsız olduklarını ifade etmiştir (Rainie - Hitlin, 2019). Bu gibi araştırmalar sosyal medya platformlarındaki gözetimin görünen küçük bir kısmının bile toplum nezdinde endişe verici olduğunu göstermektedir.

2.1.3. Mobil Uygulamalar ve Gözetim

Akıllı telefon ve tabletler gündelik yaşam içerisinde başta iletişim olmak üzere sosyalleşmek, iş süreçlerini yönetmek, fotoğraf / video çekmek veya oyun oynamak gibi birden çok amaca yönelik kullanılmaktadır. Tüm bu işlemleri yürütmek için ise söz konusu cihazlarda uygulamalara ihtiyaç vardır. İletişim kurmak için mesajlaşma, sosyalleşmek için sosyal ağ veya başka hizmetler için çeşitli uygulamalar mobil uygulama mağazalarında yer almaktadır. Veri analiz şirketi App Annie'nin 2017'de yürüttüğü bir araştırmada, ABD'li akıllı telefon sahipleri günde ortalama 2 saat 15 dakikalık bir zamanı mobil uygulamaları kullanarak geçirdiği saptanmıştır. Bu süre Güney Kore, Brezilya ve Japonya gibi ülkelerde 3 saati geçmektedir. Aynı araştırmada, bir kişinin akıllı telefonunda yüklü mobil uygulama sayısının ise 60 ile 90 arası olduğu belirlenmiştir (Thompson, 2017). eMarketer'ın Nisan 2020'de yaptığı araştırmaysa geçen üç yıllık sürede mobil cihazlarda geçirilen sürenin arttığına işaret etmektedir. Araştırmada mobil internette geçen ortalama zamanın 4 saatten fazla olduğu, bu sürenin %88'inin mobil uygulamalarda olduğu hesaplanmıştır (Wrumser, 2020). Statista verilerine göre Eylül 2020 itibariyle yalnızca Google Play'de 3 milyon, Ağustos 2020 itibariyle Apple Store'da 4.4 milyon mobil uygulama yer almaktadır (Clement, 2020). Google Play'de yer alan uygulamaların %96'sı ücretsizken (Clement, 2020b), bu oran Apple Store'da sadece %8 (Clement, 2020c) olarak karşımıza çıkmaktadır. Tüm bu araştırma ve veriler, mobil uygulamaların ne kadar sık kullanıldığını ve kullanıcılar için ne kadar değerli olduğunu ortaya koymaktadır. Uygulama üreticileri tarafından bakıldığında ise kullanıcının değeri azımsanmayacak kadar önemlidir.

Mobil cihazlar insanın her an yanında taşıyacağı, konumu kolayca belirlenebilen, kamerası ve mikrofonu olan bir cihaz olarak tasarlanmış ve bu özellikleri onun bir gözetim aracına dönüşmesine katkı sağlamıştır. En mahrem ve hassas bilgilerin üretildiği, paylaşıldığı ve emanet edildiği cihazların başta işletim sisteminin kendisi olmak üzere mobil uygulamalar tarafından gözetlendiği aşikârdır. Akıllı telefonların yaygınlaşmasından önce, 2008 yılında, Google *mobil cihazlar için açık ve kapsamlı bir platform* geliştirmek için teknoloji üreticileri ve telsiz

operatörleriyle bir anlaşmaya varır. O dönemde yorumcular, Android telefonla Google'ın Apple ile rekabet etme fırsatı yakaladığını ve pazardaki pastadan pay alabileceğini düşünür; fakat Google'ın hedefi farklıdır. Google, Android işletim sistemini Samsung, Lenovo, LG vb. mobil cihaz üreticilerine ücretsiz olarak sağlar. Böylelikle Google, arama hizmeti başta olmak üzere tüm Google hizmetlerini cihaz kullanıcılarına kullandırarak onların davranışsal gözetimini sağlamayı amaçlamıştır (Zuboff, 2019: 133-134). 2009 yılında, o dönem Google Finans Müdürü Patrick Pichette'in finansal analistlere yaptığı söyleşide, bir soru üzerine verdiği cevap, Google'ın Android ile davranışsal gözetimi cep telefonlarında da devam ettirmesinden duyduğu heyecanı göstermektedir: *“Açık kaynak kodlu olduğu için maliyeti düşürerek (ucuza satarak) bu cep telefonlarının benimsenmesini sürdürürsek, kaç arama yapılacağını düşünün!”* (Schonfeld, 2009). Kendi sağladığı hizmetlerin kullanımıyla ortaya çıkan verilerin yanı sıra konum gibi veriler de Google'ın gözetimine dâhil olmuş; böylece derinlemesine bireysel gözetim ağının inşası Android işletim sistemi ile birlikte başlamıştır.

Bugün satın alınan Android işletim sistemine sahip bir akıllı telefon ilk açıldığı zaman varsayılan olarak birden çok Google hizmetine ilişkin uygulamalarla karşılaşmaktadır. Özetle bunlar Google Play Store, Google Search, Google Chrome, Google Drive, Gmail, Google Duo, Google Maps, Google Play Music, Google Photos, Google Play Movies ve YouTube gibi uygulamalardan oluşmaktadır. Çeşitli hizmetler içeren bu uygulamalar, Google sunucularıyla sürekli veri alışverişinde bulunarak çıkarılan kişi profilini zenginleştirmektedir. Aktivist Aral Balkan, 2018 yılında *Future Fest by Nesta* organizasyonunda gerçekleştirdiği sunumda, Google'ın iş modelini Apple ile kıyaslayarak şu şekilde açıklamaktadır (Nesta - The Innovation Foundation, 2018):

“Fiziksel bir ürün satın alındığında ürünü satan daha sonrası ile ilgilenmez, çünkü kârını yapmıştır. Apple da böyledir. Fakat Android işletim sistemli bir telefon alıp bunu ertesi gün çöpe attığınızda bu durum Google'ın işine gelmez. Android'in olduğu bir telefonda kullanıcının hiçbir davranış sergilememesi, onun hakkında hiçbir veri üretilmemesine neden olur. Dolayısıyla, Google'ın kâr etmesini sağlayan kullanıcının telefonu sık sık kullanmasıdır.”

Balkan'ın ifadeleri mobil gözetim bağlamında yalnızca Google üzerinden değil; neredeyse tüm mobil uygulamaları kapsayacak şekilde okunabilir. Zira her yeni teknoloji şirketi veya mobil uygulama, bedava ve yenilikçi çözümlerinin finansmanını gözetime dayandırmakta ve iş modelini gözetim üzerine inşa etmektedir. Uygulamaların bu iş modelinin finans kaynağı genellikle reklamdır ve izleme faaliyetleri hedefli davranışsal reklam hizmetlerinde kullanılmak üzere kullanıcı davranışlarının gözetimini içerir. Buna bağlı olarak birçok uygulama tüm kullanıcı davranışlarını kayıt altına alır ve birden çok üçüncü taraf izleyicilerle paylaşır. Yale Privacy Lab ve kar amacı gütmeyen bir güvenlik kuruluşu olan Exodus Privacy'deki araştırmacılar, akıllı telefon uygulamalarındaki kullanıcı izleme yazılımlarının neler olduğunu inceledikleri çalışmada 300'den fazla uygulamada 44 farklı izleyicinin olduğunu tespit etmişlerdir. Araştırmanın örnekleminde küçük ve ortak ölçekli uygulamalar olduğu gibi Spotify, Soundcloud veya Tinder gibi milyonlarca kişi tarafından indirilen uygulamalar da yer almıştır (O'Briend - Kwet, 2017). Araştırma raporu iki ana sonucu ortaya çıkarmaktadır: (1) eğer bugün izlenmiyorsanız, önümüzdeki günlerde mutlaka izleneceksiniz, (2) hava durumu, el feneri vb. görünüşte masum olan uygulamalar bile çok sayıda izleme yazılımlarıyla doludur ve hedefli reklamla doğrudan ilişki kurarak davranışsal veri toplamaya devam eder (Zuboff, 2019: 137).

Mobil uygulamaların cihazlardan ihtiyaç fazlası talep ettiği izinler gözetimin derinleşmesine neden olarak, farklı kurum ve kuruluşlara veri teminine olanak sağlamaktadır. Ekran ışığını değiştirmek için kullanılan bir uygulama kullanıcının konumuna, bir alışveriş uygulaması kişi listesine veya bir sözlük uygulaması kameraya erişmek isteyebilir. Bazen hiç sorulmadan, bazense kabul et seçeneğinden başka bir seçenek sunmadan kullanıcıyı zorlayarak kabul ettirilen bu erişim talepleri ile cihaz, hiç bilinmeyen uygulamalar tarafından gözetlenmeye başlamaktadır. Elde edilen veriler genellikle üçüncü taraflarla paylaşılabilir, reklam uygulamalarında kullanılabilir veya satılabilir. Aralık 2019'da The New York Times'ta yayımlanan bir makale, çeşitli mobil uygulamaların 12 milyondan fazla ABD'li vatandaştan topladığı 50 milyardan fazla konum verisini ele almakta ve konuyu hem gözetim hem de gizlilik

bağlamında tartışmaktadır (Thompson - Warzel, 2019). Makalede verilerin bir Telekom şirketinden, Facebook / Google gibi büyük teknoloji şirketlerinden veya devletin gözetim araçlarından değil; sıradan uygulamaların farkında olunmadan sessizce topladıkları konum bilgisinden geldiğine yer verilmiştir. Daha açık şekilde ifade etmek gerekirse, bir sözlük uygulaması kişinin o an nerede olduğunu, kiminle buluştuğunu, akşamı kiminle geçirdiğini, nerede alışveriş yaptığını, hangi psikoloğa gittiğini veya nereyi sıklıkla ziyaret ettiğini bilme becerisine sahiptir. Bu verileri arz ve talep doğrultusunda satabilir veya kişi hakkında farklı uygulamalardan başka veriler satın alarak elindeki veri setini zenginleştirebilir. Makalede ayrıca konum verilerini toplayan şirket ve uygulamaların gözetimi meşrulaştırmak için üç söyleme yer verdikleri belirtilmiştir: (1) insanlar izlenmeye rıza gösterir, (2) toplanan veriler anonimdir, (3) veriler güvendedir. Rıza ve güvenlik konuları tartışmalıdır zira verilerin The New York Times'a gönderilmesi onun güvenli olmadığını açıkça bir kanıttır ve şirketlerin rıza olarak bahsettiği şey baskıyla el koymak olarak ifade edilebilir. Bunun dışında konum verilerinin şahsın adı, soyadı veya e-posta adresleriyle birebir ilişkilendirilmediği ve anonim olduğu doğru bir yaklaşımdır. Fakat haritada gösterilen konum noktaları ve günlük rutin birleştirildiğinde kişinin kim olduğunu tespit etmek çok da zor değildir. Örneğin, de Montjoye vd. (2013) bir buçuk milyon insanın beş aylık hareket verilerini incelemiş ve dört mekân-zamansal (saat ve konum) veri noktasına sahip olmanın bireylerin kim olduğunu tahmin etmede %95 oranında yeterli olduğunu ortaya koymuşlardı. Bu çalışma gösteriyor ki anonimlik belirli rutinleri bir araya getirerek anlam üreten algoritmalar karşısında pek mümkün değildir. Çevrim içi gözetim endüstrisi, mobil cihazlardan ihtiyacından fazla izin talep eden uygulamaların bunu meşrulaştırma ve sıradanlaştırma eylemleri ile büyümeye devam etmektedir. Kullanıcıların gözetimden kaçınmasıysa neredeyse imkânsız hâle gelmiştir.

Mobil uygulamaların kullanıcıları nasıl gözetlediğini ele alan bir örnek paylaşmak yerinde olacaktır. Tablo 2.3'de Google Play üzerinden 10 milyondan fazla indirilmiş bir fener uygulamasının detaylı gözetim tablosu yer almaktadır. Bu tabloda hem uygulamanın cihazdan erişmek istediği izinler, hem de uygulama kullanım verilerini paylaştığı üçüncü taraf platformlar yer almaktadır.

11 İzleme Kodu		15 Cihaza Erişim İzinleri	
Facebook Analytics > analytics	Google Firebase Analytics > analytics	! ACCESS_COARSE_LOCATION yaklaşık konuma erişim (ağ tabanlı)	! SYSTEM_ALERT_WINDOW Diğer uygulamaların üzerinde görünebilme
Facebook Login >	Inmobi >	! ACCESS_FINE_LOCATION kesin konuma erişim (GPS ve ağ tabanlı)	WAKE_LOCK Uyku modunu engelleme
Facebook Places >	Integral Ad Science >	ACCESS_NETWORK_STATE ağ bağlantılarını görüntüle	! WRITE_EXTERNAL_STORAGE SD kartın içeriklerini değiştirme veya silme
Facebook Share >	Moat > analytics advertisement	ACCESS_WIFI_STATE Wi-Fi bağlantılarını görüntüle	BILLING
Google AdMob > advertisement	Twitter MoPub > analytics advertisement	! CAMERA fotoğraf ve video çekme	RECEIVE
Google CrashLytics > crash reporting		INTERNET İnternete tam erişim	BIND_GET_INSTALL_REFERRER_SERVICE
		! RECORD_AUDIO Ses kaydı	READ_GSERVICES
			C2D_MESSAGE
El Feneri  		RV AppStudios Araçlar PEGI 3	
		! İşareti olanlar Google'ın güvenlik politikalarına göre "Tehlikeli" ve "Özel" olarak kabul edilir.	

Tablo 2.3: RV AppStudios Tarafından Geliştirilen El Feneri (Flashlight - Torch LED Light) Mobil Uygulamasında Yer Alan İzleme Kodları ve Uygulamanın Cihazdan Talep Ettiği Erişim İzinleri.

Analiz, Exodus Privacy aracılığıyla gerçekleştirilmiştir.

(Kaynak: <https://reports.exodus-privacy.eu.org/en/reports/com.rvappstudios.flashlight/latest/>)

RV AppStudios şirketi tarafından geliştirilen fener uygulaması kullanıcılarına çeşitli özelliklerle “ışık” vadetmektedir. Uygulamanın gözetim araçları incelendiğinde karşımıza ilk olarak Facebook, Google ve Twitter gibi büyük şirketlerin izleme yazılımları çıkmaktadır. Bunlar analiz (Facebook Analytics), reklam (Google AdMob) ve uygulama geliştirmeye ilişkili (Google CrashLytics) yazılımlardan oluşmaktadır. Söz konusu bilinen platformların yanı sıra Hindistan merkezli mobil reklam şirketi Inmobi, ABD’li reklam doğrulama hizmetleri sağlayan Integral Ad Science ve Oracle’ın dijital reklam analiz aracı olan Moat izleme faaliyetleri arasında yer almaktadır. Tüm izleme faaliyetleri kullanıcının davranışlarına ve dikkatine odaklanmaktadır. Ayrıca, belirtilen izleme kodlarının kullanıcının başka uygulamalarında da yer alması olasıdır. Örneğin Google AdMob veya Inmobi’nin izleme yazılımları kullanıcının indirdiği başka bir uygulamalarda da yer alıyorsa, bu sistemler farklı kanallardan veriler elde ederek kişi hakkında inşa edilen profili rahatlıkla zenginleştirebilir.

El feneri uygulamasının içerisindeki üçüncü taraf izleyicilerin kimler olduğunu ve ne amaçla izleme faaliyetinde bulunduklarını tespit ettikten sonra söz konusu uygulamanın cihazdan hangi izinleri talep ettiğini ve nerelere erişebildiğini inceleyebiliriz. İzinler uygulamanın cihazda hangi eylemlerde bulunabileceğini açıklar. Tablo 3’de yer aldığı gibi, uygulama cihazdan 15 adet izin talep etmiş ve bu alanlara erişim sağlamıştır. Bunların 6’sı Google’ın Android güvenlik seviyesine göre “tehlikeli” ve “özel” izin kategorisinde değerlendirilmiştir. Hassas olarak ifade edebileceğimiz 6 iznin nelerden oluştuğunu ve neden “tehlikeli” olduğunu aşağıdaki gibi inceleyebiliriz:

- 1) *ACCESS_COARSE_LOCATION*: Ağ tabanlı olarak, WIFI veya mobil hücre verisini (veya her ikisini) kullanarak cihazın ortalama konumunu tespit eder.
- 2) *ACCESS_FINE_LOCATION*: WIFI ve mobil hücre verisinin yanı sıra küresel konumlandırma sistemini de (GPS) kullanarak cihazın net olarak konumunu belirlemeye çalışır.
- 3) *CAMERA*: Cihazın kamerasına erişebilir ve tüm özellikleriyle kullanabilir. Video ve fotoğraf çekebilir.
- 4) *RECORD_AUDIO*: Cihazın mikrofonuna erişebilir.
- 5) *SYSTEM_ALERT_WINDOW*: Bu izin, bir uygulamanın kullanıcıyı bilgilendirmede diğer uygulamaların üzerinde bir pencere görüntülemesini sağlayabilir. Bankacılık uygulamalarının oturum açma sayfalarıyla aynı tasarım ve görüntüyü oluşturarak bilgi toplayan casusluk durumlarına neden olabilir (Cobb, 2017).
- 6) *WRITE_EXTERNAL_STORAGE*: Bu izin verildiğinde, uygulamalar harici depolama alanına dosya kaydedebilir, düzenleyebilir veya silebilir.

Verilen izinler nedeniyle el feneri uygulaması, kullanıcının nerede olduğunu bilir, sesini kaydedebilir, fotoğraf / video çekebilir, depolama alanına erişerek tüm dosyaları görüntüleyebilir ve silebilir.

Bankacılık uygulamalarından yemek siparişine kadar hayatı kolaylaştırmaya yardımcı tüm hizmetlerin insanın yanı başından ayırmadığı cihazlarda yer alması ne kadar değerliyse, cihazın kendisiyle sıkı bir ilişki içinde olan kullanıcının verileri ve

bu verilerin kimlerle paylaşıldığını bilmesi de bir o kadar değerlidir. Mobil uygulamaların topladığı veriler kendi hizmetlerini geliştirmede fayda sağlayabilir. Fakat ihtiyacından fazlasını habersiz toplaması, saklaması ve üçüncü taraflarla paylaşması bir problem olarak karşımıza çıkmaktadır. Ayrıca bu verilerin başka kişi, kurum ve kuruluşların eline geçmesi veya meta biçiminde pazarda satışa sunulması ihtimali de göz ardı edilmemelidir. Kullanıcıların şeffaf bir kullanım deneyimine sahip olması, verilerin dağıtımını yönetebilmesi ve üçüncü taraflarla paylaşılan verilerin mobil cihazda saklanması gerektiğini ifade edebiliriz.

2.1.4. Nesnelerin İnterneti (IoT) ve Gözetim

2013 yılında bir milyar cihaz internete bağlanırken, bugünden itibaren her beş yılda bir internete bağlanan “şey”lerin ikiye katlanacağı tahmin edilmektedir. Bu büyümeyi sağlayan faktörler arasında sensör maliyetlerinin azalması, internet bant genişliğinin artışı, kablosuz bağlantı ve bulut hizmetleri ile dijital enformasyonun saklanma ve erişim maliyetlerindeki kayda değer azalma yer almaktadır (Chaston, 2015:23). İnternete bağlanan cihazlar ve nesnelerin interneti fenomeni genellikle olumlayıcı bir bakış açısıyla tartışılır. Bernard Marr (2018), nesnelerin interneti teknolojisini üretici ve tüketicinin karşılıklı faydasına olan bir “yenilik” olarak görmektedir. Ona göre, nesnelerinin interneti kişi zorlandığında ona yardımcı olmak, stres seviyesi yükseldiğinde uyarmak, zor bir gün geçirdiğini anlayıp ona göre müzik seçimi yapmak, aydınlatmayı düzenlemek (2018: 18) gibi birçok konuda yardımcı olacak büyük bir potansiyel taşır. Ayrıca, insanların giyilebilir teknoloji verilerini çeşitli kurumlara açarak indirimler kazanabileceğini (sağlık verilerini sigorta şirketleriyle paylaşmak gibi) örneklendirerek (2018: 53-54) insanların “*bir ürün/hizmet veya maddi ödül karşılığında kendi özel verilerinin ticaretini yapma*” imkânına sahip olduğunu belirtir. Marr’ın olumlu açıdan yorumladığı nesnelerin interneti teknolojisi, gözetim bağlamında eleştirel perspektifle irdelenmesi gereken birçok konu barındırmaktadır.

Günümüzde gözetim çoğunlukla somut olanı izleme üzerine değil, elle tutulmayacak dijital verilerin takibi, toplanması ve analiz edilerek öngörüler üretilmesi

amacıyla gerçekleşmektedir. Sürecin dönüşümünde ise her şeyin dijitalleşmesi yer almaktadır. Özellikle düşünce, durum ve eylemlerin dijitalleşmesi onları gözetlenebilir nesneler hâline getirmiştir. Tüm bu aktiviteler cihazlar üzerinde dijital hâle gelirken, yeni yazılım sistemleri ve algoritmalar cihazları izleyerek kişi hakkında bilgi sahibi olmaya başlamıştır. Akıllı cihazlar, kullanımı sırasında veya hiç kullanılmadığı zamanda bile sayısız veri üretebilir, kişinin rutinini yakalar ve bazen bir kısmı hassas, özel nitelikli olan veriler de üretimin içerisinde yer alır. Ağlara bağlanabilen cihazların gözetim nesnesine nasıl dönüştüğü, hem üreticisine hem de üçüncü taraflara nasıl veri sağladığı önemli bir tartışma konusudur.

Veri büyüklüğündeki artışın bir önemli nedeni nesnelerin internetidir. Nesnelerin interneti, ağ üzerinden veri toplayan ve ileten tüm cihazları ifade etmek için kullanılır (Marr, 2018: 15) ve gelecekte herhangi bir ürün veya cihazın internete bağlanabilme ihtimalini içinde barındırmaktadır (Lokke, 2018: 30). Nesnelerin internetinin temel bileşeni yerel internet protokolü (IP) adresleri aracılığıyla internete bağlı bir grup cihazdan oluşmasına rağmen, radyo vericileri yoluyla belirli bir amaç için bir ağa bağlanan bir grup cihaz olarak daha doğru biçimde tanımlanabilir (Friedland, 2017:200). Özellikle teknoloji şirketleri nesnelerin interneti alanına ve buna yönelik çalışmalara yüklü yatırımlar yapmaktadır. Google, 2014 yılında akıllı ev otomasyon şirketi olan Nest'i 3,2 milyar dolara satın almıştır. Google, Nest'i satın aldığı zaman bağımsız bir şekilde faaliyetlerine devam edeceğini ifade etmiştir. Yani, Nest'in evlerden topladığı veriler ile Google hizmetleri arasında bir birliktelik söz konusu olmayacaktı. 2018 yılına gelindiğinde ise Nest'i Alphabet'in bünyesine alacağını duyurmuştur. Nest'in donanımı ile Google yazılımlarının birleşiminin “daha düşünceli bir ev yaratmak” çabasına destek olacağı belirtilmiştir (Osterloh, 2018). Nesnelerin interneti pazarına olan iştahı Zuboff şu şekilde yorumlamaktadır:

“Eğer Google bir arama şirketiye neden akıllı ev cihazlarına, giyilebilir cihazlara ve şoförsüz arabalara yatırım yapıyor? Facebook bir sosyal ağ ise, neden insansız hava araçları ve artırılmış gerçekliğe yatırım yapıyor? Bu çeşitlilik bazen gözlemcilerin aklını karıştırabilir, ancak genellikle vizyoner yatırım olarak görülür ve alkışlanır. Yatırımların asıl amacı ise gelecek üzerine mükemmel tahmin yürütülmesidir.” (Zuboff, 2019: 129).

Zuboff'a göre teknoloji şirketlerinin satın alma veya yatırım yapma amacı, ellerindeki veri setini zenginleştirme girişimidir. Google gibi şirketler hâlihazırda aramalardan, web sitelerinden, mobil uygulamalardan ve sağladıkları çeşitli dijital hizmetlerden veri toplamaktadır. Bunun yanı sıra internete bağlanabilen farklı cihazlardan erişebilecekleri veriler, sahip oldukları mevcut verilerin genişlemesine katkıda bulunarak insan hakkında daha fazla bilgi sahibi olunmasını yardımcı olur. Her kaynaktan bir araya getirilecek veriler ise insanın geleceğini tahmin etmede büyük bir avantaj sağlar.

Nesnelerin internetinin geliştiği ve yaygınlaştığı bazı alanlar arasında sağlık sektörü, giyim ve giyilebilir ürünler, elektronik cihazlar, evler ve taşıtlar bulunmaktadır. Friedland (2017: 202 - 209) bu alanları şu şekilde açıklamaktadır:

a) Sağlık: Fitbit cihazlar, atılan adımları, kalp atımını, nabızı, uyku yeterliliğini ve diğer biyometrik (kişiyi tanımlayan özel) verileri özenle ölçmektedir. Cihazlar, biyometrik verileri kaydedip aktarır, böylece saklanabilir, sınıflanabilir ve değerlendirilebilir hâle gelir. Aktarılan veriler cihaz üreticileri ve diğer üçüncü taraflarla kolayca paylaşılabilir.

b) Giyilebilir teknoloji: Başta kol saati olmak üzere, takılar, gömlekler ve diğer kıyafetler en yaygın giyilebilir teknoloji ürünlerdir. Yakın zamanda daha da çeşitlenecek giyilebilir teknolojilerin, milyarlarca bayt veri toplayıp üreticilerine iletebilecek yerleşik veri noktaları hâlini alması öngörülmektedir. Bazı kıyafetler kalp atışını ve nefesi ölçebilir, hatta kasların kullanım hareketliliğinin takip edebilir. Giyilebilir teknolojilerin potansiyelini bunlarla sınırlı değildir. De Mooy ve Yuan (2017), sensör sayısı arttırıldığında giyilebilir teknolojilerin vücudun tüm bölümlerinden veri toplayabileceği gibi, bu verilerin içerisinde koku gibi çevresel öğelerin ve kişinin ruhsal durumunun da olabileceğini ifade etmektedir. Yani, giyilebilir teknolojik bir ürün, kişinin duygusal durumunu vücut sıcaklığındaki ani değişimlerden veya hareketlerinden anlayıp bunu paylaşabilmektedir.

c) Geleneksel elektronik cihazlar: Bu cihazlar arasında cep telefonları, oyun platformları, müzik çalarlar ve televizyon gibi cihazlar yer alır. Özellikle telefonlar, mini bir bilgisayara dönüşürken nesnelerin interneti için çok amaçlı bir radyo vericisi işlevini sürdürür. Örneğin, telefon hattının bağlandığı baz istasyonu, telefon şirketleri tarafından ortalama konum tespit etmek için sürekli olarak izlenir. Mobil gözetim başlığında yer aldığı gibi, telefon kullanılmadığında bile önemli veriler paylaşılır ve mobil uygulamalar hem kendilerine hem de üçüncü taraflara kişi hakkında veri sağlar.

d) Akıllı ev sistemleri: Akıllı evler, birden fazla yarı otonom ağı sahiptir: bunlar akıllı termostatlara, aydınlatma, elektrikli aletleri gibi cihazlardan oluşur. Birbirleriyle etkileşim içinde çalışan bir grup toplu öz-gözetim sistemi olarak ifade edilebilir. Ev sakinlerinin ne zaman evde olduğu, ne kadar uyuduğu, hangi odalarda zaman geçirdiği gibi veriler akıllı termostatlara aracılığıyla bilinebilir. Aydınlatma sistemleri, gece uykusundan uyanan birisinin gözünü almaması için ışığın derecesini ayarlayabilir, bu arada ne kadar sürede ayakta kaldığını kaydedebilir. Bunların yanı sıra evin elektrik tüketim bilgileri (yoğun saatler vs.) izlenebilir. Küresel akıllı ev piyasası 2020’de 78,3 milyar dolarlık bir paya sahiptir ve payın 2025’te 135 milyar dolara yükselmesi beklenmektedir (Businesswire, 2020).

e) Akıllı taşıtlar: Taşıtlarda bir süredir sensör tabanlı sistemler yer alsa da artık aracın çalışmasıyla ilgili çeşitli istatistik verileri ölçen kara kutular yer almaktadır. Bu kutular kat edilen kilometreleri, hızı ve diğer bilgileri izler. Bu bilgiler otomotiv üreticileri tarafından takip edilir. Üreticiler görünürde topladıkları verilerle kendi ürünlerini geliştirmeyi amaçlar; diğer yandan da bu verilerin yapacağı maddi katkıyı da göz ardı etmez. Örneğin, Ford’un CEO’su Jim Hackett, 2018 yılında Ford’un yeni gelir kaynağı olarak 100 milyon Ford sürücüsünden toplayacakları veriler olduğunu belirtmiştir (Seals, 2018).

Yapay zekâ ve nesnelerin interneti yukarıda değinildiği gibi geleneksel şirketler tarafından da yaygın olarak kullanılmaktadır. İnternete bağlanan cihazlar, sensörler aracılığıyla her gün yaklaşık 3,5 kentilyon bayt veri üretir; yapay zekâ,

toplanan ve depolanan verilerle kendini geliştirir. Günlük olarak toplanan veriler, tahmine dayalı modeller oluşturmak, ev işlerine yardımcı olmak veya analizler yapmak için kullanılabilir (Sharma, 2019: 9). Örneğin akıllı bir buzdolabı, sensörleri aracılığıyla sütün bittiğini anlayacak ve sipariş vermeniz için size uyarıda bulunabilecektir. Veya akıllı bir televizyona ses ile komut vermek, internete bağlanıp yayın akışını öğrenmesini sağlamak oldukça kolay bir pratik gibi gözükmektedir. İnsan hayatını kolaylaştırma işlevlerinin diğer yüzünde ise toplanan verilerin ne olduğu, kişiselleştirilmiş deneyim sunma dışında nerelerde kullanıldığı ve kimlerle paylaşıldığı soruları yer almaktadır. Zira internete bağlanabilir bir cihaz olarak televizyon insan sesiyle komut alabilirse, insan sesini duymaya hazır “açık bir mikrofon” formunda beklemektedir. Yine, her an internete bağlı bir buzdolabının sensörleri, eksikleri hatırlatmanın yanı sıra tüketim alışkanlarını da kaydederek üreticisiyle veri paylaşabilir. Üç saattir araba kullanan birisinin verisi, bir enerji içeceği şirketi tarafından anlık olarak satın alınabilir; kişi, ilk mola verdiği ve telefonu eline aldığı anda firmanın hedefli reklamıyla karşılaşabilir. Bu ve buna benzer örnekler nesnelerin interneti fenomeninin derinlemesine bir gözetim gerçekleştirdiğine işaret eder.

2.2. İletişim Teknolojilerinin Kullanıcı Emeği ve Metalaşma Süreciyle İlişkisi

Medya tarafından üretilen ve kitle iletişim araçları ile izleyici / dinleyici / okurlara sunulan içerik ve ürünler medyanın ekonomi politiği çerçevesinde meta olarak kabul edilmektedir. Kitle iletişim araçlarının kültürel metaları klasik anlamdaki metadan farklı olarak ideolojik işleve de sahiptir ve egemen yapının ve süregelen ilişkileri meşrulaştırma, yeniden üretme ve pekiştirme gibi işlevlerini de yerine getirir (Yaylagül, 2006: 127). Medya sahipleri, tüm özel kurum ve kuruluşlar gibi, kapitalist bir işletme olarak mümkün olduğu kadar yüksek kâr etme amacıyla faaliyetlerini sürdürür. Kârlılığın garanti altına alınmasını sağlayacak, hedeflere ulaşılmasına yardımcı olacak formülün merkezinde ise insan vardır. Üretilen içerik ne kadar çok insana erişir ve tüketim sağlanırsa hem ideolojik işlevi yerine getirilmiş olur hem de daha çok gelirin kaynağı yaratılır. 1970’lerle birlikte eleştirel medya çalışmaları, kitle

iletiřim araları dolayımıli iletiřimi, reklamı, izleyiciyi, emeęi ve bu kavramlarla iliřkili olarak neyin meta olduęuna veya meta olup olmadıęına iliřkin birok konuyu ele almıřtır. zellikle Dallas Smythe'nin "izleyici metası" kavramı gerek izleyicinin rettięi maddi deęere iřaret etmesi gerekse batı marksizminin yalnızca ideolojik retime baęlı kalmasını eleřtirmesi bu tartıřmaların ortasında yer almaktadır. Bu baęlamda *izleyici metası* ve *izleyici emeęi* srelerine iliřkin farklı dřnceler ve yaklařımlar literatr zenginleřtirmiřtir.

2.2.1. Medya alıřmalarında İzleyici Emeęi ve İzleyici Metası

Dallas Smythe'nin 1977 yılında yayımlanan makalesi "*Communications: Blindspot of Western Marxism*", gnmze kadar devam eden izleyici metası tartıřmalarının merkezini oluřturmaktadır (Kr Nokta tartıřması iin bkz.: Kıyan, 2015). Smythe'ye (1977) gre Batı Marksizmi kitle iletiřim aralarını yalnızca ideoloji erevesinde yorumlamaktadır ve iletiřime yeteri kadar yer vermemektedir. Hlbuki kapitalist toplum yapısında kitle iletiřim aralarının maddi deęer retim srelerinin de ele alınması gerekmektedir. Ona gre Marksizmin sorması gereken ilk soru, kitle iletiřim aralarının sermayeye hangi ekonomik katkıyı saęladıęıdır (Yaylaęl, 2006: 148). Smythe (1981), geleneksel ve burjuva iletiřim teorilerini idealist olarak tanımlar ve marksist teori de olmak zere tm literatrn kitle iletiřim aralarının temel rnn "mesaj", "bilgi", "imge", "anlam", "eęlence", "eęitim" ve "ynelim" olarak grdęn belirtir. Oysaki ona gre tekelci kapitalizmde ticari kitle iletiřim aralarının temel rn izleyici gcdr ve bu g, ticari kitle iletiřim aralarının varlıęını srdrmesinde ekonomik ve politik grevleri yerine getirmek iin kullanılan somut bir gtr. İzleyici gc retildięi, satıldıęı, satın alındıęı ve tketildięi iin talep edilir ve metadır. Smythe, sektrde izleyici metalarının demografik olarak tabir edilen zelliklere gre sınıflandıęını ve bunların arasında yař, cinsiyet, gelir, etnik durum vb. kategoriler olduęunu syler. Toplayacak olursak, izleyici metası kavramı eriřtikleri ierik karřılıęında medya sahiplerine verilen "boř zaman", "eęlence zamanı" řeklinde ifade edilmektedir (Prodnik, 2019: 345). O tarihten gnmze kimin ve neyin meta olduęu ve olmadıęı, izleyici / cretsiz emek konuları ve kitle iletiřim aralarının metalarının neler olduęu zerine derinlemesine incelemelere gerekleřmiřtir.

Smythe, izleyicilerin reklam gelirleriyle finansman yaratan gazete, televizyon ve radyolara dikkatini vermesiyle çalışmaya başladığını (izleyici emeği), bu şekilde reklamcılara satılmak üzere kendilerini meta olarak (izleyici metası) ürettiğini öne sürer (Fuchs, 2016: 92). Robert Picard medya endüstrisini ikili bir ürün pazarı olarak tanımlamaktadır; ilk meta izleyicilerin merakını uyandırmak için üretilen içerik, ikinci meta ise izleyicilerin dikkatidir (Andrew, 2019). Napoli, geleneksel izleyici piyasası modelinde izleyici metasını oluşturan birbirine bağlı dört bileşene değinir (Napoli, 2003'ten akt. Andrew, 2019): (1) izleyici: medya içeriklerine dikkatini veren kitledir, (2) medya sağlayıcı: izleyicilerin dikkatini çekmek için içerik sağlar, (3) reklamveren: arzulanan hedef kitleye ulaşmak için medya aktivitelerini planlar, (4) izleyici ölçümü: medya içeriklerinin izleyiciler tarafından ne kadar dikkat sağladığı ölçülür. Fuchs (2015:134), izleyicilerin izleyici metasının değerini ürettiğini söylerken, izleyici ölçümünün de üretilen metanın fiyatını belirlediğini, böylece izleyici meta değerinin paraya dönüşmesinde hayati bir önem taşıdığını vurgular. Prodnik (2019: 338-340), medyanın içerikten önce izleyicileri ürettiğine; boş zamandaki her bir bakir alanın metalaştırılmaya hazır bir potansiyele dönüştüğünü ve dolayısıyla boş zamanın sermayenin boyunduruğu altına alınarak paraya çevrildiğine dikkat çekmektedir. Prodnik, boş zamanı *“çağdaş kapitalizmin işleyişinde önemi giderek artan bir bileşen”* olarak ifade eder. İzleyiciler artık kapitalist amaca uygun biçimde artı değerın sökülüp alınabileceği bir hedef olarak görülmekte, izleme edimi de kazanca dönüşmektedir.

Ursula Huws (2018: 180), Smythe'nin izleyici metası kavramını kitle iletişim araçlarının doğasını anlamada değerli bir kavram olarak görmekle birlikte bazı kafa karışıklıklarını da beraberinde getirdiğini dile getirir. Ona göre Smythe, izleyiciyi “meta” olarak tanımlayarak onu alınır-satılır bir ürün olarak ifade eder. Oysaki Marx metayı *“kristalleşmiş emekten başka bir şey değildir.”* ve *“onda soyut insan emeğinin nesnelleşmiş ya da cisimleşmiş olması nedeniyle bir değere sahiptir.”* sözleri ile tanımlar. Marx'ın mantığına göre meta olarak tanımlanan herhangi bir şeyin üretken emeğin sonucu olması gerekir. Medya ve kültür üzerine çalışmalar yapan İsveçli Profesör Göran Bolin'e göre televizyon izlemek bir şey üreten bir eylem değil, reklam ve medya şirketlerince üretim sürecinde ortaya çıkarılan hammadde olarak ifade

edilebilecek bir süreçtir. Dolayısıyla, televizyon izlemeyi emek olarak değerlendirmez (Ekman, 2019: 108). Bolin ayrıca, reklamcıların izleyicileri satın almadığını, satın alınan şeyin “*reytingleri ölçen istatistikçiler tarafından oluşturulan belirli bir izleyici değeri kanaati*” olduğunu dile getirir (Fuchs, 2016: 155). Caraway (2011), izleyicilerin meta olmadığını ileri sürer ve Dallas Smythe’i eleştirir. Ona göre izleyicilerin aktiviteleri (emeği) direkt olarak kapitalistlerin denetimi altında değildir ve izleyici emeğinin yabancılaştığına dair bir kanıt yoktur. Prodnik (2019: 345), Caraway’ın kapitalistin izleyiciyi doğrudan denetim altında tutmadığına katılsa da medya sahibinin içerikle beraber izleyicinin “ilgisini” satın aldığını söyler. Bu durumda içeriği tüketmek isteyen izleyicinin karşısında çok fazla seçenek yoktur; en idealist seçenek ise televizyonu kapatmaktır.

Hebblewhite (2019: 212) reklamverenlerin kitle iletişim araçlarında reklamlarını yayımlamak için “alan” satın aldıklarına ve bu alanın meta olduğuna ilişkin geleneksel bakış açısına farklı bir yorum katar. Ona göre “alan” reklamverenlerin aldığı metanın tamamı değil yalnızca bir boyutudur. Bazı reklamların değeri kapladığı alana göre fazla olabilir. Gece kuşağında yayımlanan uzun bir reklam ile akşam kuşağında yayımlanan kısa bir reklamın değeri belirleyen ise kuşağın ortalama izleyici sayısıdır. Dolayısıyla “alan ve zaman” iletişim endüstrisindeki ana meta değildir; reklamverenlerin meta olarak satın aldığı şey Smythe’nin (1981: 234) belirttiği gibi “*öngörülebilir zamanda, öngörülebilir sayıda dikkatini verecek olan öngörülebilir özelliklere sahip izleyicilerin hizmetidir.*”

Wittel (2019: 404-406), medya çalışmalarında Marx’a atıf yapılarak ücretsiz emek kavramının sıkça kullanılmasının doğru olmadığını, zira Marx’ın klasik politik ekonomi geleneğine ilişkin geliştirdiği eleştiride “*ücretsiz emek*” kavramını kullanmadığına, onun yerine *üretken* ve *üretken olmayan emeği* birbirinden ayırdığına dikkat çeker. Wittel’e göre kapitalist sistemlerde *üretken emek* meta, mübadele değeri ve artı değer üretir. *Üretken olmayan emek* ise herhangi bir meta üretmez; bireyin emek gücü bir meta olarak satılır fakat emek gücünün ürettiği bir üründen (metadan) söz edilemez. Wittel bu bağlamda üretken olmayan emek için ev içinde yapılan temizliği örnek gösterir. Oysa Önal’a göre (2019: 140), emeğin üretken olması için ortaya illaki

somut bir ürün çıkması gerekmez. Önal, bu anlayışın üretken emeğe yönelik yanlış bir düşünce olduğunu savunur. Emeğin üretken emek olması için emek gücünün sermayeye artı değer bırakması gerekir. Evde şahsen yapılan temizlik sermayeye artı değer kazandırmayacağı için üretken olmayan emek olarak nitelenebilir fakat temizlik şirketinden çağırılan bir temizlikçinin kendisi metadır, o şirketin sermaye birikimine katkı sağlar, dolayısıyla burada üretken emekten söz edilebilir. Wittel, emek türlerinin sermaye ve meta biçimiyle ilişkisine göre farklılaştığını belirtse de; ücretsiz emeğin de üretken olmadığını iddia eder. Yurtsever (2016: 47), üretken emeği tanımlamak için emekçinin somut olarak ne yaptığına değil “sermaye açısından” ne işlevi olduğuna bakılması gerektiğini söyler. Smythe’nin “izleyici metası” kavramı ışığında ücretsiz emeğin üretken olup olmadığı sorusu akıllara gelmektedir. Wittel’in eleştirisine, ücretli ve ücretsiz emek bağlamında medya üzerinden açıklık getirmek gerekir. Medya sermayedarına artı değer bırakan (1) medya çalışanlarının ücretli emeği, (2) izleyicilerin / tüketicilerin / okurların ücretsiz emeğidir.

2.2.2. Dijital Emek ve Kullanıcı Metası: Prosumer’den Produser’a Tüketici/Kullanıcının Dönüşümü

Dijital emek kavramı, internet kullanıcılarının içerik üreticileri hâline gelmesiyle yaygınlaşmaya başlamıştır. Ağ temelli dijital medyanın temel özelliklerinden biri, bilgiyi tüketen kişinin aynı zamanda üretici hâline gelmesidir. Toffler (1984), enformasyon toplumunda üreten tüketimi işaret ederek, *producer* (üretici) ve *consumer* (tüketici) kelimelerinin birleşimiyle oluşan *prosumer* (üretketici / üretici tüketici) kavramını ortaya atmıştır. Axel Bruns (2009), kavramı yeni medyaya uyarlayarak kullanıcıların artık birer dijital bilgi üreticisi, dolayısıyla *produser* (üretlanıcı / üretici kullanıcı) olduklarını belirtmiştir. Böylece, Toffler’ın *prosumer* kavramı yeni medyaya taşınmış ve *produser* olarak evrilmiştir (Fuchs, 2014: 174). Dallas Smythe’nin izleyici metası kavramının da yeni medyayla birlikte *prosumer* veya *produser* metası hâline dönüştüğü söylenebilir. Böylece geniş çerçevede insanın, iletişimin ve dijital emeğin olduğu ağ temelli sistemlerde üç çeşit metadan söz edilebilir: kullanıcının kendisi ve dikkati bir metadır, kendi ürettiği içerik bir metadır ve arkasında bıraktığı izler birer metadır.

Geleneksel izleyici metası ile internet kullanıcı metası arasındaki fark üç maddeyle somutlaştırılmaktadır (Saraçoğlu, 2015: 13-14); (1) içerik üretimi: televizyon izleyicileri içerik üretiminde pasifken, internet kullanıcıları içerik üretebilir, yayınlatabilir ve bu içerikler alınıp satılabilir. (2) zaman kısıtı: izleyiciler serbest zamanlarında televizyona erişirken, kullanıcılar internete her an erişim imkânına sahiptir. (3) mekâna bağımlılık: izleyicilerin televizyon izleyebilmesi için belirli bir mekânda (ev, işyeri, kafe vb.) olma zorunluğu vardır, kullanıcılar için mekâna bağımlılık söz konusu değildir. Özellikle mekâna bağımlılığın ortadan kalkması, gözetim araçlarının her an tüm alanlarda insanları kâr amaçlı gözetleyerek ve veri toplayarak dünyayı kapitalist bir fabrikaya dönüştürmeye başlamasını sebep olmuştur. Süreç, her şeyin metalaşmasına doğru yol açmıştır. Bu noktada Fuchs (2016: 162-163), internet kullanıcılarının metalaşmasını her şeyin metalaşması eğiliminin bir parçası olarak görmektedir: sömürü genele yayılmıştır ve neoliberal kapitalizm meta olarak kabul edilenin sınırları ötesine genişleyerek her şeyi içine almıştır.

Dijital emek kavramı üzerine tartışmalar genel olarak internetin yaygınlaşması ve sosyal medyanın ortaya çıkışıyla eleştirel medya çalışmalarında yer bulmuştur. Fakat dijital emeği tanımlamadan önce emek kelimesinin anlamını irdelemek gerekir. Emek, anlam olarak sıkı çalışma, ıstırap ve zahmetle ilişkilendirilir. 18.yy’de kapitalist şartlar altında “çalışma” anlamına gelmiştir; bu bağlamda da emek, birden çok formda yabancılaşmış çalışmadır (Fuchs, 2015: 502). Söz konusu yabancılaşma insanın kendi emeğine, çalışmaya yardımcı olan araçlara, çalışılan nesnelere ve ortaya çıkan ürünlerine yabancılaşmasıdır. Yakın tarihte Maurizio Lazzarato (1996), *maddi olmayan emek* kavramını ortaya atmış ve metanın kültürel içeriğini üreten bir faaliyet olarak tanımlamıştır. Coté ve Pybus, 2007’de yazdıkları bir makalede o dönemin popüler sosyal ağı MySpace’i analiz ederek sosyal ağlarda bir tür maddi olmayan emeğin ortaya çıktığını; buna da “*maddi olmayan emek 2.0*” adını verdiklerini ifade etmiştir (Coté - Pybus, 2007). Bu çalışmada “2.0” olarak tabir ettikleri şey, Tiziana Terranova’nın (2000; 2015) *bedava emek* kavramıdır. Terranova’ya göre bedava emek üretimi dijital ekonomi mantığında değer yaratımı için gerekli bir emektir. Srnicek (2016: 22), geleneksel sanayi işçi sınıfının yerini giderek bilgi işçilerinin aldığını ifade ederken onları “*cognitariat*” olarak tanımlar. Cognitariat, bilişsel emeğin

fizikselliğidir. Bu kavrama göre bilişsel işçilerin sosyal varlığı yalnızca zekâyâ indirgenemez; zira ekrana bakan gözler yorulur, sürekli dikkat sınırları sertleştirir (Berardi, 2005). Dolayısıyla cognitariat kavramı, maddi olmayan emeğin maddi tarafına vurgu yapar.

Son dönemlerde ise işgücü piyasasında değişen rolleri açıklamak ve sermaye birikimi için ihtiyaç duyulan yeni tür artı değeri oluşturacak emeği adres göstermek için dijital emek kavramı popüler hâle gelmiştir. Dijital emek iki emek türüne odaklanır ve analiz eder (Fuchs, 2016: 92): (1) bilgi ve iletişim teknolojilerinin sermaye birikimi için gerekli karşılığını ödenmemiş kullanıcı emeği, (2) bu teknolojilerin üretimi aşamasındaki farklı emek biçimleri. İlk madde ağı bağlı içerik üreten ve her türlü veri sağlayan internet kullanıcılarını, ikinci aşama ise iletişim ve teknoloji şirketlerinde çalışan yazılımcılar, tasarımcılar vb. kişileri içermektedir. Benzer biçimde, Fumagalli vd. (2018) dijital emek tartışmalarının iki başlık altında toplandığını belirtir: (1) Dijital emek / işgücü kendi hesabına, düşük ücret karşılığında ve sosyal güvence olmadan çalışan bağımsız yüklenicileri tanımlamak için kullanılır. Uber, Glovo vb. platform tabanlı iş modelinde bağımsız çalışanlar örnek gösterilebilir. (2) Dijital emek “çalışma saatleri dışında gerçekleştirilen, platform tabanlı iş modelleri tarafından yakalanan ve büyük veri formunda değere dönüştürülen insan faaliyetleri kümesi” anlamına gelir. Bu başlıkta üzerinde duracağımız dijital emek tartışması genel olarak Fumagalli vd.’nin ikinci madde yer verdiği tanım üzerinden gerçekleşecektir.

Bugün hem teknoloji üretiminde çalışanların hem de kullanıcıların dijital emeğini analiz ederken çalışma, metalaşma, serbest zaman, oyun ve emeğin güncel durumunu resmetmek gerekmektedir. Günümüzde sosyal medya platformları, uygulamalar ve mobil teknolojilerin gelişimi tüm kamusal alanları potansiyel birer meta hâline dönüştürmüştür. Bu dönüşüm insanların ticari bir gözetim altında olduğuna, sürekli izlendiğine, sermaye tarafından el koyulan bedeli ödenmemiş emek icra ettiğine (Ekman, 2019: 111-112) ve izleyici metasını yaygınlaştırarak çalışmayı eve kadar taşıdığına (Fuchs, 2016: 162) işaret etmektedir. Kaldı ki Lazzarato 1996 yılında, maddi olmayan emeğin ve onun oluşturduğu ekonomik sistemin “boş zaman” ve “çalışma zamanı”nı gitgide yakınlaştırdığı ve hatta çalışmanın, yaşamın ayrılmaz

bir parçası hâline geldiğini belirtmiştir (Coté & Pybus, 2014:257). Bugünkü iletişim ve teknolojik gelişmeler ile çalışma ile serbest zaman, oyun ile emek zamanı arasındaki çizgi iyice kaybolmaya başlamıştır (Fuchs, 2015: 387). Dijital emek, ekseriyetle eğlenceli kabul edilen ve karşılığı ödenmemiş oyun emeğidir (a.e., s. 417). Çalışmak kendini oynamak gibi göstermeye başlar ve oynamak bir yönetim ideolojisi hâlini alır (a.e., s.509). Oyun zorunlu değildir, eğlencelidir, keyif almak için oynanır, severek dâhil olunur ve ekonomik kaygılardan yoksundur. Oyunun bu nitelikleri çalışmanın baskıcı, zorlayıcı ve sıkıcı yanlarının görmezden gelinmesine yardımcı olur. Oyun emeği kendini fiziksel olarak Google / Facebook gibi platformların ofislerindeki gibi ihtişamlı alanlarda gösterir; çalışanlara birçok imkân ve hizmet sunulur, fakat uzun ve düzensiz çalışma saatleri madalyonun görünmeyen kısmında yer alır. Bu büyük platformların ofisleri ücretsiz yemekten berbere, oyun alanlarından kafelere kadar her şeyi içinde barındırmaktadır. Böylece çalışanların dışarıda duyacakları hiçbir ihtiyacın olmaması sağlanır. Platform çalışanları arkadaşlarla görüşmek, kahve içmek, yemek yemek, tıraş olmak, masaj yaptırmak, oyun oynamak ve bunlara benzer şeyler için daima iş yerine gelir veya bunlar için ofisi terk etmek zorunda kalmaz. Soyut açıdan bakıldığında ise bu gibi platformların kullanımının eğlenceli olması, kullanıcı emeğini sömürülmesinin ve davranışlarının takip edilmesinin göz ardı edilmesine neden olur.

Google ve Facebook gibi büyük dijital platformlarda artı değer sömürüsü yalnızca o şirketlerin ilgili departmanlarında çalışan yazılımcılar vb. dijital emek üreticilerinin istihdamıyla değil; aynı zamanda platform üzerinde içerik üretimine katkı sağlayan kullanıcılar ve üretlanıcılar tarafından gerçekleşmektedir. Platformlar bir yanda istihdam ettiği kişilere ödeme yaparken; diğer yanda üretlanıcılara (*producer*) bağlamına göre nadiren ödeme yaparlar ya da hiç yapmazlar. Başka bir ifadeyle, üretken emek zamanı, ödemesi yapılanlar (istihdam edilenler) ile Çevrim içi zaman geçiren kullanıcıların tüm zamanını içerir. Üretilen bilgi emeği için maaş ödenir, diğer grup ise emeği bedava üretir. Platformların sermaye birikim stratejilerinden biri, bedava üretilecek emek kaynağı kullanıcıların dijital hizmetlere erişimini sağlamak, içerik üretmelerine (yorum, paylaşım, arama, gezinti, tıklama vb. her aktivite) teşvik etmek ve sonuç olarak bu emeği (dolayısıyla kullanıcıları)

toplamak, analiz etmek ve sınıflandırarak meta hâlinde reklamverenlere satmaktır (Fuchs, 2014: 175). Eğer kullanıcılar dijital aktivitelerini makul seviyede azaltır veya sonlandırır; ortada ne kullanıcı üretimi, ne dikkati ne de reklamcılar için potansiyel müşteri kalmaktadır. Kullanıcının içerikte söz sahibi olması, fiilen bir içerik üretmesi bile Çevrim içi olması ve hatta yalnızca mobil cihaz kullanması bile bu şirketler için hayati bir önem taşımaktadır.

Sosyal medya platformları kullanıcı davranış ve verilerinin hedeflenebilir metalar olarak reklamverenlere sunulmasıyla sermaye birikimini sağlar. Fuchs’a göre (2016: 144) her zamankinden daha fazlasını elde etmeye gayret gösteren kapitalist sistem yapısı, bunu gerçekleştirebilmek için ya çalışma gününü uzatmalıdır (mutlak artı değer üretimi) ya da emek üretkenliğini (görelî artı değer üretimi) arttırmalıdır. Bilgi ve iletişime dayalı teknoloji şirketlerinin ve sosyal medya platformlarının ekseriyetle her yıl artan net gelirlerinin arkasında gelişen algoritmalar ve artan sayıda kullanıcının gözetimiyle görelî artı değer üretiminin artışı söz konusudur. Geleneksel medyada belirli bir reklam, belirli bir süre içinde gösterilirken; sosyal ağlarda, arama motoru sonuç sayfalarında veya web sitelerinde aynı anda birden çok reklam gösterilebilir. Hatta bu reklamlar kullanıcının kim olduğuna ve ilgi alanlarına ilişkin ipuçları neticesinde gösterildiği için geleneksel reklamlardan daha fazla dikkat toplar. Gözetimin derinleşmesini sağlayan algoritmik sistemler, her bir internet platformunun kullanıcıyı her yönüyle teşhis etmek istemesi ve ağı bağlı her cihazın gözetim aracına dönüşmesi sonucu toplanan veriler, görelî artı değer üretiminde önemli bir role sahiptir.

Dijital emek ve ücretsiz emek kavramlarına eleştirel yaklaşan yazarlar çevrim içi etkinliklerin ve dijital iletişimsel faaliyetlerin emek olup olmadığını irdeler. Srnicek (2016: 30), kullanıcıların çevrim içi gerçekleştirdikleri faaliyetlerin “emek” olarak nitelendirilmesinin zorlama olduğunu düşünmektedir. Huws (2018: 194), kullanıcıların kendini ifade etme amaçlı yazdıkları blog veya yükledikleri fotoğraf / video gibi çevrim içi oluşturulan yayınların üretken olmayan emek olduğunu iddia eder. Kullanıcı emeği ürünü (blog yazısı, fotoğraf, video) kapitalist tarafından metanın temeli hâline dönüşerek satılsa veya çalınsa bile üretken olmayan emek niteliğini

kaybetmez. Wittel (2019: 413-414), sosyal ağlardaki “bedava emek” kavramını irdelerken çeşitli eleştirilerde bulunmaktadır. Öyle ki Wittel, bedava emek olarak nitelendirilen şarkı indirmek, çevrim içi sohbet etmek, e-posta okumak veya içerik üretmek gibi etkinliklerin birbirinden farklı olduğunu belirtir. Hatta e-posta göndermenin ücretsiz emek sayıldığı bir zamanda geleneksel yolla postane aracılığıyla somut bir mektup göndermenin neden ücretsiz emek sayılmadığını; telefonda konuşmanın telekomünikasyon şirketlerine ücretsiz emek sağlayıp sağlamadığını sorgular ve karşılaştırma yapar. Telekomünikasyon şirketleri ve sosyal medya platformlarının iş modellerinin farklı olduğunu; birinin hizmeti karşılığında tüketicilerden, diğersinin ise reklamverenlerden para aldığını, böylelikle hizmetlerini “bedava”ya sağladığını vurgular. Wittel’in bu fikirleri çok da eski olmayan bir tarihte, 2012’de, yazdığı *“Digital Marx: Toward a Political Economy of Distributed Media”* başlıklı makalesinde yer almaktadır. Wittel, insanların çevrim içi kaldığı her an gerçekleştirdiği aktivitelerin yalnızca bir değil, birden çok platform tarafından el konulduğuna değinmez. Bir web sitesine girdiğinizde, alışveriş sitesinde gezindiğinizde, tweet attığınızda, fotoğraf paylaştığınızda ve hatta yalnızca fareyi hareket ettirdiğinizde bile birden çok “izleyici” insan hareketlerini gözetler, sınıflar ve daha sonra kullanmak üzere kaydeder. Yurtsever’in (2016: 47) Marx’a atıfta bulunarak tanımladığı gibi üretken emek, ne yaptığın değil sermaye açısından neyi yerine getirdiğindir. Gözetlenerek elde edilen tüm veriler, kapitaliste artı değer üretmek için kullanılır. Dolayısıyla çevrim içi ücretsiz emek, şirketlerin iş modellerinin farklılığıyla veya “mektup gönderme” ile ilişkili değildir.

Dijital emek üzerine genel bir kanı, kimsenin sosyal medya platformlarını zorla kullanmadıkları; bilakis bunu isteyerek ve keyifle yaptıkları üzerinedir. Hâlbuki insanlar hayatını idame ettirebilmek için yalnızca yemek ve barınma ihtiyaçlarını karşılamak zorunda değildir, aynı zamanda toplumsal ilişkilere girmek ve iletişim kurmak da zorundadır. Enformasyon toplumunda insanlar için dijital medya, kendi iletişimlerini kurmak için bir etkileşim aracı anlamı taşımaktadır. Dolayısıyla, iletişim kurmak ve anlamlı etkileşimler yaratmak isteyen insanlar, Facebook gibi çok fazla kullanıcıya sahip dijital platformlara yönelmektedir. Bu platformlar ise çok fazla kullanıcıyı tekelinde barındırarak diğer insanları kendi platformu içinde iletişim

kurmaya zorlar ve bir baskı unsuruna dönüşür (Fuchs, 2015: 368-369); bir nevi ticari platformlara zincirlenirler (a.e., s. 369.). Böylelikle, toplumsallaşma ve iletişim ihtiyaçlarını gidermek isteyen insanlar bu gibi platformlara katılmak “zorunda” kalırlar ve ayıramazlar. Bu durum derin bir yanılgıyı içinde barındırır; zira insana farklı fast-food zincirlerinden (McDonalds, Burger King, KFC, Popeyes vb.) aynı tip yemekleri satın alarak özgürce tercih yaptığını düşündürür. Seçeneklerin olduğu (Facebook, Instagram, Whatsapp) fakat alternatiflerin olmadığı dijital hizmetlerde farkında olunmadan “zorla” kullanım söz konusu olabilmektedir.

2.3. Dijital Ekonomide Veri, Platformlar ve Reklam

2.3.1. Dijital Ekonomi Kavramı

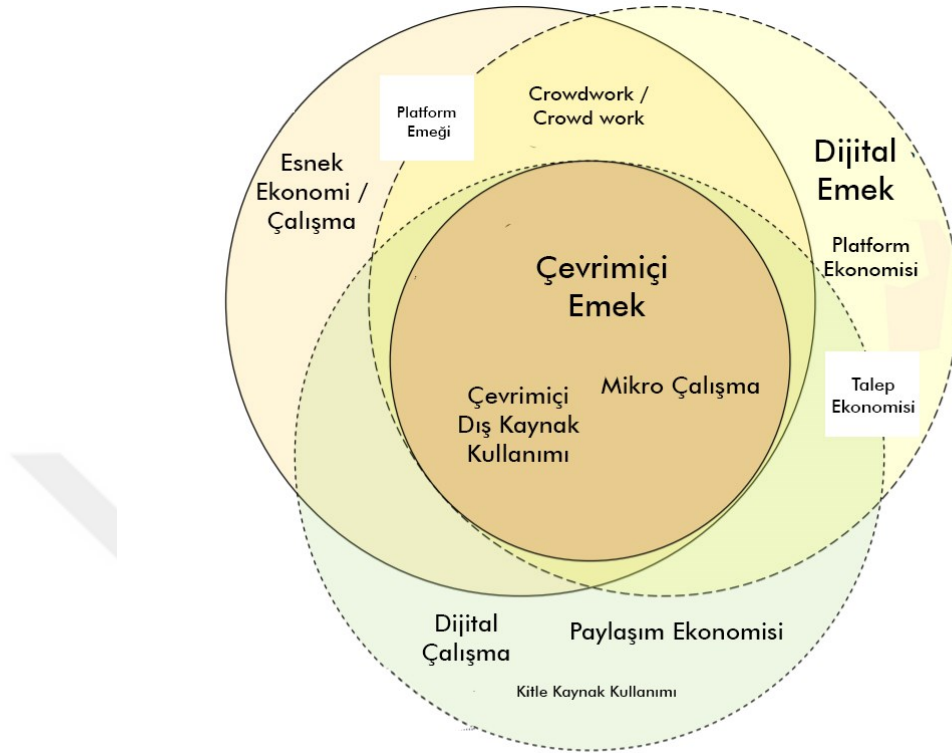
Dijital ekonomi, soyut veya somut her şey hakkında olabildiğince büyük miktardaki veriyi toplama, saklama ve analiz ederek kullanma kabiliyeti ile sürekli bir gelişim içindedir. Daha önce bahsedildiği gibi veriler web sitelerinden, sosyal medya platformlarından, mobil cihaz ve uygulamalardan, sensörlerden, ağa bağlanabilen cihazlardan, iş geliştirme yazılımlarından ve platformlardan toplanmaktadır. İletişim ve bilgi teknolojilerindeki gelişmeler, ağa bağlanan insan ve cihaz sayısındaki artış ve yapay zekâ kapasitesindeki ilerlemeler dijital ekonomide verinin hem daha verimli kullanılacağına hem de veriyi daha doğru anlamlandırarak geleceği öngörebilmede önyak olacağına işaret ediyor. Bu yenilikler dijital ekonomiyi tüm ekonomik yapının ayrılmaz bir parçası ve hatta önemli bir işlevi hâline getiriyor.

Don Tapscott, dijital ekonomiyi “*insan zekâsı ağına dayalı yeni ekonomi*” olarak tarif eder (akt. Terranova, 2000: 37). Dijital ekonomi, iş modelleri için gün geçtikçe daha fazla bilgi teknolojisine, veriye ve internete güvenen şirketlere atıfta bulunmaktadır (Srnicsek, 2016: 4). Şirketlerin defter değeri ile piyasa değeri arasında oluşan fark “maddi olmayan varlıklar” neticesinde gerçekleşir. Bu varlıklar fiziksel olarak muhasebeleşmeyen her şeydir; yetenek, marka değeri, strateji. Son yıllarda gözle görülür biçimde maddi olmayan varlıkların artışı ile şirketlerin sahip olduğu

kullanıma hazır veriler arasında pozitif bir ilişki ortaya çıkmıştır (Mayer-Schönberger - Cukier, 2013: 126). Bu durum dijital ekonomide verinin önemini vurgulamaktadır.

Dijital ekonominin farklı teknolojik ve ekonomik yönleri üç başlıkta toplanmaktadır (UNCTAD, 2019: 4 - 5): (1) Dijital ekonominin temel yönleri; temel yenilikleri (yarı iletkenler, işlemciler), temel teknolojileri (bilgisayarlar, iletişim cihazları) ve altyapı sağlayan sistemlerini (İnternet ve telekom ağı) içerir. (2) Dijital platformlar, mobil uygulamalar ve ödeme hizmetleri dâhil olmak üzere temel dijital teknolojilere bağlı ana ürün ve hizmet üreten dijital ve bilgi teknolojisi sektörleri. (3) Dijitalleşen sektörler. Buna e-ticaret, finans ve turizm şirketleri gibi dijital ürün ve hizmetlerin gittikçe daha fazla kullanıldığı sahalardan dâhildir. Bu bileşenler dijital ekonominin kapsamını ve etkisini ölçmek için temel alınarak çeşitli bağlamlarda kullanılmaktadır.

Dijital ekonomi, çeşitli alt kategorilere ayrılmaktadır ve her biri hem birbiriyle kesişen hem de birbirinden ayrı özelliklere sahiptir. Paylaşım ekonomisi, talep ekonomisi, esnek ekonomi, platform ekonomisi gibi kavramlar dijital ekonomi ekosisteminde belirli bölümlere atıfta bulunmaktadır. Heeks, dijital emek ve dijital ekonomide iç içe geçen kavramları ele alarak tablolastırmıştır (bkz.: Tablo 2.4).



Tablo 2.4: Literatür Taraması Sonucu Ortaya Çıkan Dijital Ekonomi Tablosunun Özeti.

Kaynak: (Heeks, 2017).

Tablo 2.4’teki ekonomi türlerini dijital ekonomiyi daha iyi anlamak adına kısaca incelemekte yarar vardır. *Talep ekonomisi*, ürün ve hizmetlerin anında sağlanması yoluyla tüketici talebini karşılayan teknoloji şirketlerinin yarattığı ekonomik faaliyetlerdir (Jaconi, 2014). Ulaşım, turizm ve yemek siparişi gibi hizmetler bu kategori altında yer alır. *Paylaşım ekonomisi*, genellikle platform tabanlı bir şirket tarafından, mal ve hizmet alışverişine veya paylaşımına olanak sağlayan ekonomik bir modeldir. Bu pazar, paylaşım ile birebir ilişki içinde olmayan, yıla onu net gelir artışı hedefleyen milyar dolarlık şirketler tarafından kontrol edilmektedir. Lyft, Uber, Airbnb gibi “kurumsal” şirketlerin metaları, satıcı ile alıcı arasındaki dijital iletişim süreçleridir (Lobel, 2018). *Esnek (gig) ekonomi*, bağımsız, sözleşmeli ve çoğunlukla sosyal güvenliği olmadan geçici süreli çalışanları barındıran sistemdir. Glovo motor kuryeleri veya Trendyol Go kargo çalışanları esnek ekonomiye bağlı geçici işçi kapsamında değerlendirilebilir. *Platform ekonomisi* ise genellikle internet

platformları tarafından gerçekleştirilen ekonomik faaliyetleri tanımlamak için kullanılan bir terimdir (Chen, 2018). Birbirine çok yakın ve dirsek dirseğe olan tüm bu kavramlar, dijital ekonominin büyümesi ve gelişmesinde önemli rollere sahiptir.

2.3.2. Platformlar ve Yeni Birikim Modelleri

Srnicek, *Platform Kapitalizmi* adlı kitabında platform tabanlı şirketlerin yükselişini ve çağdaş kapitalizmdeki sermaye birikimin nasıl gerçekleştiğini analiz etmektedir. Srnicek (2016: 25), dijital platformları, “*iki veya daha fazla grubun etkileşimde bulunmasını sağlayan altyapılar*” olarak ifade eder. Platformlar, bu nedenle, kendilerini farklı kullanıcıları bir araya getiren araçlar olarak konumlandırılır. Bunlar arasında müşteriler, reklamcılar, hizmet sağlayıcılar, üreticiler, tedarikçiler ve fiziksel nesneler yer alabilir. Platformların çalışma prensibinin merkezinde veri vardır; veri, bu işletmeleri ileri taşıyan ve onlara rakiplerine karşı avantaj sağlayan temel kaynaktır (Srnicek, 2017). Srnicek, dijital ekonomi yoluyla birikim sağlayan ve bunu fiziksel bir ürün satmaktan ziyade platformun kendisine sahip olmakla elde eden beş farklı platform türü olduğunu belirtir (Srnicek, 2016: 22-45):

1) Reklam platformları: Google ve Facebook gibi platformlar, hizmet ve sosyalleşme platformlarından ziyade daha çok reklam platformları olarak tabir edilir. Facebook, 2019’da elde ettiği 70 milyar dolarlık gelirin 69 milyar dolarını reklamcılık hizmetleriyle sağlamıştır (Menlo Park, 2020). Aynı yıl Google ise 161 milyar dolar toplam gelir elde etmiş, bunun 134 milyar doları reklam aracılı gelir olarak belirtilmiştir. Srnicek (2016: 29), reklam platformlarının gelirlerini analiz ederken artık tüm sosyal etkileşimlerin bedava emek hâline dönüştüğünü söyler. Buna bağlı olarak Google, Facebook gibi reklam platformları için bedava emeğin birden çok veri kaynağından yalnızca biri olduğunu yineler. Bunlar arasında daha önce sözü edildiği gibi kredi kartı işlemleri, nesnelerin interneti, uygulamalar, kurumsal şirket verileri, sağlık ve sigorta verileri, özel ve genel gözetime ait toplanan tüm veriler yer almaktadır. Dijital ekonomide gözetim ve kâr sağlama birbiriyle iç içe geçmiştir ve reklam

hizmetlerinde platformlar tarafından yoğun şekilde veri gözetimi gerçekleştirilmektedir. Reklam platformları yüksek gelirleri, kayda değer kâr oranları ve sahip oldukları enerji ile en başarılı çevrim içi ticari platformlar arasındadır.

2) Bulut platformlar: Amazon Web Services (AWS) ve Salesforce gibi bulut tabanlı platformlar bu kategoriye örnek gösterilebilir. Amazon'un bulut sistemleri sayısız Çevrim içi bilgini saklandığı ve veri analizlerinin yapıldığı sunuculardan oluşur. Bulut platformlarının arkasında da kapitalist mantık vardır. Zira bulutta saklanan tüm veriler, bulutun sahibi tarafından çeşitli amaçlar doğrultusunda incelenebilir. Amazon'un CEO'su Jeff Bezos'un AWS'yi elektrik tedarik sistemine benzetir: ilk fabrikalar açıldığında her birinin kendi elektrik jeneratörü varken zamanla elektrik üretimi merkezileşti ve elektrik bu fabrikalara kiraya verildi (Srnicsek, 2016: 33). AWS'nin yaptığı da aynı şekilde internet için gerekli altyapılara sahip olmak ve ihtiyacı olanlara kiraya vermek. AWS tabi ki yalnızca kiraya vermekle kalmayıp içindeki bilgileri de gözetim altında tutabiliyor. Yani AWS'nin yaptığı şuna benziyor; kiralık bir eve çıktığınızda eve hem para ödeyip hem de ev sahibinin yerleştirdiği kameralar tarafından gözetleniyorsunuz. AWS'nin 2013'te geliri 3 milyar dolarken 2019'da 35 milyar dolara yükselmiştir (Copolla, 2020). 6 yılda 10 kat artan gelir, daha fazla sunucu kiraya vermenin yanı sıra daha fazla veriye erişme ve bundan artı değer ürettiği anlamına gelmektedir.

3) Sanayi platformları: Veri toplama, saklama ve analiz işlemleri ucuzlamaya başladıkça daha fazla şirket geleneksel üretim sahalarını dijitale taşımaya başlamıştır. Endüstriyel amaçlı bulut tabanlı nesnelerin interneti platformları bunların başını çekmektedir. Örneğin, General Electrics'in Predix platformu ve Siemens'in MindSphere platformu endüstriyel nesnelerin interneti sistemlerine örnek gösterilebilir. İş geliştirme süreçleri, verimlilik, hataları azaltma, problemleri öngörme, eksiklikleri giderme gibi birçok konuda şirketlere yardımcı olmaktadır. Şirketler kendi yazılımlarını üretmek yerine Predix veya MindSphere gibi sistemleri satın alabilirler. Tıpkı diğer

platformlar gibi bu platformlar da veri çıkarmaya güveniyor ve verinin rakipleri karşısında avantaj sağlayan bir araç olduğunu biliyor. Fabrikalar, tüketiciler ve uygulama geliştiriciler arasında bir nevi aracı olan bu platformlar, en küçük işleticiden en büyük fabrikaya kadar küresel üretimin nasıl işlediğinin takibini yapabiliyor (Srnicsek, 2016: 37).

4) Ürün platformları: Ürün platformları, geleneksel ürünleri hizmete dönüştürmek için diğer platformları kullanarak ve bunları kiralayarak veya aylık abonelik ücreti toplayarak gelir elde eder. Örneğin Spotify müziği, Netflix film ve dizileri dijital bir hizmete çevirerek bunlara erişim için belirli bir bedel talep eder.

5) Yalın platformlar: Uber ve Airbnb gibi şirketler sahipliği en aza indirir (evleri ve arabaları yoktur) ve platform üzerinde gerçekleşen işlemlerden rant sağlar. Çalışanlar güvencesizdir ve fason olarak çalıştırılır. Kısacası yalın platformlar, mal sahibi olmadan hizmet veren platformlardır denilebilir. Yine de en önemli sahip olduğu varlık yazılım ve veri analiz platformlarıdır.

Srnicsek'in kategorilendirdiği platform türlerinin her birindeki en önemli unsur kapitalistin illa ki fiziksel bir ürün üretmesi ve buna bağlı olması değil, platforma sahip olmasıdır. Platformlar ise bu yüzyılın kapitalistler için en değerli hammadde olan veriyi toplar, ayıklar, analiz eder, kullanır ve satar. Platformlar bir nevi hammadde çıkarılması için gerekli kaynaklara dönüşür. Reklam platformları reklamverenlere sunmak için veri toplarken, başka platformlar yalnızca hizmet iyileştirmesi için de kullanılabilir. Tek bir ortak nokta var ki veri her türlü toplanmakta, analiz edilmekte ve platformların iş modelinin merkezinde yer almaktadır.

2.3.3. Veri Şirketleri ve Gözetleme Araçları

Gözetleme, veri toplama rutin hâle geldiğinde gerçekleşir (Christl - Spiekermann, 2016: 9). Veri tüccarı (*Data broker*) olarak tanımlanan şirketler, insanlar hakkında rutin olarak veri toplayan ve satan gruplar olarak ifade edilebilir. Veri

tüccarlarının misyonu Çevrim içi ve çevrimdışı sahalardan veri toplamak ve bunları bir araya getirerek kişi hakkında net bir profil çıkarmaktır (Fry, 2019:42). Çıkarılan net insan profili, birer meta olarak, diğer tüccarlara, sosyal ağlara, reklam platformlarına, sigorta şirketlerine, finans gruplarına, yani talep eden birçok gruba satılmaktadır. Söz konusu veri tüccarları çoğu insanın adını daha önce duymadığı, milyar dolarlık şirketlerdir. 2012 yılında veri tüccarlığı endüstrisi 156 milyar dolar gelir sağlamıştır. Bu gelir açıkça insanın özel hayatını gözetleyerek ayrıntılarını satmakla gerçekleşmiştir (United States Congress, 2015: 2). Bugün veri toplayan ve satan yüzlerce veri şirketi vardır (Grauer, 2018). Veri gözetleme sektörünün öncüleri arasında Acxiom ve Oracle'ın sahip olduğu BlueKai yer almaktadır.

Acxiom şirketi, 1969 yılında müşteri ilişkileri yönetimi konusunda şirketlere danışmanlık yapmak üzere kurulmuştur. Şirket, internet çağıyla birlikte zamanla faaliyet alanını genişleterek müşterilerine özellikle e-posta, banner reklamlar, arama motoru optimizasyonu (SEO) ve cep telefonları aracılığıyla “sadık (ve kârlı) ilişkiler kurma, geliştirme ve muhafaza etme” konusunda hizmet sağlamaya başlamıştır (Turow, 2016:145). Bugün Acxiom'un piyasada hızla yükselmesinin altında yatan neden, hedefleme amaçlı kullanılacak verilere erişme ve sağlama kapasitesidir (a.e., 2016:138). Acxiom, her gün yirmi üç binden fazla sunucuyu çalıştırarak elli trilyondan fazla veri işlemi gerçekleştirmektedir (akt. Goodman, 2019: 101). Kendi web sayfalarındaki açıklamaya göre, “60'tan fazla ülkede 11.000'den fazla veri niteliğine sahiptir ve markaların 2,5 milyar insana erişmesine yardımcı olur.” (Acxiom, 2020). Bunun anlamı, 60'dan fazla ülkedeki 2,5 milyar insanın verisine ve/veya anlık erişim gücüne sahiptir. Diğer bir ifadeyle, 2,5 milyar insanın verileri bir şekilde Acxiom'da yer almaktadır; insanlar kendilerinden habersiz bu şirket tarafından rutin biçimde gözetlenmektedir veya daha önceden hakkındaki bilgiler onunla paylaşılmıştır. Veri kaynakları arasında en önemlilerinden birisi LiveRamp izleme pikselidir. Tüm internet trafiğinin yüzde 1,3'ü LiveRamp tarafından izlenebilmektedir ve en çok ziyaret edilen 10 bin web sitesinin yüzde 10'unu gözetleyebilmektedir (Whotracksme, 2020). LiveRamp'in yanı sıra Epsilon, IBM, Microsoft gibi yüzden fazla veri sağlayıcısı; Ibotta uygulaması (alışveriş), Samba TV (Akıllı TV uygulaması), Veeva Crossix (Sağlık platformu) ve Freckle I.O.T şirketinden veri sağlamaktadır (Christl, 2017: 54).

Ad, soyad ve e-posta adresi gibi veriler dışında inanç, ırk veya etnik kimlik verilerini de veri tabanlarında saklar. Örneğin, bir kişinin adı, soyadı ve coğrafi konum verisini bilerek “Müslüman”, “Yahudi”, “Ortodoks” gibi inanç çıkarımları yapar; ayrıca ad, soyad ve konum verisini ve diğer sahip olduğu verileri bir araya getirerek etnik kökenini tahmin edebilir (Acxiom Data Bundles, 2020). Örneğin bir kişiyi “hispanik kökenli, afro-amerikan, alışverişini indirim marketlerinde yapan, ergenlik çağında çocukları olan düşük-orta sınıf, çalışan ebeveyn” gibi seçeneklerle daraltabilmektedir (akt. Goodman, 2019: 102). Genel olarak şirket 2,5 milyar tüketici hakkında binlerce veri niteliğine sahiptir. Bunlar eğitim, meslek, ebeveynlik, siyasi görüş, ilgi alanları, satın alma, medya tercihleri, sahip olunan mülkler ve araçlar, banka ve sigorta işlemleri, gelir, kredi borçları, sağlık durumu, ekonomik durum gibi var olan örneklerden veya geleceği öngören çıkarıma dayalı (iş değiştirme ihtimali, çocuk sahibi olmaya niyetli vb.) veri niteliklerinden oluşmaktadır (Christl, 2017: 55).

Acxiom’dan daha büyük bir veri şirketi, köklü bir yazılım şirketi olan Oracle’dır. Oracle, çevrim içi gözetimini mükemmel hâle getirmek ve reklam sektöründe daha güçlü var olabilmek için 2014’ten bu yana milyarlarca dolar harcayarak büyük satın almalar gerçekleştirmiştir. 2014 yılında 400 milyon dolara BlueKai, 1,2 milyar dolara ise Datalogix gibi büyük veri tüccarlarını Oracle çatısı altında birleştirmiş; ayrıca 2016’da AddThis, 2017’de MoaT (Oracle, 2020) gibi hizmetleri de bünyesine ekleyerek en zengin veri havuzlarından birine sahip olmuştur. Özellikle web sitelerin sosyal ağlarda paylaşma ve beğenme yazılımı AddThis ile Oracle internet trafiğinin %2.1’ini anlık olarak izlemektedir (Whotracksme, 2020b). 2016 yılındaki verilere göre sosyal medyadan, bloglardan, ürün inceleme sitelerinden, video sitelerinden günde ortalama 700 milyondan fazla mesaja erişebilmektedir. Oracle, bu sayede *Gizli Anlamsal Analiz* (Latent Semantic Analysis) adını verdiği teknoloji ile veri bombardımanı arasında gürültüyü keserek daha doğru ve kesin içgörüler sağladığını müşterileriyle paylaşır (Oracle Social, 2020). BlueKai’nin çok çeşitli alt kategorilere sahip sınıflandırılmış kullanıcı grupları vardır. Kategoriler ne kadar detay içerirse satış fiyatı da o oranda yükselir (Liu - Wang, 2020:127). En büyük veri kaynakları arasında bulut platformları yer alır. Yanı sıra Christl (2017), Oracle’a veri temin edenleri şu şekilde listelemiştir;

- a) Visa: Milyarlarca kredi kartı işlemini sağlıyor.
- b) MasterCard: Kart sahiplerinin işlem verilerini sağlıyor.
- c) i-Behavior: 339 milyon insanın psikografik verileri satın aldı.
- d) Acxiom
- e) Experian: 700 milyon insanın finansal ve satın alma dâhil verilerine sahiptir.
- f) TransUnion: 90 bin kaynaktan bir milyar insan verisine sahiptir.
- g) Lotame: İzleme pikselleri ve çerezler aracılığıyla milyarlarca insana erişir.
- h) PlaceIQ: 100 milyon akıllı telefondan konum verisi ve rutin hareket kalıpları topluyor.
- i) Proxama: Otobüs, tren, mağaza veya tiyatro gibi alanlara yerleştirdiği Bluetooth vericileri ile konum verisi toplar.

Oracle ve Acxiom gibi büyük veri tüccarları, onlarca büyük şirketten ve kaynaktan veri toplamakta ve bunları birleştirerek kapsamlı ve derinlemesine insan profilleri oluşturmaktadır. Bu profiller bankacılık, otomotiv ve sigortacılık sektörlerinde riskleri minimuma indirme ve net geliri yüksek tutma amaçlı kullanılır. Veri tüccarlarının genel amacı “davranışsal saptama” (behavioral targeting), “öngörü saptama” (predictive targeting) veya “kişiyi özel davranışsal analiz” (Premium proprietary insights) gibi yöntemler ile insana ve insan hayatına dair her şeyi bilmek ve başkalarıyla paylaşmaktır (satmaktır). Goodman’ın (2019: 101) yalın ifadesiyle söz konusu yöntemler karar alım sürecindeki şirketler, pazarlamacılar ve reklamcılar arasında en yüksek fiyatı verene satabilmek için insanın en net şekilde profilini çıkarmaya yönelik çalışmalar anlamına gelmektedir.

US Annenberg Public Policy Center’ın Haziran 2005’te yayınladığı raporda, Amerikalıların büyük çoğunluğunun kişisel verilerinin şirketler tarafından nasıl kullanıldığına dair bilgi sahibi olmadıkları, profillemeye ve sınıflandırmaya karşı oldukları ve kişisel verilerin meta olarak şirketlerden satın alınmasına yönelik olumsuz yönde görüş belirttikleri yer almaktadır (Lyon, 2013: 271). Veri tüccarlarının bu kadar çok insan hakkında bu kadar çok bilgiye erişmesi ve bunu açık rıza almadan yapabilmesi başlı başına bir sorunken, bu bilgilerin güvenliği de ayrı bir problem

yaratmaktadır. MEDbase200, sađlık ve tıp alanında veriler satan řirket, “tecavüz mađdurları” kiři listesi de dâhil olmak üzere “ereksiyon problemi yařayanlar”, “alkol sorunu olanlar”, “AIDS’li hastalar” gibi sınıflandırmaları 1000 kiři bařına 79 dolar fiyatla satılıđa çıkarmıřtır (Hill, 2013). ABD’li bir babanın evine gönderilen OfficeMax A4 kağıt reklam katalogu, ticari gözetimi gözler önüne sermektedir. Mike Seay isimli kiřinin evine gelen katalogta “*Mike Seay, kızı trafik kazasında öldü.*” etiketi yer almıřtır. Gerçekten de Seay’in kızı bir yıl önce trafik kazasında hayatını kaybetmiřtir. OfficeMax firması Seay’i arayıp özür dileyse de bu hataya neyin sebep olduđunu ve en önemlisi kızının öldüđu verisini kimden aldıđını paylařmamıřtır. Sonuç olarak Seay, OfficeMax’i bir kere yazıcı almak için tercih etmesine rađmen OfficeMax’ın onun hakkında hassas bilgiler de dâhil olmak üzere veri toplamıřtır (Goodman, 2019: 102 - 103). Zack Whittaker (2020), Oracle BlueKai’nin bir sunucusunu řifresiz bıraktıđı için dünya çapında milyonlarca insanın milyarlarca çevrim içi hareketini içeren verilerin internete sızdıđını tespit etmiřtir. Whittaker, internete sızan verilerin neler olduđunu açıklarken örneklerinden birisi Türkiye’deki bir kaydı içermiřtir. Bu kayıтта İstanbul’da yařayan bir kiřinin 899 dolar deđerinde mobilya sipariři verdiđi yer almıřtır. Sunucunun řifresiz oluřu, sözü edilen kiřinin adı, e-posta adresi gibi sipariřle ilgili tüm bilgilerine giriř yapılmadan eriřilmesini sađlamıřtır. Veri tüccarlarının ticari gözetimi, veri alıřveriři ve insan hakkında doymak bilmeyen bilgi ihtiyacı tahmin edilmesi zor seviyelere evrilmesi beklenmektedir. Topladıkları tüm bilgi parçalarını bir araya getiren ve anlamı bir bütün inřa ederek talep edenlere satan tüccarların hammaddesi insanın benliđi, iletiřimi ve davranıřları olmaya devam edecektir.

2.3.4. Veriye Dayalı Reklamcılık ve Çevrim İçi Reklam Endüstrisi

Çevrim içi reklam sektörünü irdelemeden önce bu sektörü klasik reklam ve pazarlamadan faaliyetlerinden ayıran anahtar özelliđini, yani veriye dayalı olarak insanları tanımlama ve sınıflama becerisini ve bunun reklam / pazarlama ile ilgili tarihsel sürecini kısaca paylařmak gerekir. Psikologlar uzun yıllar insanı insan yapan özellikleri ölçümlemeyi amaçlamıřtır; bu amaç, söz konusu özellikleri soyut zeminden olarak daha somut, kesin ve ölçülebilir řeylere dönüřtürme çabasını içermiřtir. İngiliz

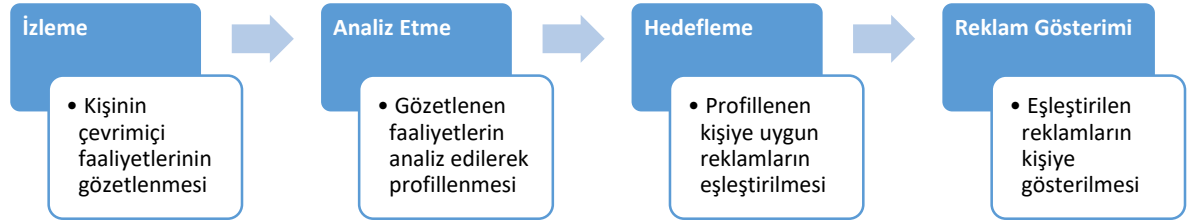
Psikolog Hans Eysenck'in 1940'lı yıllarda kişiliğin boyutlarını ve davranışlardaki bireysel farklılıkları ele aldığı kişilik teorisi bu alanda yapılmış orijinal çalışmalardan birisidir. İnsanı ve onun kişiliği tanımlamaya, ölçmeye ve sayısal hâle getirmeye yönelik gelişmeler şirketlerin, müşterilerin ve potansiyel müşterilerin seçimlerini etkileyebilecek kadar iyi tanımaları gerekliliğini ortaya koymuştur. Bu durum pazar araştırması endüstrisinin doğmasına yol açmıştır. Pazar araştırmaları yüz yüze veya telefon yoluyla yapılan anketlerden oluşur; tüketicilerin ihtiyaçlarını belirleme ve onlar hakkında bilgi toplama amacına dayanır (Strong, 2015: 90).

Pazar araştırmacıları ayrıntılı alışveriş ve işlem verilerinin peşinde olmasına rağmen çeşitli sorunlarla karşılaşmıştır. Tüketiciler az meblağ ödeyerek yaptıkları alışverişlerde genellikle ne aldıklarını, ne zaman ve nerede aldıklarını hatırlamakta güçlük çekmişlerdir. Günlük hayatın yoğunluğu içerisinde bu durum kabul edilebilir bir durum olmuştur. Araştırmacılar hâliyle sınırlı sayıdaki basit davranış verilerini anket yoluyla toplamışlardır. Söz konusu problem, alışveriş kayıtlarını tutan müşteri ilişkileri yönetimi veri tabanları ile çözüme kavuşmuştur. Böylece pazar araştırmasına katılan insanların söyledikleriyle, veri tabanlarındaki alışveriş verisi karşılaştırılmış ve anlamlı bir ilişki ortaya çıkarılmıştır (Strong, 2015: 90). Bu noktada reklamverenler, araştırma şirketleri gibi aracı kurumlardan veri setleri satın alarak tüketicileri daha iyi anlamaya ve reklamların etkisini ölçmeye yönelik çalışmalar yürütmeye başlamıştır. Fakat satın alınan veri setlerinde alışveriş geçmişi olmasına rağmen alışveriş yapanın kim olduğunun bilinmemesi bir problem olarak teşkil etmiştir. Dolayısıyla alınan veri setleri bir nevi temsili grupların sınırlı bilgilerini içermiştir. Aynı zamanda veriler sürekli olarak güncel tutulmuyordu, bu nedenle de dinamik bir değişkenlik ve anlık eğilimlerin bilinmesi söz konusu değildi. Neticede, geleneksel araştırma yöntemleri çoğunlukla kitleleri yorumlanabilir büyük gruplara ayırmış ve gruplara ilişkin geçici varsayımlar üretmiştir (Chen vd., 2019).

Veri, tarihsel olarak, tüketicilerin satın alma davranışlarının analizini yapmak için büyük veri tabanlarında saklanmıştır. Verilerin çoğu, tüketici davranışını daha geniş bir biçimde anlamak için toplandıysa da tüketicileri satın almaya teşvik edecek çalışmalar kapsamında kullanılmamıştır. Son zamanlara kadar verinin reklam ve

pazarlamada kullanmamasını Nesamoney (2017: 17 - 18) şu maddelerle açıklar: (1) Veri genellikle tek bir eylemi referans göstermiştir (Siyah tişört satın alan erkek gibi). (2) Veriler arası ilişki kurmak zordu. Her veri sahibi kendi verisine sahipti ve ortak bir paydada buluşup birleşim gerçekleşmiyordu. (3) Veriler büyük oranda anonimdi. Perakende satın alma verilerinde satın alan kişinin kaydı tutulmuyordu. (4) Ekstra satın almayı teşvik etmek için gerekenler genellikle çevrimdışı yapıyordu (eve hediye kuponu gönderme gibi). (5) Veriler fazla ayrıntılı değildi ve geniş sınıflamalara sahipti. Cinsiyet, yaş ve belki satın alma verisini içeriyordu. (6) Pazarlama kampanyaları amacıyla veri toplamak, işlemek ve kullanmak bir hayli maliyetliydi. (7) Gizlilik ve mahremiyet savunucuları, pazarlamacıların müşteri verilerini agresif biçimde kullanmasını engelledi. İnternetin yaygınlaşması ile verinin reklamcılıkta kullanılmamasına neden olan tüm bu etmenler yavaş yavaş kaybolmaya başlamıştır.

1993 yılında Michael Schrage yazdığı bir makalede internet için *“hiç kimse internetin sahibi değildir.”*, *“internet kimse tarafından yönetilmez.”* ifadelerini kullanmış ve internetin önemli bir reklam mecrasına dönüşeceğini öngörmüştür (Turow, 2016: 61; Schrage, 1993). İletişim teknolojilerinin gelişimi ve internete erişen kişi sayısındaki artış ile birlikte Schrage’in öngörüsü varlığını hissettirmeye başlamıştır. 1994 yılında ilk reklam bannerının internette yerini alması, internetin reklam sahasına dönüşmesine önayak olmuştur. Aynı zamanlarda çerez teknolojisi ve arkasından izleme piksellerinin web’te yaygınlaşması, internet reklamlarını geleneksel medyadaki reklamlardan daha farklı bir pozisyona taşımıştır. Cihazlara yerleştirilen çerezler ve kullanıcı etkinliklerini kaydeden izleme pikselleri ile gözetleyiciler insanları çeşitli kategoriler altında sınıflamış; reklamcılar ise bu sınıfları hedefleyerek reklam göstermeye başlamıştır. Gözetlenerek toplanan veriler ve bu verilere dayalı hedefli reklamcılık anlayışı, günümüz çevrim içi reklam endüstrisinin en zengin yöntemidir. Veriye dayalı reklamcılık, mesajın hedeflenen kitleye ulaşacağına dair belirli bir inancı temel alan ve neredeyse iki yüzyıldır varlığını sürdüren reklamcılık anlayışını yıkarak ampirik kanıtlara dayalı hedeflemeyle kitleye mesaj ulaştırmaya olanak sağlamıştır (Vaidhyanathan, 2018:84). Bunun anlamı, insan artık takip edilen, davranışları sayısallaştırılmış, farklı davranışları bir araya getirilerek ne yapacağı öngörülen ve rahatlıkla manipüle edilebilir bir hâle bürünmüştür.



Tablo 2.5: Çevrim İçi Davranışsal Reklam Süreci.

Kaynak: (Berber, 2014: 22).

Çevrim içi reklamcılığın en belirgin özelliği, reklamverenlere davranış verilerine dayalı hedefleme olanağı sunmasıdır. Tablo 2.5’te Çevrim içi davranışsal reklamın süreçleri özet olarak verilmiştir. Tablo 2.5, Dijk’ın (2018: 176) internet gözetimini tanımlarken kullandığı ifadeyi hatırlatır: “*bırakılan izlerin bumerang gibi ilgili kişiye dönüşü.*” Süreç, aslında bir döngü olarak ilerler. İzlenen kişi, hedeflenen kişi olur ve reklam gösteriminden sonra daha doğru ve kesin reklamlar gösterilmesi için tekrar izlenmeye devam edilir. Bu noktada reklamverenlere bir parantez açmak gerekir. Reklamverenler veri setini satın almaz, hedefleme kriterlerine uygun kitlenin kim olduğunu, isimlerini, e-posta adreslerini veya tanımlayıcı herhangi bir özelliğine ulaşamaz. Reklam platformları veri setlerini nihai bir meta olarak sunar, belirli bir bütçe karşılığında hedef kitleyi “kiralamış” olur. Reklamverenler aynı zamanda verilerin nereden geldiğiyle ve hikâyesiyle de ilgilenmez; tıpkı manavdaki elmanın nasıl yetişerek manava geldiğiyle veya kuyumcu dükkânındaki pırlantanın hikâyesinin müşterisini ilgilendirmediği gibi. Yalnızca nitelikli ve doğru sınıflanmış insan metalarını hedeflemek ve yatırımlarının karşılığını almak isterler. İnterneti bir pazar olarak düşünürsek; izleyen, toplayan, analiz eden ve sınıflayan aktörler ile reklam platformları insanı daha iyi tanımak ve gelirlerini sürekli arttırmak için Çevrim içi reklam endüstrisinin çarklarını bir an bile durmadan çalıştırmaya devam etmektedir.

Son olarak çevrim içi reklam dikkat ekonomisi ilişkisinden bahsedebiliriz. Çevrim içi reklam endüstrisinin kullanıcıların dikkatine verdiği önem dikkat ekonomisi ile açıklanmaktadır. Dikkat ekonomisi, insanın dikkatinin değerin yaratıcısı olduğu önermesi üzerine inşa edilmiştir. Bu ekonomide yayın ağları, reklamverenlere

“insan bakışlarını” satma hayalleri kurarlar. Böylece dikkat, yeni bir meta türü olarak karşımıza çıkar (Beller, 2014:190-191). Web’teki anlamıyla dikkat ekonomisi, 90’lı yıllarda içeriğin ücretsiz olması gerektiği anlayışının yerleşmesiyle görünür olmuştur. Dijital içeriklerin ücretsiz olması ve özgürce dolaşabilmesi gerektiği fikri, masraflarını karşılaması gereken şirketlerin gelir modeli olarak reklamı tercih etmesini tetiklemiştir. Yahoo ile başlayıp Google ile zirveye ulaşan reklamların, maddi ihtiyaçları karşılaması beklenmiştir (Vaidhyanathan, 2018:81).

2.3.4.1. Çevrim İçi Reklam ve Reklam Platformları

Çevrim içi reklamlar, mobil pazarlama, görüntülü reklam, arama motoru reklamları, yeniden pazarlama, e-posta pazarlama, video reklamları gibi çeşitli alt başlıklara sahiptir ve gün geçtikçe bu alt başlıklar zenginleşmektedir. Reklamların kime gösterileceğine ilişkin hedefleme söz konusu olduğunda Çevrim içi reklam türleri dört başlıkta toplanabilir: (1) davranışsal reklamcılık: kullanıcı etkinliklerine ve çıkarımlara dayalı, (2) demografik reklamcılık: kişinin demografik özelliklerine dayalı, (3) içeriksel (bağlamsal) reklamcılık: reklam ile reklamın yayınladığı sitenin içeriğinin uyuşmasına dayalı, (4) bağımsız reklamcılık: hedefleme olmaksızın reklam gösterimi (Berber, 2014: 7 - 8). Bu türlere ilişkin en sık kullanılan ücretlendirme yöntemleri arasında ise reklamın bin gösterim başına (CPM) ve tıklama başına (CPC) fiyatlandırılmasıdır.

Geleneksel medyaya reklamverenler, reklam verecekleri mecraları seçerken reytingleri ve genel satış tirajlarını dikkate almıştır. Aynı şekilde reklamın fiyatı tiraj ve reyting sayılarına göre hesaplanıyordu fakat reklamı kimlerin gördüğüne ilişkin net bir bilgiye erişemiyorlardı. İnternet ortamında ise *tıklama*, şirketlerin reklamı ölçümlemesine olanak sağlamış ve geçmişten beri akıllarda soru işareti olan, reklamın görünüp görünmediği – göründüyse ne gibi tepkiler aldığı gibi sorulara cevap bulma imkânı yaratmıştır (Turow, 2016: 62 - 74). Ek olarak, reklamın maliyeti gösterim yapılan kişi sayısına veya tıklanma sayısına göre hesaplanma özelliğini kazanmıştır. Örneğin, arama sonuçlarında gösterilen reklamların fiyatlandırılması tıklama başına maliyet üzerinden hesaplanır. Reklam algoritması anahtar kelimeye, onun değerine ve

rekabetine göre anında bir fiyat çıkarır. Bu fiyatın oluşmasında satılan malın / verilen hizmetin değeri dışında potansiyel müşterinin yaşam boyu müşteri değeri de hesaplanmaktadır. Bu nedenle hukuk, banka, sağlık, kumar, sigorta vb. sektörler genellikle daha yüksek maliyetlerle tıklama satın alırlar.

2019 yılında dünya genelinde dijital reklam harcaması 325 milyar dolar olmuştur. Bu sayının 2024 yılında 500 milyar doları geçmesi öngörülmektedir (Guttmann, 2020). Bu harcamanın yaklaşık yarısı Google ve Facebook platformlarında gerçekleşmiştir. Özellikle Google, gerek yenilikçi çözümleri, gerek satın almalar gerekse sahip olduğu devasa veriyle çevrim içi reklam endüstrisinin lokomotif ve çoğu şirketin idolü konumundadır.

Google ilk yıllarında arama motoru kapsamında topladığı verileri arama sonuçlarını iyileştirme amacıyla kullanmıştır. 1999'da aldığı 25 milyon dolarlık yatırımdan sonra elinde gelir elde edebileceği bir değer kalmaması kazanç sağlamanın yeni yollarını aramaya teşvik etmiştir. Sonucunda, arama verilerini, çerezler ve diğer bilgi biçimleriyle birlikte giderek otomatikleşen bir açık artırma sistemi aracılığıyla reklamverenlere hedeflenen reklam alanı satmak için kullanmaya başlamıştır. Ekim 2000'de Google, AdWords'ü piyasaya sunmuştur ve artık veriler hizmetleri iyileştirmenin bir yolu olmaktan çok reklam geliri elde etmenin bir yolu hâline dönüşmüştür (Srnicsek, 2016: 29). Google, yeni bir sistem olarak ihtiyacından fazlasını gözetlemesi ve davranışsal verilerden arda kalanları depolamasıyla 2001 yılında net geliri bir önceki yıla göre %400 oranında artış göstermiş ve ilk defa kâr elde etmiştir. Davranışsal veri fazlalıklarını toplayarak dört yıl içinde %3590 oranında etkileyici bir gelir artışı sağlamıştır (Zuboff, 2019: 87).

Google'ın AdWords ile yakaladığı başarının arkasında o dönemki rakibi, Bill Gross'un kurucusu olduğu arama motoru GoTo.com (Daha sonradan adı Overture olarak değişti) iş modelini gözlemlemesi yatmaktadır. GoTo.com, tıklama başına açık arttırmaya dayalı reklam modeline sahipti ve Google, GoTo'nun modelini geliştirerek açık arttırmayı kazananları belirlemek için algoritmaları kullanmaya başlamıştır. Söz konusu algoritmik yapı yalnızca teklif edilen ücretin yanı sıra görüntülenmek istenen reklam ile tanımlanan anahtar sözcükler arasındaki ilişkiyi de incelemiş; ölçümleme

kısmını da önceki benzer reklam kampanyalarının elde ettiği tıklama sayısını göz önüne alarak yapmıştır (Turow, 2016:107). GoTo'nun Çevrim içi reklamcılığa getirdiği en büyük yenilik; 1) gösterim başına ücretlendirme yerine tıklama başına ücretlendirmeyi getirmesi, 2) aranan anahtar kelimeyle ilişkili reklamları kullanıcılara sunarak alakalı reklam göstermesi, 3) anahtar kelimeye en yüksek parayı teklif edenin reklamını en üstte göstermesidir.

AdWords'ün zaman içinde gösterdiği başarı ve yarattığı gelir, gözetim mantığının internete yerleşmesinde büyük ölçüde etkili olmuştur (Zuboff, 2019: 83). Google, tüm interneti kendi bünyesine bağlayacak ve gözetleyebilecek hizmetler üretmiş, yazılımlar geliştirmiş ve satın almalar gerçekleştirmiştir. AdWords sistemini geliştirmenin yanı sıra, ilk reklam servislerinden biri olan ve binlerce web sitesine erişim sağlayan DoubleClick'i 2007 yılında 3,1 milyar dolara satın alarak reklam sektöründeki tekelleşmesini sürdürmüştür. Google bu hamlesiyle yalnızca arama sonuçlarında değil, görüntülü reklam gösterimlerinde de etkinliğini arttırmayı hedeflemiştir (Story - Helft, 14 Nisan 2007).

İnternetin ilk zamanlarında görüntülü reklamlar, yayıncılar ve reklamverenler arasında “Reklam Rezervasyon Sözleşmeleri” adıyla bilinen önceden anlaşılmış sözleşmeler aracılığıyla satılmaktaydı. *Doğrudan Satın Alma* olarak da adlandırılan rezervasyon sözleşmesinde reklamverenler ve yayıncılar fiyat, hedefleme kriterleri ve belirli bir süre içinde arz edilecek gösterim sayısı üzerinde anlaşma sağlardı; örneğin, İstanbul'daki erkek ziyaretçilere Ocak ayında 1000 TL karşılığında 100.000 gösterim satın alınabilirdi (Sayedi, 2018). Bugün, reklamverenlerle yayıncıları buluşturan birden çok dijital platform, borsa ve ağ söz konusudur.

2000'li yılların ortalarıyla birlikte programatik reklam mantığının ortaya çıkmasıyla kullanıcılar belirli sınıflar hâlinde, açık arttırmayla satılan ticaret nesnesi hâline dönüşmüştür. Bardowicks ve Busch, programatik reklamcılığı “*kişiye özel reklam gösterme fırsatlarına dayalı dijital reklamların gerçek zamanlı otomatik olarak sunulması.*” şeklinde tanımlar (akt. Busch, 2015: 8). Busch, tanımı yaparken programatik reklamcılığın beş özelliğinden yararlanır: (1) Ayrıntı olma: belirli bir reklamı belirli bir kişinin görüntülemesini sağlama, (2) Gerçek zamanlı ticaret: en son

verilere dayanarak anında reklam gösterebilme, (3) Gerçek zamanlı bilgi: şimdiye kadar toplanan verilerle son derece kişiselleştirilmiş ve öngörüye dayalı olma, (4) Gerçek zamanlı oluşturulma: açık arttırmayı kazanır kazanmaz reklamı gösterme, (5) Otomasyon: reklam yerini otomatik ayırtma ve görüntülenmesini sağlama (Busch, 2015: 8). Kısacası, programatik reklam mantığında kitlelerin ticaretinin gerçekleşmesi yalnızca birkaç milisaniye sürer ve gerçek zamanlı olarak anında tamamlanır. Bir internet kullanıcısı programatik ticaret ağıyla işbirliği içerisinde olan bir web sitesini ziyaret ettiğinde kullanıcının kim olduğu anında tespit edilir ve web sayfası tam olarak yüklenene kadar hangi reklama maruz kalacağı en yüksek teklifi verene açık artırma ile satılır. Anlık açık artırma tamamlanmadan kullanıcının göreceği reklam belirsizdir (Andrew, 2019).

Programatik reklam, arz yönlü platformlar (SSP) ile talep yönlü platformlar (DSP) arasında bir bağlantı kuran reklam verme yöntemidir (Smyrnaio, 2018:122). Programatik reklamda arz ve talep metanın değerini belirler. Arz yönlü platformlar, yayıncıların veya reklam ağlarının ellerindeki reklam envanterini, yani yayıncıların reklam için uygun alanları, reklam borsalarına bağlayarak satmalarını sağlayan araçlardır. Örneğin, bir web site sahibi sayfasındaki beş reklam alanını reklam borsalarına bağlayarak dinamik biçimde reklam göstermeye başlayabilir. Talep yönlü platformlar ise reklamverenlere reklam satın alma ve reklam düzenleme aşamasında yardımcı olmaktadır. *Google DoubleClick* tipik bir talep yönlü bir platformdur. Bu iki platformun bulunduğu alan, reklam borsalarıdır. Reklam borsaları, yayıncıları ve reklamverenleri bir araya getiren çevrim içi pazar yerleridir. Reklam borsalarının çalışma prensibi, menkul kıymetler borsaları, emtia borsaları, döviz piyasaları, kripto para piyasalar veya vadeli işlem piyasalarıyla aynıdır. Bir “şey”in belirli bir fiyattan satıcısı ve o “şey”e belirli bir miktar ödemeye razı bir alıcı vardır. Reklam borsalarında da yayıncı, reklam alanı için minimum bir fiyat; reklamveren ise vereceği reklam için maksimum bir fiyat belirler. Her iki değişken birbiriyle eşleştğinde reklam, yayıncının web sitesinde / mobil uygulamasında yayınlanır.

Yayıncıların reklam envanterlerini sunduğu arz yönlü platformları bir kenara bırakırsak, programatik reklam ticareti iki araç üzerine inşa edilmiştir: Veri yönetim

platformu (DMP) ve talep yönlü platform. Reklamverenler, talep yönlü platform aracılığıyla makine öğrenimi algoritmalarını kullanarak stratejik olarak teklif vermek ve her bir potansiyel reklam gösterimini avantajlı biçimde değerlendirmek için veri yönetim platformu tarafından sağlanan büyük miktardaki kullanıcı verisinden yararlanır (Chen vd., 2019). Veri yönetim platformları, birinci, ikinci ve üçüncü taraflardan veri toplayan ve analiz ederek reklam borsalarında satışa çıkaran sistemlerdir. İnternet siteleri, mobil uygulamalar, çevrimdışı etkinlikler, ağa bağlanan cihazlar ve sensörlerden veri toplayarak bunları kapsamlı insan profilleri oluşturmak için kullanır. Veri şirketi BlueKai, Lotame ve LiveRamp (Oracle) örnek bir veri yönetim platformudur. Veri yönetim platformları, hedef kitleyi daha iyi tanımlamak isteyen reklamverenlere sunduğu ekstra veriler karşılığında belirli komisyonlar alır.

Programatik reklamcılığa 2019 yılında yalnızca Avrupa kıtasında 26 milyar euro'luk bir harcama gerçekleştirmiştir. 2013 yılında 2,5 milyar euro iken, programatik reklamcılık harcamaları 6 yılda 10 kat artış sağlamıştır (IAB Europe, 2020). 2019 yılında küresel çapta programatik reklamcılık harcamaları ise 100 milyar doları aşmıştır (Guttmann, 2020b). Reklamverenlerin kitleyi avuçlarının içinde bulmasını sağlayan programatik reklamın zamanla daha da popüler hâle gelerek yaygınlaşacağını tahmin etmek zor değildir. Bu pazar yerlerinde reklamverenlere sunulan yalnızca hedef kitle grupları değil, insan deneyimleri, iletişimi ve etkinliklerinin yanı sıra insanın metalaşmış geleceğidir. Habersiz gözetlenen insanlar, bir alışveriş metası olarak programatik reklam ticaretinin başrolünde yer almaktadır.

2.4. Gözetim Kapitalizmi: Gözetim Temelli Dijital Ekonomiye Eleştirel Bir Bakış

Kapitalizm, servetin; gözetim, bilginin artışıyla ilgilidir. Aral Balkan'ın (2020) ifadesiyle birikmiş serveti olanların daha da fazla zenginleşmek için insan yaşamı hakkında özel içgörüler sağlayan gözetim sistemlerine yatırım yapmasıyla gözetim ve kapitalizm bir araya gelmektedir. Gözetim kapitalizmi, bu sürecin bir döngü hâline gelmesiyle oluşur. Yani, servet sahipleri daha çok servet yapmak için gözetime yatırım yapar; gözetime yatırım yaptıkça zenginleşmeye devam eder ve zenginleştikçe

gözetim sistemlerine yatırım yapmayı sürdürür. Bu döngünün interneti nasıl dönüştürdüğünü anlamak için Snowden’ın (2020) şu sözleri bizlere yardımcı olacaktır:

“Kâr elde etmek ve güç kazanmak için insanın özel hayatının kayıtlarını tuttular ve bir araya getirdiler. Böylece bir zamanların ücretsiz interneti kendini, çağdaş bir yozlaşmanın, gözetim kapitalizminin içinde buldu.”

Gözetim kapitalizminde insanlar kendi verilerini üretmekte, verili metalar olarak üretilmekte ve kendisi hakkında üretilen metaları geri almaktadır. Bu durumda insan aynı anda hem üretici, hem ürün hem de tüketici olmaktadır (Bloom, 2019: 8). Bu sürecin ortaya çıkışı ve büyümesi yirmi yıllık bir zaman dilimi içinde olmuştur. Özellikle yeni yüzyılın ilk on yılı biterken verinin nasıl kullanılacağına dair bir zihniyet değişimi yaşanmıştır. Veri, toplandıktan sonra işlevsiz hâle gelen statik bir şey olmak dışında artık “yeni bir ekonomik değer biçimi yaratmak için kullanılan bir iş hammaddesi” hâline gelmiştir (Mayer-Schönberger - Cukier, 2013: 13). Bu dönüşümün odağında, gözetim kapitalizminin de doğmasına yol açan, platformların hizmet iyileştirmeleri için gerekenden daha fazla kullanıcı verisi toplama mantığı yatmaktadır.

Gözetim kapitalizminde sosyal ağlar, çevrim içi platformlar, reklam ve analitik şirketler, mobil uygulamalar, girişimler (start-up’lar) ve veri şirketleri gibi özel sektör oyuncularını ön plandadır. Her biri hem kendisi hem de çevresi aracılığıyla devasa boyutta veri toplayabilmektedir. Ölçümlenmesi her ne kadar zor olsa da, neredeyse herkes özel sektörün herhangi bir devlet kurumundan daha fazla veri topladığından emindir (Rosenzweig, 2016:126). Özel sektör kuruluşlarının derinlemesine gözetimi, devlet gözetimi kadar tehlikeli bir olgudur. Fakat genel yapısı itibarıyla gözetim kapitalizmi, devlet gözetiminden farklıdır. Devlet gözetimi disipline dayalı, daha düz ve yüzeyselken gözetim kapitalizmi göze çarpmayan, oyalayıcı ve rahat tasarlanmıştır (O’Shea, 2021: 57).

İnsanların geride bıraktıkları dijital izleri tanımlamak için ortaya atılan bir terim olan “veri dışatımı”⁶ temelde eylem ve faaliyetler sonucu ortaya çıkan ikincil verilere vurgu yapmaktadır. Birçok şirket ikincil verileri hizmetlerini iyileştirme, özelleştirme ve geliştirme amacıyla toplayıp işlemek için kullanmakta ve altyapılarını bunları elde edebilecek biçimde tasarlamaktadır (Mayer-Schönberger - Cukier, 2013: 120). Zuboff, veri dışatımının platformların kendilerini iyileştirme çalışmalarında kullanılmasını madalyonun yalnızca bir tarafını oluşturduğuna dikkat çekmektedir. Zuboff’a göre gözetim kapitalizmi bedava hammadde olarak gördüğü insan deneyimlerine tek taraflı el koyar ve davranışsal verilere dönüştürür. Bu verilerin bir kısmı Mayer-Schönberger ve Cukier’in ifade ettiği gibi hizmet iyileştirme ve geliştirme faaliyetlerinde kullanılsa da geri kalan “üretim fazlası veriler” belirli işlemlerden geçerek kişinin şimdi, yakında ve gelecekte neler yapacağını öngören ürünler hâline gelmektedir. Öngörü ürünleri, Zuboff’un “davranışsal vadeli işlem piyasaları” olarak adlandırdığı yeni nesil piyasalarda alınıp satılır metalar olarak sunulmaktadır. Bu ticari operasyonlar ise gözetim kapitalistlerinin zenginleşmesinde büyük rol oynamaktadır (Zuboff, 2019: 8).

Öngörü ürünleri yalnızca gelecek davranışların alınıp satıldığı yeni bir pazar türünde satılmaktadır. Gözetim kapitalizminin elde ettiği kâr genellikle davranışsal vadeli işlem piyasasından gelmektedir. Her ne kadar ilk zamanlar reklamverenler bu yeni pazar yerinin baskın oyuncularına olsa da, bu tür pazarların bu gruplarla sınırlı olmadığı aşikârdır. Zuboff’un dediği gibi yeni öngörü sistemleri, Ford’un seri üretim sistemlerinin tesadüfen sadece otomobille ilgili olduğu gibi, yalnızca tesadüfen reklamlarla ilgilidir. Her iki durumda da sistemler diğer birçok alana uygulanabilmektedir. Hâlihazırda görünür olan eğilim, insan davranışları hakkında olasılıksal bilgi satın almak ve/veya insanın gelecekteki davranışlarını etkilemekle ilgilenen herhangi bir aktörün, bireyin veya grubun “davranışsal öngörü ürünlerini” satın almak için pazara istediği zaman giriş yapabileceğidir (Zuboff, 2019: 96).

⁶ İng: data exhaust.

Sevignani (2016: 51), gözetim temelli çevrim içi iş modellerini, “*internet kullanıcıları hakkındaki verilerden üretilen metaları sunan ticari faaliyetler*” olarak tanımlar. Ona göre kullanıcı gözetimi, çevrim içi davranışların metalara dönüştürüldüğü bir modeldir ve söz konusu iş modeli çevrim içi ekonomide kârlılığı arttırmada belirleyici hâle gelmiştir. Aynı bakış açısıyla gözetim kapitalizminin, insanların profilini çıkarmak ve yalnızca para kazanmak için onların davranışlarını anlamak üzerine kurulduğu ifade edilebilir. Gözetim kapitalistleri verileri yalnızca anlık davranışları tahmin etmek ve yönlendirmek için değil aynı zamanda makine öğrenimi aracılığıyla kişinin gelecekteki kimliğinin profilini çıkararak şirketlere gelecekteki karar ve davranış kalıplarını etkileme gücü vermek için kullanmaktadır. Altında yatan bu özellikleri neticesinde gözetim kapitalizminin etik olmadığı söylenebilmektedir (Falbe vd., 2020: 29 - 30).

Gözetim kapitalizminin temelleri altı beyan üzerine inşa edilmiştir ve her bir beyan bir öncekinin devamı niteliğindedir. Zuboff’a göre gözetim kapitalizmi sırasıyla aşağıdaki beyanlarda bulunur (2019: 179):

- (1) İnsan deneyimlerinin rahatça edinilebilen hammaddeler olduğunu iddia ediyoruz. Bu iddiaya dayanarak bireylerin hakları, çıkarları, farkındalıklar ve anlayışları ile ilgili düşünceleri görmezden gelebiliyoruz.
- (2) İddiamıza dayalı olarak bir bireyin deneyimini davranışsal verilere dönüştürmek için alma hakkımız olduğunu öne sürüyoruz.
- (3) Ücretsiz hammadde iddiamızdan yola çıkan “alma hakkımız”, insan deneyiminden elde edilen davranışsal verilere sahip olma hakkını verir.
- (4) Alma ve sahip olma haklarımız, verilerin neyi açığa çıkardığını bilme hakkını verir.
- (5) Alma, sahip olma ve bilme haklarımız, bilgimizi nasıl kullanacağımıza karar verme hakkını verir.
- (6) Alma, sahip olma, bilme ve karar verme haklarımız; alma, sahip olma, bilme ve karar verme haklarımızı koruyan koşullara haklarımızı verir.

Altı maddeden oluşan gözetim kapitalizmi hiyerarşisi, birbirini besleyen, geliştiren ve her bir maddenin diğerinin yolunu açtığı bir zincir şeklindedir. Oysaki

birinci maddeye izin verilmediği takdirde diğer maddelerin hiçbir işlevi ve geçerliliği yoktur. Birine izin verildiğinde ise arkasından daha fazlası gelmektedir. Zuboff, cehalet mutluluktur cümlesine atıfta bulunarak bu durumu “*bizim cehaletimiz onların mutluluğudur.*” şeklinde yorumlar. Eğer insanlar kendi varlıklarına ait fiziksel ve zihinsel tüm faaliyetlerin neden birer hammaddeye dönüşerek el konulduğunu ve sonrasında kendilerine karşı kullanıldığını sorgularsa gözetim kapitalistlerinin inşa ettiği servet üretim süreci yıkıma uğrayacaktır. Servet birikim mantığını sınırlayan ve yasaklayan kararlı bir toplumsal tepki olmadığı sürece, gözetim kapitalizmi günümüz kapitalizminin baskın türü olarak görülmeye devam edecektir (Zuboff, 2019: 53).

Gözetim kapitalizminde derinlemesine bir bilinmezlik söz konusudur. İnsanların klavyede ne kadar hızlı yazı yazdığının bile takip edildiği ve başka verilerle birleştirilerek üzerine çıkarımların yapıldığı bir sistemde verinin kaynağı olan özne durumdan haberdar değildir. Gözetim kapitalistlerinin şeffaflık olarak sunduğu birtakım genel geçer bilgiler arka plandaki gerçeği göstermede yeterli değildir. 2018’de yapılan bir araştırmada, Facebook kullanıcıların 4’te 3’ünün platformun kendilerini ilgi alanlarına göre kategorilerde altında sakladığını bilmediği tespit edilmiştir (Rainie - Hitlin, 2019). Bir başka araştırmada ise Facebook kullanıcılarının %69’u her gün işe gidip gelmenin, %72’si yeni bir işe başlamış olmanın, %66’sı ise cep telefonu kamera özelliklerinin Facebook tarafından bilinmediğini düşündükleri ifade etmişlerdir (Uluk - Aral, 2018). Bu araştırmalar ve ölçülen farkındalık düzeyi, platformların görülmesine izin verdiği, buz dağını yalnızca görünen kısmı üzerinden yapılmıştır. Bu düzeyde bile bilinmezlik durumu oldukça yüksektir.

Gizlilik ve güvenlik problemlerinin sürekli ortaya çıkmasıyla birlikte son beş yılda Facebook ve Google kullanıcılarını hangi hedefleme kategorileri altında tuttuğunu gösterse de iki nedenden dolayı büyük bir yanlış söz konusudur: (1) bizim hakkımızda sahip oldukları bilgiler, yalnızca bizimle paylaştıkları bilgilerle sınırlı değildir. (2) algoritmaların bizim hangi verilerimizi kullanarak geleceğimizi tahmin ettiği veya çeşitli verilerimizi bir araya getirerek hangi yeni veri setini oluşturduğuna dair hiçbir bilgilendirmeye ulaşma imkânımız yok.

Google ve Facebook, kullanıcılara sorunlu bir yüzeysel şeffaflık sunarken bunu dahi yapmayan birçok şirket vardır. Bugün büyük veri şirketleri başta olmak üzere reklam, analitik veya çeşitli amaçlarla kurulmuş irili ufaklı birçok şirketin bizim hakkımızda ne bildiklerine dair hiçbir bilgi yoktur. Örneğin, teknoloji şirketi New Relic'in en çok ziyaret edilen 10.000 sitenin 1591'inde kullanıcı izleme yazılımı vardır ve tüm web trafiğinin %4,5'ini takip edebilmektedir⁷. New Relic, bu şekilde devasa ve çok çeşitli veri kaynaklarına sahiptir. Alışveriş, haber, video ve oyun gibi çok farklı sitelerden kullanım verileri toplamaktadır. Aynı kullanıcının ziyaret ettiği farklı kategorilerdeki sitelerden aynı kullanıcı hakkında farklı veriler çekebilmekte; bunları analiz ederek insanlar hakkında anlamlı veriler oluşturabilmektedir. Konunu muhatabı, kaynağı ve öznesi olan insanın ise bu gelişmelerden bihaberdir. Gözetim kapitalizminin çarkları bu bilinmezliğin arkasında hızla dönmektedir.

Zuboff, gözetim kapitalizminde insanların ürün mü yoksa müşteri mi olduğunu Google örneği üzerinden sorgulamaktadır. Ona göre kullanıcılar müşteri değildir; çünkü Google ile aralarında herhangi bir ekonomik değiş tokuş süreci yoktur. Kullanıcılar işçi de değildir; çünkü kapitalistler işçileri işe aldığında onlara maaş verir ve üretim aracını sağlar. Bu sistemde kullanıcılar emekleri için ödeme almazlar ve üretim araçlarını yönetmezler. Kullanıcıların “ürün” olduğu söylene de bu da yanıltıcıdır. Böylelikle Zuboff kullanıcıları ne müşteri ne işçi ne de ürün olarak nitelendirmektedir. Ona göre kullanıcılar, hammadde arz kaynağıdır. Ürünler, hammaddenin işlenmesiyle oluşan öngörü ürünleri; müşteriler ise reklam borsalarında kullanıcıların gelecekteki davranışları üzerine ticaret yapan kuruluşlardır (Zuboff, 2019: 10; 2019: 69-70).

Gözetim kapitalizmi, bedava verdiği hizmetin karşılığında kullanıcı verilerinin toplandığına yönelik bir iddia barındırmaktadır. Kapitalistlerin yanı sıra birçok teknoloji yazarı da konu veri gizliliği ve güvenliği olduğunda verilerin “rıza dayalı” ve “hizmet karşılığında” mübadele edildiği söylemi etrafında konuyu meşrulaştırmaktadır. Bu söylem en sonunda da “eğer ürün ücretsizse, ürün sizsiniz”

⁷ https://whotracks.me/trackers/new_relic.html

cümlesiyle tamamlanır. Gerçekte ise bu düşünce oldukça sorunludur. Konunun önemini göz ardı eder, kapitalistlerin “insan deneyimlerini rahatça alınabilen hammadde” olarak görmesini meşrulaştırır. Ücretsiz hizmet ve veri mübadelesinin neden sorunlu olduğunu ve toplumu nasıl bir yanılsamaya maruz bıraktığını üç maddede açıklayabiliriz:

(1) Ücretli hizmetler: *“Eğer bir ürün için para ödemiyorsanız ürün sizsinizdir.”*

ifadesi ücretsiz hizmetlerin veri toplamasını meşrulaştırmak için kullanılmakta ve kullanıcılara sorumluluk yüklemektedir. Bu ifadenin bağlamdan kopartılarak sürekli insanların önüne çıkartılması sanki ücretli hizmetlerin davranışsal veri toplamadığı algısı yaratmaktadır. Hâlbuki akıllı saatler, akıllı telefonlar, otomobiller, buzdolapları, Google Nest gibi kişisel asistanlar, giyilebilir teknolojik aletler vb. tüm ağa bağlanabilen cihazlar tüketicisinden veri toplamaktadır. Sadece cihazlar değil; Spotify ve Netflix gibi paralı üyeliklerle hizmet sağlayan platformlar da kullanıcı derinlemesine gözetlemekte ve başka kanallardan da elde ettiği verilerle yeni anlamlar üretebilmektedir. İnsanlar, ücretsiz hizmette nasıl gözetleniyorsa ücretli hizmette de aynı şekilde gözetlenmektedir.

(2) Dayatılmış hizmetler: *“Eğer bir ürün için para ödemiyorsanız ürün sizsinizdir.”*

ifadesi eğer ürünün bedeli yoksa geçerliğini yitirmektedir. Öyle ki bir şeye para ödemek için bir şeyin satın bedelinin olması gerekir. Google uygulamalarının (Gmail, Maps, Arama vb.), WhatsApp’ın, Instagram’ın veya bunun gibi birçok uygulama ve hizmetin paralı versiyonları yoktur. Hizmetlerin ücretli alternatiflerinin olmaması, kullanıcıların bu platformları ücretsiz kullanmasını dayatmaktadır. Ücretli bir alternatif söz konusu değildir, bu durum kullanıcının pazarlık gücünü yok etmektedir. Amaç da zaten kullanıcının pazarlık etmemesini ve gerçekten “bedava” hizmetin tadını çıkartmasına aracı olmaktadır. Cegłowski (2016), şirketlerin “hizmetleri kullanmamakta özgürsünüz” şeklinde sunduğu seçenek için şöyle der: *“teoride gözetim kapitalizminden kurtulmakta insan özgürdür fakat bu elektrikten veya pişmiş yemekten vazgeçmek gibidir.”*

(3) Kullanılmayan hizmetler: “Eğer bir ürün için para ödemiyorsanız ürün sizsinizdir” ifadesi hizmetinden faydalanan platformların veri toplamasını meşrulaştırırken; hizmetinden hiç faydalanılmasa bile başka birçok şirketin kişinin verisini topladığını gizler. Örneğin, Facebook ve Google gibi şirketler, üçüncü taraf olarak birçok site ve uygulamadan kullanıcılar hakkında bilgi toplar. Ayrıca, kendi platformuna üye olmayan insanların bile verilerini toplayarak gölge profiller oluşturur (Ruckenstein - Granroth, 2019). Daha önce sözü edilen New Relic, BlueKai, Acxiom ve LiveRamp gibi şirketler kullanıcıya hiçbir hizmet sunmazken onlar hakkında olabildiğince çok yerden veri toplamakta ve bundan milyonlarca dolar para kazanmaktadır.

Yukarıda sıralanan üç başlıkta görüleceği üzere, ücretsiz hizmetin karşılığında veri toplama işlemi büyük bir yanılgıdan oluşmaktadır. “Ürün sizsiniz” söylemi, gözetim kapitalistlerinin görünmesini istemediği asıl gerçeğin üstünü örten bir örtü görevini görmektedir.

ÜÇÜNCÜ BÖLÜM

DİJİTAL VERİ BAĞLAMINDA MAHREMİYET ve ETİK WEB

3.1. Büyük Veri Kavramı

Veri kelimesinin İngilizcesi olan *Data*, Latince “olgu” anlamında “bilinen” demektir. Günümüz tanımında “*kaydedilmesine, analiz edilmesine ve yeniden düzenlenmesine izin verilen bir şey*” şeklinde karşılık bulmaktadır (Mayer-Schönberger - Cukier, 2013: 85). Büyük veri ise “*çoklu, özerk kaynaklara sahip, büyük hacimli, karmaşık, büyüyen veri kümeleriyle*” ilişkilidir (Sütcü - Aytekin, 2018: 157). Büyük veri, büyük miktarda bilgi içeren büyük miktardaki verinin toplanması anlamına gelmektedir. Bir yandan da hacimli ve devasa miktardaki verinin verimli bir şekilde analiz edilmesi ve işlenmesini içeren bir kavramdır (Mohanta vd., 2020: 5). Mayer-Schönberger ve Cukier (2013: 14) büyük verinin “*yeni içgörüler çıkarmak ya da yeni değer biçimleri yaratmak amacıyla, piyasaları, organizasyonları, vatandaşlar ile hükümetler arasındaki ilişkileri ve daha fazlasını değiştiren biçimlerde, insanın daha küçük ölçekte yapılamayacak ama büyük bir ölçekte yapabildiği şeyleri*” ifade ettiğini paylaşmaktadır.

Veri, daha önce gözetim çalışmaları başlığında yer aldığı gibi binlerce yıldır toplanmakta, analiz edilmekte ve saklanmaktadır. Veri toplamanın amacı yüzlerce yıl önce nüfus sayımı, devletlerin stratejik üstünlük kurması, hastalıkların önlenmesi ve tespiti gibi amaçlara dayalı olarak ön plana çıkarken son iki yüz yılda birçok alanda, birçok kurum ve kuruluş tarafından birçok amaca yönelik şekilde devinim göstermektedir. Çağın perspektifinden bakıldığında ise veri artık eskisi gibi toplanma amacına sadık olarak, birincil amaç doğrultusunda kullanılmamaktadır. Aksine, veri artık potansiyel kullanımıyla değer biçilen bir hâle dönüşmüştür. Dijitalleşen veri artık ne kadar kullanılırsa, analiz edilirse veya işlenirse değerinden hiçbir şey kaybetmeyen, yeni tahminlerin oluşmasına önayak olarak yeni verilerin üretilmesine katkı sağlayan bir bilgi parçacıdır.

Büyük veri temelde öngörmeyle ilişkilidir. Bu ilişki bize büyük verinin bilgisayara insan gibi düşünmesini öğretmekle ilgisi olmadığını, onun yerine tahmin yürütmek, kestirimde bulunmak ve olasılıklar çıkarmak amacıyla büyük miktarda veriyi bir dizi matematik işlemine tabi tutmakla ilgisi olduğunu açıklar. Öngörünün ne denli başarılı olduğu ise verinin miktarıyla doğrudan bağlantılıdır. Algoritmik sistemler ne kadar çok veriyle beslenirse hem tahmin yürütme performansları artar ve hem de kendi sistemlerinde iyileşme gerçekleşir (Mayer-Schönberger - Cukier, 2013: 19 - 20).

Büyük veriyi ele alırken bunun yeni bir olgu olduğunu ifade etmek yanlış olur. Onlarca yıldır araştırma şirketleri yeni bilgiler üretmek için büyük miktarda veri toplamış; istihbarat faaliyetlerinde suçu önlemek için veri kullanılmış; sigorta şirketleri, bankalar ve borsa yatırımcıları risk ve fırsatları erken tespit etmek için kapsamlı veri akışlarından yararlanarak çeşitli modeller oluşturmuştur. Farklı alanlarda toplanan verinin amacı *“olgular, kişiler ve olaylar arasındaki korelasyonların, erken göstergelerin ve neden-sonuç ilişkilerinin araştırılması ve sonucuna göre karar alınması.”* çerçevesinde birleşmektedir (Klous - Wielaard, 2016: 2). Sözü edilen büyük miktarda veri ise hâlihazırda perakende satış işlemleri, kredi kartı sensörleri, barkodlar, radyo frekansı ile ürün tanımlama, uydu tabanlı navigasyon sistemleri vb. işlemler aracılığıyla üretilmektedir. Bunlara ek olarak iş raporları, anketler, e-postalar gibi yapılandırılmamış birçok verinin analizi de büyük verinin bir parçası olarak karşımıza çıkmıştır. Bu noktada Peter Gentsch (2018: 11), büyük veriyi bugünkü anlamıyla gerçekten “büyük veri” yapan şeyin nesnelerin interneti, mobil cihazlar ve sosyal medya aracılığıyla toplanan veriler olduğunu vurgulamaktadır.

Büyük veri, *“bir teknoloji ile bir sürecin birleşiminin kısaltmasıdır.”* Bu ifadede teknoloji büyük miktardaki veriyi oldukça kısa sürede eleme, sıralama ve sorgulama yeteneğine sahip bir bilgi işleme donanım biçimi olarak kabul edilmektedir. Süreç ise model oluşturmak için veri madenciliğini, modelleri kestirime dayalı analitikle elemeyi ve analitiği yeni verilere uygulamayı kapsamaktadır. Teknolojinin ve sürecin birleşimi, veri akışlarını belirli, yüksek seviyede veri yoğun bir bilgi türüne dönüştürmek için gereken tekniği içermektedir (Cohen, 2013: 1921).

Büyük veri, elektronik işlemlerin ortaya çıkışından beri var olmuştur. Bu çerçevede büyük verinin boyutları dört V ile tanımlanmaktadır (Gentsch, 2018: 13): a) Volume (Hacim): Saklanacak ve daha sonra analiz edilecek veri miktarını belirtmektedir. b) Velocity (Hız): Bir tarafta yüksek hızla verilerin üretilmesini, diğer taraftan da aynı hızda bu verilerin depolanması, işlenmesi ve analiz edilmesini açıklamaktadır. c) Variety (Çeşitlilik): Yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış verileri kapsamaktadır. d) Veracity (Doğruluk): Büyük verinin doğruluğu, güvenilirliği, anlamlı olmasıyla ilişkilidir. Dört V'ye ek olarak Mohanta ve arkadaşları (2020: 5) beşinci V'yi ekler: Value (Değer). Bu kavram ise doğru analiz ile üretilen bilgilerin doğruluğunu artırmak ve iyileştirmekle ilgilidir. Doğru verilere dayanan kestirimler verinin değerinde önemli bir yere sahiptir. Beş boyut arasında en çok tercih edilen ve sıklıkla başvuru alanlar hacim, hız ve çeşitliliktir. Hacim, doğru çıktılar üretmek için daha güvenilir veriler analiz edilmesi bakımından önemlidir. Gerek internet gerek sensörler gerekse farklı kaynaklardan toplanan veriler üretim hızından daha hızlı şekilde işlenmelidir. Yine, farklı kaynaklardan olabildiğince çeşitli verilerin toplanması büyük veride farklı perspektiflerin oluşmasına ve daha doğru analizlerin yapılmasına katkıda bulunmaktadır (Al-Abassi vd., 2020: 41). Yukarıda yer alan büyük verinin beş temel V'si zaman geçtikçe ve teknoloji yeni olanaklar sundukça değişim içinde olmuştur ve olacaktır. Bunlara ek olarak Validity (Geçerlilik), Variability (Değişkenlik), Volatility (İstikrarsızlık), Vulnerability (Kırılganlık) ve Visualization (Görselleştirme) gibi farklı boyutlar da büyük verinin özellikleri arasında yerini almaktadır (Subramaniam, 2018).

Mayer-Schönberger ve Cukier (2013: 22), büyük verinin “neden” değil, “ne” hakkında olduğunun önemine özellikle vurgu yapmaktadır. Onlara göre bir olayın nedenini her zaman bilmek veya irdelemek gerekmez; dolayısıyla veriyi bizim konuşturmamızdan ziyade kendisinin konuşmasına izin vermek, “ne” olduğunu yönelik kayda değer bir ipucu sağlar. Yazarlar, büyük veride “neden” ve “ne” sorularını Amazon örneği üzerinden yorumlar (a.e. s. 56-60). Amazon ilk kurulduğundan beri tüketicilerin hangi kitapları satın aldığını, almaktan vazgeçtiklerini, incelediklerini ve onlara ne kadar süre baktıklarını kayıt altına almaktadır. Onlara göre tüketicilerin bir kitabı neden aldığı veya almaktan vazgeçtiğini

bilmek satışları tetiklemek için bir anlam ifade etmez. Oysaki “ne” sorusunun cevabını bilmek tüketicilerin nereye tıklayacağını yönlendirmede oldukça etkilidir.

Boyd ve Crawford (2012: 663), büyük veriyi üç kavramın etkileşimine dayanan kültürel ve bilimsel bir fenomen olarak tanımlamaktadır. Bu kavramlar;

- (1) **Teknoloji:** büyük veri kümelerini toplamak, analiz etmek, birleştirmek ve karşılaştırmak için hesaplama gücünü ve algoritmik doğruluğu en üst seviyeye çıkartmak.
- (2) **Analiz:** Ekonomik, sosyal, teknik ve yasal iddialarda bulunma amacıyla kalıplar oluşturmak için büyük veri kümelerinden yararlanmak.
- (3) **Mitoloji:** Büyük veri kümelerinin doğruluk ve nesnellik gibi daha önce imkânsız görülen tahminleri üretebilen yüksek bir zekâ ve bilgi biçimi sunduğuna dair yaygın bir inanç.

Büyük veri, yapılandırılmış, yarı-yapılandırılmış ve yapılandırılmamış şeklinde üç türe sahiptir. Yapısı belli olan sınıflanmış değerler yapılandırılmış veri için örnek gösterilebilir. Bir sütundaki ad, soyad, kimlik numarası, eğitim durumu vb. gibi başlıkların içerisinde yer alan içerikler belirli biçimlere sahip olduğu ve oradan hareketle yazıldığı için yapılandırılmış verilerdir. Günümüzde verilerin çoğu yapılandırılmamış biçimdeki verilerdir; ses, fotoğraf ve metin tabanlı dosyalar, web siteleri ve içerikleri, e-postalar ve dahası yapılandırılmamış verilere örnek teşkil eder. Bu tür verilerde satır ve sütun bulunmamaktadır. Yapılandırılmamış verilerin yapısal hâle getirilmesi için metin madenciliği gibi yöntemler kullanılır. Veri tabanlarında saklanan kısmen yapısal kısmen yapısal olmayan veriler yarı-yapılandırılmış verilerdir (Sütcü - Aytekin, 2018: 90-93).

3.2. Kişisel Veri Kavramı

“Kişisel verileriniz değerlidir. Facebook ve Google gibi şirketler kendilerine ait olmayan bir şeyden, yani bizim verilerimizden para kazanıyor. Bazılarına göre The Matrix filmindeki gibi “sağlıyoruz.” 1999 yapımı filmde, kıyamet sonrası bir robot dünyasını desteklemek için insanların enerjisi kullanılıyordu. Yanal düşünürlerden Jaron Lanier, benzer bir senaryoyla alternatif bir fikir

öne sürüyor. 2013 yılında piyasaya çıkan Geleceğin Sahibi Kim? adlı kitabında bilgisayarları pasif araçlar olarak görmememiz gerektiğini çünkü böyle yaparak insan - bilgisayar etkileşiminin nasıl gerçekleştirdiğini anlayamadığınızı dile getiriyor. Ayrıca, sadece en hızlı bilgisayar ağlarına sahip olanların değil, tüm endüstrilerin çalışmalarına değer veren bir toplum yaratarak insanların kendi ekonomik kaderlerini belirleme hakkını geri kazandırmak istiyor.” (Klous - Wielaard, 2016: 17).

Kaliforniya Tüketici Gizliliği Yasası, kişisel veriyi “*belirli bir tüketiciyi veya hane halkını doğrudan veya dolaylı olarak tanımlayan, açıklayan veya onlarla ilgili olacak şekilde ilişkilendirilmiş veya ilişkilendirme yeterliliğine sahip bilgiler.*” olarak sınıflandırmaktadır (California Legislative Information, 2018). AB Genel Veri Koruma Tüzüğü’nde kişisel veri “*kimliği belirli veya belirlenebilir gerçek kişilerle ilgili her türlü bilgi*”⁸ şeklinde tanımlanmıştır.

Kaliforniya Tüketici Gizliliği Yasası, verilerin kişisel nitelikte olması için dört koşul sunmaktadır: (1) Veri, kişiyi açıkça tanımlayan bilgiler içermelidir. Bunlar isim, fotoğraf, kimlik numarası gibi verilerden oluşabilir. (2) Veri, içeriğine göre değil amacına göre kişiyi tanımlamalıdır. (3) İlaç kullanım dozajı, reçete, reçete seri numarası veya telefon numarası gibi veriler kişiyi tanımlama amaçlı kullanılabilir. Bu tür veriler de kişisel veri kabul edilir. (4) Kurumların veri tabanlarında, yazılımlarında veya dâhili sistemlerinde verileri düzenli biçimde saklamak için izleme yapılabilmektedir. Takip sistemleri belirli bir amaca yönelik bizzat bireyleri takip etmese bile daha sonra bu gibi sistemler üzerinden elde edilecek tüm veriler kişisel olarak sınıflandırılmaktadır (Andrews, 2019).

Bu tanımlar ve açıklamalar neticesinde kimliği belirli olan veya belirlenebilen her şeyin kişisel veri olduğu söylenebilmektedir. En genel bakış açısıyla ad – soyad, fotoğraf, kimlik numarası, sosyal güvenlik numarası, cep telefonu numarası, IP adresi ve e-posta adresi gibi bilgiler birer kişisel veridir. Çünkü bu bilgilerle kişinin kimliği doğrudan belirlenebilmektedir. Öte yandan cinsiyet, eğitim seviyesi, yaş aralığı vb.

⁸ GDPR, Madde 4(1), <https://gdpr-info.eu/art-4-gdpr/>.

bilgileri tek başına kişisel veri olarak değerlendirmek mümkün değildir. Örneğin, yalnızca “erkek olmak” bilgisi tek başına bir kişiyi belirlemede yeterli değildir; zira dünyada milyarlarca erkek vardır. Fakat “erkek olmak” bilgisi başka bilgilerle yan yana getirildiğinde ve geriye doğru gidilip milyarlarca kişiden tek bir kişi filtrelenebiliyorsa o zaman cinsiyet verisini kişisel veri olarak kabul edebiliriz. Diğer ifadeyle, tek başına anonim bir veri olduğu düşünülen bu gibi bilgiler yapbozun bir parçası hâline dönüşürse ve kimliği ifşa etmede yardımcı bir rol oynarsa artık birer kişisel veri olarak değerlendirilir.

Kişisel verileri kişisel olmayan verilerden ayıran en önemli temel unsur, verinin kişinin kimliğini tanımlamada yetersiz olmasıdır. Yani bir kişinin kimliğini tanımlayamayan veri kişisel olmayan verilerdir. Yukarıda da yer verildiği gibi cinsiyet bilgisi tek başına kişinin kim olduğunu açığa çıkarmakta yeterli değildir. Hava durumu, bir şehirdeki araç sayısı, çalışma saatleri, şirketlerin kurumsal e-posta adresleri (örn: info@sirket.com) ve hisse senedi fiyatları gibi veriler kişisel olmayan veriler olarak değerlendirilebilir. Ayrıca kişisel veri olan ama anonimleştirilen veriler de kişisel olmayan veri kabul edilmektedir.

3.2.1. Türlerine Göre Kişisel Veri

Kişisel veriler genel olarak iki başlık altında toplanmaktadır. Kişilerin kim olduğunu belirleyen veya belirlenebilir kılan bilgiler kişisel veri olarak adlandırılırken bunlardan bazıları doğası gereği “hassas kişisel veri” veya “özel nitelikli kişisel veri” şeklinde literatürde yer almaktadır. Kişisel Verilerin Koruması Kanununda ⁹ özel nitelikli kişisel veriler “*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*” şeklinde sıralanmıştır. Bu verilerin dışındaki kişiyi tanımlayabilen tüm veriler için genel kişisel veriler denebilmektedir. Böylece kişisel verileri genel veriler ve hassas veriler olarak ayırabilmek mümkündür. KVKK’nın

⁹ 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kabul Tarihi: 24/3/2016

sıralamasında yer alan hassas veriler dikkate alındığında genel verilerden en temel farkının çalınması, sızdırılması veya kötüye kullanılması durumunda kişiye doğrudan zarar verme veya onu manipüle etme potansiyeline sahip olmasıdır.

Kişisel veriler genelden özel birçok alandan temin edilip birçok bileşenden oluşmaktadır. *Enterprivacy Consulting Group*, bireylerin özel, kamusal veya iş hayatıyla ilgili olabilecek birçok veriyi kategorilere ayırmıştır.

Genel Kategori	Alt Kategori	Tanım ve Örnek Veriler
İçsel	Bilgi ve inanç	Kişinin bildiği veya inandığı hakkındaki bilgiler (Dini, inanç, siyasi ve felsefi görüş)
	Doğrulama	Kişinin bildiği bir şeyle kimliğini doğrulamak için kullandığı bilgiler (Şifre, Pin kodu, annenin kızlık soyadı, güvenlik sorusu cevabı)
	Tercihler	Kişinin ilgi alanları ve tercihleri (Fikirler, beğeniler, hoşlanılmayanlar, zevkler, favori yiyecekler)
Dışsal	Tanımlama	Kişinin benzersiz ya da yarı-benzersiz olarak tanımlayabilen bilgiler (Ad-soyad, kimlik numarası, fotoğrafı, kullanıcı adı, parmak izi)
	Etnik Grup	Kişinin kökeni veya soyunu belirten bilgiler (İrk, etnik köken, dil, lehçe, aksan)
	Cinsel	Kişinin cinsel yaşamını belirten bilgiler (Cinsel yönelim, cinsiyet kimliği, cinsel eğilimler)
	Davranışsal	Kişinin davranış ve etkinliklerini tanımlayan bilgiler (Çevrim içi / çevrim dışı faaliyetler, çevrim içi aramalar, tıklanan bağlantılar, görüntülenen sayfalar)
	Demografik	Kişinin başkalarıyla paylaşılan özellikleri (Yaş aralığı, fiziksel özellikleri, gelir grubu, coğrafi konumu)
	Sağlık	Kişinin sağlık durumunu belirleyen bilgiler (Fiziksel ve zihinsel sağlık, test sonuçları, engellilik durumu, sağlık geçmişi, kan grubu, reçeteler)

	Fiziksel Özellikler	Kişinin fiziksel özelliklerini tanımlayan bilgiler (Cinsiyet, boy, kilo, yaş, saç rengi, cilt tonu, dövme, ben)
Finansal	Finansal Hesaplar	Kişinin finansal hesaplarını tanımlayan bilgiler (kredi kartı, banka hesabı)
	Mülkiyet	Kişinin sahip olduğu, kiraladığı, ödünç aldığı şeyler hakkındaki bilgiler (Araba, konut, kişisel eşya)
	Finansal İşlemler	Kişinin satın alma, para harcama ve geliri hakkındaki bilgiler (alışverişler, kredi kartı kayıtları, vergi ödemeleri, para harcama rutini)
	Kredi	Kişinin maddi itibarıyla ilgili bilgiler (kredi kayıtları, kredi puanı, kredi değeri)
Sosyal	Mesleki	Kişinin eğitim ve kariyeri hakkındaki bilgiler (maaş, iş geçmişi, referanslar, sertifikalar, bitirilen okullar)
	Sabıka	Kişinin sabıka kaydı hakkındaki bilgiler (mahkûmiyetler, suçlamalar, aflar)
	Sosyal Durum	Kişinin sosyal yaşantısı hakkındaki bilgiler (karakter, itibar, sosyal statü, medeni durum, siyasi bağlantılar)
	Aile	Kişinin ailesi ve ilişkileri hakkındaki bilgiler (aile yapısı, kardeşleri, çocukları, evlilikleri, ilişkileri)
	Sosyal Ağ	Kişinin arkadaşları veya sosyal çevresi hakkındaki bilgiler (arkadaşlar, bağlantılar, tanıdıklar, dernekler, grup üyelikleri)
	İletişim	Kişinin diğer kişilerle gerçekleştirdiği görüşmeler hakkındaki bilgi (telefon kayıtları, e-postalar, sesli mesajlar)
Geçmiş	Hayat Hikâyesi	Kişinin geçmişte yaşadığı gerek kendini gerekse çevresini etkilemiş olabilecek bilgiler (savaş, göç)
	Cihaz	Kişinin kişisel kullanım amaçlı kullandığı cihaz hakkındaki bilgiler (IP adresi, MAC adresi, tarayıcı parmak izi)

İzleme	İletişim	Kişinin başka biriyle iletişim kurmasına yardımcı olan mekanizmalar hakkındaki bilgiler (e-posta adresi, fiziksel adres, telefon numarası)
	Konum	Kişinin konumu hakkındaki bilgiler (Ülke, GPS koordinatları, oda numarası)

Tablo 3.1: Kişisel Veri Kategorileri (Cronk, 2017).

Kişisel veri kategorileri birçok yöntemle sağlanan bilgi akışıyla oluşmaktadır. Bu bilgi akışına dair Dünya Ekonomik Forumu, kişisel verilerin nasıl toplandığını üç başlık altında listelemiştir (Davis, 2014):

Kişisel veriler	Örnek Veriler
Bireysel sağlanan veriler	Fotoğraflar, e-postalar, çevrim içi işlem verileri, kayıt formları, iş başvuruları, blog yazıları, tweetler
Gözlenen veriler	Konum verisi, arama kayıtları, çevrim içi tarama verileri, güvenlik kameraları
Çıkarımsanan veriler	Kredi notu, tüketici profilleri, hedefli reklamcılık, tahmini trafik akışları, bulaşıcı hastalıkların yayılmasındaki kalıplar

Tablo 3.2: Information Accountability Foundation, Dünya Ekonomik Forumu (Davis, 2014).

- **Bireysel olarak sağlanan veriler:** Kişinin bir sosyal ağ profili oluşturması, kredi kartıyla çevrim içi alışveriş yapması, form doldurması, uygulama yüklemesi veya çeşitli çevrim içi platformlarda içerik üretip paylaşması bireysel olarak verilerini sağladığı anlamına gelmektedir. Öte yandan veriyi toplayanın kim olduğuna bağlı olarak bireysel veri sağlamak, bireyin verisine el konulması şeklinde de yorumlanabilmektedir. Fotoğraflar, videolar, blog yazıları, tweetler benzersiz kişisel ifade ve durumları barındırdığı için güçlü duygusal bağlar barındırır.

- **Gözlenen veriler:** Kişilerin gerçekleştirdiği etkinliklerin izlenmesi ve kayıt altına alınmasıyla elde edilen verilerdir. Gözlenen veriler, gözetlenen kişinin farkındalığı çerçevesinde iki türde gerçekleşir. (1) Kişinin genel farkındalığı ile aktif olarak gözlenen veriler (tarayıcı çerezleri, kredi kartı işlemleri, konum verileri vb.). (2) Farkındalığın oluşmadığı, ansızın yapılabilen ve pasif olarak gözlenen veriler (yüz tanıma teknolojileri, WIFI tarama araçları, radyo frekans tanımlama çipleri vb.). İster aktif ister pasif olsun, insanlarda kendileri hakkında hangi verilerin gözlendiği, nasıl kullanıldığı ve kimlere satıldığı konusunda farkındalık eksikliği söz konusudur.
- **Çıkarımsanan veriler:** Yapay zekâ algoritmaları ve makine öğrenimi uygulamaları farklı veri türlerini sentezleyerek yeni veri kategorileri oluşturmaktadır. Sentezlenen veriler doğrudan kişiyle bağlantılı olabildiği gibi ona bağlı olmayan verilerden de oluşabilmektedir. Genellikle farklı kaynaklı verilerin bir araya getirilmesiyle geleceği öngörmeye yönelik kullanılır. Kişinin, geleceğini tahmin etme amacıyla onun hakkında üretilen yeni veri kategorisi hakkında bilgi sahibi olması neredeyse imkânsızdır. Çıkarımsanan veriler, kişisel verilerin “yeni bir varlık sınıfı” olduğu iddiasının en güçlüsü olarak kabul edilmektedir.

Kişisel veri türlerine ait genel bir çerçeve sunarken tasarım mantığı daha fazla kişisel veri toplamak ve üretmek üzerine inşa edilen sosyal ağların bunları nasıl elde ettiği ve neleri içerdiği kategoriler altında toplanmıştır. Gizlilik ve güvenlik uzmanı Bruce Schneier’in (2010) sosyal ağ verilerini altı maddede sıralamıştır:

- a) **Hizmet verileri:** Kişinin kullanmak üzere sosyal ağlara girdiği verilerdir. Örn: Adı – soyadı, doğum tarihi veya yaş gibi veriler.
- b) **İfşa edilen veriler:** Kişinin kendi sayfasında paylaştıklarıdır. Örn: Blog yazıları, iletiler, mesajlar, yorumlar, fotoğraflar.
- c) **Bırakılmış veriler:** Kişinin başka kullanıcıların sayfasında paylaştığı verilerdir. İfşa edilen verilerden farkı, kişinin bir kere paylaştıktan sonra kontrol sahibi olamamasıdır.

- d) **Tesadüfi veriler:** Başkalarının kişi hakkında paylaştıkları verilerdir. Örn: bir kullanıcının içinde başkaları olan bir fotoğrafı paylaşması. İfşa edilen ve bırakılmış veriler ile benzer olsa da kişinin kendisinin paylaşmaması ve kontrol sahibi olmaması temel farktır.
- e) **Davranışsal veriler:** Kişinin alışkanlıkları hakkında toplanan verilerdir.
- f) **Türetilmiş veriler:** Diğer tüm veriler göz önünde bulundurularak kişi hakkında türetilen verilerdir.

Bu başlıkta genel ve hassas olmak üzere iki türde ele alınan kişisel verilerin, niteliklerine göre birçok alt kategoriye ayrılarak yapbozun parçalarını oluşturmada önemli bilgi kırıntılarına sahip olabildiğine yer verilmiştir. Kişisel veri kategorilerinin oluşumunda ise ana odağın kişilerin ifşa ettikleri verilerin yanı sıra habersiz gözetlenerek toplananlar ve veri birleşimleriyle yeni verilerin türetilmesi olduğu söylenebilmektedir.

3.2.2. Kişisel Veri Ekosistemi

Bireysel olarak sağlanan, gözlenen ve çıkarımsanan kişisel veriler birden fazla kaynaktan toplanmakta, saklanmakta ve birleştirilerek analiz edilmektedir. Kişisel veri ekosistemi, en başından en sonuna kadar tüm bu aşamaların bir araya gelmesiyle şekillenmektedir.

Kişisel veri		Bireysel sağlanan	Gözlenen	Çıkarımsanan
Kişisel veri oluşturma	<i>Cihazlar</i>	Mobil cihazlar / akıllı telefonlar, masaüstü / taşınabilir bilgisayarlar, elektronik okuyucular, akıllı cihazlar, sensörler, akıllı şebekeler		
	<i>Yazılımlar</i>	Bilgisayar uygulamaları, mobil cihaz uygulamaları, medikal cihaz uygulamaları, tüketici ürün ve aletleri uygulamaları, ağ yönetim yazılımları		
Toplama, Saklama		Perakende ürün satan çevrim içi firmalar, internet izleme şirketleri, arama motorları, elektronik sağlık veri sağlayıcıları, GSM operatörleri, internet hizmet		

	sağlayıcıları, finans kuruluşları, kamu kurum ve kuruluşları
Analiz, Ürünleştirme	Pazar araştırma borsaları, reklam borsaları, sağlık kayıtları borsaları, iş zekâsı sistemleri, kredi büroları, kamu yönetimi
Tüketim	Son kullanıcılar, kamu kurum ve kuruluşları, küçük – orta ve büyük çaplı işletmeler

Tablo 3.3: Veri Oluşumundan Veri Tüketimine Kişisel Veri Ekosistemi (WEF, 2011).

Kişisel veriler tablo 3.3'te verildiği gibi bir düzen içindedir ve nihayetinde maddiyata veya farklı değerli varlıklara dönüşür. Ayrıca bu veriler yeniden değerlendirildiğinde, yani analiz ve ürünleştirme aşamasında, yeni kullanım alanları yaratabilmektedir. Örneğin, bir süpermarkette yer alan güvenlik kamerasının kullanım amacı öncelikle ve ekseriyetle hırsızlık girişimlerini caydırmak, önlemek veya tespit etmektedir. Öte yandan bu kameralarla müşterilerin hangi reyonlarda zaman geçirdiği gibi birden çok parametre de toplanıp analiz edilebilir. Böylece toplanan verinin yaratılan yeni kullanım alanı kurumlar için geliri artıracak bir yöntem olarak karşımıza çıkar. Verinin genişletilmiş biçimde ve çoklu amaca yönelik kullanılmasına ilişkin en çarpıcı örnek Google'a aittir. Google'ın Cadde Görüntüleme (Street View) araçları tüm dünyada caddeleri, sokakları ve meydanları fotoğraflayarak Google Haritaları daha çekici ve kullanışlı hâle getirmiştir. Söz konusu araçlar sokakların fotoğrafını çekerken diğer yandan civardan toplayabildiği tüm verileri de toplamayı başarmıştır. Örneğin araçların gezintisi sırasında ofislerdeki, evlerdeki ve diğer yerlerdeki tüm modemleri tarayarak onlara ait WIFI adlarını toplamıştır. (Mayer-Schönberger - Cukier, 2013: 116).

Kişisel veriler, birçok endüstride sıkça kullanılmaktadır. Gerek bireysel gerekse kitlesel olarak toplanan kişisel verileri kullanıldıkları sektörlerle ve kullanım amaçlarına göre aşağıdaki gibi sıralayabiliriz (FTC, 2021):

- Finansal hizmetler: Bankacılık ve yatırım hesapları,
- Kredi hizmetleri: Kredi veya banka kartları; ev, otomobil, ihtiyaç kredileri,
- Sigortacılık faaliyetleri: Sağlık, otomobil veya hayat sigortaları,

- İndirim kuponları ve özel teklifler,
- Dergi ve bülten üyelikleri,
- Web ve mobil hizmetler: E-postalar, aramalar, sosyal ağlar,
- Ürün ve hizmet sektörleri: Kargo dağıtımı, kablolu yayın hizmetleri,
- Avukatlar: Dava soruşturmaları için,
- Gazeteciler: Haberin doğruluğunu kontrol etmek için,
- Pazarlama: Dijital, e-posta ve telefon yoluyla,
- Veri şirketleri: Özel şirketler ve/veya tüketiciler hakkında bilgi toplama ve tekrar satma
- Özgeçmiş araştırmaları: İşverenler ve ev sahipleri tarafından araştırmalar
- Kolluk kuvvetleri: Kayıp ve aranan kişileri bulma, görgü tanığı arama
- Araştırma: Üniversiteler, devlet kurumları ve ticari şirketler tarafından yapılan araştırmalar (sağlık, finans ve çevrim içi arama verileri)
- Dolandırıcılıkların önlenmesi ve tespiti
- Devlet hizmetleri ve faaliyetleri

Federal Ticaret Komisyonu'nun (FTC) veri şirketleri hakkındaki raporunda yer alan bu sektörler amaçları doğrultusunda kişisel verileri yoğun olarak kullanmaktadır. Kişisel veri kategorileri dikkate alındığında bu veriler kişinin açık rızasıyla alınmış veya bilgisi haricinden toplanmış olabilir. Aynı zamanda gözetim sonucu kişilerin tüketim alışkanlıklarından ve çevrim içi / çevrim dışı davranışlarından belirli kalıplar oluşturularak çıkarımlar üretilmesiyle de bilgi kategorileri meydana gelebilir. Bu kalıpların oluşmasında özellikle olabildiğince veri toplamak ve başka şirket, kurum ve kişilerle veri değiş-tokuşu yapmak veri tabanlarını daha da doldurur ve zenginleştirir (D-CENT, 2015).

Birçok araştırma, web aramalar, tarayıcı geçmişi, ürün satın alma işlemleri, Facebook beğenileri gibi davranışsal ve işlem verilerinden farklı türlerde kişisel verilerin çıkarılabileceğini göstermektedir. Örneğin, kişinin etnik kökeni, dini, siyasi görüşleri ve ilişki durumu gibi kişisel özelliklerin yanı sıra dürtüler, duygusal denge, depresyon durumu ve yaşama sevinci gibi kişilik özellikleri Facebook beğenilerinden makul düzeylerde doğru çıkarılabilmektedir. Birinin mesleği tarama geçmişinden veya

işsiz olması mobil uygulama kullanım sıklığından tahmin edilebilir. Hatta Kanadalı araştırmacılar, bir bilgisayar klavyesindeki yazma kalıplarının ritmini analiz ederek güven, sinir durumu, üzüntü ve yorgunluk gibi duygusal durumlar bile yüksek doğrulukla tahmin etmişlerdir (Christl, 2017: 71).

Kişisel veri ekosisteminde veri tabanlarının değeri, hacimleri, doğruluğu ve değişken sayısı arttıkça yükselir. Çünkü bu yükseliş beraberinde yeni çıkarımların üretilmesini ve yeni bilgi kategorilerinin oluşturulmasına yardımcı olur. Nihayetinde kişinin doğru ve detaylı profilinin çıkartılması ile veri tabanının zenginliği doğru orantılıdır.

Birçokları kendi kişisel verilerini değersiz, sıkıcı, anlamsız ve hatta utanç verici olarak görebilmektedir. Fakat pazarlama şirketleri, veri madencileri ve platformlar aynı düşünceye sahip değildir (O'Shea, 2021: 26). İki büyük veri şirketi olan Acxiom ve Oracle'ın müşterilerine sağladığı veriler tablo 3.4'te gösterilmektedir. Acxiom, Avrupa, ABD ve diğer bölgelerden 700 milyon kişinin verisine sahiptir. Her bir kişi hakkında 3000'e yakın nitelik tanımlamıştır. Oracle, insanları binlerce kategoriye bölerek 2 milyar kişi hakkında 30,000'den fazla nitelik sağlamaktadır. Bu veri örnekleri kişisel veri ekosisteminde veri çeşitliliğinin ve zenginliğinin önemini göstermede kilit bir rol oynamaktadır.

Tüketicilere ilişkin veri örnekleri	
Acxiom	Oracle
Yaş, cinsiyet, eğitim, kariyer, siyasi görüşler, ilişki durumu, çocuk sayısı, satın almalar, medya tüketimi, borç, gelir, araç ve ev sahipliği, banka ve sigorta poliçeleri, kredibilite notu, sosyo-ekonomik durum, ekonomik istikrar, etnik köken, din, sağlık durumu (engelli, diabet, kalp hastası vb.), alkol ve tütün kullanımı, şans oyunları ve kumar alışkanlıkları, sosyal ağ kullanım sıklığı, ev yaşantısı (geniş aile, çekirdek aile, karavanda yaşam), vergi ödeme	Yaş, cinsiyet, eğitim, meslek, çocukların sayısı ve yaşı, gelir, borç, hobiler, ilgi alanları, satın almalar, kredi kartı türü ve markası, yeni ebeveyn olanlar, yeni taşınanlar, detaylı satın almalar (Kahve, kraker, ağırlık kesici, dondurulmuş gıda vb.), merak duyulanlar (ev kredisi, öğrenci kredisi, eşcinsel filmler, çekiliş / şans oyunu vb.), siyasi konulara bakış açısı (vergi, göçmen konuları, sağlık, ulusal güvenlik vb.), satın alma gücü (az, orta, yüksek), aramalar (nakdi yardım, uçak,

dönemi, çocuk sahibi olma niyeti, evlat edinme niyeti	otel, kiralık araç, mide ağrısı, duyma zorlukları, kalp ağrısı, tıbbi kuruluşlar, kürtaj, eşcinsel evlilik, grev, boykot, ayaklanma vb.)

Tablo 3.4: Acxiom ve Oracle’ın Sahip Olduğu Tüketicilere İlişkin Veri Örnekleri (Christl, 2017: 64).

3.2.3. Kişisel Verilerin Korunması Üzerine Uluslararası Düzenlemeler

Kişisel verilerin korunması anlayışı yirminci yüzyılın ikinci yarısına dayanmaktadır. Kişisel verilerin korunması ile özel hayatın gizliliği farklı haklar olmasına rağmen birbirleriyle yakın ilişki içerisinde. Özel hayata saygı olarak da anılan özel hayatın gizliliği hakkı ilk olarak 1948 yılında İnsan Hakları Evrensel Beyannamesi’nde koruma altına alınmış temel insan haklarından birisi olarak karşımıza çıkmaktadır (Council of Europe, 2018). 1950 tarihli Avrupa İnsan Hakları Sözleşmesi’nde de şu şekilde yer almaktadır: *“Herkesin özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesine hakkı vardır.”* Bu hakkın korunması ve gözetilmesi ilerleyen yıllarda Avrupa Birliği’nin kişisel verilerin korunmasına yönelik gerçekleştirdiği çeşitli çalışmalar doğrultusunda daha çok geliştirilmiştir (European Court of Human Rights, 1950).

Özel hayatın gizliliği, İnsan Hakları Evrensel Beyannamesi ve Avrupa İnsan Hakları Sözleşmesi’nde bir hak olarak bilgisayar, internet veya diğer teknolojik gelişmelerin ortaya çıkmasından çok daha önce kabul edilmiştir. Bu hak toplumun ve bireyin yaşam kalitesi başta olmak üzere birçok alanda önemli avantajlar sağlamakla birlikte özel hayata saygı hakkına yönelik yeni riskleri de beraberinde getirmiştir. Kişisel bilgilerin toplanması ve kullanılmasının hangi koşullarda gerçekleşeceğini belirlemeye duyulan ihtiyaç neticesinde “bilgi gizliliği” ve “bilginin kendi kaderini tayin hakkı” gibi ifadelerle bilinen yeni bir gizlilik kavramı ortaya çıkmıştır. Söz konusu durum kişisel verilerin korunmasına ilişkin yeni kanun ve düzenlemelerin geliştirilmesine yol açmıştır (Council of Europe, 2018: 18).

1967 yılında ABD’de “Bilgi Edinme Özgürlüğü Yasası (FOIA)” adıyla bir düzenleme yürürlüğe girmiştir. Buna göre bireylere kamu kurumlarından kendileri

hakkındaki belgelere erişme hakkı tanınmıştır (FOIA, 2014). Bu yasa ile sınırlı da olsa ABD’de ilk defa kişinin kendi verilerini talep etme hakkı doğmuştur.

OECD, 1980 yılında “*Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri*” adıyla bir veri koruma kılavuzu yayımlamıştır. Bu kılavuzda bugün aktif olarak yürürlükte olan veri koruma tüzüklerine benzer maddeler yer almıştır (Kramer - Hoar, 2017):

- Veri toplamının amacı kullanım amacıyla örtüşmelidir,
- Veriler kaybolmaya ve yetkisiz erişimlere karşı korunaklı olmalıdır,
- Bireyler kendileri hakkında hangi verilerin toplandığını bilme hakkına sahip olmalıdır,
- Bireyler kendileri hakkında toplanan verilere dilediği zaman erişme hakkında sahip olmalıdır,
- Bireyler saklanan verilerine itiraz edebilmeli, kendisiyle ilgili verileri değiştirebilme veya silebilme hakkına sahip olmalıdır.

Birleşmiş Milletler (BM), 1990 yılında kişisel verilerin korunmasına ilişkin “*Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*” adlı, tamamı tavsiye niteliğinde ve devletlerin inisiyatifine bıraktıkları 10 ilke paylaşmıştır (UN General Assembly, 1990): (1) kişisel veriler kanuna uygun ve adaletli toplanmalı ve işlenmelidir. (2) kişisel verilerden sorumlu kişiler verilerin doğruluğunu ve uygunluğunu kontrol etmeli ve eksiksiz tutulmasına özen göstermelidir. (3) kişisel veriler amaca uygun kullanılmalı, ilgili kişinin rızası dışında kullanılmamalı ve saklanma süresi belirtilen süreyi aşmamalıdır. (4) Bireyler kendileriyle ilgili verilerin işlenip işlenmediğini öğrenme, düzeltme ve silinmesini talep etme hakkında sahiptir. (5) Din, ırk, siyasi görüş, inanç ve cinsel yaşam gibi hassas bilgiler toplanmamalıdır. (6) Birden dördüncü maddeye kadar olan tüm şartlar, ancak ve ancak ulusal güvenlik, kamu düzeni ve sağlığı gibi durumlarda sınırları açıkça belirtilmek suretiyle istisna sayılabilir. (7) Saklanan verileri hem doğal afetlerden hem de yetkisiz erişimlerden korunmak için üst düzey güvenliği sağlamak için önlemler alınmalıdır. (8) Her ülke kendi iç hukuk sistemine göre bu ilkelerin takip ve gözetimi için belirli bir birim tayin etmelidir. (9) Sınır ötesi veri akışı, yalnızca ilgili ülkelerin mevzuatları kapsamında

mahremiyetin garanti altında olması şartıyla serbestçe dolaşabilir. (10) Mevcut ilkeler tüm kamusal ve kişisel dijital dosyalara ve isteğe bağlı olarak geleneksel/fiziksel dosyalara uygulanabilir hâle getirilmelidir.

3.2.3.1. Dünyadaki Yasal Düzenlemeler

Avrupa’da veri koruma çalışmaları ve düzenlemeleri 1970’li yıllara dayanmaktadır. Bu alandaki ilk düzenleme bu eyalette geçerli olmak üzere Almanya’nın Hessen eyaletinde kabul edilen veri koruma kanunudur. Kanun, tapu kayıtlarına erişimin sağlanabilmesi için verilerin toplanması ve kaydedilmesine yönelik usul ve esasları belirlemek için hazırlanmıştır (KVKK, 2019: 11). 1973’te İsveç’te kabul edilen veri koruma yasası, dünyanın ilk ulusal çaptaki veri koruma düzenlemesi olmuştur. 1980’lerin ortalarıyla birlikte Fransa, Almanya, Hollanda ve Birleşik Krallık gibi ülkeler de veri koruma ile ilgili kanunları uygulamaya koymuştur (Council of Europe, 2018: 18).

28 Ocak 1981 yılında kişisel verilerin korunmasını güçlendirmek amacıyla ilk uluslararası sözleşme Avrupa Konseyi tarafından kabul edilmiştir. “*Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme*” adlı 108 sayılı bu sözleşme, hâlen veri koruma alanındaki yasal bağlayıcılığı olan tek uluslararası sözleşme niteliğine sahiptir. Sözleşme, hem özel hem de yargı ve kolluk kuvvetleri dâhil olmak üzere kamu sektörü tarafından gerçekleştirilen tüm veri işleme süreçleri için geçerlilik taşımaktadır (Council of Europe, 2018: 24). OECD’nin 1980 yılında yayımladığı ilkeler dizisindeki gibi bu sözleşme de kişisel verilerin suiistimal edilmesine karşı koruma, amacı dışında kullanılmasını ve gerekenden fazla süre tutulmasını engelleme gibi konuları ele almaktadır. Türkiye, sözleşmenin kabul edildiği tarihte ilk imzalayan ülkelerden biri olmuş ve sözleşmeyi 17 Mart 2016 tarihinde iç hukuka dâhil etmiştir.

AB, en kapsamlı ilk veri koruma düzenlemesini 1995 yılında 95/46/EC sayılı “*Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlamentosu ve Avrupa Konseyi Direktifi*” ile kabul etmiştir. Direktif,

genel hatlarıyla kişisel verilerin işlenmesini ve serbest dolaşımıyla ilgili bireylerin korunmasını içermektedir (Council of Europe, 2018: 19).

1995 yılından Mayıs 2018'e kadar kişisel verilerin korunmasına ilişkin AB'nin başlıca yasal dayanağı 95/46/EC sayılı direktif olmuştur. Avrupa Birliği Genel Veri Koruma Tüzüğü (*General Data Protection Regulation - GDPR*)¹⁰ 2016 Nisan'da AB Parlamentosunda kabul edilmiş ve 2018 Mayıs itibarıyla tamamıyla yürürlüğe girmiştir. Bu tüzük şu anda kişisel verilerin korunmasına ilişkin en güncel ve kapsamlı düzenleme olarak karşımıza çıkmaktadır.

GDPR, veri işleyen kurum ve kuruluşların yapması gereken yedi temel ilke sunmaktadır. 5. maddede yer verilen bu ilkeler şu şekildedir: (1) İşleme süreci veri sahibi için adil, şeffaf ve hukuka uygun olmalıdır. (2) Toplanan verilerin hangi amaçla kullanılacağı veri sahibine açıkça belirtilmelidir. (3) Yalnızca ihtiyaç duyulduğu kadar veri toplanmalı ve işlenmelidir. (4) Kişisel veriler güncel ve doğru tutulmalıdır. (5) Veri sahibinin kim olduğunu tanımlayan veriler yalnızca belirtilen amaçlar için gerekli olduğu sürece saklanmalıdır. (6) Veri işleme uygun güvenlik ve gizlilik tedbirleri alınarak yapılmalıdır. (7) Veri denetçisi, GDPR'ın öngördüğü tüm bu ilkelerin uygunluğunu sağlamakla sorumludur.

GDPR kapsamında bireylerin verilerini işlemek için açık rızalarının alınması gerekmektedir. Tüzüğün 7. maddesine göre veri işleme faaliyeti öncesi talep edilen rızaya ilişkin bilgiler yalın bir dilde, anlaşılır ve kolaylıkla ulaşılabilir olmalıdır. Kişi, verilerinin işlenmesine özgür biçimde rıza göstermeli ve dilediği zaman rızasını çekebileceği bir sisteme erişebilmelidir. GDPR uyarınca veri özneleri kişisel verilerine ilişkin şu haklara sahiptir (Privacy International, 2018):

- a) **Bilgi edinme hakkı:** Bireyler hem doğrudan sağladıkları hem de başka bir kaynaktan (üçüncü taraflardan) elde ettikleri kişisel verilerin nasıl işlendiği konusunda bilgilendirilmelidir.

¹⁰ General Data Protection Regulation, 2016/679, Kabul Tarihi: 26/4/2016.

- b) **Eriřim hakkı:** Bireyler, kiřisel verileri toplanırken bilgilendirilmeli ve kiřisel verilerinin iřlenmesi hakkında bilgi alabilmelidir.
- c) **İtiraz hakkı:** Bireyler, kiřisel verilerinin iřlenmesine itiraz etme hakkına sahip olmalıdır.
- d) **Düzeltilme, engelleme ve silme hakkı:** Bireyler, verilerinin doęru, eksiksiz ve güncel tutulmasını saęlamak için kendileri hakkında iřlenen verileri düzeltilme, engelleme ve silinmesini talep etme hakkında sahip olmalıdır.
- e) **Profil çıkarma ve otomatik karar vermeyle ilgili haklar:** Kanunda yer alan tüm haklar profil çıkarma ve otomatik karar verme süreçleri için de geçerli olmalıdır. Söz konusu haklar ayrıca insan müdahalesini talep etme veya kararlara itiraz etme hakkını içermelidir.
- f) **Veri taşınabilirlięi hakkı:** Bireyler, bütün kiřisel verilerini veri sorumlusundan evrensel şartları saęlayan makinelerin okuyabileceęi biçimde alma ve talep etmeleri durumunda başka hizmetlere taşıma hakkında sahip olmalıdır.
- g) **Etkili bir hukuk yoluna başvuru hakkı:** Bireyler, kiřisel verilerinin hukuka uygun olarak iřlenmedięini düşündükleri zaman yargıya başvurma hakkına sahiptir.
- h) **Tazminat hakkı:** Haklarının ihlal edildięi tespit edilen kiři, uğradıęı maddi veya manevi zararın tazmini hakkına sahiptir.

GDPR, AB'yi kapsadıęından dolayı ABD'de yařayan ABD vatandaşlarına uygulanmamaktadır. ABD'de ise GDPR benzeri geniş ölçekli bir veri koruma düzenlemesi yoktur. Bunun yerine eyaletlerin kendi veri gizlilięi düzenlemeleri mevcuttur. Bunlardan biri, 2004 yılından yürürlüęe giren “*Kaliforniya Çevrim İçi Gizlilięi Koruma Kanunu*”dur. Genel anlamda Kaliforniya’da ikamet eden vatandaşların kiřisel verilerini ve gizlilik haklarını korumak için düzenlenmiřtir. Kanun, ticari web siteleri ve çevrim içi hizmetlerde gizlilik sözleşmelerine sahip olmasını ve bu sözleşmelerde web sitelerinin hangi kiřisel verileri topladıęını ve kimlerle paylařtıęını belirtmesini şart kořmaktadır (California Legislative Information, 2004). *CalOPPA* kısaltmasıyla bilinen kanun aynı zamanda ABD’nin en büyük gizlilik yasalarından birisi olarak kabul edilmektedir. Haziran 2020’de kabul

edilen Colorado Gizlilik Yasası ve Mart 2021’de kabul edilen Virginia Tüketici Verilerini Koruma Yasası gibi düzenlemeler Kaliforniya’daki yasaya benzer ilkelerle kendi eyaletlerindeki vatandaşların kişisel verilerini korumak amacıyla ortaya çıkmıştır (Carson, 2021). Diğer yandan çeşitli sektör, grup ve pazarlara özgü gizlilik yasaları da mevcuttur. ABD’de Çocukların Çevrim İçi Gizliliğini Koruma Yasası (COPPA), Gramm Leach Bliley Kanunu (GLBA), Adil Kredi Raporlama Kanunu (FCRA) gibi çeşitli bağlamlara özgü yasalar yer almaktadır.

Yasal düzenlemeler kişisel verinin olduğu her yeri bağlamaktadır. Buna insan kaynakları departmanları, kariyer formları ve şirket içi belgeler dâhil olduğu gibi veri toplayan web siteleri ve mobil uygulamalar da dâhildir. Bilindiği üzere çevrim içi ortamda veriler genellikle çerezler ve izleme pikselleri gibi farklı takip teknolojileriyle toplanmaktadır. Çevrim içi platformları bizzat ilgilendiren ve veri toplama ve işlemenin nasıl olması gerektiğine ilişkin yasal bir talimat Danimarka’da oluşturulmuştur. Danimarka Veri Koruma Kurumu (Datatilsynet), Şubat 2021’de yayımladığı bir kılavuzda zorunlu olmayan çerez kullanan web sitelerinin ilk açılışta kullanıcılardan onay alması gerektiğine yer vermiştir. Diğer ifadeyle, web sitesini ziyaret eden bir kullanıcı izin verdiği takdirde zorunlu olmayan çerezler aktif hale gelecek ve kişi hakkında bilgi toplayabilecektir. Kılavuzda yer alan kuruluşların çerez kullanımıyla ilgili sorumluluklarını aşağıdaki gibi özetleyebiliriz (Datatilsynet, 2021):

- a) Önceden izin almadan zorunlu olmayan çerezler aktif hâle getirilmemelidir.
- b) Kullanıcılar, çerez ayarlamalarına yönelik kontrolleri kendileri yapabilmelidir.
- c) *“Bu web sitesini kullanmaya devam ederek çerez kullanımını kabul ediyorsunuz”* ifadesi aktif bir kullanıcı onayını içermemektedir.
- d) Çerez ayarlamaları sırasında yalnızca “Evet” ve “Daha fazla bilgi” butonlarının yanı sıra çerezlere izin vermeyi tamamen reddetmek için açık bir “Hayır” butonu da yer almalıdır.
- e) Çerezlerin ne amaçla yerleştirildiği ve ne kadar süreyle kalacağı anlaşılması kolay bir dille belirtilmelidir.
- f) Üçüncü taraflara hangi bilgilerin iletildiği kullanıcılara açıkça beyan edilmelidir. Örn, IP adresi, ziyaret ettiği sayfalar, tarayıcı bilgileri vb.

g) Açık rızanın geri alınması, açık rıza vermek kadar kolay olmalıdır.

3.2.3.2. Türkiye’deki Yasal Düzenlemeler

Türkiye, 28 Ocak 1981 yılında Avrupa Konseyi tarafından kabul edilen 108 sayılı sözleşmeyi ilk imzalayan ülkelerden biri olmuş ve sözleşmeyi 17 Mart 2016 tarihinde iç hukuka dâhil etmiştir (KVKK, 2019: 17).

Kişisel verilerin korunması kapsamında 5237 sayılı Türk Ceza Kanununda yer alan 135. maddeye göre, hukuka aykırı olarak kişisel verileri kaydeden kişilere bir yıldan üç yıla kadar hapis cezası verilmektedir. Yine aynı maddenin ikinci fıkrasında söz konusu verilerin siyasi, felsefi ve dini görüşlere ve ırk, sağlık, ahlaki eğilim, cinsel yaşam veya sendika bağlantılarından oluşması durumunda cezanın yarı oranında arttırılacağına yer verilmektedir. 136. maddede, kişisel verileri hukuka aykırı biçimde üçüncü kişilerle paylaşmanın, yaymanın ve ele geçirmenin iki yıldan dört yıla kadar hapis cezası olduğu yer almaktadır ¹¹.

Elektronik haberleşme sektöründe düzen ve denetim sağlamak amacıyla hazırlanan 5809 sayılı Elektronik Haberleşme Kanununda tüketici haklarının gözetilmesi bağlamında kişisel verilerin korunmasına yönelik hususlara yer verilmiştir. Bu kapsamda “*Kişisel verilerin işlenmesi ve gizliliğin korunması*” başlığında yer alan 51. Madde 13 fıkradan oluşmaktadır. 51. maddede, trafik ve konum verilerinin açık rıza alınmak şartıyla yurt dışına aktarılabilceği, kişisel verilerin işlendikleri amaçla bağlantılı olması ve işlendikleri amaç için gerekli olan süreye bağlı olarak muhafaza edilmesi gerektiği, işletmelerin saklanan kişisel verilerin güvenliğini sağlamada gerekli tedbirleri almakla yükümlü olduğu gibi esaslar ön plana çıkmaktadır ¹². Diğer yandan, Ticari İletişim ve Ticari Elektronik İletiler Hakkında Yönetmeliğinin 12’inci maddesinin (2)’nci fıkrası gereğince kişisel verilerin; üçüncü

¹¹ 5237 Sayılı Türk Ceza Kanunu, 25611 Sayılı Resmi Gazete, Kabul Tarihi: 26/9/2004

¹² 5809 Sayılı Elektronik Haberleşme Kanunu, 27050 Sayılı Resmi Gazete, Kabul Tarihi: 5/11/2008

kişilerle paylaşılabilmesi, işlenebilmesi ve başka amaçlarla kullanılabilmesi için ilgili kişiden önceden onay alınması gerekmektedir.

5982 Sayılı Kanun kapsamında 2010 yılında yapılan Anayasa değişikliği ile Anayasa'nın 20. maddesine aşağıdaki fıkra eklenmiştir (Koç, 2020: 119):

*“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.”*¹³

6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK)¹⁴, 24 Mart 2016 tarihinde kabul edilmiş ve 7 Nisan 2016'da yürürlüğe girmiştir. Kanun büyük ölçüde 95/46/EC sayılı direktif temel alınarak hazırlanmıştır (KVKK, 2019: 19). Birinci maddede yer aldığı gibi kanunun amacı *“kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.”* Kanunun 5. maddesinin 2. fıkrasında belirtilen şartlar dışında kişinin açık rızası olmaksızın kişisel veriler işlenemez. KVK Kurumunun hazırladığı rehberde kişinin yalnızca konu üzerinde değil, bununla birlikte açık rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerektiği vurgulanmaktadır. Bilgilendirme aşaması ise verilerin işlenmesinden hemen önce olmalıdır (Koç, 2020: 122).

2020 yılında Kişisel Verileri Koruma Kurumu, Amazon Türkiye'ye kişisel verileri mevzuata uygun işlemediği gerekçesiyle bir yaptırım uygulamıştır. KVK kurumunun 27/02/2020 tarihli ve 2020/173 sayılı karar özetinde¹⁵ çerez kullanımıyla ilgili bilgiler de yer almıştır. Kararda amazon.com.tr'yi ilk defa ziyaret eden bir kullanıcının, yalnızca siteye giriş yapmış olmasının verilerinin işlenmesi için açık rıza verdiği anlamına gelmediğine yer verilmiştir. Buna göre siteye giren kişinin verileri

¹³ 5982 Sayılı Kanun, 27580 Sayılı Resmi Gazete, Kabul Tarihi: 7/5/2010.

¹⁴ 6698 Sayılı Kişisel Verilerin Korunması Kanunu, Kabul Tarihi: 24/3/2016.

¹⁵ <https://www.kvkk.gov.tr/Icerik/6739/2020-173>.

işlenmeden önce kişisel verilerin işlendiğine dair aydınlatılmalı, bilgilendirilmeli ve kişinin buna onay vermesine dair bir sistem bulunmalıdır. Diğer yandan kararda, “*hizmetin açık rıza şartına bağlanmış olmasının açık rızayı sakatlayacağı*” yönündeki ifade tekrarlanmıştır. Söz konusu ifade KVKK’da açık rızanın üyelik veya hizmetin bir koşulu olarak dayatılmasının “hukuka ve dürüstlük kurallarına uygun olma”, “amaca bağlı, sınırlı ve ölçülü olma” gibi ilkelere aykırılık teşkil ettiği belirtilmiştir. Kararda amazon.com.tr’de yer alan “*sipariş verdiğinizde gizlilik bildirimi, kullanım ve satış koşullarını ve çerez bildirimini kabul etmiş olursunuz*” ifadesinin örtük irade beyanı olduğu ve bu tür bir onay almanın mevzuata uygun olmadığı değerlendirilmiştir. Bu karar, sitelerin çerez kullanımına yönelik daha sonradan emsal oluşturabilecek Türkiye’deki ilk ve kapsamlı kararlardan birisi olduğu için oldukça önemlidir.

3.3. Veri Gizliliği ve Güvenliği

Özel hayata saygı, mahremiyet ve özel hayatın gizliliği hakkı bugün ulusal ve uluslararası birçok yasal düzenleme ile güvence altına alınmıştır. Dijitalleşen dünya, insanları derinlemesine inceleyerek her bir davranışı izlemeyi ve onlar hakkında veri üretmeyi beraberinde getirmiştir. Devasa bir veri toplama sistemi, toplanan verilerden birleştirilerek uçsuz bucaksız yeni anlamlar üretilmesi ve verinin meta değerinin her geçen gün kıymetinin artması veri gizliliği, mahremiyeti ve güvenliğiyle ilgili endişelerin ortaya çıkmasına neden olmuştur.

Tim Berners Lee, 2017 yılında World Wide Web’in 28. yaşına istinaden yayınladığı mektupta web dünyasına yönelik endişelerini artıran üç eğilimden söz etmektedir:

- (1) Kişisel verilerin kontrolünün kaybolması,
- (2) Yanlış bilginin hızla yayılabilmesi,
- (3) Siyasi reklamların şeffaflık ihtiyacı.

Berners Lee, kişisel verilerin kontrolünün kaybolmasını şu sözlerle açıklamaktadır: “*Verilerimiz ambarlarda, bize gözden uzak tutuluyor ve veriler üzerinde doğrudan kontrol sahibi olamadığımız, neyi kiminle paylaşmak istediğimizi seçemediğimiz için, elde edebileceğimiz faydalardan yararlanamıyoruz.*” Bu ifade dijital teknolojinin toplumdaki vatandaşları izleyenler (bilinmez, görünmez, hesaplanamaz) ve izlenenler olarak iki gruba ayırdığını ortaya koymaktadır. Dijital haklar aktivisti Aral Balkan ise Tim Berners Lee’ye göre duruma daha kötümser bakmaktadır. Ona göre kişisel veriler “kaybolmuyor”, aksine, silikon vadisi tarafından “çalınıyor”. Balkan’a göre, Google ve Facebook gibi multi-milyarder şirketler gözetim kapitalizminin başarı hikâyeleridir.

Kişisel verilerin kötü amaçlı kişilerin eline geçebilmesi riski bağlamında bir güvenlik açığı her zaman için geçerlidir (Lyon, 2013: 236). Kişisel veri toplayan, üçüncü taraflarla paylaşan ve değiş-tokuş yapan şirketlerin çoğu son on yılda veri ihlalleri ve sızıntılarıyla sürekli olarak gündeme gelmiştir. Bazıları kullanıcılardan izinsiz veri toplamış, bazıları topladıkları verileri başkalarıyla izinsiz paylaşmış, bazıları ise gerekli saklama koşullarını sağlayamamış, yetkisiz erişimlere ve veri hırsızlarına maruz kalarak veri sızıntılarına sebep olmuştur.

2014’ün sonlarında Güney Koreli şirket LG’nin ürettiği bazı akıllı TV’lerin veri toplayıp şirketle paylaştığı ortaya çıkmıştır. Toplanan veriler arasında TV sahibinin hangi kanalları izlediği, ne zaman kanal değiştirdiği, TV’ye harici bir cihaz bağlı olup olmadığı, bağlıysa cihazın içerisinde neler olduğu gibi bilgiler yer almıştır. Bu durum bir blog yazarının kendisine gösterilen kişiselleştirilmiş reklamların izini sürmesiyle tespit edilmiştir. LG, veri toplama konusunda şeffaf bilgilendirme yapmamış; hatta söz konusu yazar tüketici veri paylaşımını kapatsa bile kullanım verilerinin LG’ye hâlâ iletildiğini belirtmiştir (Klous - Wielaard, 2016: 22).

2017’de gerçekleşen ve Microsoft Windows işletim sistemini hedef alan siber saldırılar 150 ülkede 200.000’den fazla bilgisayarı etkilemiştir. *WannaCry* adlı fidye yazılımıyla yapılan bu saldırılarda hackerlar Windows işletim sistemi kullanıcılarının bilgisayarlarına erişmiş, sabit disklerini kilitleyerek dosyalarını şifrelemiş ve şifreleri kaldırmak için fidye istemişlerdir. Bu siber saldırı, farklı siber saldırılara göre daha

büyük bir kitleyi etkilemiş ve mağdur etmiştir. WannaCry saldırısını diğerlerinden ayıran en önemli nokta ise Microsoft’a yazılım açığını ABD Ulusal Güvenlik Ajansı’nın (NSA) haber etmesidir. Çeşitli kaynaklara göre NSA, Microsoft’un bu yazılım açığını yıllardır bilmesine rağmen Microsoft’a hiçbir bildiride bulunmamıştır. NSA, kendi istihbarat faaliyetleri doğrultusunda bu açığı kullanarak hedefteki kişilerin bilgisayarlarına yıllar boyunca erişmiş ve veri sağlamıştır. NSA, hackerların da bu açığı keşfetmesiyle Microsoft’u haberdar etmek durumunda kalmıştır (O’Shea, 2021: 72).

Facebook, gerek sahip olduğu verilerin güvenliğiyle ilgili gerekse üçüncü taraf olarak başka kaynaklardan izinsiz topladığı verilere ilişkin ortaya çıkan skandallarla son yıllarda çokça hedef tahtasına oturtulmuştur. Birleşik Krallık Parlamentosu, 2019 yılında Facebook’u “Dijital Gangster” olarak tanımlamıştır. Yayınladıkları 108 sayfalık raporda, Facebook’un Airbnb ve Netflix gibi şirketlere kullanıcıların arkadaşlarının verilerini görme izni verdiği paylaşılmıştır. Ayrıca, Facebook ve uygulama geliştiriciler arasında kullanıcı kişisel verisi değiş tokuşu yapıldığına da yer verilmiştir (2019). Aynı yıl, Facebook’un şifre yönetim sistemlerinde bir açık olduğu ve Facebook ve Instagram’a kayıtlı yüzlerce milyon kullanıcının şifresinin “kriptolu” olarak değil düz metin olarak saklandığı ortaya çıkmıştır. Bu durum, binlerce Facebook çalışanının istediği zaman istediği kullanıcının şifresini düz metin olarak görebilmesi anlamına gelmektedir (Newman, 2019). Facebook’un veri güvenliğiyle ilgili yaşadığı sıkıntılar bunlarla da kalmamıştır. UpGuard Siber Risk Ekibi (2019), üçüncü taraflar aracılığıyla geliştirilen iki Facebook uygulaması veri setinin kamuya açık olarak internette paylaşıldığını duyurmuştur. Bu iki veri setinin büyük kısmının Meksikalı medya şirketi Cultura Colectiva’dan geldiği ve veri setlerinin Facebook kullanıcı etkinlikleri (beğeniler, yorumlar), hesap adları, FB kimlik numaraları gibi 540 milyondan fazla kayıt içeren 146 GB’lık veriden oluştuğu belirtilmiştir. Verilerin ne kadar zamandır kamuya açık olduğu ve kimlerin gördüğü üzerine bir bilgiye rastlanmamıştır. Fakat araştırmacılar bu iki veri setinin Amazon bulut sisteminde yer aldığını ve Facebook’la iletişime geçildikten sonra sistemden kaldırıldığını ifade etmişlerdir. Facebook, ortaya çıkarılan güvenlik skandallarının dışında kendisi de veri sızıntılarıyla ilgili açıklamada bulunmuştur. Örneğin, 2018’de büyük bir güvenlik

açığı sonucu hackerların Mark Zuckerberg de dâhil olmak üzere 50 milyon kullanıcının hesabına erişim sağladığını açıklamıştır. Bu açığın Facebook kullanıcı profil sayfasında olan “başkası gibi göster” sekmesi kaynaklı olduğu tespit edilmiştir. Kullanıcıların mağduriyeti sadece Facebook’la kalmamış; Tinder, Instagram ve Spotify gibi uygulamalara Facebook ile giriş yapan kişileri de etkilemiştir (Price, 2018). Tek bir şirket üzerinden verilen bu örnekler veri güvenliğinin ne kadar önemli olduğunun altını çizerken, aynı zamanda, güvenlik açıkları dolayısıyla yaşanan mağduriyetin yalnızca o şirketle kalmadığı ve etrafını ciddi biçimde etkilediğini de göstermektedir.

3.3.1. Veri Güvenliğinin Temel İlkeleri

Veri güvenliği kavramı genellikle kişisel verilerin suiistimallerden korunması sürecini ifade etmek için kullanılmaktadır. Privacy International (2018), “Veri Güvenliğinin İlkeleri” başlıklı metninde kişisel verileri toplayan ve kullanan özel şirket ve kamu kurumlarının bu verileri ilgili mevzuatlara göre işlemekle yükümlü olduklarının altını çizmektedir. Kurum, yerel ve uluslararası metinlerden yararlanarak verilerin işlenmesi bağlamında uyulması gereken ilkeleri ve bu ilkelerin önemini altı maddede açıklamaktadır:

- a) **Adil, yasal ve şeffaf:** Kişisel verilerin işlenmesi şeffaf, yasal ve adil olmalı. Kişisel veriler alınırken ve kimin bu verileri işleyeceği konusunda birey açıkça bilgilendirilmelidir. Eğer veri sorumlusu bu konuda şeffaf değilse verilerin başka kaynaklardan veya haksız biçimde elde edilmiş olması muhtemeldir.
- b) **Sınırlı bir amaca bağlılık:** Tüm kişisel veriler belirli ve meşru bir amaç için toplanmalıdır. Kişisel verilerin işlenmesi bu amaç doğrultusunda uygulanmalı ve en başta rıza alınan amaçlarla uyumsuz olmamalıdır. Veriler toplanırken kullanım amacı net biçimde belirlenmezse, veri hayatta kaldığı sürece başka amaçlar için kullanılabilir ve sonucunda bireyin zararına doğabilecek sonuçlara neden olabilir. Amacın bir sınıra bağlı olması gelecekteki olası sorunların ortaya çıkmasını en aza indirecektir.

- c) **Asgari kullanım:** Kişisel verilerin işlenmesi bağlam dâhilinde ve işlenme amacının gerekliliği ile sınırlı olmalıdır. Bu ilke, veri işleyenlerin amacına ulaşmak için ihtiyacı olan minimum veri miktarını belirlemesi ve toplamasıyla ilişkilidir. Daha sonra işe yarayabileceğini düşünerek veri toplama niyetine girişmek veri güvenliği bakımından kabul edilemez.
- d) **Doğruluk:** İşlenen kişisel verilerin doğru, güncel ve eksiksiz olması için gerekli tedbirlerin alınması gerekmektedir. Karar alma ve politika üretme süreçleri gün geçtikte verilere dayandırılarak gerçekleşmektedir. Verilerin doğruluğu, güncel ve eksiksiz oluşu ilgili süreçlerin yanlış olma riskini en aza indirecektir. Örneğin, güncel olmayan bir veri nedeniyle kişinin sağlık sigortası prim ücreti yüksek çıkabilir veya başvurduğu ihtiyaç kredisi olumsuz sonuçlanabilir.
- e) **Depolama sınırlaması:** Kişisel veriler yalnızca işlenme amaçları için gerek duyulan süre boyunca saklanmalıdır. Veriler adil, hukuka uygun, şeffaf olarak, sınırlı bir amaca yönelik, doğru, güncel ve asgari biçimde toplansa ve işlense dahi gereğinden uzun süre saklanmamalıdır.
- f) **Bütünlük ve gizlilik:** Kişisel verilerin kaybolması, zarar görmesi, yok edilmesi veya çalınması gibi risklere karşı güvenlik önemleri üst seviyede olmalıdır. Verilerin depolandığı alanlara yetkisiz girişlerin ve ifşalarının önlenmesi için güvenli bir altyapı kurulması ve sürdürülmesi gerekmektedir. Zayıf güvenli sistemler Facebook gibi küresel platformların yanı sıra Yemek Sepeti gibi ulusal şirketlerin de dâhil olduğu birçok şirketin veri ihlali yapmasına neden olmuştur. Verileri korumak ve altyapı güvenliğini sağlamak yasa dışı erişim risklerini ve ihlalleri en aza indirecektir.
- g) **Hesap verilebilirlik:** Kişisel verileri işleyen veya onlardan sorumlu olan yetkili kişiler veya kurumlar gerektiğinde mevzuatla ilişkili ilkelere, yükümlülüklerle ve kanunlara nasıl bağlı kaldığını ve uyduğunu gösterebilmeli ve hesap verebilmelidir. Bu ilke, etkili bir veri güvenliğinin anahtarıdır zira diğer tüm ilkeleri bir araya getirerek veri işleyenlerine ve sorumlularına yükümlülüklerle uyma sorumluluğunu yükler.

Verilerin korunmasını ve güvenliğini sağlamada etkili yöntemlerden birisi de veri anonimleştirmedir. Veri anonimleştirme, saklanan verileri ilgili kişiyi doğrudan tanımlayamayacak hâle getirme ve bu yolla verileri koruma altında tutma sürecidir. Anonimleştirme, kişisel tanımlanabilir bilgilerin “tanımlayıcı” özelliğinin bertaraf edilmesi şeklinde de açıklanabilir. Veri güvenliği ve mahremiyeti bakımından olmazsa olmazların başında gelmektedir. Veri anonimleştirme yöntemleri şu şekilde sıralanmaktadır (IAPP, 2018):

- 1) **Nitelik silme:** Bir sütundaki verilerin tamamının kaldırılmasıdır. Örneğin, veri tabanında ad-soyad, ders adı ve sınav puanına ait üç sütundan ad-soyad sütunundaki veriler silindiğinde kimin kaç puan aldığı belirli olmayacağı için bu veri seti anonimleştirilmiş olur.
- 2) **Kayıt silme:** Birden çok sütunda yer alan verilerin tamamının kaldırılmasıdır. Yukarıda verilen örnek ele alındığında yalnızca bir sütun değil birden çok sütundaki verilerin silinmesidir.
- 3) **Karakter maskeleyme:** Bir verideki değerlerin çeşitli sembollerle kullanılarak maskelenmesidir. Genellikle bütünü bir kısmın maskelenmesini içerir. Örneğin, e-posta adresinin veri tabanında a*****p@eposta.com şeklinde saklanmasıdır.
- 4) **Takma isim verme:** Kişisel tanımlanabilir bilgilerin uydurulmuş değerlerle veya farklı kodlarla değiştirilmesiyle oluşturulmaktadır.
- 5) **Genelleştirme:** Verilerin tanımlayıcı özelliğinin kasıtlı olarak azaltılmasıdır. 30 yaşında olduğu bilinen bir kişiyi 25 - 35 yaş arasında şeklinde değiştirmek örnek verilebilir.
- 6) **Yer değiştirme:** Sütunlarda sırasıyla yer alan verileri karıştırarak anonimleştirme çabasıdır. Örneğin, 30 yaşındaki Ömer ile 35 yaşındaki Mehmet’in verileri karıştırılarak Ömer 35, Mehmet ise 30 yaşında yer değiştirilerek anonimleştirilmektedir.
- 7) **Veri bozumu:** Orijinal verideki değerlerin yakın değerlerle değiştirilmesidir ve altıncı maddedeki gibi yer değiştirilmesidir.
- 8) **Sentetik veri:** Bu teknik, orijinal verilerden ayrı olarak doğrudan sentetik verilerin üretilmesiyle oluşmaktadır. Sentetik veriler orijinal veri kümesinden

türetilen istatistiklere dayalı oluşturulmaktadır. Günün belirli saat dilimlerinde okulda ortalama öğrenci sayısının türetilmesi bu tekniğe örnek gösterilebilir.

- 9) **Veri birleştirme:** Kayıt altına alınan bireysel verileri özetlenmiş değerlere dönüştürmektir. Bireysel verilerin gerekli olmadığı ve toplu verilerin amaç doğrultusunda yeterli olmasıyla ortaya çıkan tekniktir.

3.3.2. Veri Gizliliği ve Mahremiyet

“Söylediğim her sözün, yaptığım her şeyin, konuştuğum herkesin, yaratıcılığın, sevgilinin veya arkadaşlığa yönelik ifadelerin kaydedildiği bir dünyada yaşamak istemiyorum.”

Edward Snowden

Gözetim, kişisel verilere erişimi temsil ederken; mahremiyet, tam aksine kişisel verilere erişimin kısıtlanmasını içermektedir (Marx, 2015). Mahremiyet ve gizlilik hakkı, hammadde olarak gördüğü insan zekâsını, deneyimlerini ve iletişimi metalaştıran gözetim kapitalizminin egemen olduğu bir sistemde geri planda kalmakta, hatta yok sayılmaktadır. Mahremiyet, Georges Duby’nin ifadesiyle *“dokunulmazlık bölgesi”*dir (Lyon, 2018: 43). İnsan haklarının ayrılmaz bir parçası, modern devletlerde bireysel özgürlüklerin teminatıdır (Dolgun, 2015: 209). *“Yalnız kalma hakkı”*ndan, *“kendisi hakkındaki haberleşmeyi denetleme yeteneğine”* kadar çeşitli tanımlardan oluşmaktadır (Lyon, 2013: 250). *“Bir kimsenin kendi alanı, bölünmemiş özerkliğinin bölgesi”*dir. Bu alan dâhilinde kişi ne olduğuna, kim olduğuna karar verme gücüne sahiptir ve verdiği kararların tanınması ve saygıyla karşılanması için çaba gösterebilmektedir (Bauman - Lyon, 2018: 41). Mahremiyetin en önemli unsuru bireyin kendi bilgilerini denetleyebilmesi, akıbetine karar vermesi ve başkalarının kendisi hakkında hangi bilgilere sahip olduğunu bilme imkânına sahip olmasıdır (Lokke, 2018: 24). Günümüz dijital dünyasında ise mahremiyet, Zuboff’un (2019: 52) ifade ettiği gibi, *“kişinin nerede, nasıl ve ne zaman isterse istesin bilgi, iletişim ve diğer dijital ürünler gibi çok çeşitli ödüle sahip olması için ödemesi gereken bedel”* olarak görülmektedir.

Mahremiyet tarihsel kökenlere sahip bir kavram iken onunla dirsek teması içinde bulunan; mahremiyet ile birlikte kişisel verilerin korunmasında önemli bir yeri olan özel hayat kavramı görece daha yenidir. Özel hayata saygı hakkı daha önce bahsedildiği gibi 20. yüzyılın ortalarıyla birlikte yasal düzeyde koruma altına alınmaya başlamıştır. Kavramın kökü ise 1890 yılına dayanmaktadır. ABD’li iki avukat olan Samuel D. Warren ve Louis D. Brandeis (1890), özel hayat kavramını bir hak olarak ele alan ilk yazarlar olmuştur. Warren ve Brandeis mahremiyeti “yalnız bırakılma hakkı” olarak tanımlamış ve onu diğer tüm özgürlüklerin temeli olarak görmüşlerdir. Kaleme aldıkları “*Right to Privacy*” adlı eser, ilgili dönemde fotoğraf makinelerinin taşınabilir olması, gazetecilik ve medyanın gelişmesi ve faaliyetlerinin yaygınlaşması ile bireylerin kendi görüntüleri üzerindeki haklarına yer vermiştir (Has, 2021: 210).

20. yüzyılın ikinci yarısından itibaren izleme teknolojilerinin önemli ölçüde gelişimini sürdürmesi ve gerek ticari sektörün gerek devletin büyük bilgisayarları aktif biçimde kullanmaları mahremiyet kaygılarının kaynağı hâline gelmiştir. Jerry Rosenberg, 1969 yılında yayımlanan ve mahremiyetin sonunun geldiğini işaret ettiği “*Death of Privacy*” adlı kitabında şöyle demektedir: “*Bireyler ve örgütlerin birçok faaliyetini içeren bilgiyi, onlardan habersiz saklayacak, birleştirecek ve tek bir düğmeye dokunarak sınırsız erişim imkânına kavuşacak bir ulusal bilgisayar sistemi planlanıyor.*” Arthur R. Miller da 1971’de yayımladığı “*The Assault on Privacy*” adlı eserinde bilgisayarların veri işleme ve depolama kapasitesinin “*toplumu şeffaf bir dünyaya dönüştürecek bir izleme sisteminin kalbi olabilecek*” düzeyde olduğunu vurgulamıştır (Vincent, 2017: 179).

Helen Nissenbaum’un (2004) *bağımsal bütünlük olarak gizlilik* teorisine göre mahremiyet bilginin uygun formlarda paylaşımını gerektirir. Kişinin aile bireyleriyle paylaştığı bilgi ile üçüncü dereceden tanıdığı çevresiyle paylaştığı bilgi farklı kurallara tabi olur. Bu yönüyle hangi bilgiyi paylaşıp paylaşmayacağı kişinin içinde bulunduğu bağlama bağlıdır; paylaşım kişinin şahsi “mahremiyet” algısına ve talebine göre de değişebilir. Kısaca “*kişisel bilginin uygun şekilde akış hakkı*” olarak ifade edilir.

Büyük veri çağında kişisel veri, rıza ve mahremiyet arasındaki işbirliği ve çatışma yalnızca şimdiyi değil geleceği de içine alarak şiddetlenmektedir. Öncelikle

büyük veriyle birlikte verinin değeri yalnızca birincil amaçla değil ikincil amaçlara da bağlı olmaya başlamıştır. İkincil kullanım, şu anda mevcut yöntemleri içerebildiği gibi gelecekte olabilecek veya geliştirilebilecek yeni yöntemleri de kapsamaktadır (Mayer-Schönberger - Cukier, 2013: 160 - 162). Kişinin Google’da arama yapması Google’ın kişiyi daha iyi tanıyarak sağladığı hizmeti kişiselleştirmek ve Google’ın kendi arama hizmetini geliştirmek için kullanılabilir. Fakat bu arama sorgusunun veri tabanında saklanarak Google tarafından gelecekte başka bir amaçla da kullanılabileceği göz ardı edilemez. Bu durum açık rızanın alınmasına ilişkin iki problem yaratmaktadır: kullanıcıdan neyin rızasının alınacağını bilmeyen şirketler ne yapmalı? Neye rıza vermesi gerektiğini ve verisinin ne amaçla kullanıldığını bilmeyen kullanıcılar nasıl bilgilendirilmeli? Mayer-Schönberger ve Cukier, bu soruların cevabını ararken her bir büyük veri analizinde geriye dönüp kullanıcıdan izin almanın gerektiğini, fakat bunun teknik olarak olanaklı olsa bile maliyetinin yüksek olacağını vurgular. Yazarlar buna ek olarak iki farklı muhtemel çözümün de sorunlu olacağını altını çizer. Onlara göre verinin toplandığı anda kullanıcıdan her türlü kullanım için onay almak, rıza nosyonunun içini boşaltmaktadır. Bu sebeple toplu izin alma anlayışının mahremiyeti sekteye uğratacağı görüşünü savunmaktadırlar. Ayrıca teknik olarak mahremiyetin bir yolu olarak görülen anonimleştirmenin de birçok durumda etkisinin zayıflığına dikkat çekmektedirler. Zayıflığın nedeni ise büyük verinin “büyük” oluşundan kaynaklanmaktadır. Veri setlerinden doğum tarihi, kredi kartı numarası, isim, adres gibi kişisel veriler çıkartılsa bile büyük verinin miktar ve çeşitliliği ister istemez kimliğin saptanmasını kolaylaştırabilmektedir (a.e., s, 161).

Bugün tüm alanlarda aktif biçimde üretilen verilerin neredeyse hepsi kişisel bir bilgi kırıntısı içermektedir. Veri tek başına kişisel bilgi içermeyen bir “şey” gibi gözükse de büyük verinin sahip olduğu imkânlar neticesinde geriye doğru tarama yapılarak söz konusu verinin izi, içinden kişisel bilgi çıkana kadar sürülebilir. Bu bilgi gündelik hayatın içinden olabileceği gibi mahrem bilgiler de içerebilir (Mayer-Schönberger - Cukier, 2013: 159 - 160). Örneğin, bir evin elektrik tüketimi ele alalım. Günlük ortalama elektrik tüketim verisi tek başına sınırlı bir bilgi barındırmaktadır. Tüketim saat aralıklarına bölünmeye başladığında ev sahipleri hakkında daha çok ayrıntı ortaya çıkmaya başlar. Akşam yatma ve sabah kalkma rutinlerinden yoğun

elektrik kullanım periyodlarındaki su ısıtıcısı, bulaşık / çamaşır makinesi, fırın vb. yüksek enerjiyle çalışan aletlerin kullanım sıklığına kadar birden çok bilgi ortaya konulabilir. Bu bilgiler, sahip olunan başka bilgilerle birleştirilerek büyük bir anlam bütünlüğü oluşturulabilir.

Özel nitelikli verilerin üçüncü taraflara aktarılması veya satılması, kişinin mahremiyetine en çok zarar verecek unsurların başında yer almaktadır. Bazı araştırmalar ve detaylı incelemeler hassas verilerin, belki de platformun haberi bile olmadan, nasıl üçüncü taraflarca ele geçirildiğini göstermektedir. Privacy International (2021); BetterMe, VShred ve Noom gibi egzersiz ve diyet amaçlı web sitesi ve uygulamalarını incelemiş ve her birinin kullanıcılardan talep ettiği verileri üçüncü taraflarla nasıl paylaştığını ortaya koymuştur. BetterMe adlı uygulamada kullanıcının cinsiyet verisinin Google ve Facebook ile paylaşıldığı tespit edilmiştir. Diğer yandan Noom adlı uygulamanın kullanıcılardan topladığı tıbbi geçmiş, antibiyotik alıp almadığı, ailede diyabet hastası olup olmadığı gibi bilgileri FullStory adlı şirketle doğrudan paylaştığı görülmüştür. VShred'in ise kullanıcıların testlere verdiği cevapları URL yapısında gösterdiği belirlenmiştir (Örneğin, vshred.com/?cinsiyet=erkek&yas=35&kilo=obez). Bu verilerin Google, Pinterest ve Facebook'un yanı sıra birden fazla veri ve reklam şirketine aktarıldığı saptanmıştır. Benzer bir durum, eşcinseller için bir tanışma uygulaması olan Grindr'da yaşanmıştır. Grindr'ın, uygulamaya kayıt olurken topladığı kullanıcı verilerini üçüncü taraf şirketlerle paylaştığı ortaya çıkmıştır. Bu veriler arasında HIV-AIDS durumu, son HIV testi zamanı, cinsiyeti, konumu, vücut şekli, kilo, boy, e-posta, uygulama kullanım amacı, etnik kökeni, ilişki durumu ve tercih edilen cinsel pozisyon gibi hassas veriler yer almaktadır. Verilerin aktarıldığı üçüncü taraf şirketler arasında AdColony, Google, Smatoo, OpenX, AppsFlyer ve Mopub gibi birden çok reklam ve analitik şirketi tespit edilmiştir (SINTEF, 2018) . Norveç Veri Koruma Kurumu, Grindr'a 6,2 milyon euro ceza vermiştir (Myrstad, 2021).

Kişisel verilerin başka kurum ve şirketlerle paylaşılması veya satılması kullanıcı mahremiyetine yönelik kaygıları artırmaktadır. Konum verileri, tıpkı hassas veriler gibi bu kapsamda değerlendirilebilir. Web siteleri, mobil uygulamalar ve diğer

kaynaklardan toplanan konum verilerinin dünya çapındaki pazarı 12 milyar dolardır ve 2027 yılında 32 milyar dolar olması beklenmektedir (Grand View Research, 2020). Böylesine büyük bir pazarda çeşitli amaçlar doğrultusunda kullanıcıların konum verileri ve yer değiştirme rutinleri alınır satılır durumdadır. Örneğin, aile üyelerinin birbiriyle iletişime geçmesini ve konum paylaşmasını sağlayan Life360 adlı mobil uygulamanın kesin konum verilerini sattığı ortaya çıkmıştır. Özellikle, ebeveynlerin çocuklarının konumlarını takip etme amacıyla tercih ettiği uygulama konum verilerinin satışından 2016 yılında 693 bin dolar, 2020 yılında ise 16 milyon dolar gelir elde etmiştir (Keegan - Ng, 2021).

Verinin toplanma amacı dışında ikincil kullanımı ve sağlanan hizmet için ihtiyaç duyulandan daha fazla veri toplama işlemi mahremiyete yönelik kaygıları devlet kurumlarına da taşımıştır. ABD’li senatör Sherrod Brown’un gizlilik üzerine hazırladığı tasarı (Brown, 2020), kişisel verilerin talep edilen hizmet bağlamında kullanılması, gerekli olmayan “fazla” verilerin toplanmasının yasaklanmasını içermektedir. Bu tasarıyla bir kullanıcının internet üzerinden bir banka kartına başvurma verisi, pazarlama, satma vb. amaçlarla veri toplayan başka şirketlere gitmesinin engellenmesini önermiştir. Senatör Brown, silikon vadisi şirketlerinin her zaman yaptıkları gibi “yenilik yapmaları” gerektiğini ve iş modellerini “casusluk yapmayan” bir modele evirmelerinin gerekliliğine vurgu yapmıştır. Bu veri sömürsüne dayalı modeli şu ana kadar değiştirmemelerinin nedenini ise şu şekilde açıklar: *“Yapamadıkları için değil, denemedikleri için değiştirmediler.”*

Büyük veri yaşamların gözetim altında tutulmasına olanak tanırken anonimliğin koruması için sarf edilen çabaları da etkisiz hâle getirmektedir. Büyük verinin oluşturduğu tahminler insanları eylemlerinden değil eğilimlerinden yakalar ve söz konusu durum insan onuruna zarar vererek özgür iradeyi görmezden gelebilir (Mayer-Schönberger - Cukier, 2013: 177). 2017 yılında Avustralya’da yayımlanan *The Australian* adlı gazetenin ele geçirdiği 23 sayfalık Facebook raporu, platformun gençlerin kendilerini “değersiz” ve “güvensiz” hissettikleri ve “öзgüvene ihtiyaç duydukları” anları bilebilme kapasitesine sahip olduğunu göstermektedir. Facebook yöneticileri tarafından hazırlanan dâhili rapora göre platform Avustralyalı ve Yeni

Zelandalı gençlerin ne zaman “stresli”, “yenik”, “bunalmış”, “endişeli”, “gergin”, “işe yaramaz” ve “başarısız” hissettiklerini belirlemek için gönderileri, etkileşimleri ve fotoğrafları gerçek zamanlı olarak izlemektedir (Levin, 2017; The Australian, 2017). Sızan bu belgeye göre Facebook, gençlerin mevcut ruh halleri ve ruhsal değişimleri hakkında ayrıntılı veriler oluşturabilirken aynı zamanda onların ruh hallerini etkileyecek / manipüle edebilecek güce de sahiptir. Tüm bu gelişmeler insan onurunu inciten, mahremiyeti zedeleyen ve özgür iradeyi kendi çıkarları uğruna yönlendiren sonuçların doğmasına sebebiyet vermektedir.

Kişisel tanımlanabilir bilgiler (KTB), kişinin kimliğinin doğrudan veya dolaylı yollarla ortaya çıkarılmasını sağlayan bilgilerdir. Bireyi benzersiz şekilde tanımlamaktadır. Ad soyad, telefon numarası, kimlik numarası, sosyal güvenlik numarası, e-posta adresi, ev adresi gibi veriler KTB arasında yer almaktadır. KTB olmayan yüzlerce/binlerce kişisel veri kategorisinin neler olduğunun tespiti ise kullanıcı mahremiyetinin gerçek sınırlarının nereye uzandığını anlamakta kilit bir öneme sahiptir. González-Cabañas ve arkadaşları (2021) bu konuya odaklanarak derinlemesine bir Facebook analizi gerçekleştirmiştir. Araştırmacılar analizlerinde KTB olmayan öğeler olarak Facebook’un kullanıcılarının çevrim içi ve çevrim dışı aktivitelerine göre oluşturduğu ilgi alanlarını seçmiştir. Analiz sonucunda, Facebook’un bir kullanıcıyla eşleştirdiği ilgi alanlarından en nadir 4 veya 22 rastgele “ilgi alanı” kategorisinin bir kişiyi bizzat hedeflemede %90 oranında başarılı olduğu ortaya konmuştur. Diğer ifadeyle, Facebook’un kullanıcı davranışları dolayısıyla yarattığı binlerce ilgi alanı / veri kategorisinden en nadir 4 kategori veya rastgele seçilen 22 kategori reklam olarak hedeflendiğinde milyarlarca kullanıcı arasından tek kullanıcıyı hedefleme başarıları %90’dır. Dolayısıyla bir kişinin kim olduğunun ifşasında KTB birincil öneme sahipken, KTB olmayanlar da bir araya getirildiğinde KTB kadar etkili ve söz sahibidir. Bu sonuç çevrim içi mahremiyetin kilit unsuru olarak kabul edilen anonimliğin aslında ip üstünde olduğunun bir kanıtı niteliğindedir. Benzer bir başka çalışmada da anonim veri setleri içerisindeki insanları 15 demografik veri kategorisi kullanarak %99.98 başarı oranıyla yeniden tanımlayabilecekleri ortaya konulmuştur. Rocher ve arkadaşları (2019) modern veri setlerinin tıpkı daha önce bahsettiğimiz Oracle, Acxiom vb. şirketlerin sahip oldukları gibi yüzlerce hatta

binlerce kategoriden oluştuğunun altını çizmektedir. Yazarlar, veri şirketi Experian'ın Alteryx'e 120 milyon Amerikalı hakkında kişi başına 248 kategoriden / öznitelikten oluşan kimliksizleştirilmiş (anonimleştirilmiş) veri kümesine erişimi sattığını örnek vermiştir. Bu çerçevede 15 demografik veri kategorisinin kişiye atana yüzlerce veri arasında aslında çok da fazla olmamasına rağmen kişinin anonimliğini ortadan kaldırmada ne kadar güçlü olduğu gösterilmiştir.

3.3.3. Üçüncü Taraf İzlemeler

Web siteleri ve mobil uygulamaları ziyaret eden kullanıcılar bu platformları kullanırken girdikleri her etkileşim hem platform sahipleri tarafından doğrudan hem de platforma gömülü üçüncü taraflarca gözlenerek kayıt altına alınmaktadır. Üçüncü taraflar olarak tabir edilen kurum, kuruluş ve şirketler gerek çerezler gerekse farklı izleme teknolojileri yardımıyla başta kullanım verileri olmak üzere ziyaretçilerden birçok veri toplamakta; bu verileri genellikle analitik, reklam ve ölçüm amaçlarıyla kullanmaktadır.

Bireyler, davranış verilerinin çıkarılması için gereken hammadde kaynağı hâline gelmişken, gözetleyen ve hammaddeye el koyan şirketler bunu genellikle web sitelerine veya mobil uygulamalara yerleştirdikleri izleme yazılımları gerçekleştirir. Üçüncü taraf izlemelere ilişkin ilk araştırmalar 2000'li yılların ortalarına dayanmaktadır. Krishnarmurthy ve Wills (2009), en çok tercih edilen 10 üçüncü taraf sunucunun dönemin popüler web sitelerindeki etkisinin Ekim 2005'te %40 iken Eylül 2008'de %70'e yükseldiğini belirlemiştir. Aynı yazarların gerçekleştirdiği ve kişisel tanımlanabilir bilgilerin çevrim içi sosyal ağlar aracılığıyla üçüncü taraf sunuculara sızdırılıp sızdırılmadığı sorusuna ilişkin araştırması da bir hayli önemlidir. Krishnarmurthy ve Wills (2010), çevrim içi sosyal ağlardaki çoğu kullanıcının çevrim içi sosyal ağ kimlik bilgisiyle çerezlerin birbiriyle bağlantılı olmasına karşın savunmasız olduklarına dikkat çekmektedir. Çevrim içi sosyal ağ kaynaklı sızıntının istek URI'leri, HTTP yönlendirmeleri ve çerezler ile gerçekleştiğinin altını çizen yazarlar şu iki sonucun altını çizmektedir: (1) çevrim içi sosyal ağ çerezleri kendi dışındaki sitelerden de birkaç yıldır veri topladığından dolayı üçüncü taraf veri

toplayıcıları geçmiş ziyaretleri kullanarak kimliği ilişkilendirebilmektedir. (2) Çevrim içi sosyal ağlardaki kullanıcılar sosyal ağı veya dışındaki siteleri ziyaret etmeye devam ettikçe gelecekteki davranışları da sosyal ağ kimliğiyle bağlantılı olmaya devam edecektir.

Altawell, Good ve Hoofnagle (2015), kullanıcı gizliliği ve gözetimi üzerine yaptıkları araştırmada, en popüler 100 web sitesini ziyaret eden kullanıcıların bilgisayarından 6,000'den fazla çerez toplandığı ve bunun %83'ünün ziyaret edilen web sitesiyle ilişkisi olmayan üçüncü taraf kaynaklar olduğu tespit edilmiş. Çalışmada ayrıca Google izleme yazılımlarının ilk 100 sitenin 92'sinde ve ilk 1000 sitenin 923'ünde olduğu ortaya çıkarılmıştır. Web sitelerindeki üçüncü taraf izleme teknolojilerini açığa çıkaran bir tarayıcı eklentisi olan Ghostery'nin (2017) araştırmasında ise web sayfalarının %77,4'ünün kullanıcı hareketlerini başka şirket ve platformlarla paylaştığı saptanmıştır. Sitelerin %60'ı Google, %27'si Facebook izleme teknolojilerine sahiptir. Araştırmanın diğer bir önemli noktası ise analiz edilen sitelerin %15'inin özel nitelikli kişisel verileri (Din, ırk, cinsel eğilim vb.) on veya daha fazla izleyici operatörüyle paylaştığının ortaya çıkmasıdır. 2015'te yapılan benzer bir araştırmada benzer sonuçlar ortaya konmuştur. Timothy Libert'in web sitelerinin gizliliğe verdiği önem ve üçüncü taraf çerezler üzerine yaptığı araştırmada, en popüler bir milyon web sitesini analiz etmiş ve neredeyse her 10 web sitesinin 9'unun kullanıcı farkında olmadan onlar hakkında diğer taraflara veri sızdırdığını açığa çıkarmıştır. Bu web sitelerinin yüzde 78'inde üçüncü taraf olarak Google; yüzde 34'ünde ise Facebook'a veri gönderdiği tespit edilmiştir (Libert, 2015).

Özel nitelikli kişisel veriler üzerine Privacy International'ın (2019) yaptığı bir araştırmada, akıl sağlığıyla ilişkili web sitelerinin %98'inde üçüncü taraf izleme teknolojilerinin yer aldığı, bunların 4'te 3'ünün pazarlama amaçlı olduğu tespit edilmiştir. İncelemedeki önemli bulgulardan ikisi ise bazı sitelerdeki kullanıcı depresyon test verilerinin programatik reklam ile gerçek zamanlı açık arttırmaya çıkarılarak kullanılması ve kullanıcı siteye girdiğinde çerez politikasını kabul veya reddetmeden önce bile izleme faaliyetlerinin başlamasıdır. Bu araştırmalar, gözetimin

veri toplamanın rutinleştği anda gerçekleşmesinin yanı sıra sıradanlaştığı ve derinleştiğine de vurgu yapmaktadır.

Çerez teknolojisi üçüncü taraf izlemelerin büyük bir kısmına yardımcı olurken izleme pikselleri de yaygın olarak kullanılmakta ve kullanıcı verisi toplamaktadır. Fouad ve arkadaşları (2020) 8744 web sitesinde toplam 84658 web sayfasını tarayarak izleme piksellerinin webdeki hâkimiyeti ortaya koymuşlardır. Araştırmaya göre bu web sitelerinin %94,5'inin en az bir sayfasında görünmez tek piksellik bir görsel yer aldığı tespit edilmiştir.

Bazı web sitesi ve mobil uygulamalar, kullanıcılara çerez kullanımı için izni ekranı çıkarmasına rağmen kullanıcı henüz karar vermeden çerezleri cihazlarına yerleştirmektedir. Söz konusu durum hem etik hem de yasal bağlamda sorun doğurmaktadır. Matte ve arkadaşları (2020) IAB Avrupa'nın Şeffaflık ve Rıza Çerçevesi standartlarına uygun, rıza yönetim platformları tarafından oluşturulan çerez izin ara yüz tasarımlarının arkasındaki yasal ihlalleri gün yüzüne çıkaran bir araştırma gerçekleştirmiştir. Araştırmaya göre incelenen 1426 web sitesinin 141'i kullanıcı henüz bir onay vermeden arka planda çerezlerin kullanımına izin vermekte; 236'sı seçenekleri önceden belirleyerek kullanıcıları onaylamaya zorlamakta; 27'si ise kullanıcı açıkça izin vermese bile izin vermiş gibi çerezleri aktif hâle getirmektedir. Ayrıca incelenen web sitelerinin %54'ünde en az bir ihlal tespit ettikleri ifade edilmiştir. Araştırmacılar sonuç olarak Şeffaflık ve Rıza Çerçevesinin gizliliği önceleyen ve yasal düzenlemeleri uygulamaya koymaya yardımcı olan bir sistem olsa da etik açıdan iyileştirmeye ihtiyaç duyduğunun ve ihlallere yönelik aktif bir tepki geliştirmeleri gerektiğinin altını çizmektedir. Benzer bir araştırmayı çok daha geniş ölçekte Trevisan ve arkadaşları (2019) gerçekleştirmiştir. 35.000'den fazla web sitesinde tarama yapan araştırmacılar sitelerin neredeyse yarısının çerez kullanımıyla ilgili yasal düzenlemeleri ihlal ettiklerini; bu ihlallerin büyük bir kısmının ise Google, Facebook gibi büyük şirketlerin reklam izleyicilerinden kaynaklandığını saptamıştır.

Üçüncü taraf kütüphaneler ve ek yazılımlar, mobil uygulama geliştirme aşamalarında sıkça kullanılmaktadır. Yazılım geliştirme kiti (SDK), mobil uygulamaların programlanmasında kullanılan araç setleridir. Bir uygulamanın

çalışmasına yardımcı olan paketlerden oluşur. Örneğin, Apple ve Android yazılım geliştiricilere kendi işletim sistemleriyle uygun kitleri sunar ve uygulamanın kendi platformlarında çalışmasını sağlar. Aynı zamanda Facebook ve Google gibi platformlar da geliştiricilere kendi SDK'larını sunar. Mobil uygulamaya üye olmadan Facebook ile giriş yapmak için Facebook Giriş SDK'sı, Google ile giriş yapmak için Google Giriş SDK'si kullanılması gerekir. SDK'lar geliştiricilere kolaylık sağlaması bakımından faydalı olsa da platformların kullanıcı hareketlerini izlemesine olanak sağlar. Dolayısıyla uygulama içindeki kullanıcı davranışları genellikle sadece uygulamada kalmaz; sosyal ağ platformlarına, pazarlamacılara ve veri tüccarlarına veri satan üçüncü taraf kuruluşlarla da paylaşılır (Morrison, 2020)

Yale Privacy Lab'in kurucusu Sean O'Brien mobil uygulamalar ve SDK'ların bulunduğu ortak noktayı hız üzerinden anlamaya çalışır: *“Eğer yeni bir girişim (start-up) olsam, uygulamayı mağazaya hemen yüklemek isterim, zira oldukça hızlı olmam gerekir. Çeşitli SDK'ları bir araya getiririm, uygulamayı tamamlarım ve APP Store'a gönderirim.”* (Morrison, 2020). O'Brien'in ifadesindeki gibi genellikle zamanla yarışan ve işe odaklanan küçük ölçekli fakat potansiyelli şirketler, uygulamalarını hızla son kullanıcıya ulaştırmak ister. Bu süreçte mobil uygulamada üyelik sistemi yazmak yerine kullanıcı girişleri için Facebook, Google veya Twitter ile giriş yapma özelliği ekleyebilirler; bildirimler için Amazon SDK'sını kullanabilirler, anlık kullanıcı takibi için Firebase Crashlytics SDK'sını, reklam ve pazarlama için AdMob SDK'sını kullanabilirler. SDK'ların kendisi bir izleme aracı olmasa bile veri alışverişi sırasında uygulamadan ihtiyacından fazla veri toplayabilir ve saklayabilir.

3.3.4. Gizlilik Sözleşmeleri ile Gözetimin Sıradanlaşması

Gizlilik sözleşmeleri, bir kuruluşun veri toplama, kullanma ve ifşa etme uygulamalarını tanımlamak için hazırlanan belgelerden oluşmaktadır (Earp vd., 2005). Kullanıcı haklarının neler olduğunu ve haklarında toplanan verilerinin kullanımını kontrol etmek için hangi seçeneklere sahip olduklarını açıklayan ve kullanıcıyı güçlü kılan bilgiler içermektedir. Kişisel verilerin kullanımına yönelik sınırlar bu sözleşmelerde yer almaktadır. Bu sözleşmeler genellikle “hizmet kullanım koşulları”

sözleşmesinin içinde yer almaktadır ve site ile kullanıcı arasındaki ilişkiyi düzenleyen belgelerdir (Steinfeld, 2016). GDPR kapsamında veri sahipleri, yani kullanıcılar, gizlilik sözleşmelerinde dört soruya cevap bulabilmelidir: (1) Hangi veri hangi amaçla toplanıyor, (2) Toplanan veri nasıl işleniyor, (3) Ne kadar süreyle saklanıyor, (4) Verilerin silinmesi için kiminle iletişime geçilmeli? Bu soruların cevapları sözleşmelerde açık, net ve kolaylıkla erişilebilir olmalıdır.

Gizlilik politikaları, aydınlatma metinleri, kullanıcı sözleşmeleri ve hizmet koşulları gibi yasal belgeler, özel olarak kullanıcının bilgisi veya rızası olmadan kurum tarafından herhangi bir zamanda tek taraflı olarak değişime uğrayabilmektedir. Onlarca sayfadan oluşan kâğıt sözleşmeler müşterilerin ıslak imzasına ihtiyaç duyarken; tam aksine, bu tür sözleşmeler önemsiz birer metinler dizisi muamelesi görmektedir. Zuboff (2019: 49), önemsiz olarak nitelediği bu sözleşmelerin hiçbir masrafa girmeden genişletilebildiğine, çoğaltılabildiğine, kısaltılabildiğine, değiştirilebildiğine ve yeniden üretililebildiğine dikkat çekmektedir. Genellikle hizmet koşullarına ilişkin sorumluluk almadan ve belirtmeden ortaklar, tedarikçiler, pazarlamacılar, reklam araçları vb. diğer şirketleri de içerir. Bu sözleşmeler, kullanıcıyı galip gelemeyeceği bir sonsuz gerilemeye¹⁶ zorlamakta ve hukuk profesörü *Nancy Kim* tarafından “sadistçe” olarak tanımlanmaktadır.

En çok ziyaret edilen 100 web sitesinden 45’inin gizlilik sözleşmelerini inceleyen Steinfeld (2016), ortalama 2400 kelimeden oluşan sözleşmelerin yalnızca 7’sinde kayıtlı kullanıcıları bilgilendirmeden sözleşme metnlerinin değiştirilemeyeceği, 18’inde ise şirket tarafından gelecekte yapılacak sözleşme değişikliklerinin tüm kayıtlı kullanıcıları bağlamaya devam edeceği belirtilmiştir. Diğer bir ifadeyle, sözleşmelerin büyük çoğunluğu kullanıcılara haber vermeden sözleşmeye yeni maddeler ekleyebilecek veya madde silebilecek hakka sahip düzenlemeler içermektedir. Öte yandan, sözleşmelerin 35’i şirketlerin “hizmet iyileştirmesi” için, 23’ü şirketin kullanıcılar hakkında topladığı verileri reklam

¹⁶ Ing: Infinite regress. Her bir ögenin başka birini ürettiği sonsuz bir döngüdür. Mevcut inançların nedenlerinin nedenlerini irdelerek her birinin diğerine yol açtığı bir dizi ilişkili nedenler biçimidir (Cameron, 2018).

amacıyla, 18'i arařtırmalarda kullanılmak üzere üçüncü taraflarla paylaşmasına olanak tanımaktadır. Yalnızca 7 sözleşme kullanıcılara kişisel verilerinin üçüncü taraflarla paylaşılmasına itiraz etme hakkından söz etmekte, 9'u kullanıcıların itiraz hakkının olmadığını belirtmekte, geri kalan 29'u ise böyle bir haktan hiçbir seçenekte bahsetmemiştir. Arařtırma sonucu göstermektedir ki řirketler kadar kullanıcıları da koruması gereken yasal sözleşmelerin çoğu veri toplama ve işleme bağlamında yalnızca řirketlerin çıkarlarını korumak için hazırlanan metinlerden oluşmaktadır. Bu metinler kullanıcı gözetimini normalleřtiren unsurların oluşmasına katkı sağlamaktadır.

Gözetim süreçleri, gizlilik politikaları ve kullanıcı sözleşmelerinin arka sayfalarında küçük harflerle yer alır, bu nedenle izleme faaliyetleri neredeyse tüm kullanıcılar için görünmezdir (Tanner, 2014: 162). Litman-Navarro (2019), en sık kullanılan yaklaşık 150 web sitesi ve mobil uygulamanın gizlilik sözleşmelerini inceleyerek metinlerin okunma sürelerini ve anlaşılma zorluklarını içeren bir arařtırma gerçekleřtirmiştir. Bu arařtırmaya göre Google, Facebook, Twitter, Apple, Instagram, Spotify, Tumblr, Netflix ve WhatsApp gibi řirket ve uygulamaların gizlilik sözleşmeleri lisans eğitimi alan bireylerin anlama becerileriyle eşdeğerdir. Arařtırmada okunması en uzun süren web sitesi 35 dakika ile Airbnb, anlaşılması en zor ise Çinli arama motoru Baidu ve CNN olduğu belirlenmiştir. Arařtırma kapsamında en yalın dille yazılmış ve en kısa metne sahip gizlilik sözleşmesinin BBC'ye ait olduğu paylaşılmıştır.

Gizlilik politikaları ve hizmet kullanım koşullarıyla ilgili kullanıcı kaynaklı bir sorun olarak sözleşmelerin okunmaması karşımıza çıkmaktadır. Kullanıcıların bu sözleşmeleri genellikle okumadığı ve hakkında toplanan verilerin nasıl toplandığını, nerede saklandığını ve kimlerle paylaşıldığını bilmedikleri söylenmektedir. 2004 yılında ABD'de iki binden fazla katılımcıyla yapılan bir arařtırma, kullanıcıların gizlilik politikalarındaki dili çok fazla hukuki bulduklarını, dolayısıyla anlaşılması zor olduğu için metinleri okumadıkları tespit edilmiştir (Milne - Culnan, 2004). 2019'da 150 web sitesi analiz edilerek yapılan arařtırmada ise, web siteleri kullanıcılarına gizlilik bağlamında veri gözetim kanallarını reddetme şansını sunmasına rağmen bunu

nasıl yapacaklarına ilişkin oldukça karışık yollar ortaya çıkarmaktadır (Habib vd., 2019). Diğer ifadeyle, kullanıcılar web sitelerindeki gizlilik ayarlarını bularak zorunlu olmayan çerez ve izleme teknolojilerini devre dışı bırakmakta oldukça zorlanmaktadır. Sözleşmelerin anlaşılmasının zor ve dolambaçlı yollara sahip olmasının bir nedeni vardır; bunlar kullanıcıyı değil büyük teknoloji şirketlerini korumak için tasarlanmıştır (Brown, 2020).

Bir başka araştırma tıklama temelli sözleşmeler üzerine yapılmıştır. Hukukçular hizmet kullanım sözleşmelerini genellikle “onaylama sözleşmeleri” olarak tanımlarlar. Çünkü bu metinler kullanıcılar beğense de beğenmese de “kabul et veya terk et” anlayışıyla dayatma üzerine inşa edilmiştir (Zuboff, 2019: 48). Tıklama sözleşmeleri de bu tür sözleşmelerdir. Tıklama sözleşmeleri, çevrim içi tüm faaliyetlerde kullanıcıların karşısına çıkan ve tek bir hareketle “kabul ediyorum” seçeneğinin tıklanmasıyla yürürlüğe giren yasal düzenlemelerdir. Bir program indirilirken, yüklenirken veya web sitesi ziyareti sırasında kullanım koşullarının belirttiği alanlarda yaygın olarak kullanılmaktadır. Plaut ve Bartlett (2012), yaptıkları araştırmada tıklama sözleşmelerinin okunmamasının sözleşmelerin çok uzun olması, zaman kaybı olarak görülmesi, hepsinin aynı şeyleri söylemesi ve kabul etmekten başka bir seçenek olmaması gibi nedenlere bağlı olarak geliştiğini tespit etmiştir.

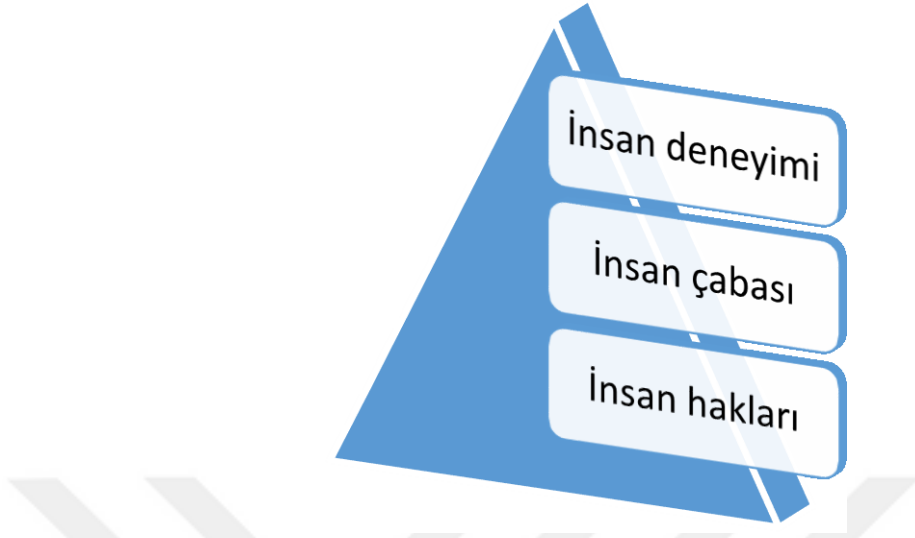
İster bir ütü ister bir termostat isterse bir buzdolabı olsun, bugün ağa bağlanan her cihaz artık hizmet kullanım koşulları ve gizlilik sözleşmesi gibi yasal metinleri de beraberinde getirmektedir (Goodman, 11 Mart 2015). Tüm bu sözleşmelerin oluşturulmasının temel dayanağı yasal zeminde toplanan ve paylaşılan verilerin meşruluğunu sağlamak ve doğrudan kullanıcıların verilerine erişmek için izin almaktadır. Noto La Diega ve Walden (2016), nesnelerin interneti araçlarının hizmet sözleşmelerini Google’ın akıllı ev aletlerini sistemlerini içeren Google Nest ürünleri örneği üzerinden incelemiştir. Nest ürünleri ile müşterilerin mobil cihaz ve uygulamaları ve Google sunucuları arasındaki veri paylaşımına ilişkin yasal metinlerden çıkardıkları bulgular gözetimin normalleşmesi açısından kayda değer bir öneme sahiptir. Örneğin sözleşmede *“bu bilgiler belirli üçüncü taraf ürün ve hizmetlerle paylaşıldığında, onlar tarafından bilgilerin kullanımı Nest’in gizlilik*

sözleşmesine değil, üçüncü tarafın gizlilik sözleşmesine tabi olacağı” metni yer almaktadır. Yazarlara göre bu cümle belirsiz ve geniş bir evrene atıfta bulunmaktadır. Zira bu yolla eline veri geçen ve veriyi paylaşan hiçbir şirket verinin ne olduğuna veya olacağına ilişkin bir sorumluluk almamaktadır. Nest, kullanıcıların istedikleri zaman veri paylaşımını durdurabileceklerini söylese de üçüncü taraflarla veri alışverişine izin verilmediği takdirde Nest hizmetinden düzgün olarak yararlanamayacaklarını ve yeni yazılım güncellemelerinden mahrum kalacaklarını belirtmektedir.

3. 4. Etik Web Tasarım ve Geliştirme

Etik iletişim, yanıltıcı / yönlendirici iletilerden arınmış, doğru bilginin aktarılmasıyla oluşan bir süreçtir. Etik tasarım ve yazılım geliştirme anlayışı, gerek görsel gerek yazılım gerekse proje mimarisi olarak söz konusu iletişimin sağlanmasında katkı sağlayacak olmazsa olmaz bir unsurdur. Etik web tasarım ve geliştirmenin merkezinde kullanıcıya saygı yer almaktadır. Harris (2009), kamu yararını içeren dört etik web tasarım prensibi önermektedir: (1) bilgi gizlenmemeli, rahatça erişilebilir olmalı; (2) bilgi uygun izin alınmadan kullanılmamalı ve başkalarıyla paylaşılmamalı; (3) Onay, uygun ve açık bir rıza ile alınmalı; (4) gizlilik korunmalıdır. Prensipler, doğrudan kullanıcıya saygıyla ilişkilidir.

Aral Balkan ve Laura Kalbag’ın (2015) kurduğu ve dijital çağda sosyal adaletin sağlanmasını misyon edinmiş bir girişim olan *Ind.ie*, etik tasarımın temelini “İhtiyaçların etik hiyerarşisi” piramidiyle üç basamakta açıklamaktadır:



Grafik 3.1: İhtiyaçların Etik Hiyerarşisi (Aral - Kalbag, 2015).

- a) **İnsan deneyimine saygı:** İnsan deneyimine saygı duyan teknoloji önemlidir ve kişiye keyif verir. Arka planda çalışır, sadece işinizi görür. Size destek olur ve hayatınızı daha iyi hâle getirir.
- b) **İnsan çabasına saygı:** İnsan çabalarına saygı duyan teknoloji, işlevsel, kullanışlı ve güvenilirdir. Düşünceli ve uzlaşmacıdır. Kibirli ve talepkâr değildir.
- c) **İnsan haklarına saygı:** İnsan haklarına saygı duyan, uçtan uca şifreli, açık kaynak kodlu, özgür, sürdürülebilir, uyumlu bir teknoloji olmalıdır. Sivil özgürlere saygı duyar ve korur, eşitsizliği azaltır; demokrasiye katkı sağlar.

Piramitte verildiği üzere bir üstteki katman bir alttakine dayanmaktadır ve herhangi biri zarar gördüğünde bir üstteki bundan etkilenme tehlikesiyle karşılaşacaktır. Diğer ifadeyle, insan haklarına saygı duymayan bir tasarım anlayışının ne insan emeğine ne de insan deneyimine saygı duyması ve etik olması söz konusu değildir.

O'Shea (2021: 25), teknolojik ilerlemenin, çoğunlukla insanlardan habersiz olarak onlar hakkında mahrem bilgiler edinmek ve en derinlere inerek kişinin ruhsal olarak ana hattını çıkarmak amacıyla kullanıldığının üstünde durmaktadır. O'Shea'nın

paylaştığı ve çekirdeğinde gözetim kapitalizmi mantığının yer aldığı mevcut tablo her ne kadar iç karartıcı olsa da teknolojinin “iyi” kullanımına ve etik web’e ilişkin çözüm önerileri geliştirilmiştir. Beard ve Longstaff (2019), etik tasarım ve iyi teknolojinin temellerini sekiz ilke ile açıklamaktadır:

- 1) **–ebilme’den önce –meli:** Etik tasarım, yapılan işin mümkün olan en iyiyi yaratmasına yardımcı olmakla ilgilidir. İnşa edilecek şeyin yapılıp yapılmayacağını bilmeden önce onun neden inşa edildiğini idrak etmek gerekir. Bu nedenle bir şeyi yapabiliyor olmak, yapılması gerektiği anlamına gelmez.
- 2) **Araçsal olmayan:** Bazı şeyler ölçülemeyecek ve fayda-değer ilişkisine indirgenemeyecek derecede önemlidir. İnsanlar, bir makinenin veya tasarım sisteminin parçası değil, tasarımdan yararlananlar olmalıdır.
- 3) **Hür irade:** Teknoloji, insan iradesinin bir uzantısıdır ve insanın özgürlüğüne müdahalede bulunmaması gerekir. İnsanların teknolojiyle ilişki kurma ve yaşama biçimleri konusunda özgür seçim yapabilecekleri tasarımlar yapılmalıdır.
- 4) **Sorumluluk:** Teknoloji genellikle belirli bir amaç doğrultusunda tasarlanır. Kullanıcılar amacın dışında kullandığında ise bazı sorunlar ortaya çıkabilir. Bu nedenle kullanıma ilişkin tüm olası senaryolar düşünülmeli ve ona göre tasarım yapılmalıdır.
- 5) **Net fayda:** Üretilen şeyler dünyaya pozitif bir katkı sağlamalı ve onu daha iyi bir hâle getirmelidir. Etik tasarım, yalnızca pozitif katkı sunmasının yanında olumsuz etkileri de mümkün olduğu kadar azaltmaya yardımcı olmalıdır.
- 6) **Adalet:** Teknolojik tasarımların önyargı içermemesi gerekir. Din, dil, ırk gibi hassas bilgilere göre farklı davranışlar sergilenmesi adalet ve eşitlik ilkesini zedeleyecektir. Çevrim içi dijital yüz tanıma sistemlerinde siyahilerden ziyade ilk önce beyazların daha hızlı tanımlanması eşitsizlik çerçevesinde örnek verilebilir.
- 7) **Erişilebilirlik:** Belirli bir grup hedeflendiğinde, diğer gruplar dışlanma riskiyle karşı karşıya kalır. Tasarım, en düşük teknoloji okur-yazarlık seviyesine sahip kullanıcılara da erişebilmelidir.

- 8) **Amaç:** Tasarım, kullanıcıların karşılaştığı bir sorunu çözmek üzere bir vaat taşımaktadır. İyi bir tasarım dürüst, açık ve amaca uygun olmalı; vadettiği etik çerçevede verimli şekilde gerçekleştirmelidir.

Beard ve Longstaff'ın etik teknoloji tasarlarken göz önünde bulundurulması gereken temel ilkeleri paylaştığı bu sekiz madde, etik açıdan ortaya çıkacak potansiyel krizleri önlemede ve tüm çevrim içi ağları ve işleyiş yapılarını etik açıdan iyileştirmede oldukça değerli bilgiler içermektedir. Bu maddelerin hepsi yalnızca görsel bir tasarımı değil; web sitelerinin, algoritmaların, makine öğreniminin, araçsal akıl mantığıyla toplanan kişisel verilerin ve tabi ki gözetim kapitalizminin tasarım mantığını da içermektedir. Dolayısıyla her bir madde irdelendiğinde şirketler, kullanıcılar, iletişim, veri ve veri toplanma yöntemleri arasındaki ilişkinin nasıl olması gerektiğine dair ipuçları taşıdığı görülmektedir. Örneğin, birinci madde kullanıcı verilerini “yalnızca toplayabiliyor olduğu için toplayan” ve onu sermaye birikim kaynağı olarak gören şirket ve platformların etik açıdan nasıl sınıfta kaldığını göstermektedir. Keza aynı şekilde fayda-değer ilişkisi, özgür irade, amaca uygunluk, pozitif etki sağlama ve adil olma gerekliliği üzerine yapılan vurgular gözetim kapitalizmine ait bütün unsurların yalnızca yasal değil aynı zamanda etik sorgulamadan da geçerken ne kadar zayıf olduğunu düşündürmektedir.

Avrupa Dijital Hakları Ağı'nın (EDRi) hazırladığı *Etik Web Sitesi Geliştirme ve Bakım Kılavuzu* web sitesi geliştirenlerin kullanıcı mahremiyetine değer vermek için nasıl bir yol izlemeleri gerektiği ve buna ilişkin hangi alternatif teknolojilerden yararlanabilecekleri üzerine bilgiler içermektedir (EDRi, 2020). Raporda, etik bir web'in inşası için ilk etapta üçüncü taraf yazılımlarla ilişkinin azaltılması gerektiği vurgulanmaktadır. Buna göre web geliştiricileri öncelikle tüm dosyalarını kendi sunucu (hosting) hizmetlerinde tutmalıdır. Diğer bir deyişle, görseller, videolar, ses dosyaları, JavaScript kodları, CSS dosyaları, yazı karakterleri ve çerezler gibi tüm dosyalar web sitesinin bulundurulduğu sunucuda yer almalıdır.

Birçok web sitesi ve mobil uygulama kısıtlı zaman, bütçe yetersizliği vb. nedenlerden dolayı bazı hizmetleri harici kaynaklar vasıtasıyla web sitelerine entegre etmektedir. Geliştiricilerin ücretsiz olarak temin ettiği bu hizmetler kullanıcı tarafında

birer üçüncü taraf yazılımlardır. Örneklendirirsek, geliştiriciler sitelerinde ikon kullanmak için *Font Awesome*, farklı yazı karakterleri için *Google Fonts*, harita için *Google Maps / Yandex Maps*, video için *YouTube / Vimeo*, hızlıca kullanıcı kaydı oluşturmak için *Facebook API / Google API*, sosyal ağlarda paylaşma butonları için *AddThis*, spam iletilerden korunmak için *Google Recaptcha* ve web sitesi ziyaret analizlerini görüntülemek için *Yandex Metrica / Google Analytics* gibi sistem ve yazılımları üçüncü taraf olarak web sitelerine eklemektedir. Harici çağırılan bu yazılımlar geliştiriciye sağladığı ücretsiz hizmetler dışında kullanıcıların web sitesi kullanım verilerini toplayabilmektedir. Kurum hazırladığı kılavuzda sunucuda tutulabilecek dosyaların sunucuda tutulmasını, harici çağırılacak yazılımların ise mahremiyet öncelikli alternatiflerinin tercih edilmesini önermektedir.

3.4.1. Yönlendirici Tasarımlar: Çerez Onay Kutu Tasarımları ve Açık Rızaya Etkileri

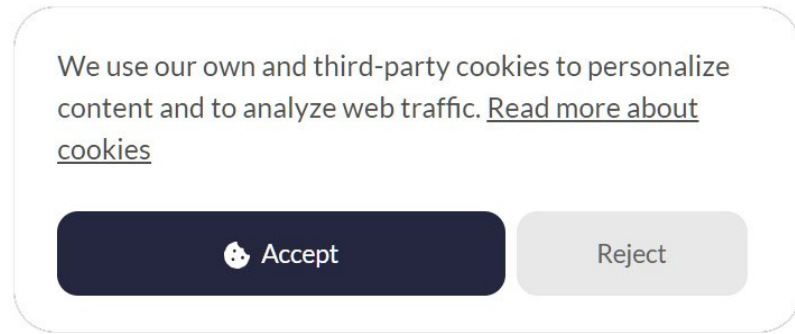
Tasarım, mahremiyet algısını şekillendirme gücüne sahiptir. Bu güç bireylerin teknolojiyi nasıl kullandığını ve ona nasıl yanıt verdiğini de şekillendirmektedir (Hartzog, 2018: 36). Bugün bireyler tıpkı sosyal hayatlarında olduğu gibi çevrim içi oldukları her an çeşitli mesajlarla bir şeylere inandırılmaya çalışılmakta ve bir şeyleri satın almaya teşvik edilmektedir. Çevrim içi ortamda ikna etme temelli bu süreçler kullanıcıların genellikle görsel olarak karşısına çıkmaktadır. İkna edici tasarımlar, “insanları tıklamaya, satın almaya, kaydolmaya veya ziyaret edilen web sitesinin birincil hedefi olarak kabul edilen herhangi bir eyleme motive etmek ve yönlendirmek için tasarlanmış mekanizmalar” olarak tanımlanmaktadır (Falbe vd., 2020: 34).

Kullanıcıda istenen davranışı yaptırmaya yönelik tasarımlar kendisini çerez onay kutularının tasarımlarında göstermektedir. Çevrim içi platformların kullanıcıların cihazlarına çerez yerleştirmek ve onların davranışlarını izlemek için izin istedikleri bu kutular hem farklı tasarım mantıklarına hem de çeşitli kelime oyunlarına sahiptir. Çekin (2021), *Çerezler ve Açık Rıza Bağlamında Güncel Gelişmeler* başlıklı sunumunda çevrim içi platformların kullanıcıların açık rızasını almaya yönelik çalışmalarını “Nudging” ve “Dark Patterns (Karanlık Desenler)” kavramlarına yer

vererek açıklamaktadır. Bu kavramlar başta çerez onay kutusu tasarımları olmak üzere web'in hâkim tasarım anlayışını ve etik web tasarımı algılamada yardımcı kavramlar olarak karşımıza çıkmaktadır.

Nudging kavramı ekonomi profesörü Richard Thaler ve hukuk profesörü Cass Sunstein tarafından ortaya atılmıştır. Bu teknik, profesörlerin seçim mimarisi olarak adlandırdıkları şey aracılığıyla insanların hayatını iyileştirmek için tasarımdan yararlanmaktadır. Seçim mimarları ise tasarımcılar ve mühendislerdir (Hartzog, 2018: 35). İngilizce kelime anlamında olduğu gibi, *kişiyi kibar bir biçimde bir şey yapmaya yönlendirmek* şeklinde tanımlanabilmektedir. Farklı açıdan bakıldığında “*kişinin tercihlerini çalmanın uysal bir yolu*” olarak da ifade edilebilir (Zheng, 2018). Bu özelliği onu *daha yumuşak bir karanlık desen* olarak kabul etmemize yardımcı olmaktadır.

Nudging tekniğinin kullanıcıların karar verme aşamasındaki etkisi yadsınamaz (Utz vd., 2019). Bu teknikle kullanıcının açık rızasının nasıl alındığına yönelik bir örnek şekil 3.1’de verilmiştir. Görüldüğü üzere kullanıcının onayını almak için “Kabul Et” butonunu renkli ve daha büyük; “Reddet” butonunu ise daha geri planda ve silik bir renk tonuyla tasarlanmıştır.

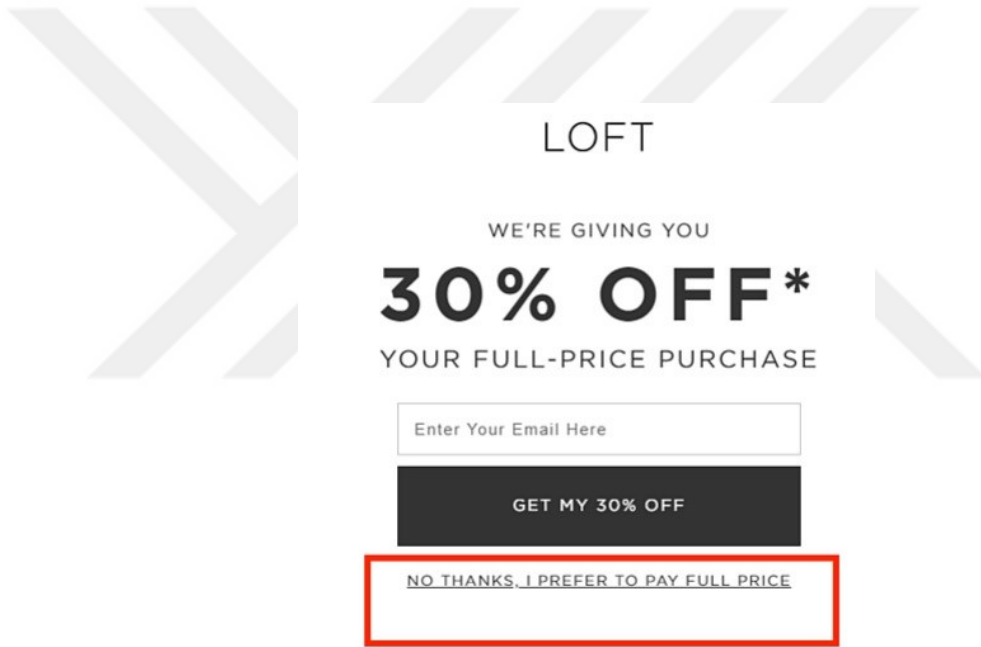


Şekil 3.1: Nudging Tekniğiyle Tasarlanmış Bir Açık Rıza Onay Kutusu.

Bir diğer kavram olan karanlık desenler, *bilinçaltı yöntemlerin kullanıldığı yönlendirme tekniği* olarak kabul edilmektedir. Kullanıcı deneyimi tasarımcısı Dr. Harry Brignull tarafından ortaya atılan terim, kullanıcıların istenmeyen bir şey

yapmasını sağlamak için oluşturulan ve kasıt içeren yanıltıcı tasarım desenleridir (Falbe vd., 2020: 46).

Karanlık desen yöntemi başta e-ticaret siteleri olmak üzere pratikte birçok alanda karşımıza çıkmaktadır. Örneğin, şekil 3.2’de görüldüğü üzere bir e-ticaret sitesi e-posta adresinin girilmesi şartıyla %30 indirim vadetmektedir. Hemen altında, e-posta adresini girmek istemeyen kullanıcıların tıklamasını gerektiren bağlantıda yer alan ifade ise kişiyi etkilemek ve bilinçaltını harekete geçirerek alışveriş yapmayacak olsa bile e-posta adresini girmesini sağlamak üzere yazılmıştır.



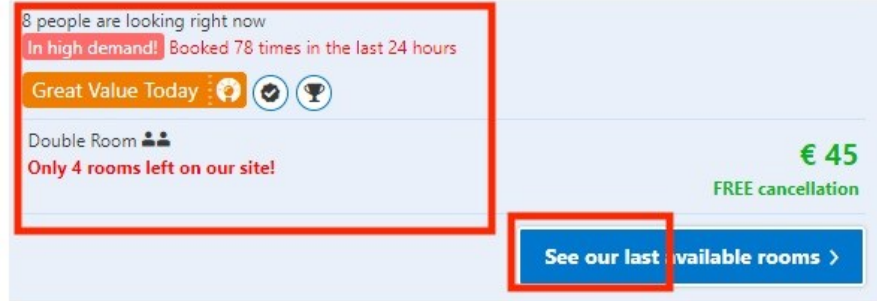
Şekil 3.2: Karanlık Desen Örneği.

Karanlık desenlere yönelik bir başka örnek sayaçlar ve zaman üzerinden verilebilmektedir. Şekil 3.3’te, bir e-ticaret sitesinde yer alan pop-up’ta kullanıcıya belirli bir süre tanınarak o süre zarfında alışveriş yaparsa indirimden yararlanabileceği sunulmaktadır. Kullanıcı, herhangi bir şey almak üzere web sitesini ziyaret etmemiş olsa bile karşısına çıkan indirimın sayaca bağlı olması kişinin alışveriş yapma isteğini tetikleyebilmektedir. Şekil 3.4’te yer verilen son örnekte bir hotel sitesinde oda rezervasyonu sırasında çeşitli alanlarda bulunan ifadeler karanlık desenleri anlamada önem teşkil etmektedir. “Şu kadar saat içinde şu kadar kişi gördü”, “yüksek talep”,

“sadece şu kadar oda kaldı”, “son kalan odaya hemen rezervasyon yap” gibi ifadeler bilinçaltını harekete geçirerek kişide arzulanan davranışın sergilenmesini sağlamada kilit rol oynamaktadır.



Şekil 3.3: Karanlık Desen Örneği.



Şekil 3.4: Karanlık Desen Örneği.

Karanlık desenler, 2018 yılında AB ülkelerinde GDPR’nin yürürlüğe girmesiyle kendisini web sitelerinde çerez izin bildirimleri ve açık rıza onay kutularında sıkça göstermiştir. Söz konusu izin talebi bilindiği üzere birinci taraf zorunlu çerezler dışında kalan çerezlerin cihaza yerleştirilmesi için kullanıcının açık rızasını almak amacını taşımaktadır. Çerez izin talebinin istenmesine ilişkin yasal metnin ve tüm alana ait tasarımın kullanıcının özgür iradesini etkilememesi gerekmektedir. Kullanıcılar ne için izin istendiğini kolayca anlayabilmeli ve bu izni herhangi bir görsel / algısal yönlendirme olmadan verme veya vermeme özgürlüğüne

sahip olmalıdır. Şekil 3.5’te verilen çerez izin kutusu tasarımı söz konusu hür iradeyi algısal bağlamda etkilemesi bakımından kötü bir örnek olarak değerlendirilebilir.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

Çihazınız hakkında bilgileri veya siteyi kullandığınız şekilde çalışmasını üzere kullanılmaktadır. Bilgiler çoğunlukla sizi doğrudan tanımlamaz ancak size daha kişiselleştirilmiş bir web deneyimi sunabilir. Bazı tanımlama bilgisi türlerine izin vermemeyi seçebilirsiniz. Daha fazla bilgi edinmek ve varsayılan ayarlarımızı değiştirmek için farklı kategori başlıklarına tıklayın. Bununla birlikte, bazı tanımlama bilgisi türlerini engellediğinizde site deneyiminiz ve sunabildiğimiz hizmetler bu durumdan etkilenebilir.

Onay Tercihlerini Yönet

+ Zorunlu Tanımlama Bilgileri	Her Zaman Etkin
+ Performans Tanımlama Bilgileri	☒
+ İşlevsel Tanımlama Bilgileri	☒
+ Hedefleme Amaçlı Tanımlama Bilgileri	☒
+ Sosyal Medya Tanımlama Bilgileri	☒

Seçimlerimi Onayla

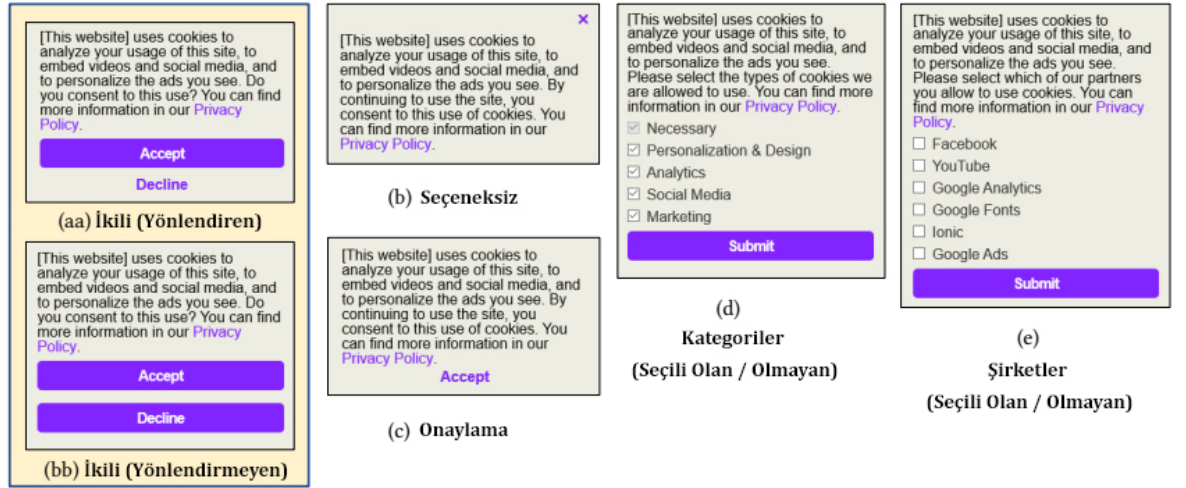
Powered by **OneTrust**

Şekil 3.5: Hurriyet.com.tr Adresinde Rıza Onay Kutusunda Yer Alan Seçenekler Aktif Olarak Kullanıcıya Sunulması.
(ekran görüntüsü tarihi: 15 Kasım 2021)

Çevrimiçi platformlar kullanıcılara verilerinin nasıl kullanılacağına ve bu verilerin nasıl yönetileceğine dair nadiren bir tercih sunar; bu nedenle “rıza” kavramı bu işleyiş içerisinde anlamını yitirmektedir (O’Shea, 2021: 25). Rıza almak, olması gerektiği için geçirtilerek olan, ana amacın yanında sorulmak için sorulan bir formalite hâline dönüşmektedir. Açık rıza onay kutusunda seçili gelen çerez kategorileri bu formalitenin oluşmasına zemin hazırlarken aynı zamanda karanlık

desen bağlamında da önemli bir örnek teşkil etmektedir. Şekil 3.5'te de örneği bulunan bu yöntemin kullanımının etik olmaması kadar yasal zeminde de problemli olduğu söylenebilmektedir. Bu problem Planet49 davası olarak bilinen davada ele alınmış ve neticelenmiştir. Davaya ilişkin Avrupa Adalet Divanı'nın (CJEU) 1 Ekim 2019'da yayımlanan kararında, önceden işaretlenerek sunulan onay kutularının kullanıcıların açık rıza verdiği anlamına gelmediği ve kullanıcıların aktif bir davranış sergileyerek kendilerinin onaylaması ve kabul etmesi gerektiği belirtilmiştir (InfoCuria Case-law, 2019). Karar, GDPR'ın yürürlüğe girmesi sonrasında web sitelerinin çerez ve izleme faaliyetleri ile ilgili izin ve onay süreçleriyle ilgili verilen ilk karardır. Dava sonucunda olduğu gibi kullanıcılara seçili hâle sunulan tüm işlemler açık rıza nosyonunu karşılamamaktadır.

Web siteleri, sosyal ağ platformları ve mobil uygulamalar kullanıcıların rızalarını farklı tasarım, yöntem ve tekniklerle almaya çalışmaktadır. Şekil 3.6'da çerez onay kutularının kullanıcılara farklı yöntemlerle nasıl sunulduğuna dair bir örnek yer almaktadır.



Şekil 3.6: Web Sitelerinin Çerez Onay Kutularına Ait Farklı Tasarım ve Rıza Talep Örnekleri. Kaynak: (Utz vd., 2019).

Utz ve arkadaşları (2019), GDPR sonrası rıza talep bildirimlerinin web sitelerinde nasıl değiştiğine yönelik bir çalışma yürütmüş ve bu sitelerin sahip olduğu çerez onay kutularını şekil 3.6'daki gibi sınıflandırmıştır. Bu sınıflama, internette

karşılaşılan birçok onay kutusunun sistematik bir düzen içinde gösterimi ve tanımlanması bakımından oldukça değerlidir. Buna göre onay kutuları beşe ayrılmaktadır:

a) İkili Tercihler:

aa. *İkili (Yönlendiren)*: Manipülatif tekniklerin uygulandığı, kontrast bir renk ile *Kabul Et* seçeneğinin öne çıkarıldığı onay kutusu.

ba. *İkili (Yönlendirmeyen)*: *Kabul Et* ve *Reddet* seçeneklerinden herhangi birinin görsel olarak öne çıkarılmadığı onay kutusu.

b) **Seçeneksiz**: Rıza almak için herhangi bir seçeneğin sunulmadığı, yalnızca çerezlerin kullanıldığının beyan edildiği kutulardır.

c) **Onaylama**: Yalnızca *Kabul Et* seçeneğinin olduğu kutulardır.

d) **Kategori Tercihleri**: Çerez kategorilerinin sıralandığı kutulardır.

aa. *Seçili Olan Kategorileri*: Manipülatif tekniklerin uygulanarak rıza vermeksizin tüm kategorileri seçili olarak kullanıcıya sunan kutulardır.

ba. *Seçili Olmayan Kategoriler*: Çerez kategorilerinin kullanımını kullanıcının aktif seçimine bırakan onay kutulardır.

e) **Şirket (Üçüncü Taraf Sağlayıcı) Tercihleri**: Çerez kategorilerinden ziyade üçüncü taraf şirketlerin listelendiği kutulardır.

aa. *Seçili Olan Şirketler*: Manipülatif tekniklerin uygulanarak rıza vermeksizin tüm şirketleri seçili olarak kullanıcıya sunan kutulardır.

ba. *Seçili Olmayan Şirketler*: Şirketlerin veri toplayıp toplamayacağını kullanıcının aktif seçimine bırakan kutulardır.

Nouwens ve arkadaşları (2020), web sitelerinin çerez izinlerini nasıl bir ara yüz tasarımı ile istedikleri ve bu tasarımların kullanıcıların açık rıza davranışlarını nasıl etkilediği sorularının cevaplarını Birleşik Krallık'ta web sitelerini tarayarak araştırmıştır. En çok ziyaret edilen 10.000 web sitesinden en popüler beş rıza yönetim platformunu¹⁷ kullanan 680 sitenin örneklem dâhilinde olduğu araştırmada, sitelerin

¹⁷ Web sitesi veya uygulamaların GDPR vb. gizlilik yasalarına uygun biçimde kullanıcıların kişisel verilerini toplamak ve işlemek amacıyla yasal izin aldıkları bir yazılımdır. OneTrust en çok tercih edilen rıza yönetim platformlarından biridir. İng: Consent Management Platform.

yalnızca %11,8'inin araştırma için GDPR'den derlenen minimum gereksinimleri karşıladığı ortaya çıkarılmıştır. Beş büyük rıza yönetim platformundan seçilen sekiz ara yüz tasarımının davranışlara etkisini 40 katılımcıyla araştıran yazarlar, tasarımda “vazgeç / reddet” butonu olmadığında onaylamanın %22 oranında arttığını; “ayrıntılı seçenekleri gör” butonu olduğunda ise izinlerin neredeyse %20 oranında azaldığını belirlemiştir.

Danimarka Veri Koruma Kurumunun daha önce sözü edilen çerez yönetimine ilişkin hazırladığı kılavuzda onay kutu ve butonlarının tasarımıyla ilgili öneriler yer almaktadır. Bu öneriler karanlık desenlerin etkisini azaltmaya yöneliktir. Kurum, özellikle çerezleri onaylama ve reddetme butonlarındaki görselliğe dikkat çekmektedir. Buna göre butonların boyutları, rengi ve konumu aynı olmalıdır (Datatilsynet, 2021). Örnek olarak Şekil 3.7’de verilmiştir.



Şekil 3.7: Yasal ve Etik Zemine Uygun Olarak Tasarlanmış Bir Açık Rıza Onay Kutusu Tasarımı.

Sonuç olarak nudging ve karanlık desen yöntemlerinin tasarım anlayışlarında sıkça tercih edildiği, açık rıza nosyonunun görmezden gelindiği ve iinin boşaltıldığı, iletişimsel faaliyet gözetiminin sıradanlaştığı, insan haklarına ve deneyimlerine saygı duyulmadığı, insani ihtiyaç ve amaçların geri planda tutularak para kazanmanın her şeyin önüne geçtiği bir ürün / hizmetlerin ve buna bağılı olarak yaratılan tasarımların etik olması söz konusu değildir. Bu nedenle davranışları çok büyük oranda yalnızca para kazanmak amacıyla toplayıp analiz eden, kişinin davranış kalıplarını inceleyerek gelecekteki kararlarını etkileme gücüne sahip olan gözetim kapitalisti şirketlerin de doğası gereği etik olmadığını söylemek mümkündür.

DÖRDÜNCÜ BÖLÜM

GÖZETİM KAPİTALİZMİ, ÇEVİRİM İÇİ KULLANICI GÖZETİMİ ve ETİK WEB ÜZERİNE KARMA BİR ARAŞTIRMA

4.1. Araştırmaya Giriş

Ağlara bağlı bilgi ortamının sürekli olarak gelişmesi ve yaygınlaşmasıyla insanın düşünce ve eylemleri daha hızlı biçimde dijitalleşmeye başlamıştır. Dijitalleşme ise gözetimin daha derinlikli gerçekleşmesine olanak sağlamaktadır. İletişimsel aktivite ve davranışların kâr amaçlı gözetlenmesi, dijital ekonomide iş modeli olarak yeni bir birikim mantığına ve sisteme işaret etmektedir. İletişim ve insan davranışlarının kaynak oluşturduğu bu birikim modeli; bilgi kapitalizmi (Fuchs, 2016; Fuchs, 2015), platform kapitalizmi (Srnicek, 2016; 2017), iletişimsel kapitalizm (Dean, 2014), büyük veri kapitalizmi (Fuchs, 2019) ve gözetim kapitalizmi (Foster & McChesney, 2014; Zuboff, 2015; 2019; Cegłowski, 2016) gibi çeşitli kavramlarla tartışılmaktadır. Söz konusu kavramlar, ağ toplumu, bilgi toplumu veya sanayi sonrası toplum gibi ifadelerle açıklanan günümüz toplumlarında ağların olumlu etkilerinden ziyade ağ üzerinde gerçekleştirilen tüm çevrimiçi hareketlerin izlenmesine ve buna bağlı olarak sermayenin yeni bir birikim modeli oluşturmaya işaret etmektedir.

Kâr odaklı ticari çevrim içi gözetim gerçekleştiren şirket ve platformlar iletişimsel tüm aktiviteleri ve insan doğasına ait tüm eylemleri Zuboff'un ifadesiyle (2019:8) “*bedava hammadde*” olarak görür ve bunlara tek taraflı el koyarak davranışsal verilere dönüştürür. Bu veriler insanın şimdi, kısa zamanda ve ileride ne yapacağını kestirmek amacıyla belirli işlemlerden geçerek analiz edilir, sınıflandırılır ve “davranışsal vadeli işlem piyasası” olarak adlandırılan yeni tür pazaryerlerinde kullanılır.

Çevrim içi reklam endüstri gözetim kapitalizmi mantığının doğmasında öncül bir yere sahiptir. Çevrim içi davranışsal reklam piyasasının büyüklüğü (Statista, 2020), iletişimsel faaliyetlerin ve insan davranışlarının platformlar ve şirketler için ne denli değerli metalar olduğunu göstermektedir. Geleneksel kapitalizmdeki emeğin sonsuz

sömürüsü, bugün yerini insan faaliyetlerinden beslenen gözetim kapitalizmine bırakmıştır. Bununla birlikte web'in hayatı kolaylaştırma, bilgiyi eşit dağıtma ve ona kolaylıkla erişme, daha verimli bir yaşam için ihtiyaçları karşılama gibi idealleri ve ağların özgürleştirici vaatleri geri planda kalmış; söz konusu dijital dünya ağa bağlanan her kanaldan her şeyi toplayan ve kâra dönüştürmeye çalışan bir sistem hâlini almıştır.

Literatürde gözetim kapitalisti olarak ifade edilen şirket ve platformlar kendi web sitesi ve uygulamalarında, sahip oldukları akıllı cihazlarda, başka şirketlerle yaptıkları işbirlikleriyle ve üçüncü taraf olarak başka platformlara yerleştirdikleri izleme kodları aracılığıyla tüm iletişim süreçlerini, çevrim içi kullanıcı hareketleri ve deneyimlerini takip edebilmektedir.

Çalışmanın konusu, çevrim içi iletişimi ve insan davranışlarını gözetleyen ve bunu iş modeli hâline getirerek kâr sağlayan şirket ve platformları Türkiye'nin en çok ziyaret edilen web siteleri ve kullanılan mobil uygulamaları aracılığıyla ortaya çıkarmak ve incelemektir. Aynı incelemede söz konusu web sitelerindeki davranışsal kullanıcı faaliyetlerinin üçüncü taraf şirket ve platformlara hangi izinlerle aktarıldığı, paylaşıldığı ve bunların hem etik hem de yasal olarak nasıl ifade edildiği de yer almaktadır. Çalışma ayrıca literatürü kapsamında ve araştırma bulguları neticesinde konuyla ilgili uzman görüşlerine yer vererek gözetim kapitalizmini teknoloji, kapitalizm, reklam, mahremiyet, veri ve hukuk gibi kavramlar çerçevesinde bütüncül bir yaklaşımla irdelemekte ve etik bir web'in inşasına yönelik bir kılavuz oluşturulmasına yardımcı olmaya çalışmaktadır.

4.1.1. Araştırmanın Amacı

Çalışmanın iki temel amacı vardır. Birinci amaç gözetimi kapitalizminin çevrim içi izini sürmek ve aktörlerini ortaya çıkarmaktır. İkinci amaç gözetim kapitalizmini tüm alanlarıyla inceleyerek ondan kaynaklı sorunları tespit etmek ve web'i daha etik hâle getirmek için çerçeve bir metin çıkarmaktır.

Bireyler ücretsiz yararlandıkları hizmetler (Google, Facebook), satın aldıkları fiziksel ürünler (Akıllı cihazlar) ve hizmetler (Netflix, Spotify), paylaşım ekonomisi temelli platformlar (Uber, Airbnb) ve doğrudan hiçbir ilişkilerinin olmadığı veri şirketleri (Oracle, Acxiom), reklam şirketleri (Criteo, Pubmatic), araştırma şirketleri (Gemius) gibi birçok kuruluş tarafından sürekli gözetime maruz kalmaktadır. Her biri yalnızca kendi platformlarının kullanımıyla değil; çeşitli web siteleri (gazeteler, alışveriş siteleri), mobil uygulamalar (oyunlar, araçlar, hizmetler) ve hatta çevrim dışı aktivitelerden de devamlı veri elde etmektedir. Özellikle reklamcılıkta bireyin geleceğini öngörme durumu milyar dolarlık bir sektör hâline gelmiştir. Bireyler ise gözetimin ne derece derin olduğu, nerelerde gerçekleştiği ve nereye kadar uzandığına dair oldukça yüzeysel bir bilgiye sahiptir.

Çalışmada, çevrim içi iletişimin ve insan deneyimlerinin üçüncü taraf şirketlere web siteleri ve mobil uygulamalar aracılığıyla nasıl aktarıldığı incelenmektedir. Araştırma kapsamındaki web sitelerinin kullanıcı verilerine erişirken ne tür bir rıza aldıkları irdelenmiş; söz konusu sitelerin veri gizliliği, güvenliği ve kullanıcı mahremiyeti açısından çerez politikaları ve gizlilik sözleşmeleri analiz edilmiştir. Çalışma kullanıcıları gözetleyen ve haklarında veri toplayan üçüncü taraf şirketlerin kimler olduğunu ortaya çıkararak *“insanlar hakkında çok şey bilenlerin insanlar tarafından bilinmemesi”* problemini azaltmaya katkı sağlayacaktır.

Çalışma ilk amacı doğrultusunda hâkim gözetim kapitalizmi mantığının nasıl işlediğine yönelik belirli bir alanın izin sürerken, ikinci amaç doğrultusunda ise gözetim kapitalizmini bütüncül bir bakış açısıyla ele alarak web’in nasıl daha etik hâle gelebileceğini ele almaya çalışmaktadır. Çalışma, literatürde yer alan bilgiler ve araştırmanın nicel bulguları eşliğinde teknoloji, iş modelleri, etik, mahremiyet, tasarım, hukuk, veri, çevrim içi reklamcılık gibi başlıklarla tartışmalar yürüterek etik web anlayışının oluşması için gerekenleri ortaya koymayı amaçlamaktadır.

4.1.2. Araştırmanın Önemi

Mevcut literatürde devlet gözetimi, işveren gözetimi, dijital gözetim, insanın insanı gözetlemesi (dikizleme), sosyal ağlarda kullanıcı mahremiyeti ve kullanıcı gözetim farkındalığı gibi çeşitli bağlamlarda araştırmalar yer alırken, bu çalışma yeni dijital ekonomide iletişim, gözetim ve kârlılığın yaklaşmasıyla ortaya çıkan kâr odaklı veri gözetimine eleştirel bir bakış açısıyla odaklanmaktadır. 21. yüzyıl ile birlikte çevrim içi ve çevrim dışı insan davranışları daha fazla gözetlenir hâle gelmiştir. Gözetleyenler için ise her bir insan davranışı birer hammadde kaynağı olarak görülmektedir. Hayatın her alanında yer alan gözetleme araçları ile şirketler ticari çıkarlarını ve ekonomik hedeflerini ön planda tutarak insanları derinlemesine araştırır, değerlendirir, sınıflandırır ve gerek farklı gruplara satar, gerek riski minimuma indirmek için kullanır gerekse reklamverenlere sunar. Dünyanın en değerli şirketlerinin teknoloji şirketleri olduğu düşünüldüğünde, iletişimin ve insan deneyimlerinin nasıl gözetlendiği, metalaştığı ve ekonomik bir değere dönüştüğünün günümüzde tartışılması oldukça önem arz etmektedir. Çalışmada elde edilecek niceliksel veriler ile bu alandaki eksikliğin giderilmesine katkı sağlanması beklenmektedir. Ayrıca, yerli literatür taramasında etik web kavramıyla ilgili çalışmaların yetersiz olduğu gözlemlenmiştir. Bu çalışma, etik web çerçevesi üzerine yapılan tartışmaların “etik web” kavramının yaygınlaşmasına yardımcı olması ve web’i daha etik hâle getirmek için sunduğu öneriler bakımından öneme sahiptir.

4.1.3. Araştırma Soruları

Çalışmada iki genel amaca dayalı olarak on ana soruya cevap aranmaktadır. Bu sorular aşağıdaki gibidir:

- 1) Hangi platform ve şirketler, web siteleri ve mobil uygulamalar aracılığıyla veri toplamaktadır?
- 2) Hangi tür gözetleme araçları ve teknolojiler hangi amaçlara dayalı olarak kullanıcı verilerini toplamaktadır?

- 3) Web siteleri, üçüncü tarafların izleme teknolojilerini kullanması için kullanıcılardan nasıl izin almaktadır?
- 4) Web sitelerinin çerez politikaları ve gizlilik sözleşmeleri kullanıcı faaliyetlerinin çevrim içi gözetlenmesini nasıl ele almaktadır?
- 5) Teknoloji şirketleri ve gözetleme faaliyetleri arasında nasıl bir ilişki söz konusudur?
- 6) Kişisel verilerin korunmasına ilişkin yasal düzenlemeler, kullanıcı gözetimini azaltmaya yönelik nasıl bir katkı sunmaktadır?
- 7) Çevrim içi reklam endüstrisinde gözetim faaliyetleri nasıl ele alınmaktadır?
- 8) Gözetim ve mahremiyet arasındaki ilişki kişisel verilerin korunması ve kişisel veri farkındalığının artmasıyla nasıl bir değişime uğramaktadır?
- 9) Gözetim kapitalizmini etik hâle getirmek ne derece mümkündür? Sistemdeki değişiklikler, gözetim kapitalizminin olumsuz etkilediği alanların azaltılmasında bir rol oynayabilir mi?
- 10) Etik web'in oluşumunda hangi yolların izlenmesi gerekmektedir?

Bu soruları genel olarak açmak faydalı olacaktır. İlk soruda web sitelerinde ve mobil uygulamalarda bulunan üçüncü taraf izleme teknolojilere kimlerin sahip olduğuna cevap aranmıştır. İkinci soruda analitik, pazarlama, tercih ve zorunlu çerezler bağlamında çevrimiçi platformlardaki çerezler mercek altına alınmıştır. Üçüncü soruda kullanıcılar siteye ilk girdiklerinde web sitelerinin izleme teknolojilerini aktif hâle getirmek veya uygulamak için onlarda nasıl izin aldıkları ortaya konulmuştur. Dördüncü soruda çevrimiçi gözetim hukuksal çerçevede analiz edilmiş; kullanıcı sözleşmelerinin yasalara ve bireysel haklara uygunluğu tartışılmıştır. Beşinci soru gözetleme faaliyetlerinin teknoloji ve girişim şirketleri tarafından neden öncül bir gelir kapısı olarak tercih edildiği üzerinedir. Altıncı soruda GDPR ve KVKK gibi yasal düzenlemelerin ülkemizdeki ve dünyadaki yansımaları çalışma konusu çerçevesinde ele alınmıştır. Yedinci soru, çevrim içi reklam endüstrisinin kullanıcı verilerinin

toplanmasına yönelik bakış açılarına yer vermeyi amaçlamaktadır. Sekizinci soruda kullanıcıların kendi verileri hakkında hak sahibi olması ve verilerinin değerini bilmesinin nasıl gerçekleştirilebileceği araştırılmıştır. Dokunuzcu soru, gözetim kapitalizminden bazı unsurların çıkarılmasının gözetim kapitalizmini daha etik yapıp yapamayacağıyla ilişkilidir. Son soruda ise web'teki mevcut sorunu bertaraf ederek daha etik bir web'in inşası için ihtiyaç duyulan yaklaşımlara cevap aranmıştır.

4.2. Araştırmanın Yöntemi

Çalışmada, her iki ana amaca hizmet etmek ve araştırma sorularına cevap bulmak amacıyla hem nicel hem de nitel araştırma teknikleri kullanılarak karma bir yöntem izlenmiştir. Karma yöntemde temel araştırma deseni olarak “açıklayıcı sıralı desen” kullanılmıştır. Bu yöntemde araştırmacı ilk olarak nicel verileri toplayacağı araştırmayı tasarlar ve uygular. İkinci aşamada ek bir açıklama gerektiren nicel sonuçları yorumlamak ve araştırmayı geliştirmek için nitel veri toplama ve analizi gerçekleştirir (Creswell - Clark, 2018).

Nicel olarak ilk etapta Türkiye'nin en çok ziyaret edilen ilk 50 web sitesinin ve en çok indirilen ilk 50 mobil uygulamasının içerisinde yer alan üçüncü taraf izleme teknolojileri tespit edilmiştir. İkinci aşamada, örneklem grubuna dâhil olan web sitelerinin çerez yerleştirme için nasıl açık rıza aldıkları araştırılmış; çerez politikaları ve gizlilik sözleşmeleri içerik analizi yöntemiyle incelenmiştir.

Araştırmanın ikinci aşamasını nitel yöntem oluşturmaktadır. Başta elde edilen nicel veriler olmak üzere çalışmanın literatürü ve araştırma soruları doğrultusunda konuya ilişkin alanında uzman kişilerle yarı yapılandırılmış görüşmeler yapılmıştır. Görüşmelerde yoruma ihtiyaç duyulan nicel bulgular değerlendirilmiş ve çevrim içi gözetimin iletişim odaklı ekonomisi, reklam alanındaki yeri, hukuku ve insanın benliğine etkisi irdelenmiştir. Araştırmanın bu ayağı olan nitel bölümle ilgili mülakatların gerçekleşmesi sürecine dair kısa bir not düşmek gerekmektedir. Nitel araştırmanın büyük bir bölümü nicel araştırmada yorumlanmaya ihtiyaç duyulan bulguların katılımcılara sorulması üzerine planlanmışken, bununla beraber görüşmeler

sırasında gözetim kapitalizmi ve web üzerinde daha geniş bir yelpazede tartışmalar yürütülmüştür. Farklı bağlamlarda yürütülen tartışmalar yalnızca nicel bulguların yorumlanmasına yardımcı olmamış; aynı zamanda gözetim kapitalizminden etkilenen doğrudan veya dolaylı tüm alanların derinlemesine incelenmesini ve etik web'in inşasına yönelik farklı bakış açılarından yararlanılmasını sağlamıştır.

Tüm bulgular çerçevesinde insanın iletişim ve etkileşim faaliyetleri ile kâr amaçlı gözetim arasındaki ilişkinin azaldığı, kişisel verilerin sahipliğinin değiştiği ve öneminin vurgulandığı, insan haklarına saygının arttığı, mahremiyet ve gizlilik kaygılarının azaltıldığı etik bir web'in nasıl inşa edilebileceği ortaya konulmaya çalışılmıştır.

4.2.1. Evren ve Örneklem

Araştırmanın ilk ayağını oluşturan nicel araştırmada Türkiye'nin en çok ziyaret edilen ilk 50 web sitesi ve en çok indirilen ilk 50 mobil uygulaması *similarweb.com* aracılığıyla örneklem alınmıştır. En çok ziyaret edilen siteler 1 Ekim 2021'de; en çok indirilen uygulamalarda AppStore 20 Kasım 2021'de, Google Play 14 Kasım 2021'de derlenmiştir.

Araştırmanın ikinci ayağını oluşturan nitel araştırmada ölçüt örnekleme yoluyla seçilen uzmanlarla mülakat yapılmıştır. Ölçüt örnekleme, belirli kriter ve niteliklere sahip kişi veya durumların örneklemesidir (Baltacı, 2018). Çalışma içerisinde yer alan gözetim, kapitalizm, iletişim, reklam, tasarım ve yasal düzenlemeler gibi başlıca konular sivil toplum, akademi, kamu kuruluşları, tasarım, reklam ve hukukçuların ilgi alanına girmektedir. Bu sebeple araştırmada bu alanlardan ilgililerle görüşülerek mevcut durum incelenmiş, nicel araştırma bulguları daha sağlıklı olarak yorumlanmış, araştırma sorularına cevap aranmış ve çözüm önerileri üzerinde durulmuştur.

4.2.2. Araştırmanın Sınırlılıkları

Nicel araştırmada yalnızca üçüncü taraf şirketlerin web siteleri ve mobil uygulamalardaki izleme teknolojileri tespit edilmiştir. Diğer bir ifadeyle, *siteadi1.com* web sitesinin içinde yer alan *ucuncutarafsite.com*'a ait bir izleyici yazılımı araştırma kapsamında üçüncü taraf olarak kabul edilmiş ve araştırmaya dâhil edilmiştir. Web siteleri ve uygulamaların kendi alan adlarına ait izleyici yazılımları, reklam veya analitik amaçlı kullanılsa bile, araştırma kapsamı dışında tutulmuştur.

En çok indirilen mobil uygulamalar IOS (AppStore) ve Android (Google Play) uygulama mağazalarına göre değiştiği için her iki platformdaki uygulamalar karşılaştırılmış ve birbiriyle çakışan uygulamalar araştırma haricinde tutularak toplam 74 uygulama elde edilmiştir. 74 uygulamadan 72'si araştırmaya dâhil olmuştur; zira *Samsung Notes* ve *Samsung Email* adlı uygulamalara erişim sağlanamamıştır. Bu nedenle 72 mobil uygulamada yer alan üçüncü taraf izleme teknolojileri incelenmiştir.

En çok ziyaret edilen ilk 50 web sitesinden 48'i araştırmaya dâhil olmuştur. İki siteye Türkiye'den erişim engelli olduğu için araştırmaya dâhil edilmemiştir.

Araştırma kapsamındaki 48 sitenin 3'ünde çerez politikası veya gizlilik sözleşmesi bulunamamıştır. Bu nedenle 45 web sitesinin çerez politikası ve gizlilik sözleşmesi içerik analizi yöntemiyle incelenmiştir.

Web siteleri ve mobil uygulamaların taranmasını içeren nicel araştırma Ekim - Kasım 2021 arasında gerçekleşmiştir.

Araştırma kapsamında bir Facebook çalışanı ve bir programatik reklam şirketi çalışanı ile mülakat yapmak için iletişime geçilmiştir. Fakat şirketlerin çalışanlarıyla yaptıkları oldukça sıkı gizlilik ve güvenlik sözleşmelerinin tarafıma bildirilmesi nedeniyle onlarla mülakat gerçekleştirilememiştir.

Başta haber siteleri olmak üzere nicel araştırma kapsamındaki tüm web sitelerine e-posta yoluyla araştırma hakkında bilgilendirme yapılmış ve söz hakkı tanınmıştır. Ayrıca KVK Kurumu ile de iletişime geçilip görüşme yapılmak istenmiştir. Fakat söz konusu taraflarla bir görüşme sağlanamamıştır.

4.2.3. Verilerin Toplanması, Analizi ve Çözümlemesi

Web sitelerindeki üçüncü taraf çerez sayıları ve türleri, her bir sitede en az üç sayfa gezmek koşuluyla *Thunderbeam-Lightbeam* tarayıcı eklentisiyle tespit edilmiştir. Bu aşamada sitelerin cihazlara yerleştirdikleri çerezlerin türleri ve toplamı tespit edilmiştir. Ayrıca üçüncü taraf izleme sistemlerinin sahipleri ve sitelerdeki alan adları ortaya konulmuştur.

Mobil uygulamalardaki izleyicilerin tespiti için *Exodus Privacy*'nin yazılım sistemi kullanılmıştır. Toplam izleyici sayısı, izleyicilerin kimler olduğu ve uygulamanın cihazdan talep ettiği erişim izinleri ortaya konulmuştur.

Araştırma kapsamındaki 48 web sitesinin çerez bildirimi ve kullanıcılardan rıza alma biçimleri, Utz ve arkadaşlarının (2019) açık rıza talep örnekleri sınıflandırması örnek alınarak analiz edilmiştir. Çerez politikası ve gizlilik sözleşmelerine uygulanan içerik analizinde yedi soruya cevap aranmıştır. Bu sorular; hangi verilerin toplandığı, hangi amaçla toplandığı, verilerin nasıl işlendiği, kimlerle paylaşıldığı, çerezlerin saklanma süresinin olup olmadığı, verilerin silinmesine yönelik iletişim bilgisi ve sözleşmelerin başka sözleşmelere sorumluluk yıkıp yıkmadığıdır.

Nicel araştırma bulgularına, çalışmanın literatürüne ve araştırma sorularına bağlı olarak teknoloji, iletişim, reklam, tasarım ve hukuk alanına özgü konularda yetkinlik sahibi uzmanlarla yarı yapılandırılmış görüşmeler gerçekleştirilmiştir. Görüşmeler sonucunda toplanan veriler temalara ayrılarak tartışılmıştır.

4.3. Araştırmanın Bulguları

Bu bölümde araştırmanın hem nicel hem de nitel sonuçları yer almaktadır.

4.3.1. Nicel Araştırma

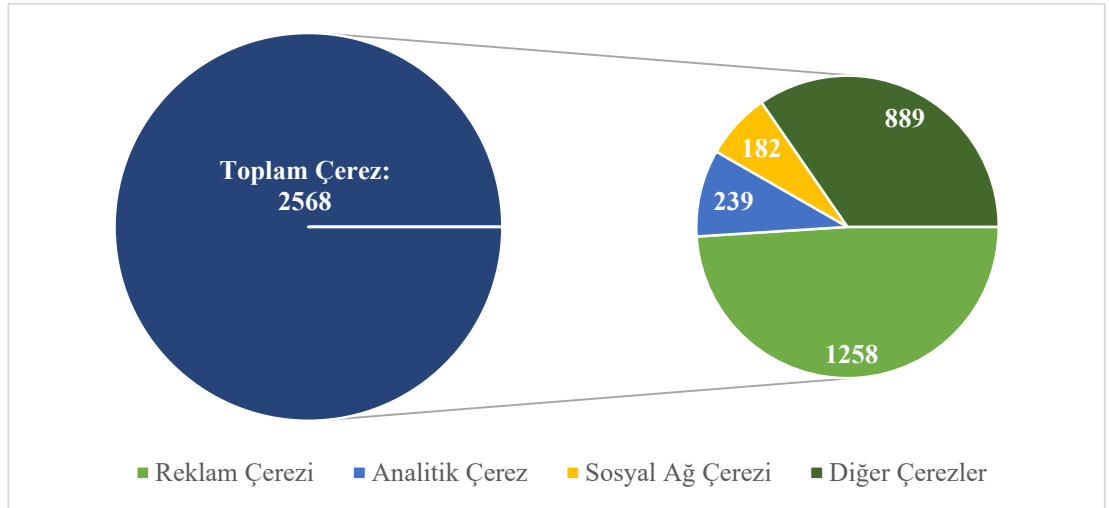
Bu bölümde nicel araştırmaya ait bulgular bulunmaktadır. Web siteleri ve mobil uygulamalarda kullanıcıları izleyen üçüncü taraf şirketlerin kimler olduğuna,

sitelerin çerez kullanımı için kullanıcıyı nasıl bilgilendirdiklerine, açık rıza aldıklarına ve bu sitelerin çerez politikaları ve gizlilik sözleşmelerinin içerik analizine yönelik araştırma sonuçlarına bu bölümde yer verilmiştir.

4.3.1.1. Web Sitelerindeki Üçüncü Taraf İzleyiciler

Üçüncü taraf çerezler, ziyaret edilen web sitesi dışındaki bir site tarafından oluşturulan ve yerleştirilen dosyalardır. Doğrudan ziyaret edilen sitenin dışında farklı bir alan adına ait sunucudan gelen bir JavaScript izleme koduyla yerleştirilmektedir. Genellikle reklam gösterme, yeniden hedefleme ve farklı site ziyaretleri sırasında takip ederek kullanıcıları analiz etme amacıyla kullanılmaktadır.

Araştırma kapsamında incelenen 48 sitede toplam 2568 adet üçüncü taraf çerez tespit edilmiştir. Bu çerezlerin %49'u (n=1258) reklam, %9,30'u (n=239) analitik amaçlı olup; %7'si (n=182) ise sosyal ağların yerleştiği çerezlerdir. Çerezler birden çok kategori altına dâhil olabilmektedir. Örneğin, bir çerez hem analitik hem de reklam amaçlı bir sosyal ağ çerezi olabilmektedir.



Tablo 4.1: Sitelerde Tespit Edilen Çerezlerin Tür ve Amaçlarına Göre Dağılımı.

Tablo 4.1'de yer alan diğer çerezler kategorisi, siteleri tarama aşamasında kullanılan *Thunderbeam-Lightbeam* uygulaması tarafından belirlenen zorunlu,

yönlendirme, takip, optimizasyon veya zararlı yazılım gibi kategorilerin birleşiminden oluşmaktadır.

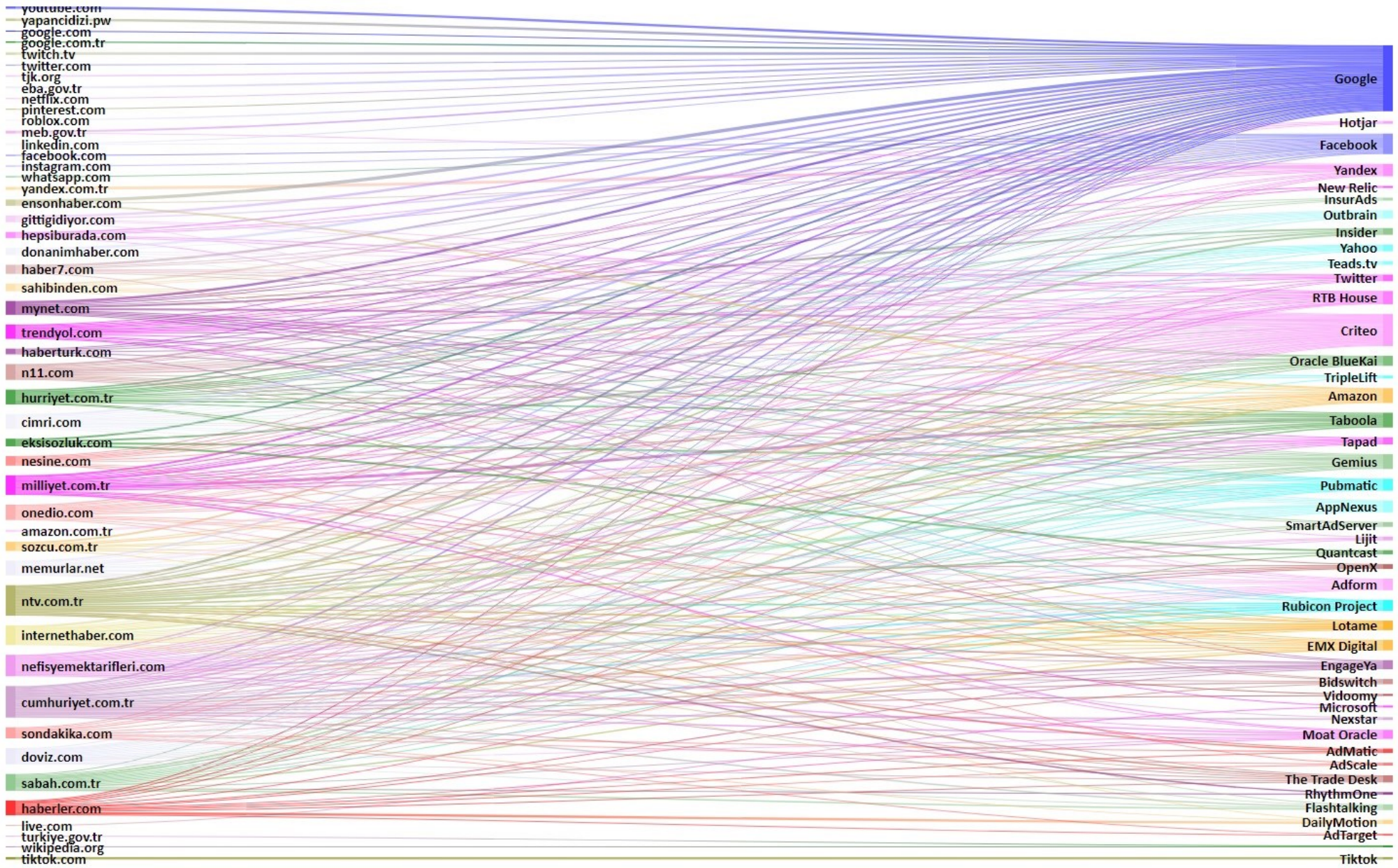
Araştırma kapsamında incelenen 48 sitede en az 112 farklı şirkete ait üçüncü taraf çerez tespit edilmiştir.

48 site tarandığında en çok çerez yerleştiren toplam 15 şirket tablo 4.2’de verilmiştir. Bu şirketler tek bir siteyle birden çok kez iletişime geçerek farklı alt kaynaklarından kullanıcıların cihazlarına farklı çerezler yerleştirebilmektedir. Örneğin, sahibinden.com’da Criteo’ya ait “static.criteo.net”, “gum.criteo.com”, “sslwidget.criteo.com” ve “csm.fr.eu.criteo.net” alt alan adlarından gelen 4 adet çerez tespit edilmiştir.

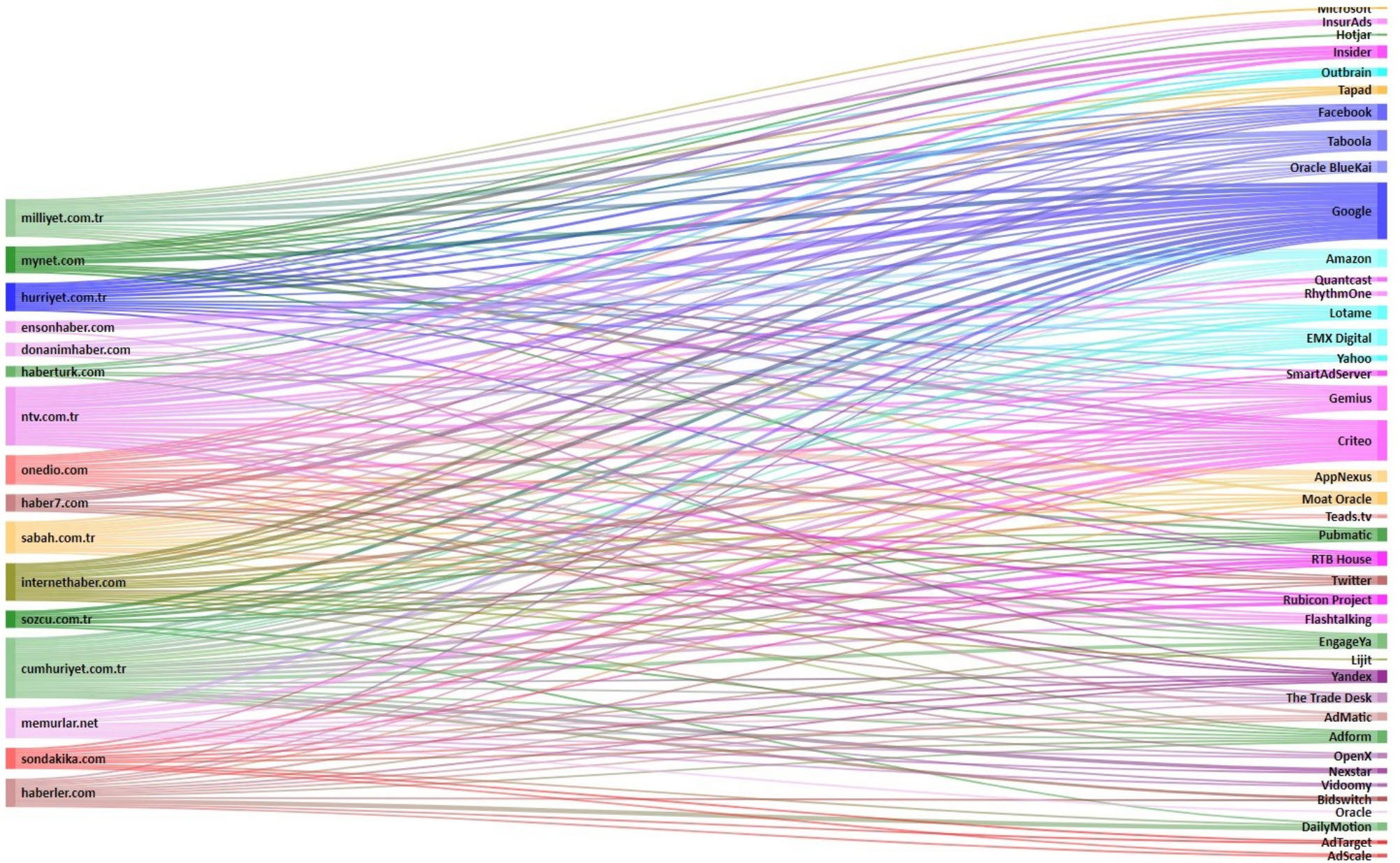
Şirketler	Çerez Sayısı
Google	708
Criteo	171
Taboola	93
Moat Oracle	45
Facebook	42
Gemius	37
Amazon	36
DailyMotion	35
Insider	31
Pubmatic	29
Rubicon Project (Magnite)	27
Twitter	23
Adform	23
AppNexus	23
The Trade Desk	22

Tablo 4.2: En Çok Çerez Yerleştiren 15 Şirket ve Çerez Sayıları.

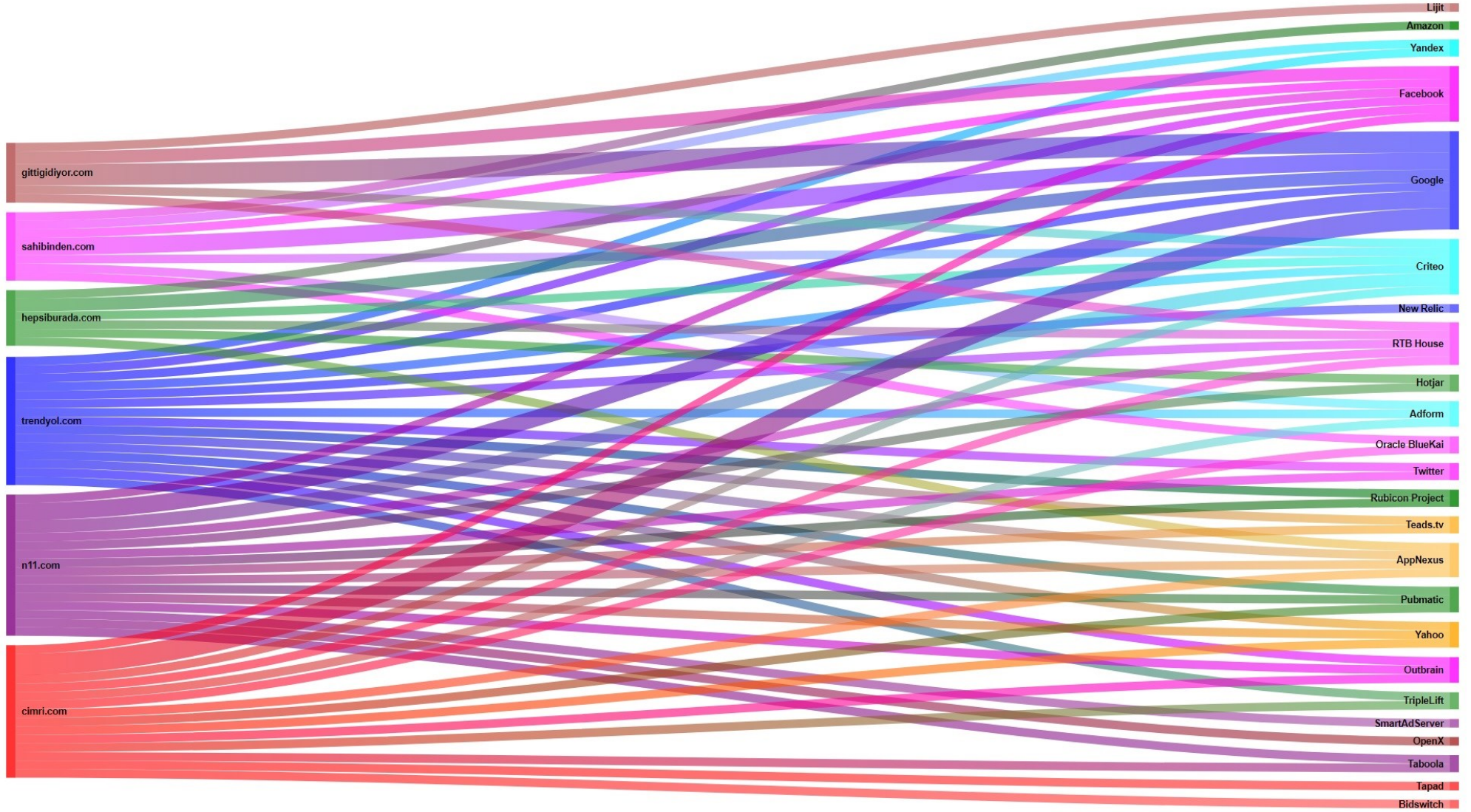
48 site aracılığıyla kullanıcıların cihazlarına en çok çerez yerleştiren 43 şirket ile sitelerin veri alışveriş haritası aşağıdaki tablo 4.3’de paylaşılmıştır. Ayrıca 48 siteyi filtrelediğimizde 16 adet haber sitesi (Geleneksel medya ve çevrim içi siteler) ve 6 adet e-ticaret sitesi yer aldığı görülmektedir. 16 haber sitesinin bu üçüncü taraf şirketlerle ilişkisi tablo 4.4’te, 6 e-ticaret sitesinin ilişkisi ise tablo 4.5’te paylaşılmıştır. Ayrıca, 100’den fazla üçüncü taraf çerez yerleştiren 11 site tablo 4.6’da yer almaktadır.



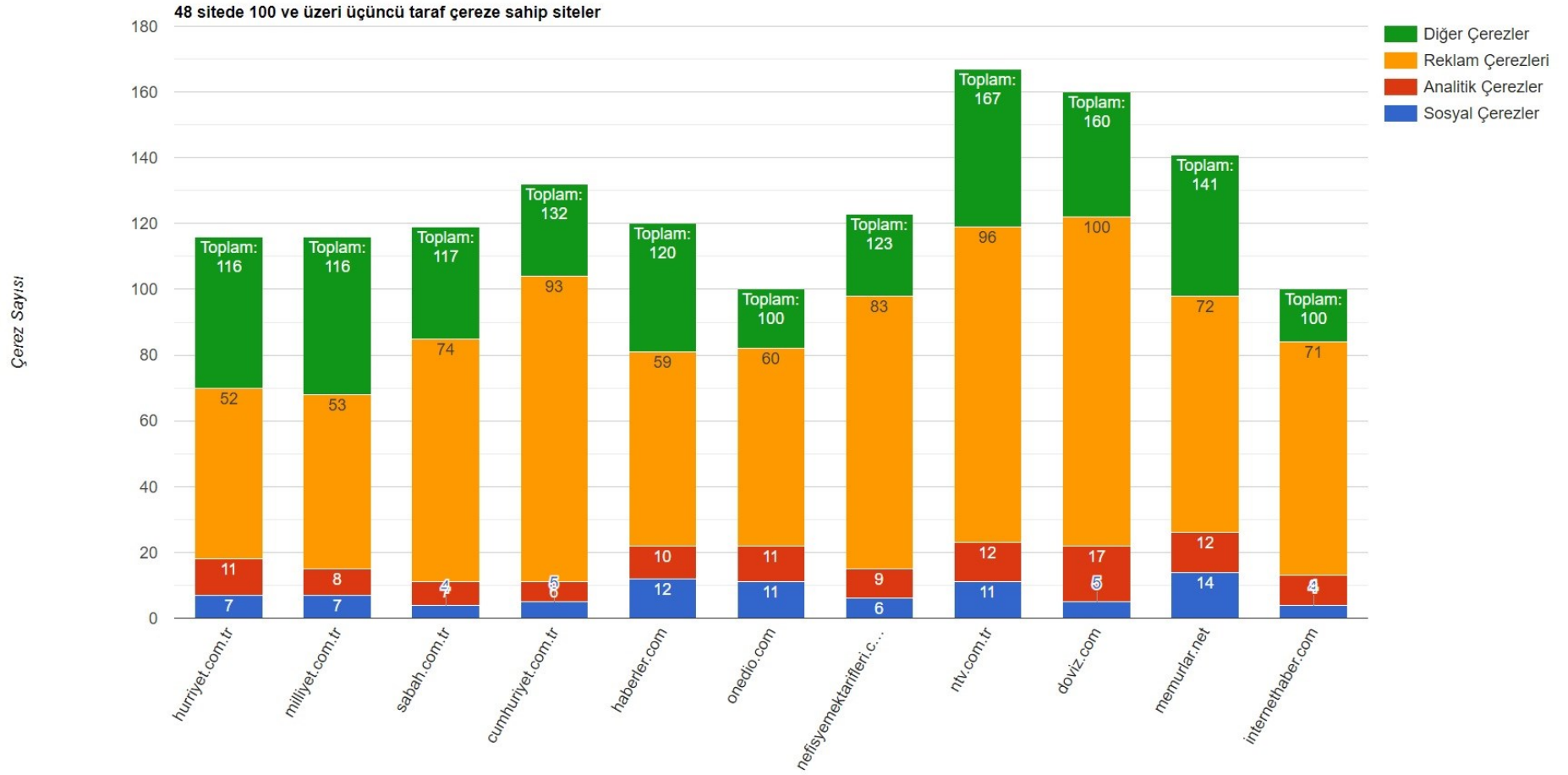
Tablo 4.3: 48 Site ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışverişi Ağı.



Tablo 4.4: 16 Haber Sitesi ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışveriş Ağı.

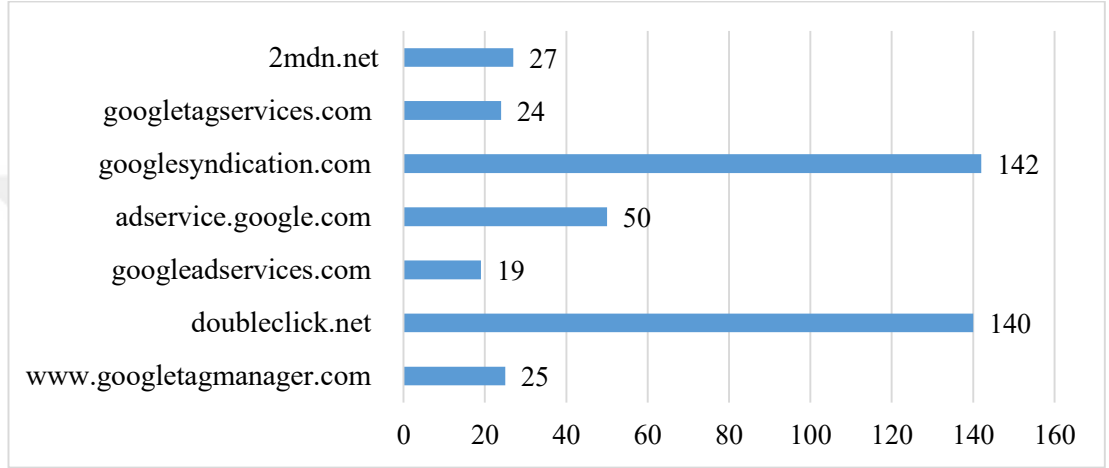


Tablo 4.5: 6 E-Ticaret Sitesi ile Üçüncü Taraf Çerez Sahibi Şirketlerin Veri Alışverişi Ağı.



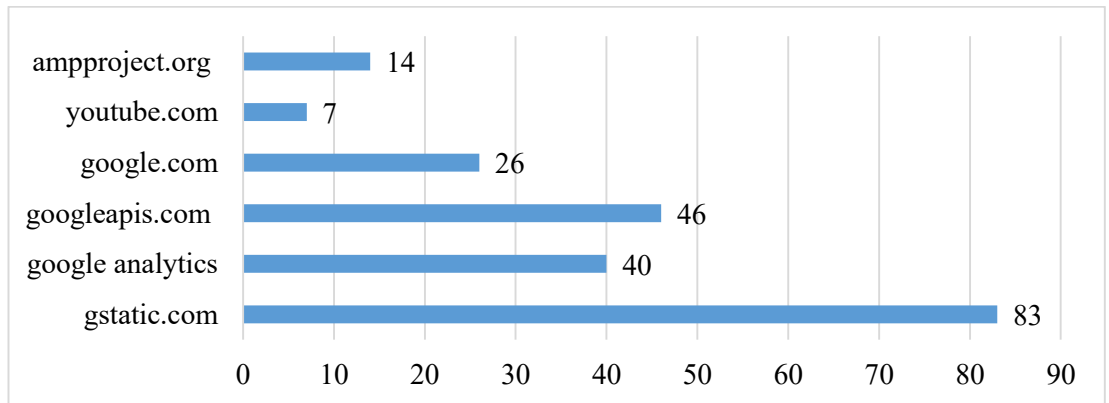
Tablo 4.6: 100 ve Üzeri Üçüncü Taraf Çerez Yerleştiren 11 Web Sitesi.

48 sitede bulunan 708 çerez bağlantısı ile Google üçüncü taraf olarak web sitelerinde en çok tercih edilen şirket durumundadır (Bkz.: Tablo 4.2). Bu çerezlerin %60'ından fazlasını Google'ın reklam ürünleri oluşturmaktadır. Tablo 4.7'de verilen alt alan adları araştırma sırasında en çok tespit edilen Google reklam ürünlerine ait çerezlerin kaynağıdır.



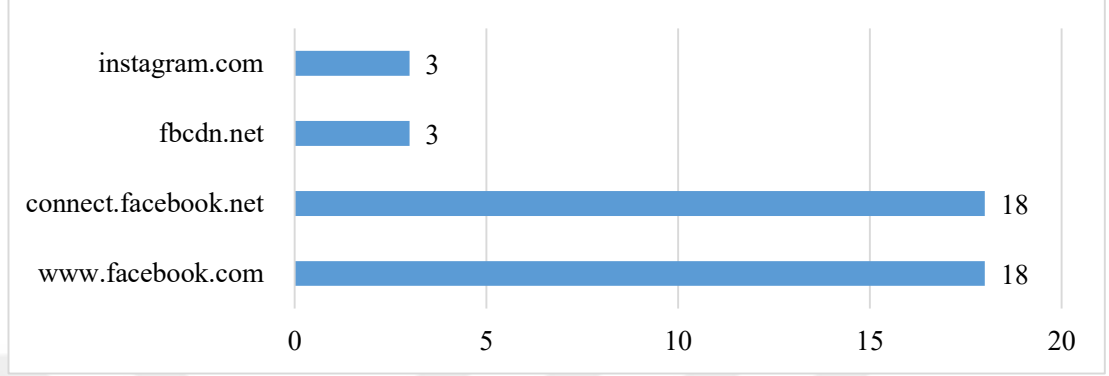
Tablo 4.7: 48 Web Sitesinde Bulunan Google Reklam Ürünlerine Ait Çerezlerin Sayısı ve Alan Adı Uzantıları.

Google çerezlerinin geri kalan kısmı analitik ve çeşitli hizmet (video, içerik dağıtım ağı, yazı karakterleri vb.) amaçlı kullanılmaktadır (Bkz.: Tablo 4.8).



Tablo 4.8: 48 Web Sitesinde Bulunan Diğer Google Çerezlerine Ait Alan Adı Uzantıları.

Bir diğer şirket Facebook’a ait 42 çerez tespit edilmiştir (Bkz.: Tablo 4.2). Bunlara ait dağılım Tablo 4.9’da verilmiştir.



Tablo 4.9: 48 Web Sitesinde Bulunan Facebook Çerezlerine Ait Alan Adı Uzantıları.

Bu verilere bakıldığında 48 siteden en az 18’inde Facebook’un kullanıcıları izlemeye devam ettiği anlaşılmaktadır. Facebook Connect, sitelerin hızlı kullanıcı kaydı oluşturması için Facebook ile bağlan hizmeti sunarken, aynı zamanda Facebook Piksel ile de reklam amaçlı kullanıcı verisi de toplamak üzere kullanılmaktadır.

Google, Facebook, Twitter vb. bilinen teknoloji şirketleri dışında araştırma kapsamında en çok çerez yerleştirdiği tespit edilen şirketlerin kimler olduğu ve hangi alan adına bağlı JavaScript kodları ile çerez yerleştirdikleri aşağıdaki gibidir:

Rubicon Project: 2007’de kurulmuş ABD’li çevrim içi reklam teknolojileri şirkettir. Telaria ile birleşimiyle birlikte yeni adı Magnite Inc.’dir. 2019 yılında toplam geliri 156 milyon dolardır.

pixel.rubiconproject.com	fastlane.rubiconproject.com	eus.rubiconproject.com
beacon-ams3.rubiconproject.com	video-ads.rubiconproject.com	optimized-by.rubiconproject.com
prebid-server.rubiconproject.com	beacon-nf.rubiconproject.com	beacon-fra2.rubiconproject.com
token.rubiconproject.com	post.update.rubiconproject.com	

Criteo: 2005 yılında kurulmuş, çevrim içi görüntülü reklam sağlayan Fransız bir reklam şirkettir. Criteo’nun geliri 2021 yılında bir önceki yıla göre %9 artarak

2,2 milyar doları aşmıştır. Piyasa değeri 2,5 milyar dolardır. Oracle ve LiveRamp ile veri ortaklığı söz konusudur.

static.criteo.net	gum.criteo.com	dis.criteo.com
csm.nl.eu.criteo.net	sslwidget.criteo.com	bidder.criteo.com
3pd.criteo.com	cat.criteo.com	ads.eu.criteo.com
cat.fr.eu.criteo.com	pix.eu.criteo.net	csm.eu.criteo.net
rtb.nl.eu.criteo.com	widget.eu.criteo.com	

Taboola: 2007 yılında kurulmuş, çevrim içi haber sitelerinde sıkça yer alan “Sizin için önerilenler” şeklinde sponsorlu bağlantılar paylaşan bir reklam şirkettir. 2021’in üçüncü çeyreğinde toplam 338 milyon gelir elde etmiştir.

cdn.taboola.com	c2.taboola.com	widget.perfectmarket.com
trc.taboola.com	15.taboola.com	images.taboola.com
vidstat.taboola.com	impramp.taboola.com	wf.taboola.com
pips.taboola.com	am-match.taboola.com	am-vid-events.taboola.com
impr.taboola.com	opps.taboola.com	am-wf.taboola.com
vidstat.taboola.com	sync-tl.taboola.com	

Moat Oracle: Kullanıcıların gerçek zamanlı dikkatlerini ve ilgisini analiz eden teknoloji hizmetidir. Reklamların etkileşimini ısı haritaları oluşturarak ölçümler. Oracle’a aittir.

z.moatads.com	px.moatads.com	geo.moatads.com
mb.moatads.com	quantcast584928381.s.moatpixel.com	svastx.moatads.com
dailymotionjsvideo432290662219.s.moatpixel.com	pgthetradedeskvideo910663478306.s.moatpixel.com	

Gemius: Uluslararası bir araştırma ve teknoloji şirkettir. Çevrim içi reklam kampanyalarının yönetimi alanında veri ve öneri sağlamaktadır. Genellikle Türkiye’de kullanıcılardan anket yoluyla veri toplamasıyla biliniyor.

trgde.adocean.pl	gdetr.hit.gemius.pl	ls.hit.gemius.pl
gatr.hit.gemius.pl	tr.hit.gemius.pl	pro.hit.gemius.pl

Insider: Kanallar arası verileri birbirine bağlama ve kullanıcıların gelecekteki davranışlarını tahmin etme üzerine reklamcılara hizmet sağlayan bir platformdur.

hurriyet.api.useinsider.com	milliyet.api.useinsider.com	location.api.useinsider.com
hit.api.useinsider.com	segment.api.useinsider.com	assets.api.useinsider.com
log.api.useinsider.com	eitri.api.useinsider.com	carrier.useinsider.com
image.useinsider.com	recommendation.api.useinsider.com	

Pubmatic: Ajanslar ve reklamveren yayıncılar için çevrim içi reklam yazılımları ve stratejileri sunan bir şirkettir. 2020 yılında bir önceki yıla göre geliri %31 artışla 148,7 milyon dolar olmuştur.

simage2.pubmatic.com	hbopenbid.pubmatic.com	image8.pubmatic.com
aktrack.pubmatic.com	s.update.rose.pubmatic.com	image4.pubmatic.com
vpaid.pubmatic.com	ads.pubmatic.com	vid.pubmatic.com
aktrack.pubmatic.com	hbopenbid.pubmatic.com	sshowads.pubmatic.com

Adform: 2002’de kurulmuş, Danimarkalı çevrim içi reklam teknolojileri sunan bir şirkettir. Tüm dünyada 20’den fazla ofisi yer almaktadır. 2020 yılında 74,3 milyon Euro gelir elde etmiştir.

cm.adform.net	adx.adform.net	server.seadform.net
track.adform.net	s1.adform.net	s2.adform.net
dmp.adform.net		

AppNexus: Gerçek zamanlı teklif vermeye yönelik hizmet sağlayan bir reklam teknoloji şirketidir. Programatik reklamcılıkta hem talep hem de arz yönlü kullanılabilir. 2018 yılında AT&T tarafından 1,6 milyar dolara satın alınmıştır.

secure.adnxs.com	ib.adnxs.com	cdn.adnxs.com
fra1-ib.adnxs.com	acdn.adnxs.com	prebid.adnxs.com
acdn.adnxs-simple.com		

The Trade Desk: Yayıncıların ve reklamverenlerin veriye dayalı çevrim içi reklam satın almak için kullandıkları bir yazılım ve küresel teknoloji şirketidir. 2020 yılı geliri bir önceki yıla göre %26 artarak 836 milyon dolar olmuştur.

match.adsrvr.org	insight.adsrvr.org	ad.adsrvr.org
del-bid.adsrvr.org	data.adsrvr.org	

EngageYa: Yayıncılara, ajanslara ve reklamverenlere native reklamcılık hizmeti sunan bir reklam şirkettir.

widget.engageya.com	recs.engageya.com	images9.engageya.com

AdMatic: 2014 yılında kurulmuş, çevrim içi reklam şirkettir.

cdn.admatic.com.tr	cdn2.admatic.com.tr	cdn3.admatic.com.tr
cdn4.admatic.com.tr	ads3.admatic.com.tr	cdn5.admatic.com.tr

BlueKai Oracle: Şirketlerin çevrim içi, çevrim dışı ve mobil pazarlama reklam kampanyalarını kişiselleştirmelerini sağlayan bulut tabanlı bir veri yönetim platformudur. Oracle'a aittir.

tags.bluekai.com	stags.bluekai.com	tags.bkrtr.com

RTB House: Reklamverenlere yapay zekâ teknolojileri destekli çevrim içi kişiselleştirilmiş reklam hizmetleri sunan bir reklam teknoloji şirkettir. 2016 yılından 2019 yılına kadar geliri %810 artarak 169,4 milyon euro olmuştur.

prebid-eu.creativecdn.com	ams.creativecdn.com	statics-europe.creativecdn.com
creativecdn.com		

Teads.tv: Yayıncılara ve reklamverenlere çevrim içi reklamcılık hizmeti sunan bir şirkettir. Telekomünikasyon şirketi Altice'e aittir. 2020 yılında 540 milyon dolar gelir elde etmiştir.

criteo-sync.teads.tv	a.teads.tv	s8t.teads.tv
t.teads.tv	sync.teads.tv	

Lotame: Yayıncıların, ajansların ve reklamverenlere detaylı kitle verisi sunan bir veri yönetim platformudur. Üçüncü taraf kitle veri segmentleri satar.

tags.crowdctrl.net	bcp.crowdctrl.net	sync.crowdctrl.net

EMX Digital: Çevrim içi programatik reklam hizmeti sunan bir şirkettir.

cs.emxdgt.com	hb.emxdgt.com	biddr.brealtime.com
el.emxdgt.com		

AdScale: Reklamverenleri ve yayıncıları bir araya getiren gerçek zamanlı bir çevrim içi reklam platformudur.

cotads.adscale.de	hb.adscale.de	trx.adscale.de
ih.adscale.de	js.adscale.de	

Tapad: Markalar, ajanslar ve yayıncılar için cihazlar arası reklam ve içerik dağıtımını sağlayan bir şirkettir. İnternet ve cihaz verilerini analiz ederek iki veya daha fazla cihazın aynı kişiye ait olup olmadığını tahmin eden algoritmik sistemler geliştirmişlerdir. 2020 yılında Experian tarafından 280 milyon dolara satın alınmıştır.

pandg.tapad.com	pixel.tapad.com	

SmartAdServer: Kullanıcı verilerine göre reklamları optimize eden, arz yönlü hizmet sunan Fransız programatik reklamcılık şirketidir. 2020 yılı geliri 151,6 milyon dolardır.

rtb-csync.smartadserver.com	prg.smartadserver.com	www8.smartadserver.com
csync.smartadserver.com	prg.smartadserver.com	

Flashtalking: 2009’da kurulmuş, çevrim içi reklamları gerçek zamanlı olarak kişiselleştirme hizmeti sunan bağımsız reklam kuruluşudur. Mediaocean, 2021 yılında Flashtalking’i 500 milyon dolara satın almıştır.

servedby.flashtalking.com	cdn.flashtalking.com	secure.flashtalking.com
d9.flashtalking.com	ad-events.flashtalking.com	

Outbrain: 2006 yılında kurulmuş, yayıncıların sitelerine sponsorlu bağlantılar yerleştiren bir native reklamcılık şirketidir. 2020 yılı geliri 767 milyon dolardır.

sync.outbrain.com	widgets.outbrain.com	mcdp-chide2.outbrain.com
widget-pixels.outbrain.com	tcheck.outbrainimg.com	log.outbrainimg.com
odb.outbrain.com	mcdp-nydc1.outbrain.com	

OpenX: 2008’de kurulmuş, ABD’li programatik reklam teknoloji şirketidir. Reklam borsasıdır.

firstimpression-d.openx.net	vidoomy-d.openx.net	eu-u.openx.net
us-u.openx.net	adpone-d.openx.net	ox-delivery-prod-europe-west1.openx.net
underdogmedia-d.openx.net	kiosked-d.openx.net	

Bidswitch: 2013’de kurulmuş, programatik reklam çözümleri sunan Alman şirkettir.

ghent-gce-sc.bidswitch.net	x.bidswitch.net	

InsurAds: 2017’de kurulmuş, yayıncıların çevrim içi reklam gelirlerini artırmaya yönelik çözümler sunan Portekizli bir şirkettir.

cdn.insurads.com	services.insurads.com	messaging.insurads.com

Lijit: 2006’da kurulmuş bir çevrim içi reklam şirkettir. ABD’li Sovrn Holding’e aittir.

ap.lijit.com	gslbeacon.lijit.com	vaplams1.lijit.com
pxdrop.lijit.com	ce.lijit.com	

RhythmOne: 2004’te kurulmuş ABD’li çevrim içi reklam şirkettir.

sync.lrx.io	tag.lrx.io	

Quantcast: 2006’da kurulmuş gerçek zamanlı reklam, kullanıcı ölçümleme ve içgörü oluşturma konusunda hizmet veren ABD’li bir şirkettir.

secure.quantserve.com	rules.quantcount.com	pixel.quantserve.com

AdTarget: Türkiye’de yer alan bir reklam yayın ağıdır.

sync.console.adtarget.com.tr	ghb.console.adtarget.com.tr	cdn11.adtarget.com.tr

TripleLift: Native reklamcılık alanında hizmet veren ABD’li bir reklam şirkettir.

eb2.3lift.com	tlx.3lift.com	

Nexstar: 2014’de kurulmuş, yayıncılar ve reklamverenler için video reklam hizmetleri sunan ABD’li şirkettir.

ad.lkqd.net	v.lkqd.net	t.lkqd.net

Vidoomy: 2017’de kurulmuş, video reklam hizmetleri sunan İspanyol bir şirkettir.

ads.vidoomy.com	a.vidoomy.com	player.vidoomy.com

New Relic: 2008’de kurulmuş, yayıncı web sitelerini ve mobil uygulamalarını gerçek zamanlı olarak izleyerek analiz eden ve performanslarını ölçen ABD’li bir teknoloji şirketidir. 2021’de bir önceki yıla göre geliri %11 artarak 668 milyon dolar olmuştur.

js-agent.newrelic.com	bam-cell.nr-data.net	bam.nr-data.net

Hotjar: 2014 yılında kurulmuş, kullanıcıların çevrim içi davranış ve etkileşimlerini takip ederek analizler üreten bir şirkettir.

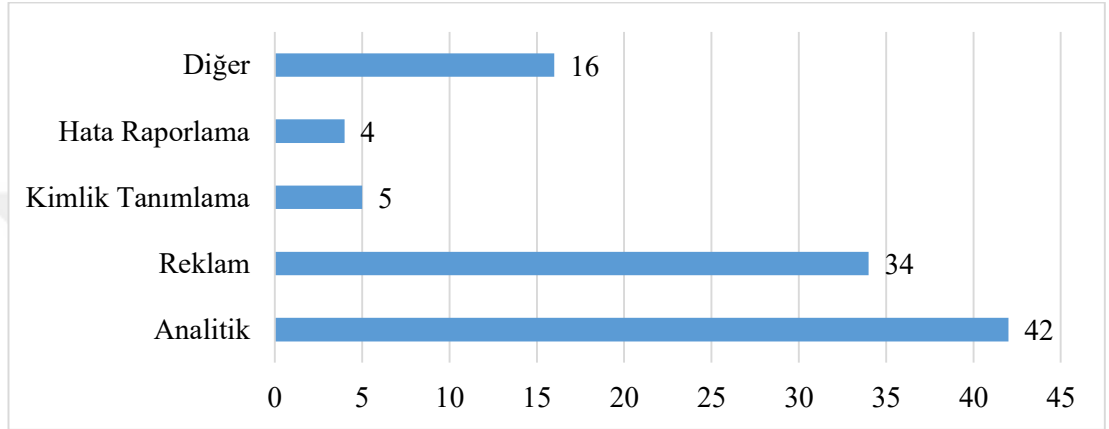
static.hotjar.com	script.hotjar.com	vars.hotjar.com

Analitik ve reklam amaçlı izleyicilerin dışında bazı sitelerin güvenlik ve hız açısından iyileştirmeler yapmak için üçüncü taraf olarak CloudFlare kullandığı tespit edilmiştir. Bir bulut sistemi olan CloudFlare, içerik dağıtım ağı, güvenlik ve sitenin hız performansını optimize eden hizmetler sunmaktadır. Trendyol, Hürriyet, Milliyet, Ekşi Sözlük, Sabah, Cumhuriyet, Haberler.com, Sondakika.com, Onedio, NTV, Yabancidizi.pw, Ensonhaber.com, Memurlar.net ve Internethaber.com sitelerinde CloudFlare’e ait izleyiciler bulunmuştur.

4.3.1.2. Mobil Uygulamalardaki Üçüncü Taraf İzleyiciler

Türkiye’de hem IOS hem de Android işletim sistemlerine sahip mobil cihazlarda en çok indirilmeye sahip 72 ortak mobil uygulama araştırma kapsamına dâhil edilmiştir.

Araştırma kapsamında taranan 72 mobil uygulamada 84 farklı izleyicinin (tracker) toplam 387 kere kullanıldığı tespit edilmiştir. Her bir izleyicinin birden farklı amaçla da kullanılıyor olması dikkate alınarak bu izleyicilerin 42'sini analitik, 34'ünün reklam, 5'inin kimlik tanımlama, 4'ünün hata raporlama ve 16'sının ise çeşitli amaçlara dayalı diğer izleyiciler olduğu şeklinde bir kategorik ayırım yapılmıştır.



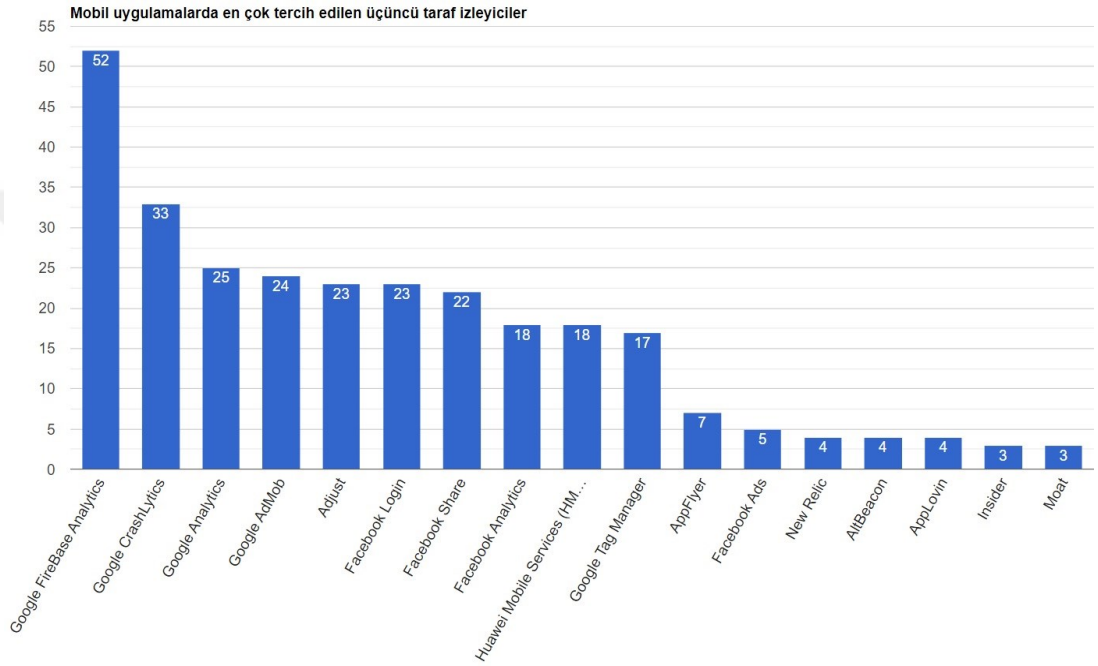
Tablo 4.10: 72 Mobil Uygulamadaki Tespit Edilen İzleyicilerin Kullanım Amaçları.

Not: Bir izleyici birden çok amaçla kullanılabilir.

İzleyiciler amaçlarına göre aşağıdaki gibi tanımlanabilir:

- 1) Reklam:** Uygulama içi reklam gösterimleri, reklam ölçüm ve analizleri, reklamlarla ilişkili bileşenler için kullanılır.
- 2) Analitik:** Gerçek zamanlı kullanım verileri, uygulama içi deneyimler, istatistikler, hata ayıklama, kullanıcı etkileşim takibi, cihaz ve ağ verileri, hedef kitle oluşturma, yeniden hedefleme gibi amaçlarla kullanılır.
- 3) Kimlik:** Başka bir platformdaki hesap bilgilerini kullanarak uygulamaya giriş yapılmasını sağlar (Örn: Facebook ile giriş yap).
- 4) Hata raporlama:** Uygulamalar kilitlendiğinde veya çöktüğünde otomatik hata raporlarının oluşturulmasını sağlar.
- 5) Diğer izleyiciler:** Uygulamadaki bilgileri sosyal ağlarda paylaşma, bildirim gönderme, konum verilerini toplama, müşteri ilişkileri yönetimi, rıza yönetimi gibi izleyicilerden oluşmaktadır.

Araştırma kapsamında taranan 72 mobil uygulamanın %72'sinde (n=52) Google FireBase Analytics, %45'inde (n=33) Google Crashlytics, %34'ünde (n=25) Google Analytics ve %33'ünde (n=24) Google AdMob'a ait izleyiciler tespit edilmiştir. Google ürünlerine ait izleyicilerin ardından ise %32 (n=23) ile analitik şirketi Adjust'un yer aldığı görülmüştür.



Tablo 4.11: 72 Mobil Uygulamada En Çok Yer Verilen Üçüncü Taraf İzleyiciler.

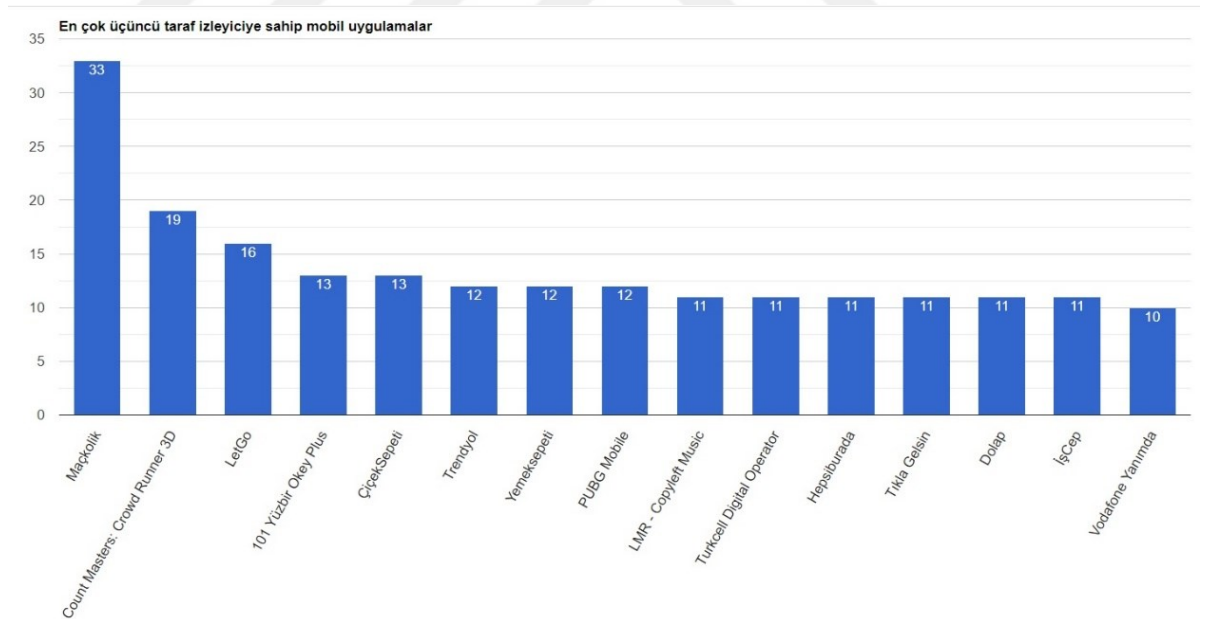
Tablo 4.11'de verilen izleyicilerin tanımları ve kullanım amaçları aşağıdaki gibidir:

- **Google FireBase Analytics:** Kullanıcı etkileşimi ve uygulama kullanımı ile ilgili analitik çözümler sunan ücretsiz bir hizmettir. Analitiğin yanı sıra veri tabanlarına ve hata raporlamalarına erişim sağlanmasına yardımcı olur. Hem kullanıcıların hem de uygulamanın performansı hakkında çözümler sunar.
- **Google CrashLytics:** Uygulamalardaki gerçek zamanlı hataların ortaya çıkarılması, toplanması, analiz edilmesi ve raporlanmasına yardımcı olan bir hizmettir.

- **Google Analytics:** Uygulamaların kullanım performanslarını ölçen ücretsiz bir hizmettir.
- **Google AdMob:** Uygulama içi reklam gösterimi sağlayan bir platformdur. İki reklam hizmeti Google DoubleClick ve AdMob Mediation Google AdMob'un içinde yer alır.
- **Adjust:** Mobil pazarlama analitik platformudur. Kullanıcı davranışlarını ve reklam performanslarını ölçer.
- **Facebook Login:** Kimlik tanımlama hizmetidir. Uygulamaya Facebook hesabı ile giriş yapılması için kullanılan bir yazılım geliştirme kitidir.
- **Facebook Share:** Uygulama içindeki deneyimlerin Facebook'ta paylaşılmasını sağlar.
- **Facebook Analytics:** Uygulama kullanım alışkanlıklarının ve reklam performanslarının ölçümlemesini sağlar. Aynı zamanda Facebook reklamları aracılığıyla kullanıcı yeniden hedefleme gibi hizmetlerin kullanılmasına yardımcı olur.
- **Huawei Mobile Services Core:** Huawei'nin kendi oluşturduğu bir sistemdir. HMS Core, Huawei'nin ortakları ve uygulamala geliştiriciler için yapılmış bir araç koleksiyonudur. İçerisinde reklam, analitik, konum ve benzeri hizmetler vardır.
- **Google Tag Manager:** Uygulamalarda kullanıcı performanslarını ölçümleme ve sonradan onlara erişmek için kullanılan bir hizmettir. Dönüşüm izleme, uygulama analizi, yeniden hedefleme ve birçok hizmeti içinde barındırır.
- **AppsFlyer:** Uygulama optimizasyonu, mobil iş performansını artırma, mobil pazarlama ölçümleme, analitik vb.hizmetler sunan bir şirkettir.
- **Facebook Ads:** Uygulamaların Facebook reklamlarını göstermek için kullandığı hizmettir.
- **New Relic:** Kullanıcıların uygulama kullanım performanslarını izleyen ve buna göre çözümler sunan bir analitik şirkettir.

- **AltBeacon:** Apple iBeacon'un Android versiyonudur. Kişinin fiziksel konumuna dayalı reklam gösterme tekniği olan beacon (işaretçi) reklamcılık için bir protokol özelliği taşımaktadır.
- **AppLovin:** Veriye dayalı mobil reklamcılık şirkettir.
- **Insider:** Cihazlar arası kullanıcı verilerini birbirine bağlayan ve kullanıcıların gelecek davranışlarını tahmin eden bir analitik / reklam şirkettir.
- **Moat Oracle:** Reklam etkinliklerinin ve kampanyaların performanslarının ölçülmesini sağlayan bütüncül bir analitik hizmetidir.

Bazı uygulamalar çeşitli amaçlara yönelik olarak birden çok üçüncü taraf izleyiciye sistemlerinde yer verir. Buna göre araştırma kapsamında taranan uygulamalarda en çok izleyiciye sahip olanlar tablo 4.12'de verilmiştir.



Tablo 4.12: En Çok Üçüncü Taraf İzleyiciye Sahip 15 Mobil Uygulama.

Maçkolik mobil uygulaması 33 adet üçüncü taraf izleyiciye sahip olmasıyla en çok izleyici barındıran uygulama konumundadır. Onu *Count Masters: Crowd Runner 3D* oyunu ve *LetGo* alışveriş uygulaması takip etmektedir.

Söz konusu 15 uygulama kategorilere ayrılarak bakıldığında;

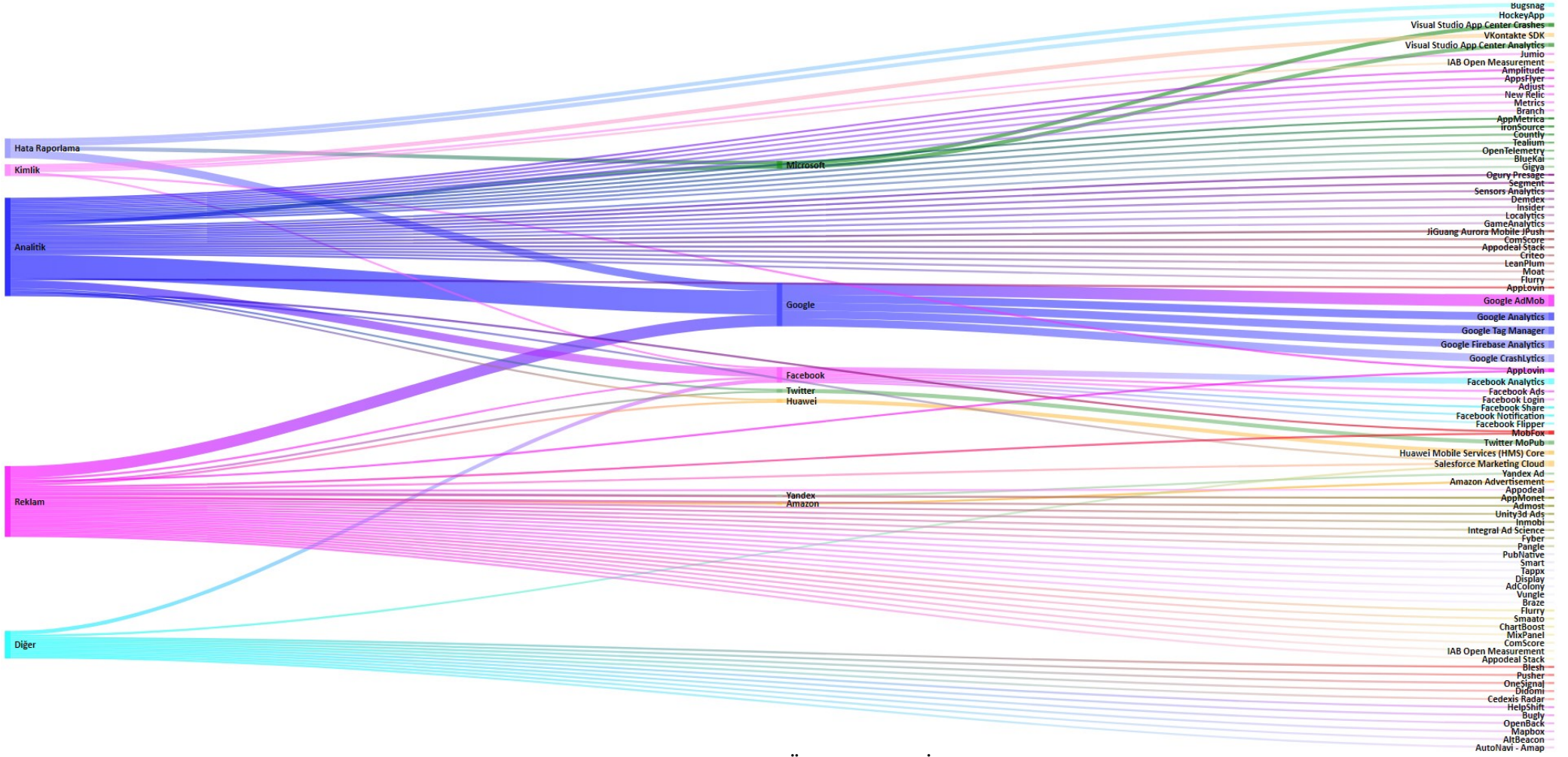
- Alışveriş ve satın almayla ilişkili 7 uygulama (LetGo, ÇiçekSepeti, Trendyol, Yemeksepeti, Hepsiburada, TıklaGelsin, Dolap),
- Oyun oynamayla ilişkili 3 uygulama (Count Masters: Crowd Runner 3D, 101 Yüzbir Okey Plus, PUBG Mobile),
- GSM operatörlüğüyle ilgili 2 uygulama (Vodafone Yanımda ve Turkcell Digital Operator),
- Bankacılıkla ilgili 1 uygulama (İşCep), müzik çalma ile ilgili 1 uygulama (LMR – CopyLeft Music) ve spor ile ilgili 1 uygulama (Maçkolik) şeklinde sıralanmaktadır.

Aşağıda yer verilen tablo 4.13'te araştırma kapsamında yer alan mobil uygulamaların üçüncü taraf şirketlerle veri alışveriş ilişkisi görselleştirilmiştir.

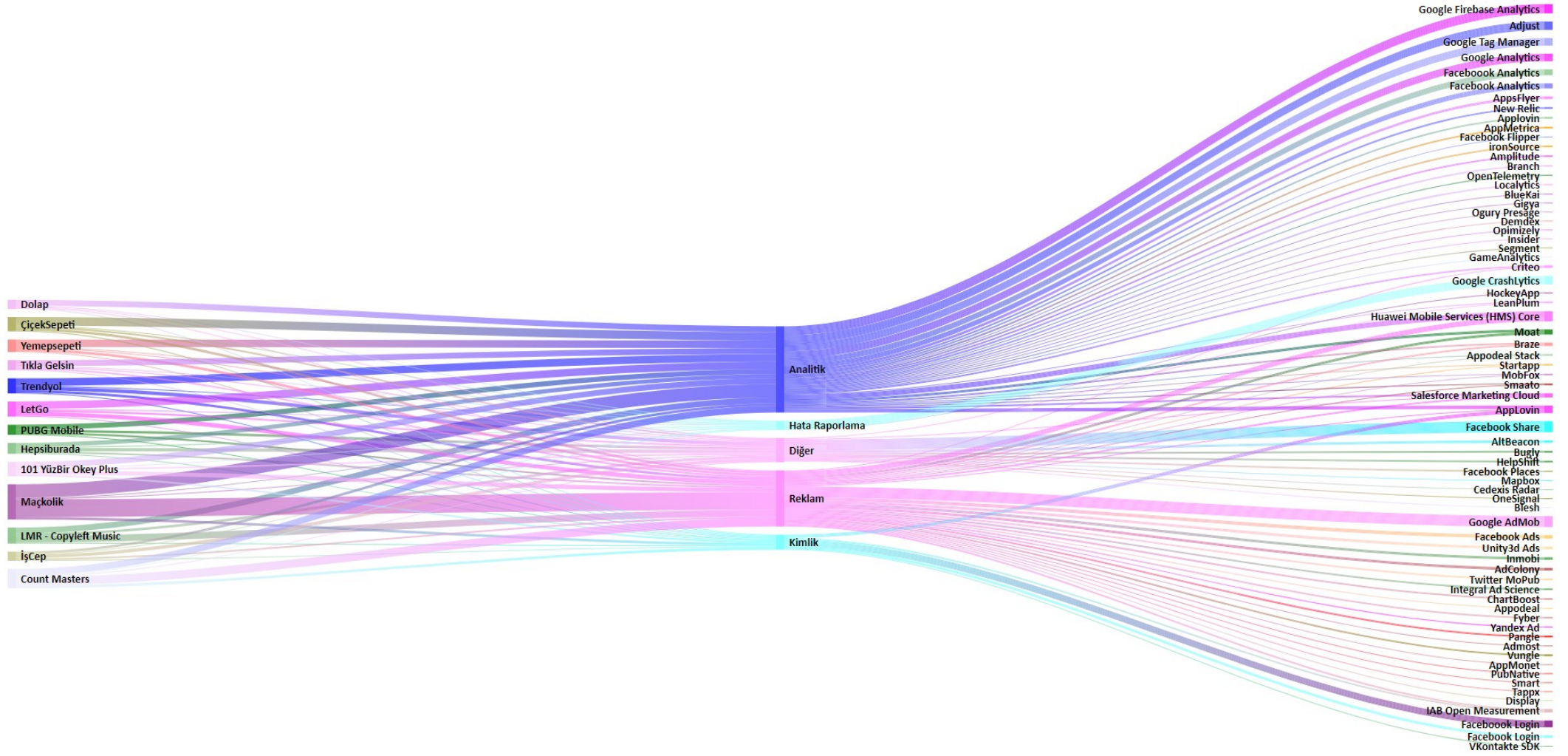
Tablo 4.14'te en çok üçüncü taraf izleyiciye sahip mobil uygulamalar filtrelenmiş ve onların amaçlarına dayalı olarak hangi şirketlere izin verdiği görselleştirilmiştir.

Tablo 4.15'te yalnızca reklam amaçlı üçüncü taraf izleyicileri barındıran uygulamalar ile söz konusu reklam şirketlerinin ilişkisi görselleştirilmiştir.

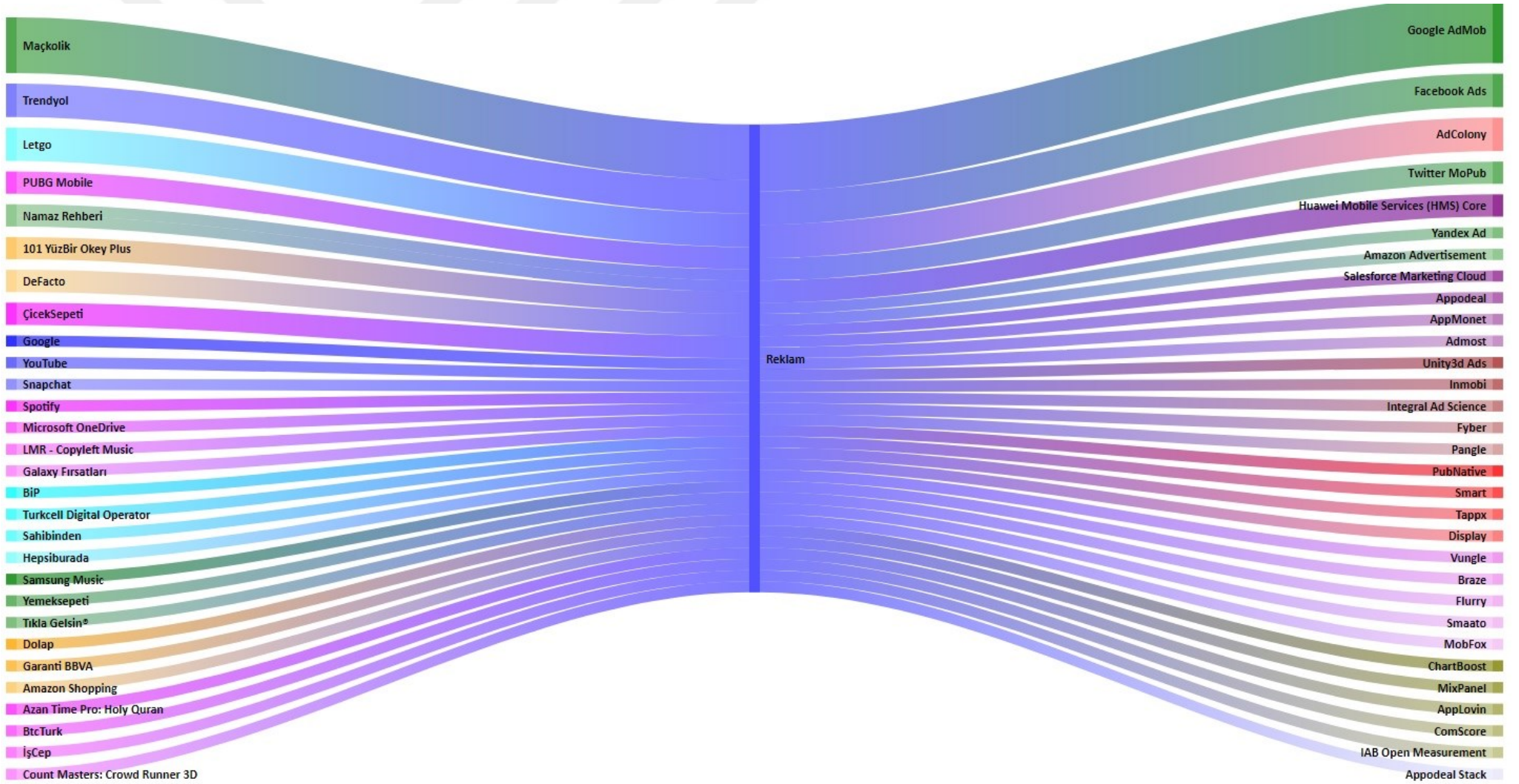
Tablo 4.16'da Google, Facebook, Twitter, Yandex, Huawei ve Amazon gibi büyük teknoloji şirketleri filtrelenerek, onların üçüncü taraf olarak hangi amaçlara dayalı ürünleriyle uygulamalarda yer aldığı görselleştirilmiştir.



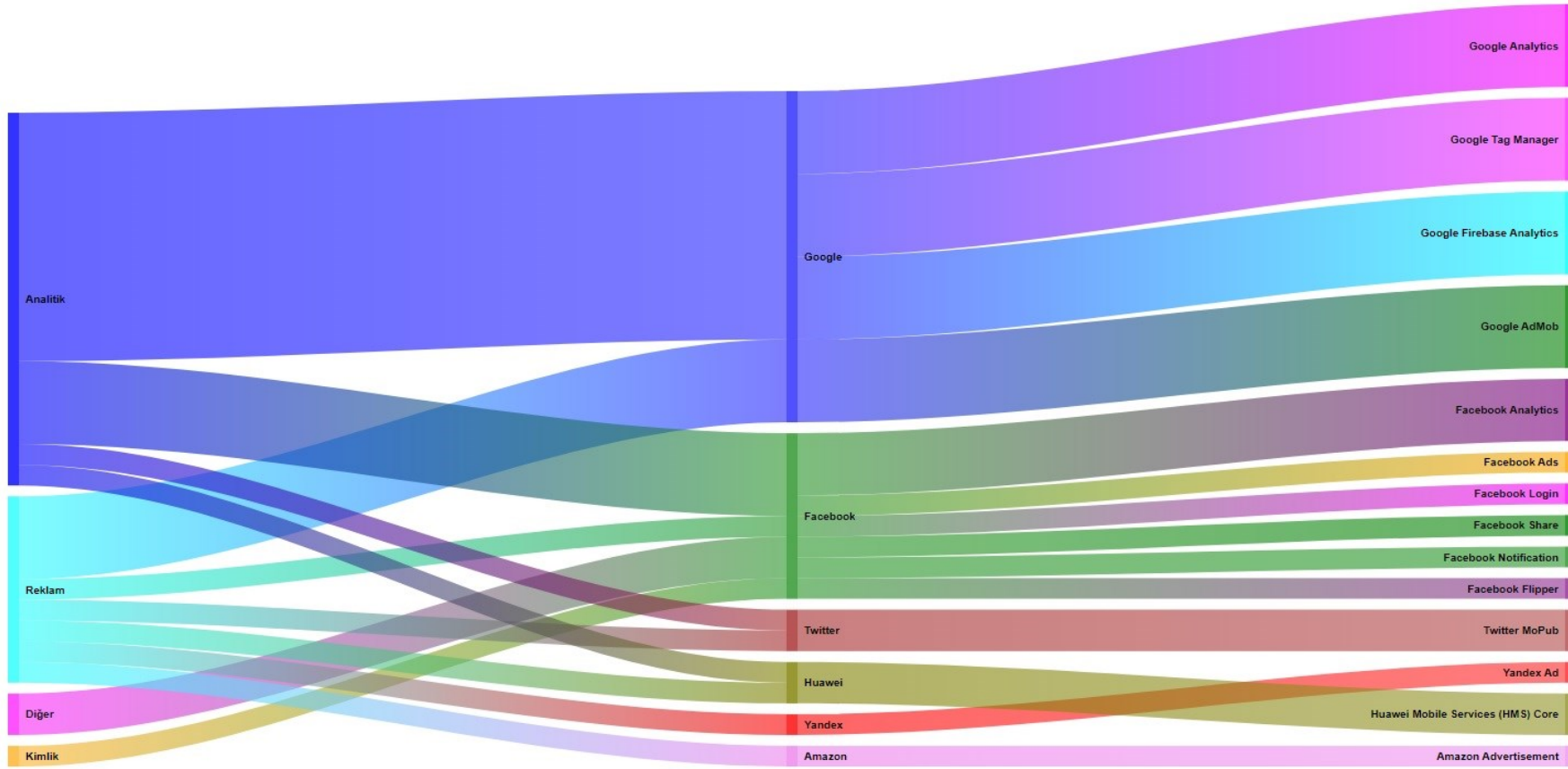
Tablo 4.13: 72 Mobil Uygulamada Tespit Edilen Üçüncü Taraf İzleyicilerin Ağ Haritası.



Tablo 4.14: En Çok Üçüncü Taraf İzleyiciye Sahip Uygulamaların Kimlere Veri Sağladığını Gösteren Ağ Haritası.



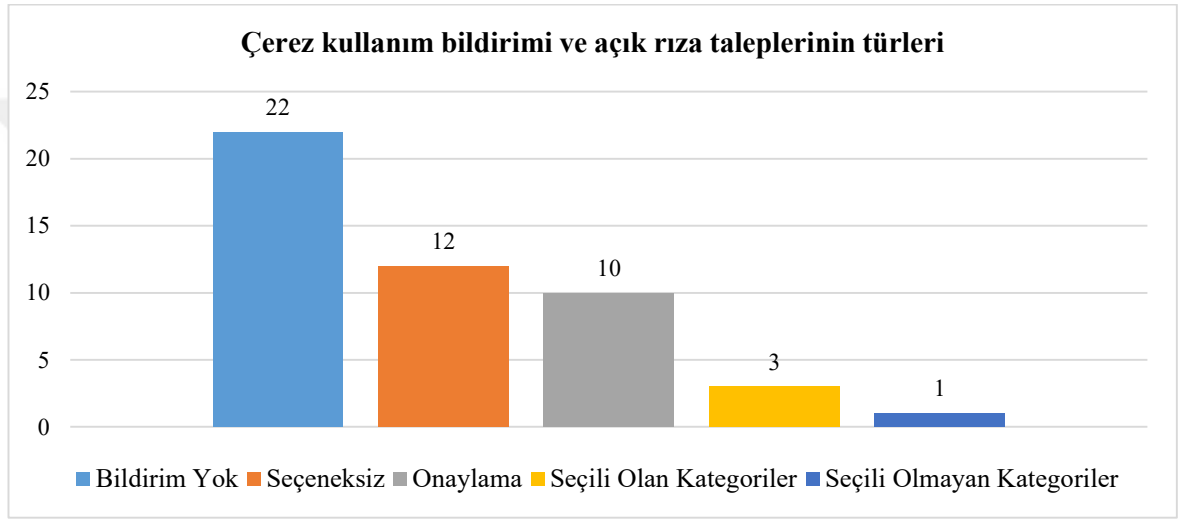
Tablo 4.15: Üçüncü Taraf Reklam İzleyicilere Sahip Uygulamalar ile Veri Paylaştığı Reklam Şirketlerinin Ağ Haritası.



Tablo 4.16: Büyük Teknoloji Şirketlerinin Üçüncü Taraf Olarak Uygulamalarda Hangi Amaçlar ve Ürünlere Yer Aldığını Gösteren Diyagram.

4.3.1.3. Web Sitelerinin Açık Rıza Alma Biçimleri

Araştırma kapsamındaki 48 web sitesinin çerez kullanımına ilişkin kullanıcıları nasıl bilgilendirdiği ve/veya kullanıcıları izlemek için hangi tür bir şablonla açık rıza talep ettikleri araştırılmıştır. Araştırma sonucu, Utz ve arkadaşlarının (2019) önerdiği rıza talep örnek sınıflandırmasına¹⁸ göre ayrılarak tablo 4.17’de verilmiştir.



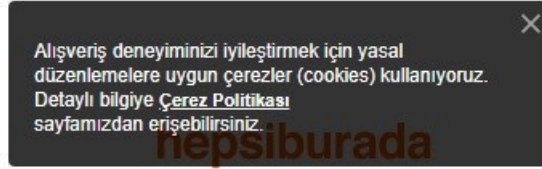
Tablo 4.17: 48 Sitenin Çerez Kullanım Bildirimi ve Açık Rıza Taleplerinin Türleri.

Bildirim Yok: 22 sitede kullanıcı siteyi ziyaret ettiği anda birinci veya üçüncü taraf çerez kullanımına, aydınlatma beyanına, veri politikasına veya gizlilik sözleşmesine yönelik hiçbir bildirim sunulmamaktadır. Bunların arasında kendisini ziyaret eden kullanıcının cihazına 132 adet üçüncü taraf çerez yerleştirdiği tespit edilen *cumhuriyet.com.tr*; 123 adet üçüncü taraf çerez yerleştirdiği tespit edilen *nefisyemektarifleri.com* gibi siteler yer almaktadır. Diğer yandan Google, YouTube ve

¹⁸ Bkz.: 3.4.1. Yönlendirici Tasarımlar: Çerez Onay Kutu Tasarımları ve Açık Rızaya Etkileri

Instagram gibi platformlar da bu listeye dâhildir. VPN¹⁹ ile söz konusu platformlara girildiğinde ise çerezlere ve gizlilik sözleşmesine ilişkin bir bildirim çıkmaktadır.

Seçeneksiz: 12 web sitesinde kullanıcıya çerez yönetimi için herhangi bir seçeneğin sunulmadığı, yalnızca çerezlerin kullanıldığının bildirildiği bir sistem yer almaktadır. Bu sistemi kullanan siteler genellikle “*Bu hizmeti kullanarak çerez politikasını kabul etmiş sayılırsınız*” ifadesini kullanmaktadır. Hepsiburada, n11, GittiGidiyor gibi e-ticaret sitelerinin yanı sıra Sabah, Onedio, Haberler.com, Ensonhaber gibi haber siteleri de kullanıcıya yalnızca bilgi vererek çerezleri aktif hâle getirmektedir.



Grafik 4.1: Seçeneksiz Çerez Bildirimi Örneği.
(hepsiburada.com, ekran görüntüsü tarihi: 25 Kasım 2021)

Onaylama: Kullanıcıya sadece sözleşmeyi onaylaması için seçenek sunan sistemlerdir. 10 web sitesi bu yöntemle kullanıcıların açık rızalarını almaktadır. Trendyol, Sahibinden, Ekşi Sözlük, Habertürk, NTV, Mynet, Donanımhaber ve İnternethaber gibi siteler onaylama sistemini kullanmaktadır.

Ntv.com.tr diğerlerinden farklı olarak onaylama butonunun adını “Kabul Et” veya “Onayla” değil, “Okudum” şeklinde kullanıcılara sunmaktadır.



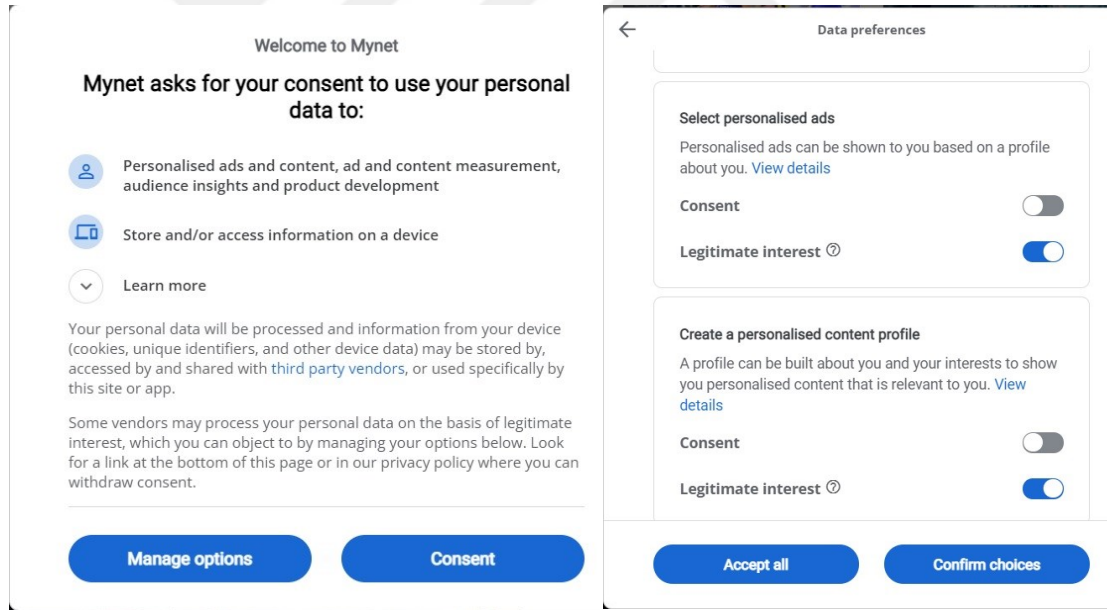
Grafik 4.2: Onaylama Bildirim Mantığı ve “Okudum” Butonu (Ntv.Com.Tr).
(ekran görüntüsü tarihi: 23 Kasım 2021)

¹⁹ Tür: Sanal özel ağ. Fiziksel bir ağa bağılıymış gibi yapan ve o ağa bağılı olarak veri alışverişinde bulunulan sistemdir. Araştırmada VPN, farklı ülke sunucularıyla ilgili web sitelerini ziyaret etme amaçlı kullanılmıştır.

Bu kategoride bir diğer dikkat çeken web sitesi *mynet.com*'a aittir. Mynet, Türkiye'den gelen ziyaretçilere onaylama bildirim sistemini sunarken, yurt dışından girenlere seçeneklerin çok olduğu ve detaylı şekilde bilgilendirmenin yapıldığı bir açık rıza talep kutusu sunmaktadır.



Grafik 4.3: Mynet.com Adresini Türkiye'den Ziyaret Eden Bir Kullanıcının Karşılaştığı Onaylama Bildirim Kutusu.
(ekran görüntüsü tarihi: 25 Kasım 2021)

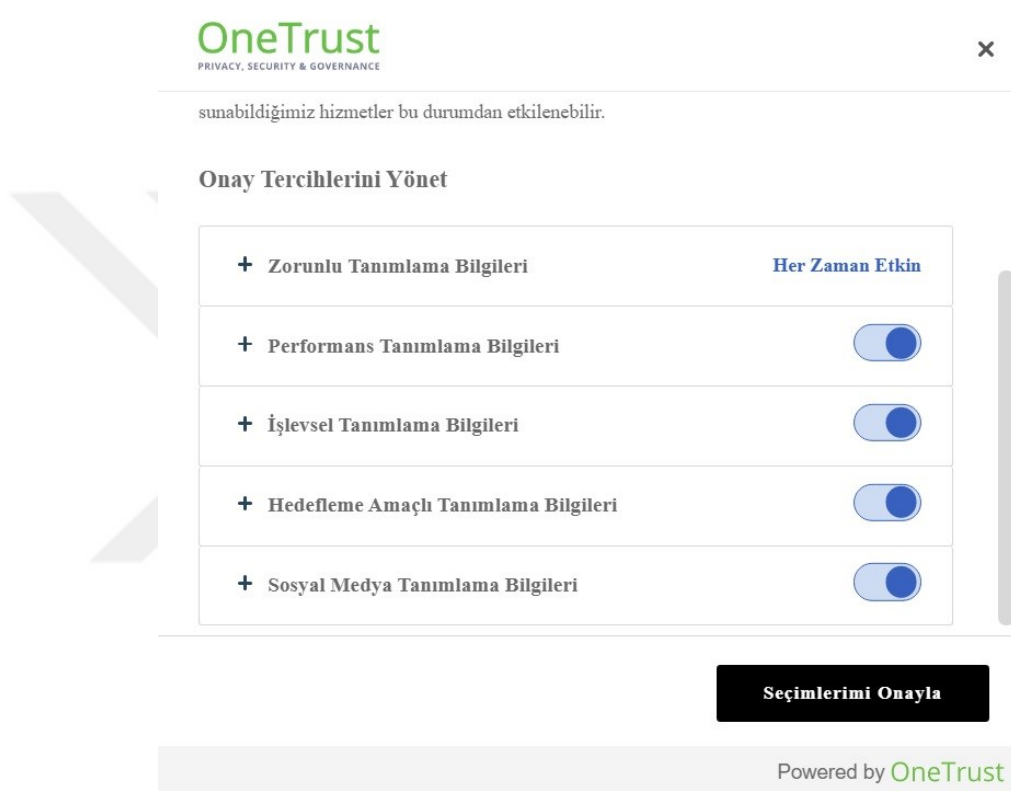


1) Yurt dışından mynet.com'u ziyaret eden bir kullanıcı ilk önce bu pencereyle karşılaşır. *Consent* butonuna basıldığında açık rıza alınır. *Manage options* butonunda ise sağ taraftaki 2 numaralı pencere açılır.

2) *Manage options* butonuna tıklayan kullanıcı burada çerez kullanımıyla ilgili detaylı olarak bilgilendiriliyor ve çeşitli bağlamlarda toplanan verilerinden istediğini özgür biçimde kısıtlayabiliyor veya izin verebiliyor.

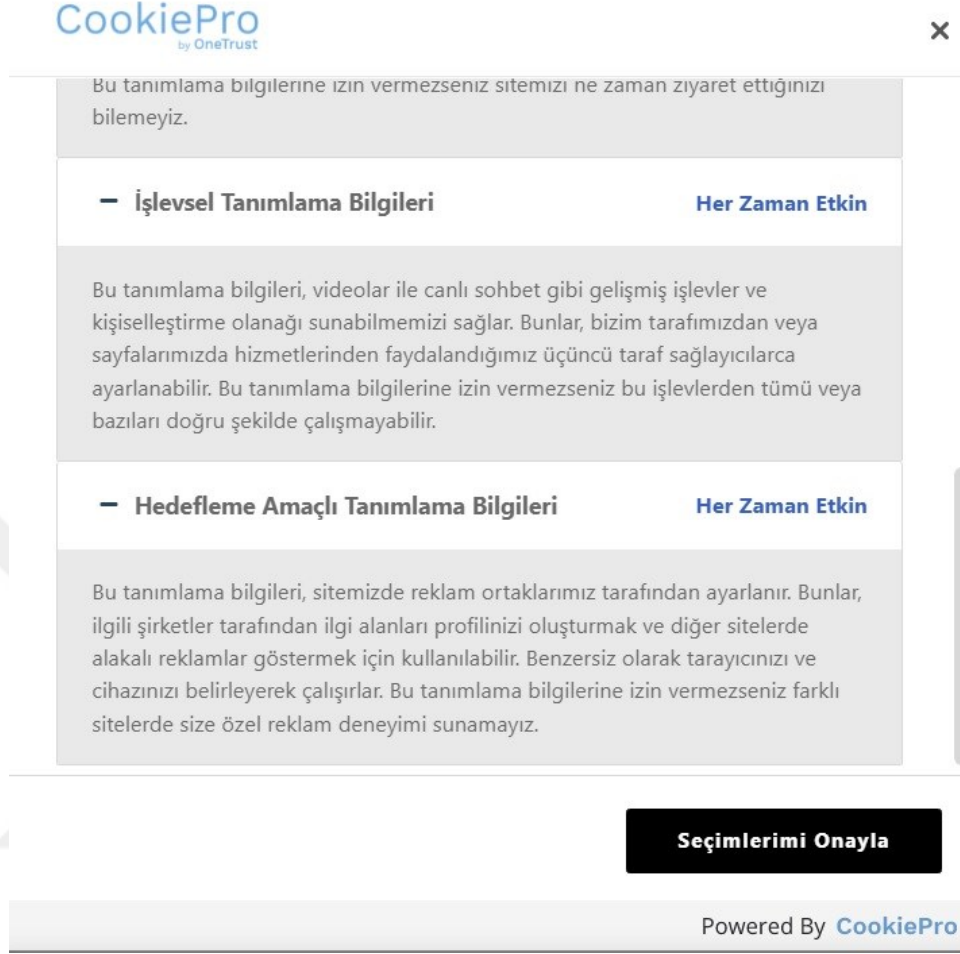
Grafik 4.4: Mynet.com Adresini Yurt Dışından Ziyaret Eden Bir Kullanıcının Karşılaştığı Onaylama Bildirim Kutuları.
(ekran görüntüsü tarihi: 25 Kasım 2021)

Seçili Olan Kategoriler: Hürriyet, Milliyet ve Sözcü gazetelerinin web sayfaları kullanıcılara çerez kategorilerinin önceden seçili olarak sunmaktadır. 3 sitede de çerez bildirim kutusunda “Kabul Et” butonu ve yanında “Seçenekler” bağlantısı yer almaktadır. Seçenekler bağlantısına tıklandığında çerez kategorilerinin hepsi aktif olarak kullanıcının karşısına çıkmaktadır.



Grafik 4.5: Çerez Kategorilerinin Hazır Seçili Olarak Sunulmasına Bir Örnek.
(hurriyet.com.tr, ekran görüntüsü tarihi: 15 Kasım 2021)

Hürriyet ve Milliyet çerez kategorilerini hazır seçili olarak kullanıcılara sunmasına rağmen yine de onlara bu seçenekleri pasif hâle getirme olanağı sunmaktadır. Oysaki Sözcü gazetesine baktığımızda çerez kategorileri tek taraflı olarak aktif haldedir.



Grafik 4.6: Çerez Kategorilerinin Listelenmesi.
(sozcu.com.tr, ekran görüntü tarihi: 28 Kasım 2021)

Bu grafikte görüldüğü gibi Sözcü gazetesi çerez bilgilendirme ekranında tüm kategoriler “her zaman etkin” olarak işaretlenmiştir. Bu etkin olma durumu kullanıcı tarafından hiçbir şekilde değiştirilememekte ve kullanıcıya yalnızca “seçimlerimi onayla” butonuna basma seçeneği sunulmaktadır.

Seçili Olmayan Kategoriler: Bu türde yalnızca Amazon yer almaktadır. Amazon.com.tr adresini ziyaret eden bir kullanıcı “Çerezleri Özelleştir” ve “Çerezleri Kabul Et” şeklinde iki seçenekle karşılaşmaktadır. Çerezleri Özelleştir seçeneğine tıklandığında çerez kategorileri seçili olmayan / pasif şekilde kullanıcının karşısında çıkmaktadır.

Reklam Çerezleri

☐ Açık ☒ Kapalı

Ayrıca çerezleri, Amazon'da bulunmayan ürün ve hizmetler ve ilgilerinize ilişkin belirli reklamlar da dahil olmak üzere belirli reklam türlerini sunmak için kullanılmaktadır. Amazon hizmetlerini kullanırken etkileşimde bulunduğunuz onaylı üçüncü taraflar da çerez bırakabilir. Üçüncü taraflar, ilgilerinize ilişkin reklamlar dâhil olmak üzere içerik sunma, reklamlarının etkililiğini ölçme ve Amazon adına hizmetler yürütme süreci sırasında çerez kullanır.

Amazon'un ilgiye ilişkin reklamları nasıl sağladığı konusunda daha fazla bilgi edinmek için lütfen [İlgiye İlişkin Reklamlar bildirimine](#) bakın. İlgiye ilişkin reklam tercihlerinizi ayarlamak için lütfen [Reklamcılık Tercihleri](#) sayfasına gidin.

Tanıtım Çerezlerini Özelleştir

Amazon Reklamları

☐ Açık ☒ Kapalı

Onaylı Üçüncü Taraf Reklamları

☐ Açık ☒ Kapalı

Grafik 4.7: Çerez Kategorilerinin Pasif Olarak Sunulmasına Bir Örnek.
(amazon.com.tr, ekran görüntüsü tarihi: 17 Kasım 2021)

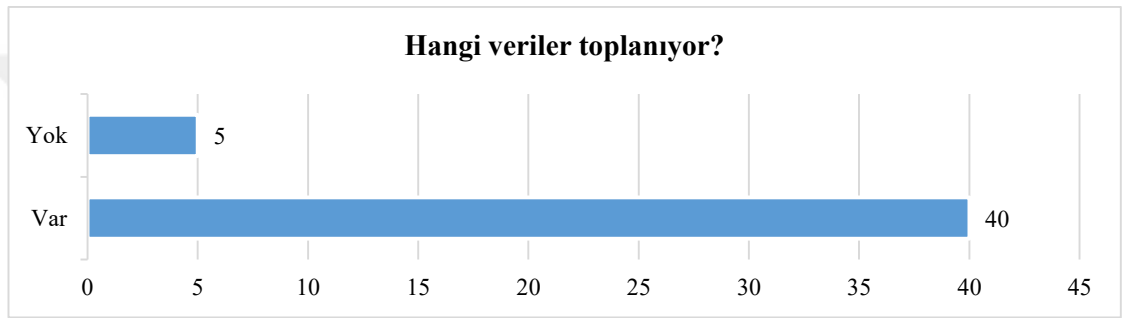
48 web sitesi dikkate alındığında kullanıcıya aktif bir davranış sergileyerek açık rıza vermesi için imkân sunan tek sitenin *amazon.com.tr* olduğu ortaya çıkmaktadır.

4.3.1.4. Web Sitelerinin Çerez Politikaları ve Gizlilik Sözleşmelerinin İçerik Analizi

Web sitelerinin çerez politikaları ve gizlilik sözleşmeleri kullanıcı ve site arasındaki ilişkiyi düzenleyen, sitelerin sorumluluklarını belirleyen ve genellikle hukukçular tarafından oluşturulan yasal belgelerdir. Belgelerde sitelerin kendi hak ve sorumluluklarının yanı sıra kullanıcılara ait haklar da yer almaktadır. Bu hakların en başında kullanıcıların verileri üzerinde kontrol sağlamalarına yardımcı olacak bilgiler gelmektedir. Ayrıca sözleşmeler veri güvenliği, gizliliği, üçüncü taraflarla paylaşımı ve hangi enstrümanlar aracılığıyla hangi verilerin toplandığı gibi önemli açıklamaları da kapsamaktadır.

Araştırma kapsamında yer alan 48 web sitesinin 3'ünde (yabancidizi.pw, meb.gov.tr ve eba.gov.tr) çerez politikası veya gizlilik sözleşmesi bulunamamıştır. Bu nedenle 45 web sitesinin çerez politikası ve gizlilik sözleşmesi içerik analizi yöntemiyle incelenmiştir. Yasal düzenlemeler, veri gizliliği, veri güvenliği ve mahremiyet başlıkları dikkate alınarak çerez politikalarında ve kullanıcı gizlilik sözleşmelerinde yedi soruya cevap aranmış ve bu çerçevede analiz gerçekleştirilmiştir.

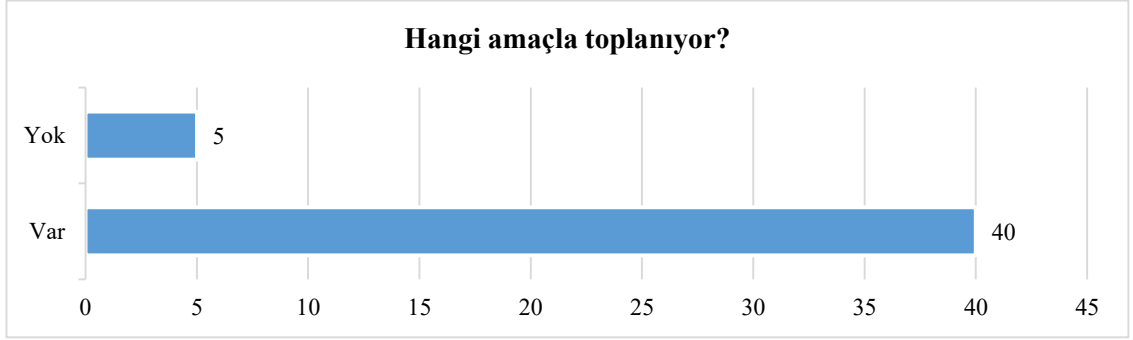
1) Hangi veriler toplanıyor?



Tablo 4.18: Hangi Verilerin Toplandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

Sözleşmelerde ilk olarak hangi kişisel verilerin toplandığında dair metinler aranmıştır. Yalnızca çerezlerin ve izleme teknolojilerinin hangi kullanıcı verilerini topladığı değil, aynı zamanda sitede yer alan formlar aracılığıyla da nelerin toplandığı incelenmiştir. IP adres, siteyi ziyaret saati, hangi cihazla sitenin ziyaret edildiği veya formlardan toplanan ad, soyad, e-posta adresi gibi verilerin sözleşmelerde yer alması yeterli kabul görülmüştür. Bu çerçeveden bakıldığında 40 sitenin hangi verileri topladığını belirttiği, 5 sitede ise yeterli bilginin yer almadığı görülmüştür.

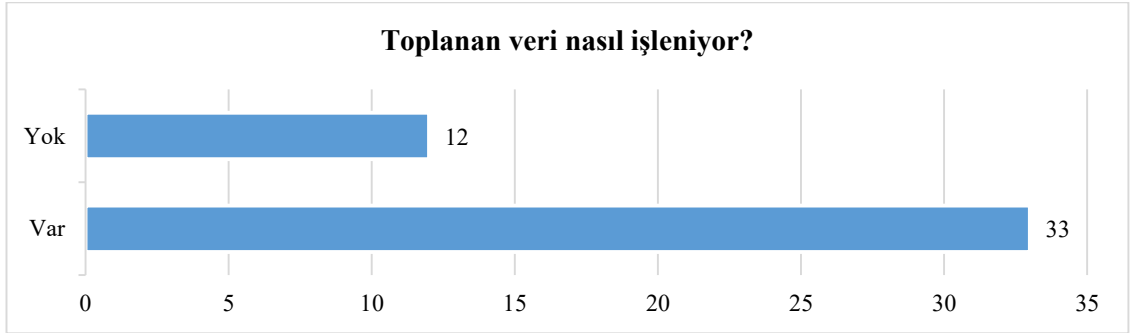
2) Veriler hangi amaçla toplanıyor?



Tablo 4.19: Verilerin Hangi Amaçla Toplandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

Veriler kişiselleştirilmiş reklam, pazarlama faaliyetleri, site performansını arttırma, kullanıcı deneyimini iyileştirme, istatistik ve analitik gibi nedenlerle toplanabilmektedir. Bunlar ve benzer amaçlarla verilerin toplandığıyla ilgili 40 sitede çeşitli metinler yer almaktadır. İnternethaber, Donanımhaber ve Haber7 gibi siteler de dâhil olmak üzere 5 sitede verilerin hangi amaçla toplandığı bilgisine ulaşılammıştır.

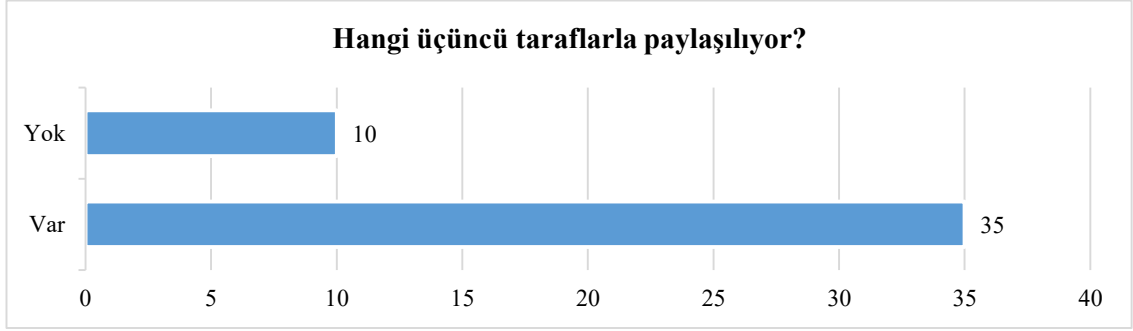
3) Toplanan veriler nasıl işleniyor?



Tablo 4.20: Verilerin Nasıl İşlendiği Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

33 sitenin gizlilik sözleşmesinde toplanan verilerin nasıl işlendiği ve/veya işleme süreçlerinin nasıl gerçekleştiğiyle ilgili en temel düzeyde de olsa bilgiler yer almaktadır. 12 sitede verilerin işlenmesiyle ilgili bilgi tespit edilememiştir.

4) Veriler hangi üçüncü taraflarla paylaşıyor?



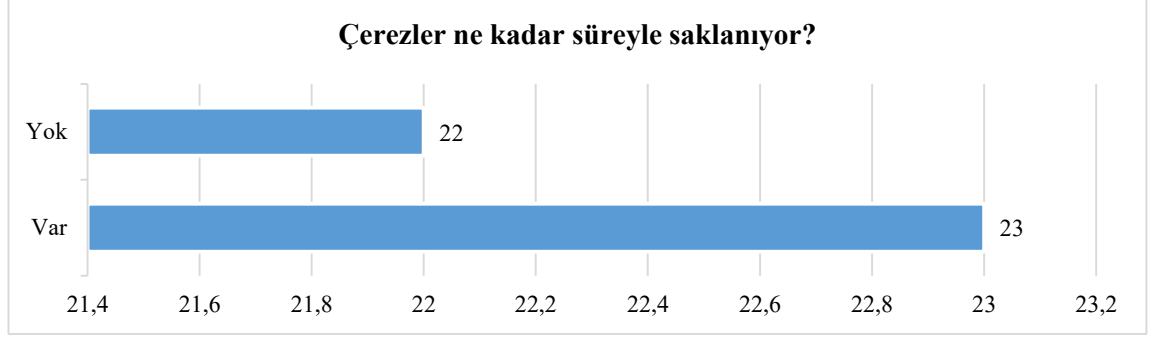
Tablo 4.21: Verilerin Hangi Üçüncü Taraf Şirket veya Sektörlerle Paylaşıldığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

35 sitenin sözleşmesinde hangi şirketlere veya sektörlerle hangi amaçlarla kullanıcı verilerinin paylaşıldığının bilgisine yer verilmiştir. Fakat bu sitelerin büyük bir kısmı bizzat üçüncü taraf şirketlerin isimlerini yazmaktan ziyade “iş ortaklarımız, reklam şirketleri, sosyal medya platformları, analitik bilgi toplayan hizmet sağlayıcılar” vb. ifadeler kullanarak üçüncü tarafları sektör bazında belirtmektedir. Habertürk’ün çerez politikasında ise üçüncü taraf şirketlerin kimler olduğu teker teker açıklanmıştır.

AppNexus	Reklam çerezi	Vazgeç	Gizlilik politikası
Comscore	Performans çerezi	Vazgeç	Gizlilik politikası
Facebook pixel	Reklam çerezi	Vazgeç	Gizlilik politikası
Google Adwords	Reklam çerezi	Vazgeç	Gizlilik politikası
Google Adx	Reklam çerezi	Vazgeç	Gizlilik politikası
Google Analytics	Performans çerezi	Vazgeç	Gizlilik politikası
Google DoubleClick	Reklam çerezi	Vazgeç	Gizlilik politikası
Microsoft Bing	Reklam çerezi	Vazgeç	Gizlilik politikası
Nielsen	Reklam çerezi	Vazgeç	Gizlilik politikası
OpenX	Reklam çerezi	Vazgeç	Gizlilik politikası
Twitter	Reklam çerezi	Vazgeç	Gizlilik politikası
Admost	Reklam çerezi	Vazgeç	Gizlilik politikası
Adocean	Reklam çerezi	Vazgeç	Gizlilik politikası
Gemius	Performans çerezi	Vazgeç	Gizlilik politikası
Reklamport	Reklam çerezi	Vazgeç	Gizlilik politikası
Adform	Reklam çerezi	Vazgeç	Gizlilik politikası

Grafik 4.8: Haberturk.com’un Çerez Politikasında Yer Alan Üçüncü Taraf Şirketlerin Listesi.

5) Çerezler ne kadar süreyle saklanıyor?



Tablo 4.22: Çerezlerin Ne Kadar Süreyle Saklandığı Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

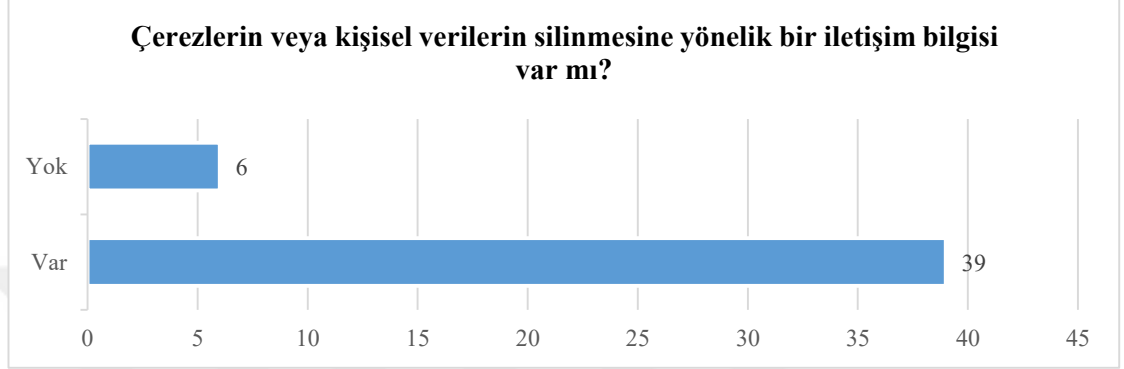
Yalnızca 23 sitede yerleştirilen çerezlerin ne kadar süreyle cihazda kalacağına dair bilgiye yer verilmiştir. Örneğin, Grafik 4.9’da doviz.com’un çerez politikasında yer alan üçüncü taraf çerezler ve cihazda saklanma süreleri gösterilmektedir. Öte yandan 22 sitede Grafik 4.9’dakine benzer çerezlerin ne kadar süreyle saklanacağına dair şeffaf bir bilgiye rastlanmamıştır.

Google Analytics	_ga	Ölçümlemelerde kullanmak üzere kullanıcıyı tanımlamak amacıyla kullanılır.	Performans ve Analiz Çerezleri	2 Yıl
Google Analytics	_gat_dovizcom_web	Ölçümleme amaçlı gönderilen isteklerin sıklığını kontrol altında tutmak amacıyla kullanılır.	Performans ve Analiz Çerezleri	1 Dakika
Google Analytics	_gid	Ölçümlemelerde kullanmak üzere kullanıcıyı tanımlamak amacıyla kullanılır.	Performans ve Analiz Çerezleri	24 Saat
Criteo	uid	Kullanıcı verisini reklam amaçlı tutabilmek için kullanılır.	Reklam Çerezleri	400 Gün
Criteo	optout	Kullanıcı verisinin işlenmemesi gerektiğini hatırlamak amacıyla kullanılır.	Reklam Çerezleri	3 Yıl
DoubleClick	IDE	Kullanıcı verisini reklam amaçlı tutabilmek için kullanılır.	Reklam Çerezleri	2 Yıl
DoubleClick	DSID, FLC, AID, TAID, and exchange_uid	Kullanıcı verilerinin cihazlar arası aktarılabilmesi amacıyla kullanılır.	Reklam Çerezleri	1 saat

Grafik 4.9: Doviz.com’un Çerez Politikasında Yer Alan Çerez Listesi.

(ekran görüntüsü tarihi: 28 Kasım 2021)

6) Çerezlerin veya kişisel verilerin silinmesine yönelik bir iletişim bilgisi var mı?



Tablo 4.23: Çerezlerin veya Kişisel Verilerin Silinmesi İçin Bir İletişim Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

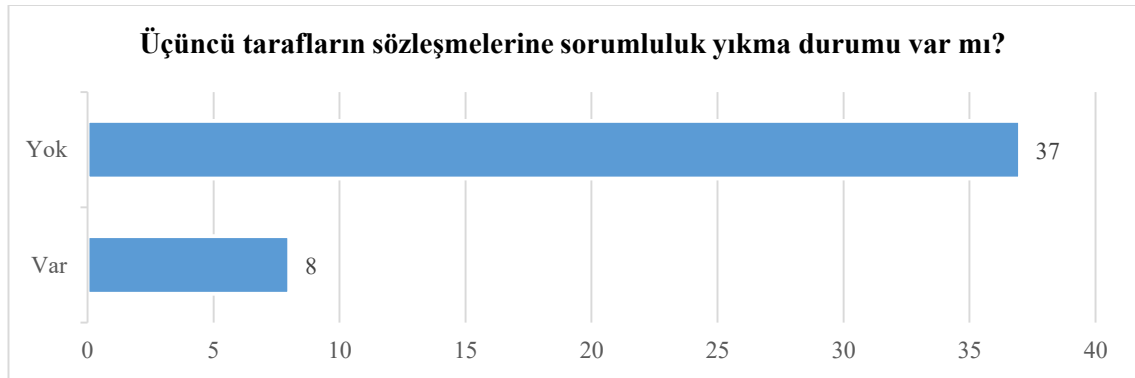
39 sitede kişisel verilerin silinmesini talep etmek için bir iletişim bilgi yer almaktadır. Bu noktada sözleşmelerde çerezlerin silinmesi ve kişisel verilerin silinmesi genellikle birbirinden ayrılmaktadır. Söz konusu sitelerde kullanıcıların oluşturdukları talep veya doldurdıkları formlar aracılığıyla toplanan ad, soyad, e-posta veya telefon numarası gibi kişisel verilerin silinmesi için kurumsal bir e-posta ve mektup adresi tanımlanmıştır. Diğer yandan üçüncü taraf çerezlerin kaldırılması veya reddi için sıklıkla tarayıcılarda çerezlerin nasıl engellenebileceği ve nadiren farklı çevrim içi kanallardan çerezleri nasıl iptal edebileceklerine ilişkin bilgiler paylaşılmıştır. Sözleşmelerde çerezlerden kurtulmak için en sık paylaşılan çevrim içi kanallardan üçü optout.aboutads.info, optout.networkadvertising.org ve youradchoices.com siteleridir. Bu siteler veri toplayan birçok üçüncü taraf şirketi içinde barındıran ve kullanıcılara şirketlerin bir listesini sunarak onların takibinden kaçınmasına yardımcı olan sitelerdir. Fakat bu platformların gerçekten işe yarayıp yaramadığına yönelik yeterli bir veri bulunamamıştır.

Şirket	Etkin/Devre Dışı	Status	Bilgi
1plusX	☐ Etkin ☒ Devre Dışı	✗	▼
4W MARKETPLACE SRL	☒ Etkin ☐ Devre Dışı	✓	▼
ADEX	☒ Etkin ☐ Devre Dışı	✓	▼
Adform	☒ Etkin ☐ Devre Dışı	✓	▼
AdGear	☒ Etkin ☐ Devre Dışı	?	▼
ADITION	☒ Etkin ☐ Devre Dışı	✓	▼
Adobe	☒ Etkin ☐ Devre Dışı	✓	▼
advanced store	☒ Etkin ☐ Devre Dışı	✓	▼
Amazon Ad System	☐ Etkin ☒ Devre Dışı	✗	▼
Amobee	☒ Etkin ☐ Devre Dışı	✓	▼
Beeswax	☒ Etkin ☐ Devre Dışı	✓	▼
Captify	☒ Etkin ☐ Devre Dışı	✓	▼
Criteo	☐ Etkin ☒ Devre Dışı	✗	▼
Delta Projects	☒ Etkin ☐ Devre Dışı	✓	▼
Disqus	☒ Etkin ☐ Devre Dışı	✓	▼

Grafik 4.10: EDAA (Avrupa İnteraktif Dijital Reklam Birliği) Tarafından Oluşturulan Youronlinechoices Web Sitesinde Yer Alan Şirketler ve Kullanıcıya Sunduğu Seçenekler.

(Kaynak: youronlinechoices.com/tr/reklam-tercihleriniz)

7) Üçüncü taraf sözleşmelere sorumluluk yıkma durumu?



Tablo 4.24: Sitesinde Üçüncü Tarafların Sözleşmelerine Sorumluluk Verme Bilgisinin Çerez ve Gizlilik Sözleşmelerindeki Varlığı.

Bu başlıkta üçüncü taraf çerezlere sitesinde yer veren, fakat ileride söz konusu taraflarca yaşanabilecek bir risk, sızıntı veya ifşa durumlarında hiçbir mesuliyet kabul etmediğini sözleşmelerinde açıkça ifade eden siteler yer almaktadır. Diğer bir ifadeyle, 8 site kendi sitelerinden üçüncü tarafların topladığı kullanıcı verilerini kötü amaçlı

kullanması veya çeşitli ihlallere uğratması durumunda sorumluluk almamaktadır. Sözleşmelerdeki örnek ifadeler aşağıdaki gibidir:

“Bununla birlikte, kişisel verileri alan üçüncü kişinin veri koruma politikalarından dolayı ve üçüncü kişinin sorumluluğundaki risk alanında meydana gelen ihlallerden Trendyol sorumlu değildir.” (Trendyol)

“Üçüncü partiler tarafından işletilen site ve web mülkiyetleri (her çeşit uygulamalar dâhil olmak üzere, ancak bunlarla sınırlı olmaksızın) dâhil olmak üzere, üçüncü partilerin gizlilik, bilgi ve diğer uygulamaları, işbu Politika kapsamında değildir ve bu uygulamalardan dolayı sorumlu tutulamayız.” (Mynet)

“Söz konusu üçüncü tarafların gizlilik uygulamalarından TikTok sorumlu değildir ve söz konusu üçüncü tarafların veri uygulamaları, bu Gizlilik Politikası kapsamında değildir.” (TikTok)

“Üçüncü kişi çerezler, üçüncü kişi gizlilik politikası kapsamındadır.” (GittiGidiyor)

Örneklerde görüldüğü gibi dışarıdan gelen üçüncü taraf çerezlerin topladığı verilerin akıbeti ile ilgili üçüncü taraf şirketlerin sözleşmelerinde ne yazdığına bağlıdır.

4.3.1.4.1. Çerez Politikası ve Gizlilik Sözleşmeleriyle İlgili Genel İzlenimlerin Oluşturduğu Bulgular

Çerez ve gizlilik sözleşmeleri adından anlaşıldığı gibi çerez kullanımının nasıl olduğu ve kullanıcı güvenliği / gizliliği hakkında düzenlemeleri içermektedir. Bazı sözleşmeler gözetimi ve veri alışverişini sıradanlaştırmakta, bazıları kullanıcılara seçme özgürlüğü tanıdığını beyan ederken bunu nasıl yapabilecekleri konusunda bir alan oluşturmamakta, bazı sözleşmeler ise ülkelere göre değişebilmektedir. Bu başlıkta sözleşmeler analiz edilirken karşılaşılan farklı durum ve problemlerle ilgili tespitlere yer verilmektedir.

TikTok’un çerez politikasındaki çerez kullanımının Türkiye’de başka, yurt dışında başka biçimde olmasıyla başlayabiliriz. TikTok’un sözleşmesinde *“Platform’u kullanmanız hâlinde, Çerez kullanımımıza onay vermiş sayılırsınız.”* ifadesine yer

verilmiştir. Oysa VPN ile Avrupa ülkesindeymiş gibi platform ziyaret edilip sözleşmeye bakıldığında ifade değişmektedir: *“We ask for your consent to access or use your information for specific purposes. If we do, you’ll always be able to revoke your consent through the device permissions or in-app settings.”* Açıkça görülüyor ki Türkiye’den gelen ziyaretçiler otomatik olarak çerez kullanımına maruz kalırken, GDPR’a tabi ülkelerden yapılan ziyaretlerde çerez kullanımı için kullanıcıların açık rızası aranmaktadır.

Üçüncü tarafların bağlı oldukları birçok site ve mobil uygulamadan kullanıcılar hakkında topladıkları verileri kendi sahip olduklarıyla birleştirerek daha detaylı bir kullanıcı profili oluşturdukları bilinmektedir. Bu duruma ilişkin bir metne GittiGidiyor’un çerez politikasında rastlanmıştır:

“Facebook ve Google Sitemiz üzerinden topladığı verileri kendi verileriyle eşleştirebilir ve elde ettiği kişisel verileri kendi gizlilik politikalarına göre işleyebilir.”

Buna göre Facebook ve Google, kullanıcıların GittiGidiyor’da hangi ürüne ne kadar baktıkları, neyi satın aldıkları, siteye hangi konumdan hangi cihazla saat kaçta bağlandıkları, hangi ürünleri sepete veya favorilere ekledikleri gibi verilere erişebilmektedir. Seçeneksiz bir çerez bildirimine sahip GittiGidiyor ise bu verilerin kullanıcılardan habersiz olarak toplanmasına aracılık etmekte; ayrıca platformların o kullanıcılar hakkında detaylı bir profil çıkartmalarına yardımcı olmaktadır.

Benzer bir ifade onedio.com’da da yer almaktadır:

“Onedio’nun sosyal ağların eklentiler aracılığıyla işlediği veriler üzerinde herhangi bir kontrolü yoktur.”

Onedio sitesi özellikle kullanıcılara sunduğu eğlenceli testlerle onların sitede “keyifli zaman” geçirmesini sağlayan içerikler üretmektedir. Bu testler yemek, psikoloji, astroloji, ilişki, karakter ve genel kültür gibi geniş bir yelpazeden oluşmaktadır. Bu testlerde işaretlenen cevaplar kullanıcıların ruhsal ve fiziksel durumları hakkında birçok veriyi açığa çıkarmaktadır. Daha önce paylaşılan ve Privacy International’ın yaptığı bir araştırmada olduğu gibi, bu verilere anlık olarak üçüncü tarafların erişimi ile kullanıcı hakkında hassas verilerin yaratılmasına katkı

sağlanabilir ve onu manipüle edecek reklamlarla karşılaşmasının yolu açılabilir. Dolayısıyla üçüncü tarafların kullanıcıların verilerini birleştirme işlemlerinde herhangi bir kontrole sahip olmamak ile onların hassas olabilecek kullanıcı verilerine erişim imkânı sağlamak arasında pozitif bir ilişki yoktur. Yani, verilerin yönetimi ve kontrolü kullanıcılara verildiğinde Onedio üçüncü tarafların kullanıcı verisiyle ne yaptıkları üzerine kontrolü olmadığını beyan edebilir.

Web site ve mobil uygulamaların en sık yer verdiği üçüncü taraf şirketlerden birisi olan Facebook, gizlilik sözleşmesinde bir kullanıcının Facebook hesabı olmasa bile ziyaret ettiği platformda takip edildiği ve hakkında verilerinin toplandığını belirtmektedir.

“Ortaklarımız, Facebook hesabınızın olup olmaması veya Facebook'a giriş yapmış olup olmamanız fark etmeksizin cihazınız, ziyaret ettiğiniz internet siteleri, yaptığınız alışverişler, gördüğünüz reklamlar, hizmetlerini nasıl kullandığınız gibi Facebook dışında gerçekleştirdiğiniz hareketler hakkında bize bilgi verir.”

Facebook, bu platformları “ortaklarımız” olarak nitelerken, onlar aracılığıyla topladıkları verilerin yasal dayanağının olmasını zorunlu kıldıklarını belirtmektedir. Fakat zorunluluğu nasıl ve ne ölçüde yaptıkları bir soru işaretidir.

“Bu ortaklardan her birinin bize herhangi bir veri gönderebilmesi için, verilerinizi toplama, kullanma ve paylaşma konusunda gerekli yasal haklara sahip olmalarını zorunlu kılarız.”

Hürriyet ve Milliyet gazeteleri çerez bildirim ve kullanıcıya çerez seçeneklerini sunmak amacıyla OneTrust adlı sistemi kullanmaktadır. Her iki sitede de çerez kullanım seçenekleri pasif yapılsa bile üçüncü taraf izleyicilerin takibi devam etmektedir. Diğer deyişle, kullanıcıdan aldıkları açık rızanın pratikte hiçbir yansıması gözlenmemiştir.

Siteyi ilk ziyaret sırasında kullanıcıya çerez kullanımına dair bir bildirim sunan Amazon hariç bütün sitelerin o andan itibaren üçüncü taraf çerezleri aktif hâle getirdiği gözlemlenmiştir. Bunlar arasında en emrivaki ifade internethaber.com haber sitesinde görülmüştür:

“Kullanıcılar bu sayfada yayınlanan şartları kayıtsız şartsız kabul etmiş sayılacaktır.”

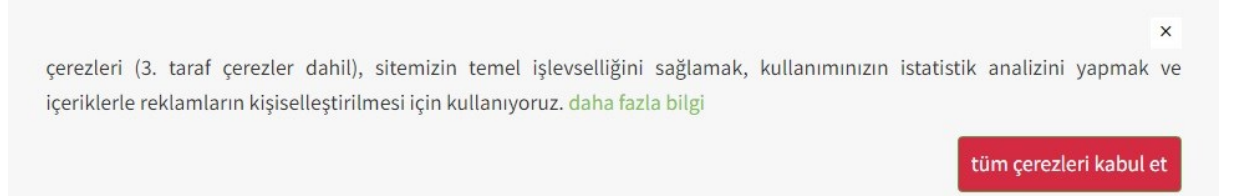
Sahibinden.com’un çerez politikasında ise şu ifade yer almaktadır:

“Portal’de yer alan Çerez bilgilendirme uyarısının kapatılması ve Portal’in kullanmaya devam edilmesi hâlinde Çerez kullanımına rıza verildiği kabul edilmektedir.”

Aynı şekilde eksisozluk.com’da da söz konusu problem aşağıdaki şekilde yer almaktadır:

“‘tüm çerezleri kabul et’ seçeneğini tercih etmeniz hâlinde çerez kullanımına izin vermektedir.”

Pratikte tüm çerezleri kabul et butonuna basmak bir açık rıza göstergesidir ve dolayısıyla Ekşi Sözlük’ün üçüncü taraf çerezleri aktif hâle getirmesine zemin hazırlamaktadır. Fakat site ziyaret edildiğinde kullanıcıya sunulan tek seçenek “tüm çerezleri kabul et” ise açık rızadan söz etmek mümkün değildir.



Grafik 4.11: Eksisozluk.com’un Kullanıcıya Sunduğu Çerez Bildirim Kutusu.
(ekran görüntüsü tarihi: 28 Kasım 2021)

Bu ve buna yakın ifadeler ve durumlarla normalleştirilen üçüncü taraf çerezlerin kullanıcı davranışlarını izlemesi, hem etik hem de açık rızanın özgürce beyanı bakımından sorunlu kabul edilmektedir.

Türkiye’den gelen ziyaretçilere herhangi bir çerez kullanım bildirimi yapmayan Cumhuriyet gazetesinin web sitesinde “Ziyaretçilerin kendilerine ait hangi kişisel verilerin toplanabildiği konusunda tercihlerini serbestçe kullanabilmesi cumhuriyet.com.tr için son derece önemlidir.” ifadesine yer verilmiştir. Aynı şekilde, memurlar.net web sitesinde de “Web sitemizi kullanmak için çerezleri kabul etmeniz gerekmez, ancak kullanıcı deneyiminizin kalitesi düşebilir.” ifadesi yer almaktadır. Oysaki ne ilk ziyaret sırasında, ne de çerez politikasında kullanıcıların özgürce

iradelerini ortaya koyabilecekleri bir ekran sunulmamaktadır. Kullanıcıya tercih imkânı sunulmasının yalnızca yanılısamadan ibaret olduğu görülmektedir.

Sözleşmeler incelenirken bazı sözleşmelerin birbiriyle aynı olduğu tespit edilmiştir. Örneğin, YouTube, Google'ın; Instagram, Facebook'un çerez politikalarına tabidir. Sahipliği aynı olan haberler.com ve sondakika.com sitelerinin çerez politikaları da aynıdır. Bu iki haber sitesinde yer alan ortak sözleşmede aşağıdaki ifade dikkat çekicidir:

“İş ortaklarımız, reklam platformları, sosyal medya platformları ile analitik bilgileri toplama hizmeti veren, sitemiz genelinde kullanılan bu servis sağlayıcılar hizmetlerini sunabilmeleri için sitelerimizi ziyaret ettiğinizde, bizim yerimize cihazlarınıza çerez kaydetmelerine izin verebiliriz. Bu çerezler hakkında daha fazla bilgi edinmek ve bu çerezlerin nasıl kontrol edileceğine ilişkin ayrıntılı bilgi için, lütfen bu üçüncü parti kurum ve kuruluşların gizlilik politikalarını veya çerez politikalarını inceleyiniz.”

Üçüncü taraf çerezlerin üçüncü tarafların sözleşmelerine bağlı olduğunun bildirildiği bu sözleşmede Google hariç üçüncü tarafların kim olduğuna yönelik herhangi bir şirket paylaşılmamıştır. Örneğin, araştırmada incelenen Haberler.com sitesinde 120 adet üçüncü taraf çerez bulunmuş; bu çerezlerin sahipleri arasında Twitter, AdMatic, Moat, Gemius, Yandex, AdTarget, AdScale, Criteo, Bidswitch, DailyMotion gibi şirket ve sitelerin olduğu tespit edilmiştir. Açıkça görülmektedir ki bu sözleşme kullanıcılara kim olduklarını söylemediği üçüncü taraf şirketlerin gizlilik sözleşmelerini okumalarını tavsiye etmektedir. Oldukça benzer bir durum eksisozluk.com'da da yaşanmaktadır.

“ekşi'de yer alan 3. tarafların çerezlerinden eğer imkân sunuyorsa ilgili 3. şahsın internet sitesini ziyaret ederek vazgeçebilirsiniz.”

Google hariç üçüncü tarafların kimler olduğunu sözleşmesinde açıklamayan Ekşi Sözlük, kullanıcılara onların web sitelerini ziyaret ederek çerezlerini pasif hâle getirebilecekleri önerisinde bulunmaktadır. Hâlbuki yapılan analize göre eksisozluk.com'da yalnızca Google değil; Criteo, AdPushUp, AdRecover, Quantcast, Gemius ve Semasio gibi üçüncü tarafların izleme teknolojilerine rastlanmıştır.

Üçüncü taraf şirket ve uygulamaların çerezleri hakkında sözleşmelerde olması gereken detaylı bilgi Grafik 4.12’de görülmektedir. Ntv.com.tr’nin çerez politikasından alınan bu ekran görüntüsünde çerezlerin adı, hangi türe ait olduğu, hangi alan adına bağlı olduğu (dolayısıyla hangi şirkete bağlı olduğu) ve cihazda saklanma süresi detaylı olarak paylaşılmıştır.

ssi, _ssuma	Hedefleme Çerezleri	sitescout.com	365 Gün, 30 Gün
OAID	Hedefleme Çerezleri	cdn.firstimpression.io	Oturum
KTPCACCOOKIE, KRTBCOOKIE_xxxx, PugT, PUBMDCID	Hedefleme Çerezleri	pubmatic.com	90 Gün, 90 Gün, 30 Gün, 90 Gün
am-uid	Hedefleme Çerezleri	admixer.net	730 Gün
ccpa	Hedefleme Çerezleri	contextweb.com	30 Gün
csync, pbw, TestIfCookieP, pid, TestIfCookie	Hedefleme Çerezleri	smartadserver.com	395 Gün, 395 Gün, 395 Gün, 395 Gün, 2914012 Gün
audit, sharedid	Hedefleme Çerezleri	id.sharedid.org	28 Gün, 28 Gün
ADKUID, ADK_EX_11	Hedefleme Çerezleri	adkernel.com	30 Gün, 14 Gün
TDCPM, TDID	Hedefleme Çerezleri	adsrvr.org	365 Gün, 365 Gün
google_push, tuuid, c, bsw_origin_init, tuuid_lu, custom_data	Hedefleme Çerezleri	bidswitch.net	Birkaç saniye., 365 Gün, 365 Gün, Birkaç saniye., 365 Gün, Birkaç saniye.
recs_xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Hedefleme Çerezleri	outbrain.com	Birkaç saniye.
everest_g_v2	Hedefleme Çerezleri	everesttech.net	365 Gün
demdex	Hedefleme Çerezleri	demdex.net	180 Gün
IDE, DSID, test_cookie	Hedefleme Çerezleri	doubleclick.net	390 Gün, Birkaç saniye., Birkaç saniye.
AFFICHE_W	Hedefleme Çerezleri	weborama.fr	93 Gün
_kuid	Hedefleme Çerezleri	adsby.bidtheatre.com	7 Gün
mc, d	Hedefleme Çerezleri	quantserve.com	396 Gün, 90 Gün
browser_data	Hedefleme Çerezleri	dnacdn.net	390 Gün
INGRESSCOOKIE	Hedefleme Çerezleri	bh.contextweb.com	Oturum
ab	Hedefleme Çerezleri	agkn.com	365 Gün
mako_uid, SERVERID	Hedefleme Çerezleri	eyeota.net	365 Gün, Birkaç saniye.
tuuid_lu, tuuid, c	Hedefleme Çerezleri	perf-serving.com	730 Gün, 730 Gün, 730 Gün
dyn_u	Hedefleme Çerezleri	dyntrk.com	365 Gün
A6, u2, eyeblaster	Hedefleme Çerezleri	serving-sys.com	90 Gün, 90 Gün, Birkaç saniye.

Grafik 4.12: Ntv.com.tr’nin Çerez Politikasında Yer Alan Çerezlere İlişkin Detaylı Bilgilerden Bir Kısımı
(ekran görüntüsü tarihi: 28 Kasım 2021)

Üçüncü taraf şirketlerin sözleşmelerini referans gösteren, onlara sorumluluk veren ve bilgi almak için onların sitelerinin ziyaret edilmesi gerektiğini söyleyen sitelerin ntv.com.tr’de olduğu gibi bu şekilde bir liste oluşturması gerekmektedir. Bu bağlamda Grafik 4.12’deki tablonun doğru bir örnek oluşturduğu söylenebilir.

Bazı sitelerin sözleşmelerini istedikleri zaman tek taraflı olarak değiştirme hakkına da sahip olduğunu beyan ettiği gözlemlenmiştir:

“Nefis Yemek Tarifleri kullanım koşullarını önceden bildirmeksizin değiştirebilir.”

“Haber7.com yönetimi yukarıda belirtilen kullanım koşullarını dilediği her zaman geliştirebilir ve güncelleyebilir.”

Bu siteler zaten çerez kullanımı için herhangi bir onay mekanizmasına sahip olmadıkları için sözleşmede değişiklik olduğu zaman kullanıcılara bildirim yapma ihtiyacı da hissetmeyeceklerdir.

Özetleyecek olursak nicel araştırma bulgularında ilk önce Türkiye'deki web siteleri ve mobil uygulamalar aracılığıyla gözetleyen aktörlerin kimler olduğu ve gözetimin hangi amaçlara bağlı olarak nasıl gerçekleştiği ortaya konulmuştur. Örneklem kapsamındaki web sitelerinde sırasıyla Google, Criteo, Taboola, Moat, Facebook ve Gemius'un üçüncü taraf olarak yer aldığı ve ilgili sitelerdeki kullanıcı davranışlarını takip edebildikleri görülmüştür. Web sitelerine baktığımızda ise özellikle haber sitelerinde üçüncü taraf izleyicilerin sıkça yer aldığı tespit edilmiştir. Bunlar arasında Hürriyet, Milliyet, Sabah, Cumhuriyet, Haberler.com, Onedio, NTV, İnternethaber ve Memurlar.net gibi platformlar yer almaktadır. Bu sitelerin gelir modeli büyük oranda reklama bağlı olduğu için ulusal ve uluslararası birçok reklam ve analitik şirketi üçüncü taraf olarak sitelerde bulunmaktadır. Mobil uygulamalardaki üçüncü taraf izleme teknolojileri incelendiğinde ise web sitelerinde olduğu gibi Google'ın hâkimiyeti karşımıza çıkmaktadır. Hem web sitelerinde hem de mobil uygulamalarda üçüncü taraf olarak sıkça yer alan Google'ın baskın bir gözetleyici aktör olduğu ve Google'dan habersiz neredeyse web'te hiçbir şey yapılamayacağını söylemek mümkündür.

Nicel araştırmanın ikinci basamağında web sitelerinin üçüncü taraf şirketlerin izleyicilerini aktif hâle getirmeden önce kullanıcılardan izin alıp almadığı ve bu bildirimi nasıl yaptıkları incelenmiştir. Sitelerin neredeyse yarısında gizlilik sözleşmesi veya çerez politikasıyla ilgili herhangi bir bildirimle karşılaşılmamıştır. Bildirim yapılan sitelerin ise hiçbirinde kullanıcılara ilk etapta çerez kullanımını reddedecek bir seçenek sunulmadığı görülmüştür. Çerezleri özelleştir seçeneğiyle zorunlu olmayan çerez kullanımının tercihinin kullanıcılara bırakılması nadiren gerçekleşmiştir. Bu bulgular eşliğinde web sitelerinde kullanıcıların açık rızasını alarak onların verilerinin çerezler yoluyla işlenmesi çerçevesinde sorunlar olduğu tespit edilmiştir.

4.3.2. Nitel Araştırma

Araştırmanın bu ayağında alanında uzman katılımcılarla yarı-yapılandırılmış görüşmeler gerçekleştirilmiştir. Nicel araştırma bulgularının yorumlanmasına yardımcı olunması ve araştırmaya ait diğer sorulara cevap aranması bakımından teknoloji, iletişim, reklam, tasarım ve hukuk alanında uzman kişilerle görüşülmüştür. Her bir kişiye aynı soruları sormak yerine, kendi uzmanlık alanları ile araştırmanın bulgu ve amaçlarının aynı çatı altında bulunduğu yerlerden sorular yöneltilmiştir. Katılımcı 1, kimliğinin yazılmasını istediği için adı paylaşılmıştır.

Görüşmeler neticesinde elde edilen veriler nicel araştırma bulguları ve araştırma soruları göz önünde bulundurularak beş ana temada değerlendirilmiştir. Katılımcılarla görüşmeler videolu çevrim içi ortamda gerçekleştirilmiştir.

Katılımcılar	Uzmanlık Alanı / Meslek
Katılımcı 1 (Aral Balkan)	Dijital Haklar Aktivisti
Katılımcı 2	Kullanıcı Deneyimi Tasarımcısı
Katılımcı 3	Avukat
Katılımcı 4	Akademisyen / Reklamcılık Bölümü
Katılımcı 5	İletişimci / Yazar
Katılımcı 6	Reklam Teknolojileri Yöneticisi
Katılımcı 7	Dijital Pazarlama Uzmanı

Tablo 4.25: Görüşmecilerin Listesi ve Meslekleri.

Ana Tema	Alt Tema
1) Gözetim Kapitalizmi	a. Sorun Gözetim Mi? Kapitalizm Mi? b. Gözetim Kapitalistleri: Google, Facebook ve Diğerleri c. Sahipliğin Sorgulanması: Kullandığımız Cihazlar Kimin?
2) Kişisel Veriye Dayalı Çevrim İçi Reklamcılık	
3) Kişisel Verilerin Korunmasına Yönelik Yasal Düzenlemeler	a. KVK Kanunu Çerezleri ve Açık Rızayı Nasıl Değerlendiriyor? b. Türkiye’de Web Siteleri Yasal Açıdan Ne Derece Sorunlu? c. Yasaların Uygulanabilirliği ve Cezaların Caydırıcılığı
4) Veri / Gözetim Farkındalığı ve Mahremiyet	a. Mahremiyet Tartışması b. “İstemiyorsan Kullanmamakta Özgürsün”

	c. “Verilerimin Toplanması Umrumda Değil” d. Veri Farkındalığı / Bilinci
5) Etik Bir Web’in İnşası	a. Mevcut Sistemdeki Problem b. Verilerin Kontrolünü Kullanıcılara Vermek c. Hizmetlerin Ücretli Olması Neyi Değiştirir? d. Etik Bir Web’i Nasıl Sağlarız?

Tablo 4.26: Nitel Araştırma Sonucu Çıkarılan Ana ve Alt Temalar.

4.3.2.1. Gözetim Kapitalizmi

George Gerbner (1983:358), “*Marx bugün yaşıyor olsaydı, temel eserinin adı Kapital değil, İletişim olurdu.*” diyerek bu yüzyılın koşullarına dair çarpıcı bir yorumda bulunmaktadır. Son yarım asırda gelişen gözetim teknolojileri, gözetlenen iletişimsel faaliyetler ve zenginliğin gözetim ve enformasyon kaynaklı yükselişine bakıldığında Gerbner’in yorumuna katılmamak son derece zordur.

Gözetim kapitalizmi kavramı, şirketlerin hammadde olarak gördüğü insan deneyimleri ve iletişimsel faaliyetlere tek taraflı olarak el koyduğu, onları yapay zekâ yoluyla davranışsal veriler hâline getirdiği ve bu verileri kişinin anını ve geleceğini tahmin etmeye yönelik ürünlere dönüştürdüğü fikri üzerine inşa edilmiştir. Zuboff’un ifadesiyle (2019: 9) Marx’ın geleneksel kapitalizm imgesi sonsuz emek sömürsüne bağlıyken, gözetim kapitalizmi insanın her türlü deneyimiyle beslenen bir sistemdir.

Bu ana tema altında aşağıdaki alt temalar belirlenmiş olup bunlara ilişkin katılımcı yorumlarına yer verilmiştir.

4.3.2.1.1. Sorun Gözetim Mi? Kapitalizm Mi?

Gözetim kapitalizminde sorunun nerede olduğu bir merak konusudur. Tarihsel olarak ele alındığında gözetim hiçbir zaman zenginleşmenin ana yolu olarak kullanılmamıştır. Gözetim her zaman baskı, denetim, disiplin gibi kavramlarla bir araya getirilmiştir. Bugün geline nokta “gözetim kapitalizmi” kavramı Zuboff’un belirttiği gibi (2019: 93) “*Google’ın liderliğinde hızla internetteki bilgi kapitalizminin varsayılan bir modeli hâline gelen (...)*” bir duruma işaret etmektedir. Gözetim

kapitalizmini irdelerken gözetleme olmasa bilgi kapitalizmini normal mi karşılayacağız? Yoksa gözetim kapitalizmi yaklaşımı gözetlemeyi eleştirirken aynı zamanda kapitalizmi mi de eleştiriyor mu? gibi sorularla bu alt temaya ilişkin tartışmalar yürütülmüştür.

Öncelikle Katılımcı 5, “gözetim” ifadesi yerine “gözetleme” ifadesinin kullanımını daha doğru bulduğunu söylemektedir:

“Gözetim değil, gözetleme kapitalizmi olarak çevrilmesini doğru buluyorum. Daha önceden ben de gözetim diye kullanıyordum. (...) Çünkü gözetim dediğiniz zaman biraz da bir şeyi korumak, kollamak anlamına geliyor. Gözetleme deyince kelime biraz daha oturuyor.” (Katılımcı 5)

“Bir panoptikonun içerisinde, insanların verilerini gözetleyerek, o verileri gözetleyip biriktirerek bir varlık oluşturuyorlar. O yüzden öncelikle isminin gözetleme olarak çevrilmesini doğru bulduğumu söyleyeceğim.” (Katılımcı 5)

Katılımcı 1, gözetim kapitalizmini kendi perspektifinden açıklarken Zuboff’un bakış açısını sorunlu bulduğunu söylemektedir:

“Gözetim kapitalizmi kavramı Shoshana Zuboff tarafından ortaya konmuş bir kavram. Zuboff ile bizim ayrıldığımız nokta, Zuboff’a göre gözetim kapitalizmi, kapitalizmin bir bozulması. Yani kapitalizm genel olarak iyi bir şey, ama bu teknoloji şirketleri bunu kötü bir yola göndermeye başladılar. Bu da gözetim sistemleri yaratarak oldu. Benim görüşüm gözetim kapitalizmi sadece kapitalizm. Ona gözetim kapitalizmi derken, kapitalizmin bugünkü hâli. Kapitalizmin batıdaki başlangıcına bakarsak köleliğe kadar gidebiliyoruz. Ve kölelikteki elde edilen sermayelerin nasıl kullanıldığı. Ve köleliğe bakarsak o da tamamen gözetim üzerine kurulmuş bir şey. İnsanların her yaptığı gözetim altındaydı. Yani başından beri var. Ben bu terimi kullanıyorum çünkü önemli... Zuboff bunu kapitalizmin bozulması olarak görüyor, ben ise kapitalizmin ağ çağındaki hâli olarak görüyorum. Gözetim olayını kapitalizmden ayıramayız. Keşke bu şirketleri daha iyileştiresek diye bir şey yok. Facebook’u daha çok iyileştiremeyiz. Bütün sistem gözetim üzerine kurulmuş. O zaman tamamen başka bir şirket olur; artık Facebook olmaz. (...). Gözetim kapitalistlerini daha iyileştiremeyiz. Daha farklı bir sisteme ihtiyacımız var.” (Katılımcı 1)

Katılımcı 1, “kapitalizmin bozulması” ifadesini şu şekilde açmaktadır:

“Zuboff’a göre eğer bu gözetim faktörünü ortadan kaldırabilirsek problemi çözüyoruz. Kapitalizmin genelinde, enformasyon tarafını çözebilirsek, şirketlerin büyümesi bir problem değil. Bu zaten kapitalizm. Keşke daha iyi davranşalar diye bir görüşü var. Benim görüşüm öyle değil.

Ben onlara daha iyi davranın demek istemiyorum. Ben onları daha iyi teknolojilerle, daha iyi kurumlarla değiştirmek istiyorum. “ (Katılımcı 1)

Katılımcı 1, sistemin olağan ekonomik işleyişinin kapitalizm mantığını barındırmasının sindirildiğini ve bunun sadece gözetim aracılığıyla olmasının yanlış olduğunu söylemenin hatalı olduğunu vurgulamaktadır. Kapitalizmin içkinleştirilmesi bağlamında Amerikalı ile Avrupalıların düşünme pratiklerinin birbirinden ayrıldığına şöyle değinmektedir:

“Ben bunu sürekli görüyorum. Avrupalı olan teknolojistlerle, Amerika’da olanlar arasında çok büyük fark var. Amerika o kadar içselleştirmiş ki evet tabi ki kapitalizm, tabi ki büyük şirketler. Başarı bir trilyon dolar yapmak. Orada bunlar o kadar içselleşmiş ki, alternatifler üzerine çalışmak isteyenler bile kendini bu kriterler içinde buluyor.” (Katılımcı 1)

Katılımcı 1, Amerika’nın egemen ekonomik sisteminde kapitalizme alternatif olmaya niyetli sistemlerin bile kapitalist mantıkla inşa edildiğini vurgulamaktadır. Sistem Amerika’da nesilden nesile o kadar içselleşmiş ki; her yıl kârlılığı artırmak ve sermaye birikimini mükemmel bir işleyişle düzenli hâle getirmek dışında başka bir sistemin varlığı söz konusu olmamıştır. Katılımcı 1’e göre kavramın öncüsü Zuboff da dâhil gözetim kapitalizmi üzerine bakış açısına sahip Amerikalı yazarlar kapitalizmden ziyade gözetimle ilgili eleştiriler sunmaktadır. Bu bağlamda Katılımcı 1, sorunun gözetimde olduğu kadar kapitalizmde de olduğuna dikkat çekmektedir.

Katılımcı 5, Katılımcı 1’in söylediklerine paralel olarak kapitalizmi Amerika bağlamında şöyle değerlendiriyor:

“Amerika’da ilk önce sistemi korumayı dert ediyorlar. Ve kapitalizme çok fazla dokunmak istemiyorlar. Amerika’nın bildiğimiz anlamda Amerika olmasını sağlayan şey kapitalizm. Kapitalizmin neredeyse merkez noktası diyebiliriz. O yüzden o tarafı çok kurcalamak istemiyorlar. Gözetleme kapitalizmi, kapitalizm çerçevesinden değerlendirilmelidir.” (Katılımcı 5)

Katılımcı 1, Avrupalılar ve Amerikalıların mevcut duruma hem düşünce biçimi hem de yasal pratikler bakımından farklılıklarını eski bir Facebook çalışanının Avrupa ziyaretinde sarf ettiği sözler üzerinden örneklendiriyor:

“Facebook’un ‘meşru ifşacısı’²⁰ Frances Haugen, Avrupa turuna çıktı. Hem Brüksel’e hem de Londra’ya gitti. Hem Londra’daki parlamenterlerle hem de AB’nin parlamenterleriyle görüşti. Onun bu görüşmelerden sonra söylediği şey büyük teknoloji şirketlerini düzenleme konusunda Avrupa’nın ABD’den daha ilerde olduğuydu. “(Katılımcı 5)

“Avrupa’nın perspektifi çok değerli. Amerika’nın sorunu çözebilmek için AB’den ilham alması gerekiyor.” (Katılımcı 5)

Bu tartışmalar çerçevesinde gözetim ve sermaye birikimi arasındaki ilişkinin Avrupa ve Amerika’da farklı ele alındığı ve gözetleme mekanizmaları eleştirilirken kapitalizmin de göz ardı edilmemesi gerektiği yapısal ve önemki bir tartışma konusu olarak kendini göstermektedir.

4.3.2.1.2. Gözetim Kapitalistleri: Google, Facebook ve Diğerleri

İş modelini tamamen gözetlemeye dayandıran veya işinin bir ayağını gözetim oluşturan tüm şirketlerin günün sonunda kullanıcı verisini toplamak, saklamak, birleştirmek ve anlamlandırmak istediği söylenebilir. Bu veriler ilgi duyduğumuz spor branşından ne kadar hızlı yazı yazdığımıza kadar değişebilmektedir. Bunların en bilineni Google ve Facebook’tur. Google ve Facebook, sağladıkları hizmetlerin kullanımlarından ve üçüncü taraf olarak ağa bağlı diğer uygulamalardan veri toplayabilirler. Her yıl tırmanan milyarlarca dolarlık kârları insanların gelecekteki adımlarını daha iyi tahmin etme sistemleriyle daha da artma potansiyeline sahiptir. Bu şirketlerden habersiz ağda neredeyse hiçbir şey olmazken, bir zaman sonra insanların sosyal hayatlarında neler yaptıkları merak edilmeye başlandı: evde ne yaptığı, kiminle tartıştığı, sokakta kiminle karşılaştığı, evde olmasına rağmen çalınan zile neden bakmadığı gibi. Bunlara uygun üretilen veya satın alma yoluyla şirket bünyesine dâhil edilen teknolojilerle gözetim, çevrim içi ve çevrim dışı insan hayatının her bir noktasına erişerek zenginleşmenin bir yolu olarak görülüyor.

²⁰ İng: Whistleblower. Facebook’un içerisinden bilgi sızdırmıştır.

Katılımcı 1, gözetim modelli sistemi açıklarken bunun artık varsayılan bir iş modeli olduğunu söylemektedir:

“Bu sistem (gözetim kapitalizmi) o kadar yaygın ki yani teknoloji alanındaki şirketlerin %99’u bu sistem üzerine kurulu. Küçük şirketler var, geleneksel şirketler var. Ama bu büyük şirketlerin hepsi aynı sistem. Apple bile artık bu yöne gitmeye başladı. (...) Düşündüğün zaman Facebook değil sadece, Google değil sadece, Snapchat, Tiktok hepsi. Bütün yayıncıların hepsinin sistemi bu.” (Katılımcı 1)

Bir bakıma klasik kapitalizmde artı değer üretmek için hammaddeye ve insan emeğine bağımlı olan sermaye, bilgi teknolojilerinin egemen olduğu günümüzde de aynı şeylere ihtiyaç duyuyor. Zuboff (2019: 94), sanayi kapitalizminin doğanın hammaddelerini metaya dönüştürdüğünü; aynı şekilde gözetim kapitalizminin de yeni bir meta üretmek için insan doğasına ait “şeyleri” talep ettiğini söylüyor. Görülen o ki bu “şeylerin” talebi artık tüm teknolojik şirketlerin veya teknolojiye ayak uyduran şirketlerin varsayılan talebi olarak karşımıza çıkıyor.

Zuboff’a göre Google ve Facebook, gözetimin kapitalizminin bayrak tutucusu ve rol modelidir. Kısacası bu sistemin oluşmasındaki öncü şirketlerdir. Peki, bu şirketler yarın bu modeli bıraksa veya problemin çözümü için kurban edilseler neler değişir? Katılımcı 1, gözetim kapitalizmi mantığının ve girişim sermayedarlarının buna yaklaşım biçimini şöyle paylaşmaktadır:

“Silikon Vadisi gerekirse Facebook’u kurban eder. Facebook’u kurban ederek problemi çözdük diyebilirlerse ederler. Facebook zaten girişim sermayedarları için yapacağı kadar parayı yaptı. Bundan sonra daha ne kadar büyüyecek. Onların baktığı şey bundan sonra yeni Facebook kim olacak. Model falan değiştirmeyi düşünmüyorlar. Facebook yarın ortadan kaybolda hiçbir problem çözülmez. Çünkü yarın bir başka Facebook onun yerini alacak aynı sistem tarafından yatırım yapılmış.” (Katılımcı 1)

Katılımcı 1’in paylaştığına göre bu sistem hem oyuncuları hem de yatırımcıları ile o kadar büyük ki, her zaman yeni bir girişimin milyonlarca dolar yatırım alarak bu sistemi sürdürme ve büyütme potansiyeli var olacaktır. Üstelik gerekirse en iyi oyuncusunu kurban etme pahasına bile.

Google ve Facebook'un gelir modeli eleştirel perspektifte "gözetime dayalı" olarak adlandırılırken, farklı bir perspektifte "veriye dayalı" olarak ayrılabilir. Katılımcı 4, bu platformların gözetim şirketi değil veri şirketi olduklarını belirtiyor:

"Ben Facebook ve Google'ı kullanmazsam beni gözetleyemez. Bunlar gözetim şirketi değil, veri şirketi." (Katılımcı 4)

"Google ve Facebook bir gözetim şirketi demek bana biraz hatalı geliyor. Onlar bir veri şirketi ve verimizi topluyorlar. Zaten çalışma biçimi olarak ona ihtiyacı var. Google, senin benim verimi toplayacak ki üçüncü bir kişi geldiğinde o bizden aldığı bir veriyi de onlara sunabilirsin. Dijital mecralarının tamamının çalışma mantığı zaten veriye dayanıyor. Onlara bizim verimizi toplamayın lütfen deme lüksümüzün olmadığını düşünüyorum. Yeter ki bunu net bir şekilde açıklasınlar, biz de bunu bilelim ve buna göre davranalım." (Katılımcı 4)

Bu bakış açısına göre kişisel veri gözetlenerek değil platforma kullanıcı tarafından bizzat sağlanarak toplanmakta ve işlerin platform tarafında sağlıklı yürümesi için maddi bir kaynak yaratmaktadır. Bu bağlamda Katılımcı 4 ile Katılımcı 1'in yaklaşım biçimleri farklıdır. Katılımcı 4, tüm dijital platformların çalışma prensibinin merkezinde veri olduğunu söylerken; Katılımcı 1 bunu gözetim kapitalizmi olarak değerlendirmiştir. Şirketlerin "ne olduklarına" yönelik bu iki farklı bakış açısı, iş yapış biçimlerini nasıl gördükleri üzerine de farklılık yaratmaktadır.

Katılımcı 1, gözetim kapitalizmi eleştirilerinde Google ve Facebook'un sürekli merkez alınmasının nedenini şu sözlerle açıklamaktadır:

"Google ve Facebook insanlar onları kullandıkları için en önde. Sadece Google ve Facebook üzerinde durmamız baya tehlikeli. Bunu ben de yapıyorum. Bir tweet atacaksın, 250 karakterin var. Bir şekilde bir tembellik de bu. Biz Google ve Facebook deyince herkes anlıyor sanıyoruz." (Katılımcı 1)

Google ve Facebook; herkesin bildiği, en çok ziyaret edilen, içerisinde en çok zaman harcanan ve en çok kullanılan ürünlere sahip şirketlerdir. Gözetim kapitalizmini eleştirenlerin Google ve Facebook'u örneklem seçerek bunun üzerinden bir eleştiri inşa etmeleri Katılımcı 1'e göre kabul edilebilir bir durumdur. Öte yandan Facebook veya Google gibi yüz milyarlarca dolarlık şirket olmayan, fakat gözetim kapitalisti

olarak nitelendirilebilen şirketler hakkında bir bilgi olmamasını Katılımcı 1 şu şekilde yorumlamaktadır:

“Öbürleri hakkında konuşmuyoruz evet. Yani bazı köşelerde konuşuyoruz. Bir açıdan bakıldığında da tarihsel olarak bakarsak son 10 senede falan mesela. Bunun böyle olmasının nedeni de, ilk başlarda Google ve Facebook hakkında da konuşmuyorduk. Bugünlerde bile bunların bu kadar açık konuşulması, bir balon. Kendi balonumuz içinde konuşuyoruz. Genel topluma bakıldığında hâlâ yine konuşulmuyor.” (Katılımcı 1)

“Mesela Criteo veya diğer şirketler hakkında konuşulunca kimsenin umrunda bile değil. Kim bunlar diyorlar. Ne anlamı var diyorlar. Eğer gösterebilirsen sizin şu verilerinizi alıyorlar, şöyle bir olay oldu gibi o zaman insanlar ilgi duymaya başlıyor. Onun dışında ya onlar hakkında konuşuyorsun ya da bir muhasebe şirketi hakkında konuşuyorsun. İnsanların umrunda değil yani.” (Katılımcı 1)

Buna göre Google ve Facebook ile benzer iş modeline sahip farklı şirketlerin sıkça tartışılmamasının altında yatan bir neden de kimsenin onlarla ilgilenmiyor oluşudur. Ancak neler yaptığıyla, elinde ne olduğuyla, onu nasıl kullandığıyla ve nasıl veri topladığıyla ilgili bir tablo sunulduğunda insanlar ilgi duymaya başlıyor. Onun dışında tüm tartışmalar insanların kendi filtre balonları arasında gerçekleşiyor.

Katılımcı 1, çoğu insanın bilmediği, gözetim kapitalizminin korkutucu bir yansıması olarak Japon SoftBank şirketini örnek vermektedir:

“SoftBank, Japon şirket. 100 milyar dolarlık girişim sermayesi var. Sahibi Masayoshi Son. ‘Kim veriye yönetirse dünyayı o kontrol eder’ sözünün sahibi. Hedefi, dünyada yapılan tüm işlemlerin kendilerinden geçmesi. Taksi çağırdığında bu işlem SoftBank’tan geçmeli. Hastaneye gittiğinde oradaki işlemler SoftBank ile ilgili olmalı. Bir şeyden korkman gerekiyorsa Google ve Facebook’tan değil, SoftBank’ten korkmalı. Oldukça korkutucu.” (Katılımcı 1)

SoftBank üzerine kısa bir araştırma yapıldığında yeni teknolojik girişimlere sıkça yatırım yaptığı görülmektedir. Bu girişimlerin finans, e-ticaret ve sağlık gibi farklı sektörleri kapsadığı ve dolayısıyla kendilerinden habersiz dünyada hiçbir şeyin olmaması üzerine bir imparatorluk kurmaya niyetli oldukları söylenebilir. Katılımcı 1’in korkutucu bulduğu durum Masayoshi Son’un şu ifadesiyle daha da anlaşılır

kılınılmaktadır: “Bir yapay zekâ devrimine gidiyoruz ve bu devrimin yatırımcı şirketi biz olacağız.”²¹”

Şirketlerin ellerindeki kullanıcı verisi ile devletin vatandaşı hakkında sahip olduğu veri bazen niceliksel ve niteliksel olarak karşılaştırılmaktadır. Özellikle özel sektörün devlet kurumlarından daha fazla veri topladığına yönelik bir kanaat söz konusudur (Rosenzweig, 2016: 126). Hatta mahremiyet ihlali bağlamında ticari işletmelerin hükümetlerden daha tehlikeli olduğu düşünülmektedir (a.e., s.124). Bu düşüncenin odak noktasında şirketlerin çok farklı kanallardan topladıkları veriler ve bunları anlamlandıran ve içgörüler çıkarabilen yapay zekâları yer almaktadır. Katılımcı 1, gözetim kapitalistleri ile devlet gözetimi arasında kaydadeğer bir fark olmadığını ve her ikisinin de iç içe geçtiğini söylemektedir:

“Şirket gözetiminin en az devlet gözetimi kadar tehlikeli olduğunu düşünüyorum. Birisinin diğeri kadar tehlikeli olduğunu ve bunların birbirinden ayrı olmadığını düşünüyorum. Birisi öbürüne veri sağlıyor. Çok güzel bir deyiş var: “NSA bir anda uyanıp hadi herkesi gözetleyelim demedi. Baktılar ve ‘vay be şirketler herkesi gözetliyor, hadi kendimize bir kopya alalım’ dediler. Bu çok güzel bir anlatım. Bu şirketler zaten bu verileri toparlıyor, he biz o zaman bunun bir kopyasını alalım. O yüzden devlet gözetimi ve şirket gözetimi farklı değil.” (Katılımcı 1)

Güvenlik Uzmanı Bruce Schneier’in ifadesine atıfta bulunan Katılımcı 1, tüm sistemlerini gözetim üzerine oturtmuş şirketlerin hâlihazırda devlet organları için de birer kaynak olduklarını dile getirmektedir. Devletlerin Apple, Google veya diğer teknoloji şirketlerinden belirli konular hakkında bilgi toplamak istediği fakat onların bu bilgileri vermediği nadiren de olsa karşımıza çıkmaktadır. Katılımcı 1, bu konuyu verilerin birer meta olmasıyla açıklamaktadır:

“Bazen görüyoruz, Google devlete karşı koyuyor, verileri devlete vermeyeceğini söylüyor vs. Bunlar sadece sahip olma. Bazı şirketler bazı devletlerden daha güçlü tabi. Paraları var çünkü. Ve bu verilere sahip olmak istiyorlar, çünkü bunlar onlar için hammadde. Ama devlet verilere el koymak isterse bu şirketler ‘bunlar benim verilerim’ diyor. Kendi mallarını korumak istiyorlar. Seni korumaya çalışmıyorlar.” (Katılımcı 1)

²¹ <https://group.softbank/en/philosophy/happiness-empowered-ai/global>

Buna göre şirketler duruma yalnızca araçsal akılla yaklaşmaktadır. Katılımcı 1, araçsal aklın kapitalist şirketlerdeki yerleşik durumunu yaptığı bir konuşmada paylaştığı örnek üzerinden paylaşmaktadır:

“Yakın zamanda yaptığım bir konuşmada IBM’in İkinci Dünya Savaşında yaptığıyla ilgili bir kitaptan paylaşım yapıyorum. O kitapta şöyle diyor: IBM, Hitler’e nazi oldukları için yardım etmedi; ideolojik olarak yakın hissettiği için de yardım etmedi, yalnızca iş yapıyordu. Bu beni daha fazla korkutuyor. İdeolojik olarak yaklaşan insanı anlarsın. Bu sadece para, ideolojin ne olursa olsun. Bu çok korkunç bir şey işte. O yazarın dediği gibi ‘iş onların göbek adı’.” (Katılımcı 1)

Bu tartışmalar çerçevesinde bugüne egemen olan gözetim kapitalizmi anlayışının geleneksel kapitalizmden, bu anlayışı iş modeli benimseyen şirketlerin ise Ford gibi geleneksel kapitalist şirketlerden farkının olmadığını söylemek mümkündür.

4.3.2.1.3. Sahipliğin Sorgulanması: Kullandığımız Cihazlar Kimin?

Teknolojinin topluma sunduğu yeniliklerden birisinin de ağlara bağlanabilen akıllı cihazlar olduğunu söyleyebiliriz. Üretken birer kaynak olan bu cihazlar bir yandan onu kullanan kişiye hizmet eder, aynı zamanda kullanım faaliyetlerini de kayıt altına alır. Bugün yalnızca cep telefonları değil; buzdolapları, fırınlar, diş fırçaları, saatler, arabalar ve daha birçok nesne veri toplayabilme özelliğine sahiptir. Maliyeti karşılanıp satın alınan bu cihazların gözetim kapitalizmi yaklaşımı içerisinde bir yeri ve önemi vardır. Çünkü tıpkı web siteleri ve mobil uygulamalar gibi bu akıllı araçlar da kullanım verilerini toplayabilmekte ve paylaşabilmektedir. Yani insanlar hem ürünü alırken bir bedel öder, hem de o ürünü kullanırken bir bedel ödemeye devam eder.

İlki peşin, diğeri cihaz bozulana kadar taksit taksit ödenen bedeller cihazın aslında kimin olduğunu sorgulatmaktadır. Katılımcı 1, teknolojik tasarım mantığını eleştirirken cihazların sahipliğini şu şekilde sorgulamaktadır:

“Şu andaki sistemlerimiz bu şirketler tarafından sahipleniliyor. Kontrol onların elinde ve onlar sahipler. Belki sen satın alıyorsun ama telefon gerçekten senin değil. Telefon hâlâ bir şekilde Google’a, bir şekilde Apple’a ait. Onlar hâlâ senin onun üzerinde yaptığın şeyleri görebiliyorlar. Google,

Apple'dan daha fazla mesela. Ve bu araçlar senin aracın değil, onların aracı.”
(Katılımcı 1)

Buna göre örneğin cep telefonunun sahibi, kontrolü elinde tutan ve telefonda yapılan her bir işlemi görebilen kişi veya şirketlerdir. Bu bakış açısına göre cihazdaki etkinliklerin başkaları tarafından görüntüleniyor olması kullanıcının araçsal bağımsızlığını engellemektedir:

“Şimdi Apple mesela, bir süredir bunu yapıyor. Algoritmalar senin cihazında çalışıyor, benim bilgisayarlarımda değil diyor. Ama yine ne yapıyor o algoritmalar. Google Haberlere gidiyorsun okuduğun haberlere bakıyor şu reklamı göster diyor sana, Apple bile. Ama diyor ki bu veri bize gelmiyor senin aracın sana öneriler sunuyor. Ama kimin çıkarında? Yine Apple'ın çıkarına.”
(Katılımcı 1)

Çoğu dijital şirket, verileri kendi sunucularına aktarırken Apple kullanıcıların cihazlarında tutmaktadır. Ona rağmen söz konusu cihazların içinde verileri yaratılan yapay zekânın kimin çıkarına çalıştığı sorusu sorulduğunda cevap yine de kullanıcı olmuyor. Katılımcı 1, cihazın sahibinin kimin çıkar sağladığıyla ve teknolojinin sahibi ile ilgili olduğunu dile getiriyor:

“Senin fiziksel dünyada düşüncelerinin nasıl kendine ait olduğunu sanıyorsan sanal dünyada öyle değil. Sen bir düşünceni telefona yazdığında düşüncen sana mı ait, Google'a mı ait, neden Google görüyor onu?” (Katılımcı 1)

“Şirketin çıkarları için mi çalışıyor, senin çıkarların için mi? Şu anda şirketin çıkarları için çalışıyor. Ve bu şirketler sahip senin teknolojiye. (...) Senin teknolojinin yalnızca senin çıkarların için çalışmalı.” (Katılımcı 1)

Bu bakış açısı sahipliğin cihazlarda üretilen verilerin uzak sunuculara gönderilmesiyle veya cihazın içinde kalmasıyla değişmediğini; tümünden teknolojinin kime en çok fayda sağladığıyla ilgili olduğunu betimlemektedir.

4.3.2.2. Kişisel Veriye Dayalı Çevrim İçi Reklamcılık

Hedefli reklamcılık, davranışsal reklamcılık, kişiselleştirilmiş reklamcılık gibi isimlerle de bilinen ve her kullanıcıya çevrim içi faaliyetlerine ve kişisel verilerine bağlı farklı reklam gösterilmesine dayanan çevrim içi reklamcılık türünün merkezinde

izleme yer almaktadır. Bu reklamcılık türü çevrim içi kullanıcı davranışlarının takibi sonucu toplanan ya da çıkarımsanan demografik ve psikografik verilere göre ilgili kişilere reklam sunmayı içermektedir. Reklam şirketleri topladıkları veriler neticesinde belirli nitelikteki kişileri veya grupları bir araya getirerek onları reklamverenlerin hedeflemesine izin verir. Çevrim içi reklam endüstrisi bugün yüz milyarlarca dolarlık bir işlem hacmine sahiptir. Çevrim içi reklam pazarının kaydadeğer bir kısmının gözetleme üzerine inşa edilmesi dolayısıyla gözetim kapitalizminin olumsuz yansımalarını reklam bağlamında da tartışmak gerekmektedir.

Katılımcı 1, gözetim kapitalizminde reklamın veri toplamak için bir bahane hâline dönüştüğünü ifade etmektedir:

“Bu sistemin ilk yaratılmasında çok büyük rolü oldu. Bugün için sorarsan bence tabi ki rolü var. Mesela Google gibi bir şirket çok kar yapıyor. Veri şirketleri milyarlar yapıyor bu sistemde. Ama bu artık sadece reklamcılıkla ilgili değil.” (Katılımcı 1)

“Kişiselleştirilmiş reklam bir şekilde bugün veri toplamanın mazereti hâline geldi. Kullanıcı deneyiminizi iyileştireceğiz diye. Aynı şekilde bir mazeret.” (Katılımcı 1)

Buna göre çevrim içi kişiselleştirilmiş reklam gösterimi için toplanan veriler bir mazeret hâline gelmiştir. Katılımcı 1’in ifadesi tıpkı Zuboff’ın kullanım fazlası artık verileri tanımlamak için kullandığı, kişiselleştirilmiş kullanıcı deneyimi sağlamak bahanesi ile ihtiyacı olandan çok daha fazla verinin toplanması yorumuna benzemektedir. Katılımcı 1’e göre kişisel veriye dayalı reklam, gözetim kapitalizmi mantığının ortaya çıkışında büyük bir öneme sahiptir ve hâlen kişisel veri toplanması için bir maske olarak kullanılmaktadır.

Katılımcı 4, dünyadaki hâkim kapitalist sistemin altını çizerek yalnızca kişisel veriye dayalı hedefli reklamcılığın eleştirilmesinin doğru olmadığını ifade etmektedir:

“Dijital pazarlamayı, reklamcılığı eleştirirken dünyanın geneline hâkim olan ekonomik düzene hiç itiraz etmeyip onun içinde onun kurallarına göre davranan kurumlara kızmak bana biraz haksızlık gibi geliyor.” (Katılımcı 4)

Katılımcı 4, çevrim içi ortamda reklam şirketlerinin sattığı ile reklamverenlerin satın aldığı şey arasında ona yüklenen anlam bakımından bir fark olup olmadığını şöyle açıklamaktadır:

“Reklamverenler açısından bakarsak, reklamveren neticede bir alan satın alıyor. Yani medyadan bir alan ya da zaman satın alıyor. Ama reklamveren açısından alınan satılan şeyin sadece bir reklam alanı veya zamanı olmasının dışında aslında orada alınan satılan başka bir durum olduğu söz konusu. Reklam alanını sağlayan yayıncı elbette ki bu alanın reklamverenlerin amaçlarına daha iyi hizmet edebilmesi için pek çok kullanıcı verisini alıp işleyip; hatta o alanı daha etkin hâle getirip satmak için bu verileri kullanıyorsa elbette meta hâline gelen şeyin kullanıcı verisi olduğunu söyleyebiliriz. “ (Katılımcı 4)

Katılımcı 4, kullanıcıların artık kendileriyle ilgisiz reklam görmekten rahatsız olduğunu, ilgi alanlarına dayalı reklamların platformların doğal akışlarına uyduğunu fakat onun da bıçak sırtı bir duruma neden olduğunu belirtmektedir:

“İnsanlar artık bir siteyi açtıklarında kendileriyle alakasız ya da en azından sitenin bağlamıyla alakasız bir sürü bambaşka içerik görmekten rahatsız oluyorlar. Dolayısıyla reklamcılar da en azından oranın bağlamına uygun reklam çıkıyorlar. Mesela bir Instagram’da veya Facebook’ta sponsorlu bir içerik ya da bir doğal reklam gördüğümüzde o sitenin doğal akışına uygun oluyor. Burada yine bıçak sırtı bir durum var. Hatta benim de yararlandığım bir makalede “iki ucu keskin kılıç” şeklinde bir metaforla anlatıyorlar bunu. Bir yandan bağlama uygun, dolayısıyla kullanıcıyı daha az rahatsız ediyor. Bu iyi bir şey kullanıcı için. Bir yandan da reklam olduğu dahi anlaşılamıyor, o zaman da aldatıcı mı? sorusunu akıllara getiriyor. Doğal reklamcılıkta da böyle bir tartışma var. “ (Katılımcı 4)

Katılımcı 3, kişiselleştirilmiş reklamın açık rıza alınması kaydıyla gösterilmesinin hukuka aykırı olmadığını ama özgür iradeyi yanıltabilecek sonuçlar doğurabileceğini belirtmektedir:

“Ben gerçekten benimle ilgili olmayan reklamlardan bunalmış olabilirim, sadece ilgimi çekenler karşıma gelsin diyebilirim. Bu bir seçenek ve bunun kural olarak açık rızayla alınarak yapılması lazım. Bana sebeplerini açıklayarak açık rızamı almış bir platform bana benimle ilgili reklamlar sunabilir. Hukuka aykırı gözüküyor. Ama bunun başka bir zorluğu olabilir. Sosyal medyanın kendi yapısından kaynaklanan yankı odaları, benim sürekli bir taklidimin bana sunulması dayatılması şeklinde gerçekleşebilir. Bu da özgür iradenin yanıltılmasıyla sonuçlanabilir. “ (Katılımcı 3)

Peki, bugün gözetlemeye ve kişisel veriye değil de web sitesi veya mobil uygulamanın içeriğine bağlı bir çevrim içi reklam sistemi daha aktif bir rol oynasa çevrim içi reklam endüstrisi ne kaybeder? Katılımcı 4, reklamverenlerin, yayıncıların ve reklam şirketlerinin birer işletme olduğunu hatırlatarak cevap vermektedir:

“%1’i bile niye kaybetsin, böyle bir durum da var. İşletmeye giriş dersi gibi, bütün şirketler kârlarını maksimize etmeye çalışırlar. Daha fazla kazanabilecekse neden kaybetsin?” (Katılımcı 4)

Katılımcı 4, ayrıca yalnızca bağlamsal reklam gösterme fikrinin günümüz reklamcılığı için naif kalacağını belirtmektedir:

“Benim verimi kullanma da web sitenin bağlamı neyse onu kullanarak reklam göster. Hiç benim kim olduğum, yaşı, cinsiyetim gibi özelliklerimle ilgilenme, ben o siteyle ilgileniyorsam bana ona göre reklam göster. Bu anlayış çok masumane bir yaklaşım, reklamcılar bunu neden yapsın diye bir soru çıkıyor ortaya. Dijital reklamcılar geleneksel işler için söyledikleri bir laf var ‘sık ve dua et’ ki doğru kitleye ulaşsın. Biz öyle değiliz biz hedefliyiz diye kendilerini öne çıkarıyorlar. Biraz buna benziyor, aslında her şey bağlamsal. Televizyona reklam vermek de bağlamsal. Ama onu dijitalde hedefli hâle getirmesi mümkünse bunu neden yapmasın? Bunu tercih etmemesi gibi bir durum bence söz konusu değil.” (Katılımcı 4)

Katılımcı 6, kullanıcının her halükârda bir reklama maruz kalacağını, alâkalı reklam görmesinin onun yararına olacağını söylemektedir:

“Kişiselleştirilmiş reklamların kitlesel reklamlara göre hem kullanıcıya hem de reklamverene avantajı olduğunu düşünüyorum. Reklamveren için daha alakalı daha doğru bir kitleye ulaşmak yararlı olacaktır. Reklama maruz kalan kullanıcılar için günümüz dünyasında bu reklam alanlarından zaten reklama maruz kalacağı değişkenini değiştirmediklerimizden alakasız bir reklam yerine daha alâkalı bir reklam görmesi kullanıcının zararına olmayacaktır.” (Katılımcı 6)

Araştırmanın nicel sahasında web siteleri ve mobil uygulamalardaki izleme teknolojilerinin tespiti sırasında onlarca reklam ve analitik çerezi tespit edilmiştir. Hatta başta gazete siteleri olmak üzere birden çok sitede ondan fazla analitik ve reklam şirketine ait çerezlerin yer aldığı belirlenmiştir. Katılımcı 6, özellikle büyük platformların kendi gelir optimizasyon ekipleri olduğunu ve onların reklam gelirlerinden en yüksek performansı almaya yönelik çalışmalar yaptıklarını paylaşmaktadır:

“Sitelerin kendi gelir modellerini inşa etmeleri için AdSense dışında diğer reklam borsalarını da kullanabilmeleri için programatik reklamcılığı kullanmaları gerekiyor. Programatik ile kısaca reklamveren ile yayıncıyı milisaniyeler içerisinde bir reklam alanının en doğru reklamverenle buluşturabilmektedir. Normalde AdSense’te 1000 gösterimi 1 TL’ye olan bir alanı yayıncı herkesin alımına kapatıp bu alana daha fazla bir fiyat koyabilir. Büyük siteler reklam alanlarını genelde diğer sitelere göre daha yüksek fiyata satabilirler, trafikleri daha değerlidir. (...) Reklam alanların daha fazla gelir elde etmesi için bazı optimizasyon çalışmaları yapılıyor. ” (Katılımcı 6)

Buna göre reklam yayınlayan web sitelerinin dâhili departmanlarında reklam alanlarından en yüksek verimi almaya yönelik çalışan kişiler, birçok analitik ve reklam şirketiyle çalışarak gelirini en üst seviyede tutmayı hedeflemektedir.

Katılımcı 6, programatik reklam satın alma sisteminin görüntüleme başına maliyet şeklinde ücretlendirildiğini fakat sistemde birçok aracının yer aldığını belirtmektedir:

“Programatik gösterim üzerinden maliyetlendiriliyor. Criteo veya Taboola tıklama başına maliyetle satıyor reklamverene mesela ama sattıkları alanı da günün sonunda gidip yayıncıdan gösterim başına maliyet ile satın alıyor. Yani yayıncı gösterim başına para kazanıyor. Yani sen reklamveren olarak üçüncü taraf bir yer ile çalışıyor ve tıklama başına ödüyor olabilirsin. Ama o üçüncü taraf orada bir arbitraj yapıyor. Aracılar olabiliyor, aracılardan aracısı olabiliyor. ” (Katılımcı 6)

“Teknik olarak tüm sistem araçlar üzerine çalışıyor. Google’ın, Amazon’un, Microsoft’un, Rubicon’un sistemini kullanıyor herkes. İnternet bir nevi insanların malı gibi. Bir sektör üzerine kurulmuş bir sürü kol gibi düşünebiliriz. ” (Katılımcı 6)

Katılımcı 6, çevrim içi reklamcılık içinde de tıpkı diğer teknolojik alanlarda veya platformlarda olduğu gibi tekelleşmenin söz konusu olduğunu söylemektedir. Buna bağlı olarak başta programatik olmak üzere çevrim içi reklam endüstrisinden şöyle söz etmektedir:

“Yayıncılar genelde Google ile çalışıyor. OpenX, Rubicon, Index gibi borsalar da var. 10 tane borsa vardır alanın %99’una hâkim. Bir borsa üzerinden reklam satın alınabiliyor. Borsalar da Google gibi. Aynı mantıkta çalışıyor. Yayıncının bir reklam alanı var, o alan tüm üçüncü taraf kodları çağırıyor. Birisi kazanıyor ve reklam gösteriliyor. Kazanma kısmı da değişkene bağlı olarak belirleniyor. Hedefleme değişkeninin merkezinde. ” (Katılımcı 6)

Katılımcı 6, ticari değeri oldukça yüksek olan konum verilerinin programatik ile nasıl kullanıldığını şöyle örneklendirmektedir:

“Konum verileri çok pahalıya satılıyor. Konum verisi bu arada İstanbul’u hedeflemek değil. Mesela bir benzin istasyonu zinciri kampanya yapacak. Her şubesinin 100 metre civarında reklam göstermek istiyor. Lokasyonda eğer koordinat verirsen o alana gösterebilirsin. Yalnızca yuvarlak olarak da değil, beşgen olarak da çizilebiliyor alan. Oralarda reklam gösteriliyor. Ya da outdoor reklamımın etrafında olan insanlara reklam göstermek istiyorum diyorlar. Hem outdoor’u görsün hem de telefonunda görsün reklamı isteyebiliyorlar. Bu gibi kullanılabiliyorlar. Normalde şehir hedeflemeye para vermezsin ama böyle niş kullanımlarda konum verileri satılıyor. Bin gösterim başına birkaç dolara satılabiliyor. Programatikte bunu yapabiliyorsun.” (Katılımcı 6)

Katılımcı 6, GDPR ve KVKK gibi düzenlemelerle birlikte teknoloji şirketlerinin de üçüncü taraf çerezlerin kullanımına kısıtlama getirdiğini ama bunun izlemenin son bulacağı anlamına gelmeyeceğini belirtmektedir:

“Apple kendi tarayıcısında çerez toplanmasını IDFA ile engelledi. Chrome yine 2022’de çerezlerin toplanamayacağını açıkladı. Bundan sonra cookie-less world adını verdiğimiz dünyaya geçtiğimizi söyleyebiliriz. Tabii çerez olmaması bundan sonra hiçbir kullanıcının takip edilemeyeceğini söyleyemeyiz. Bunun yapılış şekli değişmektedir.” (Katılımcı 6)

Özellikle yasal düzenlemeler üzerine Katılımcı 4, böylesine büyük bir endüstrinin kaderine terk edilmeyeceğini düşündüğünü söylemektedir:

“Kişisel veriler üzerine gelen düzenlemeler bir şeyleri zorluyor, bir şeyleri değiştiriyor olabilir ama benim gözlemim şöyle: Bu insanlar bu işten para kazanıyor. Onu etkileyecek, engelleyecek, zorlaştıracak bir şey varsa sürekli bir arka kapı bulma arayışı olduğunu görüyorum.” (Katılımcı 4)

Hatta yasal düzenlemelerin şirketlerin işine gelebilecek şekilde onları dönüştürdüğü fikrine de atıfta bulunuyor:

“GDPR ile birlikte mesela Google çok fazla şeyi değiştiriyor, dönüştürüyor ama bu konuda çalışan farklı akademisyenlerin söylediği şey Google aslında işleri kendisi için daha verimli hâle getiriyor. Kanunlar onları sınırlasa da, onlar o kanunlara uygun olmak koşuluyla iş verimliliğini yine de arttırıyorlar.” (Katılımcı 4)

Apple, geçen yıl yaptığı IOS güncellemesiyle kullanıcılara uygulamaların onları takip edip etmeme kontrolünü vermişti. Bu kontrol gözetlemeyi kontrol altına alma fırsatı sunduğu için doğrudan kişisel veriye dayalı reklamla da ilişkiliydi. Katılımcı 5, bu konuyla ilgili Amerika’da çıkan Facebook ve Apple arasındaki tartışmayı paylaşmaktadır:

“Zuckerberg, geçen sene Apple ile bir tartışma yaşamıştı. Apple cihazlarında izlemeyi kabul edip etmeme özelliğini kullanıcıya bırakacağını ilan etmişti. Bu özellik geldiğinde birçok insan kabul etmez. Ben kabul etmedim mesela. Uygulamalar beni izlemesin dedim. Facebook buna çok büyük bir yaygara çıkardı. O dönem Amerika’da tam sayfa ilanlar vardı ve savları da şuydu. Dediler ki, ‘Apple küçük esnafı bitirmeye çalışıyor. İnsanlar ticaret yapamaz hâle gelecek çünkü ben en küçük işletmeye bile hedefli reklam verme hakkı tanıyorum. Bunu da insanları takip ettiğim için verebiliyorum. Apple bunu izne tabi tuttuğu için insanlar izin vermeyecek, o zaman küçük esnaf batacak.’ Zuckerberg’in en büyük tehdidi de şuydu, böyle yaparsanız biz de Facebook’u paralı yapmak zorunda kalabiliriz. E yap o zaman. Neden yapmıyorsun? Yapamaz çünkü daha büyük bir gelirden, daha büyük kârlardan, dünya devi şirket olma özelliğinden feragat etmek zorunda kalır. ” (Katılımcı 5)

Toplam yıllık gelirinin %90’dan fazlasını reklam gelirleri yoluyla elde eden Facebook, Katılımcı 5’e göre bu gelirini korumak için elinden geleni yapmakta ve karşısına çıkacak olası tehlikeleri bertaraf etmeye çalışmaktadır. Bu çaba, kişisel verilere dayalı reklamcılığın platformlar için ne denli önemli olduğunun somut bir göstergesidir.

4.3.2.3. Kişisel Verilerin Korunmasına Yönelik Yasal Düzenlemeler

Bu ana tema altında hukukun kişisel verilerin korunmasını nasıl sağladığına ve buna ilişkin katılımcı görüşlerine yer verilmiştir. Nicel araştırmada tespit edilen üçüncü taraf çerezlerin, farklı amaçlarla yerleştirilen farklı izleme teknolojilerinin, çerez bildirimlerinin ve açık rıza onay kutularının hukukî açıdan değerlendirilmesine ihtiyaç vardır. Bu amaç doğrultusunda kişisel verilerin korunması üzerine uzman olan ve bu işi profesyonel olarak sürdüren bir avukat olan Katılımcı 3’ün değerlendirmeleri aşağıdaki alt temalara ayrılarak paylaşılmıştır.

4.3.2.3.1. KVKK Kanunu Çerezleri ve Açık Rızayı Nasıl Değerlendiriyor?

Katılımcı 3, Kişisel Verileri Koruma Kanununu şu sözlerle tanımlamaktadır:

“KVKK, 30 kusur maddeden oluşan çerçeve bir kanun. KVKK bütün kişisel veri düzenlemelerini teker teker işlemiyor. Hatta mümkün oldukça bundan kaçınmış durumda. Her alana uygulanabilecek bir yapı kuralım, böylelikle bütün kişisel veri işlemlerini denetleriz diye oluşturulmuş bir yapı.” (Katılımcı 3)

KVKK’da çerezlerin varlığına ilişkin bir madde bizzat yer almamaktadır. Bu çerçevede Katılımcı 3, kanunun çerezleri nasıl değerlendirdiğini şu şekilde açıklamaktadır:

“Peki KVKK çerezleri düzenliyor mu? Açıkçası düzenliyor. GDPR’da da açıkçası sadece bir yerde yazıyor çerez, o da çok spesifik bir konu. Çerez ile ilgili verilen kararların veya cezaların sebebi o hüküm mü? Değil.” (Katılımcı 3)

KVKK’da doğrudan çerez kelimesi yer almamasına rağmen kanunun çerezleri kapsamasının nedeni şöyledir:

“Eğer ben çerezle bir kişisel bilgi işliyorsam o da bir kişisel veridir. Yani çerezle ilgili işlediğim veriler sadece isim, soyisim gibi bilgiler olmak zorunda da değil. Hangi haberi okuduğum, hangi fotoğrafı görüntülediğim, bir sayfada ne kadar kaldığım, mouse’u hangi saniyede ne kadar durduğum ve bunlarla birlikte ve bunlarla bağlantılı hakkımda çıkarım yapılabilecek pek çok uygulama.” (Katılımcı 3)

Buna göre çerezlerin topladığı tüm kullanıcı verisi KVKK kapsamında değerlendirilmektedir. Bu noktada Katılımcı 3, kullanıcı verisi ile açık rıza arasındaki süreci kanun çerçevesinde şöyle açıklamaktadır:

“Çerezle ben bu veriyi işledim. Kural olarak açık rızasını almam gerekiyor mu? Evet. Kural olarak almamam gereken bir durum var mı? Bazı durumlarda olabilir, mesela kullanıcı bir alışveriş sitesinde üye girişi yaptı, bir ürünü görüntüledi ve ürünü sepete ekledi. Sitede başka sayfaları gezdi, üye girişi ve alışveriş sepetini hâlâ hatırlanmasını sağlayan şey çerezler. Buradaki çerez yapısını bir güvenlik tedbiri olarak düşünebilirsiniz. Yani bazı durumlarda sözleşme gereği için olabilir, hakkın korunması için olabilir diyebiliriz. Ancak bu özel olarak verdiğimiz örnekler dışındaki bütün örneklerde çerezler için açık rıza alınması lazım. Özellikle birkaç başlıkta sıralayabilirim: reklam kontrolü yapan, hedefli reklamcılık çerezlerinin bütünü

için kuşkusuz tüketiciye açıklama yapılarak açık rıza alınması lâzım. Ben sizin bu amaçla verilerinizi toplayım karşınıza bu ürünleri çıkaracağım, buna izin veriyor musunuz? Yapış metodum da bu, daha ayrıntılı bilgi istiyorsanız size veririm, bu çerezi kullanmak istiyor musunuz diye sorulması gerek. Aynı şekilde analitik ya da teknik ölçüm çerezleri vs. Sonuçta çerezle veri işlemek için kullanıcının açık rızasına ihtiyacımız var.” (Katılımcı 3)

Görüldüğü üzere, sitenin sadece verimli çalışmasıyla ve kullanıcı deneyimini sağlıklı biçimde yürütmesiyle ilişkili kendi çerezleri KVKK kapsamında açık rızaya tabi değilken diğer amaçlarla kullanılan çerezler söz konusu kanunda açık rızaya ihtiyaç duymaktadır. Diğer yandan bu durum başka bir soruyu da beraberinde getirmektedir. Üçüncü taraf olmayan, birinci taraf olan, yani sitenin kendi alan adıyla yer alan bir reklam veya analitik çerezi için web siteleri açık rıza almalı mıdır? Sorunun cevabını Katılımcı 3 şöyle izah etmektedir:

“Birinci taraf çerez web sitesinin çalışması için zorunluysa o zaman açık rızaya gerek yok. Ama yine analitik amaçlı vs. kullanılacaksa çerez, birinci taraf olsa bile açık rıza alınmasına gerek var.” (Katılımcı 3)

Buna göre çerezlerin aktif hâle gelmesi ve veri toplaması için kullanıcılardan açık rızasının alınması gerekmektedir. Açık rızaya ilişkin şu ifade oldukça önemlidir:

“Açık rıza bir sözleşme şartı olarak öne sürülürse, yani şu imzayı vermezsen seninle bu sözleşmeyi yapmam demek açık rıza değildir. Artık o sözleşme geçerli bir sözleşme değildir.” (Katılımcı 3)

Katılımcı 3’ün bu ifadesi “siteyi ziyaret ederek çerez politikamızı kabul etmiş sayılırsınız” metnlerinin yer aldığı çerez bildirim kutularının hükümsüz olduğuna işaret etmektedir. Çerez bildirimlerinin ve açık rıza onay kutularının web sitelerinde nasıl yer alması gerektiğini şöyle izah etmektedir:

“Çerezleri özelleştir, kabul et ve reddet butonları olmalı. Özelleştir kısmında yalnızca yüzeysel; yani analitik, reklam gibi kategorilendirmeler değil, tüm şirketlerin isimleri yer almalı. Bir kullanıcı Adobe’a veri göndermek isteyip, Google’a göndermek istemeyebilir. Bunların seçimi kullanıcıya bırakılmalı.” (Katılımcı 3)

Hukuk çerçevesinde değerlendirildiğinde kullanıcılar bir web sitesini ziyaret ettiğinde veya mobil uygulamayı kullanmaya başladığında izleme teknolojilerinin

aktif hâle gelip gelmemesi kullanıcının açık rızasına bırakılmalıdır. Katılımcı 3 bunu net bir şekilde ifade etmektedir.

4.3.2.3.2. Türkiye’de Web Siteleri Yasal Açıdan Ne Derece Sorunlu?

Katılımcı 3, hem Türkiye’de hem de dünyada web sitelerinin, mobil uygulamaların ve diğer dijital platformların hukukî bağlama uygunluklarını ilgili ülke ve yasalara göre değiştiğini söylemektedir:

“Sadece Türkiye’de değil dünyanın her yerinde web sitesi var ve her ülkenin kendi egemenlik hakkı var. Doğal olarak her ülkenin demokrasiye, insan haklarına, mahretmiyete bakış açısı farklı. ABD’nin, Avrupa’nın ve Türkiye’nin bakış açıları farklı. Örneğin Avrupa’daki kıstasların daha yukarıda, ABD’nin daha aşağıda gözükebilir. Türkiye’den baktığımızda ise Türkiye’deki web siteleri hukuka çok uygun değil.” (Katılımcı 3)

Görüşmeci, bir araştırmayı örnek sunarak GDPR’ın etkin olduğu Avrupa ülkelerinde web siteleri ve mobil uygulamaların yasalara uygunluğunun kısıtlı olduğuna yer vermektedir:

“Avrupa’da durumlar nasıl? Bununla ilgili bir çalışma yapılmış. Bu çalışma sonucunda web sitelerinin yalnızca %34’ü GDPR’la uyumlu çıkmış. Hele ki bu oran Almanya gibi bu işin temelinde olan ülkelerde daha yüksek çıkmışken doğu Avrupa ülkelerinde hiç denecek kadar az çıkmış. Portekiz %17 uyumlu çıkmış, Danimarka, Estonya, Hollanda çok daha az uyumlu ülkeler olarak karşımıza çıkıyor. Avrupa, bu işin merkezî olmasına rağmen oranlar çok düşük.” (Katılımcı 3)

Nicel araştırma bulgularında web siteleri ve mobil uygulamalarda tespit edilen izleme teknolojilerinin hemen hemen tamamı yurt dışı kaynaklı şirketlere aitti. Dolayısıyla kullanıcı bilgilerini toplayan bu şirketler verileri kendi sunucularına aktarmaktadır. Buradaki sorun, KVKK kapsamında verilerin yurt dışına aktarılmasının suç olmasıdır. Katılımcı 3, bu bulguyu şöyle değerlendirmektedir:

“Türkiye’deki web sitelerinin büyük bir kısmı sunucularını yurt dışında tutuyor. Yurtdışı sunucuları hem ucuz, hem güvenli Türkiye’deki sunuculara göre. Hem de hızlı çalışıyor. Amazon, Microsoft, Google’ın sunucuların Türkiye’de bir alternatifi yok. Ama KVKK’ya göre yurtdışına veri aktarımı bir suç.” (Katılımcı 3)

Buna göre yalnızca Google, Facebook, Amazon veya Twitter değil; Criteo, Taboola, Pubmatic, Moat Oracle ve diğer analitik ve reklam şirketleri de Türkiye’deki site ve uygulamalardan topladıkları kullanıcı verilerini kendi sunucularına aktarırken yasa kapsamında suç işlemektedirler.

Katılımcı 3, Türkiye’deki web sitelerinin hukuka uygunluk durumunu tartışırken Kişisel Verileri Koruma Kurumu’nun dört büyük bankaya verdiği cezanın nedenini ve sonucu paylaşmaktadır:

“Bankacılık sırları en büyük sırlardır. Devlet sırrından sonra özel olarak sır saklama yükümlüğünün ilk girdiği kanunlardan birisidir. Banka gizliliğe özel bir önem vermesi gereken bir kurum. Türkiye’nin dört büyük bankası saçma sapan aydınlatma politikaları hazırlamışlar ve bundan dolayı bir meslektaşımız şikâyet etmişti. Kişisel Verileri Koruma Kurumu bu dört bankaya ceza verdi. Yanlış olan şey ise banka sadece şunu yazmış: ‘Web sitemize girip bizim hizmetlerimizden faydalaniyorsanız kişisel verileriniz bankacılık işlemlerinin gerçekleştirilmesi, işlem sonuçlarının hazırlanması, gerekli yerlere verilmesi için kanunun 5. ve 6. maddesi gereğince işlenecektir. Başka hiçbir bilgi yok. Yani ben şunun cevabını alamıyorum, sen benim bu bilgimi neden işliyorsun cevabı yok. (...) Spesifik olarak hiçbir şey açıklamıyor. Sonra kurum bu dört bankaya ceza verdi. Bunlarda birine özellikle bu yanlıştır, bunları faaliyet bazlı düzelt dedi. (...) Karar verdi, talimatlandırdı ve banka hiçbir işlem yapmadı. Bir ay sonra kurum yine toplandı, talimatlandırdı, yine ceza verdi banka yine bir şey yapmadı. Sanırım bu şekilde üç tane üst üste ceza aldı, dördüncüsünü bilmiyorum ama gördüğüm herhangi bir gelişme de yok. Türkiye Cumhuriyeti’ndeki kurumların KVKK’ya uygunluğu buradan görülebilir.” (Katılımcı 3)

Web sitelerinin ve özel sektördeki kurum ve kuruluşların KVKK ile uyumluluğun sorgulanması beraberinde devlet kurumlarının KVKK uyumluluğunun ne durumda olduğunu gündeme getirmiştir. Katılımcı 1’e göre devlet kurumlarının kişisel verilerin korunmasına yönelik durumu özel şirketlerden farklı değil:

“Türkiye Cumhuriyeti’ndeki en fazla veriyi işleyen veri sorumlusu kim derseniz devlet ve bakanlıklardır derim. Ancak hangi bakanlık KVKK’ya uyumlu hareket ediyor, faaliyetlerinde aydınlatma yapıyor, kişileri bilgilendiriyor derseniz belki biraz Sağlık Bakanlığı, o da HES dolayısıyla diyebiliriz. En çok veriyi İç İşleri Bakanlığı işliyor. Ama İç İşleri Bakanlığının KVKK ile ilgili bir tane adım yok.” (Katılımcı 3)

Devlet kurumlarının kişisel veriler üzerine şeffaf bir metne sahip olmamasını nicel araştırma sırasında eba.gov.tr’de ve meb.gov.tr’de çerez politikası veya gizlilik

sözleşmesi olmaması örneğinde görmüştük. Dolayısıyla kendi bağlamı içerisindeki bulgularımız, Katılımcı 3'ün ifadesine ek bir katkı sağlamaktadır.

4.3.2.3.3. Yasaların Uygulanabilirliği ve Cezaların Caydırıcılığı

Gerçek hayatta birisinden izin almadan ona ait belgeleri karıştırmak, ondan habersiz dosyalarını almak, kopyalamak veya çoğaltmak yasalara göre suçtur. Çevrim içi ortamda bu işlemler daha farklı ve esnek görülebilmektedir. Genel kanı, insanların çevrim içi olduklarında artık özel bir şeylerinin kalmadığı ve isteyen kişiyle ilgili istediği veriyi toplayabileceği şeklindedir. Peki, gerçekten de fiziksel dünyada birisinin dokümanını habersiz almakla, dijital dünyada birisinin verisini habersiz toplamak arasında bir fark var mı? Katılımcı 3, farkın olmadığına şöyle değinmektedir:

“Aralarında bir fark yok. İkisi de aynı şekilde suç. Aradaki fark karar alıcılar ve karar vericilerin cehaleti. Bir karar alıcı ya da verici bir çerezin nasıl çalıştığını biliyor olsaydı, gerçek anlamıyla, bunun TCK'nın 135. ve 136. maddeleri kapsamında olduğunu çok iyi bilirdi. Hatta bu maddeler bile değil TCK 243, 244 kapsamında, bir sisteme veri yerleştirme ve bu verileri alıp başka yere götürme, olduğunu çok rahat bilirdi. Neden, çünkü benim hiçbir fikrim yok bununla ilgili, bir uyarı bile yapılmıyor, birden benim haberim bile olmadan bütün tıklamalarım bütün Mouse hareketlerim, öncesinde yaptığım web'teki tüm hareketler bir şekilde başka birinin sunucusuna gidiyor. Yani benim cihazımda toparlanıyor öncesinde ne yaptıklarım. Gizli dinleme cihazı gibi düşünün. Dinleme cihazını yerleştiriyor benim cihazıma, akabinde bu verileri topluyorlar ve başka birine gönderiyorlar. Bu açıkça verileri bozma, başka birine gönderme, verme, ele geçirme suçudur TCK 244 kapsamında. Sebep aynı sonuç aynı. Eğer bir ülkede karar alıcılar ya da karar vericiler bir konu hakkında yeterince bilgi sahibi değilse onların bilmediği bütün işlemler yapılabilir o ülkede.” (Katılımcı 3)

Bu ifade gösteriyor ki kişinin cihazına açık rızasını almadan bir çerez yerleştirmenin masasının altına gizli bir dinleme cihazı koymaktan bir farkı yoktur. Her ikisi de suçtur; hukuk karşısında biri diğerinden daha hoşgörülebilir bir durumda değildir. Birisi hayatı önem taşıyan bir dosyayı çalabilir, diğeri yalnızca reklam amaçlı veri toplayabilir. Amaçları ve sonuçları farklı olsa bile her iki durum kişiden habersiz gerçekleşmektedir.

Katılımcı 3'ün yorumunda dikkat çeken bir başka nokta verdiği yasal dayanakların KVK kanunundan değil, Türk Ceza Kanunundan olmasıdır. Yani, KVKK'dan önce TCK kapsamında da bu durum suç teşkil etmektedir.

Bir diğer önemli nokta, Katılımcı 3'ün yasaların uygulanması hakkındaki düşünceleridir. Gerek nicel araştırma bulgularında, gerekse Katılımcı 3'ün yorumlarında gördüğümüz üzere birçok çevrim içi platformun veri toplama ve paylaşma biçimi hem KVKK'ya hem de TCK'nin ilgili maddelerine uygun değildi. Katılımcı 3, bu platformlara bir yaptırım olmamasının nedenini karar alıcılar ve karar vericilerin çerezlerin kullanımı, işlevi ve özellikleri hakkında bilgi sahibi olmamasına bağlamaktadır. Açık rıza almadan çerezleri aktif hale getirerek veri işlemeye yönelik verilen tek ceza, daha önce paylaşıldığı gibi Amazon.com.tr'ye verilmişti. Oysaki karar özeti okunduğunda diğer birçok e-ticaret sitesinin Amazon'daki noksanlıklara sahip olduğu görülebilmektedir. Emsal oluşturması gereken bir cezanın diğer sitelere ve platformlara uygulanmaması da ayrı bir soru işaretidir. Katılımcı 3, bu ayrıklığın kendi sektörü içindeki yansımalarını ve firmaların duruma bakış açısını şöyle özetliyor:

“Şirketler, hatta benim hizmet verdiğim firmalar da bana bunu soruyor. Siz bana bunu söylüyorsunuz ama rakibim patır patır çerez kullanıyor, bunun için izin de almıyor, ceza da yemedi. Ama ben burada her çerez kullanmadığım gün için şu kadar zarar ediyorum aslında diyor. Burada edeceğim zarar mı daha fazla yoksa KVKK'ya 100 bin lira, 200 bin lira, 1 milyon mu daha fazla. Böyle bakınca şirketler de doğal olarak kendi varoluş amaçları olan kârlılıklarını gözetiyorlar. Bunun çözümü, bir hukuku tesis etmek. İki kanunları uygulanır kılmak. Başka bir çözümü yok.” (Katılımcı 3)

Kişisel verilerin güvenlik açıkları neticesinde çalınması, aydınlatma eksikliği veya bütüncül bir bakış açısıyla verilerin toptan işlenmesi gibi nedenlerle bugüne kadar bazı şirketlere KVK Kurumu tarafından ceza verilmiştir. Diğer yandan cezaların caydırıcı olup olmadığı da farklı bir tartışmayı beraberinde getirmektedir. Çünkü Katılımcı 3'ün daha önce ifade ettiği gibi, özel bir banka dört kere ceza yemesine rağmen aydınlatma metnini düzeltmeyerek cezaya çarptırılmasına neden olan biçimde kişisel verileri işlemeye devam etmektedir. Katılımcı 3, verilen cezaların etkisini ve caydırıcılığını Yemeksepeti üzerinden örneklendirmektedir:

“Yemeksepeti yakın zamanda 20 milyon kişinin bütün kişisel verilerini çaldırdı. Dediler ki, ama merak etmeyin şifreler şifreliydi. Yani kendi şifreleri kırılarak sistemlerine girilebileceğini kabul ediyor, ancak kendi şifreleme metoduyla yaptıkları şifrelemenin kırılacağına ihtimal vermiyor. Bunun karşılığında KVKK’ya bir bildirim yaptılar, muhtelemeden KVKK en üst sınırdan bir ceza kesecek Yemeksepeti’ne. Ne kadarlık bir ceza kesecek? 2 milyon lira civarı. Peki, bu kadar kişinin bu kadar verisini; kullanıcı adlarını, adreslerini, ‘şifreli olan şifrelerini’ ve bütün diğer kayıtlarını çaldıran Yemeksepeti, 2 milyon lira vererek bir şey kaybedecek mi? 2 milyon lira ile Yemeksepeti’nin herhangi bir zarara uğramadığını görüyoruz. Zaten büyük bir organizasyon olan Yemeksepeti hiçbir şekilde etkilenmeyecek. Avrupa’da olsa etkilenecekti, neden? Avrupa’da GDPR diyor ki 20 milyon euro ya da yıllık global cirosunun %4’ü kadar ceza verebilirim, hangisi daha yüksekse. Büyük ve caydırıcı bir ceza esasında. Ama 2 milyon tl Yemeksepeti için caydırıcı bir ceza değil. O yüzden hiçbir şey meydana gelmiyor, bir şeyle karşılaşmıyorlar.” (Katılımcı 3)

Bahsi geçen bu örnek, cezaların şirketler üzerindeki sınırlı da olsa etkisini anlamak noktasında dikkat çekicidir. Yemeksepeti veya milyonlarca insanın verisini tutan bir başka şirket yarın yine söz konusu verileri çaldırırsa birkaç milyon lira ceza dışında herhangi bir denetim veya yaptırımla karşılaşmayacaktır. Şirketlerin daha önce paylaşılan veri güvenliğinin temel ilkelerini gözden geçirerek buna uygun hareket etmesi, karar alıcı ve verici kurumların kişisel verilerin toplanmasına, işlenmesine veya çaldırılmasına yönelik daha ciddi bir bakış açısı ve uygulama geliştirmesi gerekmektedir.

4.3.2.4. Veri / Gözetim Farkındalığı ve Mahremiyet

Bu tema altında kullanıcıların veri gözetimi üzerine farkındalıkları, veri gizliliği, mahremiyet, özgür irade, manipülasyon ve teknoloji hizmetlerden mahrumiyet gibi çeşitli konular yer almaktadır. Birden çok katılımcının görüşleri belirli alt temalar oluşturularak işlenmiştir.

4.3.2.4.1. Mahremiyet Tartışması

Mahremiyet hakkı bugün insanın en temel haklarından birisi olarak kabul edilmektedir. Katılımcı 3, kişisel verilerin korunma ihtiyacının ve mahremiyetin bugüne özel bir durum olduğunu açıklarken şu ifadeleri kullanmaktadır:

“Kişisel verilerin korunması ya da genel hatlarıyla mahremiyet genel ve zamansız değil, yerel ve bu zamana özgü bir ihtiyaçtır. Örneğin, diyelim ki 16. yüzyılda bir Fransızınız. Aşk romanı yazan biri geliyor ve size ‘harika bir aşk hayatınız var’ deyip sizin adınıza bir kitap çıkarıyor. O dönem sizin adınızın bir kitapta geçmesi büyük bir onur olarak karşınıza çıkıyor. Ya da M.Ö. 13. yüzyılda Tutankamon’un adının Mısır kil tabletlerinde veya piramitlerin üzerinde kazınmış olması Tutankamon için büyük bir onurdu. Yani bir verisinin bir yere işleniyor olması. Bunun anlamı, tarihte bizim bugün kişisel verilere verdiğimiz anlam verilmiyordu. Gelecekte de belki verilmeyecek.” (Katılımcı 3)

Katılımcı 3, kişisel verilerin korunmasına ve mahremiyete atfedilen önemin ve ona olan ihtiyacın zamandan zamana değiştiğini dile getirmektedir. Önem ve ihtiyacın oluşmasındaki temel nedenin tabii ki yeni medyada ortaya çıkan gelişmeleri olduğunu söylüyor:

“2010’lardan sonra sosyal medya ve üçüncü nesil web ile artık biz diyoruz ki herkesin çılgınlar gibi fotoğraf video yüklediği, kendiyle ilgili her şeyi paylaştığı, yanımızda gezdirdiğimiz akıllı saatlerimizle cep telefonlarımızla izlendiğimiz bir dünyada artık bizim kendi bilgilerimizin bize karşı kullanılmasından korunmamız gerekiyor.” (Katılımcı 3)

Mahremiyete bakış açısı farklı çıkarlar doğrultusunda da şekillenebilmektedir. Facebook kurucu CEO’su Mark Zuckerberg 2010 tarihli bir röportajında *“insanların yalnızca daha fazla ve farklı bilgileri paylaşmakla kalmayıp, aynı zamanda daha açık olarak daha çok insanla rahat hissettiğini”* ve mahremiyetin artık sosyal bir norm olmadığını dile getirmiştir. Aynı kişi muhtemelen mahrem alanını genişletmek için Palo Alto’daki evinin bitişiğindeki dört evi 30 milyon dolar karşılığında satın almıştır (Greenwald, 2014: 158).

Mahremiyet tartışmalarında saklayacak bir şeyi olmayanların korkacak da bir şeyi olmadığı sıklıkla dile getirilir. Genellikle bu söylem sakladığı hiçbir şey olmadığını düşünen insanlar tarafından söylenir. Ayrıca benzer bir konuya şirket yöneticileri de değinmektedir. Google’ın o dönemki CEO’su Eric Schmidt 2009 yılında şöyle bir ifadede bulunmuştur: *“Başkalarının bilmesini istemediğiniz bir şeyler yapıyorsanız, belki de her şeyden önce bunu hiç yapmamanız gerekmektedir.”* Bu ifade, şirketin kendi sorumluluklarından sıyrılıp olası sorunları mahremiyet talep eden insanların üstüne bindirmekte ve Katılımcı 1’in ifadesiyle “kurbanı suçlama” şeklinde

kendini göstermektedir. Düşünür Lars Fr. H. Svendsen ise “*Mesele saklayacak bir şeyimizin olması değil, insanın, sakladığı bir şeyi olup olmadığını düşünmeye hiç mi hiç gerek duymadığı alanlarının olmasıdır.*” (Lokke, 2018: 22) diyerek konuyu kurbanı suçlama mantığından almış ve insana saygı perspektifine yerleştirmiştir.

Katılımcı 1, ‘saklayacak bir şeyim yok’ fikrine ilişkin fikirlerini aşağıdaki gibi açıklamaktadır:

“Bunun köküne gelirsek, saklamakla ilgili bir şey değil. Saklayacak bir şeyim yok diyenler, oldu saklayacak bir şeyin yok ama bu benimle her şeyi paylaşmak istediğin anlamına mı geliyor? Bu farklı bir şey. Evet belki saklayacak bir şeyim yok, evet farklı bir şey yapmıyorum. Ama bu aynı zamanda seninle her şeyi paylaşmak istediğim anlamına da gelmez. Zaten mahremiyetin anlamı da bu. Neyi kendine saklamak istediğine, neyi başkalarıyla paylaşmak istediğine karar verme hakkı.” (Katılımcı 1)

Katılımcı 4, veri toplayan platformların, sitelerin ve üçüncü taraf şirketlerin kullanıcılara bunu açıkça bildirmeleri gerektiğini savunmaktadır. Diğer yandan bu bildirimin bazı durumlarda mahremiyet kaygısını azaltmak yerine aksine artırabileceğine de dikkat çekmektedir:

“Bir internet kullanıcısı olarak baktığımda veri toplayanlar bilgilendirme yapmak zorunda. Nasıl olsa anonim ne istersem toplanır diye bir dünya yok. Benim anonimlerim de değerli. Burada bilgilendirmenin şart olduğunu ama bunun da mahremiyet kaygısını azaltması gerektiğini düşünüyorum. Ama aksine bir insanın eğer hiçbir şekilde böyle bir veri topladığına dair bilgisi yoksa o zaman da böyle bir açıklamanın yapılması durup dururken bir mahremiyet kaygısı yaratabilir. İş burada dönüp dolaşıp dijital okuryazarlığa geliyor. İnsanlar bir zahmet internet kullanımının ne olduğunu bilsinler. Kendilerine hizmet veren kurumların kar amacı gütmeyen hayır kurumları değil, birer işletme olduklarını bilsinler ve ona göre davransınlar. “ (Katılımcı 4)

Benzer şekilde, Katılımcı 7 de verilerin toplanmasına yönelik bir bildirimin hiç yoktan bir tepki yaratacağını dile getirmektedir:

“Bu şirketlerin ‘biz sizlerin verinizi topluyoruz’ demesi dikkat edilmeyen bir konuyu gündeme getirdiğinden dolayı insanların tepkisi artacaktır. Gündemde olmayan bir konuyu dile getirmek, yanlış bir strateji olur.” (Katılımcı 7)

Buna göre, hakkında veri toplanması da dâhil dijital süreçlerin nasıl gerçekleştiğine dair hiçbir bilgisi olmayan kullanıcılar karşısına bir anda çıkan çerez bildirim ve açık rıza onay kutusunu gördüklerinde panik yaşayabilirler. Dijital okuryazarlığı düşük olan ve hangi verilerinin toplandığını bilmeyen bir kullanıcıya, hangi verilerinin toplandığı bildirilirse ve “kabul et” seçeneği sunulursa muhtemelen bu durum onun için kaygı verici olacaktır.

4.3.2.4.2. “İstemiyorsan Kullanmamakta Özgürsün”

Ceglowski (2016), hizmetleri kullanmayarak gözetim kapitalizminden kurtulmakta insanın her zaman özgür olduğunu fakat bunun artık neredeyse elektrikten vazgeçmekle eşdeğer olduğunu söylemektedir. Diğer yandan bakıldığında, “verilerinin toplanmasını istemiyorsan ilgili platformları kullanma” fikri de sıkça karşımıza çıkmaktadır.

Katılımcı 4, platformların birer şirket olduğunu hatırlatarak söz konusu fikri açmaktadır:

“Google’da bir şey aradığımızda Google’ın bizim verimizi toplamamasını istememiz gibi bir lüksümüz yok. Çünkü Google bir şirket, kamu kurumu veya hayır kurumu değil.” (Katılımcı 4)

Katılımcı 7, hizmetlerin maliyetlerinin karşılanması için bir gelir kaynağına ihtiyaç olduğunu ve mahremiyetine önem veren insanların bu modele sahip sistemlerin alternatiflerine yönelmeleri gerektiğini belirtmektedir:

“Bir hizmetin ücretsiz olmasının ‘genel’ sebebi, verilerimizin kullanılmasındandır. Bir hizmetin sunucusunun olması, o sunucunun ve hizmetin teknik desteğinin olması, pazarlamasının ve satışının gerçekleştirilmesi için bir gelir kaynağına ihtiyaçları olmasındandır. Evet, açık kaynaklı birçok aktivistin ve topluluğun oluşturduğu hizmetler mevcuttur fakat sürdürülebilir bir gelir modelleri olmadığından dolayı bu hizmetler ya kapanmaktadır ya da bize o ücretsiz hizmetleri sağlayan diğer şirketlere satılmaktadır. Kullanmamak bir çözüm değildir, korunmak ve mahremiyetini nasıl sağlayacağını bilmek çözümdür. Ublock gibi birçok script engelleyici, DuckDuckGo gibi açık kaynaklı uygulamalar, Debian gibi işletim sistemleri ile mahremiyetimizi koruyabiliriz. Kullanmayan insan modern hayattan soyutlanmaz.” (Katılımcı 7)

Her yıl daha fazla kâr elde etmek için çalışan web platformları tıpkı diğer işletmeler gibi kârlılığını artırmanın yollarını aramaktadır. Bu bağlamda birer işletme olan bu platformların penceresinden bakarsak kullanıcılar ya hizmet karşılığında verilerini paylaşacak (ki işletme kâr elde edebilsin) ya da hizmeti kullanmayarak bu sürecin içinde olmayacaklar.

Katılımcı 5, “istemiyorsan kullanma”nın bir çözüm olmadığını ve bunun kişinin tercihine kalmadığını Fuchs’un yorumlarına atıfta bulunarak paylaşmaktadır:

“Kullanmamak gibi bir lüksümüz maalesef yok. Örneğin, WhatsApp’ta yoksan emekçi olarak bile var olma hakkın yok. Bugün bir tesisatçı Signal kullansa bomboş bekleyebilir, rakibi WhatsApp kullandığı için işler ona gidebilir. Böyle bir lüks yok. Ne akıllı telefon kullanmama lüksümüz var, ne de büyük platformları kullanmama lüksümüz var. Zaten Christian Fuchs dijital emek ile ilgili çalışmalarında bunu vurguluyor. Bu senin kendi tercihin diyemezsin diyor. İnsanlar artık sosyal bağlantılarını kaybetmemek için buna mecbur. Buna mecbur olduğun için de sen onun oradaki mecburiyetini kullanıyorsun. Sömürüyorsun o mecburiyeti. (...) Bu platformlar tercihine bağlı gibi bir durum yok.” (Katılımcı 5)

Katılımcı 1, Ceglowski’nin ifadesine benzer şekilde hizmetlerin kullanılmaması önerisini şu ifadelerle eleştirmektedir:

“Bir başka durum, istemiyorsan kullanma. Bu artık geçerli değil. Hiçbir zaman geçerli değildi ama bugün görebiliyoruz ne kadar geçersiz olduğunu. Çünkü bu Silikon Vadisinin de savunmasıydı. İşte sevmiyorsan Google’ı, onu kullanma, başka şey kullanırsın. Veya bu web sitesine gitme, bu gerekli değil ki yaşamak için. Bugün bakıyorsun, iki tane şirket neredeyse tüm cep telefonlarına sahip. Android ve IOS. Şimdi eğer beğenmiyorsan kullanma dediğinde kendini modern hayattan sök diyorsun. Bugün Ikea yeni evler yapıyor, akıllı evler yapıyor. İçine akıllı cihazlar koyuyor. Yakında eğer istemiyorsan kullanma, o evde oturma anlamına gelecek. Öyleyse araba kullanma, çünkü bütün arabaların içinde olacak bu.” (Katılımcı 1)

Katılımcı 1, mevcut durumu bütüncül bir bakış açısıyla değerlendirmektedir. Katılımcı 5 ise kimlerin istemiyorsa kullanmayacağı lüksüne sahip olduğunu oldukça basit bir örnek ile açıklıyor:

“Verilerinin toplanmasını istemiyorsan telefonunu kullanma. O lükse sadece süper zenginler sahip. Çok zengin olacaksın, emrinde onlarca insan çalışıyor olacak. O yüzden sen hiçbir sosyal medya platformuna girmeyeceksin. Senin yerine oradaki sosyal bağlantılarını sekreterin,

asistanların kuracak. Ancak o zaman kullanmayabilirsin. Zaten dizilerde de (Black Mirror dizisine işaretle) bunun işlendiğini görüyoruz. Büyük teknoloji sahibi, internetin ve telefonun çekmediği kilometrelerce uzaktaki bir çölde kendisine bir mabed yapmış. Orada yoga yapıyor, terapi yapıyor. Neden? Çünkü öyle bir lükse sahip. Bir şey olunca da ona hemen helikopterle gidip müdahale ediyorlar. Bizim emrimizde çalıştırabileceğimiz böyle bir şey yok. İstemiyorsan kullanma bu yüzden saçma ve olayı anlayamamak.” (Katılımcı 5)

Katılımcı 5’in bu yaklaşımı hâkim teknolojinin tabandaki varlığının ne kadar zorunlu ve hayatını idame ettirebilmek için önemli hâle geldiğini anlatmaktadır. Eskiden belirli bir teknolojiye üst sınıf gelir grubuna ait insanlar erişebilirken artık herkes erişebiliyor. Bu teknolojilerin tabana yayılması iş yapış biçimlerinden ve iletişime her süreci kendi içine dâhil etmesiyle sonuçlanmıştır. Dolayısıyla artık ona erişmeme tercihi yalnızca süper zenginlerin bir tercihi hâlini almıştır.

Başta nesnelerin interneti olmak üzere birbirini takip eden tüm teknolojiler veri toplamakta ya da gelecekte eninde sonunda veri toplamak üzere tasarlanmaktadır. Dolayısıyla hizmeti kullanmama seçimi ile modern hayattan soyutlanma arasında pozitif bir ilişki ortaya çıkmaktadır.

Sistemik problemler kişisel problemlere dönüştürülüyor. İklim değişikliği gibi. Teknolojide de aynı şey: ‘niye kullanıyorsun o zaman’, ben ne kullanacağım o zaman? ” (Katılımcı 1)

Katılımcı 1, kişilerin suçlanmasının sistemsel problemin üstünü kapatmadığını ve asıl sorunun “istemiyorsan kullanma”da değil, mevcut sistemde olduğunu söylemektedir:

“Bu çok büyük bir problem ve bu kurbanı suçlama. Sen yatırılacak paranın %99’unu bu sistemin içine yatırıyorsan ve bütün platformların ve ürünlerin iş modeli aynıysa, ondan sonra da ‘sen bunları kullanıyorsan senin hatan.’ Hayır, bu sistemik bir problem, bu kapitalizm problemi, gözetim kapitalizmi problemi. Niye biz paraları bu platformlara yatırıyoruz, niye biz bu platformları yaratıyoruz, sonra da insanlara bunları kullanma diyoruz.” (Katılımcı 1)

Katılımcı 1, hizmetlerin tekelleşmesi ve tüm teknolojik yeniliklerin hâkim gözetim sisteminin üzerine inşa edilmesi nedeniyle “istemiyorsan kullanma” görüşünün geçersiz olduğunu söylemektedir.

Bir başka durum, Katılımcı 7'nin bahsettiği alternatif açık kaynaklı yazılımların ve gözetime direnme uygulamalarının kullanımıyla ilgilidir. Katılımcı 1 bu alternatiflerle ilgili şu ifadeleri kullanmaktadır:

“Buna rağmen alternatifler var WhatsApp yerine Signal kullanabilirsin. Ama Facebook trilyon dolarlık bir şirket, Signal’i yapanlar birkaç sene önce bir avuç insandı. Ne kadar uzun süreli bir alternatif olur bilinmez. Ama bu alternatifler istatistiksel olarak yok gibi.” (Katılımcı 1)

Alternatiflerin istatistiksel olarak neredeyse yok denecek kadar az olduğu bir yana, Katılımcı 1 bazı gizlilik savunucusu alternatif uygulamaların arka planına bakıldığında gözetim kapitalizminden beslenen sistemlerin olduğunu söylüyor:

“Tek yapman gereken parayı takip et. Çünkü o kadar hızlı büyüyorlar ki. Mozilla’ya bakıyorsun biz sizin haklarınızı koruyoruz diyorlar. Bütün paranız nereden geliyor diye sorduğunda Google’dan geliyor. Ondan sonra neye ihtiyaç var ki. Bu ne yazık ki çoğu yerde böyle. Alternatifler üzerine çalışanlar aynı sistem tarafından fonlanıyor.” (Katılımcı 1)

Özetleyecek olursak hizmeti kullanmamakta özgür olan bir kullanıcıyı bir soyutlanma beklemektedir. Fuchs (2015: 401), insanların sosyal varlık olduklarını ve başkalarıyla girdikleri ilişkilerle var olduklarını dile getirir. Bu bağlamda iletişimin, insanın varoluşunun sosyal bir boyutu olduğunu ima eder. Günümüzde bu hizmetleri kullanmamak, bir anlamda iletişimi ortadan kaldırarak insanın sosyal bir varlık olmasını tehlikeye atmaktadır. Bu tehlikenin oluşumu Katılımcı 1 ve Katılımcı 5’in görüşlerinde yer almaktadır.

4.3.2.4.3. “Verilerimin Toplanması Umrumda Değil”

Birçok insan gerek gözetimi gerekse verilerinin farklı platform ve şirketler tarafından toplanmasını umursamama eğilimindedir. Kullanıcıların umursamamasının altında yatan nedenler farklı farklı olsa da genel olarak “topladıkları verilerle ne yapabilirler ki” veya “benim verilerim onlar için neden önemli olsun ki” gibi görüşler etrafında şekillenmektedir. Hatta bu durumun bir güldürü unsuru olarak da popüler kültür içinde işlendiği görülebilmektedir; örneğin Cem Yılmaz'ın “CIA senin hesabını ne yapsın” gibi bir durum canlandırması ile toplumsal hafızada yer ettiği söylenebilir.

Öte yandan şirketler genellikle topladıkları verileri anonim olarak tuttuklarını, dolayısıyla kimsenin durumdan endişe duymaması gerektiğini beyan etmektedir.

Katılımcı 4, hem şirket hem de kullanıcı tarafından bakarak uç noktalarda durumun yanlış olduğunu dile getiriyor:

“Veri toplamayı tümünden reddetmek ne kadar yanlışsa, aman canım ne olacak demek de bir o kadar safça.” (Katılımcı 4)

Katılımcı 5, verilerinin toplanmasını umursamayan insanları sınıf bilinci olmayan işçilere benzetmektedir:

“Verilerinin toplanmasını umursamayan insanları sınıf bilinci olmayan emekçilere, işçilere benzetiyorum ben. Sömürüldüğünü anlamayan insanlardaki bilinçsizlik nasıl bir bilinçsizlikse ve o halk kitlelerinin aydınlatılması gerekiyorsa, umurunda olmayanlar da aynı yerde.” (Katılımcı 5)

Katılımcı 1, verilerinin toplanmasını umursayanlar ve umursamayanların farklı toplumsal gruplar olduğunu belirtmektedir:

“Çoğunlukla böyle söyleyen insanlar, oldukça ayrıcalıklı insanlar. Türk toplumunda hetero bir erkeksen senin o toplumdaki yerin ayrıcalıklıdır. Her şey senin için işler. Eşcinsel bir kadınsan toplumda çok farklı bir yerin var. Yolda yürürken sorun yaşayabilirsin. Bunu söyleyen insanlar ayrıcalıklı insanlar. Çünkü sistemin etkisini şu anda hisseden insanlar olsalardı; örneğin Amerika’daki siyahiler çoğunlukla böyle demiyorlar. Çünkü yanlış bir veri yüzünden vurulabilirler. Veya zengin olan insanlar böyle demiyorlar, çünkü etkilenmiyorlar bu sistem hakkında, en azından şu anda belki. Onlar da etkilenecekler. Çünkü örneğin onların buzdolabı ne yediklerini biliyor, sigorta şirketine haber veriyor. Ondan sonra da onların primleri yükseliyor. O zaman fark edecekler. Ama bazı insanlar için de bu yaşam ve ölüm konusu. Facebook mesela senin transseksüel olduğunu biliyor ve sen kimseye söylemedin. Ve bunu bir şekilde yanlışlıkla açıklıyor. Diyelim ki verdiği seçeneklerle vs. O insanlar bunu bir problem olduğunda fark ediyorlar. Ayrıcalıklı insanlar ise fark etmiyor. Ama henüz fark etmiyor. Bunun anlamı ben daha bir şey hissetmedim. Ben daha bunun kötü bir yanını hissetmedim. Bu dar bir görüş.” (Katılımcı 1)

Katılımcı 1’e göre avantajlı toplumsal gruplar, azınlık gruplarla karşılaştırıldıklarında daha avantajlı ve ayrıcalıklı bir konumda yer almaktadırlar. Sahip olunan bu ayrıcalık, verilerinin toplanmasına ilişkin endişe duymamalarına yardımcı olmaktadır. Verilerinin toplanması konusunda endişe duyanlar ise bir nevi

altkültüre ait, mevcut inanışları, düşünce biçimleri veya yaşam tarzları ile azınlık olarak konumlanan gruplardır.

Katılımcı 1, verilerin toplanmasıyla ilgili herkesin bir gün ufak ya da büyük bir tecrübe yaşayacağını söylemektedir. Bugün bir tecrübe yaşamamış olanlar verisinin toplanmasını umursamıyorken, yarın karşlarına çıkacak bir durum ile bunun farkına varabileceklerine dikkat çekiyor. Bir kişinin akıllı saati ondan habersiz nabız verisini toplayarak kişi hakkında bir çıkarımda bulunulmasına yardımcı olabilir. Örneğin, kişide kalp ritim bozukluğu varsa bu veri üçüncü taraflarla paylaşıldığında veya satıldığında kişinin banka kredi puanı düşebilir veya sağlık sigortası primi artabilir. Kişi bu gerçeğe yüzleştğinde sorunu akıllı saatinin topladığı veride bulmak aklına bile gelmeyebilir. Ya da farkına varırsa, umrunda olmadığı verilerin neden olduğu bir deneyim kazanmış olur.

Katılımcı 5, toplanan verilerin gelecekteki etkisini ve yaşanan deneyimi 2016 ABD seçimleri üzerinden örneklendirir:

“Veriler bugün bizim bugünümüzle ilgili değil yarınımızla ilgili. Yani bir sonraki adımımızı tahmin etmek ve onu tahmin ederek orada ne yapmak gerektiğini fark etmek.” (Katılımcı 5)

“Bir gün hiç farkına varmayacağınız bir şey olur ve verilerinizin kıymetini anlarsınız. Bir kısım Amerikalı bunu Donald Trump başkan olduğunda anladı.” (Katılımcı 5)

Katılımcı 5, sınıf bilinci kazanma aşamasında yaşanabilecek durumları örneklendirerek birgün herkesin bir bedel ödeyerek verilerinin toplanmasını umursayacağını öngörmektedir:

“Umurunda olmayan insanlar aslında tamamen sınıf bilinci olmayan işçiler gibidir. Her emekçi de bir gün sınıf bilincinin ne kadar önemli olduğunu öğrenir. Bir gün işten atılır, öğrenir; maaşı çok düşük kalır, öğrenir; örgütlenmediği için arkadaşları işten çıkarılır, öğrenir. Aynı şekilde verilerin umursanmamasının da bir bedeli olduğunu herkes öğrenecek.” (Katılımcı 5)

Verileriyle ilgili herhangi bir tasarrufta bulunmayan insanlar için Katılımcı 1 nüktedan bir biçimde şöyle bir örnek vermektedir:

“Onlara da şu denilebilir, he öyle mi saklayacak bir şeyin yok mu şu telefonunu aç bir bana ver 5 dakika bir bakacağım. Bakalım kaç tanesi veriyor. Çünkü onlar da biliyorlar.” (Katılımcı 1)

Burada dikkat edilmesi gereken nokta aslında özel hayatın işin içine girerek bir ironiyi barındırmasıdır. Cep telefonu, içinde her türlü görsel ve iletişimsel faaliyetin yapılabildiği cihazlardır. McLuhan’ın bakış açısıyla insanın bir uzantısıdır. Sorun tam da burada ortaya çıkmaktadır. Kimse mesajlaşmalarının okunmasını, tarayıcı geçmişinin kurgulanmasını ya da arama geçmişinin başkaları tarafından görüntülenmesini istemez. Başkası rahat erişemesin diye telefon tuş kilidi her zaman aktif haldedir. Tüm bunlar için endişe duyan ve güvenlik tedbiri alan insanlar, zararı olmayacağını düşünerek haklarında hiçbir şey bilmediği şirketlerin onlar hakkında veri toplaması konusunda oldukça esnek davranmaktadır. İroni tam da burada ortaya çıkmaktadır.

Gerek fiziksel gerek dijital alanda toplanan ve işlenen tüm veriler insanların bazen tasavvur bile edemeyecekleri sorunlarla karşılaşmasına neden olabilmektedir. Buradaki sorun, Katılımcı 1’in ve Katılımcı 5’in dediği gibi umursamayanların henüz bir problemle karşılaşmaması ve/veya hak ihalleri üzerine yetersiz bilgi sahibi olmasıdır. Üstelik bu durum yalnızca reklamlarla ilişkili de değildir. Örneğin, kürtajın yasak olduğu Polonya’da hükümet gerek kendi araçları gerekse işbirliği yaptığı veri şirketleri aracılığıyla kadınların potansiyel hamilelik belirtilerini Twitter hesabından, kredi kartı harcama özetinden, özel mesajlaşmalarından veya hareket izleme kayıtlarından tarama yaparak elde edebilir (Ceglowski, 2016). Böylesi bir olayın gerçekleşmesi ihtimaline karşı kim verilerinin toplanmasına karşı umursamazlık içinde olabilir? Katılımcı 1, geçmişten ve bugünden birer örnek vererek kişinin bugün veriye dayalı bir mağduriyete uğramamasının yarın uğramayacağı anlamına gelmediğine vurgu yapmaktadır:

“İkinci Dünya Savaşında Hollanda’da nüfus sayımı yapıldı. Ondan sonra naziler geldi, o nüfus sayımı ile Yahudileri buldular. Bunlar bilgisayarda yapılan nüfus sayımı değildi, veriler yoktu. Sadece Yahudi mi değil mi, nerede yaşıyor. Ve kaç kişi katledildi. Ve şu anki verileri düşün. Google olsun, Facebook olsun, Uber olsun mesela hangi politikacının kiminle yattığını kalktığını biliyor. Bu demokrasiye nasıl bir etki edecek? Uber’deki birinin mesela bundan sonraki başkan olacak kişiye “şuradaki kadınla ilişkini

biliyoruz şu saatte gidip şu saatte dönüyorsun” bir konuşalım bizim çıkarlarımız için diyebilir. Bunlar küçük küçük şeyler. Yani sana ait verilerin başkalarının elinde olması hükümet olsun, şirket olsun demokrasiye zararlı, insan haklarına zararlı.” (Katılımcı 1)

Yukarıda verilen örnekler ve Katılımcı 1’in ve Katılımcı 5’in aydınlatıcı yorumları, insanların kendilerinden habersiz verilerinin toplanması, saklanması, birleştirilmesi, paylaşılması ve satılmasından neden endişe duymaları gerektiğini açıklamaktadır. Yine Katılımcı 1’in belirttiği gibi, insanlar farkında olmasa bile tüm bu süreçler demokrasiyi ve insan haklarını sekteye uğratmaktadır.

4.3.2.4.4. Veri Farkındalığı / Bilinci

Bireyler her gün onlarca mobil uygulamaya giriyor, web sitesi ziyaret ediyor; mesajlaşıyor, paylaşıyor, oynuyor; kısacası ağa bağlı bir cihazla faaliyette bulunuyor. Peki, insanların verilerinin toplandığına ilişkin ne derece bir farkındalığa sahip? Ya da veriler üzerine farkındalık/şeffaflık talepleri görülebiliyor mu? Bazı katılımcılar bu konu hakkında çeşitli önerilerde bulundu.

Katılımcı 4, veri farkındalığının oluşmasında kullanıcılara karşı şeffaf olma ve net bir bilgilendirmenin olumlu etkisinin olacağını belirtmektedir:

“Kullanıcılara, bak ben senin bu verini topluyorum. Bunu da sana daha doğru içerik, daha doğru reklam göstermek için kullanacağım. Sen de bunun farkına var, burada buna göre hareket et demenin yapılabilecek tek çıkış noktası olduğunu düşünüyorum. (...) Net bilgilendirme, şeffaf olma ve sonrasında ona göre hareket etme.” (Katılımcı 4)

Bu farkındalığın oluşmasının gerekliliğini gündelik yaşamdan bir örnekle açıklıyor:

“Ekmek alacağımız fırının temiz olup olmadığını denetlemek ne kadar normal bir şeyse kullandığımız web sitesi veya sosyal medya platformunun da etik davranıp davranmadığını, bizim verimizi ne yapıp yapmadığını bilmemiz gerekiyor. Bunun farkında olmamız gerekiyor. Eğer başka denetleyen yoksa bizi bizden başka kim nasıl koruyacak?” (Katılımcı 4)

Katılımcı 3, konuyu hukukî çerçevede ele alarak toplumun kendi verileri üzerinde ne kadar farkındalığı olduğunu sorgulamaktadır:

“Buradan Türkiye Cumhuriyeti vatandaşlarına seslensek ve bana kimlik fotokopisini getirene 20 TL para vereceğim desek kaç kişi kaç tane kimlik fotokopisi getirir düşünebiliyor musunuz? Açık rızasını da alıyorum, form da imzalattıyorum. Bu ne demek oluyor? Kişiler böyle bir farkındalığa sahip değil ve iradeleri yanıltılabilir. Bu nedenle kişisel verilerin korunmasını sadece kişilere bırakmak çok doğru değil benim kanaatimce. “ (Katılımcı 3)

Buna göre toplumda zayıf olan yalnızca çevrim içi üretilen ve başkaları tarafından toplanan veriler hakkındaki bilgi değil. En temel kişisel veriler bilinçli olunmadığında manipüle edilerek toplanabilir. Katılımcı 3, kişisel veri bilincinin yanında kanunların da verileri koruması gerektiği kanaatini paylaşmaktadır. Fakat Katılımcı 4’ün *“eğer başka denetleyen yoksa bizi bizden başka kim nasıl koruyacak”* ifadesi de önemlidir. Çünkü Katılımcı 3’ün daha önce sözünü ettiği *“karar alıcılar ve karar vericilerin cehaleti”*, denetimin ve yasaların uygulanmasının önünü tıkadığı gözlemlenmektedir.

Yine hukuk çerçevesinde değerlendirildiğinde, web sitelerinin çerez politikaları ve gizlilik sözleşmelerinin çeşitli araştırmalarda genellikle okunmadığı tespit edilmiştir (Milne & Culnan, 2004). Buna bağlı olarak Katılımcı 4 de, hazırlanan sözleşmelerin hem dijital okuryazarlık hem de veri farkındalığına hizmet ettiğini ama genellikle okunmadığını dile getirmektedir:

“Türkiye’de kaç kişi çerezin ne demek olduğunu, bunla nasıl veri işlendiğini, Facebook’ta yaptığı hareketler neticesinde nasıl bir sonuçların ortaya çıktığını konusunda ne kadar bir bilgiye sahip. Bilgi sahibi olmaları için biz gizlilik politikaları yapıyoruz, açıklamalar ve aydınlatmalar yapıyoruz. Bunları kaç kişi okuyor.” (Katılımcı 3)

Katılımcı 5, 2016 ABD başkanlık seçimleri sonrasında ortaya çıkan olayların toplumda veri bilinci oluşturduğunu ve farkındalığın daha öncesine kıyasla arttırdığını dile getirmektedir:

“Dünyada 2016 ile 2020 arasındaki süreçte veri farkındalığında büyük bir gelişme oldu. Bu, özellikle 2016’da Cambridge Analytica skandalının seçimden sonraki süreçte ortaya çıkmasıyla arttı.” (Katılımcı 5)

Söz konusu dönemde yaşanan skandallar sonrası Facebook şeffaflaşmaya yönelik birçok adım atsa da çoğu genç kullanıcıyı platformda tutamamıştır. Fakat burada ironik olan ise genç kitlenin yine bir Facebook ürünü olan Instagram’ı sık

kullanmalarındır. Yine buna bir örnek olarak 2021 yılında Türkiye’de tartışmaya açılan WhatsApp gizlilik sözleşmesi düzenlemesi verilebilir. Medyada bir anda yer bulan, kullanıcıların tepki gösterdikleri bu sözleşme güncellemesi veri farkındalığının oturmasına ilişkin bir işaret olsa da yalnızca popülizmden ibaretti. Katılımcı 5, WhatsApp gizlilik sözleşmesi ve toplumun tepkisi üzerine şunları söylemektedir:

“Whatsapp verilerimizin Facebook ile paylaşılmasıyla ilgili asıl büyük değişikliği 2016’da yapmıştı. O tarihte anahtarı verdik, hiçbirimiz farkında olmadan. 2016’da verdiğimiz izne göre 2021’deki değişiklik daha basit bir değişiklikti. Basit değişiklik WhatsApp Business ürünündeydi. (...) Küçük bir parçaydı, büyüğünü daha önce verdik. O ara ya çıktı önümüze ve kabul et dedik, ya da başka bir şey oldu. “ (Katılımcı 5)

“Amerika’da çıkan tartışmalar zamanla bizim gibi ülkelere de gelmeye başladı. Ama yalan yanlış geldi. WhatsApp benim arkadaşımın yaptığı konuşmanın peşinde değil ki. Herkes öyle yorumladı. WhatsApp bizim meta verimizin peşinde. Kullandığımız cihazın markası bile olabilir. Şarj durumu olabilir.” (Katılımcı 5)

WhatsApp üzerine tartışmaların Türkiye’deki insanların veri farkındalığını sağlamak bakımından önemli bir yeri olduysa da sonuçta insanlar bunu WhatsApp gruplarında; Facebook, Twitter vb. platformlar üzerinden tartışmıştı. Sorun, anlık bir kıvılcımla her yerde konuşulmuşken sonrasında ise bir anda ortadan kaybolmuştur.

Katılımcı 5, teknoloji hızla ilerlerken bedellerin ödendiğini ama hem yasal düzenlemelerin hem de toplumdaki veri bilincinin artmasının sorunların çözümüne katkı sağlayacağını düşünmektedir:

“Bence veri farkındalığı yavaş yavaş oluşuyor. Teknolojiler böyledir, önce gelirler sonra arkasında yasal düzenlemeleri gelir. Otomobilin icadıyla emniyet kemerinin yasal olarak zorunlu hâle gelmesi arasında yüz yıllık bir süre var. Yani insanlar yüzyılda ‘şu emniyet kemerini takayım da kazalarda korunayım’ durumunu zorunlu hâle getirmiş. Şu anda tabi çok daha hızlı ilerliyor. Ama bu hızlı ilerlerken de bedeller ödeniyor. Demokrasilerden, hukuktan, ifade özgürlüğünün kötü kullanılmasından gibi birçok yere kadar bedeller ödeniyor. Bu bedeller ödendikçe ve farkındalık arttıkça çözülecektir. Facebook 2004 yılında kuruldu, en eski sosyal medya diye kabul etsek 17 yıl var arada. İnsanlık tarihi için çok kısa bir süre bu.” (Katılımcı 5)

WhatsApp tartışmalarındaki gibi yüzeysel değil de oturmuş, sindirilmiş bir veri bilincine ve veriye bakış açısına sahip olmanın en temel yollarından birisi tabii ki eğitimidir. Katılımcı 5, eğitiminin olmazsa olmaz olduğunu dile getiriyor:

“İnsan hakları eğitimi nasıl veriliyorsa, bu eğitimi eğitim sistemi içerisinde vermeniz gerekiyor. Veri hakları, veri bilinci, veri bilinci kazanmanın önemi, verileri korumanın önemi. Bunlar artık hep eğitim sisteminin vazgeçilmez bir parçası olması lazım.” (Katılımcı 5)

Türkiye’deki eğitim müfredatında yer alan medya okuryazarlığı ise veri farkındalığından ziyade daha genel çerçevede geleneksel medyayı kapsamaktadır:

“Medya okuryazarlığı eğitimi içerisinde veri okuryazarlığı, veri bilinci kazanma var mı? Hayır. Türkiye’de hâlâ altıncı sınıftan sonra seçmeli ders bu. Onun da büyük kısmı eski medyayı okutmak üzerine. Ama Finlandiya’da bu iş okul öncesinden başlıyor. Ancak buradan başlatabilirsen verilerinin ne kadar kıymetli olduğu bilincini oturtabilirsin.” (Katılımcı 5)

Katılımcı 5, küçük yaşta bu bilinci kazandırmayla ilgili Umberto Eco’nun yazılarına atıfta bulunmaktadır:

“Umberto Eco son yazılarında okulların tek derdinin internet ve onunla ilişki olmalı diyordu. Okulların bundan başka bir derdi olmaması gerektiğini söylüyordu. İnsanlara zaten artık internette bulabileceği bilgiyi ezbere ezbere öğretmenin bir mantığı yok. Ama bu internetle nasıl bir ilişkiye gireceğim ben.” (Katılımcı 5)

Eco’ya referans verilerek yapılan bu yorum, insan hayatında kritik bir yer edinen internetin insanlar tarafından nasıl kullanılması gerektiğinin önemine vurgu yapılmaktadır. İnternetle girilen ilişkide bilinç düzeyi arttıkça, veri farkındalığı da aynı düzeyde gelişmeye devam edecektir.

4.3.2.5. Etik Bir Web’in İnşası

World Wide Web Konsorsiyumu (W3C), web’in şeffaf, insanlara yardımcı olan, onlara pozitif bir sosyal fayda sağlayan, iletişim ve bilgi paylaşımını kolaylaştıran, güvenlik ile mahremiyetin zorunlu olduğu ve çoklu sistemleri teşvik

eden bir platform olması gerektiğini belirtmektedir ²². Bugün gelinen noktada web; çoklu, evrensel, ortak ve açık bir sistem olmaktan öte teknoloji şirketlerinin liderliğinde gözetlemeye dayalı iş modellerinin kâr sağladığı bir alan hâlini almıştır. Bu tema altında web'i bugünün şartları altında ve yeni bir anlayışla nasıl daha etik ve adil bir hâle getirebiliriz konusu tartışılmıştır.

4.3.2.5.1. Mevcut Sistemdeki Problem

Tim Berners-Lee'nin web'i icadıyla bugünün web'i arasında otuz yıl civarı kısa bir süre olmasına rağmen, O'Reilly'nin web 2.0 tanımlamasından bugüne web hızlı bir değişim yaşamıştır. Bu değişim beraberinde çalışmada daha önce tartışılan ve tartışılmaya da devam edilen problemleri beraberinde getirmiştir. Katılımcılar hem web hem de teknoloji bağlamında sistemde tespit ettikleri problemleri farklı bakış açıları doğrultusunda değerlendirmektedir.

Katılımcı 1, bugünkü teknolojiyi “sömürgeci” olarak nitelendirmektedir.

“Ben bu yüzden bu tür teknolojiye kolonyal diyorum. Bir grup tarafından yapılıyor, başka bir grup tarafından kullanılıyor. Bunlara da kullanıcı diyoruz. Yaratanlar bu teknolojiye sahip. Kullananlar değil. Bu bir tasarım problemi. Ama değiştirmemiz gereken şey bu.”(Katılımcı 1)

Katılımcı 1'e göre bugünün teknoloji tasarımı tamamen bir grubun çıkarına çalışma üzerine inşa edilmiştir. Daha önce de belirtildiği gibi bu sistemde kullanıcı tarafından üretilen her şeyin sahibi kullanıcı değil, şirketlerdir.

Katılımcı 1'in sisteme yönelik kaygılarından birisinin “kontrol” oluşturmaktadır. Bu kadar çok veri toplanması insanları etkileme ve kontrol açısından da sorun teşkil etmektedir:

“(…) Ondan öte kontrol. Yani mesela Google'da Eric Schmidt vardı. Neden Jared Cohen ile yazdı kitabını²³. Cohen, Condoleezza Rice'in asistanıydı. Schmidt mesela şu anda Amerikan askeriyesine danışman olarak

²² W3C TAG Ethical Web Principles. <https://www.w3.org/2001/tag/doc/ethical-web-principles/>

²³ Sözü edilen kitap: Yeni Dijital Çağ. İnsanların, Ulusların ve İş Dünyasının Geleceğini Yeni Baştan Şekillendirmek

atandı. Bu kadar veriyi eline aldığı zaman yalnızca reklamcılıktan çok daha öteye gidiyor. İnsanları kontrol aşamasına geliyor. Hükümetler ilgilenmeye başlıyor, askeriye ilgilenmeye başlıyor. “ (Katılımcı 1)

En başta bu kadar çok veri toplamak bir problemken bu verilerin başka kurumlar tarafından talebi ve el değişimi de başka bir problem olarak karşımıza çıkıyor. Katılımcı 1, kontrol tehlikesini ayrıca Metaverse örneği üzerinden de açıklıyor:

“2 yıl önce Facebook 70 kişi çalışıyor düşüncelerinizi okumak için dedi. Mesela Metaverse. Neden bir sanal gerçeklik sistemi üzerinde çalışıyor. Sanal gerçeklik sisteminde çünkü bütün dünyayı yaratabiliyor. Her şeyi kontrol edebiliyor. Ve senin ona vereceğin karşıt yanıtları kontrol edebiliyor. Şu anda dünyadan örnekleme alması lazım. (...) ama şu anda tam her şeyi alamıyor. Yani ona verdiği verileri alabiliyor, onu kullandığın zaman öğrendiklerini öğrenebiliyor. Ama seni sanal bir dünyanın içerisine koyduğunda her şeyi kontrol edebiliyor. Mesela şu ışığı biraz değiştirdiğimde ne biçim bir etkisi olacak. Artık gerçek dünyayı algılamak zorunda değil kendisi yaratıyor. Yani anlıyoruz ne kadar başarılı olur olmaz o başka konu. Ama çabaladığı şey bu. Bir laboratuvar yaratıp, ki zaten bir laboratuvar olarak görülüyor ama her açısından kontrolünün olduğu bir laboratuvarda senin daha iyi etkileyebilecek, tanyabilecek. Ama bu sistem başarılı olursa eninde sonunda bir otokrasiden bahsediyoruz. İnsan bir birey olmaktan çıkıyor böyle bir sistemde. “ (Katılımcı 1)

Katılımcı 1'e göre kurgusal bir evren olan Metaverse, bir laboratuvar gibi her şeyin kontrol edilebildiği bir sistem yaratacaktır. Bugün bizi bir AVM'deki gözetleme kameralarının gözetlemesiyle bir sosyal medya platformunun gözetlemesi arasındaki en önemli fark birinin fiziksel gerçekliğimizi birinin diğerininse yaşantı, duygu evrenimize dair en detay bilgileri görebilmesidir. Metaverse evreni bu bilmeyi daha öteye taşıma potansiyeline ve amacına sahip gibi görülmektedir.

Katılımcı 1, şu anda tüm dünyada gözetim kapitalizmi ve onun tüm teknolojik unsurlarının politikacılar, teknolojistler veya kanaat önderleri tarafından nasıl ele alındığını örnekler vererek açıklamaktadır:

“O politikacıların şovuydu (2018'de ABD Kongresine Zuckerberg'in verdiği ifadeler). Orada gördüğün gibi hiç bu konudan anlamayan insanlar saçma sapan sorular sordular. Birkaç kişi düzgün soru sordu. Hepsi 'vaov Zuckerberg'le beraberiz' dediler.” (Katılımcı 1)

Buna göre Mark Zuckerberg'in ABD kongresine ifade vermesi bir şeyleri iyileştirmek bir yana, politikacıların siyasi bir şovuna dönüşmüş ve hepsi Zuckerberg gibi bir profile soru sormanın keyfini tatmıştır. Katılımcı 1, bunun Avrupa'da da pek farklı olmadığını söylemektedir:

“Avrupa'ya davet ettiler Mark Zuckerberg'i işte AB parlamentosuna hesap vermesi için. Ondan sonra İsveç Parlemlenterisi Zuckerberg ile selfie çekindi.” (Katılımcı 1)

Bu platformlara yönelik tutum görünürde her ne olursa olsun bir araya gelindiğinde bir şekilde davranışlar farklılaşmaya başlıyor:

“Problem bu, ben bunu kendi gözümle gördüm. Burada İnternet Güvenliği Günü diye bir etkinlik vardı; çocuk güvenliğiyle ilgili. Oraya davet ettiler beni konuşma yapmam için. Facebook'un İngiltere temsilcisi de oradaydı. O da bir konuşma yapacaktı. Ben konuşmamı yaptım orada, ondan sonra etkinlik yöneticileri neden Facebook hakkında böyle konuşuyorsun dediler. Ondan sonra kendi videolarını gösterdiler, onların başındaki kadın Facebook'ta gezdiriliyordu. Ve sanki Disneyland'de gibi. Bunlar çocuk güvenliği ile ilgili bir şey yapacaklar... Daha sonra okullarımıza Facebook koymalısınız dediler.” (Katılımcı 1)

Katılımcı 1, çocukların güvenli internete erişimiyle ilgili konuşma yapmak için davet edildiği etkinlikte Facebook hakkındaki yaklaşımı üzerine etkinlik yöneticileri tarafından eleştirildiğini dile getirmektedir. Ve aslında görülen, etkinlikte Facebook'un çalışma ortamı ve işleyişi övülmüş olacak ki okullardaki bilgisayarlara Facebook eklenmiştir. Katılımcı 1, orta ve üst yönetici gruplarının, akademisyenlerin, politikacıların veya yasal karar alıcıların veya vericilerin bu tür sistemlere hayranlıkla bakmalarının nedenini kişisel/kurumsal çıkar ile ilişkilendirmektedir:

“Çoğunun da finansal olarak çıkarları var. Ya belki birkaç sene sonra Google'da Facebook'ta çalışmak istiyor kendisi, ya da oradan para alıyor. Problemler var.” (Katılımcı 1)

Katılımcı 5, temel sorunu internetin merkezîleşmesiyle açıklıyor:

“Bence gözetleme kapitalizmindeki temel sorun internetin merkezîleşmesi ve milyarlarca insanın verisinin tek bir noktada birikiyor olması.” (Katılımcı 5)

“Gözetleme kapitalizmi insanların verilerini merkezî bir platformda toplayarak, topladıkları o veriler üzerinden artı değer üreterek; insanların verilerini hammadde olarak kullanarak yeni bir varlık ortaya çıkartıyor.” (Katılımcı 5)

Katılımcı 5, gözetlemeye dayalı ekonomik model ve onun mihenk taşı olan veri birikiminin oluşturduğu yeni duruma atıfta bulunurken aynı zamanda insanları etkilemek amaçlı kullanımını da bir örnekle paylaşıyor:

“Amerika’daki seçmenin tercihlerinin Rusya merkezli bir operasyonla manipüle edildiği bir dünya. O da gözetleme kapitalizminde biriken veri sayesinde oluyor. Oradaki veriyi çekiyor, seçmenin kişiliğini anlıyor ve yorumluyor. Buradan bir iletişim kampanyası yürütüyor. Sadece kapital değil bu, insanın siyasi görüşünü şekillendirebilecek de bir veri bu. ” (Katılımcı 5)

Katılımcı 5, bugünkü merkezî internet platformlarının ne internetin ortaya çıkma amacını ne de Tim Berners-Lee’nin web’i icat ederkenki idealini yansıttığını belirtmektedir:

“WWW protokolünü icat etmiş biri Berners-Lee de ‘biz bunu hayal etmemiştik’ diyor. Biz insanların Facebook, Instagram, Twitter veya YouTube gibi birkaç platformda toplanıp bu şekilde sömürüldüğü bir internet hayal etmedik diyor. Bundan daha büyük bir açıklama olamaz. Berners Lee WWW Foundation’ı bu yüzden kurdu, interneti yeniden düzeltmek için kurdu.” (Katılımcı 5)

“İnternetin icat edilme nedeni, Arpanet’ten beri, nükleer saldırılara karşı bütün verileri tek bir yerde toplamayalım. Merkeziyeti daraltmamız lazım diye inşa edilmiş bir internet. Ama şu anda bunun tam tersinde. Merkezî noktalarla örülmüş durumda.” (Katılımcı 5)

Katılımcı 5’e göre tekelleşme ve merkezîleşme sorunu bugünkü web’in ve teknolojinin en temel problemleri arasında yer almaktadır.

“Ben Instagram’ı kapatıp Instagram muadili bir yere giderken oradaki verilerimi taşıyamıyorsa problem. Şu an WhatsApp’tan neden ayrılamıyoruz? Whatsapp’tan Signal’e, Whatsapp’tan Telegram’a, Whatsaptan Bip’e neden mesaj gönderemiyoruz? Çünkü bunlar merkezî platformlar. Eğer benim şöyle bir lüksüm olsaydı; WhatsApp’taki arkadaşlarımı Signal’e taşıyorum. Onlar WhatsApp’ta kalsalar bile ben Signal’deyken onların mesajlarını alabileceğim gibi lüksümüz olsaydı o zaman bağımsızlıktan söz edilebilirdi. Ama şu anda kendi içlerine sokuyorlar ve buradan çıkarsan bitersin diyorlar. Ne verimi taşıyabiliyorum, ne

arkadaşlarımı taşıyabiliyorum. Signal'e gidersem tek başıma oturacağım. Bu durum insanları korkutuyor ve bunu kullanıyorlar. " (Katılımcı 5)

İnsanlara ücretsiz hizmet sunup onları kendilerine bağımlı hâle getirerek tekelleşen platformların algoritmaları da tartışılmaya açılmakta ve sorunun bir parçası olarak görülmektedir. Bu sistemde algoritmalar merkezîleşmiş şirketlerin devamlılık sağlamasına yardımcı olurken kullanıcı ekseninde problemlere neden olabilmektedir.

"Bütün dünya yuvarlak değildir düzdür diyenleri bir araya toplayabilen bir algoritma insanlığa nasıl hizmet etsin ki? Dünyanın şeklini Galileo'dan beri biliyoruz. Ama birileri çıkıyor dünya düzdür diyor ve algoritma onları birbiriyle buluşturuyor. Büyümeye başlıyorlar. Onlar o hakikatten kopup dünyanın düz olduğunu kabul etmeye başlıyorlar." (Katılımcı 5)

"Tamamıyla herkes istediğini yazsın ama Jack sorumlu olmasın, Mark sorumlu olmasın. Ama bir yandan da Mark bunun üzerinden para kazansın. Benim öfkemin üzerinden para kazansın. Bu demokrasileri yok eder, hakikati yok eder." (Katılımcı 5)

Katılımcı 1, algoritmaların gerçeği filtreleme gücünü ve mevcut sistemi neden sömürgeciliğe benzettiğini şöyle vurgulamaktadır:

"Şu anda bu şirketlerin ellerindeki güç, gerçeği filtreleyebiliyorlar. Şu anda 'şunlar oluyor' diyorlar. Ama bu filtrelenmiş bir akış. Facebook algoritması 'şunu gör, şunu gör, şunu görme, şunu gör' diyor. Yani bundan daha başka ne olabilir ki. (...) 'Gerçeğin ne olduğunu belirlemek istiyoruz' diye Eric Schmidt demişti. Tamamen seni etkilemek için. O yüzden buna kolonyalizm diyorum. Ama hiçbir zamanda yaşanmamış bir kolonyalizm. Tamamen küresel bir şekilde. Küçük bir grubun herkesi tamamen kontrol edebilmesi." (Katılımcı 1)

Her iki katılımcı da kendi perspektiflerine göre teknolojinin ve web'in mevcut sorununu paylaşmışlardır. İnsan haklarına, deneyimine, demokrasiye ve insanın bizzat kendisine saygı duyan alternatif bir web inşasında neler olmaması gerektiğini anlamak için sorunları ele almak oldukça önemlidir.

4.3.2.5.2. Verilerin Kontrolünü Kullanıcılara Vermek

Mevcut sistemde insanlar kişisel verilerinin kontrolünü yalnızca kendilerine sunulan imkânlar doğrultusunda sağlayabiliyor. Örneğin, Facebook "Facebook

Bilgilerin” sekmesi altında kişi hakkında kendi oluşturduğu ve reklamverenlere hedefleme yapmaları için sunduğu kategorileri paylaşıyor. Google, “Reklam Tercihleri” bağlantısında kullanıcılara aynı olanağı tanıyor. Bunlar dışında, insanlar eğer kimlerin onlar hakkında bilgi sahibi olduğunu biliyorsa ki bunu bilmek mümkün değil, tek tek o şirketlerle iletişime geçerek sahip oldukları verileri sildirebilirler. Onun dışında “şu verimi sil, şu verimi kullanma, şu verim sende kalabilir” gibi bir seçenek yoktur.

Kişisel verilerin kontrolü tamamen kişiye ait olduğunda daha etik bir web’ten söz edebilir miyiz? Egemen ideoloji içinde yaşayan sıradan bir insan bu soruyu sorduğunda ardından ikinci bir soru hemen belirir: kendi verilerimi ben satabilir miyim? Veriyi istediğim kişi/grupla paylaşarak para kazanabilir miyim? Teoride herkesin isteyebileceği ve talebinde ısrarcı olabileceği bir durum yaratır, çünkü ucunda bir gelir kapısı var; pratikte ise gözetlemeyi ve kapitalizmi ortadan kaldırır mı?

Katılımcı 5, Web’in mucidi Tim Berners-Lee’nin Solid²⁴ projesini, Pods’u²⁵ ve kişisel verilerin sunucularda değil kişilerde tutulduğu bu sistemi anlatıyor:

“Tim Berners-Lee’nin merkezîyetsiz internet projesi Solid, hepimize birer pods almamızı söylüyor. Bu pods şöyle çalışıyor. Eğer ben Solid sistemi içinde bir uygulamaya girdiysem verilerimin hepsi uygulamanın bağlı olduğu sunucuya değil benim pods’uma düşüyor. Veri benim pods’umda birikiyor. Hiçbir uygulama veya platform hiçbir verinizi biriktiremiyor. Olabilecek bütün veriler sizin kendinize ait parasını ödediğiniz pods’unuzda yer alıyor.” (Katılımcı 5)

Solid projesinin temelinde yer alan ve güvenli birer kişisel web sunucusu olan Pods’lar, kişinin kendi verilerine sahip olmasını ve verilerine kimlerin erişip erişemeyeceğini kontrol etmesini sağlıyor.

“Yarın Facebook’tan çıkıyorum ve X platforma gidiyorum dediğiniz zaman verileriniz de o platformun içine aynen aktarılır. Sen sadece Facebook’a girerken o pod’u onlarla ortak kullanma hakkı tanıyorsun. Merkezîyeti önlemek için iyi bir fikir.” (Katılımcı 5)

²⁴ Solid hakkında detaylı bilgi için: <https://solidproject.org>

²⁵ İng: Personal Online Data Stores.

İnsanların kendi verisini sahip olması ve yönetmesi bakımından Solid projesinin bir umut vaddettiği söylenebilmektedir.

Bu veya benzeri bir sistemin varlığından söz edildiğinde akla “madem kişi kendi verisine sahip, neden kendisi satmasın?” gibi bir soru gelmektedir. Bu yalnızca veri değil, bir dijital emek de olabilir. Katılımcı 5, sosyal medya platformu olan Steemit üzerinden bir örnek paylaşmaktadır:

“Steemit diye bir platform var. Orada yaptıklarınız, paylaşımlarınız etkileşim aldığı anda, Steemit’in kendi kripto parası var, bu parayla size ödeme yapmaya başlıyor. Bir anda varlığınız dijital emeğiniz bir karşılık bulmaya başlıyor. Aynı zamanda bu iş blokzincir teknolojisi üzerine kurulu olduğu için veriler tek merkezde birikmiyor. Dağıtılarak dünyadaki tüm bilgisayarlarda biriktiği için merkezî bir veri biriktirme noktası da yok.” (Katılımcı 5)

Steemit platformunda yaratıcı içeriğin, etkileşimlerin paraya dönüşmesi ve platformun blokzincir tabanlı olması şu ana kadar karşılaşılan sosyal medya platformlarının yerleşik algısını kırmaktadır. Fakat yaş, cinsiyet veya davranış verisinden ziyade platform içindeki yaratıcı emeğin bir maddi değeri vardır. Bu yaş, cinsiyet veya gelecek davranış verilerinin bizzat kullanıcının kendisi tarafından satılması durumunda ne olur?

Katılımcı 1, verinin kontrolünü kullanıcıya vererek kişinin bunu satması mantığı üzerine inşa edilebilecek bir sistemin, çemberin içindeki başka bir sistem olduğunu düşünüyor:

“Veriyi istediğim kişiyle paylaşayım modeli milyarderlerin yeni piyasaya sunduğu bir şey. Diyorlar ki şu anda bu Google’lar, Facebook’lar sizin verinize sahip. Şimdi ben yeni bir sistem oluşturun. Kendi verinizi kendiniz satacaksınız diyorlar. Bu şu gibi, kölelik iyi bir şey değil. Başkası sana sahip olmasın, sen kendine sahip ol ki sen de kendini satabil. Ben niye kendimi satmak isteyeceğim? Bu insanlar neden böyle diyorlar? Sen kendini satarken ben de içinden kendi payımı alacağım. Çünkü yaptıkları iş bu.” (Katılımcı 1)

Katılımcı 5, söz konusu kişisel veriyi kişinin kendisinin satmasının yalnızca veri farkındalığına katkı sağlayabileceğini; hatta başka problemlere yol açabileceğini söylemektedir:

“Eğer verimin kıymetini kabul ediyorsam ve bunun paraya çevrileceğini düşündüğüm bir emtia olduğunu düşünüyorsam daha bilinçli hareket etmeye başlarım. Satsam da satmasam da. Veri farkındalığına hizmet eder. Bu da bir düzelmeye yol açar. Ama manipülasyonları arttırır. İnsanlar daha fazla para kazandıracağını düşündüğü yalanları söylemeye ve paylaşmaya başlayabilir. İnsan kendi verisini satarsa bu riskler var. Şimdiki sistemden daha kötü olmaz ama sadece veri farkındalığını sağlayacağı için.” (Katılımcı 5)

Katılımcı 5’e göre, kişi eğer verisinin satılabilir bir şey olduğunu bilseydi muhtemelen buna sahip çıkmak için elinden geleni yapacak, sevdiği bir eşyasına verdiği özeni verecek ve koruyacaktır. Sonrasında ise içselleşmiş bir kapitalist mantıkla daha fazla para kazanmanın yollarını arayabileceğini ve bu nedenle hakikatin zedelenebileceğini dile getirmektedir. Diğer yandan Katılımcı 1, kapitalistlerin bu sistemi deyim yerindeyse “kabul edilebilir” ve “paylaşımçı” göstermek için bu yola gidebileceğinin ama çevrim içi kapitalist mantıktan hiçbir şeyin eksilmeyeceğinin altını çizmektedir.

Katılımcı 3, insanların kişisel verileri hakkında tek hak sahibi olmaması gerektiğini belirtmektedir. Fakat buradaki ikincil bir tarafın hak sahipliği bir şirket veya özel kuruluş değil; yasalar tarafından korunmasını içermektedir.

“Bireyler her zaman kişisel verileri üzerinde tek hak kişiler sahibi olmamalı. Bununla ilgili KVK Kurulunun iki tane kararı oldu bizde. Birincisi şu: bir spor salonuna avuç içi ile giriş yapılıyordu ve kişilere üye olurken zorunlu olan bir açık rıza metni imzalamaları isteniyordu. (...). Kurul buna istinaden dedi ki senin yaptığın şey hukuka aykırıdır. Zorla sözleşmenin ön şartı olarak sundun. Açık rızası hukuka aykırıdır. Avuç içi okuma sistemini kaldırı, sana ceza veriyorum dedi. Bundan birkaç ay sonra başka bir spor salonu şikâyet edildi. Spor salonu şunu iddia etti: evet sizin böyle bir kararınız var ama ben burada kişilerin özgür iradelerine bırakıyorum. İsteyene kart veriyorum isteyen açık rızasını veriyor ve avuç içiyle giriyor. Yani spor salonu benim modelimde kişi kendi verileri üzerinde tasarruf etme hakkına sahip diyor. Kurul buna da ceza verdi ve dedi ki; her ne kadar böyle bir şey koysan da bu bilgi o kadar önemli bir bilgidir ki kişiler her zaman bunun bilincinde olmayabilir, o sebeple spor salonuna giriş gibi basit bir işlem için avuç içi izini hiç almaman gerekir dedi ve ceza verdi.” (Katılımcı 3)

İnsanlar kişisel verilerini kontrol etse ve kendileri kabul ederek başkalarıyla paylaşırsa bile paylaşılan verinin önemiyetini bilemedikleri için gelecekte bir sorunla karşılaşabilirler. Diğer yandan veri paylaşımı bir manipülasyonun etkisi altında

gerçekleşebilir. Çünkü insan bazen kendi yaptığı tercihleri kendisi tercih ettiğini düşünerek yapsa da bir manipölasyon altında olabilir. Veya “ne olabilir ki?” diyerek gelecekteki yansımalarını öngöremeyebilir. Dolayısıyla Katılımcı 3, bu gibi durumların yaşanabilirliğinden ötürü veri bilinci olsa bile verinin korunması gerektiğini ifade etmektedir.

4.3.2.5.3. Hizmetlerin Ücretli Olması Neyi Değiştirir?

“İstemiyorsan kullanmamakta özgürsün” söylemi doğrudan bireyi hedef almakta ve onu suçlamaktadır. Fakat “kâr etmiyorsan veya zarar ediyorsan hizmeti sağlamamakta özgürsün” söylemi üzerinde bir fikir inşa edilip tartışılmamıştır. Hâlbuki ne Google ne Facebook ne de diğer teknoloji şirketleri aslında bu işi mecburiyet altında yapmamaktadırlar. Peki, bu şirketler madem ücretsiz ve tüm giderlerini kullanıcı verilerini toplayarak ve işleyerek elde ediyor, neden bu hizmetleri ücretli vermiyorlar? 2010 yılından önce bu sorunun cevabı genellikle insanların bedavaya alışmasıyla ilişkilendirilmiştir. Yani bedava bir hizmet için para alınmaya başlanırsa veya bir hizmet en başta ücretli olarak piyasaya çıkarsa başarılı olamayacağı düşünülmüştür. Aslında insanlar elektriğe, internet ve televizyon aboneliğine veya GSM operatörüne düzenli ödeme yaptıkları gibi bugün Spotify, Netflix vb. birçok dijital platforma da ödeme gerçekleştirme alışkanlığına sahiptir. Dolayısıyla on yıl önceki yaklaşımın büyük oranda kırıldığını söyleyebiliriz.

Gözetim kapitalizminin hâkim güçleri Google ve Facebook tüm ürünlerinin ücretli sürümlerini yapsa ve karşılığında kimsenin verisini toplamıyorum dese ne olur ve ne değişir? Daha etik bir web için bir çözüm sunar mı?

Katılımcı 1, bunun sistemsel bir problem olduğunu yineleyerek hizmetlerin ücretli olmasının gözetim kapitalizminden hiçbir şey azaltmayacağını düşünüyor:

“Facebook dese ki yarın WhatsApp için bana para ver, bunu kolaylıkla yapabilir. Çoğu bedava kullanabilir ama isterseniz bize para verin, o zaman gizli yapabiliriz. Ama bu hiçbir şeyi değiştirmez. Çünkü genel sistemleri değişmiyor. “ (Katılımcı 1)

Katılımcı 1, isteyen ücretli isteyen ücretsiz kullandığı bir hizmet olarak Youtube’u örnek gösteriyor:

“Bazıları yapmaya başladı, mesela Youtube. Youtube para ödeyebilirsin, o zaman reklam görmeyeceksin diyor. Bu sadece reklam değil ama kullanıcıyı izlemeye de devam ediyorlar. Bu sadece başka bir şekilde para kazanması onun. Sistemin geneli, iş modelinin geneli değişmiyor. Yanında bir ek olarak geliyor.” (Katılımcı 1)

Buna göre hizmetin ücretli olması sadece reklama maruz kalmama üzerine inşa edilmiştir. Benzer şekilde Netflix ve Spotify gibi platformlarda da süreç böyle işlemektedir. Yani, ücretli hizmetler “izlenmeme” üzerine bir tasarruf yapmamakta yalnızca reklam göstermeme vaadi sunmaktadır. Katılımcı 1, hizmet için ödenen ücretin yalnızca bir ek gelir olduğunu ve asıl iş modelinden vazgeçilmediğini belirtiyor. Diğer yandan şu konuyu da tartışmaya açıyor:

“(…) Neden ücretli yapmıyorlar anlamıyorum, bu akıllıca bir şey olur onlar için. O zaman insanlara işte bak para ver hiçbir şekilde seni izlemiyorum diyebilirler. Yapabilirler bunu yarı. Ama işlerinin temeli hiçbir zaman o olmayacak. Onu yapsalar bile bu sadece halkla ilişkiler olacak.” (Katılımcı 1)

Ücreti karşılığında mahremiyeti önceleyen, kullanıcıyı takip etmeyen veya belgelerini taramayan bir Google veya Facebook hizmeti almak diye bir durum söz konusu değildir. Katılımcı 1, bunun yapılsa bile bir halkla ilişkiler faaliyetinden ibaret olacağını belirtmektedir.

Katılımcı 5, şu anda ücretsiz olan hizmetlerin ücretli olmasının şirketlerin işlerine gelmeyeceğini ve rekabeti artıracaklarını vurgulamaktadır:

“Bunu yaparlarsa bu kadar çok insanı toplayamazlar. Bu kadar çok insanı toplayıp merkezileştiremedikleri için sistemde bunun üzerinden istedikleri geliri elde edemezler. Zararlı çıkarlar. Bu tarafı işlerine geliyor; Parasız yapmak ve veriyi toplayıp bunu kullanmak ve para kazanmak. Bu her zaman daha kazançlı bir yöntem. Öteki türlü farklı farklı sistemler çıkacak ve Facebook 25 dolar istediğinde başka bir yer çıkacak 10 dolar diyecek. Bir anda pasta bölünmeye başlayacak. Bunun yerine o merkezietiyi korumak, veriyi toplamak, satmak ve kullanmak; ama aynı zamanda da insanların işine gelen bir iş yapıyormuş gibi görünmeyi tercih ediyorlar.” (Katılımcı 5)

Katılımcı 5, WhatsApp’ın Facebook’a katılma süreci üzerinden hizmetin neden ücretsiz olduğunu şöyle açıklıyor:

“WhatsApp’ın eski sahibi Brian Acton’un Facebook’tan ayrılma gerekçelerinden birisi bu. Facebook, WhatsApp’ı satın aldığı zamanlarda Acton WhatsApp’ı düşük de olsa paralı hâle getirmek istiyordu. Acton, maliyetini çıkarmak için aylık 1 dolar da olsa paralı olması gerektiğini söylüyordu. Facebook satın aldıktan sonra WhatsApp’ın paralı olma süreci erteleniyor. Zuckerberg ve Facebook yönetimi ücretli yapmaya karşı çıkıyor ve yavaş yavaş Acton ile görüş ayrılıkları yaşanmaya başlıyor. (...) Satın almadan sonra kalması gereken süreyi doldurunca Facebook’tan ayrılıyor.” (Katılımcı 5)

“Platformlar herkes orada olduğu zaman anlamlı. Herkes orada olduğu zaman da inanılmaz bir veri birikimi var. Veri birikimi de insanlardan ücret almaktan daha mantıklı.” (Katılımcı 5)

Buna göre şirketler ücretsiz olarak sundukları hizmetlere olabildiğince insan toplayarak istediklerini elde ediyorlar. Ellerindeki hizmetler insanlara her alanda o kadar detaylı ürünler sunuyor ki o hizmetlerden ücret almak yerine kullanım verilerini toplamayı tercih ediyorlar. Ücretli olsa ve sadece buna dayalı bir gelir modeli oluşturulsa yalnızca bugün para kazanabilirlerken, veri birikimi ile yarınların kazancını da garanti altına alıyorlar.

Katılımcı 4, ücretli hizmet meselesinin en baştan sorunlu olduğunu ve böyle büyük gücün ne yaptığının bilinmesinin imkânsıza yakın olduğunu ifade ediyor:

“Google’ın ücretli olmasında şöyle bir yanılsama var. Verini toplamayacağım, bunun için bana para ver demek var. Ya da ücretsiz kullanıyorsun ben de senin verini topluyorum demek var. İstese paralı olduğu halde yine onu yapabilir, böyle bir güç de var ya. Bir yandan da bu bana pek gerçekçi gelmiyor. Verini zaten toplayabiliyorum ama para ver toplamayayım. Ama ‘ya yine topluyorsan’ sorusunun cevabı yok. Güvenmek dışında denetlemek gerekiyor.” (Katılımcı 4)

Tüm araçlarını ve hizmetlerini veri toplama üzerine inşa etmiş olan ve rol model alınan bu güçlerin “seni izlemiyorum” demesinin denetimini sağlayacak bir mekanizmanın varlığı farklı bir tartışmayı açmaktadır.

Mevcut durumda hizmetlerin ücretli olmasının vaadi kullanıcıya reklam göstermemek üzerinedir. Fakat hiçbir ücretli hizmet, reklamın yanında hizmet kullanım verilerinin toplanmasından vazgeçecek bir öneri geliştirmemiştir. Bu noktada ücretsiz olması nedeniyle kullanıcı verisinin toplanması, ücretli olsa bile hâlen

toplanmaya devam etmesine evrilmektedir. Bir diğer sorun ücretli olma gibi bir alternatiflerinin olmayışıdır; zira kullanıcı kaybederler ve istedikleri veri havuzundan mahrum olurlar. Diğer yandan, bu hizmetler veri toplamayacaklarını beyan ederek hizmeti ücretli sağlasa bile bunun denetimi neredeyse olanaksızdır. Etik web anlayışına giden yolda hizmetlerin ücretli alternatiflerinin olması veya tamamen ücretli olmasının yapacağı katkı soru işareti barındırmaktadır.

4.3.2.5.4. Etik Bir Web’i Nasıl Sağlarız?

Gözetlemeye ve bunun üzerinden sermaye birikimine dayalı bugünkü web daha adil ve etik olabilir mi? Yoksa mevcut sistemin yerine bambaşka bir sisteme mi ihtiyaç var? Mahremiyete ve açık rızaya önem veren, bireye saygı duyan, bireyin kendi çıkarına çalışan, ihtiyaçlarını karşılayan ve onu manipüle etmeyen, verilerin şirketlerde toplanmadığı, algoritmaların şeffaf olduğu ve yasal düzenlemelere riayet eden teknolojilerin gelişmesi etik web için bir çıkış yolu sunabilir mi? Bu alt temada sözü edilen konular etrafında web’in daha etik, adil ve insana saygı duyan bir sisteme dönüşmesinin nasıl olabileceği tartışılmıştır.

Etik bir web’in inşasında ilk olarak tasarım kavramı karşımıza çıkmaktadır. Zira karanlık desenlerin veya yönlendirici tasarımların insanları yanıltabildiği bir web’in etik olmaktan uzak olduğu söylenebilmektedir. Katılımcı 2, tasarımı ve kullanıcı deneyim tasarımcısını şöyle tanımlamaktadır:

“Tasarım bir çözüm vadediyor olmakla beraber bizim için tasarım kullanıcının ihtiyacıyla ürünü satan ya da hizmeti satan kişinin ihtiyaçlarının eşitlenmesidir. Bu ortaklık, bu eşitlik sağlandığı zaman tasarımın esas başarısı olur. (...) Tasarım olarak bizim işimiz her iki taraf için de dengeyi bulmak. Sadece kullanıcıya odaklanmak ya da sadece müşteriye odaklanmak yanlış olur, arada dengeyi yaratmak gerek. Bir arabulucu gibi görebilirsiniz deneyim tasarımcısını.” (Katılımcı 2)

Katılımcı 2, ürün/hizmetle kullanıcıyı buluşturan bir arabulucu olarak kendisini tanımlamakta ve tasarımın kullanıcıya bir çözüm vaadi sunmasının yanında her iki tarafın da ihtiyaçlarını karşılaması gereken bir olgu olduğunu söylemektedir. Katılımcı 2, etik tasarımı ve manipülasyonu ise şöyle açıklamaktadır:

“Etik tasarım, kullanıcıya hiçbir eylemini bilinçsiz yaptırmamadır bana göre. (...) Kullanıcıya bazı şeyleri zorlayarak ya da farkında olmadan bir şeyler yaptırmak kabul edilebilir bir şey değil. (...) Ben her zaman yapılan manipülasyonda kullanıcının finansal ya da manevi olarak zarara uğrayıp uğramadığını bakarım. Bir oyun içinde ya da bir chat kısmında oralarda biraz daha makul karşılayabilirim. Çok art niyetli olduğunu hissetmediğim sürece. Özellikle çevrim içi satış sitelerinde böyle şeylerin kesinlikle olmaması gerektiğini düşünüyorum.” (Katılımcı 2)

Katılımcı 2, etik tasarıma ve manipülasyona ilişkin yorumlarında yalnızca web siteleri veya uygulamaların değil devletlerin de bu yola başvurarak istediklerini elde ettiklerini söylemektedir:

“Benim eğitimlerde verdiğim bir örnek var; Avrupa’da 15 ülkenin online ehliyet başvurusu sırasında organ bağışıyla ilgili. 15 ülkenin 12’sinde %80 civarında bağış yapılırken, 3’ünde İngiltere, Almanya ve ismini hatırlamadığım bir ülkede daha %7 %8 civarında organ bağışı. Bunun tek bir sebebi var. Yüksek oranlı formlarda organ bağışlıyorum tiki seçili geliyor ve kullanıcılar bunu fark etmeden geçiyorlar. (...) Ama eğer organ bağışlamayı kabul ediyorum varsayılan olarak seçili değilse o zaman insanlar seçme gibi bir eyleme düşmüyor. Burada ne taraftan baksanız; bir taraftan hayat kurtarıırken, diğer taraftan insanların bilinçli olarak bu bağışı yapıp yapmadıkları bir soru işareti. Hükümetler bile bunu kullanabiliyorlar.” (Katılımcı 2)

Seçeneklerin seçili hâle gelmesinin daha önce KVK korunması üzerine paylaşılan bulgularda yer verildiği gibi “gerçek bir açık rıza” olmadığı vurgulanmıştır. Katılımcı 2’nin paylaştığı örnek, web sitelerinde varsayılan olarak seçili hâlde gelen çerez kullanım seçeneklerine benzemektedir. Deneyim tasarımının etik olması kişinin kendi seçimlerini ve kendi geleceğini tayin etme hakkına sahip olmasıyla doğru orantılıdır.

Katılımcı 3, hukukun gerçekten uygulanması ile web’in daha etik hâle geleceğini ifade ediyor:

“Bizim kurallarla ilgili bir problemimiz yok, bizim kuralların uygulanmasıyla ilgili bir problemimiz var. Örneğin KVKK’da çerezler içinde açıkça yer almasa bile çerezleri kapsıyor. Bütün manipülatif içeriklerin ortadan kaldırılması için her şeyi ortaya koyuyor. (...) Tek sorun uygulama. Benim kanaatimce şu an herkes kanunlara kurallara uygun davranırsa bütün web etik olur ve tüm toplumsal hayat etik olur. ” (Katılımcı 3)

Katılımcı 5, etik bir web'in oluşması için ilk olarak yasal düzenlemelerin ulus üstü bir anlayışla yapılması gerektiğini belirtmektedir:

“Önce yasal düzenleme. Uluslararası hukuk ile çözmemiz lazım. Bu hukuku her ülkenin kendi hukuku içerisinde kalacak ve dağınık olarak değil de uluslararası bir merci olmalı. Yani Birleşmiş Milletler nasıl varsa, Avrupa İnsan Hakları Mahkemesi gibi kuruluşlar nasıl varsa. Ve bu organizasyonun içinde tüm dünyadan temsilciler yer almalı. Benim ülkemde çözemediğim bir problemi orada çözmem gerekiyor. Hukuk olmazsa hiçbir şey olmaz.” (Katılımcı 5)

Birleşmiş Milletlere göre bugün 194 ülkeden 128'inde kişisel veriler ve mahremiyetin korunmasına yönelik yasal düzenleme yer almaktadır. Katılımcı 5, her ülkenin farklı yasalar ve maddeler yayımlaması yerine Avrupa İnsan Hakları Sözleşmesi gibi bir ulus üstü düzenlemeye ihtiyaç olduğunu belirtmektedir.

Katılımcı 1, insan haklarının çevrim içi ortamda olmayışını şöyle dile getirmektedir:

“Fiziksel dünyada senin bazı hakların var, (...) ama sanal dünyada bu yok. İnsanlık kavramı yok.” (Katılımcı 1)

“Eğer biz bu araçları kullanarak kendimizi genişletiyorsak o zaman insanlığı korumak için teknolojinin bir parçası olarak insan hakları yasalarını da genişletmeliyiz. Bu düşüncelere daha çok uzaktayız.” (Katılımcı 1)

“Politik olarak bir çözüm olacağını pek sanmıyorum. Politik olarak bir çözüm olmadan da bunu çözemeyeceğiz. Ama şu andaki politikacılara baktığımızda o kadar uzaktalar ki bu konuyu anlamaktan.” (Katılımcı 1)

Buna göre İnsan Hakları Sözleşmesi gibi fiziksel dünyayı içeren yasalar bütünüünün dijital ortamı kapsayacak gerçek anlamda bir yansıması bulunmamaktadır. İnsanı zenginleştiren bir uzva dönüşen çevrim içi uygulama ve hizmetler için belirli bir ulus üstü sözleşmenin yokluğu problem olarak karşımıza çıkmaktadır. Katılımcı 1, siyasilerin bu düşünceleri algılamada çok uzak olduklarını ama onlar da işin içine girmeden bu düzenlemelerin yapılamayacağını ifade etmektedir.

Veriyi toplama, birleştirme, anlamladırma ve yorumlayarak yeni veriler üretme noktasına gelindiğinde algoritmalar ve onların çalışma prensipleri karşımıza çıkmaktadır. Mevcut sistemde algoritmaların birincil olarak şirketlerin kârlılığını

sağlamak amaçlı çalıştığı söylenebilmektedir. Öte yandan bu algoritmaların şeffaflığı konusunda da şüpheler söz konusudur. Etik bir web için algoritmaları ve algoritmik şeffaflığın gerekliliğini Katılımcı 5 şöyle açıklamaktadır:

“Bir önceliklendirme algoritması kullanıyorsan bunu önce neden kullandığını açıklayacaksın. Şeffaf olmak gerek. Ben böyle bir algoritma yaptım, bundan dolayı böyle bir içerik göreceksin. En çok mesajlaştığın arkadaşının mesajını göreceksin.” (Katılımcı 5)

“Algoritmaların toplum yararına kullanılması çok mümkün. Bir verinin birikmesi her zaman kötü bir anlama gelmez. Ama veriye ben sahipsem.” (Katılımcı 5)

“(…) Ancak böyle sistemlerin içinde (Merkezîyetsiz web) algoritmalar işe yarayabilir. O zaman bana şeffaf bir algoritma sunabilir. Belki algoritmayı bile kendim belirleyeceğim onun içinde. Ya da algoritmaları hiç kullanmak istemiyorum diyeceğim.” (Katılımcı 5)

Katılımcı 1, algoritmaların şu anda şirketlerin çıkarı için çalıştığını ve insanın çıkarına çalışması için algoritmayı değiştirmenin bile gerek olmadığını ifade etmektedir:

“Algoritma dediğin şey bir program. Kimin çıkarları için çalışıyor. Bu algoritmaları farklı yazmak vs. değil, değişik bir algoritmaya bile gerek yok. O algoritmanın bulduklarının nasıl paylaşıldığı çok önemli. Şirketle mi paylaşıyor veya onla paylaşmıyorsa bile senin telefonunun üzerinde ‘şu reklamcılar bunlarla ilgi gösterebilir’ diye oradan reklam gösterebiliyor. O şirkete verin hiç gitmedi. Ama yine de senin çıkarına değil. Yine de senin depresyonda olduğunu anlayıp sana reklam gösterebiliyor. Apple’ın haberi yok. Apple ‘ben senin mahremiyetini hiç bozmadım’ diyor. Senin mahremiyetini yine de ihlal etti. Çünkü senin çıkarın için çalışmıyor o algoritma. Bu teknolojik bir problem değil, algoritmayı değiştirme problemi de değil, teknolojiye kimin sahip olduğuyla ilgili.” (Katılımcı 1)

Algoritmaların şeffaf olmaması ile kimin çıkarı için çalıştığı sorunu etik web’in önündeki bir engel olarak karşımıza çıkıyor. Katılımcı 1, algoritmaların insanlığın kendi çıkarına çalışması için gereken modeli şöyle açıklamaktadır:

“Nasıl böyle bir sistem yaratabiliriz? Çok basit. Algoritmalar kendi cihazlarında olacak. Google ya da Facebook’un sunucularında değil. Senin telefonunda, senin bilgisayarında veya senin sahip olduğun bir yerde olacak. Sunucu bile olabilir. Senin kontrolünde değilse eğer uçtan uca şifreli olarak senin sahip olduğun kanıtlanabilecek. Veriler orada olacak. Algoritmalar senin elinde olacak, cihaz senin elinde olacak.” (Katılımcı 1)

İnsanların kendi verilerine kendisinin sahip olması ve algoritmaların bu verilerle şeffaf biçimde işlem yapması Katılımcı 1'in önerisinde yer almaktadır. Buradaki "veri sahipliği" kendisinin daha önce de ifade ettiği gibi kişinin veriye sahip olması ve kendisi satması değildir. Katılımcı 1'in deyişiyle buradaki sahipliğin mantığı *"kendine sahip olmak ve kendini kontrol edebilmek zorundasın ki başka birisi sana sahip olmasın ve kontrol edemesin."* anlamı taşımaktadır. Böyle bir modelin kapitalizme bile karşı olmadığını belirtmektedir:

"Bu sistem kapitalizme bile karşı değil. Kapitalizm sevgilisi değilim ama ona bile karşı değil. İnsanlar hâlâ cihazları yaratıp satabilirler, hâlâ bu sistemler için uygulama geliştirebilirler. Güncellemeler için para alabilirler. Hatta bunu şu anki sistemde bile yapabiliriz. Ama şu anda gördüğümüz kadar büyük bir kârlılık getirmez." (Katılımcı 1)

Teknoloji şirketleri ve üreticilerinin mallarını veya yazılım hizmetlerini satarak hâlâ kâr sağlayabileceği bu modelde "gözetleme" ve "veri birikimi" ortadan kalkacağı için asıl gelir kaynağı yok olacaktır. Katılımcı 1, bu iki kavramın getirdiği kârı, kölelik sistemine benzetmektedir:

"Şu anki kâr kölelik zamanında gelen kâr gibi. Tabi kölelik çok güzel bir işti, eğer o zaman köle sahibiyse. Hiç para vermiyordun, ne güzel işlerini yapıyorlar. Ama insan hakları yok. Aynı şey şu anda. Alternatif olarak yaratacağımız sistemlerde teknolojik olarak bir sorun yok. (...) Yatırımcı problemi var, siyasi irade problemi var." (Katılımcı 1)

Başarı kriteri milyon dolar kazanmak olan girişim sermayedarlarının yerine insana saygı duyan etik teknolojilere yatırım için kaynak bulma problemi ortaya çıkmaktadır. Katılımcı 1, vergi kaynağıyla fonlanabilecek kâr amacı gütmeyen bağımsız teknolojik kuruluşların web'te ve teknolojide daha etik alternatifler üretebileceğini düşünmektedir:

"Biz vergi veriyoruz değil mi? Hükümet yapsın bunu demiyorum, ama bu vergileri kullanarak bu alternatifleri yarattırabiliriz. Mesela bağımsız kurumlar kurarak. Devlete bağlı değil ama vergilerimiz kaynaklı. Silikon Vadisinde nasıl bir adam geliyor ve al beş milyon, al beş milyon diye dağıtıyor. Bu yatırımlarının arasında birisi tuttuğunda milyar dolarlık bir şirket oluyor. Onun yerine vergilerimizden al bir milyon dolar, yeter. Aynı sistemi kullanalım. 10 tane organizasyon bul, al ne kadar istersen vergi içinden." (Katılımcı 1)

“Ama teknoloji şirketlerinin başarı kriteri farklı. Silikon Vadisinde milyar dolarlık şirket olacaksın, sonra girişimini elden çıkaracaksın vesaire. Ama sizin başarı kriteriniz topluma yararlı bir şey yapılması. Sürdürülebilir olacak. Bedava ve açık kaynaklı olacak ki herkes alıp onu değiştirebilsin. Bunları neden yaratmıyoruz?” (Katılımcı 1)

Katılımcı 1, büyük teknoloji şirketlerini AVM'lere benzeterek dijital “parklar” inşa etmenin gerektiğini vurgulamaktadır:

“Mesela biz bir parka o parayı harcıyoruz değil mi? Herkese ait bir park yaratıyoruz. Teknolojideki problem şu anda park yok. Her yer alışveriş merkezi gibi. Parklara ihtiyacımız var.” (Katılımcı 1)

Park metaforu ile Katılımcı 1, sadece insanın çıkarına çalışan topluma yararlı bir teknolojinin üretilmesi için değerli bir öneri sunmaktadır. AVM'lerde de her ne kadar banklar, oyun parkı vb. alanlar olsa bile onlar ticari bir amacın yan unsurlardır. Hâlbuki parklar toplumdaki her kesimin kendi amacı doğrultusunda kullanabileceği alanlardır.

Katılımcı 5, ulus üstü yasal düzenlemelerin yanında web'in merkeziyetçi yapısından uzaklaşılması gerektiğini vurgulamaktadır. Bu bağlamda daha önce paylaştığı Solid projesinin değerli bir öneri sunduğunu dile getirirken onun anlaşılması ve yaygınlaşmasındaki muhtemel problemleri de şöyle açıklamaktadır:

“Solid gibi sistemleri kolaylaştırmaları lazım. Çünkü yaşlılara nasıl anlatacağız pods alacaksın ve onun içerisinde veri olacak. Herkese hem bir maliyet oluşturuyor hem de zorluk oluşturuyor. Zaten merkezi internetin gelişmesinin en büyük nedeni kolaylığı. Çok kolay kullanılabiliyor olması. Onun sayesinde büyüklerimiz bu platformlara girebiliyorlar. Önceden biraz kod yazman veya çeşitli beceriler gerekebiliyordu. İşleri kolaylaştırdıkları için merkezileştiler. Bu kolaylığı diğer taraflarda da sağlamak lazım. ” (Katılımcı 5)

Web'e hâkim merkezî platformların kolaylığı onların tüm kesimlere yayılmasında büyük bir avantaja sahiptir. Öte yandan onların opak çalışma prensipleri de merkeziyetçiliğin oluşumunda rol oynamaktadır. Örneğin, Facebook, Instagram, Twitter gibi platformların mobil uygulamalarında bile tıklanan bağlantılar bir tarayıcıda değil kendi uygulaması dâhilinde açılmaktadır. Diğer tüm unsurlar bir yana,

bu bile merkezîyetçiliğin başlıca göstergelerinden birisidir. Katılımcı 5, e-posta sistemi üzerinden merkezîyetsiz web'in ne olduğunu anlatmaktadır:

“En merkezîyetsiz internet e-posta'dır. Benim Gmail'im varsa Hotmail'e posta gönderebilirim. Hotmail'den Yahoo'ya posta gönderebilirim. Bir merkezi yok çünkü. Ama şu an ne var? WhatsApp'tan Telegram'a mesaj atamıyorum şu anda. Ama internet bunun tam tersi için inşa edilmiş.” (Katılımcı 5)

Bu örnek merkezîyetin oluşturduğu kendine bağlılığı resmetmede oldukça değerlidir. Katılımcı 5, merkezîyetsiz web için potansiyelin blokzincir teknolojisinde olduğunu düşünmektedir:

“Solid, çok iyi niyetli ve çok iyi bir fikre sahip ama daha çok blokzincir teknolojisinde bir gelecek görüyorum. Blokzincir, interneti merkezsizleştirmeye giden teknoloji.” (Katılımcı 5)

“Blokzincir'de bir potansiyel var ama bunun kitleselleşmesi, tabana yayılması biraz zaman alacak. Blokzincir üzerine kurulu bir sosyal medyada insanlığın iyiliğine doğru bir gelecek görüyorum.” (Katılımcı 5)

Katılımcı 5, blokzincir üzerinde merkezî olmayan platformların inşasıyla etik kodların işlev kazandığı bir web'in inşa edilebileceğini belirtmektedir. Bu alt temada katılımcıların değerlendirmelerini özetlersek; ulus üstü yasal düzenlemeler oluşturulmalı, buna bağlı olarak yasalar ama'sız ve fakat'sız uygulanmalı, teknolojiler ve algoritmalar bireylerin çıkarına ve faydasına çalışmalı, etik tasarım ilkelerine bağlı olmalı ve merkezîyet ortadan kalkmalıdır.

Özetleyecek olursak, nitel araştırma bulguları gözetim kapitalizmi, çevrim içi reklam, kişisel veriler ve hukuk, veri farkındalığı, mahremiyet ve etik web temaları çerçevesinde ele alınmıştır. Her bir tema ihtiyaç doğrultusunda alt temalara ayrılmış ve söz konusu alt temalarda katılımcı yorumlarına yer verilmiştir. Her katılımcıya hem çalışmayla ilişkili ortak hem de uzmanlık alanları doğrultusunda özel sorular sorulmuştur. Nitel araştırma, araştırmanın nicel bulgularının yorumlanmasına yardımcı olması ve nicel olarak ölçülemeyen araştırma sorularının cevaplanmasına katkı sağlaması bakımından değerli yorumlara sahiptir. Gözetim kapitalizmi teması içerisinde genel olarak gözetim ve kapitalizm ilişkisi, gözetimi bir iş modeli olarak benimseyen şirketler ve teknolojik hizmet ve cihazları sahipliği irdelenmiştir. Çevrim

içi reklamcılık temasında reklamcılığın mevcut konumu dikkate alınarak gözetim bağlamında tartışılmıştır. Yasal düzenlemeler temasında kanunların verilerin toplanması, işlenmesini ve aktarılmasını nasıl ele aldığı ve cezaların ne derecede caydırıcı olduğu üzerine yorumlarda bulunulmuştur. Veri farkındalığı ve mahremiyet temasında çevrim içi mahremiyetin önemi paylaşılmış; mahremiyetin ne kadar değerli olduğu ve veri farkındalığının artmasıyla bu değer daha da açığa çıkacağı fikirleri belirli metaforlar üzerinden aktarılmıştır. Son olarak, etik web teması altında web'in mevcut problemi ve web'i daha etik hâle getirmenin olası çözüm yolları tartışılmıştır. Tartışmalar neticesinde katılımcıların etik bir web için paylaştığı çözüm önerilerine yer verilmiştir.

4.4. Araştırma Bulgularının Yorumlanması ve Tartışma

Bu başlıkta hem nicel hem de nitel araştırma bulguları yorumlanmakta ve araştırma sorularına cevap aranmaktadır.

AS1: Hangi platform ve şirketler, web siteleri ve mobil uygulamalar aracılığıyla veri toplamaktadır?

Araştırma kapsamında incelenen 48 sitenin 10'unda üçüncü taraf çerez tespit edilmemiştir. Bunlar Google (Google.com ve Google.com.tr), Facebook, WhatsApp, Wikipedia, Microsoft Live, Amazon, Tiktok, Yandex ve Türkiye E-Devlet (turkiye.gov.tr)'dir.

Google, halihazırda hem arama motoru hem sahip olduğu e-posta, harita, takvim, video oynatıcı vb. birçok ürünü hem de android işletim sistemi ve Google uygulamaları aracılığıyla muazzam bir kullanıcı verisi toplamaktadır. Mevcut durum değerlendirildiğinde bu konuda dünyada tektir, tekeldir; neredeyse tüm yeni girişimlerin örnek aldığı bir modeldir. Dolayısıyla kendi platformlarında üretilen davranışsal verileri başka üçüncü taraflarla paylaşması veya onların bu verileri görüntülemesi söz konusu dahi olamaz. Kendi iş modeli bağlamında dışarıdaki şirketlerden alması gereken hiçbir hizmet yoktur. Kendi içine dâhil etmek istediği tüm ürün ve hizmetleri satın alacak güce sahiptir. 2005 yılında video barındırma sitesi

YouTube, 2006 yılında mobil reklamcılık şirketi AdMob, 2007 yılında reklam şirketi DoubleClick, 2014 yılında akıllı ev otomasyon sistemi Nest, 2019 yılında veri analiz şirketi Looker ve giyilebilir teknoloji cihazı Fitbit, Google tarafından satın alınmıştır. Google'ın tek ihtiyacı olan tüm ürünlerinin olabildiğince çok insan tarafından düzenli olarak kullanılmasıdır. Her bir anın ve deneyimin gözetimi, kişinin şimdi ne olduğu ve sonra ne olacağına ilişkin mükemmel bir profil çıkartılmasını mümkün kılmaktadır.

Instagram, Facebook, Yandex, Türkiye E-Devlet, WhatsApp, Wikipedia, Microsoft Live, Amazon ve Tiktok hariç tüm sitelerde en az bir Google hizmetine ait çerez bulunmaktadır. Kâr amacı gütmeyen Wikipedia ve devletin resmî hizmeti Türkiye E-Devlet'i ayırırsak, verilen diğer şirketlerin Google ile veri paylaşmaması gayet olağandır. Çünkü her biri yalnızca Türkiye'de değil dünya çapında bilinen, kullanılan ve oldukça değerli kullanıcı verilerinin üretildiği platformlardır.

Facebook da tıpkı Google gibi dışarıdan hiçbir hizmete ihtiyaç duymamaktadır. O da Google gibi insan davranışlarını bütüncül olarak anlamlandırmak, şimdi ve gelecekte neler olacağını tahmin etmek için hem kendi platformundaki hem de ürünleri aracılığıyla kullanıcı verilerini toplamaktadır.

38 site gerek reklam gerekse analitik amaçlı en az bir adet üçüncü taraf çerez barındırmaktadır. Birden çok siteye erişimi olan aynı üçüncü taraf şirketlerin çerezleri, kullanıcıları siteler arası takip edebilmekte ve aynı kullanıcıya ait farklı davranışsal verileri birleştirerek kullanıcı hakkında zengin bir profil oluşturabilmektedir.

Başta Safari ve Firefox olmak üzere çeşitli tarayıcılar üçüncü taraf çerezlerin erişimini kısıtlama girişimi içindedir. Söz konusu analitik ve reklam şirketleri ise birkaç yıldır web siteleri ve kendi sunucuları arasında veri alışverişine izin veren, üçüncü taraf çerez olmayan ama belirli tanımlayıcılara dayanan çözümler üretmektedir. Özellikle üçüncü taraf şirketlerin, sitelerin doğru ve verimli çalışmasını sağlayan, yasal olarak herhangi bir sakıncası olmayan kullanılması zorunlu birinci taraf çerezler aracılığıyla veri alışverişinde bulunacakları öngörülmektedir. Örneğin, Criteo üçüncü taraf çerezlerin tarayıcılar tarafından engellenmesini bir tehlike olarak

görmektedir, zira iş modelinin yarısı hâlâ üçüncü taraf çerezlere bağlıdır ²⁶. Criteo bu sorunu aşmak için çerezlerinin yer aldığı sitelerin alan adlarına kendi belirledikleri CNAME kaydı ekletmek istemiştir. Bu yöntemin kullanılmasıyla Criteo artık yer aldığı sitelerde üçüncü taraf değil, birinci taraf olacaktır. Ayrıca üçüncü taraf çerezleri engelleyen tarayıcılar, eklentiler veya reklam engelleme uygulamalarını rahatlıkla aşabilecektir. İlerleyen zamanlarda diğer şirketlerin de bu yöntemi benimsemesiyle şu anda kullanıcıları izleyen şirketlerin onları izlemeye devam edeceği görülmektedir. Konuyla ilgili güncel gelişmeler “*Çerezsiz Dünya ve İzleme Teknolojilerinin Geleceği*” başlığında yer almaktadır.

Araştırma kapsamında incelenen 72 mobil uygulamanın 55’inde en az bir adet başka bir şirkete ait izleyici tespit edilmiştir. Diğer 17 uygulamada kendi analitik ve reklam izleyicileri hariç hiçbir üçüncü taraf izleyici bulundurmayan uygulamalar şunlardır:

- Facebook,
- Google ürünleri (Google, Chrome, Duo, Çeviri, Rehber, Gboard, Telefon, Haritalar, Gmail, Fotoğraflar, YouTube, Drive, Carrier Services)
- Meb E-Okul
- Binance TR
- Samsung Internet Tarayıcısı

Araştırmada uygulamaların en çok tercih ettiği üçüncü taraf izleyicilerin ilk dördünü Google hizmetlerinin oluşturduğu gözlemlenmiştir.

Sonuç olarak web sitelerinin %79’unda 112 farklı şirkete ait izleme ortaya çıkarılmıştır. Mobil uygulamaların ise %76’sında 84 farklı üçüncü taraf izleyici tespit edilmiştir. Büyük teknoloji şirketlerinin kendi platform ve uygulamalarında rakip hizmetleri üçüncü taraf olarak kullanmadıkları göz önünde bulundurulduğunda diğer

²⁶ https://criteo.investorroom.com/download/Deck_CriteoOnlineIdentification.pdf

site ve uygulamaların ortalama %95'inin üçüncü taraf izleyicileri barındırdığını söylemek mümkündür.

AS2: Hangi tür gözetleme araçları ve teknolojiler verilerin toplanmasında rol oynamaktadır?

Araştırmanın nicel bulgularında görüldüğü üzere üçüncü taraf şirketlerin neredeyse hepsi reklam ve analitik amaçlı hizmetler vermektedir. Analitik şirketleri hem reklamların performanslarını analiz etmekte, hem kullanıcı hakkında sahip oldukları verileri zenginleştirmekte hem de kullanıcıları anlık olarak izleyerek sitenin performansını artırmaya yönelik hizmetler sunmaktadır. Örneğin, Hotjar'a ait izleme kodları hepsiburada.com'da ve n11.com'da yer almaktadır. Hotjar, bu iki sitede de kullanıcıların çevrim içi davranışlarını takip ederek her bir hareketi üzerinden ısı haritaları oluşturmaktadır. Hotjar bu hizmeti sunarken kullanıcının nereye tıkladığı, ne hızla yazdığı, nereye baktığı veya nereyi görmezden geldiği ve sayfanın ne kadar aşağısına kadar indiği gibi bütüncül bir izleme gerçekleştirir.

Reklam şirketlerinin hepsi, bulgularda verilen alan adlarına ait izleme kodlarının yerleştiği tüm sitelerde kullanıcıları takip etmekte, onların sitedeki davranışsal verilerini toplamakta, analiz etmekte, bir araya getirmekte ve onlara kişiselleştirilmiş reklam göstermektedir. Örneğin, Taboola'ya ait izleme kodları hürriyet.com.tr, milliyet.com.tr, internethaber.com, cimri.com, ntv.com.tr, nefisyemektarifleri.com, onedio.com, nesine.com, mynet.com ve sabah.com.tr adreslerinde yer almaktadır. Taboola, bu şekilde söz konusu siteleri ziyaret eden kullanıcıları anlık takip edebilir, onlara saniyenin onda birinde hazırlanan kişiselleştirilmiş reklam ve içerikler gösterebilir. Detaylı olarak ele aldığımızda Taboola, bir kişinin hangi haberleri okuduğunu (haber siteleri), hangi bahisleri yaptığını veya hangi takımı tuttuğunu (nesine.com), hangi çevrim içi testleri cevapladığını (onedio.com), hangi ürünlerin fiyatlarını takip ettiği, görüntülediği ve satın aldığı (cimri.com) ve hangi yemekleri sevdiği (nefisyemektarifleri.com) hakkında veri toplayabilmektedir. Bu verileri analiz ederek kişiyi alışveriş

alışkanlığına, tuttuğu takıma, adrenalin seviyesine, psikolojik durumuna, siyasi görüşüne ve yeme alışkanlığına göre gibi birçok kategori altında sınıflandırılabilir.

Bir başka şirket Tapad'a ait izleme kodları milliyet.com.tr, mynet.com, onedio.com, nefisyemektarifleri.com ve doviz.com'da yer almaktadır. Tapad, kullanıcıları farklı cihazlarda tanıyarak cihazlar arası reklam gösterebilmektedir. Cihazlar arası reklamcılık, reklam hedeflemesine maruz kalan bir kişinin hem bilgisayarında hem de cep telefonunda aynı reklamı görmesini ifade etmektedir. Privacy International, 2018 yılında hazırladığı bir raporda Tapad şirketinin üç temel ürününden dolayı endişe duyduklarını dile getirmiştir. Bu ürünler; (1) Tapad Grafiği: pazarlamacıların farklı cihaz ve kanallar aracılığıyla çok sayıda tüketici yakalamasını ve kitleselden bireyselle doğru hedefleyebilmelerini sağlar. Tapad grafiği dünya çapında kullanımda olan milyarlarca dijital cihaz hakkında veri içerir. (2) Cihaz Grafiği Erişimi (DGA): Bu ürün Tapad müşterilerinin cihazlar arası verilere erişmelerine olana tanır. (3) Tapad Müşteri Veri Platformu: Telekom ve mobil ağ operatörlerinin Tapad Grafiği ile çeşitli dâhili ve yayıncı verilerini (üçüncü taraf olarak yer aldıkları site ve uygulamalardan elde ettikleri veriler) bir araya getirerek müşteri deneyim ve kazanımına katkı sağlar²⁷. Görüleceği üzere Tapad cihazlar arası reklam gösteriminin yanı sıra topladığı kullanıcı verilerini bir meta olarak ürünlerinin içerisinde tutmaktadır.

Web sitelerinde Google'dan sonra sayıca en çok tespit edilen izleyici kodları Criteo'ya aittir. Fransız şirket, devasa bir kullanıcı veri tabanı olan *Criteo Müşteri Grafiği (Shopper Graph)* adında bir sisteme sahiptir. Bu sistemdeki veriler reklamcılardan, veri alışverişi yaptığı diğer şirketlerden (Oracle, LiveRamp) ve yayıncılardan toplanan (izleme kodlarını yerleştirdiği web site ve uygulamalar) ve makine öğrenmesi yoluyla Criteo'nun oluşturduğu verilerden oluşmaktadır²⁸. Criteo, müşteri grafiğinin dünyadaki çevrim içi alışveriş yapanların %72'sinden gelen 35

²⁷ <https://privacyinternational.org/sites/default/files/2018-11/08.11.2018%20Final%20Complaint%20AdTech%20Criteo%2C%20Quantcast%20and%20Tapad.pdf>

²⁸ https://criteo.investorroom.com/download/Deck_CriteoOnlineIdentification.pdf

milyar günlük tarama geçmişi ve işlem aktivitelerine ve 120’den fazla alışveriş niyet sinyali²⁹ dayandığını belirtmektedir³⁰. 2 milyardan fazla kişiyi cihazlar arası tanıyarak oluşturduğu kimlik grafiği ile gerçek zamanlı kişisel hedefleme imkânına sahiptir ³¹. Criteo’nun kimlik grafiğinin oluşmasındaki temel yöntemlerden birisi de üçüncü taraf olarak web sitelerine yerleştirdiği çerezler ve mobil uygulamalardaki izleyici kodlarıdır. Türkiye’nin en çok ziyaret edilen ilk 48 web sitesinde 171 adet Criteo çerezi tespit edilmişti. Bu çerezlerin yer aldığı siteler her bir ziyaretçi geldiğinde gerçek zamanlı olarak Criteo’nun hem müşteri grafiğini hem de kimlik grafiğini beslemekte ve zenginleştirmektedir.

Mobil uygulamalarda yer alan üçüncü taraf analitik ve reklam izleyicileri anlık olarak kullanıcıların uygulama içi her bir aktivitesi hakkında bilgi toplamaktadır. Bunların arasında uygulamayı açma, kapama, kullanım süresi, görüntüleme, ekran kaydırma, tıklama, sepete ekleme, satın alma ve konum bilgisi gibi birçok işlem yer almaktadır. Uygulamaların kullanıcıdan talep ettiği erişim izinlerine bağlı olarak üçüncü taraflar telefon rehberine, mesajlara veya cihazdaki fotoğraflara kadar erişim sağlayabilmektedir.

Siteler arası kullanıcı takibi olduğu gibi, uygulamalar arası ve cihazlar arası takip de söz konusudur. Geçmiş site ziyaretleri ve mobil uygulama kullanımları kişilerin ayrıntılı profillerini çıkarmak için kullanılabilir. Google hem kendi hizmetleri aracılığıyla, hem de üçüncü taraf olarak web siteleri ve mobil uygulamalardan topladığı verilerle web’in tekeli durumundadır. Başka bir ifadeyle, neredeyse Google’dan habersiz bir kişi oyun oynayamaz, alışveriş yapamaz, haber okuyamaz, bir yere gidemez ve fotoğraf paylaşamaz.

AS3: Web siteleri, üçüncü tarafların izleme teknolojilerini kullanması için kullanıcılardan nasıl izin almaktadır?

²⁹ Potansiyel müşterilerin ürüne veya markaya ilgi gösterdiğini gösteren veri noktalarıdır. Ing: Intent Signal.

³⁰ https://support.criteo.com/s/article?article=Criteo-Shopper-Graph&language=en_US

³¹ https://criteo.investorroom.com/download/Criteo_Q1_2020_Investor_Presentation.pdf

Kullanımı zorunlu olmadığı sürece çerez, piksel ve benzeri tüm izleme teknolojileri için kullanıcıdan açık rıza alınması gerekmektedir. Çerezler yalnızca üçüncü taraf değil, birinci taraf bile olsa analitik veya reklam amacıyla kullanıcı davranışları hakkında veri toplanması kullanıcının açık rızasına bağlıdır.

Araştırma kapsamında incelenen 48 siteden 38'inin üçüncü taraf şirketlere ait çerez barındırdığını paylaşmıştık. Üçüncü taraf çerez barındıran ve barındırmayan tüm sitelerin çerez bildirim ve açık rıza onay kutularını nasıl sunduğunu aşağıdaki gibidir:

- 22 web sitesinde kullanıcılara çerezlerle ilgili hiçbir bildirim yapılmadığı gözlemlenmiştir. Dolayısıyla açık rıza söz konusu değildir.
- 12 web sitesinin yalnızca çerez kullandıklarına ilişkin bir bildirim yaptıkları ve kullanıcılardan herhangi bir açık rıza almadıkları belirlenmiştir.
- 10 web sitesi, çerez kullandıklarına ilişkin yaptıkları bildirimde yalnızca kullanıcıların onaylamasına yönelik tek bir butona yer vermektedir. Başka bir seçenek olmadığı için açık rıza söz konusu değildir.
- 3 web sitesi, çerez kullandıklarına ilişkin yaptıkları bildirimde kullanıcıların onaylaması için bir buton koymanın yanı sıra çerezleri kategorilerine göre “etkin” veya “etkin değil” şeklinde düzenleyebilecekleri bir bağlantı da sunmaktadır. Fakat söz konusu çerez kategorileri varsayılan olarak etkin gelmektedir. Son olarak tek bir sitenin çerezleri kabul et ve çerezleri özelleştir butonu koyduğu ve çerezlerin etkin olarak gelmediği tespit edilmiştir.

İncelenen 48 sitenin hiçbirinde siteye ilk girildiği zaman yaptıkları çerez kullanım bildirim ekranında “çerezleri reddet” seçeneğine yer vermediği görülmüştür.

Araştırma kapsamındaki siteleri ziyaret eden bir kullanıcı üçüncü taraf çerez barındırmayan siteler ve Hürriyet, Milliyet ve Amazon haricindeki 35 sitede şeffaf, özgür iradeye ve açık rızaya dayalı aktif bir seçim ile çerezleri reddetme imkânına sahip değildir.

AS4: Web sitelerinin çerez politikaları ve gizlilik sözleşmeleri kullanıcı faaliyetlerinin çevrim içi gözetlenmesini nasıl ele almaktadır?

Web sitelerinin %6'sında (n=3) herhangi bir çerez politikası veya gizlilik sözleşmesine rastlanmamıştır. Bu sitelerin ikisinin devlete ait siteler (meb.gov.tr ve eba.gov.tr) olduğu tespit edilmiştir.

Geriye kalan 45 sitenin sözleşme metinlerinde, araştırmacının hazırladığı yedi soruya minimum gereksimleri karşılayacak düzeyde cevap aranmıştır. Buna göre sözleşmelerin;

- %88'inde (n=40) hangi verilerin toplandığı,
- %88'inde (n=40) verilerin hangi amaçla toplandığı,
- %73'ünde (n=33) toplanan verilerin nasıl işlendiği,
- %77'sinde (n=35) kategorik düzeyde de olsa hangi üçüncü taraflarla paylaşıldığı,
- %51'inde (n=23) çerezlerin ne kadar süreyle cihazda saklandığı,
- %87'sinde (n=39) kişisel verilerin silinmesi için bir iletişim bilgisinin yer aldığı,
- %18'inde (n=8) üçüncü taraf sözleşmelere sorumluluk yıkma durumu tespit edilmiştir.

Yukarıda verilen bulgular doğrultusunda sözleşmelerin minimum gereksinimlere sahip olduğunu söylemek mümkündür. Genel anlamda iletişim formları, üyelik bültenleri veya farklı formlar aracılığıyla toplanan kişisel verilerin yanı sıra izleme teknolojilerine ilişkin açıklayıcı ve bilgilendirici metinler sitelerin neredeyse yarısında yoktur. Örneğin, hangi üçüncü taraf çerezlerin cihaza yerleştirildiği ve o çerezlerin ne kadar süreyle cihazda kalacağına ilişkin şeffaf bir açıklama yalnızca 23 sitede yer almaktadır.

Üçüncü taraf çerezlerin sıkça tercih edildiği sitelerde genellikle üçüncü taraf şirketlerin adlarından ziyade söz konusu şirketlerin çerezlerini hangi amaçlarla kullandıklarına ilişkin bilgi verilmiştir. Örneğin Ekşi Sözlük, kullanıcı verilerinin

ölçüm, reklam, hedefleme ve analiz gibi nedenlerle üçüncü taraflarla veri paylaşıldığını ifade etmektedir. Araştırma kapsamında bu ifadenin “hangi üçüncü taraflarla paylaşıldığı” sorusuna cevap verdiği varsayılmıştır. Dolayısıyla minimum gereksinimi karşılamadan kasıt iyi niyetin aranmasıyla paraleldir. Gerek etik bağlamda gerekse yasal bağlamda ise durumun sorunlu olduğu açıktır. İsteyen kullanıcıların bir web sitesini ziyaret ettiklerinde sitedeki faaliyetleri, IP adresi vb. tüm verilerinin kimlere aktarıldığını bilmeye hakkı vardır.

Avukat olan Katılımcı 3, GDPR ile KVK kanunun çerezlere aynı perspektiften baktığını ifade etmişti. Diğer ifadeyle, Türkiye’deki bir web sitesinin Avrupa’dan gelen ziyaretçilere açık rıza talep eden bir çerez bildirim kutusu gösterirken, Türkiye’den girenlere böyle bir seçenek sunmaması diye bir durum yasal prosedürler bakımından söz konusu olamaz. Türkiye’deki yasalar da kullanıcıdan açık rıza alınmasını öngörmektedir. Oysa daha önce paylaşılan ve Grafik 4.3 ve Grafik 4.4.’te yer alan mynet.com’un çerez bildirim kutuları yurt içi ve yurt dışında farklılık göstermektedir. Yurtdışından gelen ziyaretçiler oldukça şeffaf, anlaşılır ve açık rızaya dayalı bir bildirim kutusuyla karşılaşırken, Türkiye’den giren ziyaretçilere bu imkân sağlanmamaktadır.

Kişisel verilerin nasıl silineceğine dair bir iletişim adresi ise 39 sitede yer almaktadır. Diğer yandan sitelerde kullanıcıların çerezleri nasıl pasif hâle getirebileceğine ilişkin genelgeçer açıklamalar vardır. Sözleşmelerde özellikle tarayıcılar üzerinden üçüncü taraf çerezlerin nasıl engelleneceği bilgisi paylaşılmıştır. Bazı sözleşmelerde nadiren de olsa *youradchoices.com* gibi üçüncü taraf şirketlerin sıralandığı ve kullanıcılara “onlar beni takip etmesin” olanağı sunduğu varsayılan öneriler sunulmuştur. Sözleşmelerdeki bu öneriler şu nedenle sorunlu gözükmemektedir: Bir kullanıcı ziyaret edilen sitedeki üçüncü taraf çerezleri engellemek istiyorsa neden tarayıcı üzerinden bunu yapmalı? Çünkü yalnızca ziyaret edilen sitede üçüncü tarafların onu izlemesini istemiyor olabilir. Eğer kullanıcı mevcut sitede üçüncü taraf çerez istemiyorsa bütünüyle bu sistemi engellemeli şeklindeki öneri kullanıcıya bir dayatmadır. Bir kullanıcı ruh veya cinsel sağlığı gibi özel nitelikli sayılabilecek işlemler üzerinden üretilen verilerin o web sitesinde başkaları tarafından görülmesini

ve kayıt altına alınmasını istemeyebilir. Dolayısıyla web sitelerinin açık rıza almak yerine sözleşmelerinde inşa ettiği çeşitli rıza simulakr'larının hem etik hem de yasal zeminde sorunlu olduğunu söylemek mümkündür.

AS5: Teknoloji şirketleri ve gözetleme faaliyetleri arasında nasıl bir ilişki söz konusudur?

Aral Balkan, 2015 tarihli bir yazısında hizmetler ve kullanıcılar arasındaki ilişkiyi Kobe bifteği üzerinden örneklendirmektedir. Ona göre Wagyu sığırlarına yapılan masaj sığırın yararına değildir. Masaj, sığırı daha iyi bir ürün hâline getirmek için yapılır. Sonunda dünyaca ünlü Kobe bifteği çıkar ³². Google ve Facebook gibi teknoloji şirketlerinin, Criteo gibi reklam şirketlerinin, BlueKai gibi veri şirketlerinin gelirlerinin artması ve yeni teknolojik girişimlerin daha çok yatırımcıyla buluşması kullanıcılara nasıl “daha iyi ve farklı masaj tekniklerini” uyguladıklarıyla yakından ilgilidir.

Bireyin davranışlarını, iletişimini ve dijital emeğini gözetleme temelli iş modelleri bugün teknoloji altyapılı girişimlerin çoğunun benimsediği bir sistemdir. Google'ın öncülüğünde başlayan çevrim içi davranışsal faaliyetlerden artı değer üretilmesi tüm şirketlerin bu yola girmesine ön ayak olmuştur. Günümüzde ağa bağlanabilen teknolojik bir hizmete veya ürüne bedelini ödeyerek sahip olmak onun kişiyi takip etmeyeceği anlamına gelmemektedir. Şirketler yalnızca bir ürün satarak kâr elde etmez; o ürünü kullananları gözetleyerek ürünün kullanımından da artı değer elde etmeye devam eder. Gözetim ve kârlılık birbirini besleyerek zenginleşmeyi getirir. Gözetim kapitalizminin diğer kapitalizm sınıflandırmalarından farkı da bu noktada ortaya çıkmaktadır.

Araştırmanın nicel bölümünde tespit edilen üçüncü taraf şirketler reklam ve analitik şirketleri olarak tanımlansa da işlerinin temelinde gözetleme olduğu için bir yandan da gözetim şirketleridir. Reklam teknolojileri ekosistemindeki tüm aktörler için aynı şeyi söylemek mümkündür. Söz konusu aktörler üçüncü taraf olarak yer

³² <https://ar.al/notes/the-3-rs-of-ethical-design/>

aldıkları web siteleri ve uygulamalarda kullanıcıları daha iyi tanımak için gözetlerler. Gözetleme sonucu oluşturulan kişi hakkındaki detaylı bilgiye dayanarak ona kişiselleştirilmiş reklam gösterilmesi sağlanır. Bu hedefli reklamın gösterilme sürecinde gözetleme önemli bir yere sahip olduğu için bu şirketler aynı zamanda gözetim odaklı iş üretmektedirler.

İnsanların ne yaptığı, nereye gittiği, kiminle konuştuğu, neye ihtiyacı olduğu ve şu an nerede olduğu gibi insana ait yüzlerce durum birçok şirket tarafından merak edilmekte ve gözetlenmektedir. Bunlar arasında Google, Facebook, Amazon veya diğer büyük teknoloji şirketleri olabildiği gibi basit bir el feneri mobil uygulaması da gözetleme sürecine dâhil olabilmektedir. El fenerinin konum verisini (Bkz.: Tablo 2.3) talep etmesinin altında yatan neden ile gözetimin baskın bir iş modeli olmasında paralellik vardır. Bu durumda el feneri uygulamasının hangi amaçla üretildiği sorusu akıllara gelmektedir: insanlara bir hizmet sağlamak için mi? yoksa konum verisi toplamak için mi? Diğer bir ifadeyle, el feneri uygulamasının sağladığı hizmet kullanıcıları gözetlemek ve haklarında veri toplamak için bir mazeret midir? Bu sorular “gözetim kapitalizmi” çerçevesinde değerlendirildiğinde el fenerinin amaca ulaşmak için bir araç olduğunu söylemek mümkündür. 2027 yılında konum verisi pazarının bugüne kıyasla 3 kat artarak 37 milyar dolar olması beklenmektedir (Grand View Research, 2020). Bu beklentinin oluşmasında hem arzın hem de talebin artış yaşayacağı öngörüsü yer almaktadır. Kişinin konum bilgisi ve rutini gibi yalnızca tek bir verinin piyasadaki değeri, konum bilgisine ihtiyaç duymayan uygulamaların konum verisini toplaması veya konum verisi toplamak için ücretsiz ilgi çekici uygulamalar oluşturarak uygulama mağazasına yerleştirilmesi ile sonuçlanmaktadır.

Gözetimin baskın bir iş modeli olması bugünün kazancıyla değil yarının kazancıyla ilişkili olmasındandır. Katılımcı 1’in örnek verdiği SoftBank’in geleceğe dair yaklaşımının merkezinde “gözetleme” vardır. Toplamı yüz milyarlarca doları aşan satın almalarının arkasında dünyada yapılan her bir işlemin kendi dolayımıyla geçmesi arzusu yer almaktadır. İrili ufaklı yüzlerce teknoloji girişimine yaptığı yatırımlarla gözetleme sahasını genişletir. Satın aldığı veya yatırım yaptığı şirketlerin iş modellerinin herhangi bir yerinde gözetim olmasaydı, SoftBank’in ilgi radarına dâhil

olmazlardı. Çünkü SoftBank, bünyesinde topladığı farklı alanlardaki şirketler aracılığıyla bireyler hakkında sonsuz akışkan bir veri havuzu oluşturmayı hedefler. Yapay zekâ yatırımları ile bu verileri işleyerek yarının kârını ve gücünü elinde bulundurmaya planlar.

Katılımcılarla yapılan görüşmelerde teknoloji alanındaki şirketlerin neredeyse hepsinin kullanıcıların gözetlenmesinden beslendiğine ve bu yolla zenginleştiğine dikkat çekilmiştir. Son kullanıcıya fayda sağlayan çoğu ücretsiz hizmetin, hizmetleri karşılığında kullanıcı verisi topladığı söylemi dile getirilmektedir. Haber siteleri haberleri, mobil oyunlar oyunları karşılığında kullanıcı verilerinin işbirliği yaptıkları reklam ve analitik şirketleriyle paylaşımını sağlar. Ücretsiz hizmet sağlayıcılar (Google, Facebook vb.) sağladıkları hizmetler karşılığında hem kendi platformlarında hem de başka platformlarda kişiyle ilişkili gözetimini sürdürür. Örneğin, Google gözetime dayalı iş modelini terk ederek ücrete dayalı bir politika geliştirse ne olur? Daha açıkça ifade edersek, hizmetin ücreti karşılığında bedel ödenerek satın alınmasıyla ücretsiz hizmet ve kullanıcı verisi alışverişi sonlandırılmasının önündeki engel nedir? Tabii ki Google. Bir ürün satın alındığında satan taraf kârını elde eder ve süreç orada son bulur. Ücretsiz hizmet ve gözetleme ilişkisinde süreklilik söz konusudur. Kâr, her kişiden tek seferlik alışverişle değil; tek kişiden devamlı sağlanan bir şeydir. Google, YouTube hizmetinin ücretli versiyonunu yapmış olsa da kullanıcıları gözetlemediğini belirtmez. Yalnızca reklam göstermeme taahhüdünde bulunur. Gözetleme devam eder. Çevrim içi tüm platformlarda sağlanan hizmetlerin ücretsiz olmasının nedeni kapsamına olabildiğince insan almaktır. Bağımlılık yaratacak hizmetler üretilir, ücretsiz olarak sunulur ve içerisinde gerçekleşen tüm faaliyetler şirketler tarafından gözetlenir. Gözetleme yalnızca kendisiyle sınırlı değildir; gözetleyenler erişimlerinin olduğu farklı platformlarda da gözetlemeye devam eder. Her şirket, herkes hakkında olabildiğince veri toplar, onlar hakkında öngörüler üretir ve geleceklerini tahmin eder. Öngörü ürünlerinin stoğu tek bir satış ile azalmaz; yenilenebilir, genişleyebilir ve yeni anlamların doğmasını sağlayabilir. Tüm bunlar gelir döngüsünün çarklarını kuvvetli biçimde döndürür.

AS6: Kişisel verilerin korunmasına ilişkin yasal düzenlemeler, kullanıcı gözetimini azaltmaya yönelik nasıl bir katkı sunmaktadır?

Çalışmanın literatüründe kişisel verilerin korunması üzerine dünyadaki ve Türkiye’deki güncel yasal düzenlemelere yer verilmiştir. Söz konusu düzenlemeler doğrultusunda çevrim içi platformlarda üçüncü taraf şirketlere ait çerezlerin aktif hâle gelebilmesi için kullanıcılardan açık rıza almaları gerektiği ifade edilmiştir. Nicel araştırmada incelenen web sitelerinin hiçbirinin çerez bildirim kutularında “kabul etmiyorum” seçeneği yokken; yalnızca üç sitede çerezlerin amaçlarına göre kategorilerine ayrılarak aktif veya pasif hâle getirilebilmekte olduğu tespit edilmiştir.

Kullanıcı gözetiminin en temel amacı, kişiyi tanımak ve gelecek davranışlarını öngörmektir. Buradaki özne olan kullanıcı genellikle kimin, nerede ve nasıl onu gözetlediğinden, toplanan bilgilerin neler olduğundan ve ne amaçla kullanıldığından bihaberdir. Gözetleme sonucu kişinin kullandığı işletim sisteminin ne olduğundan henüz teşhis edilmemiş hastalığının ne olduğuna dek geniş bir yelpazede öngörü yapılabilmektedir. Bir yazılım veya program, kullanıcıdan gizli olarak kişisel bilgisayarından bilgi toplarsa bu “casus yazılım” veya “kötü amaçlı yazılım” olarak tanımlanır. Bir kişinin evine gizlice ve izinsiz olarak girerek evraklarını karıştırmak, kopyalamak ve çoğaltmak suç olarak nitelenir. Açık rızasını almaksızın kullanıcıları gözetlemek, haklarında veri toplamak ve üretmek ise olağan karşılanmaktadır. Fakat bu durum yalnızca etik çerçevede sorunlu değildir; aynı zamanda hukuken suçtur.

2018’de yürürlüğe giren KVK Kanununda çerezler ile ilgili doğrudan bir ifade geçmemesine rağmen kanun çerezleri kapsamaktadır. Çünkü çerezlerle kişisel bilgi işlenmektedir. Bundan öte, TCK’nın 135. maddesinde *”hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.”* cümlesi yer almaktadır. Hatta TCK’nın 243. maddesindeki *”Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adli para cezası verilir.”* ifadesi de çerezlerin yerleştirilmesi, cihazda kalması ve çerezin sahibiyle iletişime geçmesi süreciyle doğrudan bağlantılıdır. Diğer bir ifadeyle, KVKK olmasa bile TCK kapsamında kişiden habersiz onu izlemek, cihazına çerez yerleştirmek, hakkında veri toplamak ve bu verilerden

anlam çıkarmak suçtur. Tüm bu gerçekler göz önünde bulundurulduğunda olması gereken sistemlerin hukuka uygun bir şekilde işlemesi gerektiğidir. Nicel ve nitel araştırma bulguları ise bunun tam tersini ortaya koymaktadır.

Reklamcı Rory Sutherland 2009 yılında yaptığı bir Ted konuşmasında şöyle der: *“bir şey korunmaya layıkça çalınmaya da layıktır.”*³³ Kişisel veriler yasalarca koruma altına alınmaya çalışılırken, onu “ele geçirmeye” çalışanlar da daima olmaktadır. Fakat kişisel verilerin korunması gerektiği yasalar tarafından düzenlenmişken yasalar pratikte uygulanmaz ise “korunmaya layık veriler” bir yaptırımla karşılaşmaz; basitçe sermaye odaklarının insafına terk edilebilir hâle gelir. Karar alıcılar ve karar vericilerin konu hakkındaki bilgisizliği veya aldırışsızlığı nicel araştırmada karşımıza çıkan üçüncü taraf çerezlerin hiçbir izin almadan kullanıcıların cihazlarına yerleştirilmesine cesaret vermektedir. KVKK, üç yıldır; TCK’nın ilgili maddeleri uzun süredir yürürlüktedir. Üçüncü taraf çerezleri yerleştirmek için kullanıcının rızasını alma gereği bile duymayan platformlar ve çerezler aracılığıyla veri toplayarak onları yurt dışındaki kendi sunucularına aktaran şirketler herhangi bir yaptırımla karşılaşmamaktadır. Türkiye’de bu çerçevede yalnızca Amazon Türkiye benzer bir durumdan ceza almıştır. Karar özeti incelendiğinde aynı problemlere sahip diğer platform ve şirketlerin de ceza alması gerektiği görülmektedir. Şu ana kadar herhangi bir işlem gerçekleştirilmemiştir.

Karar alıcı veya vericilerin konu hakkında yeterince bilgisinin olmaması veya gözetimi ve doğurduğu sorunları ciddiye almamaları yasaların uygulamasını kısıtlamaktadır. Kişisel verilerin korunmasına yönelik yasaların uygulandığı durumlarda ise verilen cezalar caydırıcı bir özelliğe sahip değildir. Hatta öyle ki bazı şirketler ceza ödemeyi kabul ederek KVK Kurumunun talep ettiği düzeltmeleri yapmamakta ısrarcı bile olabilmektedir. Böyle bir durumda cezalar öneri gibi bir nitelik taşımaktadır. Yasalara uymayan çevrim içi platformlar ve şirketler ya yukarıda belirtildiği gibi hiç ceza almamakta ya da cüzi miktarlarda ceza almaktadır.

³³ https://www.ted.com/talks/rory_sutherland_life_lessons_from_an_ad_man/transcript?language=tr

Türkiye’deki çevrim içi platformlarda üçüncü taraf izlemeler ve açık rıza arasındaki ilişkinin oldukça sorunlu olduğu görülmektedir. GDPR’a tabi Avrupa ülkeleri bu konuda nispeten daha iyi olsa da mevcut durum Türkiye’den pek farklı değildir. KVKK’nın üst limit cezası 2 milyon TL’ye yakınken, GDPR’da ise bu ceza 20 milyon euro veya şirketin küresel cirosunun %4’ü kadardır. GDPR kapsamında verilen en yüksek cezalar olarak Amazon 746 milyon euro, WhatsApp 225 milyon euro, Google 50 milyon euro, H&M 35 milyon euro şeklinde karşımıza çıkmaktadır (Tessian, 2021). Fransa Veri Koruma Kurumu (CNIL), Google ve Amazon’a kullanıcıların açık rızasını almadan çerez yerleştirdikleri gerekçesiyle toplam 100 milyon euro ceza vermiştir (Lomas, 2020). Türkiye’de ise Amazon kişisel verilerin korunmasına yönelik muhtelif ihlallerden dolayı 1,2 milyon TL ceza almıştır.

GDPR’da maddi cezaların caydırıcılık gücü yüksek olsa da tabanda üçüncü tarafların kullanıcı gözetiminin nadiren azaldığı görülmektedir. 2018 yılında vpnMentor’un yaptığı bir araştırmada GDPR’a tabi Avrupa ülkelerindeki web sitelerinin yalnızca %34’ünün yasalara uygun olduğu tespit edilmiştir (vpnMentor, 2018). Trevisan vd. (2019), Avrupa’da yer alan web sitelerinin neredeyse yarısının kullanıcının rızasını almadan cihazlarına çerez yerleştirdiklerini ortaya koymuştur. Matte vd. (2020), inceledikleri binden fazla web sitesinin %54’ünde GDPR kapsamında en az bir ihlal yaptığını belirtmişlerdir. Nouwens vd. (2020), Birleşik Krallık’ta en çok ziyaret edilen siteleri taramış ve yaklaşık %90’ının GDPR kapsamındaki minimum gereksinimleri karşılamadığını açıklamışlardır.

Teknolojik gelişmeleri takiben hazırlanan yasal düzenlemeler kişisel verileri “korunması gereken” bir değer olarak görmektedir. Teknoloji şirketlerinin gözetimi, web’in en ücra köşelerinde bile kullanıcının karşısına çıkmakta ve korunmak istenen değere habersizce el koymaya çalışmaktadır. Yasaların bu el koymayı sınırlandıracak maddelere sahip olduğu görülmektedir. Fakat yasaların uygulanmasındaki aksaklıklar kullanıcıların derinlemesine gözetlenmesini azaltmada bir engel oluşturmaktadır.

AS7: Çevrim içi reklam endüstrisinde gözetim faaliyetleri nasıl ele alınmaktadır?

Gözetim kapitalizminin doğmasına önayak olan ve bugün veri toplamanın bir mazereti hâline getirilen çevrim içi reklamcılık, küresel çapta 500 milyar dolara yaklaşan reklam harcamaları ile çok farklı aktörlerin yer aldığı devasa bir sektördür. Sektörün bu denli büyümesinin altında yatan sebepler arasında internet kullanıcı sayısındaki artış, reklam gösterilen alan ve cihazların çeşitlenmesi, küçük ölçekli işletmelerin kolaylıkla reklam verebilmesi ve kişiselleştirilmiş reklam mantığı sayılabilmektedir. Reklam şirketleri çeşitli sitelerde reklam göstermek için o sitenin içine bir yazılım yerleştirir; o yazılım sayesinde siteyi ziyaret eden her bir kullanıcı kendisiyle ilgili olabilecek reklamlarla karşılaşır. Başka bir deyişle her kullanıcı, reklam şirketi onu nasıl tanıyorsa ona uygun reklam görür. Reklam şirketinin kullanıcıyı siteler arası, mobil uygulamalar arası, cihazlar arası gibi olabildiğince çok platformda takip etmesi onu daha iyi tanımasına vesile olacağı ve böylelikle de onun hakkında en alakalı reklamın gösterileceği varsayılmaktadır. Bu duruma eleştirel perspektiften yaklaşanlar genellikle gözetime maruz kalma, manipülasyon, güvenlik ve şeffaflık sorunları ve veri üzerinden sağlanan gelire odaklanmaktadır.

Yapılan mülakatlarda reklam üzerine çalışan katılımcılar insanların kendileriyle ilgili reklam görmesiyle ilgili bir problemlerinin olmadığını ifade etmektedirler. Fakat kullanıcıyla ilgili reklamların yapılma şeklinin hukuka uygun olarak gerçekleşmesi gerektiği vurgulanmaktadır. Reklamveren reklam verirken ödediği bedel karşılığında reklam alanı ve süre aldığını; fakat yayıncının ve reklam şirketinin meta olarak sattığı şeyin aslında kullanıcı verisi dile getirilmiştir. Kişiselleştirilmiş reklam, kullanıcının bir ağ deneyimi yaşarken karşılaştığı doğal akışın bir parçası olarak görülmektedir. Genel kanı, kişinin kendi bağlamıyla alakasız bir reklam görmesinin onu rahatsız edeceğidir. Katılımcı 4, dersine konuk olarak katılan bir reklam şirketi yöneticisinin “*web sitelerinde bazen karşınıza çıkan anket sorularını doğru cevaplayın ki sizin hakkınızda daha iyi bir bilgiye sahip olalım; erkeklere kadın pedi, kadınlara sakal tıraşı bıçağı reklamı göstermeyelim. Bu sizin faydanıza.*” dediğini aktarmıştır. Bu örnekteki yaklaşım, reklam tarafının hâkim bakış açısını anlamak bakımından oldukça değerlidir.

Çevrim içi reklam endüstrisinin kişiselleştirilmiş reklam yerine yalnızca site ve uygulamanın içeriğiyle bağlantılı bağlamsal reklam göstermesinin anlamsız olacağı görüşü hâkimdir. Kullanıcılar web siteleri ve uygulamalarda her hâlükarda reklam göreceği için alakalı reklamların gösterilmesi hem platforma hem de kullanıcıya avantaj sağlamaktadır. Yayıncılar, reklamverenler ve reklam şirketleri gösterdikleri reklamın performansını ölçebilir; kullanıcılar kendileriyle ilgili reklamlar görerek çeşitli fırsatlardan haberdar olabilir. Reklam endüstrisi açısından mevcut teknolojik gerçeklik ele alındığında veri toplamama gibi bir durum söz konusu dahi olamaz. Hem yayıncıların hem de reklam şirketlerinin birer şirket olduğu düşünüldüğünde varoluş amaçları olan maksimum gelir ile kâr elde etmelerini riske atacak hiçbir girişim içine girmeyeceklerdir.

Yasal düzenlemelerin ve çeşitli tarayıcıların gizlilik amaçlı güncellemelerinin reklam şirketlerini ve yayıncıları veri toplama faaliyetleri bakımından zora soktuğu düşünülmektedir. Katılımcılar genel olarak reklam şirketlerinin veri toplamak ve buna dayalı kişiselleştirilmiş reklam göstermek için yeni yollar üretmek üzerine çalıştığını belirtmektedir. Bu gelişmeler çerçevesinde kullanıcıların gözetlenmesi sonlanmayacak; sadece biçim değiştirerek farklı çözümler üretilerek farklı formatlarda devam edecek.

AS8: Gözetim ve mahremiyet arasındaki ilişki kişisel verilerin korunması ve kişisel veri farkındalığının artmasıyla nasıl bir değişime uğramaktadır?

Mahremiyet, yalnızca saklayacak bir şeyleri olan insanların talep ettiği bir şey olarak görülmemelidir. Mahremiyet insanın kendisi hakkındaki şeyleri kiminle paylaşıp paylaşmayacağına karar verebilmesiyle ilişkilidir. Bu şeyler illa ki gizli veya paylaşmaktan korkulan bilgiler olmak zorunda değildir. Oysaki mahremiyet tartışmalarındaki odağı insandan (yani kurbandan) alıp teknolojinin tasarım mantığına yerleştirirsek farklı bir bakış açısı geliştirilebilir. Teknoloji şirketleri varsayılan özellikleri neticesinde kullanıcı verisi toplar ve bunların kendi sunucularında “güvenle” saklandığını dile getirirler. Burada olması gereken verilerin güvenli olarak saklanması değil, kullanıcıların en başta gözetlenmemesidir. Bir çevrim içi platform eğer gizliliğe ve kullanıcı mahremiyetine önem verdiğini iddia ederek kullanıcıları

gözetlemeye devam ediyorsa burada mahremiyete verilen değerden söz etmek mümkün değildir. Gözetleme talebi ile mahremiyet hakkı arasındaki ilişki kimin, nereden ve nasıl baktığına göre değişebilmektedir. En geniş perspektiften ele alırsak mahremiyet hakkı, gözetleyenlerin topladıkları verileri anonim veya güvenli şekilde tutmalarıyla karşılanmaz; insanların en başta kiminle neyi paylaştığını kontrol edebilmesi ve bunun üzerinde hak sahibi olmasıyla elde edilir.

Gerek Türkiye'deki gerek Avrupa'daki yasal düzenlemeler şirketlerin yalnızca amaca uygun olarak ve kişinin açık rızasını alarak veri toplamasına; topladıkları veriyi ise güvenli şekilde saklaması gerektiğine vurgu yapmaktadır. Kullanılan tarayıcının ne olduğu, ziyaret edilen web sitesi, sitede geçirilen süre, cihazın ekran çözünürlüğü, işletim sistemi versiyonu, pil durumu vb. birçok veri bir araya getirildiğinde bir kişiyi belirleyebiliyorsa o zaman bunların hepsi için kişisel veri denilebilmektedir. Tüm bu veriler bir şirket tarafından gözetlenebiliyor ve toplanıyorsa, yasalara göre bunu yapmak için kişinin açık rızası alınmalı ve neden pil durumuna veya cihazın ekran çözünürlüğüne ihtiyacın olduğu beyan edilmelidir. Bu bilgiler ilk bakışta sıradan gelse de başka bilgilerle bir araya getirildiğinde kişi hakkında hassas bir veri ortaya çıkarılabilir. Dolayısıyla kanun, kişiyi ve kişinin mahremiyetini henüz gözetleme talebinin gerçekleşmesi aşamasında korumaktadır.

İnsan, iradesi yanıltılabilen bir varlıktır. Yasal düzenlemeler, yukarıda paylaşılan verileri veya kimlik numarası, cep telefon numarası gibi doğrudan kişiyi belirleyebilen kişisel verilerin önemini sıradan bir insanın bilemeyeceğini veya bilme bilincine sahip olamayacağını düşünerek kişisel verilerin korunması gerektiğini de söylemektedir. Bir kurum, kişinin açık rızasını alarak 20 TL karşılığında onların kimlik fotokopisini toplayabilir. Burada açık rıza bilinçli şekilde verilse bile kişinin o kimlik fotokopisiyle neler yapılabileceğine ilişkin bir farkındalığının olmaması, kişisel verilerinin korunması gerekliliğini doğurur. Yasalar, kişisel veri farkındalığına sahip olmayan veya iradesi kolaylıkla yanıltılabilen bireyleri de korumayı amaçlamaktadır.

Yasal düzenlemeler bireyin kişisel verilerini korumaya çalışırken bireylerin de kendi verileri üzerinde bir farkındalığa sahip olması beklenmektedir. Neredeyse herkes, kendisi hakkında bilmediği bir bilginin hiç tanımadığı biri tarafından biliniyor

oluşundan rahatsızlık duyabilir. Hatta çoğu insan, kimlerin sürekli onu gözetleyerek hakkında bilgi topladığını öğrendiğinde bunu büyük bir şaşkınlıkla ve öfkeyle karşılayabilir. Kişinin oturduğu apartmandan kaçta çıktığı, nereye gittiği, ne satın aldığı ve kaçta eve döndüğü gözcüler tarafından kayıt altına alınsa ve kimlerle paylaşıldığı bilinmese neredeyse kimse “umrumda değil” şeklinde bir tepki vermez. Fakat bu durum fiziksel bir alandan çevrim içi ortama taşındığında ise bir vurdumduymazlık ve tembellik ortaya çıkmaktadır. Mahremiyet, en çok da çevrim içi ortamda gereklidir. Fiziksel bir alanda yalnızca yapılanlar görünür; çevrim içi ortamda toplanan verilerden uçsuz bucaksız anlamlar çıkartılabilir. Analitik, reklam, veri ve teknoloji şirketleri bireyleri yaşı, cinsiyeti, ırkı, göz rengi, ruh hâli, ilgi alanları gibi binlerce nitelikle tanımlayabiliyorken tam da bu noktada mahremiyete, özel alanların varlığına, kişisel verilerin kontrolüne ve korunmasına ihtiyaç vardır.

Bireyler verilerinin durumunu sorguladıkları zaman karşılırlarına genellikle iki söylem çıkmaktadır: 1) madem verilerinin değerli olduğunu düşünüyorsun, o zaman mobil uygulamaları kullanma, siteleri gezme, sosyal medya platformlarının ücretsiz hizmetlerinden yararlanma. 2) şirketler senin verini ne yapsın? Bu söylemlerin görünürde “kurbanı suçlama” bakış açısından hiçbir farkı yoktur. Problemin çarpıtılması, kurbanın suçlanması ve gözetim kapitalizmine dayalı sermaye birikiminin perdelenmesi tam da burada başlamaktadır. Oysaki sistemin işleyişini ve hangi aktörlerin bu düzen içerisinde oyunun kurallarını belirlediğini ve ne tür sosyal sonuçlar doğurduklarını tespit edebilmek için problem kaynağına yönlendirilmelidir: 1) Neden uygulamalar, siteler, sosyal medya platformları beni gözetlemekten başka bir alternatif sunmuyor? 2) Verilerim madem değersiz o zaman neden hakkımdaki her şeyi öğrenmek için beni gözetliyorsunuz? Bu soruların cevabı gözetimin kimin çıkarına çalıştığıyla doğrudan ilintilidir. Tekelleşen, veri gözetimine dayalı bir sermaye birikim modelini benimseyen ve çoğunlukla şeffaf çalışma prensiplerini takip etmeyen şirketlerin domine ettiği sistemin getirdiği problemlerin bireylerin tercihleri ve sorunları olarak tartışılmasının önüne geçilerek asıl odak noktasının toplumsal öncelemeyen bu sermaye birikim mantığında aranmasında gerektiği vurgulanmalıdır. Veri farkındalığının oluşmasındaki ilk koşul bakış açısını değiştirmek ve kurbanın suçlanmasına bir son vermektir.

Teknolojinin tasarımı ve yarattığı sistemsel problemler, sözü edildiği gibi bireysel problemlermiş gibi yansıtılmaktadır. Başka bir deyişle, bireyin kendisi hakkında olan bilgileri kontrol etmek istemesi yalnızca azınlığa özgü bir talepmiş gibi davranılmaktadır. Hâlbuki özel hayata saygı ve mahremiyet hakkı insanın en temel hakları arasındadır. Mahremiyet, insanların kendi verileri hakkında bilgi sahibi olması ve değerinin farkına varmasıyla azınlığın talebi değil, çoğunluğun hakkı hâlini alacaktır. İnternetin nasıl kullanılması gerektiği, kişisel verinin ne olduğu, ne olabileceği ve neden korunması gerektiğine dair eğitimin, eğitim sistemi içine dâhil edilmesi gerekmektedir. Okul öncesi ve ilköğretim düzeyinde veri bilincinin geliştirilmesi verilen eğitimin bir parçası olabilir. Orta ve üstü yaştaki insanları verinin ne olduğunu bilmedikleri için suçlamak veya mahremiyet hakkını talep etmedikleri için yargılamak bizi “kurbanı suçlama” noktasına taşır. Bu yaştaki insanlara daha şeffaf yönerge ve kılavuzlar hazırlanarak yardımcı olunabilir. Eksik ve yanlış bir bilincin oluşturulması durumunda WhatsApp’ın popüler bir uygulama olduğu için gizlilik sözleşmesi değişiminin bir anda gündem olması, buna insanların tepki göstermesi fakat neye tepki gösterdiklerini doğru olarak bilmemesi gibi durumlarla karşılaşılır. Aynı zamanda tepkiler gündem olduğu hızda yine gündemden düşer. Bir kişinin çevrim içi günlük rutininde “WhatsApp” gibi yüzlerce uygulama ve web sitesiyle etkileşime girdiği ve bu platformların her birinin, az veya çok, kişinin bilgilerinin topladığı doğru şekilde anlatılmalıdır. Yasaların uygulanabilirliğindeki problemler aşıldığında ve toplumun kendisine ait olanı talep etme ve kontrol altında tutma bilinci oluştuğunda teknolojiler, insan haklarına ve mahremiyete saygı duyan güncellemeler ile kullanıcıların karşısına çıkmak zorunda kalacaktır.

AS9: Gözetim kapitalizmini etik hâle getirmek ne derece mümkündür? Sistemdeki değişiklikler, gözetim kapitalizminin olumsuz etkilediği alanların azaltılmasında bir rol oynayabilir mi?

Gözetim kapitalizmi, bireylerin günlük rutinlerinin takip edilmesi, onlar hakkında bilgi toplanması ve bu bilgilerin ürün hâline getirilerek satılabilir metalar hâline dönüşmesi sürecini anlatan bir yaklaşımdır. Bilgi toplama aşaması gözetime, bu ticari operasyonun zenginleşmeyi sağlaması kapitalizme vurgu yapmaktadır. Bireyler

eşsiz bilgilerin toplandığı hammadde kaynakları, metalar hammaddelerin işlenmesiyle ortaya çıkarılan ürünler, müşteriler ise bu ürünleri satın alan kuruluşlardır. Hammaddenin çıkarılması aşamasından satın almanın gerçekleştiği son aşamaya kadar gözetim kapitalizmi içindeki operasyonel süreçler şeffaflıktan uzaktır. Zuboff'un da değindiği gibi (2019: 11), gözetim kapitalistleri bireyler hakkında her şeyi bilirken bireyler gözetim kapitalistleri hakkında neredeyse hiçbir şey bilmezler. Tıpkı bu bilinmezlik gibi, ticari operasyonlar da bilinmeme üzerine tasarlanmıştır. Toplanan verilerle insanın geleceğini insan için değil, başkaların kazancını artırmak için öngörmektedirler. 21. yüzyılda kapitalist zenginlik ve gücün kaynağı üretim araçları sahipliğinden gözetleme temelli veri toplama, işleme ve öngörü ürünlerinin sahipliğine doğru geçiş yapmaktadır. Bu başlık kapitalizmin egemen türü hâline doğru yol alan gözetim kapitalizminin yarattığı temel problemlerden bazılarını irdeleyerek onun etik hâle gelip gelemeyeceği veya etik hâle gelmeyi isteyip istemeyeceğine cevap aramaktadır.

Gözetim kapitalizmine dair en büyük yanılsamalarından birisi gözetim kapitalizminin zorunlu ve alternatifsiz olduğu düşüncesidir. Gözetleme, teknolojinin çalışması için hayati öneme sahip bir özellik gibi sunulmaktadır. Gözetim kapitalizmini tek bir araca, platforma veya uygulamaya indirgemek mümkün değildir ama tüm bu teknolojilerin kazanç sağlamak için gözetlemeden başka bir seçenekleri yok gibi görülmektedir. Bu durumda sosyal bir varlık olarak teknolojileri kullanan bireyler bir yandan da gözetlenerek hammadde kaynağına dönüşmektedir. Hammaddenin toplanması ve işlenmesi ekseriyetle bireyden habersiz gerçekleşmektedir. Diğer yandan şunu söylemek mümkündür; bir kişi hangi şirketlerin kendisi hakkında neleri öngördüğüne dair hiçbir şey bilmemektedir. Bu bilinmezlik olgusu da tıpkı gözetlemenin tek yöntem olduğu gibi teknolojik gelişmelerin bir normudur. Gözetim kapitalizmi bireyi nesne olarak görür ve ona uygun davranır. Bireylerin kendi verilerini kendilerinin kontrol etmesi, kendi verileri üzerinde söz sahibi olması ve hakkında öngörülen durumlardan faydalanabilme imkânına kavuşması gözetim kapitalizminin olumsuz etkilerini azaltır mı? Kullanıcıların kendi verilerini kendi cihazında tutması, hangi verilerini kiminle paylaşabileceğini seçmesi ve algoritmaların bu verilerden kişiler hakkında çıkardığı öngörülerin bilinmesi

teknolojinin bireysel faydasını açığa çıkartır. Fakat bu sistem artık gözetim kapitalizmi olarak adlandırılmaz. Veriler bilinmeyen şirketlerin uzak sunucularında değil kullanıcıların cihazlarında olursa ve kontrolünü kullanıcılar sağlarsa bu insan haklarına uygun bir yöntem olur; dolayısıyla gözetim oyun dışı kalır. Kapitalizm ise kullanıcılar kontrol altında tuttukları verilerini satmak isterse sisteme tekrar dâhil olur. Fakat herkesin kendi verisini satacağı bir sistem hakikatin ortadan kaybolmasına, manipülasyona ve kapitalist sistemin sahip olduğu diğer sorunların açığa çıkmasına sebep olabilir. Ayrıca, “herkesin kendi verisini satabileceği” fikri gözetim kapitalistlerinin kendilerini temize çıkarmak ve insan haklarına duydukları saygının bir göstergesi olarak sunabilecekleri bir yöntem olarak bile piyasaya sunulabilir. Bu durum onların ticari operasyonlarını daha etik hâle getirdiklerinden ziyade yeni bir gelir kapısı oluşturdıklarına işaret eder.

Google ve Facebook hem silikon vadisinin hem de tüm dünyanın örnek aldığı en büyük teknoloji şirketleridir. Büyük olma özelliklerini yıllık cirolarına, ürün çeşitlerine, girişimlerine ve kullanıcı sayılarına bağlamak doğru olacaktır. Bu özelliklerin ilişki ağı bir bağlamda onları gözetim kapitalisti yapmaktadır. Sağladıkları çevrim içi hizmetlerin tamamı neredeyse ücretsizdir. Bu sayede milyarlarca kullanıcıyı barındırırlar. Bazı hizmetlerinin ücretli versiyonları da vardır. Ücretli hizmetlerinde reklam göstermemeyi taahhüt ederler. Fakat Google, Facebook ve benzer iş modellerine sahip şirketler, ücretli hizmet sağlasa bile kullanıcıları gözetlememeyi taahhüt etmez. Ücretli hizmetlerden toplanan gelir yalnızca istatistiksel bir sayıdır. Toplam gelirleri arasında yok denecek kadar azdır. Çünkü iş modelleri sağladıkları hizmeti satmak üzerine inşa edilmemiştir. Ücretsiz hizmet sağlamak gözetlemenin bir bahanesidir. Bu bahane sayesinde şirketler artı değer yaratır. Google, Facebook ve benzeri büyük şirketler hizmetleri için aylık/yıllık bir ücret talep etse gözetim kapitalizminin yarattığı sorunlarda azalma olur mu? Eğer olabildiğince veri toplama son bulacaksa ve hizmetlerin kişiselleştirilmesi için amaca uygun ve açık rızaya dayalı sınırlı bir veri toplama söz konusu olacaksa evet, bir nebze iyileşmeden söz edilebilir. Fakat böyle bir sistemin geliştirilmesi yalnızca bireyin yararına olacağı için pratiğe geçmesi oldukça zor görülmektedir. Bugün pratikte ücretli olan hizmetlerin birçoğunda “beni takip etme” gibi bir seçenek dahi yoktur. Örneğin, Netflix’in gizlilik

sözleşmesine bakıldığında bu durum görülebilmektedir. Üyelik bilgileri gibi platforma verilen bilgiler dışında Netflix, platformun kullanımına ilişkin otomatik olarak veri toplar. Aynı zamanda “iş ortaklarından” ve “diğer kaynaklarından” olarak tanımladığı bilinmeyen gruplardan kullanıcıyla ilişkili veri topladıklarını beyan etmektedirler. Yine sahip oldukları kullanıcı verilerini kim oldukları net olmayan üçüncü taraf şirketlerle “belirli amaçlar doğrultusunda” paylaştıklarını belirtmektedir.³⁴ Bireyler ücretini ödeyerek aldığı hizmetin kullanımını sırasında oluşturduğu istatistiki verileriyle birlikte kullanılan cihaz türü, ağ bağlantı türü, tarayıcı ve IP adresi gibi üst verileri Netflix’le paylaşmak zorunda kalmaktadır. Netflix üstelik bu bilgileri paydaşlarıyla paylaşabilmekte ve onlardan kişi hakkında bilgi toplayabilmektedir. Ücretli bir platformun kullanıcıya yalnızca “ne izlemek istediğini” gösterme niyetiyle böylesine büyük bir gözetim ağı kurması akıllarda soru işaret bırakmaktadır. Gözetim kapitalizmine bağlı tüm aktörler gözetim ağlarını genişletmeye ve gizlilik sözleşmelerinde ufak puntolarla belirttikleri “iş ortaklarıyla” veri alışverişi yapmaya devam ederken bu sistemin yarattığı sorunlarla ilgilenmedikleri düşünülmektedir. Çünkü onlara göre birey hizmeti satın alacak bir müşteri değildir; birer hammadde kaynağıdır. Bu denklemde onları rahatsız eden hiçbir durum yoktur.

AS10: Etik web’in oluşumunda hangi yolların izlenmesi gerekmektedir?

Etik web insan haklarına, deneyimine ve insanın emeğine saygı duyan; erişilebilirlik, şeffaflık, güvenlik ve gizlilik esaslarına dayalı sistemlerin yaratılmasıyla ilgilidir. Bu kapsamda bugünkü web’in etik olduğunu söylemek pek mümkün değildir. Çalışmanın literatüründe paylaşılan bilgilere, çalışmanın nicel ve nitel araştırma bulgularına bakıldığında mevcut tablonun etik açıdan sorunlu olduğu görülmektedir. Çevrim içi hizmet sağlayan şirketlerin gözetime dayalı iş modelleri, teknolojinin egemen üretim ve gelir mantığı, tekelleşen sosyal medya şirketleri, algoritmalar ve kişisel verilerin sahipliği göz önünde bulundurulduğunda web’in sorunlu alanları karşımıza çıkmaktadır. Maslow’un ihtiyaçlar hiyerarşisini, web’in ihtiyaçlar hiyerarşisine doğru evirdiğimizde en temel ihtiyacın etik olduğunu söyleyebiliriz. Temelinde etik prensiplerin yer almadığı bir web anlayışı, sonraki katmanlarda yer

³⁴ <https://help.netflix.com/tr/legal/privacy>, 1 Ocak 2022 Tarihli Gizlilik Bildirimi.

alacak ihtiyaçların anlamını yitirmesine sebebiyet verebilir. Bu durum, örneğin, Mark Zuckerberg'in "*Future is Private*" yaklaşımı ile geleceğin gizlilik olduğunu söylemesi gibi bir ironi barındırır. Etik prensiplere bağlı olmayıp gizliliğe önem verdiğini söylemek yanılsamadan ibarettir. Çevrim içi platformlar etik bir temel üzerine inşa edilmeli ve bu temel üzerinde ürün veya hizmetlerini sağlamalıdır.

W3C, internetin son kullanıcılar için olduğunu ve kullanıcı ihtiyaçlarının öncelikli olarak karşılanması gerektiğini belirtir. Burada ifade edilen son kullanıcı mutlaka homojen bir gruba atıfta bulunmak için kullanılmamıştır; son kullanıcı, interneti çeşitli amaçlar doğrultusunda kullanan kişilerdir. Web'te gezinen, oyun oynayan, video konferans yapan, mesajlaşan kısacası çevrim içi bir aktivitede bulunan herkes son kullanıcıdır (Nottingham, 2020). Son kullanıcı, platformlarla girdiği etkileşim sırasında hem madden hem de manen zarar görmemelidir. Etik platformlar geliştirmek hem kullanıcıların ihtiyaçlarını sağlamak hem de çeşitli ihlaller neticesinde zarar görmelerini engellemek bakımından gereklidir.

Etik web'in inşasına en alt kademeden başlanıldığında etik web tasarım ve geliştirme karşımıza çıkmaktadır. Avrupa Dijital Hakları Ağı'nın (EDRi) *Etik Web Sitesi Geliştirme ve Bakım Kılavuzu* değerli bilgiler paylaşmaktadır. Bu kılavuzda yazılım geliştiricilerin üçüncü taraflara bağlılığını olabildiğince azaltmaları gerektiği özellikle belirtilmektedir. Örneğin, bir web sitesi Google Fonts üzerinden bir yazı karakteri çağırdığında site artık üçüncü taraf yazılım kullanmaya başlamış bulunur. Hem etik hem de kişisel verilerin korunması kapsamında söz konusu site Google Fonts'u aktif hâle getirmeden önce onun açık rızasını almak zorundadır. Oysaki yazı karakterini kendi sunucusunda barındırsa ve web sitesinde kendi sunucusu üzerinden çalıştırsa ne yasal ne de etik olarak hiçbir sorun ortaya çıkmayacaktır. Bu nedenle geliştiricilerin kullandıkları ürünleri olabildiğince kendi sunucusunda tutması etik çerçevede gerekli bir adımdır.

Etik web için çözüm yolları aranırken tasarım aşamasında da dikkat edilmesi gereken hususlar vardır. Tasarım, hizmeti sunan grupla kullanıcının ihtiyaçlarını eşitlemek için bir çözüm vadetmektedir. Etik tasarım anlayışı bu ihtiyaçların bir tarafta baskın olmamasını gerektirir. Kişiyi istenen davranışa yönlendirici ve kasıt içeren

yanıltıcı tasarım desenleri web'in etik açıdan sorunlu yanlarından birisidir. Bu tasarım desenleri genellikle bir şeyleri satmak için kişinin bilinçaltını kışkırtan ve özgür iradesini yanıltmaya çalışan renkler ve içeriklerden oluşur. Ayrıca birçok site çerezleri aktif hâle getirmek için kullanıcıya sunulan çerez bildirim kutularında yanıltıcı tasarım mantığını kullanmaktadır. Bu mantık genellikle “kabul et” butonunun mavi renk ve büyük; “reddet” butonunun silik bir renkte ve daha küçük olarak tasarlanmasıyla kendini gösterir. Hatta metin olarak ele alındığında bazı bildirimlerde evet seçeneği “Evet, Teşekkürler”, hayır seçeneği ise “Daha Sonra” olarak yer alır. Diğer ifadeyle, “hayır” bir seçenek değildir; “evet” diyene kadar yalnızca bir erteleme vardır. Web, özgür düşünceyi vadeder. Platformlar düşüncelerin özgürce dile getirildiği ortamlar olarak kendilerini tanımlıyorlarsa, kullanıcılara sundukları seçeneklerin de ifade özgürlüğünü zedelememesi gerekir. Bu gibi pratikte aksaklık yaratan sorunlar etik web tasarımının geliştirilmesinin önündeki engellerdir. Sonuç olarak, üçüncü taraf yazılımların ve kullanıcıyı istenen davranışa yönlendirici, manipülatif tasarım ve uygulamaların web tasarımı, yazılımı ve mobil uygulama geliştirme süreçlerinde yer almaması etik web'in inşasında önemli bir adım olacaktır.

Yasal düzenlemelere uygun sistemler geliştirildiğinde etik kaygıların belirli bir kısmı giderilmektedir. Bu bakımdan yasal düzenlemeler etik web'in inşası için önemli bir yere sahiptir. Hukukun uygulanabilirliği sağlandığında, amaca hizmet edecek şekilde ve açık rızaya dayalı olarak kişisel verilerin toplanması, saklanması ve gerektiğinde silinmesinin talep edilmesi ile web'in etik bakımdan iyileşmesi sağlanabilir. Fakat bu iyileşmenin gerçekleşmesinin tek koşulu web sitesi veya uygulamanın yalnızca hizmetlerini iyileştirmesi ve buna bağlı sınırlı bir veri toplaması ile gerçekleşebilir. Bu kapsamda da analitik amacıyla veri toplayacağı için kişinin açık rızasını alarak amaç dâhilinde veri toplamalıdır. İş modelinin koşulsuz şartsız gözetleme üzerine inşa edildiği bugünkü gibi bir sistemde, yasalar doğru uygulansa bile etik sorunların tamamı giderilmez. Bunun başlıca nedeni, gözetimin yasalarda bir açık bularak yoluna devam etme niyeti içinde olmasıdır. Birçok reklam ve analitik şirketi, kullanıcıların açık rızasını almadan onları nasıl takip edebilecekleri üzerine

çalışmalar gerçekleştirmektedir³⁵. Yasal düzenlemelerin etrafından dolaşabilecek alternatif gözetim fikirlerinin üretilmesi mevcut yasaların aşılmasına yardımcı olurken etik sorunların daha da büyümesine sebep olmaktadır. Gözetimin bu girişimleri gerektirecek kârlı bir iş olması, kişiselleştirilmiş hizmetlerin veya reklamların yalnızca son kullanıcının ihtiyacını karşıladığı yaklaşımla çelişmektedir. Etik teknoloji olabildiğince her şeyin her an amaçsızca gözetlenmesi ve bunu arka kapılar oluşturarak gerçekleştirmesi anlamına gelmemelidir. Yasal düzenlemelere bağlı olarak hukuk uygulayıcıları gözetleyenlerin kanunları aşma girişimlerini tespit ederek yaptırım kararları alabilirse etik web için kıymetli bir adım atılmış olur.

Etik bir web için yasalar, kapsamlı ve uygulanabilir olmalı; fakat bu yasalar dağınık olmamalıdır. Bugün dünya ülkelerinin %69'unda gizlilik ve veri koruma üzerine yasal düzenleme vardır. %10'unda ise düzenlemeler taslak aşamasındadır. Benzer amaçları taşıyan fakat farklı ülkelere ait farklı yasal düzenlemeler yerine uluslararası bir sözleşme ile veri ve gizliliğin korunması sağlanmalıdır. Web'in olağan bir özelliği, tüm toplumlar için olması ve ulusal sınırları aşmasıdır. Tıpkı insan hakları sözleşmesi gibi ulus üstü bir düzenleme ve karşılaşılan tüm problemlerin o çerçevede ele alınması eşitliğin ve adaletin sağlanması ve hukunun uygulanması açısından etik bir web'e katkı sağlayacaktır. Gün içinde ağı bağlı kalınan zamanın her yıl arttığı bir dönemde böyle bir uluslararası düzenlemenin olmayışı büyük bir eksiktir.

Mevcut teknolojinin gözetime bağlı geliştirilen iş modelleri, bireyi hizmetten faydalanan konumundan alarak, hizmetin bir parçası konumuna taşımaktadır. Yani platformlarla girilen etkileşimde birey, bir hizmetten faydalanırken aslında başka şirketlere de hizmet sağlamaktadır. Bu iş yapış biçiminde kullanıcı bir hammadde kaynağı olarak görülerek farklı gruplara sunulan asıl ürün veya hizmetin bir parçası hâlini almaktadır. Bir teknolojiyi toplum yararını gözetken ve etik olarak değerlendirebilmenin bir koşulu sağladığı hizmetin kimin çıkarına olduğunu tespit etmektir. Bireyin hizmetin bir parçası olduğu denklemde sistemin teknolojiyi elinde tutan, veriye sahip olan ve onu kontrol eden grupların çıkarına işlediğini söylemek

³⁵ Bkz.: 2.1.1.3. Çerezsiz Dünya ve İzleme Teknolojilerinin Geleceği.

mümkündür. Birey için üretilen teknoloji birey için bireyin çıkarına çalışmalıdır. Etik web platformları ve teknolojiler kullanıcının ürettiği verinin kontrolünü yine kullanıcıya vermelidir. Büyük şirketler hâlâ teknolojiler üretebilir, satabilir; bir işletme olmanın doğası gereği bu süreçten kâr elde edebilir. Fakat bireyi bir hizmetin parçası olmaktan sıyırmak gerekmektedir. Kişisel veriler, etkileşime girilen platformlar ve onların kullanıcıyı görmesine izin verdiği üçüncü taraf şirketlerin sunucularında değil kişinin cihazında kalmalıdır. Bu veriler kişinin geleceğini öngörmek isteyen gruplara değil bizzat kişilere hizmet etmelidir. Verilerin yönetimi ve kontrolü söz konusu grupların inisiyatifine kalmamalıdır. Etik web, bireyin yalnızca hizmetten faydalandığını düşündüğü ve verileri hakkında bilincinin olmadığı durumlarda onun tarafında yer almalı ve onu korumalıdır.

Web'in kurucu değerleri arasında web teknolojisi ve platformların çoklu yapılarda çalışabilmesi yer almaktadır. Web platformları, yalnızca tek bir tarayıcıda veya tek bir cihazda çalışır şekilde tasarlanmamalıdır. Bugün geline nokta tekelleşme ve bunun getirdiği sorunlar vardır. Google, Facebook ve Amazon gibi şirketler gerek ürün ve hizmet ağını genişleterek, gerekse büyüme potansiyeli olan girişimleri bünyesine katma yoluyla web ortamında büyük tekeller hâline gelmektedir. Örneğin, Netflix, Zoom, Adobe, Reddit, Tiktok, Etsy gibi popüler site ve uygulamalar Amazon'a ait olan web sunucuları (AWS) içinde barınmaktadır. Ek olarak, dünyada en çok ziyaret edilen ilk on bin sitenin %56'sının sunucuları Amazon'da yer almaktadır³⁶. Amazon'un sunucularında gerçekleşecek bir problem web'in işleyişinde büyük bir aksaklığa neden olacaktır. Tekelleşmeye bir başka örnek Instagram üzerinden verilebilir. Instagram uygulamasında bir web sitesi bağlantısına tıklanıldığında, o siteye ziyaret cihazdaki Safari, Opera vb. bir tarayıcı aracılığıyla değil uygulamanın kendi tarayıcısıyla (in App-Browser) gerçekleşmektedir. Yani başka bir web sitesinin görüntülenmesi hâlen Instagram içerisinde gerçekleşmektedir. Aynı özellik Facebook uygulamasında da mevcuttur. Böylelikle uygulama içi tarayıcı ile platformlar kullanıcının uygulamadan ayrılmasını engeller ve ziyaret ettiği web sitesiyle girdiği etkileşimi gözetleyebilir. Tekelleşmenin yansımaları bu alanlarda

³⁶ <https://trends.builtwith.com/hosting/Amazon>, Ocak 2022.

kendini göstermektedir. Söz konusu tekelleşme merkezîleşmeyi beraberinde getirmektedir. İnternetin ortaya çıkışı merkezîyeti ortadan kaldırma girişimlerinin bir sonucuyken gelineen noktada yeniden bir merkezîleşme söz konusudur. Merkezîleşme, web'i daha etik hâle getirme çabalarının karşısındadır. Web'in tüm parçaları belirli bir azınlığa bağlı olarak çalışmaktadır ve onlara bağlı olma durumu azatılmalıdır. Web, büyük kümelerden oluşan azınlık sistemlerin yerine küçük kümelerden oluşan binlerce kümeden oluşmalıdır. Merkezîyetsiz bir web, etik web için olmazsa olmazdır.

Algoritmalar, algoritmaların sahipliği, çalışma prensipleri, şeffaflık sorunları ve kimin çıkarı için çalıştığı web'in etik sorunları arasında yer almaktadır. Bugün veriler, gözetleyenlerin uzak sunucularında toplanıyor, onların oluşturduğu algoritmalar ile işleniyor ve istenen sonuç bu şekilde elde ediliyor. Algoritmalar, e-ticaret sitelerindeki ürün önerileri, Twitter ve Facebook gibi platformların haber akışları, kişiselleştirilmiş reklam gösterimleri ve kişi hakkındaki öngörülerin oluşturulması gibi birçok alanda faaliyet göstermektedir. Bu faaliyetlerin temelde hepsi kullanıcının çıkarına değil platformun çıkarına dayalı olarak gerçekleşmektedir. Alakalı ürünlerin gösterimi satın alma ihtimalini, kişiselleştirilmiş reklam tıklanma ihtimalini, haber akışlarını kişiselleştirme platformda bulunulan süreyi artırmayı amaçlamaktadır. Algoritmalar, şirketlerin çıkarları doğrultusunda onların kârlarını maksimize etmeye yönelik çalışmaktadır. Algoritmaların nasıl çalıştığında dair kullanıcılara şeffaf bir bilgilendirme yapmak zorunludur. Bugün Google gibi çeşitli platformlarda genelgeçer şeffaflık söz konusudur. Araştırmanın nicel bulgularında yer alan reklam ve analitik şirketlerinin ise algoritmaları hakkında hiçbir şeffaf bilgi söz konusu değildir. Öte yandan veriyi üreten bireylerin, algoritmaların onlar hakkındaki öngörülerinden faydalanabilme imkânına sahip olması gerekmektedir. Kişinin kalp krizi geçirme ihtimali bir öngörü ürünü olarak uzak sunucularda tutuluyorsa ve bu ihtimal sigorta şirketlerine, bankalara veya reklamverenlere satılabilir bir meta olarak değerlendiriliyorsa teknolojinin toplumsal fayda sağlaması söz konusu değildir. Verilerin, bireylerin cihazlarında tutulması ve kontrolünün bireylerde olması etik web için ne kadar gerekliyse, algoritmaların da bireylerin çıkarı için çalışması bir o kadar gereklidir. Bireyin algoritmalarından sağladığı çıkar yalnızca bireyin isteyebileceğinin düşünüldüğü ürünleri ona göstermek veya sık görüştüğü arkadaşlarının gönderilerini

haber akışlarında üst sıralarda göstermek değildir. Verileri üzerinden öngörülen potansiyel tehdit ve fırsatlardan haberdar olmasıdır. Fakat teknolojiye kimin çıkar sağladığı göz önüne alındığında teknoloji sahiplerinden toplumsal fayda beklemek kölelerin köle tüccarlarından özgürlük beklemesi gibidir. Yine de, etik bir web için algoritmaların şeffaf olması, toplumsal ve bireysel fayda sağlaması ve kontrolünün kullanıcıda olması gerektiği söylenmelidir.

Web'e bağlı platformları ele aldığımızda bugün teknoloji sahipliğinin kullanıcı verisi toplayan aktörlerin elinde olduğu görülmektedir. Tekelleşme ve iş modelinin veriye dayandığı bir sistemle web, kuruluşundaki temel etik ilkelerin terkedildiği bir ortama dönüşmüştür. Bu dönüşüm; insanların hiçbir üçüncü grubun çıkarına dayalı olmadan özgürce yürüyebildiği, spor yapabildiği, nefes alabildiği, çocuklarıyla vakit geçirebildiği alanların yıkılarak alışveriş merkezlerinin inşa edilmesine benzemektedir. İnsanlar alışveriş merkezlerinde yine de çocuklarını eğlendirecek aktivitelerde bulunabilir veya banklarda oturarak soluklanabilir. Fakat alışveriş merkezleri insanların çeşitli aktivitelerden faydalanması için inşa edilmemiştir. Dolayısıyla AVM'lerin sağladığı hizmetler bir çıkara dayalıdır ve o çıkar kişiye sağlayacağı faydaya bağlı olarak oluşturulmamıştır. Web'in diğer tüm problemlerini de içine alan çerçeve bir problem şudur: bugün web'te parklar yoktur. Neredeyse tüm alanlar gözetleme altındadır ve her köşe başında AVM'ler yer almaktadır. Yalnızca insanın çıkarını gözetten alanlar yok edilmiştir. Web'in bugün parklara ihtiyacı vardır. Etik web anlayışı, ağların yalnızca AVM'lerden oluşmadığı, parkların da sayıca onlar kadar olduğu bir web'e ihtiyaç olduğunu vurgulamaktadır. Parkların inşasının inisiyatifi gözetim kapitalistlerine bırakılmamalıdır; zira onlar zaten parkları AVM hâline getirmişlerdir. Onların inşa edecekleri parklar ile inşa ettikleri AVM arasındaki fark, McDonalds ile Burger King arasındaki farkla aynı olacaktır. Seçenekler değil alternatifler üretilmelidir. Web aracılığıyla iletişim bir lüks olmaktan çıkıp bir ihtiyaç hâline gelmişken parkların inşası da lüks bir talep değildir. Bireysel çabalarla bu alanlar inşa edilebilir. Sivil toplum kuruluşları parkların geliştirilmesine bütçe ayırabilir. Ya da toplanan vergilerin bir kısmı nasıl toplum için harcanıyorsa, aynı şekilde bu parkların oluşturulmasındaki yatırımcı problemi bu şekilde aşılabılır. Bugünkü teknolojik gelişmişlik seviyesi, hepsinin altından kalkabilecek güce sahiptir.

Onu nasıl kullandığımız, ondan nasıl faydalandığımız ve onun kimin çıkarına çalıştığını üzerine bir sorgulamaya ve çözüm üretimine ihtiyaç vardır. Etik web'in park ideali, egemen kapitalist sistemin zihinlerimizde oluşturduğu referans çerçevesinden uzaklaşıldığı anda gerçekleşmesi zor bir ihtimal olarak görülmemelidir. Web'in bir sahibi yoktur. Web'in mucidi milyarder değildir. Web'i para kazanmak için icat etmemiştir. Web, tüm toplumlar içindir ve tüm toplumların web üzerinde parklara ihtiyacı vardır.



SONUÇ

Gözetim olgusunun geçmişi izleme, kaydetme ve denetleme çerçevesinde milattan öncesine kadar dayandırılmaktadır. Öte yandan içinde bulunduğumuz yüzyılda bu faaliyetlerin servet birikimi sağlamadaki konumu tarihte hiç olmadığı kadar merkezî bir yerdedir. Gözetim kapitalizmi tam da bu şartlar altında, dijitalleşmenin hızlanmasıyla hacmi muazzam bir biçimde büyüyen yeni bir çehre olarak ortaya çıkmıştır. 11 Eylül saldırıları sonrası, Ağustos 2002’de, bireysel veri bankası kontrol programı olan TIA (Temel Bilgi Farkındalığı) programının sunuculuğunu yapan John Poindexter, sistemi anlatırken “*Teröristlerin tespit edilmesi, sınıflandırılması, tanımlanması ve takip edilmesi gerekir, böylece onların planlarını anlayabilir ve bu planları gerçekleştirmelerine engel olabiliriz.*” ifadelerini kullanmıştır (Mattelart, 2012:217). Bu program gelen tepkiler üzerine ilerleyen zamanlarda rafa kaldırıldıysa da bu mantığın gözetim kapitalizminin gelişmesine ve yaygınlaşmasına ilham verdiği söylenebilmektedir. Bireyleri tespit etme, sınıflama, tanımlama, takip etme ve geleceğini öngörme yaklaşımı teknoloji şirketlerinin ve web platformlarının varsayılan iş modeline dönüşmüştür. Bu sistemde bireylerin iletişimsel faaliyetleri ve deneyimleri “*ücretsiz hammadde*” olarak kabul edilir ve bu hammaddeler işlenerek öngörü ürünleri hâline getirilir. Sosyal medya platformlarının, teknoloji şirketlerinin ve web platformlarının her yıl artan gelirlerinin kaydadeğer bir bölümünde öngörü ürünlerinin payı vardır. Bireyler gözetim kapitalizminin çalışma prensibine ilişkin neredeyse hiçbir bilgiye sahip değildir. Gözetleyen aktörlerin bilinmezliği, gözetim kapitalizminde işlerin başarılı bir şekilde yürümesini sağlamaktadır. Gözetleyenler bireyler hakkında her şeyi bilirken, bireyler gözetleyenler hakkında hiçbir şey bilmemektedir.

Bu çalışma iki ana amaç üzerine inşa edilmiştir. İlk olarak gözetim kapitalizmine ait aktörlerin kimler olduğunu ve hangi amaçlarla veri topladıklarını belirli bir örneklem dâhilinde ortaya çıkarmaktır. Böylelikle gözetim kapitalizminin bilinmezliği kısmen de olsa azaltılmıştır. İkinci amaç, gözetim kapitalizmi sistemini daha geniş bir perspektifle ele alarak ona ait ve onun neden olduğu sorunları irdelemek

ve sonucunda etik bir web'in nasıl oluşturulabileceği üzerine bir tartışma başlatmaktadır. Çalışmada bu amaçlara hizmet eden on araştırma sorusuna cevap aranmıştır.

İlk araştırma sorusu gözetleyen aktörlerin kimler olduğunu ortaya çıkarma amacı taşımıştır. Bir web sitesi ve mobil uygulamadaki üçüncü taraf olarak kullanıcı verilerini toplayan şirket ve platformlar ortaya çıkarılmıştır. Öncelikle, araştırma kapsamında taranan web sitelerin %79'unda, mobil uygulamaların %76'sında üçüncü taraf izleyiciler tespit edilmiştir. Söz konusu web sitelerinde 112 farklı şirkete ait izleyici olduğu görülmüştür. En çok izleme teknolojisine (çerez, piksel vb.) sahip şirketler çoktan aza doğru Google, Criteo, Taboola, Moat, Facebook, Gemius, Amazon, DailyMotion, Insider, Pubmatic, Rubicon Project, Twitter, Adform, AppNexus ve The Trade Desk şeklinde sıralanmaktadır. Üçüncü taraf izleyicilere sahip web sitelerinin %29'unun toplam 100 ve üzeri izleyiciye sahip olduğu belirlenmiştir (Her bir şirkete ait birden fazla izleyici olabilir). İncelenen 72 mobil uygulamada 84 farklı izleyicinin 387 kere kullanıldığı görülmüştür. Uygulamaların üçüncü taraf olarak en çok yer verdiği izleyiciler sırasıyla Google FireBase Analytics, Google CrashLytics, Google AdMob, Adjust, Facebook Login, Facebook Share, Facebook Analytics, Huawei MSC, Google Tag Manager, AppsFlyer, Facebook Ads, New Relic, AltBeacon, AppLovin, Insider ve Moat'tır. İncelenenler arasında en çok üçüncü taraf izleyiciye sahip mobil uygulamalar sırasıyla Maçkolik, Count Masters Crowd Runner 3D, LetGo, 101 Okey Plus, Çiçek Sepeti, Trendyol, Yemeksepeti ve PUBG Mobile adlı uygulamalardır.

İkinci araştırma sorusu gözetleme araçlarının verilerin toplanmasındaki rolünü sorgulamaktadır. Araştırmada üçüncü taraf olarak ortaya konulan şirketlere bakıldığında bunların sosyal medya platformları, reklam teknoloji şirketleri, analitik şirketleri, performans ölçüm şirketleri gibi alanlara ait şirketler oldukları görülmektedir. Her üçüncü taraf şirket öncelikle yer aldıkları site ve uygulamalara hizmetler sunmakta, kullanıcılar hakkında veri toplamakta ve var olan verilerle birleştirerek kişiselleştirilmiş reklam gösterimi sağlamaktadır. Birçoğu farklı sitelerde ve uygulamalarda yer alan izleyicileri sayesinde kullanıcıları takip ederek onlar hakkında detaylı profiller oluşturmaktadır. Örneğin, reklam şirketi Taboola; Hürriyet,

Milliyet, İnternethaber, NTV, Cimri, Nefis Yemek Tarifleri, Nesine, Mynet ve Onedio web sitelerinde üçüncü taraf izleyici kodlarına sahiptir. Bir kişi bu web sitelerini ziyaret ettiğinde ve sayfalarda çeşitli etkileşimlerde bulunduğunda Taboola bu ziyaretlerin aynı kişi tarafından yapıldığını bilir. Bu erişim neticesinde her bir sayfa etkileşime istinaden kişi hakkında detaylı bir profil oluşturulmaya başlanır. Farklı site ve platformlarda bulunan üçüncü taraf şirketlerin gözetleme araçları verilerin toplanması, tanımlanması ve eşleştirilmesinde önemli bir rol oynamaktadır.

Üçüncü araştırma sorusu web sitelerinin üçüncü taraf aktörlerin izleyicilerini kullanmak için hem etik hem de yasal olarak kullanıcılardan izin alıp almadığının cevabını aramaktadır. Araştırmada incelenen tüm sitelerin çerez bildirimine ve açık rızaya ilişkin yaklaşımları şu şekilde çıkmıştır. Sitelerin %46'sında çerezlerin kullanımıyla ilgili hiçbir bildirimle karşılaşılmamıştır. %25'inde yalnızca çerez kullanıldığınına ilişkin bir bildirim yapılmıştır. %21'inde çerez kullanıldığınına ilişkin bir bildirim yapılmış ve yalnızca kullanıcının kabul etmesine yönelik bir buton sunulmuştur. %8'inde ise çerez kullanımına ilişkin bir bildirim, kabul et butonu ve çerezleri özelleştirme (aktif veya pasif yapma seçeneği) geldiği görülmüştür. Hiçbir sitede doğrudan çerezleri reddetmek için bir buton olmadığı tespit edilmiştir. Web sitelerinin kullanıcıların açık rızasını alarak çerez yerleştirme durumundan oldukça uzak olduğu gözlemlenmiştir.

Dördüncü araştırma sorusu web sitelerinin çerez politikaları ve gizlilik sözleşmelerinin gözetlemeyi nasıl ele aldıklarına ilişkindir. Sitelerin %6'sında herhangi bir çerez politikası veya gizlilik sözleşmesi bulunamamıştır. En minimum gereksimleri karşılayacak şekilde sitelerin %88'inde hangi verilerin toplandığı ve hangi amaçla toplandığı, %73'ünde toplanan verilerin nasıl işlendiği, %77'sinde kategorik düzeyde de olsa üçüncü taraflarla paylaşıldığı bilgisi, %51'inde çerezlerin ne kadar süreyle cihazda saklandığı ve %87'sinde kişisel verilerin silinmesiyle ilgili bir iletişim bilgisi yer aldığı görülmüştür.

Beşinci sorudan itibaren katılımcı görüşlerinin ağır bastığı bir çerçevede sorulara cevaplar aranmıştır. Beşinci soru gözetleme faaliyetlerinin neden varsayılan bir iş modeli hâline geldiğini anlamak üzerinedir. Buna göre verinin, veri sahipliğinin

ve yapay zekâ ile işlenmiş verilerin günümüzde kârlılığı bir üst noktaya çıkarması nedeniyle tüm şirket ve kuruluşların daha fazla veri toplamak için farklı tekniklerle kullanıcıları gözetleme modelini benimsediği ortaya konmuştur. Fiziksel bir ürünün satışıyla tek seferlik ve bugün elde edilen kazanç yerini, gözetleme sonucu sürekli toplanan ve işlenen verilerin hem bugün hem de yarının kazanç garantisine bırakmaktadır.

Altıncı soru Türkiye’de ve dünyada ortaya çıkan kişisel verilerin korunmasına yönelik yasal düzenlemelerin gözetlemeye etkisini tartışmaktadır. Gözetleme aracı olarak çerezler ve pikseller kişisel veri işledikleri için aktif hâle gelmeden önce kullanıcıdan açık rıza alınması gerekmektedir. Nicel araştırma bulgularında ve üçüncü sorunun cevabında görüldüğü üzere Türkiye’deki web siteleri üçüncü taraf izlemeleri aktif hâle getirirken kullanıcılardan açık rıza almamaktadır. Dolayısıyla KVK Kanununa sirayet etmemektedirler. Söz konusu nicel bulgular dışında katılımcılar da Türkiye’deki sitelerin çoğunun kanun bakımından sorunlu olduğunu dile getirmektedir. Görünen o ki, yasalar gözetlemeyi azaltacak etkiye sahipken yasa uygulayıcıların bilgisizliği veya ilgisizliği gözetlemenin sınırlandırılması önündeki bir engeldir.

Yedinci soru çevrim içi reklam endüstrisinin gözetlemeyi nasıl ele aldığıyla ilgilidir. Gözetim çalışmaları çoğunlukla konuya eleştirel bir perspektiften yaklaşmaktadır. Gözetim kapitalizmi kavramı da böyledir. Hatta gözetim kapitalizminin ortaya çıkmasına vesile olan durumun çevrim içi reklam endüstrisi olduğu ve bugün gözetleme faaliyetlerinin mazereti olarak yine çevrim içi reklam endüstrisinin gösterildiği dile getirilmektedir. Reklamcılar ve reklam konusunda uzman kişiler yapılan görüşmelerde verilerin açık rızaya dayalı olarak toplanması görüşü hâkimken, araştırmacı olarak gözlemlerime göre “gözetleme” ifadesi ilgili kişileri rahatsız etmiştir. Genel kanı, yayıncıların (web sitesi ve platformlar) birden çok reklam ve analitik şirketiyle çalışarak (izleyicilerini platformlarında barındırarak) reklam dolaylı kârlarını maksimize etmek istedikleri; kullanıcıların kendilerine alakalı reklam gösterilmesinden hoşnut oldukları üzerine yoğunlaşmaktadır. Reklam şirketleri bu durumu sağlamak için kullanıcıları platformlar ve cihazlar arası takip ederek onu

en iyi şekilde tanımayı amaçlamaktadır. Ayrıca, reklam endüstrisinin üçüncü taraf çerezlerin engellenmesi ve yasal düzenlemelerin iş modellerine yönelik tehditlerini bertaraf etmek için yeni veri toplama teknikleri üzerinde çalıştıkları belirtilmiştir.

Sekizinci soru kişisel verilerin yasalarca korunmasının ve kullanıcılarda kişisel veri bilincinin artmasının mahremiyet ve gözetim arasındaki çatışmayı nasıl etkilediğini anlamaya yöneliktir. Kanunlar, insanları korumak üzere hazırlanmıştır. Kişisel verilerin korunması da aynı kapsamdadır. Bireyler kişisel verilerinin önemi hakkında bir bilince sahip olmasa veya iradelerinin yanıtlanması yoluyla verileri onlardan alınsa bile kanunlar insanları koruma altına almaktadır. Yasal düzenlemeler bu bağlamda kişinin mahremiyetini korumak üzere adımlar atmaktadır. Veri farkındalığının ve bilincinin gelişmesi, mahremiyetin korunmasını bir adım öteye taşımaktadır. Bireyler, “verilerimin toplanması umrumda değil” yaklaşımı yerine, bu verilerle neler yapılabildiği ve yapılabileceği hakkında temel düzeyde bir farkındalığa sahip olmalıdır. Bireylerde kendilerine ait olan bir eşyayı koruma bilinci vardır. Aynı bilincin kendilerine ait olan verileri korumaya yönelik geliştirilmesi, yasalardan önce bireyin kendi mahremiyetine sahip çıkmasına yardımcı olur. Gözetleme faaliyetleri, bireylerin birbirini suçlayacağı kişisel problemler değil; sistemsel problemler yaratmaktadır. Veri bilinci taşıyan bir kişinin gözetlenmemek istemesi ve mahremiyet hakkı talep etmesi bir insan hakkıdır. Gözetim kapitalizmine dair sistemsel problem, söz konusu kişinin gözetlendiği hizmeti kullanmamasıyla çözülmemektedir. Veri bilinci arttıkça ve yasaların uygulanırılığı önündeki engeller kalktıkça sistemsel problemleri yaratan gözetim azalacak ve mahremiyetin önemi artacaktır.

Dokuzuncu soru gözetim kapitalizminin temel unsurlarını ele alarak onun etik hâle getirip getirilemeyeceğine cevap aramaktadır. Gözetleme mantığı, web teknolojileri üreticilerinin, teknoloji şirketlerinin ve yeni girişimlerin sıklıkla tercih ettiği bir iş modelidir. Bu model genellikle alternatifsiz görülmekte; dolayısıyla kazanç sağlamanın zorunlu bir yöntemi olarak kabul edilmektedir. Buna ek olarak gözetleme, web sitelerinin, uygulamaların, akıllı telefonların ve ağlara bağlanan tüm cihazların çalışmasını sağlayan hayati bir fonksiyonmuş gibi sunulmaktadır. Bu durumda insanlar platformları kullananlar değil, platformlar tarafından kullanılanlara

dönüşmektedir. Zira asıl çıkarı gözetleyerek platformlar sağlamaktadır. Oysaki gözetim kapitalizminde kullanıcılara sunulan ücretsiz hizmetler, gözetlemenin bir mazeretidir. Google, Facebook, Amazon ve diğer tüm büyük şirketlerin hiçbirinde, ücretli fakat kullanıcıyı gözetlemeyen bir ürün/hizmet yoktur. Örneğin, YouTube'un ücretli versiyonu kullanıcıya yalnızca reklam göstermemeyi vadeder. Gözetlenmeyeceğini vadetmez. Netflix gibi ücretli platformlar hem kullanıcı verilerini toplamakta hem iş ortaklarıyla bu verileri paylaşmakta hem de yine iş ortaklarından kendi kullanıcısı hakkında farklı veriler toplamaktadır. Gözetleme bir zorunluluk değildir; tercihtir. Bu tercihin nedeni gözetlemenin kârlılık sağlamasıdır. Diğer yandan kişiler hakkında toplanan veriler uzak sunucularda tutulmaktadır. Bireyin yararına değil, platformların yararına işlenmekte ve kullanılmaktadır. Bireyler kendi verilerinden sağlayabileceği potansiyel faydaya erişememektedir. Bu durumlar göz önüne alındığında gözetim kapitalizmi aktörlerinden etik olmalarını beklemek, köle tüccarlarından özgürlük beklemekle eşdeğerdir.

Onuncu ve son soru etik web'in inşasında nelerin gerektiğiyle ilgilidir. Bugünkü web'te neyin eksik olduğu ve etik web'in geliştirilmesi için hangi yolların izlenmesi gerektiği bu soru içerisinde tartışılmıştır. Önceki dokuz sorunun cevapları, nitel ve nicel araştırma bulguları ve çalışmanın literatürü etik web'e ilişkin bu öneri kılavuzunun hazırlanmasına ışık tutmuştur:

- 1) Web'in bir sahibi yoktur. Web herkes içindir; erişilebilirdir, çoklu sistemler içerir, şeffaftır, hakikati savunur, tekelleşmeye karşıdır ve merkezî değildir.
- 2) Web platformları etik bir temel üzerine inşa edilmeli ve bu temelde ürün ve hizmetleri kullanıcıyla buluşturmalıdır. Etik temel, ihtiyaçların etik hiyerarşisi bağlamında insan haklarına, insan deneyimine ve insan emeğine saygı olarak üç prensipten oluşmaktadır.
- 3) Web sitesi ve mobil uygulama geliştirme aşamalarında üçüncü taraf hizmetlere ve SDK'lara bağımlılık olabildiğince azaltılmalıdır. Yararlanılan kütüphaneler, yazılımlar, stiller, yazı karakterleri, videolar, fotoğraflar vb. ürünler platformların kendi sunucularında yer almalıdır.

- 4) Web ve mobil uygulama tasarım aşamasında kullanıcıların bilinçaltını harekete geçirecek, onları istenilen davranışa yönlendirerek manipüle edecek ve onlara maddi / manevi zarar verecek tasarım desenleri kullanılmamalıdır.
- 5) Kullanıcılar çevrim içi bir deneyim yaşarken hizmetten faydalanan olmalı, gözetlenerek başka bir hizmetin parçası olmamalıdır. Web, azınlık grupların çıkarına değil bireylerin çıkarına hizmet etmelidir.
- 6) Web platformları kullanıcı verilerini yalnızca sınırlı ve amaca uygun olarak toplamalıdır; bunun için kullanıcıları şeffaf şekilde bilgilendirmeli ve açık rızalarını almalıdır.
- 7) Kullanıcıların verileri farklı ve bilinmeyen şirketlerin sunucularında değil, kullanıcıların kendi cihazlarında, sunucularında veya bulut sisteminde tutulmalıdır. Bu veriler uçtan uca şifreli olmalı ve platformlar kullanıcının kontrolü dâhilinde verilere erişebilmelidir. Etik web platformları, verinin kontrolünü kullanıcıya vermekle yükümlüdür.
- 8) Web platformlarının algoritmaları kullanıcının çıkarına çalışmalıdır. Kullanıcılar kendisi hakkında öngörülen potansiyel tehdit ve fırsatlardan haberdar olmalıdır. Algoritmaların çalışma prensipleri şeffaf olmalı ve yönetimi kullanıcının tercihiyle bırakılmalıdır.
- 9) Web platformları merkezîleşmemelidir. Platformlar, tıpkı e-posta sistemi gibi merkeziyetsiz olmalıdır. Bir e-posta sunucusundan diğer e-posta sunucusuna nasıl ileti gönderilebiliyorsa platformlar arası iletişim ve veri taşıma mümkün olmalıdır.
- 10) Çevrim içi gözetime ve kişisel verilerin korunmasına yönelik uluslara özgü değil, uluslararası ortak bir yasal düzenleme tesis edilmeli; kullanıcılar web’te maruz kaldıkları hak ihlallerini bu düzenlemeye bağlı olarak çözmeli ve yaptırımlar ülkeden ülkeye göre farklılık göstermemelidir. Örneğin, Fransa’da Google’a verilen cezaya neden olan problem, yalnızca Fransa’dan Google’a erişimde düzeltilmiş olmamalı; tüm ülkelerde düzeltilmiş olmalıdır.
- 11) Bugün web’in her köşesi deyim yerindeyse AVM’ler tarafından sarılmıştır. Web’in ise parklara ihtiyacı vardır. Etik bir web oluşturulmasında parkların

önemi büyüktür. İnsanlar parklarda egzersiz yapar, sakinleşir, dinlenir, çocuklarıyla vakit geçirir, arkadaşlarıyla görüşür ve şehrin karmaşasından uzaklaşma fırsatı bulur. Parklar insanların çıkarına hizmet eder. Web'in icadı, kendi yapısı içerisinde birçok parkın inşa edilmesi ve herkesin parklardan faydalanması idealini taşımaktadır. Gözetim kapitalizmi mantığı park alanlarına alışveriş merkezleri inşa etmiştir. Park alanlarının çoğalması, web ve teknolojiyi daha etik yaparak sistemin yarattığı sorunları azaltacaktır.

Bu çalışmada gözetim kapitalizmi tüm bileşenleriyle ele alınarak çalışma mantığı hakkında kapsamlı bir içerik oluşturulmaya çalışılmıştır. Gözetim kapitalizminin yarattığı sorunların tespiti ve etkilediği alanlar bütüncül olarak tartışılarak etik bir web için olması gerekenler ortaya konulmuştur. Nicel araştırma, gözetimin pratikte ne derece yaygın olduğunu somut bir şekilde belirlemek ve yasalara uygunluğunu ortaya çıkarmak amacıyla gerçekleştirilmiştir. Nitel araştırma basamağında ise çevrim içi reklamcılık, teknoloji, yasal düzenlemeler, kişisel veri ve mahremiyet gibi gözetim kapitalizminin içinde yer alan konular hakkında uzman görüşlerine yer verilmiştir. Çalışma, gözetimin izini sürerken üçüncü taraf izlemelerin kimler tarafından gerçekleştirildiğini ortaya çıkarmasıyla bu alandaki yerli literatüre ilk katkıyı veren çalışmalardan birisidir. Aynı şekilde çalışma sınırlı bir örneklemle de olsa web sitelerinin kişisel verilerin korunması kanununa ne derece uygun olduğunu ortaya çıkarması nedeniyle gelecekte iletişim alanında yapılacak çalışmalara teknik olarak yol göstermektedir. Çalışma ayrıca etik web kavramının literatüre kazandırılması ve web'in daha etik hâle getirilmesi için yapılması gerekenleri belirlemesi bakımından önemlidir.

KAYNAKÇA

- Acxiom: “The World’s Best Customer Data to Fuel Marketing”, **Acxiom**, 2020, (Çevrimiçi) <https://www.acxiom.com/customer-data/>, 12.12.2020.
- Acxiom Data Bundles: “Data Services API: Data Bundles”, 2020, (Çevrimiçi) <https://developer.myacxiom.com/code/api/data-bundles/bundle/eTechDemographics>, 12.12.2020.
- Al-Abassi, Abdulrahman vd.: “Industrial Big Data Analytics: Challenges and Opportunities”, **Handbook of Big Data Privacy**, ed. Kim-Kwang Raymond Choo, Ali Dehghantanha, Cham, Springer International Publishing, 2020, s. 37-61.
- Alakuş, Meral: **Bilgi Toplumu**, 1. bs, Ankara, Kültür Bakanlığı Kütüphaneler Genel Müdürlüğü, 1991.
- Allmer, Thomas: “Critical Internet Surveillance Studies and Economic Surveillance”, **Internet and Surveillance: The Challenges of Web 2.0 and Social Media**, ed. Christian Fuchs vd., New York, Routledge, 2012, s. 123-143, (Çevrimiçi) <https://westminsterresearch.westminster.ac.uk/item/8z76z/introduction-internet-and-surveillance>, 05.12.2020.
- : **Towards a Critical Theory of Surveillance in Informational Capitalism**, New York, Peter Lang AG, 2012.
- Altaweel, Ibrahim, Nathan Good, Chris Jay Hoofnagle: “Web Privacy Census”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 15.12.2015, (Çevrimiçi) <https://papers.ssrn.com/abstract=2703814>, 01.05.2020.
- Andrew, Dan: “Programmatic trading: the future of audience economics”, **Communication Research and Practice**, C. 5, No: 1, 2019, s. 73-87.
- Andrews, Eric: “4 Types of Personal Data Under the California Consumer Privacy Act (CCPA)”, **Securiti**, 2019, (Çevrimiçi) <https://securiti.ai/blog/ccpa-types-of-personal-data/>, 08.10.2021.
- Andrews, Lori: **I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy**, Reprint edition., Delran, Free Press, 2013.
- Anić, Ivan-Damir: “The Development Of Database Marketing: Does Consumer Information Privacy Matter?”, **Zbornik Radova**

Ekonomskog Fakulteta Sveučilišta u Mostaru, No: 21, 2015, s. 39-56.

Armstrong, Gary,
Clive Norris:

The Maximum Surveillance Society: The Rise of CCTV, 1st edition., Oxford ; New York, Berg Publishers, 1999.

Auxier, B. vd.:

“Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information”, **Pew Research Center: Internet, Science & Tech**, 15.11.2019, (Çevrimiçi)
<https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>, 05.12.2020.

Balkan, Aral, Laura
Kalbag:

“Ethical Design”, Ind.ie, 2015, (Çevrimiçi)
<https://ind.ie/ethical-design/downloads/ethical-design.pdf>, 08.10.2021.

Balkan, Aral:

Cyborg rights activist, designer & lead developer Aral Balkan | Creative Ville 2019, 2020, (Çevrimiçi)
<https://www.youtube.com/watch?v=k2Go4uPdysU>, 05.12.2021.

Baltacı, Ali:

“Nitel Araştırmalarda Örneklem Yöntemleri ve Örnek Hacmi Sorunsalı Üzerine Kavramsal Bir İnceleme”, **Bitlis Eren Üniversitesi Sosyal Bilimler Dergisi**, C. 7, No: 1, 2018, s. 231-274.

Bangemann Group:

“Europe and the global information society Recommendations of the high-level group on the information society to the Corfu European Council”, **Growth, competitiveness and employment: white paper follow-up ; Report on Europe and the global information society ; Interim report on trans-European networks ; Progress report on employment**, ed. Commission of the European Communities, Bulletin of the European Union. Supplement, Supplement 2/94, Brussels, European Commission, 1994.

Baruh, Lemi:

“Read at Your Own Risk: Shrinkage of Privacy and Interactive Media”, **New Media & Society**, C. 9, No: 2, 2007, s. 187-211.

Bauman, Zygmunt:

Akışkan Modernite, çev. Sinan Okan Çavuş, 2. bs, İstanbul, Can Yayınları, 2017.

Bauman, Zygmunt,
David Lyon:

Akışkan Gözetim, çev. Elçin Yılmaz, 3. bs, Ayrıntı Yayınları, 2018.

- Beard, Matthew, Simon Longstaff: “Ethical By Design: Principles for Good Technology”, The Ethics Centre, 2019, (Çevrimiçi) https://ethics.org.au/wp-content/uploads/2019/03/The-Ethics-Centre_PRINCIPLES-FOR-GOOD-TECHNOLOGY.pdf.
- Beaud, Michel: **Kapitalizmin Tarihi / 1500-2010**, çev. Fikret Başkaya, İstanbul, Yordam Kitap, 2016.
- Bell, Daniel: “The Coming of the Post-Industrial Society”, **The Educational Forum**, C. 40, No: 4, 1976, s. 574-579.
- Beller, Jonathan: “Bilişsel Kapitalist Pedagoji ve Hoşnutsuzlukları”, **Bilişsel Kapitalizm! Eğitim ve Dijital Emek**, ed. Ergin Bulut, Michael A. Peters, çev. Tahir Emre Kalaycı, 1. bs, Ankara, Notabene Yayınları, 2014.
- Berardi, Franco: **And. Phenomenology of the End : Cognition and Sensibility in the Transition from Conjunctive to Connective Mode of Social Communication**, Finland, Aalto University, 2014.
- : **Precarious Rhapsody: Semiocapitalism and the Pathologies of Post-Alpha Generation**, London, Autonomedia, 2009.
- : “What Does Cognitariat Mean? Work, Desire and Depression”, **Cultural Studies Review**, C. 11, No: 2, 2005, s. 57-63.
- Berber, Leyla Keser: **Çevrimiçi Davranışsal Reklamcılık (Online Behavioral Advertising) Uygulamaları Özelinde Kişisel Verilerin Korunması**, On İki Levha Yayıncılık, 2014.
- Birleşik Krallık Parlamentosu: “Disinformation and ‘fake news’: Final Report published”, House of Commons, 2019, (Çevrimiçi) <https://publications.parliament.uk/pa/cm201719/cmselect/cmc/umeds/1791/1791.pdf>, 06.11.2021.
- Blattberg, Robert C., Byung-Do Kim, Scott A. Neslin: **Database Marketing: Analyzing and Managing Customers**, New York, Springer, 2008.
- Bloom, Peter: **Monitored: Business and Surveillance in a Time of Big Data**, London, Pluto Press, 2019.

- Body, Danah, Kate Crawford: “Critical Questions for Big Data”, **Information, Communication & Society**, C. 15, No: 5, 2012, s. 662-679.
- Boyne, Roy: “Post-Panopticism”, **Economy and Society**, C. 29, No: 2, 2000, s. 285-307.
- Brown, Sherrwod: “Privacy Isn’t a Right You Can Click Away”, **Wired**, 2020, (Çevrimiçi) <https://www.wired.com/story/privacy-isnt-a-right-you-can-click-away/>, 01.08.2020.
- Bruns, Axel: “From Prosumer to Produser: Understanding User-Led Content Creation”, **Transforming Audiences 2009**, 2009, (Çevrimiçi) <https://eprints.qut.edu.au/27370/>, 08.12.2020.
- BuiltWith: “Google Analytics Usage Statistics”, 2020, (Çevrimiçi) <https://trends.builtwith.com/analytics/Google-Analytics>, 26.11.2020.
- Bulut, Ergin, Michael A. Peters: “Bilişsel Kapitalizm, Eğitim ve Dijital Emek”, **Bilişsel Kapitalizm! Eğitim ve Dijital Emek**, ed. Ergin Bulut, Michael A. Peters, çev. Barış Yıldırım, 1. bs, Ankara, Notabene Yayınları, 2014.
- Busch Oliver, (ed.): **Programmatic Advertising: The Successful Transformation to Automated, Data-Driven Marketing in Real-Time**, 1st ed. 2016 edition., Springer, 2015.
- Businesswire: “\$135.3 Billion Worldwide Smart Home Industry to 2025 - Featuring Schneider Electric, United Technologies & Amazon Among Others - ResearchAndMarkets.Com”, 24.07.2020, (Çevrimiçi) <https://www.businesswire.com/news/home/20200724005173/en/135.3-Billion-Worldwide-Smart-Home-Industry-to-2025---Featuring-Schneider-Electric-United-Technologies-Amazon-Among-Others---ResearchAndMarkets.com>, 05.12.2020.
- California Legislative Information: “Business And Professions Code - Bpc Division 8. Special Business Regulations [18400 - 22949.51]”, 2004, (Çevrimiçi) https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC&sectionNum=22575, 07.10.2021.
- : “California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100]”, 2018, (Çevrimiçi) https://leginfo.ca.gov/faces/codes_displayText.xhtml

division=3.&part=4.&lawCode=CIV&title=1.81.5,
08.10.2021.

Cameron, Ross: “Infinite Regress Arguments”, **The Stanford Encyclopedia of Philosophy**, ed. Edward N. Zalta, Fall 2018., Metaphysics Research Lab, Stanford University, 2018, (Çevrimiçi)
<https://plato.stanford.edu/archives/fall2018/entries/infinite-regress/>, 08.11.2021.

Caraway, Brett: “Audience Labor in the New Media Environment: A Marxian Revisiting of the Audience Commodity”, **Media, Culture & Society**, C. 33, No: 5, 2011, s. 693-708.

Carson, Angelique: “Data Privacy Laws: What You Need to Know in 2021”, **Osano**, 2021, (Çevrimiçi)
<https://www.osano.com/articles/data-privacy-laws>,
07.10.2021.

Castells, Manuel: “The Network Society From Knowledge to Policy”, **The Network Society: From Knowledge to Policy**, ed. Manuel Castells, Gustavo Cardoso, Washington, DC, Center for Transatlantic Relations, Johns Hopkins U.-SAIS, 2005, s. 3-23.

Castells, Manuel: **Ağ Toplumunun Yükselişi**, çev. Ebru Kılıç, 2. bs, İstanbul, İstanbul Bilgi Üniversitesi Yayınları, 2008.

Cegłowski, Maciej: “Remarks at the SASE Panel On The Moral Economy of Tech”, 26.06.2016, (Çevrimiçi)
https://idlewords.com/talks/sase_panel.htm, 31.05.2020.

Chaston, I.: **Internet Marketing and Big Data Exploitation**, Palgrave Macmillan UK, 2015.

Chen, Gang vd.: “Understanding Programmatic Creative: The Role of AI”, **Journal of Advertising**, C. 48, No: 4, 2019, s. 347-355.

Chen, Julie Yujie: “Platform Economies: The Boss’s Old and New Clothes”, 2018, 5.

Christl, Wolfie: “Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions”, 2017.

Christl, Wolfie,
Sarah Spiekermann: **Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy**, Facultas, 2016.

- Clarke, Roger: “Information technology and dataveillance”, **Communications of the ACM**, C. 31, No: 5, 1988, s. 498-512.
- Clement, J.: “Distribution of Free and Paid Android Apps 2020”, **Statista**, 2020b, (Çevrimiçi)
<https://www.statista.com/statistics/266211/distribution-of-free-and-paid-android-apps/>, 29.11.2020.
- : “Distribution of Free and Paid IOS Apps 2020”, **Statista**, 2020c, (Çevrimiçi)
<https://www.statista.com/statistics/1020996/distribution-of-free-and-paid-ios-apps/>, 29.11.2020.
- : “Number of Available Applications in the Google Play Store from December 2009 to September 2020”, **Statista**, 24.11.2020, (Çevrimiçi)
<https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/>, 29.11.2020.
- Cobb, Michael: “How Can Android App Permissions Be Exploited by Attackers?”, **SearchSecurity**, 2017, (Çevrimiçi)
<https://searchsecurity.techtarget.com/answer/How-can-Android-app-permissions-be-exploited-by-attackers>, 30.11.2020.
- Cohen, Julie E.: “What is Privacy For”, **Harvard Law Review**, C. 126, No: 7, 2013, s. 1904-1933.
- Copolla, Daniela: “Amazon Web Services Revenue 2019”, **Statista**, 26.11.2020, (Çevrimiçi)
<https://www.statista.com/statistics/233725/development-of-amazon-web-services-revenue/>, 11.12.2020.
- Coté, Mark, Jennifer Pybus: “Learning to Immaterial Labour 2.0: MySpace and Social Networks”, **Ephemera**, C. 7, No: 1, 2007, s. 88-106.
- Council of Europe: **Handbook on European Data Protection Law**, LU, Publications Office of the European Union, 2018.
- Creswell, John W., Vicki L. Plano Clark: **Designing and Conducting Mixed Methods Research**, 3. bs, Los Angeles, SAGE Publications, 2018.
- Cronk, R. Jason: “Categories of Personal Information”, **Enterprivacy Consulting Group**, 01.03.2017, (Çevrimiçi)
<https://enterprivacy.com/2017/03/01/categories-of-personal-information/>, 08.10.2021.

- Çakır, Mukadder: “Bilgi Toplumu Kuramları ve Prekarya Tartışmaları”, **Bilgi Toplumu Tartışmaları**, ed. Mukadder Çakır, 1. bs, İstanbul, Pales Yayınları, 2018, s. 19-114.
- : “Yeni Medyaya İlişkin Eleştirel Yaklaşımları ve Tespitleri ile Christian Fuchs”, ed. Mukadder Çakır, İstanbul, Doğu Yayınları, 2014, s. 81-130, 09.12.2020.
- Çekin, Mesut Serdar: **Çerezler ve Açık Rıza Bağlamında Güncel Gelişmeler**, Çarşamba Seminerleri, Kişisel Verileri Koruma Kurumu, 2021, (Çevrimiçi) <https://www.youtube.com/watch?v=7Z3eKZBHflw>, 03.11.2021.
- Daems, Tom: **Electronic Monitoring: Tagging Offenders in a Culture of Surveillance**, 1st edition., Palgrave Pivot, 2019.
- Datatilsynet: “Quick-guide til at sætte cookies”, Danimarka Veri Koruma Kurumu, 2021, (Çevrimiçi) <https://www.datatilsynet.dk/Media/E/7/Quickguide.pdf>, 03.11.2021.
- Davis, Marc E.: “Rethinking Personal Data: A New Lens for Strengthening Trust”, thk. A. T. Kearney, World Economic Forum, 2014, (Çevrimiçi) https://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.
- D-CENT: “Research on Identity Ecosystem”, 2015, (Çevrimiçi) https://dcentproject.eu/wp-content/uploads/2015/08/D3.3-Research-on-Identity-Ecosystem_part1.pdf.
- De Mooy, Michelle, Shelten Yuen: “Towards Privacy-Aware Research and Development in Wearable Health”, **Hawaii International Conference on System Sciences 2017 (HICSS-50)**, 2017.
- Dean, Jodi: “Communicative Capitalism and Class Struggle”, Text, **Spheres**, 11.11.2014, (Çevrimiçi) <http://spheres-journal.org/communicative-capitalism-and-class-struggle/>, 31.05.2020.
- Deleuze, Gilles: “Postscript on the Societies of Control”, **October**, C. 59, 1992, s. 3-7.
- Dijk, Jan van: **Ağ Toplumu**, çev. Özlem Sakin, 2. bs, Kafka Kitap, 2018.

- Dimova, Yana vd.: “The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion”, **arXiv:2102.09301 [cs]**, 2021.
- Dobb, Maurice: **Kapitalizmin Dünü ve Bugünü**, çev. Feyza Kantur, İstanbul, İletişim Yayınları, 1990.
- Dolgun, Uğur: **Şeffaf Hapishane Yahut Gözetim Toplumu**, 3. bs, Ötüken Neşriyat, 2015.
- Doucek, Petr, Antonin Pavliceck, Ladislav Luc: “Internet of Things or Surveillance of Things?”, **Research and Practical Issues of Enterprise Information Systems**, ed. A Min Tjoa vd., Lecture Notes in Business Information Processing, Cham, Springer International Publishing, 2018, s. 45-55, doi:10.1007/978-3-319-94845-4_5.
- Drucker, Peter F.: **Kapitalist Ötesi Toplum**, çev. Belkıs Çorakçı, İstanbul, İnkılap Kitabevi, 1993.
- Dua, Tanya: “How Coca-Cola Targeted Ads Based on People’s Facebook, Instagram Photos”, **Digiday**, 16.05.2017, (Çevrimiçi) <https://digiday.com/marketing/coca-cola-targeted-ads-based-facebook-instagram-photos/>, 04.05.2020.
- Dura, Cihan, Hayriye Atik: **Bilgi Toplumu Bilgi Ekonomisi ve Türkiye**, 1. bs, İstanbul, Litetatur Yayıncılık, 2002.
- Earp, Julia vd.: “Examining Internet Privacy Policies Within the Context of User Privacy Values”, **Engineering Management, IEEE Transactions on**, C. 52, 2005, s. 227-237.
- EDRi: “Guide for Ethical Website Development and Maintenance”, European Cultural Foundation, European Digital Rights, 2020, (Çevrimiçi) https://edri.org/files/ethical_web_dev_web.pdf, 05.11.2021.
- Ekman, Mattias: “Birikimi Anlamak : Marx’ın İlk Birikim Kuramı’nın Medya ve İletişim Çalışmaları Açısından Önemi”, **Marx Geri Döndü – Medya, Meta ve Sermaye Birikimi**, ed. Vincent Mosco, Christian Fuchs, çev. Zafer Kıyan, Hakan Yüksel, 2. bs., Ankara, Nota Bene Yayınları, 2019, s. 83-118, (Çevrimiçi) <http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-48529>, 25.05.2020.
- Elmer, Greg: **Profiling Machines - Mapping the Personal Informat: Mapping the Personal Information Economy**, Cambridge, Mass, 2003.

- European Court of Human Rights: “European Convention on Human Rights”, Council of Europe, 1950, (Çevrimiçi)
https://www.echr.coe.int/Documents/Convention_ENG.pdf.
- Falbe, Trine, Martin Michael Frederiksen, Kim Andersen: **The Ethical Design Handbook**, Smashing Media AG, 2020.
- Ferguson, Andrew Guthrie: “Big Data Surveillance: The Convergence of Big Data and Law Enforcement”, **The Cambridge Handbook of Surveillance Law**, ed. David Gray, Stephen E. Henderson, Cambridge Law Handbooks, Cambridge, Cambridge University Press, 2017, s. 171-197, doi:10.1017/9781316481127.008.
- Fisher, Eran: “Daha Az Yabancılaşma Nasıl Daha Fazla Sömürü Yaratır? Sosyal Paylaşım Sitelerinde İzleyici Emegi”, **Marx Geri Döndü – Medya, Meta ve Sermaye Birikimi**, ed. Vincent Mosco, Christian Fuchs, çev. Gökçe Baydar, 2. bs., Ankara, Nota Bene Yayınları, 2019.
- FOIA: “The Freedom of Information Act - Department of Justice”, 2014, (Çevrimiçi)
<https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/foia-final.pdf>, 07.10.2021.
- Foster, John Bellamy, Robert W. McChesney: “Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age”, **Monthly Review**, 01.07.2014, (Çevrimiçi)
<https://monthlyreview.org/2014/07/01/surveillance-capitalism/>, 04.05.2020.
- Fouad, Imane vd.: “Missed by Filter Lists: Detecting Unknown Third-Party Trackers with Invisible Pixels”, 2020.
- Foucault, Michel: **Büyük Kapatılma**, çev. Işık Ergüden, Ferda Keskin, İstanbul, 2007.
- : **Hapishanenin Doğuşu**, çev. Mehmet Ali Kılıçbay, 8. bs, İmge Kitabevi Yayınları, 2019.
- : **İktidarın Gözü**, çev. Işık Ergüden, 4. bs, Ayrıntı Yayınları, 2015.
- Friedland, Steven I.: “The Internet of Things and Self-Surveillance Systems”, **The Cambridge Handbook of Surveillance Law**, ed. David Gray, Stephen E. Henderson, Cambridge Law Handbooks,

Cambridge, Cambridge University Press, 2017, s. 198-224, doi:10.1017/9781316481127.009.

- Fry, Hannah: **Merhaba Dünya**, çev. İpek Çıgay Güneş, İstanbul, Hep Kitap, 2019.
- FTC: “Personal Data Ecosystem”, Federal Trade Commission, 2021, (Çevrimiçi)
https://www.ftc.gov/sites/default/files/documents/public_events/exploring-privacy-roundtable-series/personaldataecosystem.pdf.
- Fuchs, Christian: “Bilişsel Kapitalizm ya da Enformasyonel Kapitalizm? Enformasyonel Ekonomide Sınıfın Rolü”, **Bilişsel Kapitalizm! Eğitim ve Dijital Emek**, ed. Ergin Bulut, Michael A. Peters, çev. Kemal Özdil, 1. bs, Ankara, Notabene Yayınları, 2014.
- : **Dijital Emek ve Karl Marx**, çev. Tahir Emre Kalaycı, Senem Oğuz, 1. bs, Ankara, Notabene Yayınları, 2015.
- : “Introduction: Internet and Surveillance”, **Internet and Surveillance: The Challenges of Web 2.0 and Social Media**, ed. Christian Fuchs vd., New York, Routledge, 2012, s. 1-28, (Çevrimiçi)
<https://westminsterresearch.westminster.ac.uk/item/8z76z/introduction-internet-and-surveillance>, 05.12.2020.
- : “Karl Marx in the Age of Big Data Capitalism”, **Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data**, London, University of Westminster Press, 2019, s. 53-71.
- : “New Media, Web 2.0 and Surveillance”, **Sociology Compass**, C. 5, No: 2, 2011, s. 134-147.
- : “Social Media Surveillance”, **Handbook of Digital Politics**, 2015.
- : **Sosyal Medya: Eleştirel Bir Giriş**, çev. Diyar Saraçoğlu, İlker Kalaycı, Notabene Yayınları, 2016.
- Fulcher, James: **Capitalism: A Very Short Introduction**, 1. bs, USA, Oxford University Press, 2004.
- Fumagalli, Andrea vd.: “Digital Labour in the Platform Economy: The Case of Facebook”, **Sustainability**, C. 10, No: 6, 2018, s. 1757.

- Fumagalli, Andrea, Stefano Lucarelli: “A Model of Cognitive Capitalism. A Preliminary Analysis”, **European Journal of Economic and Social Systems**, C. 20, No: 1, 2007, s. 117-133.
- Galič, Maša, Tjerk Timan, Bert-Jaap Koops: “Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 03.08.2016, (Çevrimiçi) <https://papers.ssrn.com/abstract=2817813>, 24.05.2020.
- Gandy, Oscar H.: **The Panoptic Sort: A Political Economy Of Personal Information**, 1 edition., Boulder, Colo, Westview Press, 1993.
- : “The Surveillance Society: Information Technology and Bureaucratic Social Control”, **Journal of Communication**, C. 39, No: 3, 1989, s. 61-76.
- GDPR: “Cookies, the GDPR, and the EPrivacy Directive”, **GDPR**, 2019, (Çevrimiçi) <https://gdpr.eu/cookies/>, 26.11.2020.
- Gençoğlu, Aylin Yonca: “Kapitalizme Teorik Yaklaşımlar: Kapitalist Ekonomik Sistemin Temel Nitelikleri Üzerinden Karşılaştırmalı Bir Analiz”, **Temaşa Erciyes Üniversitesi Felsefe Bölümü Dergisi**, No: 14, 2020, s. 237-256.
- Gentsch, Peter: **AI in Marketing, Sales and Service: How Marketers without a Data Science Degree can use AI, Big Data and Bots**, New York, NY, 2018.
- Gezmen, Başak: “Bilgi Toplumu’ndan Veri Toplumu’na”, **Post-lar Çağında İletişim**, ed. M. Nur Erdem, Nihal Kocabay Şener, 1. bs., Konya, Literatürk Yayınları, 2019.
- Ghostery: “Tracking the Trackers”, **Ghostery**, 04.12.2017, (Çevrimiçi) <https://www.ghostery.com/study/>, 01.06.2020.
- Giddens, Anthony: **Kapitalizm ve Modern Sosyal Teori**, 2. bs, İstanbul, İletişim Yayınları, 2010.
- : **Modernliğin Sonuçları**, çev. Ersin Kuşdil, 1. bs, İstanbul, Ayrıntı Yayınları, 1994.
- : **Sosyoloji**, çev. Cemal Güzel, 1. bs, İstanbul, Kırmızı Yayınları, 2008.
- Giddens, Anthony, Philip W. Sutton: **Sosyolojide Temel Kavramlar**, çev. Ali Esgin, 3. bs, Ankara, Phoenix Yayınevi, 2018.

- Goel, Vinay: "An Updated Timeline for Privacy Sandbox Milestones", **Google**, 24.06.2021, (Çevrimiçi)
<https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/>, 27.12.2021.
- "González-Cabañas, José vd.: "Unique on Facebook: Formulation and Evidence of (Nano)targeting Individual Users with non-PII Data", 2021.
- Goodman, Marc: **Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü**, 2. bs, Timaş Yayınları, 2019.
- : "Hacked Dog, a Car That Snoops on You and a Fridge Full of Adverts: The Perils of the Internet of Things", **The Guardian**, (11.03.2015), blm. Technology, (Çevrimiçi)
<https://www.theguardian.com/technology/2015/mar/11/internet-of-things-hacked-online-perils-future>, 10.11.2021.
- Gordon, Diana R.: "The Electronic Panopticon: A Case Study of the Development of the National Criminal Records System", **Politics & Society**, C. 15, No: 4, 1987, s. 483-511.
- Graham, Philip: "Hypercapitalism: A Political Economy of Informational Idealism", **New Media & Society**, C. 2, No: 2, 2000, s. 131-156.
- Graham, Stephen, David Wood: "Digitizing Surveillance: Categorization, Space, Inequality":, **Critical Social Policy**, C. 23, No: 2, 2003, s. 227-248.
- Grand View Research: "Location Intelligence Market Size & Share | Industry Report, 2027", 2020, (Çevrimiçi)
<https://www.grandviewresearch.com/industry-analysis/location-intelligence-market>, 18.12.2021.
- Grauer, Yael: "Here's a Long List of Data Broker Sites and How to Opt-Out of Them", 27.03.2018, (Çevrimiçi)
<https://www.vice.com/en/article/ne9b3z/how-to-get-off-data-broker-and-people-search-sites-pipl-spokeo>, 12.12.2020.
- Gray, Kenneth R.: *Review of a Theory of Global Capitalism: Production Class, And State in a Transnational World*, William I. Robinson, **International Journal on World Peace**, C. 21, No: 2, 2004, s. 81-86.
- Greenwald, Glenn: **No Place to Hide: Edward Snowden, the NSA and the Surveillance State**, London, Hamish Hamilton, 2014.
- Guttmann, A.: "Digital Advertising Spending Worldwide from 2018 to 2024", **Statista**, 17.11.2020, (Çevrimiçi)

<https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/>, 12.12.2020.

———: “Global Programmatic Display Ad Spending 2021”, **Statista**, 2020b, (Çevrimiçi)
<https://www.statista.com/statistics/418035/global-programmatic-ad-spend/>, 13.12.2020.

Güçlü, Ahmet: “Kapitalizmde Vahşileşme Dışında Yeni Bir Şey Yok”, **Post-lar Çağında İletişim**, ed. M. Nur Erdem, Nihal Kocabay Şener, 1. bs., Konya, Literatürk Yayınları, 2019.

Habib, Hana vd.: “An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites”, 2019, (Çevrimiçi)
<https://www.usenix.org/conference/soups2019/presentation/habib>, 31.07.2020.

Haggerty, Kevin D., Richard V. Ericson: “The Surveillant Assemblage”, **The British Journal of Sociology**, C. 51, No: 4, 2000, s. 605-622.

Hardt, Michael, A. Negri: **Çokluk: İmparatorluk Çağında Savaş ve Demokrasi**, çev. Barış Yıldırım, 1. bs., İstanbul, Ayrıntı Yayınları, 2004.

Harris, James: “Ethical issues in web design”, **Journal of Computing Sciences in Colleges**, C. 25, 2009, s. 214-220.

Harris, Rich: “Geographies of bias and exclusion in a lifestyle databases”, 1998, (Çevrimiçi)
http://www.geocomputation.org/1998/82/gc_82.htm, 26.05.2021.

Hartzog, Woodrow: **Privacy’s Blueprint: The Battle to Control the Design of New Technologies**, Harvard University Press, 2018.

Harvey, David: **Marx’in Kapital’i İçin Kılavuz**, çev. Bülent O. Doğan, 1. bs., İstanbul, Metis Yayınları, 2012.

Has, Murat: “Aihm Kararları Bağlamında Görüntü Hakkı”, **Anayasa Yargısı**, C. 38, No: 1, 2021, s. 205-242.

Hebblewhite, William Henning James: “Üretim Araçları Olarak İletişim Araçları”, **Marx Geri Döndü – Medya, Meta ve Sermaye Birikimi**, ed. Vincent Mosco, Christian Fuchs, çev. Zeynep Saygın Sarbay, 2. bs., Ankara, Nota Bene Yayınları, 2019, (Çevrimiçi)
<http://urn.kb.se/resolve?urn=urn:nbn:se:oru:diva-48529>, 25.05.2020.

- Heeks, Richard: “Digital Economy and Digital Labour Terminology: Making Sense of the ‘Gig Economy’, ‘Online Labour’, ‘Crowd Work’, ‘Microwork’, ‘Platform Labour’, Etc.”, **SSRN Electronic Journal**, 2017.
- Hill, Kashmir: “Data Broker Was Selling Lists Of Rape Victims, Alcoholics, and ‘Erectile Dysfunction Sufferers’”, **Forbes**, 19.12.2013, (Çevrimiçi)
<https://www.forbes.com/sites/kashmirhill/2013/12/19/data-broker-was-selling-lists-of-rape-alcoholism-and-erectile-dysfunction-sufferers/>, 12.12.2020.
- Huws, Ursula: **Küresel Dijital Ekonomide Emek**, çev. Cemre Şenesen, İstanbul, Yordam Kitap, 2018.
- IAB Europe: “Programmatic Advertising Spend in Europe”, 01.10.2020, (Çevrimiçi) <https://iabeurope.eu/wp-content/uploads/2020/10/Programmatic-Market-Advertising-Spend-2019-Report.pdf>, 13.12.2020.
- IAB France: “L’IAB France publie son guide cookieless & consentless 2022”, **IAB France**, 01.12.2021, (Çevrimiçi)
<https://www.iabfrance.com/publication/liab-france-publie-son-guide-cookieless-consentless-2022>, 31.12.2021.
- IAPP: “Guide to Basic Data Anonymization Techniques”, Personal Data Protection Commission, 2018, (Çevrimiçi)
https://iapp.org/media/pdf/resource_center/Guide_to_Anonymisation.pdf, 07.11.2021.
- InfoCuria Case-law: “(Reference for a preliminary ruling — Directive 95/46/EC — Directive 2002/58/EC — Regulation (EU) 2016/679 — Processing of personal data and protection of privacy in the electronic communications sector — Cookies — Concept of consent of the data subject — Declaration of consent by means of a pre-ticked checkbox)”, 01.10.2019, (Çevrimiçi)
<https://curia.europa.eu/juris/document/document.jsf?jsessionid=D064FC9AE5825F3BBCEE9089B8ED0E56?text=&docid=218462&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=912249>, 03.11.2021.
- Jaconi, Mike: “The ‘On-Demand Economy’ Is Revolutionizing Consumer Behavior — Here’s How”, **Business Insider**, 2014,

- (Çevrimiçi) <https://www.businessinsider.com/the-on-demand-economy-2014-7>, 12.12.2020.
- Jenkins, Richard: “Identity, Surveillance and Modernity: Sorting out Who’s Who”, **Routledge Handbook of Surveillance Studies**, ed. David Lyon, Kristie Ball, Kevin D. Haggerty, London, Routledge, 2012, 16.05.2021.
- Jones, Frank: “Will Your New PC Turn into a Spy?; Pentium: Intel’s New Microchips Will Contain Information That Would Easily Identify Individual Computers.”, **Baltimoresun.Com**, 25.01.1999, (Çevrimiçi) <https://www.baltimoresun.com/news/bs-xpm-1999-01-25-9901250194-story.html>, 30.05.2021.
- Keegan, Jon, Alfred Ng: “The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users – The Markup”, 06.12.2021, (Çevrimiçi) <https://themarkup.org/privacy/2021/12/06/the-popular-family-safety-app-life360-is-selling-precise-location-data-on-its-tens-of-millions-of-user>, 18.12.2021.
- Kerov, Zubritski Mitropolski: **Kapitalist Toplum**, çev. Sevim Belli, 10. bs, Ankara, Sol Yayınları, 2014
- Khatibloo, Fatemeh: “Q&A: What Marketers Need To Know About Zero-Party Data”, **Forrester**, 2018, (Çevrimiçi) <https://www.forrester.com/report/QA-What-Marketers-Need-To-Know-About-ZeroParty-Data/RES145095>, 27.12.2021.
- Kıyan, Zafer: “Eski(meyen) Bir Tartışma: İzleyici Metası”, **Akdeniz Üniversitesi İletişim Fakültesi Dergisi**, No: 24, 2015, s. 230-255.
- Klous, Sander, Nart Wielaard: **We Are Big Data: The Future of the Information Society**, 1st ed. 2016 edition., New York, NY, Atlantis Press, 2016.
- Kocka, Jürgen: **Capitalism: A Short History**, Princeton, 2016.
- Koç, Serhat: “Kişisel Veri Olarak Konum Verisi(nin Korunması) ve Bu Bağlamda Karşılaşılan Hukuki Sorunlar”, **Konumsal Medya**, ed. Cemile Şahoğlu Tokgöz, Betül Aydoğan, 1. bs, İstanbul, Siyasal Kitabevi, 2020, s. 113-141.
- Kramer, Jay, Sean Hoar: “GDPR, Part I: History Of European Data Protection Law”, **Digital Insights**, (2017), (Çevrimiçi) https://lewisbrisbois.com/assets/uploads/files/GDPR,_Part_I-

History_of_European_Data_Protection_Law.pdf,
07.10.2021.

- Krishnamurthy, Balachander, Craig Wills: “On the Leakage of Personally Identifiable Information Via Online Social Networks”, **Computer Communication Review**, C. 40, 2010, s. 112-117.
- : “Privacy diffusion on the web: A longitudinal perspective”, 2009, s. 541-550, doi:10.1145/1526709.1526782.
- Kristol, David M.: “HTTP Cookies: Standards, privacy, and politics”, **ACM Transactions on Internet Technology**, C. 1, No: 2, 2001, s. 151-198.
- KVKK: “Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi”, Ankara, Kişisel Verileri Koruma Kurumu, 2019, (Çevrimiçi) <https://www.kvkk.gov.tr/Icerik/4197/Kisisel-Verilerin-Korunmasi-Kanununa-Iliskin-Uygulama-Rehberi>.
- Lace Susanne, (ed.): **The Glass Consumer: Life in a Surveillance Society**, 1st edition., Bristol, Policy Press, 2005.
- Lauer, Josh: “Plastic Surveillance: Payment Cards and the History of Transactional Data, 1888 to Present”, **Big Data & Society**, C. 7, No: 1, 2020, s. 1-14.
- : “Surveillance History and the History of New Media: An Evidential Paradigm”, **New Media & Society**, C. 14, No: 4, 2012, s. 566-582.
- Laughey, Dan: **Medya Çalışmaları Teoriler ve Yaklaşımlar**, çev. Ali Toprak, Kalkedon Yayınları, 2010.
- Law, Philip: “The Accuracy of Customer Reward Program as Loyalty Marketing Tool”, Blekinge Institute of Technology, 2008.
- Lazzarato, Maurizio: “Immaterial Labour”, **Radical Thought in Italy: A Potential Politics**, ed. Paolo Virno, Michael Hardt, ABD, University of Minnesota Press, 1996.
- Levin, Sam: “Facebook Told Advertisers It Can Identify Teens Feeling ‘insecure’ and ‘Worthless’”, **The Guardian**, (2017), blm. Technology, (Çevrimiçi) <https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens>, 11.11.2021.

- Libert, Timothy: “Exposing the Invisible Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites”, **International Journal of Communication**, C. 9, No: 0, 2015, s. 18.
- Litman-Navarro, Kevin: “Opinion | We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.”, **The New York Times**, (2019), blm. Opinion, (Çevrimiçi)
<https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>,
<https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>, 08.11.2021.
- Liu, Peng, Chao Wang: **Computational Advertising: Market and Technologies for Internet Commercial Monetization**, 2nd Edition., CRC Press, 2020.
- Lobel, Orly: “Coase and the Platform Economy”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 2018, doi:10.2139/ssrn.3083764.
- Lokke, Eirik: **Mahremiyet Dijital Toplumda Özel Hayat**, çev. Dilek Başak, Koç Üniversitesi Yayınları, 2018.
- Lomas, Natasha: “France Fines Google \$120M and Amazon \$42M for Dropping Tracking Cookies without Consent”, **TechCrunch**, 2020, (Çevrimiçi)
<https://social.techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent/>, 04.01.2022.
- Lyon, David: **Gözetim Çalışmaları**, çev. Ali Toprak, Kalkedon Yayınları, 2013.
- : **Gözetlenen Toplum Günlük Hayatı Kontrol Etmek**, çev. Gözde Soykan, 2. bs, Kalkedon Yayınları, 2018.
- : **Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination**, 1. bs, London ; New York, Routledge, 2003.
- : **The Electronic Eye: The Rise of Surveillance Society**, Minneapolis, University of Minnesota Press, 1994.
- Mann, Steve: “‘Sousveillance’: inverse surveillance in multimedia imaging”, **Proceedings of the 12th annual ACM international conference on Multimedia**, MULTIMEDIA

- '04, New York, NY, USA, Association for Computing Machinery, 2004, s. 620-627, doi:10.1145/1027527.1027673.
- Marr, Bernard: **Veri Stratejisi**, çev. Başak Gündüz, İstanbul, MediaCat Yayınları, 2018.
- Marx, Gary T.: "Coming to terms: the kaleidoscope of privacy and surveillance", **Social Dimensions of Privacy: Interdisciplinary Perspectives**, ed. Beate Roessler, Dorota Mokrosinska, Cambridge, Cambridge University Press, 2015, s. 32-49, doi:10.1017/CBO9781107280557.003.
- : "Surveillance Studies", **International Encyclopedia of the Social & Behavioral Sciences**, Elsevier, 2015, s. 733-741, doi:10.1016/B978-0-08-097086-8.64025-4.
- : "The surveillance society: the threat of 1984-style techniques", **The Futurist**, 1985, s. 22-24.
- : "What's New About the 'New Surveillance'? Classifying for Change and Continuity.", **Surveillance & Society**, C. 1, No: 1, 2002, s. 9-29.
- Masuda, Yoneji: **The Information Society as Post-Industrial Society**, World Future Society, 1981.
- Mathiesen, Thomas: "The Viewer Society: Michel Foucault's 'Panopticon' Revisited", **Theoretical Criminology**, 1997.
- Matte, Célestin, Nataliia Bielova, Cristiana Santos: "Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework", 2020.
- Mattelart, Armand: **Gözetimin Küreselleşmesi Güvenileştirme Düzeninin Kökeni**, çev. Onur Gayretli, Kalkedon Yayınları, 2012.
- Mayer-Schönberger, Viktor, Kenneth Cukier: **Büyük Veri: Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim**, çev. Banu Erol, 1. bs, İstanbul, Paloma Yayınları, 2013.
- McGuigan, Jim: **Cool Capitalism**, Illustrated Edition., London, Pluto Press, 2009.
- Menlo Park, Calif: "Facebook Reports Fourth Quarter and Full Year 2019 Results", 29.01.2020, (Çevrimiçi) <https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Fourth-Quarter-and-Full-Year-2019-Results/default.aspx>, 11.12.2020.

- Milne, George,
Mary Culnan: “Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don’t Read) Online Privacy Notices”, **Journal of Interactive Marketing**, C. 18, 2004, s. 15-29.
- Miyazaki, Anthony D.: “Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage”, **Journal of Public Policy & Marketing**, C. 27, No: 1, 2008, s. 19-33.
- Mohanta,
Bhagyashree,
Pragyan Nanda,
Srikanta Patnaik: “Management of V.U.C.A. (Volatility, Uncertainty, Complexity and Ambiguity) Using Machine Learning Techniques in Industry 4.0 Paradigm”, **New Paradigm of Industry 4.0: Internet of Things, Big Data & Cyber Physical Systems**, ed. Srikanta Patnaik, Studies in Big Data, Cham, Springer International Publishing, 2020, s. 1-24.
- Montjoye, Yves-Alexandre De vd.: “Unique in the Crowd: The Privacy Bounds of Human Mobility”, **Scientific Reports**, C. 3, No: 1, 2013, s. 1376.
- Moore, Nick: “The information society”, Y. Courrier, World Information Report, UNESCO Reference Books, 1998.
- Morrison, Sara: “The Hidden Trackers in Your Phone, Explained”, **Vox**, 08.07.2020, (Çevrimiçi)
<https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location>, 30.07.2020.
- Moulier–Boutang, Yann: **Cognitive Capitalism**, 1. bs, Cambridge, UK, Polity Press, 2012.
- Myrstad, Finn: “Grindr hit with € 6.2 million fine in response to complaint from the Norwegian Consumer Council”, **Forbrukerrådet**, 15.12.2021, (Çevrimiçi)
<https://www.forbrukerradet.no/side/grindr-hit-with-e-6-2-million-fine-in-response-to-complaint-from-the-norwegian-consumer-council/>, 18.12.2021.
- Nesamoney, Diaz: **Personalized Digital Advertising: How Data and Technology Are Transforming How We Market**, 1st edition., Place of publication not identified, Pearson FT Press, 2017.
- Nesta - The Innovation Foundation: **Aral Balkan: Building the people’s internet**, 2018, (Çevrimiçi)
<https://www.youtube.com/watch?v=dQ4UY15uAvc>, 29.11.2020.
- Newman, Lily Hay: “Facebook Stored Millions of Passwords in Plaintext—Change Yours Now”, **Wired**, (21.03.2019), (Çevrimiçi)

- <https://www.wired.com/story/facebook-passwords-plaintext-change-yours/>, 06.11.2021.
- Nissenbaum, Helen: “Privacy as Contextual Integrity”, **Washington Law Review**, C. 79, No: 1, 2004, s. 119-157.
- Noto La Diega, Guido, Ian Walden: “Contracting for the ‘Internet of Things’: Looking into the Nest”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 01.02.2016, (Çevrimiçi) <https://papers.ssrn.com/abstract=2725913>, 10.11.2021.
- Nottingham, Mark: “The Internet is for End Users”, Request for Comments, Internet Engineering Task Force, 2020, doi:10.17487/RFC8890.
- Nouwens, Midas vd.: “Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence”, **Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems**, 2020, 1-13.
- O’Briend, Sean, Michael Kwet: “Mobile Trackers | Yale Privacy Lab”, 2017, (Çevrimiçi) <https://privacylab.yale.edu/trackers.html>, 29.11.2020.
- Olejnik, Lukasz: “Large-scale Analysis of DNS-based Tracking Evasion - broad data leaks included?”, **Security, Privacy & Tech Inquiries**, 23.02.2021, (Çevrimiçi) <http://blog.lukaszolejnik.com/large-scale-analysis-of-dns-based-tracking-evasion-broad-data-leaks-included/>, 27.12.2021.
- Oracle: “Strategic Acquisitions”, 2020, (Çevrimiçi) <https://www.oracle.com/corporate/acquisitions/>, 30.07.2020.
- Oracle Social: “Oracle Social Cloud, Social Relationship Management”, 2020, (Çevrimiçi) <http://www.oracle.com/us/products/social-relationship-mgmt-brief-1915605.pdf>, 12.12.2020.
- O’Shea, Lizzie: **Geleceğin Tarihleri**, çev. Ayşecan Ay, İstanbul, Metis Yayınları, 2021.
- Osterloh, Rick: “Nest to Join Forces with Google’s Hardware Team”, **Google**, 07.02.2018, (Çevrimiçi) <https://blog.google/inside-google/company-announcements/nest-join-forces-googles-hardware-team/>, 05.12.2020.
- Önal, Nevzat Evrim: “Marx’ın Üretken ve Üretken Olmayan Emek Ayrımının Beyaz Yakalı Emegin Kategorileştirilmesinde Önemi”, **Emek Araştırma Dergisi**, 2019, s. 134-148.

- Parr, Ben: “Collect and leverage zero-party data to personalize marketing and drive growth”, **TechCrunch**, 2021, (Çevrimiçi)
<https://social.techcrunch.com/2021/11/10/collect-and-leverage-zero-party-data-to-personalize-marketing-and-drive-growth/>, 27.12.2021.
- Peacock, Sylvia E: “How Web Tracking Changes User Agency in the Age of Big Data: The Used User”, **Big Data & Society**, C. 1, No: 2, 2014, s. 2053951714564228.
- Pecora, Vincent P.: “The Culture of Surveillance”, **Qualitative Sociology**, C. 25, No: 3, 2002, s. 345-358.
- Pedley, Paul: “Data Protection Issues for Intranets and Web Sites”, **Business Information Review**, C. 19, No: 3, 2002, s. 41-49.
- Peterson, Lisa A., Robert C. Blattberg, Paul Wang: “Database Marketing. Past, Present, and Future”, **Journal of Direct Marketing**, C. 7, No: 3, 1993, s. 27-43.
- Pietrykowski, Bruce: “Beyond the Fordist/Post-Fordist Dichotomy: Working Through ‘The Second Industrial Divide’”, **Review of Social Economy**, C. 57, No: 2, 1999, s. 177-198.
- Plaut, Victoria C., Robert P. Bartlett: “Blind Consent? A Social Psychological Investigation of Non-Readership of Click-through Agreements”, **Law and Human Behavior**, C. 36, No: 4, 2012, s. 293-311.
- Poster, Mark: “Databases as Discourse, or Electronic Interpellations”, **The Second Media Age**, 1995, 78-94.
- Price, Rob: “Facebook Just Announced It Was Hacked, and Almost 50 Million Users Have Been Affected”, **Business Insider**, 28.09.2018, (Çevrimiçi)
<https://www.businessinsider.com/facebook-security-attack-affecting-50-million-users-2018-9>, 06.11.2021.
- Privacy International: “An Unhealthy Diet of Targeted Ads: An Investigation in to How the Diet Industry Exploits Our Data”, **Privacy International**, 04.08.2021, (Çevrimiçi)
<http://privacyinternational.org/long-read/4603/unhealthy-diet-targeted-ads-investigation-how-diet-industry-exploits-our-data>, 18.12.2021.
- : “Rights of Data Subjects”, 2018, (Çevrimiçi)
<https://privacyinternational.org/sites/default/files/2018-09/Part%20of%20Data%20Subjects.pdf>.

- : “The Keys to Data Protection”, Privacy International, 2018, (Çevrimiçi)
<https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf>.
- : “Your mental health for sale: How websites about depression share data with advertisers and leak depression test results”, 09.2019, (Çevrimiçi)
<https://privacyinternational.org/campaigns/your-mental-health-sale>, 04.05.2020.
- Prodnik, Jernej: “Sürüp Giden Metalaştırma Süreçleri Üzerine Bir Not: İzleyici Metasından Toplumsal Fabrikaya”, **Marx Geri Döndü – Medya, Meta ve Sermaye Birikimi**, ed. Vincent Mosco, Christian Fuchs, çev. Zafer Kıyan, 2. bs., Ankara, Nota Bene Yayınları, 2019.
- Rainie, L., P. Hitlin: “Facebook Algorithms and Personal Data”, **Pew Research Center: Internet, Science & Tech**, 16.01.2019, (Çevrimiçi)
<https://www.pewresearch.org/internet/2019/01/16/facebook-algorithms-and-personal-data/>, 05.12.2020.
- Ritzer, George, Nathan Jurgenson: “Production, Consumption, Prosumption: The Nature of Capitalism in the Age of the Digital ‘Prosumer’”, **Journal of Consumer Culture**, 2010.
- Robinson, William I.: **A Theory of Global Capitalism: Production, Class, and State in a Transnational World**, Baltimore, Johns Hopkins University Press, 2004.
- Rocher, Luc, Julien M. Hendrickx, Yves-Alexandre De Montjoye: “Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models”, **Nature Communications**, C. 10, No: 1, 2019, s. 3069.
- Rosen, Jeffrey: **The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age**, 1st edition., USA, Random House, 2004.
- Rosenzweig, Paul: **The Surveillance State: Big Data, Freedom, and You**, Teaching Company, LLC, 2016.
- Roviaro, Nicola: “A More Private Web Can Help Businesses Grow”, **Google**, 17.12.2020, (Çevrimiçi) <https://blog.google/around-the-globe/google-europe/more-private-web-can-help-businesses-grow/>, 27.12.2021.

- Ruckenstein, Minna, Julia Granroth: “Algorithms, Advertising and the Intimacy of Surveillance”, **Journal of Cultural Economy**, C. 13, No: 1, 2019, s. 12-24.
- Saraçoğlu, Diyar: “Sömürünün Yeni ve ‘Sevimli’ Yüzü: Dijital Emek”, **Dijital Emek ve Karl Marx**, kitap editörü Christian Fuchs, çev. Tahir Emre Kalaycı, Senem Oğuz, 1. bs, Notabene Yayınları, 2015.
- Sayed, Amin: “Real-Time Bidding in Online Display Advertising”, **Marketing Science**, C. 37, No: 4, 2018, s. 553-568.
- Schneier, Bruce: “A Taxonomy of Social Networking Data”, **IEEE Security & Privacy**, C. 8, 2010, s. 88.
- Schonfeld, Erick: “Schmidt: ‘Android Adoption Is About To Explode’”, **TechCrunch**, 16.10.2009, (Çevrimiçi) <https://social.techcrunch.com/2009/10/15/schmidt-android-adoption-is-about-to-explode/>, 29.11.2020.
- Schrage, Michael: “The Internet--This Year’s Virtual Favorite for ‘Man of the Year’”, **Los Angeles Times**, 1993, (Çevrimiçi) <https://www.latimes.com/archives/la-xpm-1993-12-23-fi-4946-story.html>, 12.12.2020.
- Seals, Tara: “Ford Eyes Using Personal Data to Boost Profits”, 19.11.2018, (Çevrimiçi) <https://threatpost.com/ford-eyes-use-of-customers-personal-data-to-boost-profits/139209/>, 04.05.2020.
- Sevignani, Sebastian: **Privacy and Capitalism in the Age of Social Media**, 1. bs, New York, Routledge, 2016.
- Sharma, Lavanya: “The Rise of the Visual Surveillance to Internet of Things”, **From Visual Surveillance to Internet of Things: Technology and Applications**, ed. Lavanya Sharma, Pradeep K. Garg, Chapman and Hall/CRC, 2019, s. 3-16, doi:10.1201/9780429297922-1.
- SINTEF: **Grindr Privacy Leaks**, 2018, (Çevrimiçi), <https://github.com/SINTEF-9012/grindr-privacy-leaks>, 18.12.2021.
- Smith, Andrew, Leigh Sparks: “Making Tracks: Loyalty Cards As Consumer Surveillance”, **E - European Advances in Consumer Research**, No: 6, 2003, s. 368-373.

- Smith, Richard, M.: “The Web Bug FAQ”, 11.11.1999, (Çevrimiçi) http://web.archive.org/web/20010729060646/www.eff.org/Privacy/Marketing/web_bug.html, 28.11.2020.
- Smyrnaio, Nikos: **Internet Oligopoly: The Corporate Takeover of Our Digital World**, Bingley, UK, Emerald Publishing, 2018.
- Smythe, Dallas W.: “Communications: Blindspot of Western Marxism”, **CTheory**, C. 1, No: 3, 1977, s. 1-27.
- Smythe, Dallas W. : “On the audience commodity and its work”, ed. Meenakshi Gigi Durham, Douglas M. Kellner, **Media and cultural studies**, 1981, 230-251.
- Snowden, Edward “The Age of Mass Surveillance Will Not Last Forever”, **Wired**, (2020), (Çevrimiçi) <https://www.wired.com/story/the-age-of-mass-surveillance-will-not-last-forever/>, 01.08.2020.
- Sprague, Robert: “From Taylorism to the Omnipicon: Expanding Employee Surveillance Beyond the Workplace, 25 J. Marshall J. Computer & Info. L. 1 (2007)”, **The John Marshall Journal of Information Technology & Privacy Law**, C. 25, No: 1, 2007.
- Srnicek, Nick: **Platform Capitalism**, 1st edition., Cambridge, UK, Malden, MA, Polity, 2016.
- : “The Challenges of Platform Capitalism: Understanding the Logic of a New Business Model”, **Juncture**, C. 23, No: 4, 2017, s. 254-257.
- Stalder, Felix: “The Network Paradigm: Social Formations in the Age of Information”, **The Information Society**, C. 14, No: 4, 1998, s. 301-308.
- Staples, William G.: **Everyday Surveillance: Vigilance and Visibility in Postmodern Life**, 2nd edition., Lanham, Md, Rowman & Littlefield Publishers, 2000.
- Statista: “Digital Advertising - Worldwide | Statista Market Forecast”, **Statista**, 2020, (Çevrimiçi) <https://www.statista.com/outlook/216/100/digital-advertising/worldwide>, 30.05.2020.

- Steinfeld, Nili: “‘I agree to the terms and conditions’: (How) do users read privacy policies online? An eye-tracking experiment”, **Computers in Human Behavior**, C. 55, 2016, s. 992-1000.
- Steliac, Nela, Pop Viorel, Moisuc Diana-Aderina: “The Knowledge Society and The Information Society. The Current Situation in Romania”, **Revista Economică**, No: 1, 2012, s. 814-821.
- Story, Louise, Miguel Helft: “Google Buys DoubleClick for \$3.1 Billion (Published 2007)”, **The New York Times**, (14.04.2007), blm. Technology, (Çevrimiçi) <https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html>, 12.12.2020.
- Strong, Colin: **Humanizing Big Data: Marketing at the Meeting of Data, Social Science and Consumer Insight**, 1st Edition., London ; Philadelphia, Kogan Page, 2015.
- Subramaniam, Anushree: “What Is Big Data? | Big Data Definition | V’s of Big Data”, **Edureka**, 08.06.2018, (Çevrimiçi) <https://www.edureka.co/blog/what-is-big-data/>, 13.08.2021.
- Sütçü, Cem S., Çiğdem Aytekin: **Veri Bilimi**, 1. bs, Paloma Yayınları, 2018.
- Tanner, Adam: **What Stays in Vegas: The World of Personal Data-Lifblood of Big Business-and the End of Privacy as We Know It**, PublicAffairs, 2014.
- Tapp, Alan, Ian Whitten, Matthew Housden: **Principles of Direct, Database and Digital Marketing**, New York, 2013.
- Terranova, Tiziana: “Bedava Emek: Dijital Ekonomide Kültür Üretimi”, çev. Ergin Bulut, Ayhan Ateş, **Folklor/Edebiyat**, C. 21, No: 83, 2015, s. 343-363.
- : “Free Labor: Producing Culture for the Digital Economy”, **Social Text**, C. 18, No: 2 (63), 2000, s. 33-58.
- Tessian: “22 Biggest GDPR Fines of 2019, 2020 & 2021 (So Far) - Updated 2021”, **Tessian**, 19.11.2021, (Çevrimiçi) <https://www.tessian.com/blog/biggest-gdpr-fines-2020/>, 04.01.2022.

- Thacker, Stephen B.: “Historical Development”, **Principles and Practice of Public Health Surveillance**, ed. Lisa M. Lee vd., 3rd edition., Oxford ; New York, Oxford University Press, 2010.
- The Australian: “Facebook Targets ‘Insecure’ Kids”, 2017, (Çevrimiçi) <https://dsf.newscorpaustralia.com/theaustralian/subscription/>.
- TheTradeDesk: “Unified ID Solution 2.0 | The Trade Desk”, 2021, (Çevrimiçi) <https://www.thetradedesk.com/us/about-us/industry-initiatives/unified-id-solution-2-0>, 27.12.2021.
- Thier, Hadas: **A People’s Guide to Capitalism: An Introduction to Marxist Economics**, USA, Haymarket Books, 2020.
- Thompson, Eric: “Discover the Countries Leading in App Usage | App Annie Blog”, **App Annie**, 03.05.2017, (Çevrimiçi) <https://www.appannie.com/en/insights/market-data/global-consumer-app-usage-data/>, 29.11.2020.
- Thompson, Stuart A., Charlie Warzel: “Twelve Million Phones, One Dataset, Zero Privacy”, **The New York Times**, (2019), blm. Opinion, (Çevrimiçi) <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>, 29.11.2020.
- Toffler, Alvin: **The Third Wave**, New York, Bantam, 1984.
- : **Üçüncü Dalga**, çev. Selim Yeniçeri, 1. bs, İstanbul, Koridor Yayıncılık, 2008.
- : **Yeni Güçler Yeni Şoklar**, çev. Belkıs Çorakçı, 1. bs, İstanbul, Altın Kitapları, 1992.
- Trevisan, Martino vd.: “4 Years of EU Cookie Law: Results and Lessons Learned”, **Proceedings on Privacy Enhancing Technologies**, C. 2019, No: 2, 2019, s. 126-145.
- Trottier, D., D. Lyon: “Key Features of a Social Media Surveillance”, **The Internet and Surveillance: The Challenge of Web 2.0 and Social Media**, ed. Christian Fuchs vd., New York, Routledge, 2012, s. 89-105, (Çevrimiçi) <https://westminsterresearch.westminster.ac.uk/item/8z9q3/key-features-of-a-social-media-surveillance>, 01.12.2020.
- Tsogas, George: “The commodity form in cognitive capitalism”, **Culture and Organization**, C. 18, No: 5, 2012, s. 377-395.
- Turner, Bryan S.: **Klasik Sosyoloji**, çev. İdil Çetin, 1. bs, İstanbul, İletişim Yayınları, 2014.

- Turow, Joseph: **İzleniyoruz: Yeni Reklam Sektörünün Elindeki Kimliğimiz ve Değerimiz**, çev. Mirel Benveniste, 1. bs, İstanbul, Hil Yayınları, 2016.
- Uluk, Murat, Aral, Hande : “Hedefli Reklamcılığın Kullanıcılar Arasındaki Farkındalığı Üzerine Bir İnceleme: Facebook Örneği”, CIDA, 2018.
- UN General Assembly: “Guidelines for the Regulation of Computerized Personal Data Files”, 14.12.1990, (Çevrimiçi) <https://www.refworld.org/docid/3ddcafaac.html>, 07.10.2021.
- UNCTAD: “Digital Economy Report 2019: Value Creation and Capture: Implications for Developing Countries”, New York, United Nations Conference on Trade and Development, 2019, (Çevrimiçi) <https://doi.org/10.18356/c7dc937a-en>.
- United States Congress: **What Information Do Data Brokers Have on Consumers, and How Do They Use It?: Hearing Before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Thirteenth Congress, U.S. Government Publishing Office, 2015.**
- UpGuard: “Losing Face: Two More Cases of Third-Party Facebook App Data Exposure | UpGuard”, 03.04.2019, (Çevrimiçi) <https://www.upguard.com/breaches/facebook-user-data-leak>, 06.11.2021.
- Utz, Christine vd.: “(Un)informed Consent: Studying GDPR Consent Notices in the Field”, **Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security**, 2019, 973-990.
- Vaidhyathan, Siva: **Antisocial Media: How Facebook Disconnects Us and Undermines Democracy**, New York, NY, United States of America, Oxford University Press, 2018.
- : **The Googlization of Everything**, 1st edition., Berkeley, University of California Press, 2011.
- Vincent, David: **Mahremiyet: Kısa Bir Tarih**, çev. Deniz Cumhur Başaraner, Epos Yayınları, 2017.
- VpnMentor: “Report: Only 34% of Websites in the EU are Ready for GDPR”, **vpnMentor**, 2018, (Çevrimiçi) <https://www.vpnmentor.com/blog/report-only-34-percent-of-websites-in-the-eu-are-ready-for-gdpr/>, 04.01.2022.

- Wallerstein, Immanuel: **Tarihsel Kapitalizm ve Kapitalist Uygarlık**, çev. Necmiye Alpay, 7. bs, İstanbul, Metis Yayınları, 2016.
- Warren, Samuel D., Louis D. Brandeis: “The Right to Privacy”, **Harvard Law Review**, C. 4, No: 5, 1890, s. 193-220.
- Webster, Frank: “The Information Society Revisited”, **Handbook of New Media: Social Shaping and Consequences of ICTs**, 55 City Road, SAGE Publications, Ltd, 2002, s. 22-33, doi:10.4135/9781848608245.
- : **Theories Of Information Society**, 1st edition., London, Routledge, 2006.
- WEF: “Personal Data: The Emergence of a New Asset Class”, World Economic Forum, 2011, (Çevrimiçi) https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.
- Weller, Toni: “The Information State: A Historical Perspective on Surveillance”, Routledge, 2012, (Çevrimiçi) <https://dora.dmu.ac.uk/handle/2086/7258>, 16.05.2021.
- West, Sarah Myers: “Data Capitalism: Redefining the Logics of Surveillance and Privacy”, **Business & Society**, C. 58, No: 1, 2019, s. 20-41.
- Wheeler, Scot R.: **Architecting Experience: A Marketing Science And Digital Analytics Handbook**, 1st Edition., New Jersey, WSPC, 2015.
- Whittaker, Zack: “Oracle’s BlueKai Tracks You across the Web. That Data Spilled Online”, **TechCrunch**, 19.06.2020, (Çevrimiçi) <https://social.techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/>, 30.07.2020.
- Whotracksme: “Tracker | AddThis”, 2020b, (Çevrimiçi) <https://whotracks.me/trackers/addthis.html>, 12.12.2020.
- : “Tracker | LiveRamp”, 2020, (Çevrimiçi) <https://whotracks.me/trackers/liveramp.html>, 12.12.2020.
- Wittel, Andreas: “Sayısal Marx – Dağıtık Medyanın Ekonomi Politige Doğru”, **Marx Geri Döndü – Medya, Meta ve Sermaye Birikimi**, ed. Vincent Mosco, Christian Fuchs, çev. Özgün Dinçer, 2. bs., Ankara, Nota Bene Yayınları, 2019.
- Wrumser, Yoram: “Apps Far Outpace Browsers in US Adults’ Mobile Time Spent”, **Insider Intelligence**, 09.07.2020, (Çevrimiçi)

<https://www.emarketer.com/content/the-majority-of-americans-mobile-time-spent-takes-place-in-apps>, 29.11.2020.

- Yaylagül, Levent: **Kitle İletişim Kuramları: Egemen ve Eleştirel Yaklaşımlar**, 1. bs, Ankara, Dipnot Yayınları, 2006.
- Yurtsever, Haluk: **Orta Sınıf Efsanesi**, 1. bs., İstanbul, Yordam Kitap, 2016.
- Z. Karvalics, Laszlo: “Information Society - what is it exactly? (The meaning, history and conceptual framework of an expression)”, **Information Society: From Theory to Political Practice: Coursebook**, ed. Róbert Pintér, Macaristan, MTA Kisebbsegkutato Intezet, 2007.
- Zheng, Jan: “Designing for Nudging Is Treading towards ‘Dark Pattern’ Territory.”, **Medium**, 23.10.2018, (Çevrimiçi) <https://yawnxyz.medium.com/designing-for-nudging-is-treading-towards-dark-pattern-territory-dae4848bd1c3>, 03.11.2021.
- Zuboff, Shoshana: “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization”, SSRN Scholarly Paper, Rochester, NY, Social Science Research Network, 04.04.2015, (Çevrimiçi) <https://papers.ssrn.com/abstract=2594754>, 04.05.2020.
- : **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**, 1st edition., New York, PublicAffairs, 2019.

EKLER

Çalışmanın nicel araştırma ayağında web sitelerinde ve mobil uygulamalarda tespit edilen izleyicilerin detaylı dokümanlarına ve araştırma sırasında analiz edilen veri politikalarına aşağıdaki QR kodu vasıtasıyla erişebilirsiniz.



ÖZ GEÇMİŞ

Murat Uluk, 2014 yılında Anadolu Üniversitesi, İletişim Bilimleri Fakültesi, İletişim Tasarımı ve Yönetimi Bölümünden mezun oldu. 2018 yılında İstanbul Üniversitesi Yeni Medya ve İletişim Yönetimi Yüksek Lisans programını “*Yeni medyada ‘yalan haber’ ve hakikat sonrası çağ: Doğrulama platformu olarak Teyit.org örneği üzerine bir inceleme*” başlıklı tez çalışması ile tamamladı. 2017, 2018 ve 2019 yıllarında çeşitli vakıf üniversitelerinde misafir öğretim görevlisi olarak web tasarım derslerini yürüttü. Hâlen kurucu ortağı olduğu medya şirketinde çalışmalarına devam etmektedir.