



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Ömür TALAY

MOBİL UYGULAMA ARACILI VERİ SÖMÜRGEÇİLİĞİ: BAĞIMSIZ MOBİL
UYGULAMA GELİŞTİRİCİLERİNE YÖNELİK BİR ARAŞTIRMA

İletişim Anabilim Dalı
Doktora Tezi

Antalya, 2024



AKDENİZ ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ



Ömür TALAY

MOBİL UYGULAMA ARACILI VERİ SÖMÜRGEÇİLİĞİ: BAĞIMSIZ MOBİL
UYGULAMA GELİŞTİRİCİLERİNE YÖNELİK BİR ARAŞTIRMA

Danışman

Prof. Dr. Merih TAŞKAYA

İletişim Anabilim Dalı

Doktora Tezi

Antalya, 2024

T.C.
Akdeniz Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğüne,

Ömür TALAY'ın bu çalışması, jürimiz tarafından İletişim Anabilim Dalı Doktora Programı tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. Barış ÇOBAN (İmza)

Üye (Danışman) : Prof. Dr. Merih TAŞKAYA (İmza)

Üye : Prof. Dr. Gülseren ŞENDUR ATABEK (İmza)

Üye : Doç. Dr. Tülin SEPETCİ (İmza)

Üye : Dr. Öğr. Üyesi Hediye AYDOĞAN (İmza)

Tez Başlığı: Mobil Uygulama Aracılı Veri Sömürgeciliği: Bağımsız Mobil Uygulama Geliştiricilerine Yönelik Bir Araştırma

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

Tez Savunma Tarihi : 30/01/2024

Mezuniyet Tarihi : 08/02/2024

AKADEMİK BEYAN

Doktora Tezi olarak sunduğum “Mobil Uygulama Aracılı Veri Sömürgeciliği: Bağımsız Mobil Uygulama Geliştiricilerine Yönelik Bir Araştırma” adlı bu çalışmanın, akademik kural ve etik değerlere uygun bir biçimde tarafımdan yazıldığını, yararlandığım bütün eserlerin kaynakçada gösterildiğini ve çalışma içerisinde bu eserlere atıf yapıldığını belirtir; bunu şerefimle doğrularım.

Ömür TALAY





06/02/2024

TEZ ÇALIŞMASI ORJİNALLİK RAPORU BEYAN BELGESİ

Öğrenci Bilgileri	
Adı-Soyadı	Ömür TALAY
Öğrenci Numarası	20195243004
Anabilim Dalı	İletişim
Programı	Doktora
Danışman Öğretim Üyesi Bilgileri	
Unvanı, Adı-Soyadı	Prof. Dr. Merih TAŞKAYA
Doktora Tez Başlığı	Mobil Uygulama Aracılı Veri Sömürgeciliği: Bağımsız Mobil Uygulama Geliştiricilerine Yönelik Bir Araştırma
Turnitin Bilgileri	
Ödev Numarası	2288104102
Rapor Tarihi	06/02/2024
Benzerlik Oranı	Alıntılar hariç: %5 Alıntılar dahil: %15
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE, Yukarıda bilgileri bulunan öğrenciye ait tez çalışmasının a) Kapak sayfası, b) Giriş, c) Ana Bölümler ve d) Sonuç kısımlarından oluşan toplam 224 sayfalık kısmına ilişkin olarak Turnitin adlı intihal tespit programından Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esaslarında belirlenen filtrelemeler uygulanarak yukarıdaki detayları verilen ve ekte sunulan rapor alınmıştır. Danışman tarafından uygun olan seçenek işaretlenmelidir: (X) Benzerlik oranları belirlenen limitleri aşmıyor ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylarım. () Benzerlik oranları belirlenen limitleri aşıyor, ancak tez/dönem projesi danışmanı intihal yapılmadığı kanısında ise: Yukarıda yer alan beyanın ve ekte sunulan Tez Çalışması Orijinallik Raporunun doğruluğunu onaylar ve Uygulama Esaslarında öngörülen yüzdelik sınırlarının aşılmasına karşın, aşağıda belirtilen gerekçe ile intihal yapılmadığı kanısında olduğumu beyan ederim.	
Gerekçe:	
Benzerlik taraması yukarıda verilen ölçütlere uygun olarak tarafımca yapılmıştır. İlgili tezin orijinallik raporunun uygun olduğunu beyan ederim. Danışman Öğretim Üyesi Prof. Dr. Merih TAŞKAYA İmza	

İÇİNDEKİLER

ŞEKİLLER LİSTESİ	iii
GRAFİKLER LİSTESİ	iv
TABLolar LİSTESİ	v
KISALTMALAR LİSTESİ	vi
ÖZET	vii
SUMMARY	ix
ÖNSÖZ	xi
TEŞEKKÜR.....	xiii
GİRİŞ.....	1

BİRİNCİ BÖLÜM

GÖZETİM KAPİTALİZMİNDE AĞDAKİ VERİNİN SERMAYELEŞTİRİLMESİ

1.1. Dijital Kapitalist Düzene Doğru: Gözetim Kapitalizmi Çağı.....	21
1.2. Gözetim Kapitalizminin Anatomisi.....	25
1.2.1. Gözetim Kapitalizmine Zemin Oluşturan Unsurlar.....	26
1.2.1.1. Erişilebilir ve Kullanışlı Bilgiyi Oluşturma Çabası: Bilgiyi Organize Etme	26
1.2.1.2. Bir İletişim Stratejisi Olarak Kişiselleştirme.....	27
1.2.1.3. Davranışsal Verinin İsabet Aracı Olarak Hedefli Reklamcılık	28
1.2.2. Davranışsal Artı Değer ve Keşfi.....	29
1.2.3. Gözetim Kapitalizminin Tecimsel Kaldırıcı: Mülksüzleştirme ve Mülksüzleştirme Döngüsü.....	31
1.2.4. Gözetim Kapitalizmi ve Yönetimsel Kapitalizm Arasındaki Temel Fark	32
1.2.5. Gözetimin ve Veri Sömürüsünün Sıradanlaşması	33
1.2.6. Gözetim Kapitalizminin Getirdikleri.....	34
1.3. Dijital Ağlarda Verilerin Sermayeleştirilmesi.....	34
1.3.1. Kullanıcıları Ağlara Bağlamak	35
1.3.2. Veri Sermayedarları: Sosyal Nicelleştirme Sektörü.....	36
1.3.3. Verilerin Sermayeleştirilmesinde Emek.....	38
1.3.3.1. Maddi Olmayan Emek Üzerine	39
1.3.3.2. Dijital Ağlardaki Emek Biçimi: Kullanıcı/Ağ Emegi	42

İKİNCİ BÖLÜM

SÖMÜRGEÇİLİĞİN DİJİTAL BİR FORMU OLARAK MOBİL UYGULAMA

ARACILI VERİ SÖMÜRGEÇİLİĞİ

2.1. Dijital Dünyanın Verimli Toprakları: Kişisel Veriler ve Veri Hâkimiyetinde Sömürgeçiliğin İzleri	45
2.1.1. Sınır Tanımayan Sömürgecilik: Veri Sömürgeçiliği	48
2.1.2. Veri Sömürgeçiliğinde Büyük Verinin Önemi.....	55
2.1.2.1. Veri Yığınlarının Ayıklanma Süreci ve Bir İçgörü Mekanizması Olarak Veri Madenciliği.....	56
2.1.2.2. Veri Madenciliğinin Düşünsel Tasarımı: Algoritmalar.....	59

2.2.	Mobil Uygulama Aracılı Veri Sömürgeciliği.....	60
2.2.1.	Mobil Uygulama Ekolojisi	61
2.2.1.1.	Mobil İşletim Sistemlerine Veri Gizliliği Düzleminden Bakış	63
2.2.1.2.	Dijital Dünyanın AVM'leri: Mobil Uygulama Mağazaları.....	66
2.2.1.3.	Tüketici Olmanın Ötesine Geçen Mobil Uygulama Kullanıcıları.....	68
2.2.1.4.	Bağımsız Geliştiricilerin Bağımsızlığı Üzerine.....	70
2.2.1.5.	Mobil Uygulamaların Baskın (İstilacı) Aktörleri	72
2.2.2.	Mobil Uygulamalarda Gözetim Altyapısı	74
2.2.2.1.	Mobil Uygulamaların Kimlik Tanımlayıcıları	75
2.2.2.2.	Veri Gizliliğinde Son Kale: Uygulama İzinleri.....	77
2.2.2.3.	Uygulamanın Derinliklerine Gömülen Yazılımlar: Çevrimiçi İzleyiciler.....	78
2.3.	Merkezi Uygulamalardan Merkezi Olmayan Uygulamalara.....	81
2.3.1.	Blok Zinciri Teknolojisi	81
2.3.2.	Blok Zincirinde Gizlilik ve Güvenlik.....	83
2.3.3.	Merkezi Olmayan Organizasyonlar	86
2.3.4.	Merkezi Olmayan Uygulamalar	87

ÜÇÜNCÜ BÖLÜM

VERİ SÖMÜRGEÇİLİĞİ VE VERİ GÖZETİMİ EKSENİNDE BAĞIMSIZ MOBİL UYGULAMA GELİŞTİRİCİLERİNE YÖNELİK SAHA ÇALIŞMASI

3.1.	Araştırmanın Yöntemi	90
3.1.1.	Görüşme Protokolü.....	92
3.1.2.	Veri Toplama ve Analiz Süreci	95
3.1.3.	Araştırmanın Kısıtları	95
3.1.4.	Araştırma Soruları	96
3.2.	Araştırmanın Bulguları	96
3.2.1.	Saha Gözlemleri	97
3.2.2.	Apple ve Google'ın Gizlilik Politikası Belgelerine İlişkin Doküman Analizi.....	98
3.2.3.	Derinlemesine Görüşmelerden Elde Edilen Katılımcı İfadelerinin Tematik Analizi.....	106
3.2.3.1.	Katılımcıların Kişisel Veri ve Veri Bağlantılı Süreçlere İlişkin İfadelerinin Analizi.....	108
3.2.3.2.	Katılımcıların Mobil Uygulamalarda Gizlilik, Güvenlik ve Gözetime İlişkin Yaklaşımlarının Analizi	127
3.2.3.3.	Katılımcıların Veri Gözetimine Karşı (Mukavemet) Tepki Hamlelerinin Analizi.....	149
3.2.3.4.	Katılımcıların Deneyimleri Perspektifinden Kullanıcılara Mukavemet Önerilerinin Analizi.....	158
	DEĞERLENDİRME VE SONUÇ	169
	KAYNAKLAR.....	179
	EK 1- MAXQDA KOD SİSTEMİ.....	205
	ÖZGEÇMİŞ.....	206

ŞEKİLLER LİSTESİ

Şekil 3.1 Apple’ın Topladığı Veri Türleri - Hiyerarşik Kod-Alt Kod Modeli	100
Şekil 3.2 Google’ın Topladığı Veri Türleri - Hiyerarşik Kod-Alt Kod Modeli	100
Şekil 3.3 Üçüncü Taraflara Veri Aktarımı - Kod Teori Modeli	101
Şekil 3.4 Kişisel Veri Tanımları ve Veri Toplama - Kod-Alt Kod-Bölümler Modeli	102
Şekil 3.5 Veri Toplama Yöntem ve Yazılımları - Kod Teori Modeli	103
Şekil 3.6 Yasal Yükümlülükler - Kod-Alt Kod-Bölümler Modeli	104
Şekil 3.7 Kişisel Veri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası	109
Şekil 3.8 Veriye Atfedilen Değer - Kod Teori Modeli	111
Şekil 3.9 Gizlilik - Kod-Alt-Kod-Bölümler Modeli	113
Şekil 3.10 Veri Toplama ve Gözetim - Kod-Alt-Kod-Bölümler Modeli	120
Şekil 3.11 Reklam ve Kişiselleştirme - Kod Teori Modeli	123
Şekil 3.12 İstilacı Şirketler - Kod-Alt-Kod-Bölümler Modeli	127
Şekil 3.13 Uygulama Ekosistemi Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası	129
Şekil 3.14 İşletim Sistemi Veri Toplama İlişkileri - Kod-Alt Kod-Bölümler Modeli	134
Şekil 3.15 Google - Apple Gizlilik ve Gözetim Bağları - Kod-Alt-Kod-Bölümler Modeli...	141
Şekil 3.16 Blok Zinciri - Kod-Alt-Kod-Bölümler Modeli	147
Şekil 3.17 Gözetime Tepki Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası	151
Şekil 3.18 Gözetime Tepki - Kod-Alt-Kod-Bölümler Modeli	151
Şekil 3.19 Direniş Önerileri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası	160
Şekil 3.20 Direniş Önerileri - Kod-Alt-Kod-Bölümler Modeli	161
Şekil 3.21 Duygular - Kod-Alt-Kod-Bölümler Modeli	162

GRAFİKLER LİSTESİ

Grafik 3.1 Apple Gizlilik Politikası - Kelime Bulutu.....	98
Grafik 3.2 Google Gizlilik Politikası - Kelime Bulutu.....	99
Grafik 3.3 Kod Matrisi Tarayıcısı - Kategoriler.....	107
Grafik 3.4 Kişisel Veri Kategorisinde Yer Alan Temaların Kod İstatistiği	108
Grafik 3.5 Kişisel Veri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri.....	109
Grafik 3.6 Uygulama Ekosistemi Kategorisinde Yer Alan Temaların Kod İstatistiği.....	128
Grafik 3.7 Uygulama Ekosistemi Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri	128
Grafik 3.8 Gözetime Tepki Kategorisinde Yer Alan Temaların Kod İstatistiği	150
Grafik 3.9 Gözetime Tepki Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri	150
Grafik 3.10 Direniş Önerileri Kategorisinde Yer Alan Temaların Kod İstatistiği	159
Grafik 3.11 Direniş Önerileri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri	159

TABLÖLAR LİSTESİ

Tablo 3.1 Katılımcıların Kodlama ve Profil Tablosu	92
Tablo 3.2 Derinlemesine Görüşme Protokolü	93
Tablo 3.3 Kategori, Tema ve Alt Temaları Gösterir Tematik Analiz İçeriği	106



KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ADID	: Advertising ID - Reklam Kimliği
AI	: Artificial Intelligence - Yapay Zekâ
API	: Application Programming Interface - Uygulama Programlama Arayüzü
BM	: Birleşmiş Milletler
BDA	: Big Data Analytics - Büyük Veri Analizi
COPPA	: Children's Online Privacy Protection Rule - Çocukların Çevrimiçi Gizliliğini Koruma Kanunu
CPU	: Central Process Unit - Merkezi İşlem Birimi (İşlemci)
DAO	: Decentralized Autonomous Organization - Merkezi Olmayan Otonom Organizasyon
DAPP	: Decentralized Application - Merkezi Olmayan Uygulama
DAC	: Decentralized Autonomous Cooperative - Merkezi Olmayan Otonom Şirket
EİT	: Enformasyon ve İletişim Teknolojileri
EVÇ	: Eleştirel Veri Çalışmaları
MAANG	: Meta, Apple, Amazon, Netflix ve Google
ML	: Machine Learning - Makine Öğrenmesi
GAID	: Google Advertising ID - Google Reklam Kimliği
GDPR	: General Data Protection Regulation - Genel Veri Koruma Yönetmeliği
GOR	: Google Opinion Rewards
GPS	: Global Positioning System - Küresel Konum Sistemi
GPU	: Graphics Processing Unit - Grafik İşlem Birimi (Ekran Kartı)
IDFA	: Identifier for Advertisers - Reklamverenler İçin Tanımlayıcı
IMEI	: International Mobile Equipment Identity - Uluslararası Mobil Cihaz Kimliği
IMSI	: International Mobile Subscriber Identity - Uluslararası Mobil Abone Kimliği
IOS	: Iphone Operating System - Iphone İşletim Sistemi
KVKK	: Kişisel Verilerin Korunması Kanunu
NFT	: Non-Fungible Token - Nitelikli Fikri Tapu
PDA	: Personal Digital Assistant - Cep Bilgisayarı
P2P	: Peer-to-Peer - Eşten Eşe
SDK	: Software Development Kit - Yazılım Geliştirme Kiti
WI-FI	: Wireless Fidelity - Kablosuz Bağlantı Alanı

ÖZET

İçinde bulunduğumuz dijital medya ortamında dijital veriye sahip olmak giderek önemli hale gelmekte, *veriye* egemen olanlar veri *gücüne* de sahip olmaktadır. Bu nedenle verilere hükmetmek için kişilerin en mahrem alanlarına kadar sızmayı sağlayacak çeşitli yöntemler geliştirilmektedir. 2000’li yılların başlarından itibaren kullanımı giderek artan mobil cihazlar, teknoloji şirketleri tarafından kişilerin en yakınında konumlandırılmakta, adeta kullanıcının bir uzvu haline gelmektedir. Bu cihazların internete bağlı kalabilmeleri de işlevsellikleri için hayati öneme sahiptir ve teknolojinin tüm olanakları bunu sağlamak için seferber edilmiştir. Mobil cihazlarda çalışmak üzere tasarlanan mobil uygulamalar ise kullanıcıların gündelik hayatında önemli bir yer tutarken, her an erişilebilir olmaları ve etkileşimli yapıları sayesinde kişilerin çokça tercih ettikleri, pek çok farklı amaç için kullanılabilen yazılımlar haline gelmiştir. Özetle, mobil iletişimin kilit noktasında yer alan ve kullanıcılardan veri elde etmenin aracı haline gelen mobil uygulamalara, eleştirel bir perspektifle yaklaşılması önemlidir. Araştırmanın temel problemi, sömürgeciliğin tarihsel seyrindeki hammadde peşine düşülmesine benzer biçimde doğal bir kaynak gibi görülen kullanıcı verilerinin ve dolayısıyla insan hayatının sömürüye uğratılmasıdır. Mobil uygulamaların yaratıcıları olan bağımsız geliştiriciler de bu sömürüye en yakından tanıklık etmektedirler. Bu nedenle bağımsız mobil uygulama geliştiricilerinin veri sömürüsü ve veri gözetimine karşı varsa direniş kültürlerini ortaya çıkarmak, gözetimden kaçınma stratejileri ve gözetime tepki hamlelerini araştırmak amacıyla etnografik bir araştırma yürütülmüştür. Discord, Slack ve X platformlarındaki geliştirici topluluklarında yer alan ve amaçlı örnekleme yoluyla belirlenen 11 bağımsız geliştirici ile çevrimiçi derinlemesine görüşmeler gerçekleştirilmiştir. Derinlemesine görüşmeler, MAXQDA 2020 programı üzerinde tümevarımsal kodlamaya başvurularak tematik analize tabi tutulmuştur. Ayrıca derinlemesine görüşmelerden elde edilecek bulguları desteklemek amacıyla mobil uygulamalar için en çok tercih edilen uygulama mağazalarının oluşturucuları olan Apple ve Google’ın Gizlilik Politikalarına ilişkin belgeler de yine MAXQDA 2020 programı kullanılarak doküman analizi ile incelenmiştir. Bulgular, bağımsız geliştiricilerin kişisel veri ve veri bağlantılı konular/sorunlar hakkında bilgi sahibi olduğunu gösterirken; büyük teknoloji şirketlerinin gözetim mekanizmalarına da hâkim olduklarını göstermektedir. Geliştiricilerin veri gözetimine direniş gösterdikleri, bu direniş biçiminin toplu eylemleri içermeyen, bireysel bir mukavemet şeklinde olduğu ve gözetime karşı çeşitli tepki hamlelerinin bulunduğu da yine bulgular arasındadır. Alanında uzman olarak nitelendirilmesi gereken bağımsız geliştiricilerin,

gözetimden kaçınma stratejileri de sıradan kullanıcılar için uygulanabilir ve yol gösterici olarak değerlendirilmiştir.

Anahtar Kelimeler: Gözetim, Karşı-Gözetim, Veri Gözetimi, Veri Sömürgeciliği, Eleştirel Veri Çalışmaları, Veriye Dayalı Reklamcılık, Uygulama Çalışmaları.



SUMMARY
MOBILE APP-MEDIATED DATA COLONIALISM: RESEARCH ON INDIE
MOBILE APP DEVELOPERS

Within the contemporary digital media landscape, the acquisition and mastery of digital data have attained paramount significance. Those who possess the capacity to govern data also wield the potential to harness its potent influence. Consequently, diverse methodologies are being devised to infiltrate the most private domains of individuals, with the ultimate objective of asserting control over data. Mobile devices, whose ubiquity has soared since the early 2000s, are strategically positioned by technology enterprises in close proximity to users, effectively extending the individual's sphere of existence. The critique of these devices to remain tethered to the internet is paramount for their operational effectiveness, prompting the mobilization of all available technological advancements to ensure seamless connectivity. Mobile apps, designed specifically for mobile devices, have become ubiquitous fixtures in the daily lives of users. Initially conceived for specific functionalities, they have evolved into versatile software tools with extensive utility, fueled by their constant accessibility and interactive nature. This ubiquity and versatility necessitate a critical lens through which to examine their role in mobile communication, particularly their function as instruments for harnessing data. This research centers on the apprehension of user data exploitation, drawing an analogy to the historical pursuit of raw materials during colonialism. By framing user data as a valuable resource, this lens highlights concerns about the potential exploitation of human life in the context of mobile apps and underscores the need for a thorough examination of their impact and ethical implications. Indie developers, the architects of mobile apps, occupy a unique vantage point in the landscape of data colonialism. As close observers of the process, they offer valuable insights into potential resistance against dataveillance. An ethnographic study was conducted to explore this perspective, examining developers' strategies for evading surveillance and their reactions to such monitoring. Online in-depth interviews were conducted with 11 indie developers located in the developer communities on Discord, Slack and X platforms and determined through purposeful sampling. In-depth interviews were subjected to thematic analysis using inductive coding on the MAXQDA2020 program. In addition, in order to reinforce the findings from in-depth interviews, documents regarding the privacy policies of Apple and Google, the creators of the most preferred app stores for mobile apps, were also examined by document analysis using the MAXQDA 2020 program. The findings revealed a deep understanding among developers

of personal data issues and the intricate surveillance mechanisms employed by tech companies. While their resistance is evident, it currently manifests primarily at the individual level, lacking a strong collective dimension. However, the study identified diverse strategies employed by developers, showcasing their ingenuity in navigating the challenges of surveillance. These insights are not only relevant but also instructive for ordinary users. The expertise of indie developers provides valuable tools and perspectives for navigating the complex terrain of data privacy in the digital age.

Keywords: Surveillance, Counter-Surveillance, Dataveillance, Data Colonialism, Critical Data Studies, Data-Driven Advertising, App Studies.



ÖNSÖZ

Dijital veriler günümüzde, dijital dünyanın hammaddesi/yakıtı/petrolü olarak lanse edilen, bireylerin dijital ortamdaki hareketleri sonucunda ortaya çıkan bir değer olarak görülmektedir. Veriye atfedilen bu ayrıcalık, kişilerin bu değerın kaynağı olarak görülmesiyle sonuçlanmaktadır ki bu yüzden veriler, kişilerden hasat edilen/çıkarılan/toplanan bir ham madde niteliğine büründürölmektedir. Dijital verilerin bu şekilde nitelendirilmesi, veri ve ilgili kavramların literatürdeki kullanımına da yansımaktadır. Bu çalışmada her ne kadar bu yönde bir kullanım arzu edilmese de kavramların hem akademik yazında hem de piyasa aktörleri tarafından oluşturulan belgelerde bu şekilde kullanılması, tezin genelinde veri ve bağlantılı kavramların bu biçimde kullanılmasını gerektirmiştir.

Bugün veriler, dijital ortamdaki pek çok şirket için giderek daha fazla sahip olunması gereken bir meta haline gelmektedir. Bu durum, aynı zamanda veriye bağımlılığı da körüklemekte, veriye bağımlı hale gelen büyük teknoloji şirketleri, kullanıcı verilerini elde etmek için veri toplama yarışı içine girmektedir. Böylelikle kullanıcısı olduğı dijital araçlar tarafından gözetime tabi tutulan kullanıcılar, verinin üreticisi, yani şirket için değer üreten tüketici (üretketici) konumuna gelmektedir. Kullanıcıların ürettiğı veri, dijital emek sayesinde üretilmektedir ki bu emek biçimi, maddi olmayan bir emek biçimidir. Dolayısıyla verinin sömürüsü, emeğin de sömürüsüdür ve şirketler tarafından maddi değere dönüştürölmektedir. Bu bağlamda veri odaklı bu sömürü düzeni, gözetim kapitalizmi perspektifiyle tezin birinci bölümünde irdelenmiştir.

Tezin hareket noktası, bireylerin dijital verisinin üzerindeki gözetim ve sömürüdür. Ancak bu verilerin çeşitli yazılım araçlarıyla -özellikle mobil cihazlarda çalışan mobil uygulamalarla- kolaylıkla elde edilebilmesi, uygulamalara eleştirel açıdan yaklaşmayı gerektirmiştir. Bu nedenle ikinci bölümde, mobil uygulama ekolojisine ve mobil uygulama aracılı veri sömürüsü mekanizmalarına odaklanılmış, mobil uygulamaların veri sömürüsüne olanak tanıyan gözetim alt yapıları ortaya çıkarılmıştır. Ayrıca mobil uygulamalara alternatif olabilecek blok zinciri (Blockchain) tabanlı merkezi olmayan uygulamalar, kullanıcı mahremiyeti, veri gizliliğı ve güvenliğı bağlamında ilgili literatür çerçevesinde tartışılmıştır.

Eleştirel ekonomi politik ve kültürel çalışmalar yaklaşımlarının bir arada kullanıldığı çalışmada, tezin üçüncü bölümü, bir yandan bağımsız mobil uygulama geliştiricilerinin dijital verilere ve veriye sahip olma yarışına giren teknoloji şirketlerine dair ekonomi politik çıkarımlara odaklanmakta bir yandan da geliştiricilerin gözetime tepki, direniş kültürlerine ve taktiklerine yoğunlaşmaktadır. Çünkü geliştiriciler, veri gözetiminin ve sömürünün

gerçekleştirdiği mobil uygulama ekolojisinin -hem kullanıcı hem de geliştiren olarak- en önemli aktörlerindendir. Bu nedenle üçüncü bölümde geliştiricilerin mobil uygulamalar aracılığıyla gerçekleştirilen gözetimi engelleyebilecek, hafifletebilecek ya da bertaraf edebilecek strateji ve hamlelerinin varlığı araştırılmış, geliştiricilerin olası direniş biçimlerinin ortaya çıkarılması amaçlanmıştır. Ayrıca uygulamalardaki veri odaklı gözetim mekanizmaları, hem ilgili literatüre, hem belgelere hem de bağımsız geliştiricilerle gerçekleştirilen derinlemesine görüşmelerden elde edilen ifadelerle dayanılarak analiz edilmiştir. Bölüm, alanında uzman olan bağımsız geliştiricilerin görüşleri doğrultusunda, sıradan kullanıcıların dahi uygulayabileceği, veri gözetiminden korunmanın bireysel yollarına işaret eden çeşitli önlem ve önerilerle son bulmuştur.



TEŞEKKÜR

Lisans ve lisansüstü eğitim hayatım boyunca beni destekleyen, yüreklendiren ve eleştirel bakış açısı kazandıran değerli hocam, yol gösterenim ve danışmanım Prof. Dr. Merih TAŞKAYA'ya teşekkürlerimi borç bilirim. Tez izleme komitemde yer alan, değerli katkılarıyla sürekli yolumu aydınlatan Prof. Dr. Barış ÇOBAN'a, tezin araştırma ve yazım sürecinde bana her daim yardımcı olan Prof. Dr. Gülseren ŞENDUR ATABEK'e şükranlarımı sunarım. Yine lisansüstü eğitim hayatımda ve tez yazım sürecinde bir an olsun bile desteğini esirgemeyen Prof. Dr. Seçil Deren VAN HET HOF'a, daha önce tez izleme komitemde yer alan ve tezin kuramsal çerçevesi için değerli öneriler sunan Doç. Dr. Yeşim ÇELİK'e çok teşekkür ederim.

Tez savunma jürimde yer almayı kabul ederek beni onurlandıran Doç. Dr. Tülin SEPETCİ ve Dr. Öğr. Üyesi Hediye AYDOĞAN'a, Akdeniz Üniversitesi İletişim Fakültesi'ndeki çalışma arkadaşlarıma, Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü'nün değerli çalışanlarına ve tezin araştırma bölümünün oluşmasına ve olgunlaşmasına yardımcı olan tüm katılımcılara teşekkürlerimi sunarım.

Son olarak, hayatımın her döneminde en büyük destekçilerim olan, koşulsuz sevgilerini hep hissettiğim anneme, babama, kardeşlerime, kayınvalideme ve tezi benim kadar okuyan, katkı sunan, ne zaman umutsuzluğa düşsem beni o umutsuzluk sarmalından çıkararak odaklanmamı sağlayan ve motive eden sevgili eşim, Sosyolog Funda ALPASLAN TALAY'a yürekten teşekkür ederim.

Ömür TALAY

Antalya, 2024

GİRİŞ

Bu tez, faili büyük teknoloji şirketleri olan, internet kullanıcıları üzerindeki veri gözetimine ve veri sömürüsüne karşı bağımsız mobil uygulama geliştiricilerinin (indie app developers) bir direniş gösterip göstermediği sorusundan yola çıkmaktadır. Günümüzde kişisel veriler, hükümetler, işletmeler, çeşitli kurum ve kuruluşlarca karar verme, politika belirleme, strateji geliştirme, kullanıcı davranışına dayalı ürün/hizmet pazarlama veya toplumsal ihtiyaçları belirleme gibi konularda kullanılmakta ve giderek vazgeçilmez bir kaynak haline gelmektedir. Veri gücünün ve yarattığı ayrıcalıkların önemini kısa sürede kavrayan şirketler, kişisel verileri elde etmek için çeşitli yollara başvurmaktadır. Bunlardan biri veri gözetimidir ve bu gözetim türü, kullanıcıdan veri toplamanın önemli bir bileşeni haline gelmiştir. Kişiler dijital ortamdaki her hareketiyle dijital veri üretmektedir. Giderek veriye bağımlı hale gelen şirketler, bu verileri toplamak için çeşitli yazılım araçları kullanmaktadır. Bu yazılımlar arasında mobil uygulamalar da bulunmaktadır ve bu uygulamalar, veri gözetimini olanaklı kılmak yanında, yüksek miktarda kullanıcı verisini elde etme yeteneğine de sahiptir. Bu nedenle bu çalışma, mobil uygulamalara, daha da özelde mobil uygulama aracılı veri gözetimine ve veri sömürüsüne odaklanmaktadır.

Günümüzde konvansiyonel medya gücünü ellerinde bulunduranlar, dijital medya teknolojileri sayesinde mevcut güçlerini artırma ve kitleler üzerindeki hâkimiyetlerini genişletme eğilimindedirler. Bugün, özellikle dijital medyada *veri* kimde ise *güç* de onda toplanmaktadır. Bu nedenle veriye sahip olmak için kişilerin en mahrem alanlarına kadar sızmayı sağlayacak çeşitli yöntemler geliştirilmektedir. Veri sömürgeciliği bu yöntemlerden bir tanesidir ve kişisel verilere -insana ait derin bilgilere- el konulan sömürü biçimi olarak tanımlanmaktadır: Veri sömürgeciliği insan hayatının, kâr etmek uğruna girdiye dönüştürüldüğü, davranışlardan, deneyimlerden ve kişilerarası ilişkilerden değer elde edildiği bir girişimdir (Couldry ve Mejias 2022: 11). Bu girişim, veri gözetimi yoluyla dijital ortamlardaki kişilerin en kritik verilerini hedef alır ve sahiplenilen bu değerli veri sermayesinin çoğu, kimlikler, inançlar, davranışlar ve diğer kişisel bilgilerdir (Sadowski 2019: 6). Yeni bir sömürü biçimi olarak da adlandırılan bu sömürü mekanizmasını gelir elde etme modeline eklemleyen şirketlerin (özellikle mobil cihaz ve ürünlerini üreten, yazılım alanında faaliyet gösteren veya sosyal medya, dijital reklamcılık, e-ticaret vb. faaliyetlerde bulunanlar) giderek daha fazla kâr ederek büyümeleri de kaçınılmaz hale gelmektedir.

Dijital medyadaki tek sömürü, verilerin sahiplenilmesi değildir. Mobil cihazların üretiminden tüketimine ve demontajına, cihazlar üzerinde çalışan uygulamaların

geliştirilmesinden satış sonrası desteğe kadar pek çok aşamada emek sömürüsüne de rastlanmaktadır (bkz. Brophy, 2011; Brophy ve de Peuter, 2015; Dean, 2014). Buna ek olarak bu cihazları ve yazılımları kullananların aynı zamanda üreticisi/geliştiricisi için *değer* ürettiği gerçeğinden yola çıkarak aynı önemde görülen kullanıcı emeği, tezin odaklandığı önemli bir noktadır; zira pek çok araştırmacı bu konuyu çalışmalarında sıklıkla ortaya koymuş, kullanıcıların ürettiği bu değer, karşılığı ödenmemiş emeğinin sömürüsü olduğunu dile getirmiştir (bkz. Fuchs, 2010b, 2015; Scholz, 2010; Qiu 2021).

2000’li yılların başlarından itibaren kullanımı giderek artan mobil cihazlar, teknoloji şirketleri tarafından kişilerin en yakınında konumlandırılmakta, adeta kullanıcının bir uzvu haline gelmektedir. Bu cihazların internete bağlı kalabilmeleri de işlevsellikleri için hayati öneme sahiptir ve teknolojinin tüm olanakları bunu sağlamak için seferber edilmiştir. Mobil cihazlarda çalışmak üzere tasarlanan mobil uygulamalar ise kullanıcıların gündelik hayatında önemli bir yer tutarken, her an erişilebilir olmaları ve etkileşimli yapıları sayesinde kişilerin çokça tercih ettikleri, pek çok farklı amaç için (iletişim kurma, haber alma, eğlence vb.) kullanılabilen yazılımlar haline gelmiştir. Akıllı telefonların olmazsa olmazı olan bu yazılımlar, kullanıcılarının kişisel verilerini elde etme olanakları nedeniyle veri gözetimi ve sömürüsünde kritik bir noktadadır. Uygulamaların mobil iletişimde böylesine önemli bir konumda bulunması, onu yaratan geliştiricileri de önemli kılmaktadır. Bağımsız geliştiricilerin uygulamadaki gözetim ekosistemi hakkında bilgi sahibi olmaları, veri toplama sürecini yakından takip etmeleri ve pek çoğunun “istilacı şirketlerle”¹ mücadele halinde olmaları önemlidir. Bu noktada, alanında uzman olarak kabul edilebilecek bağımsız geliştiriciler (indie developers), gözetime direnebilecek ve karşı-gözetim olanaklarını da var edebilecek olan kişiler olarak görülmelidir.

Özetle, mobil iletişimin kilit noktasında yer alan ve kullanıcılardan veri toplamanın aracı haline gelen mobil uygulamalara, eleştirel bir perspektifle yaklaşılması önemlidir. Araştırmanın temel problemi, sömürgeciliğin tarihsel seyrindeki hammadde peşine düşülmesine benzer biçimde doğal bir kaynak gibi görülen kullanıcı verilerinin ve dolayısıyla insan hayatının sömürüye uğratılmasıdır. Çalışma bir yandan veri-emek-gözetim üçgeninin derinlemesine analizini sunarken, bir yandan da şirket-geliştirici arasındaki ilişkiyi/mücadeleyi ortaya koyarak iki yönlü bir çerçeve geliştirmektedir. Çalışma, hem veri

¹ Signe Sophus Lai ve Sophie Flensburg, doğa bilimlerinde sıklıkla kullanıldığı şekliyle, belirli canlı türlerinin yaşadığı çevrenin, güçlü ve hızlı bir şekilde yayılan türler tarafından istila edilerek diğer türlerin yaşam koşullarını değiştirmesine benzer bir metaforla, mobil uygulama ekosisteminde tekel olan şirketleri, “istilacı türler” olarak tanımlamaktadır (Lai ve Flensburg: 2021: 2303).

sömürüsünün ekonomi politik görünümünü ortaya koymayı hem de kültürel bağlamda gözetime karşı direniş yolları aramanın olanaklılığını sorgulamayı, böylelikle söz konusu sorunlu alana yönelik olası çözümleri tartışmaya açmayı amaçlamaktadır. Bu amaç doğrultusunda çalışmanın araştırma sürecinde katılımcıların dijital gözetim, veri gözetimi ve veri sömürüsüne yönelik yaklaşımları, uygulama geliştirme/yayınlama aşamalarında veri mahremiyeti ve gizliliği konusundaki hassasiyetleri, kişisel veri mahremiyetlerine ilişkin kaygı durumlarını ifade etme biçimlerinin nasıl olduğuna dair yanıtlar aranmıştır. Ayrıca, katılımcıların gözetime tepki ve karşı-gözetim hamlelerinin nasıl olduğuna, veri gözetimi ve veri sömürüsüne karşı nasıl bir strateji izlenmesi gerektiğine ilişkin görüşleri ilgili literatür eşliğinde incelenmiştir. İlgili literatür incelendiğinde, veri gözetimi ve veri sömürüsü bağlamında mobil uygulamalara ve bağımsız geliştiricilere odaklanan, eleştirel ekonomi politik ve kültürel incelemelerin bir arada kullanıldığı herhangi bir çalışmaya rastlanmadığından, çalışmanın alandaki bu boşluğu dolduracağı düşünülmektedir.

Dijital gözetim, son yıllarda ilgi gösterilen bir araştırma alanı olmakla birlikte birçok çalışma, ağırlıklı olarak web siteleri ve sosyal ağlarda mahremiyet endişesi, mahremiyet farkındalığı ve algıları gibi analizleri içerirken (Barnes, 2006; Dwyer vd., 2007; Goettke ve Christiana, 2007; 2015; Cecere, vd., 2017), mobil uygulamaların yaygınlaşması ile birlikte bu yazılımlara yönelik kullanıcı mahremiyeti ve veri gizliliğine odaklı çalışmalar (Wetherall vd., 2011; Shklovski vd., 2014; Almuhimedi vd., 2015; Vanryjel vd., 2017; Barth vd., 2019; Hassandoust vd., 2021; Kollnig vd., 2022; Ho vd., 2023; Hudson ve Liu, 2023; Pang vd., 2023) artış göstermiştir.

Mobil uygulamalar üzerine yapılan araştırmaların bir diğer kısmı (Chou vd., 2013; Kim, vd., 2015; Sunio ve Schmöcker, 2017; Liao ve Ho, 2021) kullanıcıların tutum ve davranışlarına odaklanmaktadır. Bu araştırmaların yanı sıra mobil pazarlama ve mobil uygulamaların işletmeler açısından faydaları üzerinde duran yönetsel çalışmalar da (Dinner vd., 2015; Dörndorfer ve Seel, 2016; Kashkeli vd., 2017; Li, 2018; Y. Zhang ve J. Zhang, 2021) bulunmaktadır. Mobil uygulamalara eleştirel açıdan yaklaşan ve uygulama çalışmaları (app studies) alanı adı altında, uygulama alt yapılarına odaklanan metodolojik çalışmalar da (Dieter vd., 2018; Dieter vd., 2019; Fagejord, 2012; Gerlitz vd., 2016; Gerlitz vd., 2019; Lai ve Flensburg, 2020) literatürde yer almaktadır. Ancak halen mobil uygulamalara ve uygulama aracılı gözetime eleştirel perspektiften yaklaşan çalışmaların (Lai ve Flensburg, 2022; Nieborg ve Helmond, 2019; Nieborg vd., 2020; Nieborg, 2021; Wagner ve Fernandez-Ardevol, 2016; Wilken vd., 2019) sınırlı olduğu görülmektedir.

Dijital gözetim alanı içerisinde yer alan veri gözetimi (dataveillance), odağını kullanıcı verileri üzerindeki gözetime yoğunlaştıran çalışmaları kapsamaktadır. Veri gözetimi, 1980’li yıllardan itibaren çeşitli amaçlarla toplanmış verilerin kullanılmasına yönelik çalışmalara konu olmuştur. Veri gözetimi kavramı, özellikle şirketlerin sosyal kontrol amacıyla veri gözetimi uygulamalarını genişletmesi ve çeşitlendirmesiyle beraber kitlesel ve bedensel gözetimden ayrılmış (bkz. Clarke, 1988), bireysel mahremiyetin ve gizliliğin araştırıldığı, şirketlerin iş modellerinde hedefe ulaşmak için verileri nasıl kullandığını sorgulayan çeşitli çalışmalara (Connolly ve McParland, 2012; Esposti, 2014; Dijck, 2014; Lupton ve Michael, 2017) konu olmuştur.

Veri sömürgeciliği (data colonialism) ise globalleşme bağlamında bilgi ve iletişim teknolojileri alanında yaşanan güç dinamiklerine ve bu alandaki eşitsizliklere atıfta bulunan Herbert Schiller (1976)’in elektronik sömürgecilik (e-colonialism) kavramına dayanmaktadır. Jim Thatcher vd. (2016), veri sömürgeciliği kavramını ilk kullanan araştırmacılardan olsa da genellikle, Nick Couldry ve Ullas A. Mejiya (bkz. 2020; 2022)’in çalışmalarına dayanılarak kavramın yaratıcılığı bu iki akademisyene atfedilmektedir. Bunun nedeni Couldry ve Mejiya’nın çalışmalarında bir “veri sömürgeciliği tezi” ortaya koymuş olmalarıdır. Öte yandan veri sömürgeciliği kavramı, verinin tüm biçimlerini sorgulayan, verilerin nasıl üretildiğini, düzenlendiğini ve bunların her türlü yaşam formlarına nasıl nüfuz ettiğini; kimlere güç verdiğini takip eden bir girişim olan (Iliadis ve Russo 2016: 2) Eleştirel Veri Çalışmaları (EVÇ) literatürü ile verimli bir şekilde bağlantı kurmuştur (Fraser, 2019: 193). Kavramın ana hatlarının çizilmesi ve daha genel bir zemine oturtulmasıyla veri sömürgeciliğine atıfta bulunan çalışmalar da (Ricaurte, 2019; Couldry ve Mejiya 2019; Couldry ve Mejiya 2020; Calzati, 2021; Viera Magalhães ve Couldry, 2021; Couldry ve Mejiya 2022; Clarke, 2023; Couldry ve Mejiya 2023; Lynch vd., 2023; Lehoué, 2023; Melo, 2023; Singh R., 2023; Taffel, 2023) nispeten artış göstermiştir.

EVÇ’nin çıkış noktası ise “büyük veri” tartışmalarıdır ve EVÇ terimi ilk olarak Craig Dalton ve Jim Thatcher tarafından kullanılmıştır. Dalton ve Thatcher’in amacı, teknolojinin *tarafsız* bir şey olmadığını, “teknolojik determinizm”² yaklaşan her düşünceden kaçınılması gerektiğini ve büyük veri etrafındaki beklentilere karşı eleştirel bir tutum geliştirilmesini belirtmektir (Hepp vd., 2022: 10). Özellikle veri gücü ve veri ilişkileri son derece karmaşık olgulardır; gelişmekte olan EVÇ alanı için önemli perspektifler açan ve eleştirel olmasını

² “Teknolojik determinizm, teknolojiyi toplumsal yaşamın merkezine koyan bir düşünce biçimi olarak gelişme, ilerleme, modernlik, demokrasi gibi temel kavram ve süreçlerin de belirleyicisi, taşıyıcısı, bir nevi motoru olarak ele alır” (Timisi, 2016: 18).

gerektiren tam da bu karmaşıklık halidir (Hepp vd., 2022: 10). Veri-yoğun alanların eleştirel olarak araştırılmasını gerektiren EVÇ, sosyal medya, uygulamalar ve internet platformlarındaki veri iktidarı sorunlarının yanında, istatistik, politika, araştırma ve örgütlenme de dâhil olmak üzere geniş bir iletişim sorgulama alanını kapsarken (Iliadis ve Russo 2016: 2-3), “... verinin tüm biçimlerini sorgulayan ve verilerin nasıl üretildiğini, düzenlendiğini ve bunların her türlü yaşam formlarına nasıl nüfus ettiğini; kimlere güç verdiğini takip eden bir girişim” (Iliadis ve Russo 2020: 2-3) olarak görülmektedir. Veri gözetimi ve veri sömürgeciliğine odaklanan çalışmalar son yıllarda literatürde yer bulsa da bu alanda eleştirel çalışmaların yetersiz kaldığı akademik çevrelerce dile getirilmektedir. Bu nedenle eleştirel veri çalışmaları çerçevesinde, veri ve gözetim odaklı konulara/sorunlara dikkat çekebilecek ve bunların çözümüne katkı sunabilecek/yol gösterebilecek daha fazla bilimsel nitelikli çalışmaya ihtiyaç duyulmaktadır.

Kavramsal Çerçeve

Teknoloji ürünleri hem ekonomik hem de kültürel ürünlerdir. Dolayısıyla bu ürünleri kullanan kişilere de iki farklı açıdan yaklaşmak gerekmektedir. Christian Fuchs (2015: 355)’a göre kullanıcılar, bir yandan teknolojik araçları satın alan ve onları kullanan tüketicilerdir: “Kullanıcılar, EİT [Enformasyon ve İletişim Teknolojileri] satın alan ve tüketen olarak çok farklı şekillerde hareket ederler. Teknoloji ürünlerini satın alırlar ve kullanırlar. Bütün bu rollerde, metalarla parayı mübadele eden tüketiciler olarak davranırlar”. Öte yandan kullanıcılar, “anlam yaratma kültürel süreci” içerisinde hareket eden sosyal varlıklardır: “Tüketim sürecinin kendisinde, kullanıcılar anlam yaratma kültürel sürecine kalkışırlar. Günlük yaşamlarında bu malların kullanımlarında çeşitli meta anlamları yaratırlar” (Fuchs, 2015: 355). Eleştirel medya ve iletişim çalışmalarında teknoloji ürünlerinin kullanıcıları, şirketler tarafından sömürülen kişiler olarak tanımlanmaktadır. Bu tanımlamanın temel nedeni kişilere ait olan verilerin -veya bağlantılı verilerin- işlenerek reklam verenlere satılması ve kullanıcının bu verilerinden kâr elde edilmesidir (Netchitailova, 2021: 4). Ancak bu sömürü ilişkisi yeni değildir ve geçmişten günümüze form değiştirerek varlığını sürdürmektedir: Dallas Smythe (2006: 130-131)’a göre “Tekelci kapitalizm altında materyal gerçeklik, nüfusun çoğunluğunun uyku dışındaki bütün zamanının iş zamanı olmasıyken” günümüz kapitalizminde, nüfusun büyük bir bölümü uyurken bile sömürülebilmekte, şirketler için ekonomik değer üretebilmektedir. Örneğin, akıllı telefonlarda çalışan uyku takip uygulamaları ile kişilerin uyku alışkanlıkları öğrenilebilmektedir. Bu veriler pazarlama şirketleri için paha biçilmez olabilir. Yani şirketler, kullanıcıların neredeyse yirmi dört saatini sömürme

kapasitesini, ürettiği teknolojik araçlar sayesinde elde etmekte, kişilere ait sömürülmeyen alan bırakmamaktadır; çünkü “Kapitalizm sınır tanımayan, kendisine konulan tüm sınırları aşma eğiliminde olan bir yapılandırmadır” (Çoban, 2016: 115).

Bağımsız geliştiriciler ise teknoloji ürünlerinin hem üreticisi hem de tüketicisi konumunda olan kişilerdir. Bağımsız geliştiriciler, büyük şirketlerin katkısı olmadan, sınırlı olanak ve sınırlı finans kaynaklarıyla çeşitli yazılım ürünleri yaratmaktadırlar. Günümüzde birçok platform, pek çoğu açık kaynak kodlu olmak üzere çeşitli geliştirici araçlarını yazılımcıların kullanımına sunmakta, böylelikle birçok geliştirici bireysel veya bir yayıncı şirket için yazılım üretebilmektedir. Öte yandan bağımsız geliştiriciler, şirketlere bağlı çalışan yazılımcılara göre projeleri üzerinde çok daha fazla kontrole sahip olmaları nedeniyle görece daha özgür olarak nitelendirilmektedirler. Geliştiricilerin herhangi bir baskıya ya da sınırlamaya maruz kalmaması yaratıcılığı artırabilmekte ve yenilikçi fikirlerin doğmasını sağlayabilmektedir. Bu durum kısmen olumludur; fakat özellikle sınırlı finansman kaynağı ve yayıncı örgütlenmesinden yoksun olmaları, geliştiriciler için bazı sorunları beraberinde getirmektedir. Örneğin çoğu geliştirici, uygulamasının tanıtımını yeterince yapamamaktadır; ayrıca uygulama mağazaları, büyük şirketlerin kontrolünde olduğu için bağımsız geliştiricilerin uygulamaları çoğunlukla görünür olamamaktadır. “Indie Game: The Movie”³ (2012: 1:09:25-1:09:41) adlı belgesel türü filmde, bağımsız bir geliştiriciye yöneltilen “Yerin önemi nedir?” sorusuna verilen yanıt görünürlüğün değerini vurgulamaktadır: “Epey önemli. Tıpkı dükkâna gidip arka tarafta bir oyun var mı diye sormak gibi; çünkü rafta yok”. Buradan anlaşılacağı üzere yazılım sektöründe görünür olmak, geliştiricilerin ekonomik olarak hedeflediği noktaya ulaşmasını sağlamaktadır. Bağımsız yazılım ne kadar görünür haldeyse geliştiricisi de o kadar görünür hale gelmektedir. Öte yandan bağımsız geliştiriciler açık kaynak yazılımlarını (open source software) sıklıkla kullanmaktadır. Böylelikle bir yandan açık kaynak kullanan sistemlerin geliştirilmesine katkıda bulunurken, diğer yandan da büyük teknoloji şirketlerinin analiz ve raporlama yazılımlarını kullanarak (Bu yazılımlar ücretsizdir ve geliştiricilere uygulamayı kullanan kişiler hakkında ayrıntılı veriler sunmaktadır.) onlara veri kaynağı sağlamaktadır. Bu nedenlerden ötürü bağımsız geliştiriciler de tıpkı kullanıcılar gibi şirketler için değer üretmektedir.

Trebor Scholz (2010: 343), sosyal medya şirketleri için çeşitli şekillerde değer ürettiğimizi öne sürer, bunlar: Reklamverenler için dikkat çekme, hizmetler ve gönüllü

³ “Indie Game: The Movie”, 2012 yılında yayınlanmış olan belgesel türünde bir film. Yönetmenleri Lisanne Pajot ve James Swirsky olan film, oyun endüstrisinde kendine yer açmaya çalışan bağımsız oyun geliştiricilerinin oyun yaratma süreçlerindeki zorlukları ele almaktadır.

çalışma, araştırmacı ve pazarlamacılar için dijital iz ve veri sağlamadır. Scholz'un işaret ettiği bu üç madde, FAANG⁴ (Facebook, Apple, Amazon, Netflix ve Google) şirketleri içinde yer alan diğer şirketler için de geçerlidir. Hatta bu şirketler tarafından sürekli yeni veri sömürüsü, yeni metalaşma alanları yaratılmaktadır. Böylelikle çokuluslu şirketler, kapitalist tüketim kültürünü, giderek farklı kültürleri etkisi altına alacak şekilde yaymaya devam etmektedir. Bu etkiyi de zamanın ve ortamın koşullarına uygun olarak geliştirdiği teknolojileri devreye sokarak ya da onları daha fonksiyonel hale getirerek elde etmektedir (Torlak, 2000: 154-155). Öte yandan kapitalistler için kritik öneme sahip bir konu da tüketicilerin tüketim eğilimlerinin bilinmesidir:

Tüketimi belirleyebilmek aynı zamanda üretimi belirleyebilmektir, bu yüzden sermayenin tüketime dair yaptığı planların riskini en aza indirmesi gerekir. Bunun başlıca yolu tüketicinin tüketim eğilimlerini öngörecektir şekilde üretim politikaları oluşturmaktadır. Dolayısıyla sermaye, tüketicinin tüketim algısını ve anlayışını yaratmak, yönlendirmek ve bunun zamansallığını belirlemek ister (Uca, 2016: 54).

Bugünün iletişim teknolojileri, “kişisel veriler” sayesinde yukarıda bahsedilen eğilimleri öğrenmeye ve bireysel davranışın şekillendirilmesine olanak sağlamaktadır. Özellikle bu verilerin akıllı telefonlar aracılığıyla rahatlıkla elde edilebilir, depolanabilir ve analiz edilebilir olmasıyla birlikte, akıllı telefon ve mobil uygulama pazarı ulus-aşırı şirketlerin hedefi haline gelmiştir. Shoshana Zuboff (2021: 11, 22), bu durumu şöyle açıklar: Endüstriyel kapitalizmde üretim araçlarına sahip olanlar bu üretim araçlarını yoğunlaştırmaya çalışırken, bugünün, yani “yeni ekonomik düzenin” piyasa oyuncuları -Zuboff’un tanımıyla ‘gözetim kapitalistleri’-, davranış şekillendirme araçlarının yoğunlaştırılmasına ağırlık vermektedir. Henry Jenkins (2021: 33) ise Amerikan medya düzeninde bu yoğunlaşmanın çelişkili olan tarafına dikkat çekmektedir:

Günümüz Amerikan medya ortamı, görünürde birbirleriyle çelişen iki trend tarafından biçimlendirilmektedir: Bu medya ortamı bir yandan, yeni medya teknolojileri üretim ve dağıtım giderlerini azaltmış, kullanılabilir dağıtım kanallarını genişletmiş ve tüketicilerin medya içeriğini arşivlemesini, açılmasını, düzenlenmesini ve yeniden dolaşıma sokmasını yeni, güçlü yollarla mümkün kılmıştır; diğer yandan ise, bir elin parmaklarını geçmeyecek sayıda çokuluslu medya

⁴ FAANG şirketleri, Amerikan menşeli büyük teknoloji şirketlerinin baş harflerinden oluşan bir kısaltmadır. Ancak Facebook, 2021 yılında şirketin adını “meta” olarak değiştirme kararı almıştır. Bu nedenle, bu kısaltma çalışmanın geri kalanında MAANG şirketleri olarak anılacaktır. Yukarıda anılan büyük şirketlerin kısaltmaları, literatürde GAFA, GAFAM, GAFA-M, şeklinde de geçmektedir (bkz. Moore and Tambini, 2018; De Bustos ve Izquierdo-Castillo, 2019; Ichiba, 2022). Kısaltmalardaki bu farklılıklar Microsoft’un büyük şirketlere dâhil edilip edilmemesinden kaynaklanmaktadır.

şirketinin eğlence endüstrisindeki tüm sektörlerle hükmetmesiyle ortaya çıkan ana akım ticari medya sahipliğinde, korkutucu bir yoğunlaşmaya yol açmıştır (Jenkins 2021: 33).

Jenkins'in bahsettiği eğlence endüstrisindeki yoğunlaşma, bu endüstri ile yakından ilişkili olan mobil uygulamalar için de geçerlidir. Bağımsız mobil uygulama geliştiriciler, geliştirdikleri uygulamaları, uygulama mağazalarında kullanıcılara sunabilse de birçok geliştirici, bu alandaki yoğunlaşmanın bir sonucu olarak projelerini öne çıkaramamakta ya da uygulamaları, çoğu zaman büyük şirketler tarafından satın alınarak (yutularak) yoğunlaşmanın bir parçası haline getirilmektedir. Ayrıca mobil uygulamaların büyük bir bölümünün ilk akıllı telefon alımında cihazlara yüklü olarak kullanıcıya sunulması da bu yoğunlaşmayı artıran nedenlerinden biridir. Bağımsız mobil uygulama geliştiriciler, uygulamalarını tanıtmaya olanağı bulamadan, büyük şirketlerin uygulamaları cihazlarda yerlerini almaktadır. Fuchs (2021c: 80)'a göre Blogger veya YouTube gibi uygulamalar kullanıcılara bedelsiz olarak sunulmaktadır. Bu uygulamalar sosyal ağ olarak işlev görmektedir ve kişilerin iletişim kurmasına olanak tanımaktadır. Google Dokümanlar, belgeler üzerinde ortak çalışmaya imkân verirken, Google Kitaplar ve Google Akademik, global olarak bilgiye/akademik bilgiye erişim sağlamaktadır. Şüphesiz bu uygulamaların insanlığa hiçbir şekilde kolaylık sağlamadığı ya da herhangi bir fayda getirmediğini söylemek yanlış olacaktır. Ancak tüm bunlar Google'ın kullanıcılarını ve onların verilerini metaya dönüştürerek artı değer elde eden, kâr amaçlı, reklam destekli ve tekeldi bir şirket olduğu gerçeğini değiştirmemektedir.

Günümüzde akıllı telefonlar gündelik iletişimin ayrılmaz bir parçası olmasına rağmen, mobil uygulamalar ve mobil uygulamaların veri toplama mekanizmaları hakkında nispeten çok az şey bilinmektedir (Lai ve Flensburg, 2020: 1). Mobil uygulamalar kullanıcılar için kimi zaman kullanışlı, kimi zaman eğlenceli, kimi zaman da büyüleyici olsa da aynı zamanda bağlayıcı araçlardır ve kişileri mobil cihazlarına bağlarlar. Yani kullanıcılar kişiselleştirilmiş, bireyselleştirilmiş ve özelleştirilmiş deneyimlere bağlanırlar (Dean, 2015: 233). Şirketler tarafından özellikle kişiselleştirilmeye çalışılan bu yazılımlar hakkında bilinen belki de en önemli gerçek, veri gözetimini ve veri sömürsünü olanaklı kılan ve kolaylaştıran teknolojik araçlardan biri olmasıdır. Mobil uygulamalar, deyim yerindeyse maden sahasına yerleştirilmiş bir sondaj aleti gibi kullanıcılarından verileri çekip çıkarmakta ve geliştiricisine aktarmaktadır. İster mobil uygulamalarla olsun ister web siteleri aracılığıyla, elde edilen tüm veriler şirketler tarafından kaydedilmekte, işlenmekte veya satılmaktadır.

Zuboff (2021)'a göre, veri gözetimi yoluyla elde edilen kullanıcı verilerinin işlenmesiyle ortaya çıkan değer, “davranışsal artı değer”dir⁵. Zuboff, son yıllarda çok kez telaffuz edilen “Hizmet bedavaysa ürün sizsiniz” ifadesine de karşı çıkar. Kullanıcıların davranışlarına ilişkin her veriyi, kişinin ürettiği hammadde olarak tanımlar ve şirketlerin çeşitli öngörülerini için kaynak oluşturduğunu öne sürer. Bu sürecin sonunda ise davranışsal öngörüler, üçüncü taraf şirketlere satılır:

Başkalarının ısrar ettiği gibi Google satışlarının “ürünü” de değiliz. Bunun yerine, Google’ın öngörü fabrikaları için hammaddelerin çıkarıldığı ve istimlak edildiği *objeleriz*. Davranışlarımızla ilgili öngörüler Google’ın ürünleridir ve bunlar bize değil, onun gerçek müşterilerine satılır. *Bizler başkalarının amaçları için araçlarız* (Zuboff, 2021: 123).

Fuchs (2021c: 73)'a göre de “Google, kullanıcı verilerinin ve aktivitelerinin ekonomik denetimini sağlar, bu sayede de kullanıcıları metalaştırır”. Google’ın kullanıcı verileri üzerindeki bu hâkimiyeti kullanıcıların sömürülmesiyle sonuçlanmaktadır: “Google, üst düzey ekonomik gözetim makinesi ve üst düzey kullanıcı sömürü makinesidir” (Fuchs, 2021: 73). Fuchs’un Google’ın kullanıcılar üzerindeki tahakkümünü betimlerken gözetim ve sömürü kavramlarını birlikte kullanması hiç de şaşırtıcı değildir. Çünkü sömürünün gerçekleştirilebilmesi için öncelikle gözetim mekanizmalarının devreye sokulması gerekmektedir.

Dijital gözetim çalışmaları akademisyeni David Lyon’un dijital araçlar için yaptığı gözetim tanımı, Zuboff ve Fuchs’un Google hakkında söylediklerinin veya başkaca diğer şirketlerin ve bu şirketlerin ürünlerini kullananların dâhil olduğu mobil uygulama gözetiminin bir özeti gibidir. Lyon (2013: 29, 31)'a göre gözetim, gözetleyen ve gözetlenenin dâhil olduğu, kişisel enformasyona odaklı sistemli bir süreçtir. Ona göre kimin kim hakkında ne bilmek istediği, bir bakıma veri meselesidir ve gözetim giderek dijital alanlarda yeni biçimler almaktadır. Lyon (1997: 69) ayrıca, teknolojinin geldiği noktada hem veri işleme maliyetlerinin düştüğünü (günümüzde özellikle algoritmalar ve yapay zekâ sayesinde) hem de veri toplama, saklama ve dağıtmanın (yine günümüzde mobil uygulamaların yükselişi, bulut bilişim ve mobil geniş bant olanaklarının artması) giderek daha uygulanabilir hale geldiğini ifade etmektedir. Ona göre bugün kullandığımız birçok dijital araç, yalnızca gözetim kapasitesini artırmakla kalmamakta, yeni gözetim türlerinin gelişmesine ya da karakterinin

⁵ Zuboff bu kavramı Marksist bağlamda kullanmamaktadır. Kavramı “behavioral surplus” olarak kullanmaktadır ki bu Marksist “artı değer” (surplus value) kavramından farklıdır. Zuboff’un kavramı, İnternet kullanıcılarının davranışsal öngörülerinin elde edilerek satılmasıyla ortaya çıkan kâr olarak tanımlanabilir.

değişmesine etki etmektedir (Lyon, 2013: 32). Global ticari amaçlı gözetim giderek dijital ortamlarda yaygınlaşırken, yeni gözetimin en önemli karakteristik özelliği haline gelmekte (Çakır, 2015: 11), veri gözetimi, verilerin sömürüsüyle sonuçlanmaktadır.

İlkel, köleci ve feodal sistemlerden, günümüz kapitalizmine gelinceye dek farklı üretim biçimleri ve ilişkileri var olmuş, zamanla bu üretim biçimleri ve ilişkileri değişime uğramıştır. Ancak yaşanan bu değişim sonucunda yeni sistemler, eski sistemleri tamamen yok etmemiştir. Örneğin, günümüzde tarihsel sömürgeciliğin izlerine rastlanmaktadır: “... sömürgeciliğin etkilerinin hissedilmeye devam ettiğini biliyoruz, çünkü yerli halklar bugün bile mülksüzleştirmeye, kültürel istilaya ve soykırıma direniyor” (Couldry ve Mejias 2022: 9). Marc Ferro (2017: 19)’ya göre “Sömürgecilik, yabancı bir toprağın işgalini, o toprağın işlenmesini ve oraya göçmenlerin yerleşmesini içerir”. Ancak tarih boyu yukarıda belirtilen sistemlerin değişim geçirmesi gibi sömürgeciliğin de evrim geçirmesine tanık olunmaktadır: “Önceleri askeri işgallere dayanan sömürgecilik ilişkisi 2. Dünya Savaşı’ndan sonra askeri egemenliğe dayalı olarak değil, ekonomik, siyasal ve kültürel yollarla üretilen sömürgecilik ilişkisine yerini bıraktı. Bu yeni düzene yeni sömürgecilik adı verilmişti” (Geray, 2016: 197). Şimdilerde ise bu yeni sömürgeciliğin adı konulmuş gibidir: Veri Sömürgeciliği. Couldry ve Mejias (2020: 15)’a göre veri sömürgeciliği, eski dünya sömürgeciliğinden farklı ve günümüze özgü yeni bir sömürgecilik formudur:

Toplumsal verinin yakalanması ve işlenmesi, veri ilişkileri adını verdiğimiz, gündelik yaşamın “doğal” bir biçimde veri akışına dönüştürülmesini garanti altına alan bir süreçten geçerek ortaya çıkar. Elde edilen sonuç, sürekli iz sürmeye dayalı ve sosyal ayrımcılık ile davranışsal etki konusunda yeni fırsatlar sunan, yeni bir toplumsal düzenden daha azı değildir. Bizim savımız, bu süreci anlayabilmenin en iyi yolunun sömürgeciliğin tarihine bakmaktan geçeceği yönündedir. Bu sebeple veri ilişkileri, tarihteki sömürgecilik anlayışının bölgeleri, kaynakları ve yönetilen insanları düzenlediği gibi; insanların veriler aracılığıyla sömürülmesini normalleştiren, yeni bir veri sömürgeciliği biçimini canlandırmaktadır. Veri sömürgeciliği, kapitalizmin yeni bir aşamasının yolunu açmaktadır: Yaşamın, sınırsız bir biçimde kapitalistleştirilmesi (Couldry ve Mejias 2020: 15).

Kişisel verilerin, sömürü tehdidinde açık durumda olmasının nedeni, bu verilere doğal bir kaynak niteliği atfedilmesidir. Verilerin ham petrol ya da değerli bir maden gibi lanse edilmesi, onu sömürmenin meşrulaştırıcı bir girişimidir: “Doğal kaynaklar, önceden de kendiliklerinden ucuz değillerdi, şimdi de değiller, ancak ‘orada öylece’ durdukları temeline dayandırılarak, onların böyle olduğunu mantıksallaştıracak, yasal ve felsefi çerçeveler oturtulmuştur” (Couldry ve Mejias 2020: 20). Buradan çıkarılacak sonuç, *orada öylece duran* neredeyse *bedelsiz* ve *elde edilmesi kolay* olan verilerin, belirli bir teknolojik yatırım

sonucunda üretilen dijital araçlarla rahatlıkla sömürülebilir hale getirildiğidir. Kaldı ki verilerin doğal kaynak olabilmesi için hali hazırda var olması gereklidir. Oysa verilerin kişiler tarafından üretilmesi gerekmektedir; kullanıcılar iletişim araçlarını kullanarak -emek sarfederek- veri üretmektedir. Kadir Cangızbay (2001: 108)'ın emeğin salt maddi emek olarak anlaşılmaması gereğini vurgulayarak belirttiği gibi “İnsan için her ‘iş’ ancak belirli bir çaba harcamak suretiyle gerçekleştirilebilir olduğuna göre, beşerî gerçekliğin (tabiî, bu arada insanın kendi beşerî boyutunun) evrensel temeli de emektir”. Yani sömürü yalnızca ürettiğimiz veriler üzerinde değil, emeğin de üzerindedir.

Günümüzde sanayi çağının yerini bilgi ekonomisinin aldığı tezini savunan kuramcılar, bu yeni ekonomi çağında eski emek biçimlerinin değiştiğini, giderek “maddi olmayan emek” biçimlerinin baskın hale geldiği yeni bir emek anlayışına ihtiyaç duyulduğunu, klasik iş ve işgücü gibi kavramların sorgulanması gerektiğini dillendirmektedir (bkz. Hardt ve Negri, 2018; Lazzarato, 2005). Michael Hardt ve Antonio Negri, fabrika işçisinin maddi emeğinin önemini yitirdiğini, artık maddi olmayan ve iletişimsel emek biçimlerinin merkezi rol oynadığını belirtir: “Artık-değer üretiminde önceleri kitlesel fabrika işçilerinin maddi emeğinin oynadığı merkezi rolü, bugün giderek daha fazla entelektüel, maddi olmayan ve iletişimsel emek gücü oynamaktadır” (Hardt ve Negri, 2018: 51). Maurizio Lazzarato (2005: 234)'ya göre de “maddi olmayan emek, ‘canlı emeğin’ gerçek bir mutasyonu olarak ortaya çıkar” ve “... kendini üretimle tüketim arasında yeni bir ilişkinin dönüm noktasında (ya da daha doğrusu ara yüzeyinde) bulur.”. Ona göre emeğin iki farklı yönü vardır:

Bir yandan, metanın “enformasyonel içeriği” bakımından, maddi olmayan emek; dolaysız emek için gerekli olan becerilerin artan şekilde sibernetik ve bilgisayar hâkimiyetine (ve yatay ve dikey iletişim) dair beceriler gerektirdiği endüstri sektörü ve üçüncü sektörlerdeki büyük şirketlerde çalışan işçilerin emek süreçlerinde gerçekleşen değişimlere doğrudan gönderme yapar. Öte yandan maddi olmayan emek metanın “kültürel içeriğini” üreten etkinlik bakımından, normalde “iş” olarak kabul edilmeyen bir dizi etkinliği içerir; diğer bir deyişle, kültürel ve sanatsal standartları, modayı, zevkleri, tüketici normlarını ve daha stratejik olarak kamuoyunu belirlemeye ve kurmaya yönelik etkinlikleri (Lazzarato, 2005: 227, 228).

Hardt ve Negri tarafından hegemonik bir emek biçimi olarak görülen maddi olmayan emek kavramı, postendüstriyelci ve postotonomcu kuramcılar tarafından iş dünyasındaki son yıllarda ortaya çıkan yeni iş alanları ve faaliyetleri tanımlamak için kullanılmaktadır. Ancak, zaman zaman izleyici emeği veya dijital emek olarak da adlandırılan bu yeni iş ve emek biçimlerini anlamada/tanımlamada yeni bir kavramsallaştırmaya gerek olmadığına, bu emek biçimlerinin Marksist diyalektik yöntem ile kavranabileceğine ilişkin eleştiriler birçok yazar

tarafından dile getirilmektedir (Koşar, 2018: 13, 21). Örneğin Sean Sayers (2018: 24), Marx'ın emek kavramının, modern dünyadaki yeni emek biçimlerinin doğasının kavranmasında halen önemli bir kavram olduğunu belirterek maddi olmayan emek kavramını reddetmektedir. Henrique Amorim, işçi sınıflarının belirli bir sektöre göre kategorize edilemeyeceğini dile getirirken, Steve Wright' da hizmet kolunun (maddi olmayan emek) maddi olan emeğin yerini aldığı iddiasına karşı çıkmakta ve dünya nüfusunun büyük bir bölümünün hâlâ bu emek türünü sürdürdüğünü ile sürmektedir (Koşar, 2018: 12-19). Şüphesiz Wright'ın vurguladığı gibi maddi emek tümüyle yok olmamış, maddi olmayan emek biçimleri de de tam olarak onun yerini almamıştır. Ancak her iki emek türünün bir arada sömürüldüğünü görmek de mümkündür. Örneğin mobil iletişim süreçlerindeki emek sömürsünü gözden kaçırmamak gerekmektedir.

Enda Brophy ve Greig de Peuter (2015: 61)'e göre akıllı telefonların üretilmesinden tüketimine kadar geçen süreçteki sömürü devresi, iletişim çalışmalarında nadiren incelenmektedir. Brophy ve de Peuter, mobil iletişimin gerçekleşebilmesi için üretilen teknolojik araçlarda bulunan sayısız emek sömürsünden altı ana emek sömürsüne dikkat çekmişlerdir. Bunlar çıkarma, montaj, tasarım, mobil çalışma, destek ve demontajdır. Sömürü devresinin izinin sürüldüğü ilk an, “çıkarma” anıdır. Bu araçlar için gerekli olan madenler ve mineraller çoğunlukla Afrika'da, işçiler tarafından, baskı altında ve yorucu çalışma koşulları altında çıkarılmaktadır ve onlara göre bu maddeler, iletişimsel kapitalizmin hammaddeleridir. Sömürü devresindeki ikinci an, emeğin üretken çıktısı, yani “montajdır” ve çoğu, Global Güney'deki fabrikalarda üretilmektedir (Brophy ve de Peuter, 2015, 62-64). Üçüncü emek sömürsü anı ise “tasarım”da gerçekleşmektedir (Brophy ve De Peuter, 2015: 67) ve mobil uygulama geliştirme, yüz binlerce kişinin istihdam edildiği bir endüstri haline gelmiştir (King, 2011). “Mobil çalışma”, akıllı telefonlar ve uygulamaları, tamamen normleştirilmiş, esnek işçinin -konumu ne olursa olsun- derhal bir vardiyaya çağrılmasına izin veren dolaşımdaki emeğin kontrolüne neden olmaktadır ve devrenin dördüncü anını oluşturur. Sömürü devresindeki beşinci an “destek”tir. Bir akıllı telefon tüketicinin eline geçtiğinde, akıllı telefon için teknik destek gerekmektedir. Mobil internete erişim için ya da diğer telekomünikasyon işlemleri için müşteri desteği de sunulmaktadır. Tüm bunlar, meşakkatli ve pahalıdır. Çözüm, çoğunlukla çağrı merkezidir ve sonuç olarak, çarpıcı derecede büyük ve son derece disiplinli bir iş gücü, panoptik ortamlarda çalıştırılmaktadır. Sömürü devresinde son olarak “demontaj” evresi bulunmaktadır. Asya bugün, elektronik montajının merkezi haline gelmiştir ve gencinden yaşlısına, elektronik atıkları demonte etmek, ateşle yakmak veya asit fiçilerine daldırmak gibi yöntemlerle değerli metalleri eski teknoloji atıklarından geri

dönüştürmek/kazanmak gibi zararlı olabilecek işlerle uğraşmaktan başka seçeneklerinin olmadığı bir senaryo olarak karşımıza çıkmaktadır (Brophy ve de Peuter, 2015, 68-73). Görüldüğü üzere dijital teknolojilerin içerisinde önemli yer tutan iletişim araçlarının geliştirilmesinden, dağıtılmasına, kullanılmasından yok edilmesine kadar yaşanan süreçteki emek sömürüsü, iletişimsel kapitalizmin çelişkili karakterini ortaya koymaktadır. İletişim araçlarının eşitliği artırdığı veya demokrasiyi derinleştirdiği yönündeki yaygın fikrin tersine, tanıdık sınıf ilişkilerini ve kapitalist şirketlerin güçlerini pekiştiren ağ bağlantılı bir ekonomiyi ortaya çıkardığı ileri sürülmektedir (Brophy ve de Peuter, 2015: 60-61; Dean, 2005: 54-55).

Jack Linchuan Qiu (2021: 207), modern sınıf ilişkilerine değinirken şirketlerin eski kölelik biçimini, dijital dünyaya uyarlama girişimine ait kritik bir soruyu görünür kılar. Bu “Modern kölelik hakkındaki bu anlayış çerçevesini dijital medya ve akıllı telefonların dünyasına doğru daha da genişletebilir miyiz?” sorusudur ve Qiu (2021: 203), dijital teknolojilerin yeni köleleştirme koşulları yarattığını iddia eder. Qiu, dijital ortamlardaki köleleştirme türüne iKölelik (iSlave)⁶ adını vermiştir ve bu kölelik türünün iki temel tarzı vardır: “Birincisi, “iKöle imalatı” ya da iKölelik üretim tarzıdır, Foxconn’daki Çinli göçmen işçiler buna örnektir. İkinci tarz, “imal edilmiş” veya tüketici tarzı iKölelik’tir, Facebook’taki serbest emek ve dijital cihazlara bağımlı olan insanlar buna örnek gösterilebilir.”. Qiu’nun birinci iKölelik tarzı (üretim tarzı kölelik) için vermiş olduğu örnek olan Foxconn, çalışma şartları ile gündeme gelmiş, Apple için elektronik ürünler üreten şirketin ağır çalışma şartları nedeniyle intihar vakaları ile karşılaştığı ve bu nedenle şirketin çalışanlarına intihar etmeyeceklerine dair sözleşme imzalatıldığı bilinmektedir.⁷

Qiu’nun iddia ettiği “imal edilmiş” bir kölelik tarzı olan tüketici tarzı kölelikte ise iKöle, teknoloji şirketlerinin ürünlerini kullanan/tüketen ve bu şirketler için değer yaratan kişilerdir. Köleliğin amacının köleleştirenlerin bedenleri olduğuna göre yeni kapitalizmin ve dijital platformdaki sömürünün hedefinde, modern kölelerin “gönüllü emeği” olduğu

⁶ iSlave, 2010 yılında uluslararası bir kampanyada Hong Kong ve İsviçre’deki emek eylemcileri tarafından icat edilen bir slogandır; Qiu bu kavramı “Goodbye iSlave: A Manifesto for Digital Abolition” isimli kitabında geliştirmiştir (Qiu, 2021: 203). Kavramın başında kullanılan “i” ise genelde internetin ilk harfi olarak bilirse de Qiu bunu Apple ürünlerine gönderme yapmak için kullanmış, bu küçük sihirli “i” (i-device) cihazın gücünden bahsetmiştir. David W. Hill (2019)’e göre de bu küçük “i” harfi damgası yalnızca Apple ürünlerini değil bireyleri de damgaladığından bahsetmektedir. Qiu kitabında damgalamadan da öte ve çok daha uç bir örnek bu cihazlara sahip olma hırısından bahsetmiştir: iPhone veya iPad gibi Apple ürünlerini satın almak için böbreklerinden birini satacak kadar ileriye giden bireyler olduğuna yer vermiştir (Qiu, 2021: 213).

⁷ BBC News, “Çinli Fabrika “İntihar Yok” Yemini İsted”, <https://www.bbcnews.com/id/wbna37354853> (erişim tarihi: 15.05.2022).

aşıkârdır. Ancak Qiu'nun kölelik kavramsallaştırmasının, kapitalist sistemdeki ücretli işçi ile çeliştiği öne sürülmektedir. Peter Goodwin (2021: 224), köleliğin tarihsel olarak farklı zamanlarda farklı biçimler aldığını, kapitalizmin gelişmesinin önemli parçalarından olduğunu kabul etse de Qiu'ya “bir köleyi işçiden veya proleterden ayıran nedir?” sorusunu yöneltir. İşçi ile köle ayrımının çoğu zaman belirsiz olduğunu söyleyen Goodwin, sorusunun cevabını şöyle verir: “Bir köle kapitaliste aittir ve (toplam emek gücüyle birlikte) alınıp satılabilir, ücretli bir işçi ise bir kapitaliste veya diğerine sattığı emek gücüne sahip olmaya devam eder. Bu ayrım, sosyal, siyasi, ekonomik ve tarihsel açıdan önemli bir ayrımdır.” der ve Qiu'nun tanımladığı gönüllü köleliğinin bir çeşit teknoloji bağımlılığını kastettiğini savunur. Goodwin'in kölelik ve işçi ayrımı elbette önemlidir. Ancak Qiu'nun gönüllü köleliği, modernizm öncesi kölelikten zaten farklıdır ve dolayısıyla yeni kapitalizmde, yeniden tanımlanmaya ihtiyacı olan bir kölelik tipidir. Qiu'nun kölelik tipi hem teknolojik araçlara bağımlı hale gelen/getirilen hem de karşılığı ödenmeyen gönüllü emeği sömürülen kişileri tanımlamaktadır.

Lazzarato (2016: 25) ise “Kölelik, tıpkı bir fabrika, bir işletme veya bir iletişim sistemi gibi, teknik veya toplumsal bir makinenin denetleme ve düzenleme tarzıdır” der ve makinesel kölelikten söz eder: “Makinesel kölelik, eski emperyal sistemlerin (Mısır, Çin, vb.) ‘insan köleliği’ rejiminin yerini alır ve dolayısıyla teknoloji tarafından desteklenen bir komuta, düzenleme ve yönetme tarzıdır, bu haliyle kapitalizmin özgünlüklerinden birini temsil eder”. Lazzarato (2016: 39), iki ayağı olan bir insan köleliği rejimine tabi kıldığımızı söylemektedir: “Bir yandan işletmelerin, iletişimin, refah devletinin ve finansın makinesel aygıtları tarafından köleleştirilir; öte yandan da bize kullanıcı, üretici, televizyon izleyicisi ve benzeriymişiz gibi roller, toplumsal ve üretime yönelik işlevler tahsis eden bir iktidar tabakalaşmasına tabi kılınırız”.

Lazzarato özellikle 1920'lerden itibaren televizyonun icadına ve reklamların yükselişine vurgu yapar ve sonrasında geliştirilen teknolojik araçların (İnternet tabanlı teknolojik ürünleri işaret etmektedir) önceki teknolojilere göre daha organize edilmiş birer makine olduğunu ileri sürer ve bu makinenin bir pazarlama aygıtı olarak işlev gördüğünü belirtir (Lazzarato, 2016: 38). Öte yandan Jodi Dean (2015: 233)'e göre mobil uygulamalar da özellikle akıllı telefonları etkili makineler haline getirmektedir. Uygulamalar kişileri cihazlarına bağladıkça, onları günlük hayatın baskılarından bir anlığına da olsa çekip çıkarmaktadır. Böylece bu bağlantı giderek daha da duygusal bir bağlantı biçimine doğru evrilmektedir. Dean, insanların sürekli geliştirilen yeni uygulamalarla daha da özgürleştiğini düşündüğünü, iş koşullarını daha rahat kontrol edebildiğini sandığını ileri sürmekte,

özgürlüğün aslında bir yanılsama olduğunu dile getirmektedir: *Aslında daha özgür değil, makinenin daha da kölesiyiz* (Dean, 2015: 233).

Kuramsal Çerçeve

Dijital medyada veriye bağımlı sömürgeci şirketlerin (iş modellerini veri analizi ve kullanımı üzerine inşa etmiş şirketler) eleştirel ekonomi politik açıdan incelenmesi, çalışma mimarisindeki ekonomik arka planın anlaşılması açısından gereklidir. Ayrıca bu sömürü ortamında, şirketlerin hedefinde yer alanların (kullanıcılar/tüketiciler/geliştiriciler) gözetime karşı davranış biçimlerinin kültürel çalışmalar ekseninde ortaya çıkarılması da çalışmanın kültürel tarafını güçlendirmektedir. Tez, bu iki gelenekten beslenen ve disiplinlerarası bir yol izleyen eleştirel veri çalışmaları çerçevesinde kuramsal temele oturtulmuştur.

Ekaterina Netchitailova (2021: 3)’nın değindiği üzere bugünün sosyal medya ürünleri, yalnızca birer şirket ürünü değildir; aynı zamanda kültürel bir formdur. Netchitailova (2021: 3)’nın Douglas Kellner (2009)’dan aktardığı üzere iletişim çalışmalarında, disiplinlerarası eleştirel bir sosyal kuramın kullanılması gerekmektedir:

Douglas Kellner (2009)’ın da eleştirel medya/kültürel çalışmalar olarak adlandırdığı yeni bir yaklaşıma ihtiyaç duyulmaktadır. Eleştirel medya/kültürel çalışmaları üretim, dağıtım ve tüketimin toplumsal ilişkileri bağlamındaki “okumaları, yorumları, eleştirileri yansıtan bir yaklaşım” olarak tanımlanabilir. Metin ve bağlamın diyalektiği ekonomi, politika, medya kültürünün sosyal ve kültürel boyutları arasındaki bağlantıları ve kavşakları bir araya getiren, çoklu veya disiplinlerarası eleştirel bir sosyal kuramı gerektirir (Netchitailova, 2021: 3).

Toby Miller (2014: 40) da aynı görüştedir: “... ekonomi politik, medya ve kültürel çalışmaların kaynaşmasına ihtiyacımız olduğunu görüyorum”. Ayrıca Lyon (1997: 68)’un da ifade ettiği gibi günümüz gözetiminin gerçekleştirilmesinde kullanılan teknolojik araçlar, “onların biçimlenmesini ve yönetilmesini sağlayan siyasi, ekonomik ve kültürel bağlamlardan ortaya çıkarlar”. Buna ilaveten Andreas Wittel (2019), medyanın toplumsal, kültürel ve politik işlevlere sahip olduğunu kabul eder ve bu kurumların aynı zamanda ekonomik çıkarlar tarafından yönlendirildiğini ekler. Dolayısıyla medya ve iletişim çalışmalarında böyle bir sosyal kuramın kullanılması, belki de çatlaklardan sızabilecek en küçük sorunları bile gözden kaçırmamamıza yardımcı olabileceği gibi, bütüncül bir şekilde farklı bakış açılarının zengin sonuçlar üretebileceği de öngörülebilir. Sonuç olarak bu tez “Eleştirel Kuram”ı dayanmaktadır. Çünkü “Eleştirel kuram, tahakküm ve sömürüyü haklı gösteren veya onaylayan tüm düşünce ve pratikleri sorgular” (Fuchs, 2014a: 148). Ayrıca eleştirel kuram veri, emek ve sömürü ilişkilerini açıklama ve analiz etme gücüne sahiptir.

Ekonomi politik, kaynakların üretim, dağıtım ve tüketim süreçlerini analiz eden bir disiplindir ve bu kaynakları hangi iktidar ilişkilerinin şekillendirdiğiyle ilgilenir (Fuchs, 2014a: 184; Mosco, 2009: 2; Wasko, 2006: 187-188). İletişiminin ekonomi politiği de “en geniş anlamda iletişim ve kapitalizm ile ilgilenir” (Wasko, 2006: 189). Bu çalışmada da mobil iletişim çerçevesinde bir sermaye biçimi olarak veri ve veri ilişkileri analiz edilmektedir. Veriyi bir sermaye biçimi olarak konumlandırmak, dijital kapitalizmin doğasının ve dinamiklerinin daha iyi analiz edilmesine yardımcı olmaktadır. “Verileştirme”⁸, sürekli sermaye birikimi ve dolaşımı mantığı tarafından yönlendirilen ekonomi politik bir rejim olarak şekillenmektedir. Verinin bir sermaye biçimi olarak çerçevelenmesi, veriden değer elde etme yollarına ve veri çıkarmanın normatif önemine ışık tutmaktadır. Çünkü bir sermaye biçimi olarak veri, yalın bilgiden daha fazlasıdır; dijital olarak kaydedilen, dijital cihazlarda işlenebilen, kolayca bir araya getirilebilen ve son derece hareketli olan ayrık bilgi parçalarıdır. Sosyal ve kültürel sermaye gibi veri sermayesi de belirli koşullar altında ekonomik sermayeye dönüştürülebilir. Veri sermayesi, verilerin toplanması, depolanması ve işlenmesine yönelik bilgi altyapısında, yani akıllı cihazlar, çevrimiçi platformlar, dijital ağlar ve sunucularında kurumsallaşmıştır (Sadowski, 2019: 2-4). Çalışmada, kullanıcılarından verileri toplamak üzere tasarlanan mobil uygulamaların ekonomi politiğine değinilmektedir. Çünkü veri gözetimi ve veri sömürüsünün anlaşılabilmesi için mobil uygulamaların alt yapılarının, uygulama pazarlarının ve veri gözetimi ile kesişen yönlerinin incelenmesi gerekmektedir. Literatürde de Apple ve Google gibi iş modelleri üzerine inşa edilmiş mobil uygulama ekosistemlerinin ekonomi politik yapılanma olarak görülmesi gerektiği yer almaktadır. Ayrıca uygulama ekosistemleri hem ekonomik hem de kültürel bakımdan giderek üzerine daha fazla çalışması gereken dijital araçlar haline gelmektedir (Spreeuwenberg ve Poell, 2012).

Mobil uygulamalar, çoğu kullanıcı için masumane bir iletişim aracı olarak görülmektedir; ancak kullanıcısının dijital cihazında deyim yerindeyse bir ajan gibi çalışmakta, kullanıcı verileri üzerindeki gözetim ve sömürünün olumsuz görüntüsünü gizlemektedir. Dolayısıyla sıradan kullanıcılar gündelik kullanımda bu olumsuzlukların farkına varamayabilirler. José van Dijck (2014: 206)’ın aktardığı üzere bazı araştırmacılar, kullanıcıların platformların gizlilik politikalarına ve gözetleme taktiklerine direnme kabiliyetini oldukça sınırlı bulmuştur. Ancak bu durum, kullanıcıların tamamının şirketlerin bu taktiklerine karşı koymadığını da göstermez. Sıradan insanlar, ekonomik, siyasi veya genel olarak kültürün her yerde etkili olan güçlerinden bağımsızlığını kazanmalarını sağlayan

⁸ Verileştirme, *her şeyin verileştirilmesi* olarak adlandırılan bir süreçte insan davranışının analiz edilebilir bir forma dönüştürülmesi anlamına gelmektedir (Mayer-Schönberger ve Cukier, 2013:93-94).

strateji ve taktikleri benimserler (De Certeau, 2005: 213). Ayrıca, gündelik hayattaki birçok alışkanlık da bir nevi taktiktir. Zayıf olanın güçlü olana karşı hileye başvurusu ya da tuzaklar kurması taktik olarak görülebilir (De Certeau, 2008: 55).

Tez, sıradan kullanıcılara göre uygulama geliştiricilerinin gözetim ve veri sömürüsüne karşı daha bilinçli ve dirençli olabileceği varsayımından hareket etse de gündelik hayatın pratiklerini de göz ardı etmemektedir. Bunun temel nedeni, bağımsız mobil uygulama geliştiricilerinin aynı zamanda uygulamaların kullanıcısı/tüketicisi olmalarıdır ve onlar da çoğu zaman gündelik hayatta çeşitli taktik ve stratejiler kullanmaktadır. Geliştiriciler, hem Michel de Certeau (2008: 48)'nın bahsettiği gibi “Günlük yaşamın ‘ayrıntılara’ eklemlenen çok sayıdaki ‘taktik’ sayesinde işleyişin yönünü saptırabilir” hem de teknik bilgilerini ya da uzmanlığını kullanarak karşı-gözetimi olanaklı kılacak koşulları yaratabilir. Sonuç olarak geliştiricilerin karşı-gözetimle ilişkin eylem modellerini anlamak demek, şirketlerin sömürü ve gözetim mekanizmalarına karşı güç dengesini tersine çevirebilecek olası direniş kültürüne ilişkin izleri de anlamak demektir.

Kültürel çalışmalar, önemli kültürel eğilimleri yakalamakta ve bazı durumlarda bunları öngörmekte çoğu zaman başarılı olmuştur. Ayrıca kültürel çalışmaların geleneksel odak noktası, kültürel metinler ve gündelik yaşam pratikleri gibi diğer kültürel temsil biçimleridir (Andrejevic vd., 2015: 380). De Certeau (2005: 214)'nin analizi de sıradan bireylerin gündelik yaşamlarını sürdürdükleri dayatılmış sistemlerin unsurlarını taktiksel olarak kullanma ve böylece kültürün kullanıcıları ve yorumlayıcıları olarak kendi eylemliliklerini gerçekleştirme biçimlerini incelemektedir. De Certeau'nun temel önermesi olan “yapmak” boyun eğdirilmiş grupların ve bireylerin, ister hakikati söylemeye yönelik çekişmeli iddiaları, ister egemen anlatıların altüst edilmesi, isterse de karşı anlatıların ifade edilmesi olsun, direniş taktiklerini başlatmak için erişebildikleri taktik malzemelerin kullanılmasını içermektedir (Jiwani, 2011: 335-349). Eşitsiz güç ilişkileri bağlamında, taktikler ve stratejiler, uygulanabilir bir kuramsal çerçeve oluşturmak için verimli bir zemin sağlamaktadır (Jiwani, 2011: 334).

Ağ bağlantılı bilgi iletişim teknolojilerinin ortaya çıkışının, karşı-gözetim pratikleri üzerinde derin bir etkisi olmuştur. Sosyal ağ sitelerinin yaygınlaşmasıyla birlikte, kullanıcıların devlet gözetim önlemlerini kolektif olarak izlemelerini ve atlatmalarını sağlayan yeni karşı-gözetim biçimleri mümkün hale gelmiştir (Wood ve Thompson, 2018: 20). Yeni ve mobil medyanın yükselişiyle birlikte De Certeau tarafından tarif edilen gözetimin etkisizleştirilmesine yönelik bireysel taktikler, teknolojik olarak dolayımlanmış karşı-gözetim topluluklarıyla desteklenmiştir. İnsan, teknoloji ve veri toplulukları olarak karşı-gözetim

toplulukları, konumlarını gerçek zamanlı olarak haritalandırarak gözetim önlemlerini etkisiz hale getirmeye çalışmaktadır (Wood ve Thompson, 2018: 34).

Gary T. Marx (2018: 19-23) da gözetime karşı on bir tepkiden bahsetmiştir. Bunlar:

Keşif hamleleri, sakınma hamleleri, bindirme hamleleri, rol değiştirme hamleleri, bozma hamleleri, engelleme hamleleri, maskeleye hamleleri, kırma hamleleri, reddetme hamleleri, iş birliği hamleleri ve karşı gözetim hamleleridir. Genel düzeyde bunlar direniş ve itaatsizlik biçimleridir.

Özellikle engelleme ve maskeleye hamlesi, internet ortamında kullanıcılar tarafından sıklıkla kullanılmaktadır. G. T. Marx (2018: 32), engelleme hamlesinin, kullanıcıların “iletişimi fiziksel olarak erişilemez veya yararsız kılmak” için kullanıldığını söylemektedir. Maskeleye hamlesi ise aynı zamanda engellemeyi içerir: “özgün enformasyon korunur, fakat gözetimin ilgilendiği kişi veya malzemenin kimlik, durum ve/veya konumuna ilişkin olarak aldatmaca içerdiği için engellenmenin ötesine geçer”. Karşı-gözetim hamlesi ise gözetime karşı yapılan atak hamlesidir. G. T. Marx (2018: 36)’a göre bu tür bir hamle, “işleri tersine çevirmeyi ve gözetim yapanları gözetlemeyi içerir”. Kimi yazarlara göre gözetim, düşmanca yapılan bir eylem olarak tanımlanmaktadır. Dolayısıyla da karşı-gözetim, düşmanca gözetimi “tespit etme ve hafifletme süreci”⁹ olarak görülmektedir. Sonuç olarak internetteki bu düşmanca gözetim, ister şirketler tarafından isterse de hükümetler tarafından gerçekleştirilsin, karşı-gözetim imkânlarını da var eder (Kadivar, 2018: 219). Foucault’nun da dediği gibi direniş hayati bir unsurdur ve iktidarın varlığı da direnişin varlığını zorunlu kılar (Jiwani, 2011: 335).

Yöntem

Tezin araştırma bölümünde, “çoklu niteliksel yöntem” kullanılmıştır. Çoklu niteliksel yöntem, karma yöntem araştırmalarından farklı olarak birden fazla türde nitel verinin toplandığı çok yöntemli bir araştırmadır (Creswell, 2014: 3). Bu yöntemin tercih edilmesinin nedeni ise insan davranışının karmaşık yapısı ve değişkenlerinin iç içe geçmiş olmasıdır (Arıkan, 2017: 21). Bu nedenle bu çalışmada nicel veri toplamak yerine birden fazla türde nitel veri toplama yöntemi tercih edilmiştir. Çünkü nitel araştırmalar, nicel yöntemlerin sınırlılığının aksine insanın davranışına odaklanmakta, onların görüş ve deneyimlerine önem vermektedir (Yıldırım ve Şimşek, 2016: 37). Araştırma, keşfedici bir yol izlemektedir. Bağımsız mobil uygulama geliştiricilerinin varsa direniş kültürünü ve gömülü halde

⁹ Burton, F. “Karşı-Gözetimin Sırları” <https://telluric.us/the-secrets-of-countersurveillance/> (erişim tarihi 05.02.2023).

bulunduğu düşünölen karşı-gözetim stratejilerini gün ışığına çıkarmayı hedeflemektedir. Bağımsız mobil uygulama geliştiricilerinin veri gözetimine ve veri sömürgeciliğine karşı bir direniş kültürü geliştirip geliştirmediğinin anlaşılabilmesi için “etnografi” deseni tercih edilmiştir: Çünkü “Doğası gereği kültür muğlaktır ve standardize edilmiş veri toplama araçları ile ölçölemez. Gözlenir, yaşanır, hissedilir” (Yıldırım ve Şimşek, 2016: 68).

Başlangıçta Netnografi (etnografinin çevrimiçi ortamlarda uygulanması) olarak tasarlanan araştırma deseninden, geliştiricilerin topluluklarda odaklanılan çalışma konuları hakkında etkileşimde bulunmadığı ve yeterince veri toplanamayacağı anlaşıldığı için vazgeçilmiştir. Bir süre gözlemlenen geliştirici topluluklarındaki etkileşimin, çoğunlukla yazılım geliştirme hakkında olduğı, geliştirme aşamasında yaşanan problemlerin çözümüne odaklanıldığı ve zaman zaman da topluluk görüşmeleri ve etkinlikleri şeklinde gerçekleştiğı görölmüştür. Bu topluluklarda geliştiricilerin sosyal yapısı veya iletişim biçimleri gibi çeşitli veriler elde edilebilse de veri sömürüsü, veri gözetimi ve karşı-gözetim gibi konuların topluluk içerisinde konuşulmadığı görölmüş, topluluk olarak hareket edilen aktivist bir direniş biçimine ait herhangi ize de rastlanmamıştır. Bu nedenle araştırma odağında bulunan verilere ulaşamayacağı gerçeğinden hareketle topluluklar, çalışma grubunun seçilmesi ve geliştiricilerle iletişim kurmak için kullanılmıştır. Topluluk gözlemlerine dayanarak bağımsız geliştiricilerle iletişime geçmenin görece zor olduğı tespit edilmiştir. Geliştiriciler, bir konu hakkında bilgi talep edilen gönderiye cevap vermekten çoğı zaman imtina etmektedir. Bazı geliştiriciler, gönderiyi paylaşan kişinin profiline baktıklarını (yazılımcı olup olmaması geri dönüşü etkilediğı düşünölmektedir) dile getirmişlerdir. Gönderideki soruyu yönelten kişi, topluluğun bir üyesiyse veya o geliştirici ile daha önce iletişim kurulmuşsa ya da gönderi etkileşim almışsa, gönderiye yanıt verme oranlarının yüksek olduğı görölmüştür. Bu nedenle topluluğa dâhil olmuş bir kullanıcıya yanıt verme oranlarının daha yüksek olacağı düşünölererek topluluklardan çıkılmamıştır. Aksine gözlemlmeye devam edilmiş, hatta bağımsız geliştiriciler özelinde bazı sorular sorulmuş (örneğin, bağımsız geliştirici kimdir?), bu sorulara da çeşitli yanıtlar alınmış ve bu yanıtlara tezde yer verilmiştir.

Araştırmanın “çalışma grubunu”¹⁰ *Bağımsız Android ve iOS Geliştiriciler* oluşturmaktadır. Araştırmada olasılıklı olmayan örneklem tercih edilmiş, araştırmanın amacına uygun olarak alanında uzman bağımsız geliştiriciler çalışma grubuna alınmıştır. Android ve iOS (iPhone Operating System) işletim sistemlerinin, mobil iletişim sistemleri pazar payını bölüşmeleri, iki farklı yazılımcı tipinin çalışma grubuna seçilmesinde etkili

¹⁰ Nitel araştırmalarda “Araştırmacı, tercihen kendisinin yabancı olduğı ve erişebildiğı bir çalışma grubu (veya bu grubu temsil eden bir birey veya bireyleri) belirlemelidir” (Creswell, 2018: 150).

olmuştur.¹¹ Ayrıca mobil oyun geliştiriciler ve mobil uygulama geliştiriciler aynı kapsamda değerlendirilmiştir; bunun nedeni ise her iki yazılım türünün de genel kategorizasyonda “uygulama” olarak değerlendirilmesidir. Veri toplama tekniği olarak yarı yapılandırılmış görüşme tekniği kullanılmıştır. Yarı yapılandırılmış görüşme formu kullanılarak katılımcılarla 40-60 dakika arasında görüşmeler gerçekleştirilmiştir. Elde edilen veriler, MAXQDA 2020 nitel veri analizi programında kodlanarak kavram haritaları (kod teori modeli ve kod alt kod bölümler modeli kullanılmıştır) çıkarılmıştır. Buna ilaveten Apple ve Google’ın gizlilik politikaları, tematik analizi desteklemek için doküman analizi ile incelenmiştir.¹²

¹¹ 2022 yılının 4. çeyreği itibarıyla dünya çapında mobil iletişim sistemlerinin pazar payında Android %71,8 ile lider konumdadır. İkinci sırada ise %27,6 ile iOS işletim sistemi bulunmaktadır. Diğer işletim sistemlerinin pazar payı ise %0,6’dır (Statista, 2023a).

¹² Araştırma bulgularını desteklemek amacıyla Apple ve Google’ın gizlilik politikalarının incelenmesinde herhangi bir çıkar çatışması bulunmamaktadır.

BİRİNCİ BÖLÜM

GÖZETİM KAPİTALİZMİNDE AĞDAKİ VERİNİN SERMAYELEŞTİRİLMESİ

Bu bölüm, endüstriyel evre sonrası kapitalizme, yani bugün *yeni kapitalizm* olarak da adlandırılan, dijital teknolojiyle aracılanmış kapitalizmin yeni bir biçimine odaklanmaktadır. Dijital ağlar etrafında toplanmış kullanıcı verilerinin şirketler tarafından nasıl sermayeleştirildiği ve kâr elde edildiği, “gözetim kapitalizmi” çerçevesinde açıklanmıştır.

1.1. Dijital Kapitalist Düzene Doğru: Gözetim Kapitalizmi Çağı

Gözetim kapitalizmi, dijital ağlara bağlı milyarlarca insanın her türden dijital ham verisinin, büyük şirketler tarafından toplanarak analiz edildiği, işlendiği ve elde edilen anlamlı verilerin pazarlama ve reklam amaçlı olarak kullanıldığı bir sistemi ifade etmektedir. Zuboff (2021: 11)’a göre gözetim kapitalizmi, “gözetim ekonomisinin temel çerçevesini oluşturan” ve aynı zamanda “insan hakları gaspına” neden olan “yeni bir ekonomik düzen”dir. Günümüz veri gözetimi çerçevesinde kişilerin kendi verileri üzerinde hâkimiyetinin bulunmaması, kullanıcıların rızasıyla (çoğunlukla zorunda bırakılarak) ya da rızası dışında elde edilen verilerinin nasıl kullandığına dair soru işaretleri, giderek daha fazla mahremiyet endişelerine neden olurken, şirketlerin davranışsal verileri kullanarak artı değer elde etmesi ve aşırı derecede güçlenmesi, eleştirilere neden olmaktadır.

Gözetim kapitalizmi, tarihsel kapitalizmin yeni bir evresini temsil etmektedir. Zuboff (2021: 27)’a göre gözetim kapitalizminin kendine özgü ve daha önceki kapitalizm türlerine benzemeyen bir yapısı bulunmaktadır ve kapitalizm tarihinde yeni bir aktördür. Bu iddia bölümün ilerleyen kısmında tartışılacaktır; ancak Zuboff’un söylemi, gözetim kapitalizminin tamamen benzersiz bir sistem olduğunu da göstermemektedir. Çünkü tarihsel açıdan bakıldığında kapitalizmin her bir evresi, kendinden önceki dönemin izlerini taşımaktadır. Bu nedenle gözetim kapitalizmi öncesine değinmek önemlidir.

Kapitalizmi ve kapitalist düzeni tanımlamak için önce tarihsel olarak kapitalizmi gözden geçirmek ve anlamak gerekmektedir (Hunt ve Lautzenheiser, 2019: 27); çünkü kapitalizm, “tarihsel bir toplumsal sistemdir” (Wallerstein, 2021: 15). Kapitalizmin tarihi, Orta Çağ toplumlarına dayanmaktadır. Kapitalizm, Orta Çağ toplumunun siyasi, ekonomik ve kültürel ortamından filizlenmiş (Zorlu, 2006: 6), daha önceleri kimse tarafından başarılamayan, kıtlık dönemlerini bitirebilecek, birçok açıdan zenginlik üreten toplumsal ve ekonomik bir düzen vaadiyle ortaya çıkmıştır (Wayne, 2006: 14-15). Oysaki kapitalizmin üretim amacı, kapitalistler için zenginlik üretmektir ve belli bir sınıfın sermaye birikimi

içindir: “Kapitalizmde bütün üretim piyasa içindir; mallar insan ihtiyaçlarını ve arzularını karşılamak için değil, kâr elde etmek için, daha fazla sermaye edinmek için üretilir” (Adorno, 2008: 14). Immanuel Wallerstein’ın tarihsel kapitalizm ve kapitalistler hakkındaki düşünceleri de dikkate değerdir:

Tarihsel kapitalizm daha ilk bakışta, bazı savunucularının öne sürmeye çalıştığı gibi “doğal” bir sistem olmak şöyle dursun, açıkça saçma bir sistemdir. Daha fazla sermaye üretmek amacıyla sermaye üretilmektedir. Kapitalistler, ayak değirmeninde daha hızlı koşmak için gitgide daha hızlı koşan beyaz fareye benziyor (Wallerstein, 2021: 39).

Kapitalizm, işte bu nedenlerden ötürü “dinamik bir iktisadi düzen”dir (Fuchs, 2014: 141) ve temel amacı, sermaye birikimini en çoklaştırmak, kendine yeni pazarlar açabilmek için kapitalist üretim ilişkilerini genişletmek ve yaygınlaştırmaktır (Başaran, 2014: 27). Bu düzen, onun özünde bulunan bazı özellikler sayesinde -ki Zuboff, bunu “kabiliyet ve esneklikler” olarak tanımlar- günümüze kadar varlığını sürdürmüştür. Zuboff (2021: 636)’a göre kapitalizm, kendini sosyal alanlarda yenileyerek, her çağa uygun form ve uygulama yeteneği sayesinde yeni servet üretme mekanizmaları bularak hayatta kalmıştır.

“Tarihsel olarak kapitalizmin yeni bir evreye girdiğine atıfta bulunan ‘yeni kapitalizm’, temel olarak sermayenin birikim ve örgütlenme biçimlerinde meydana gelen, endüstriyel üretim süreçlerindeki farklılaşmayı ifade etmektedir” (Emirgil, 2010: 224). Bugün yeni kapitalizm olarak anılan dönem “bilgi ve yeniliğe dayalı” bir kapitalizm aşamasıdır. Bilginin ve yeniliğin yaygınlaşması, dijital teknoloji aracılığıyla hız kazanmıştır. Marksist kuramcılar, tarihsel kapitalizmin bir diğer aşaması olarak gördükleri bu yeni kapitalizm analizlerine “bilgi/güç ilişkilerini ve sınıf çelişkilerini” dâhil etmektedirler. Marksist kuramcıların eleştirisindeki hareket noktası da tekno-iyimserlerin ve neoliberal görüşün, yeni kapitalizmi meşrulaştırıcı ve olumlayıcı -yeni kapitalizm, neoliberal görüş tarafından eşitsizlikleri sonlandıracak, iktisadi bunalıma son verebilecek ve demokrasiyi güçlendirebilecek bir yapı olarak görülmektedir- tutumlarıdır (Akçoraoğlu, 2019: 525, 530). Bu dönem, her ne kadar yeni bir kapitalizm evresi olarak görülse de kendinden önceki kapitalist sistemin özelliklerini bünyesinde bulundurmaktadır. Buna, sürekli kâr etme ve sermaye birikimi zorunluluğu da dâhildir. Fuchs (2021a: 143-144)’a göre de “Yirmi birinci yüzyıl kapitalizmi, on dokuzuncu yüzyıl kapitalizminden ne tamamen farklıdır ne de onunla tamamen özdeşir. Ancak bu temel yapılar yeni yol ve biçimlerde ifade edilmektedir”. Kapitalizm, her dönemin koşullarına göre (üretim tarzı, teknoloji vb.) şekil almıştır.

Bugün de kapitalizme şekil veren bazı boyutlar bulunmaktadır: “Günümüz kapitalizminde bilgi emeği, dijital iletişim teknolojileri ve enformasyon metaları önemli bir rol oynamaktadır. Dolayısıyla günümüzde kapitalizmin önemli bir boyutu olarak dijital kapitalizm veya iletişim kapitalizminden söz edilebilir” (Fuchs, 2021a: 11). Kapitalizmin yeni evresi olarak görülen bir başka yeni kapitalizm tanımlaması da “bilişsel kapitalizm”dir. Endüstriyel kapitalizmden bilişsel kapitalizme geçiş, sermaye-emek ilişkilerinde radikal bir dönüşümü beraberinde getirmiştir (Negri, 2023: 139). “Eğer sanayi çağı fiziki sermaye ve mülkiyet birikimiyle nitelendiyse, yeniçağ da enformasyon ve fikri sermaye paketleri içinde toplanmış, maddi olmayan güç biçimlerine üstünlük tanımaktadır” (Marazzi, 2014: 237). Endüstriyel kapitalizmin simgesi olarak gösterilebilecek üretim araçları tezgâhlar, buharlı makineler ve fabrikalarken, bilişsel kapitalizmde internet ve iletişim araçlarını içeren dijital teknolojilerdir (Akçoraoğlu, 2019: 538). “*Bilişsel* sıfatı, birikim sürecinin üstüne kurulduğu emek, değerlendirme kaynakları ve mülkiyet yapısının yeni doğası ile bu değişimin doğurduğu çelişkileri ortaya koyar” (Lebert ve Vercellone, 2015: 21). Bu terim, endüstriyel evre sonrası sermaye birikiminde dijital/maddi olmayan emek süreçlerinin kullanıldığı “dijital emek süreçleri”ni merkeze almakta (Peters ve Bulut, 2014: 31), “... dijital ağlarda bir araya gelen ve işbirliği yapan insanların kolektif entelektüel emeğine dayanmaktadır” (Akçoraoğlu, 2019: 538).

Günümüzün global dijital veri ekonomisinde, bireylerin dijital teknolojileri kullanmaları ve sensörlerle donatılmış fiziksel ortamlardaki hareketleri sonucunda sürekli olarak kişisel veri üretilmektedir (Lupton ve Michael, 2017: 254). Algoritmalar, yapay zekâ ve makine öğrenmesi gibi yazılım teknikleriyle güçlendirilen cihazlar giderek daha da fazla kişisel veri toplamakta ve veri işleme sürecine dâhil olmaktadır. Bir başka taraftan bakıldığında bu teknolojiler, insan hayatının birçok alanında -ekonomik, siyasi ve gündelik hayatta- onu oyun dışı bırakan kararlara imza atmaktadır. Buradaki temel problem, yukarıda bahsi geçen teknolojilerin insanların yerini almasından ziyade “karar vermeyi otomatikleştirebilme” ihtimalidir. “Sorun, algoritmaların ve makinelerin etiğe ve ahlaka sahip olmamasıdır” (Fuchs, 2021b: 83). Bu süreçler aynı şekilde davranışları da şekillendirmektedir:

Otomatikleştirilmiş makine süreçleri davranışlarımızı *bilmekle* kalmayıp onları büyük ölçüde *şekillendirir* oldu. Bu bilgiden güce yeniden yönelim ile artık *bizimle ilgili* bilgi akışını otomatikleştirmek yeterli değil; artık amaç bizi *otomatikleştirmek* (Zuboff, 2021: 21).

İnsan davranışlarını önceden öğrenmek ve onları şekillendirmek için geliştirilen yapay zekâ uygulamaları ya da makine öğrenmesi süreçleri, aslında dijital verilerin yükselişine denk düşmektedir. Veri yığınlarından çıkarılacak anlamlı verilerin ne kadar önemli olduğunun farkında varılmış ve tüm hesaplamalar verilerin işlenmesine, ayrıştırılmasına ve işe yarar hale getirilmesine yoğunlaşmıştır. Tüm bu gelişmeler, veri ilişkili bağlantılandırmalara neden olmuş; veri kapitalizmi gibi kavramların gündeme gelmesini beraberinde getirmiştir. Veri kapitalizmi, verilerin metalaştırılmasının, veriye erişimi olan ve veriyi anlamlandırma kabiliyetine sahip aktörlere doğru ağırlık kazanan ve asimetrik bir güç dağılımını mümkün kılan bir sistemdir (West, 2019:20). Veriye erişimdeki bu asimetrik güç “... dijital kapitalizmin belirli bir niteliği olan Büyük Veri Kapitalizminin ortaya çıkmasıyla sonuçlanmış”; “Büyük Veri, insan iletişiminin aktörlerini, yapılarını, sistemlerini, etkilerini, bağlamlarını ve güç yapılarını” değiştirmiştir (Fuchs ve Chandler, 2021: 15-16; Fuchs, 2021b: 75). Yine Fuchs (2021b: 81)’a göre “Büyük Veri kapitalizmi” dijital gözetimin de dâhil olduğu bir sisteme vurgu yapar ve bu tanımlamanın daha geniş bir perspektiften kapitalizmi açıkladığını iddia eder:

Büyük Veri kapitalizminin yükselişi daha geniş bir toplumsal –ekonomik, siyasi, ideolojik- bağlamda duruyor. Ekonomide, veri ve iletişim(ler) de dahil olmak üzere (neredeyse) her şeyin neoliberal biçimde metalaştırılarak özelleştirildiğine tanık olduk. Siyasi sistem içerisinde bir gözetim-endüstri kompleksi ortaya çıktı. Bu siyasi-ekonomik komplekse, gözetim teknolojilerinin suçu ve terörü tespit edip önleyeceği fikrini destekleyen bir ideoloji eşlik ediyor (Fuchs, 2021b: 81).

Fuchs’un yukarıdaki alıntısında büyük veri kapitalizmine atfettiği kapsayıcılık, giderek gözetimin meşru hale geldiği ve veri ilişkilerine dayanan bir sistemin yaratıldığı sonucu göstermektedir. Couldry ve Mejias (2022: 14)’ın görüşü de bu tespiti destekler niteliktedir: “Veri ilişkileri aracılığıyla insan yaşamı yalnızca kapitalizme ilhak edilmekle kalmaz, aynı zamanda sürekli izlemeye ve gözetime tabi olur”. Sonuç olarak tanımı ne olursa olsun bu yeni kapitalist sistemde insan hayatı sürekli gözetim altında tutulmakta, verilerine el konulan kişiler sermayenin boyunduruğu altında yaşamaktadır. Bu yeni sistem yine neoliberal görüşün özgürlük vaadini temelden sarsan ve insan hayatının özerkliğini yok eden bir görünüm sergilerken adeta sermayenin özgürlüğü için çalışmaktadır. Franco (Bifo) Berardi (2014: 110)’nin dediği gibi “Özgürlük bu ideolojinin kurucu mitidir, ama kimin özgürlüğü? Elbette sermayenin özgürlüğü”.

1.2. Gözetim Kapitalizminin Anatomisi

Gözetim kapitalizmi, iki farklı olgunun bir araya gelerek oluşturduğu ekonomik bir sistemdir. Gözetim ifadesi, geçmişte sıklıkla kamu güvenliğini sağlama veya potansiyel suçları önleme gibi unsurlarla anılırken, bugün dijitalleşme ile internet kullanıcılarını izleme ve veri gözetimi gibi unsurlarla iç içe geçen bir olgu haline gelmiştir. Gözetim kapitalizmi, dijital teknolojiler sayesinde var olmaktadır ve hareket noktası kişilerin dijital verilerinin izlenmesidir. Gözetim, eskiden beri devlet iktidarının destekleyici bir aracı olarak görülmüş ve devlet tarafından nüfusun davranışının izlenmesi, kontrol edilmesi ve denetimi için kullanılmıştır (Giddens, 1981: 5). Michel Foucault (1992: 178-252)'ya göre gözetim, toplum üzerinde bir iktidar otoritesi oluşturmaktadır. Foucault, Jeremy Bentham'ın gözetim modeli olan "Panoptikonu"¹³ denetim ve disiplinin metaforu olarak görmüş ve bunu modern iktidar biçimi ile ilişkilendirilmiştir. David Lyon (1997: 91) da panoptikonun hem devlet yönetiminde hem de tüketicilerin gözetiminde kullanıldığını ileri sürmüştür. Lyon'un panoptik gözetime tüketicileri dâhil etmesiyle gözetim için farklı bir boyut açıldığı görülebilir. Gözetim artık, giderek daha da "global bir dünyada", "akışkan" bir hal almaktadır (Bauman ve Lyon, 2016: 16).

Bilgi ve iletişim teknolojilerindeki gelişmeler, gözetim işlevi için paha biçilmez alanlar yaratmaktadır. Böylece bu teknolojilere bağımlı hale gelen toplumların da giderek gözetlenen toplumlar haline geldiği görülmektedir (Lyon, 2006: 11). Günümüzde fiziksel gözetimin yerini dijital gözetim almış bu da veri gözetimiyle sonuçlanmıştır. Lyon (2006: 64)'un da bahsettiği üzere bugün hükümet ve şirket yapıları giderek daha fazla kişisel veri toplanmasına bağımlı hale gelmektedir. Gözetim, enformasyona erişim için gereklidir:

Disiplin rejiminin aksine, sömürülenler *bedenler ve enerjiler* değil, *enformasyon ve verilerdir*. Güç/iktidar elde etmenin belirleyici faktörü, üretim araçlarına sahip olmak değil, psikopolitik izleme, davranış kontrolü ve tahmin işini kullanılan enformasyonlara erişimdir. Enformasyon rejimi, gözetim kapitalizmine dönüşen ve insanları veriye ve tüketim hayvanına indirgeyen enformasyon kapitalizmi ile bağlantılıdır (Han, 2022: 7).

Özellikle şirketler, sermaye birikiminin devamı için bilgiye ve dolayısıyla veriye muhtaç hale gelmektedir. "Bu bilginin çoğu kişisel olduğu için, kişisel veriler üzerine odaklanmış dikkat gözetimi gerektirir" (Lyon, 2006: 64). Zuboff (2021: 28, 89, 131), gözetim kapitalizminin "teknoloji aşılayan ve onun harekete geçmesi için komut veren bir mantık"

¹³ Panoptik sistem, iktidarın otomatik, bilinçli ve sürekli işlev gördüğü bir denetim halini simgeler. Ayrıca kişilerin, sürekli gözetim altında olduğu hissini içselleştirilmesini sağlar (Foucault, 1992: 252).

olduğunu ve dijital ortam olmadan hayatta kalamayacak bir “piyasa formu” olduğunu sürer. Dijital ortamlardaki dijital izlerimiz, yani dijital veriler, “gözetleme kapitalizminin yeni imalat süreçleri için gerekli olan hammaddedir”. Bu hammaddelerde gizli olan şey ise deneyimlerdir ve gözetim kapitalizminin piyasa mekanizmaları tarafından “davranışa” dönüştürülmekte ve gözetim kapitalistlerinin öngörü ürünleri için kullanılmaktadır. Böylece, hammadde olarak bireylerin davranış ve eğilimlerine ilişkin verilerin toplanmasına ve işlenmesine dayalı değer yaratmaya dayalı bir ekonomik sektör şekillenmektedir (König, 2017: 5).

1.2.1. Gözetim Kapitalizmine Zemin Oluşturan Unsurlar

Gözetim kapitalizmi bir anda ortaya çıkan bir sistem değildir. Serpilebilmesi için gerekli ortam oluşmuş ve uygun koşullarla birlikte giderek olgunlaşmıştır. Zuboff (2021: 75)’a göre gözetim kapitalizminin ortaya çıkışında, dijitalleşme başat unsurdur ve neoliberal ideoloji, bu sistem için uygun habitatı sağlamıştır. Ancak yalnızca dijitalleşme değil, dijitalleşmenin yarattığı bazı sonuçlar da bu sistemin olgunlaşma sürecine katkıda bulunmuş ve aşağıda detaylı bir şekilde açıklanmıştır.

1.2.1.1. Erişilebilir ve Kullanışlı Bilgiyi Oluşturma Çabası: Bilgiyi Organize Etme

Günümüzde bilgiye ulaşmak, onu kullanmak ve organize etmek giderek artan enformasyon nedeniyle çok daha zor bir hale gelmiştir. 2000’li yılların başlarında günümüzdeki veri akışının bu denli yoğun olacağı pek de tahmin edilememiştir. Şirketlerin bilgiye olan ilgisinin günümüz toplumlarının “bilgi toplumu”¹⁴ olduğu yönündeki söylemler ile daha da görülür olmaya başlamıştır ki Google bu ilgiyi fark eden şirketlerdendir. Google, “dünyanın bilgisini organize etme ve onu erişilebilir ve kullanışlı hale getirme” gibi bir misyonu üstlenmiştir (Zuboff, 2021: 80). Bireyler de internette arama yapmak için bunu organize edebilecek bir arama motoruna ihtiyaç duymuşlardır. Ancak internet kullanıcıları açısından bakıldığında ilk başta faydalı gibi görünen ihtiyacın, sonraları çeşitli sorunlara yol açabilecek bazı tehlikeleri de bünyesinde barındırdığı ortaya çıkmıştır. Bunların başında da kapitalist sermaye birikimi için yapılan dijital gözetim ve verilerin gözetimi gelmektedir. Bilginin ve sonrasında elde edilen verilerin sermaye birikimi için iştah kabartıcı bir kaynak olduğu aşikârdır, ancak aynı zamanda şirketlerin hareket alanını genişletmesinin de bir yolu

¹⁴ Sanayi toplumundan enformasyon ve bilgi toplumuna doğru bir dönüşümün gerçekleştiği konusunda tartışmalar bulunmaktadır. Bilgi ve enformasyonun, ekonomik ve toplumsal gelişmede giderek önemli hale geldiği ileri sürülmektedir. “Buradaki temel argüman, ekonomideki üretim ve dağıtım süreçlerinin gittikçe artan bir şekilde bilgi-temelli girdiler tarafından yönlendirildiğidir” (Stevenson, 2008: 297-298).

haline gelmektedir: “Gözetleme kapitalistleri bilgiyi düzenlemek için özgürlük talep ederler ve sonra da kendi özgürlüklerini korumak ve genişletmek için o bilgi avantajını kullanırlar” (Zuboff, 2021: 611). Bu özgürlüğü bir hak olarak gören şirketler, daha da saldırgan hale gelerek dijital ağları istila etmekte, insanların en mahrem alanlarına kadar sızmakta ve insana ait ne varsa sömürme eğilimine girmektedir.

1.2.1.2. Bir İletişim Stratejisi Olarak Kişiselleştirme

Günümüzde geleneksel medyaya kıyasla dijital medya, kişiselleştirilebilir özelliği ile dikkat çekmekte, kişiselleştirme, kimi yazarlara göre medya tercihinde “bireysel seçimler çağını başlatmaktadır” (Morley ve Robins, 2011: 34). Kişiselleştirme, bir ürünün veya hizmetin kullanıcısının ihtiyaçlarına göre uyarlanarak sunulması olarak tanımlanabilir. Kişilere ilgi alanlarına göre seçenekler sunulur ve ona hitap eden seçeneklerin tercih edilmesi beklenir. Ancak bu tanımlama ilk bakışta olumlu gibi gözükse de şirketlerin bu kişiselleştirmenin nasıl olacağını belirlenmesi için yine davranış verilerini kullanılmasına bağlıdır ki bu da yine verilere el konulmasıyla sonuçlanmaktadır. Bu durum, Zuboff (2021, 318)’a göre “İnsan derinliklerinin makineyle istilasına” neden olmakta ve bu istila “kişiselleştirme bayrağı altında” gerçekleştirilmektedir. Çünkü kişiselleştirme için önemli olan öngörüdür. Bu nedenledir ki kişilere ait her veri kayıt altında olmalıdır ve kişiselleştirilen her ürün -buna kişiselleştirilmiş reklam da dâhildir- öngörüler doğrultusunda kullanıcıya en uygun şekilde iletilmektedir.

Günümüzde birçok şirket kişiselleştirmeyi kullanmaktadır. Kullanıcılarına medya içeriği (televizyon dizileri, filmler, orijinal yapımlar vb.) sağlayan, 200 milyondan fazla kullanıcısı bulunan Netflix bunlardan biridir ve şirketin gelirleri yalnızca abone merkezli değildir. Gelirinin büyük kısmını kişiselleştirme sayesinde elde etmektedir. Müşterilerinin ilgi alanlarını tahmin etmek, daha başarılı ve kârlı yapımlar üretmek için arama verilerini kullanmaktadır (Bellenova ve Fuster, 2018: 1). Şirket, ayrıca video akışına yoğunlaşarak kullanıcıların nelere göz attığı veya hangi içerikleri oyladığı gibi verileri de kullanmaktadır. Netflix’in sisteminin kullanıcıların videoları beğenme veya ilgi alanlarına göre videolara geri dönme olasılığını optimize etmesi gerekir. Bunu yapmak için, kullanıcı derecelendirmeleri ve etkileşimlerinden, içerik meta verilerine kadar mevcut olan tüm verileri kullanmasının gerekli olduğu belirtilmektedir (Amatriain, 2013: 1). Yine benzer şekilde Amerikan menşeli teknoloji şirketi Amazon için de kişiselleştirme kilit roldedir. Yukarıda Netflix için ifade edilen şirket gelirlerinin yalnızca “abone merkezli” olmadığı, ifadesi Amazon için de geçerlidir. Amazon.com, en karlı e-ticaret markalarından biri olmasına rağmen kişiselleştirme

konusunda net ve saldırgan bir adım atmıştır (Montgomery ve Smith, 2009: 134). Amazon'un kurucusu ve CEO'su Jeff Bezos'un yaptığı açıklama, kişiselleştirmenin Amazon.com için önemini göstermektedir: Bezos, 20 yıldan fazla bir süre önce: *Eğer 20 milyon müşteriye sahip olmak istiyorsak, o zaman 20 milyon 'mağazamız' olsun istiyoruz. ... Misyonumuz dünyanın en müşteri odaklı şirketi olmak* demiştir (Covello, 2021). Bezos, Amazon.com'un kişiselleştirilmiş hizmet için gelişmiş filtreleme mekanizmalarına sahip olduğunu, Amazon.com'un bir müşterisinin ne satın aldığını kaydettiğini ve daha sonra bu satın almaları benzer ürünleri satın alan diğer müşterilerin toplu satın almalarıyla eşleştirdiğini söylemiştir (Ferranti, 2000). Google'dan Eric Schmidt de "tüm enformasyonu" saklamanın hayalini kurmaktadır. Schmidt, "hedefli enformasyonu, hedefli haberi, hedefli reklamcılığı size anlık ve hatasız olarak vermeyi gerçekleştirmek için sizi yeterince bilmeliyiz" der. O, bunu "şeffaf kişiselleştirme" olarak adlandırır" (Fuchs, 2014a: 184).

Kullanıcı tarafından bakıldığında kişiselleştirme, internette ya da mobil uygulama kullanımı esnasında kişilerin birtakım işlerini kolaylaştırabilmektedir. Özellikle arama motoru veya benzeri uygulamalarda arama yapan/içerik arayan kullanıcılara ilgi alanlarına göre içerikler gösterilebilir, kullanıcı, kendisine gelen medya tercihini ya da işine yarayabilecek hedefli bir reklam mesajını doğrudan kabul edebilir. Öte yandan kişiselleştirme bireyin özel olduğu hissini de yaratabilir. Ancak bu bir yanılsamadır ve bu yanılsama, kullanıcının davranış verilerinin ele geçirilerek sömürüldüğünü ve yine neoliberal ideolojinin sunduğu seçeneklerden birini tercih ettiği gerçeğini değiştirmemektedir.

1.2.1.3. Davranışsal Verinin İsabet Aracı Olarak Hedefli Reklamcılık

Hedefli reklamcılık, kullanıcının çevrimiçi etkinliğinden (örneğin, tarayıcı geçmişi, arama geçmişi ve konum gibi) toplanan verilere dayalı, ilgi alanlarına göre önceden uyarlanmış, kişiselleştirilmiş bir reklam türüdür. Kullanıcının davranış verilerine göre uyarlanan reklamlar, internet tarayıcılarıyla, arama motorlarıyla, sosyal medya ve mobil uygulamalar aracılığıyla kişilere gösterilmektedir. Hedefli reklamcılığı ilk keşfeden şirketlerden biri yine Google'dır:

Google, hedef bir reklam hizmeti sağlamak için bu tür hizmetlerin kullanımları ile ilgili verileri oluşturmakta ve depolamaktadır. Bu verileri, daha sonra Google hizmetlerini kullanan kullanıcıların aktivitelerine, aramalarına, içeriklerine ve ilgi alanlarına hitap eden reklamları veren reklam müşterilerine satmaktadır (Fuchs, 2021c: 73).

Google, başlarda daha genel ve basitleştirilmiş bir reklam politikası izlese de özellikle “anahtar kelime” stratejisini farklılaştırarak kişiyi hedef almanın yollarını aramıştır: “Reklamlar artık bir arama girişindeki anahtar kelimelerle bağlantılı olmayacak, belirli bir reklam belirli bir bireye ‘hedeflenmiş’ olacaktı” (Zuboff, 2021: 100). Google’ın hedefinde artık kişilerin ne aradığına cevap verebilecek otomatikleştirilmiş reklamlar vardır. Google sonraları hedefli reklamcılıkta daha etkin olabilmek için çeşitli ortaklıklara imza atmıştır. Bunlardan biri de DoubleClick adlı reklamcılık şirketidir. Bu iş ortaklığı sayesinde, iki farklı alanda uzman iki şirket bir araya gelerek hedefli reklamcılıkta daha da etkili olmayı amaçlamıştı: “Google’ın arama etkinliğini arama yapanların ilgi alanlarına bağlama konusundaki ustalığını ve DoubleClick’in benzersiz veri profillerine dayalı olarak kişileri izlemesini” birleştirence ortaya büyük bir sinerji çıkmıştır (Couldry ve Mejias, 2022: 54). Ancak birkaç yıl sonra anlaşılmıştır ki Google’ın “kullanıcı verilerini toplamak” için başka bir şirkete ihtiyacı pek bulunmamaktadır:

Google’ın hizmet şartları ve gizlilik politikası, çok sayıda kullanıcı verisini toplamasına ve hedef reklam stratejisi için kullanmasına yasal olarak izin vermektedir. Bu, kullanıcıya bir söz hakkı vermeyen ve kendi öz gizlilik denetiminin bir yapı özelliği olan kendi kendine tanımlanmış Google kuralları, ekonomik gözetime olanak tanımaktadır (Fuchs, 2021c: 78).

Google’ın yanı sıra birçok sosyal medya platformu da kullanıcılarının derin verisinin erişimine sahiptir. Bunlardan biri de Meta’dır. Örneğin Facebook, yıllarca kullanıcıların en derin verilerini öğrenmek adına onları profil oluşturması için teşvik etmiştir. Yani sosyal medyada var olmak bile Meta için veri ürettiğimiz anlamına gelmektedir: “Facebook’ta sadece var olmamızın reklamcılara çok değerli enformasyon sağlamasıyla ilgilidir. Bu durum, doğum tarihimizden başlayarak, hoşlandıklarımız ve hoşlanmadıklarımızın hepsinin, reklamcılar tarafından onların reklamlarda hedefledikleri kullanıcılara uygulanmasında ortaya çıkar” (Netchitailova, 2021: 4). Sonuç olarak gözetim kapitalizminin, bilgiyi organize etme misyonunu üstlenen şirketlerin, kişiselleştirmeyi etkili bir araç olarak kullanması sayesinde, kişileri hedefli reklam rüzgârını arkasına alarak yükseldiği görülmektedir.

1.2.2. Davranışsal Artı Değer ve Keşfi

Gözetim kapitalizmi öncesi kapitalizm evrelerinde, doğada bulunan kaynaklar sömürülerek kâr edilirken bugün, “insan doğasındaki şeyler” sömürülmekte ve üzerinde hak iddia edilmektedir (Zuboff, 2021: 123-124). Gözetim kapitalistlerinin insan doğasında bulunan değerleri dahi sömürebilme düşüncesi, insan davranışlarının ne denli önemli

olduğunu keşfetmelerinde gizlidir. Bu verilerden elde edilen çıktıların talep görmesi de bir başka önemli unsurdur. Bu verileri yakalamak, depolamak, işlemek ve kullanılabilir hale getirmek için gelişmiş teknoloji ve kapasite gereklidir. Bu yetenek ve kapasite de dönemin önemli aktörlerinden Google’da bulunmaktadır:

Bu yeni söylemde yer almayan şey, bu yeni hedefin arayışında Google’ın sadece milyonlarca ve sonrasında milyarlarca kullanıcıdan gelen kendine has ve detaylı davranış verisinin ortaya çıkarabileceği hassasiyetlerden faydalanarak el değmemiş bir bölgeye adım atacağıydı. Google’ın benzersiz davranış verisi erişimi ile belli bir kişinin belli bir zamanda ne düşündüğü ne hissettiği ve ne yaptığını bilmek artık mümkün olacaktı. Google’ın icadı kişinin farkındalığı, bilgisi ve ricasına aldırmaksızın tek taraflı bir ayna gibi çalışan, böylece kişisel veriye ayrıcalıklı gizli erişimi mümkün kılan, bir otomatikleştirilmiş mimari ile birey ve grupların düşünceleri, duyguları, niyetleri ve ilgi alanlarını anlamak ve bu konuda sonuca varmak için yeni kabiliyetleri ortaya çıkardı (Zuboff, 2021: 101-108).

Google, önceleri basitleştirilmiş, sade bir arayüzle web’de arama yapmamıza olanak sağlayan arama motoruyla hayatımıza girmiştir. Arama motorunun olanaklarından yararlanmış, arama motorunda reklam gösterebilmek için kendi ekosistemini yaratmıştır. Google Ads (önceden Adwords), AdSense ve Admob gibi ürünlerle reklam ağını genişletmiştir¹⁵. Böylelikle çok daha fazla kişinin cihazlarına girmiş ve sahip olduğu algoritmalar sayesinde muazzam miktardaki veriyi ele geçirmiştir. Öte yandan, Google dışında kalan şirketler de kendine has yetenek ve olanakları sayesinde bu keşiften faydalanmışlardır. Facebook bu şirketlerden biridir ve analistleri çevrim içi mesajların “milyonlarca kişide politik kişisel ifadeyi, bilgi aramayı ve gerçek dünyada oy verme davranışını etkilediğini” kavramışlardır (Zuboff, 2021: 371). Kullanıcıların oy kullanma davranışlarının manipüle edilebileceği anlaşıldığında, Facebook’un artık tek bir hedefi vardır: Davranışı değiştirerek, gündelik hayata müdahale etmek, süreci öngörmek ve hâkim olmak (Zuboff, 2021: 371-372). Bu mikro hedefleme ile seçmenlere sahte metinler, haberler veya

¹⁵ Google Ads, reklamverenlerin içerikleriyle ilgili anahtar kelimelere dayalı olarak reklam yerleştirdiği tıklama başına ödemeli bir anahtar kelime reklam hizmetidir. Buna karşılık AdSense, Google Ads programı aracılığıyla satın alınan reklamlar için en iyi konumlandırmayı belirlemek üzere Google’ın arama yeteneklerini kullanan bir reklam yerleştirme hizmetidir (Spreeuwenberg ve Poell, 2012). Admob ise uygulama geliştiricilerinin uygulama içine reklam entegre ederek kullanıcıya hedefli reklam göstermesini ve para kazanmasını sağlayan bir reklam platformudur (Moroney ve Moroney, 2017: 233).

manipülatif görseller -Byung-Chul Han, bunları “karanlık reklam olarak”¹⁶ olarak tanımlar-gösterilmektedir. Böylelikle seçmen davranışı bilinçdışı düzeyde etkilenmekte, dolayısıyla demokratik sürecin altı oyulmaktadır (Han, 2022: 24).

1.2.3. Gözetim Kapitalizminin Tecimsel Kaldıracı: Mülksüzleştirme ve Mülksüzleştirme Döngüsü

Karl Marx (2019: 686), Mülksüzleştirmeyi “ilk birikim” başlığı altında detaylandırmıştır. Bu bağlamda, topraklara el konulmasıyla emek gücünün artı değeri ile kapitalist birikim için geçerli koşulların yaratıldığı vurgulanmıştır (Jakobsson ve Stiernstedt, 2010). David Harvey ise mülksüzleştirmeyi, kimsenin mülkiyetinde bulunmayan toplumsal müştereklerin sermaye sınıfına tahsis edilmesi olarak tanımlamaktadır:

Mülksüzleştirme yoluyla birikim derken ilkel birikimi kastetmiyorum. İkel birikimde insanlar topraklarından kovulur, kamu mülkleri çitlerde çevrilir, bu süreç ücretli emek gücünün yaratılmasına yol açar. Bu değil kastettiğim. Ben zaten birikmiş servetin, üretime yatırım yapmak düşüncesi olmaksızın, sermayenin belli kesimleri tarafından temellük ya da gasp edilmesinden söz ediyorum. Bu durum farklı şekillerde vuku bulabilir. Çağdaş kapitalizmin günümüzde, canlı emeğin üretimde sömürülmesi yoluyla birikime nazaran, mülksüzleştirme yoluyla birikime giderek daha fazla bağlı olduğunu savunuyorum (Harvey, 2022: 149).

Günümüzde sosyal yaşam giderek metalaştıkça “dijital mülksüzleştirme söylemi” de giderek daha fazla gündeme gelmektedir (Joseph, 2018: 692). Zuboff (2021: 131)’a göre, “Gözetleme kapitalizmi, aşırı yüklenmiş yatırımın sabırsızlığı ve sisteme katılmak isteyen iki girişimci tarafından hayata geçirilen, dijital mülksüzleştirme davranışından kaynaklanır. Bu, Google’ın dünyasını harekete geçiren ve onu kazanca doğru yönelten kaldıraçtır”. Harvey de Google’ın “mülksüzleştirme yoluyla”¹⁷ birikimine değinir:

Mesela Google’ın yükselişine bir bakın. Bu devasa şirket şu anda bulunduğu yere gelene dek kaç küçük işletmeyi devraldı? Silikon Vadisi böyle çalışır; girişimciler küçük uygulamalar geliştirip küçük şahıs şirketleri kurar. Bir noktada büyük sermaye tarafından satın alınıp büyük bir holdingin parçası olurlar. Şirketler emek yoluyla değil, ancak başkalarının varlıklarını devralarak, yani varlık soygunu ile birikim yapabilir (Harvey, 2022: 150).

¹⁶ “Psikometrik olarak optimize edilmiş bu gizli reklamlar (Dark ADS) demokrasi için bir tehdit oluşturmaktadır. Dark ads, toplumun bölünmesine ve kutuplaşmasına katkıda bulunur ve söylem iklimini zehirler” (Han, 2022: 24).

¹⁷ Facebook da benzer bir yörüngeyi takip etmiştir. Sürekli satın almalar (örneğin, Instagram ve WhatsApp) yoluyla birikim stratejisi izlemiştir (Nieborg ve Helmond, 2019: 201).

Zuboff (2021, 178-180), bu birikim stratejisini mülksüzleştirme döngüsü ile açıklamaktadır. Google üzerinden açıkladığı döngünün dört aşaması vardır. Bunlar: İstila, alıştırma, uyarlama ve yeniden yönlendirme. *İstila*, döngünün ilk aşamasıdır ve hayatımızdaki savunmasız alanın, bir anlamda neredeyse her şeyimizin ele geçirilmesi anlamına gelir. Bu istilanın tek taraflı olduğunu dile getiren Zuboff, Google’ın istilayı başlattığından beri çeşitli şekillerde gerçekleşen direnişle (Google’a şu ana kadar birçok dava açılmış; ama Google, istilasını sürdürmeyi başarmış ve halen karşı çıkılan uygulamalarına devam etmektedir.) karşılaştığını; ancak bu direnişe bağışıklık kazandığını dile getirir. İkinci aşama ise *alıştırma*dır. Kişiler çeşitli yollarla istilaya alıştırılmaktadır. Alıştırma bazen uzlaşmayla, bazen çaresizlikten, bazen de küçük ödüllendirmeler ile gerçekleşmekte, çoğu zaman teslimiyetle sonuçlanmakta ve giderek sıradanlaşmaktadır: “Daha da kötüsü, zamanla kaçınılmaz hale gelir. Yeni bağımlılıklar gelişir. Popülasyonlar hissizleştikçe, bireyler ve gruplar için şikâyet etmek daha da zor hale gelir” (Zuboff, 2021: 180). Döngünün üçüncü aşamasında, ise *uyarlamalar* üretilir. Google taktiksel açıdan bazı küçük değişiklikler yaparak, uygulamalarına karşı tepkileri ya da yasal zorunluluk ve yaptırımları atlatır. Son aşama ise yeniden yönlendirme ve önceki aşamada yaşanan süreçler esnasında ortaya çıkar. Şirketin karşı çıkılan uygulamalarına karşı “sosyal ve yasal taleplerle uyumlu görünsünler diye, *yeniden yönlendiren* yeni söylem, yöntem ve tasarım”lar (Zuboff, 2021: 180) üretmek için örgütlenir. Sonuçta Google, bugüne kadar her direniş için bir savunma mekanizması geliştirmiş, karşı direniş hamlelerini devreye koymuştur. Böylelikle direnişe karşı bağışık hale gelmiş, mülksüzleştirme pratiğini neredeyse kusursuz hale getirmiştir.

1.2.4. Gözetim Kapitalizmi ve Yönetimsel Kapitalizm Arasındaki Temel Fark

Zuboff (2021: 22), gözetim kapitalizminin Google tarafından icat edildiğini söylemektedir. Google bu icadın önderi olsa da bugün, gözetim kapitalisti olarak tek şirket Google değildir ve bu düzene başka teknoloji şirketleri de dâhil olmuştur. Bu şirketlerin önde gelenleri, daha önce bahsedildiği üzere MAANG olarak anılan şirketlerdir. Bu şirketlerin tamamı General Motors’un icat ettiği yönetimsel kapitalizm düzeni ekseninde kurulmuş, bugün ise gözetim kapitalizminin aktörleri haline gelmiştir. Zuboff (2021: 38)’a göre şirketler, kişilerin izni çerçevesinde kendi ürün ve hizmetlerini geliştirmek için kişisel topladığında gözetleme kapitalizminden bahsedilemez, bu tam anlamıyla kapitalizmdir. Yani, MAANG şirketlerinin tamamı kapitalizmi uygulamaktadır, ancak “saf gözetim kapitalisti değildir, en azından şimdilik”. Ancak burada Zuboff’un ıskaladığı bir nokta vardır. Bu önemli nokta, gözetim kapitalizminin en temel farkının gözle görülür bir biçimde kişileri gözetliyor

olmasıdır. Öte yandan Nick Srnicek (2017), MAANG şirketlerinin sahip olduğu dağıtım platformlarının global olarak yayılmasıyla bir “platform kapitalizmi” çağının başladığını, bunun da “yeni tip” bir şirket egemenliğine işaret ettiğini dile getirmektedir. Bu yeni tip şirket egemenliğinin de doğrudan verinin gözetimi ve sömürsünün kolaylıkla bu platformlar aracılığıyla gerçekleştirilebiliyor olması ile ilişkilidir. Ayrıca kişilerin verilerinin “ürün ve hizmet geliştirme” adı altında ve sözde “açık rıza” ile toplanması, yalnızca bu amaç için kullanılıyor olmasını göstermez; ayrıca bu durum veri toplamanın göstermelik mantığıyla uyum içindedir. Dolayısıyla her ne amaçla olursa olsun şirketlerin izinsiz ya da izinsiz olarak dijital verileri toplaması gözetim kapitalizminin temel amacıdır. Gözetim kapitalizminin, yönetsel kapitalizmden ayrıldığı nokta kişisel verilerin, yani davranış verilerinin gözetimidir. İstihbarat, çalışan denetimi veya iş gözetimi gibi kapitalizmin gözetimle olan bağı, tüketicilerin gözetimine dönüşmüştür. Böylece yeni gözetim biçimi, kişilere takılmış birer mikroçip gibi işlev gören teknolojik cihazlar sayesinde tüm gözetim yöntemlerini bünyesinde toplayan, her şeyi izleyebilen bir yapıya bürünmüştür.

1.2.5. Gözetimin ve Veri Sömürsünün Sıradanlaşması

Gözetim kapitalizminin gözetime dayalı bir sistem olduğu yukarıda detaylı bir biçimde açıklanmıştır. Fakat günümüzde gözetim, tek taraflı değildir. Sosyal medya, internette *dikizleme kültürünü* beraberinde getirmiştir. Hal Niedzviecki (2019: 8-16) günümüz sosyal medya çağını “Dikizleme Kültürü Çağı” olarak görür ve dikizlemeyi, diğer kişiler hakkında “her şeyi bilme ve öğrenme arzusu” olarak tanımlar. Fakat bu arzunun bazı sonuçları vardır. Kişi, herkes hakkında bir şeyler bilmek istiyorsa, kendi hakkında da her şeyin bilinmesini kabul etmektedir. Böylece herkes dikizleme kültürünün parçası haline gelmektedir. Bu kültür, dijital alanda gözetimin sıradanlaşmasına neden olmuştur. Bu, tam da gözetim kapitalistlerinin istediği şeydir.

Öte yandan gözetim kapitalistlerinin ürünlerinin büyük çoğunluğu “ücretsizdir”. Ancak “ücretsiz bedeli” vardır ve bu bedel, kişisel verilerin şirketlere sızdırılmasıyla ödenmektedir (Meng, vd., 2016). Şirketler, ücretsiz ürünlerinin karşılığının veri olduğu düşüncesindedirler (Zuboff, 2021: 73). Ve hatta bazı kullanıcılar da şirketlerin bu tutumuna paralel görüş bildirmekte, bunun “ücretsiz” bir şey almanın bedeli olduğunu söylemekte ve olumsuz bir şey olmadığı sürece bu bedeli ödemedi herhangi bir sorun görmediklerini ifade etmektedir (Shklovski vd., 2014). Elbette tüm bunlar, kişilerin bu ürünlere olan bağımlılığının da bir göstergesidir. Ayrıca Zuboff (2021: 73)’un da dediği gibi dijital araçlar için “kaçınılmazcı söylem” de söz konusudur. Artık dijital cihazları/yazılımları kullanmamak çok

zordur ve kaçınılmaz olarak kullanılmaya devam edilecektir. Bu düşünceler yaygınlaştıkça şirketlerin veri ihlalleri de sıradanlaşmakta, gözetim kapitalizminin genişlemesine katkıda bulunmaktadır.

1.2.6. Gözetim Kapitalizminin Getirdikleri

Gözetim kapitalizminin sonuçlarını ortaya koymak, şu an için pek mümkün görünmemektedir. Çünkü bu sistem çok yenidir ve halen genişlemektedir. Ancak sistemin yaratabileceği olası tahribatları dile getirmek önemlidir. Bugünün gözetim kapitalizmi, tarihsel kapitalizmden, araçları itibarıyla farklıdır. Gözetim kapitalizmi, kişisel verileri piyasa aygıtı haline getirerek, insan iradesini blokaja uğratmakta ve insanı insan yapan özelliklere set kurarak insani değerleri tahrip etmekte, giderek demokratik haklara kasteden bir yapıya bürünmektedir. Piyasa kapitalizmi demokrasiyi ticari ifade özgürlüğü bağlamında yüceltirken, gözetim kapitalizmi kişisel verileri çoğu zaman rıza üretimi yoluyla manipüle ederek demokrasiye meydan okumakta ve piyasa kapitalizminden önemli ölçüde ayrılmaktadır (Zuboff, 2015: 75); “Şimdiki hedef *doğaya* değil, *insan doğasına* egemen olmaktır” (Zuboff, 2021: 610, 630). Ancak iki sistem arasındaki bu fark, gözetim kapitalizmi evresi öncesine hâkim olan kapitalizmin masum olduğunu da göstermemektedir. Çünkü kapitalizm tarihinin eşitsizliklerle dolu olduğu göz ardı edilemez. Ayrıca gözetim kapitalizmi öncesi kapitalizm evrelerinin tamamen ortadan kalktığı da iddia edilemez. Bugün hala doğal kaynakların sömürüsü devam etmektedir. Dolayısıyla iki egemenlik biçimi de acımasızdır. Eskiden doğanın tehlike altında olduğu gibi bugün de insan doğası ve en nihayetinde özgürlüğü tehlike altındadır.

1.3. Dijital Ağlarda Verilerin Sermayeleştirilmesi

İletişim ağları, bilginin altyapısını oluşturmaktadır ve günümüz toplumları da bu iletişim ağlarına ve bilgiye bağımlıdır (Lyon, 2006: 59). Enformasyon ve iletişim teknolojileri tarafından harekete geçirilen toplumlar, giderek bu ağlar etrafında toplanmaktadır (Castells, 2013: 623; 2016: 59). Dijital iletişim ağlarının yükselişi, internetin ve geniş bant olanaklarının gelişerek yaygınlaşmasıyla birlikte mümkün olmuştur. Ayrıca dijital cihazların boyutlarının küçülerek mobilize hale gelmesiyle, gündelik hayatın içerisine daha da nüfuz etmiş (Dijk, 2016: 77), özellikle sosyal ağlar, “kullanıcıların internet deneyimlerinin önemli bir bileşeni haline gelmiştir” (Creps, 2020: 103). Bu nedenle akademik alanda da dijital iletişim ağlarına olan ilgi artmış, dijital ağlara yönelik sorunlar/konular birçok akademik çalışmaya konu olmuştur. Bu araştırmalarda genellikle iki eğilim egemendir. İlki, dijital iyimserlerin, yani eleştirel olmayan, olumlayıcı (katılımcı kültürü öven, yeni topluluk biçimlerini ve ağ

bağlantılı eylemcilik tarzlarını var eden) yaklaşımlar, diğeri ise kötümserler, yani eleştirel (ağ bağlantılı otoriterliğe, sömürü ve gözetime dikkat çeken) yaklaşımlardır (Netchitailova, 2021: 3; Fuchs ve Chandler, 2021: 8). Buradan hareketle, bu başlık altında dijital ağlar etrafında toplanan kullanıcıların kişisel verilerinin sermayeleştirilmesi, veri-gözetim-emek çerçevesinde eleştirel bir perspektifte incelenmiştir.

1.3.1. Kullanıcıları Ağlara Bağlamak

Yukarıda da açıklandığı üzere günümüzde disiplin rejimindeki gibi sınırlayıcı ortamlar bulunmamaktadır. Panoptik dayatma artık söz konusu değildir ve artık kişiler bir bakıma kendilerini sahnelemektedir. Kapatma ve mekânsal izolasyonun yerini açık iletişim ağları almıştır ve bu yeni rejimde gözetim, veriler üzerinden gerçekleşmektedir. (Han, 2022: 8, 10). Kişiler ne kadar çok iletişim kurarsa o kadar veri üretecek, böylece gözetim de bir o kadar verimli hale gelecektir (Han, 2022: 10). Buradan şöyle bir sonuç çıkmaktadır: Ağlar genişlemeli, çok daha fazla insan bu ağlara bağlanmalıdır. Böylece sosyal ağ platformlarına erişim giderek artacak, geleneksel kitle iletişim araçlarındaki sermaye birikimine benzer bir birikim stratejisine yaklaşılabacaktır (Fuchs, 2014b: 177).

Dijital platformlar kişilerin ağlara bağlanmasına ve sosyalleşmesine katkıda bulunmaktadır. Örneğin Facebook bu platformlardan biridir; ağ oluşturmayı ve sosyalleşmeyi desteklemekte, fiziksel temastan ziyade “ilgi alanına dayalı” teması sağlamakta ve sosyal etkileşimleri artırmaktadır (Crepes, 2020: 106). Etkileşim için kullanıcıdan profil oluşturulması istenmektedir. Ne kadar bilgi, o kadar çok bağlantı ve etkileşimi beraberinde getirmektedir. Fakat etkileşimin bir karşılığı vardır: “Etkileşimli medyanın kullanıcıları kendileriyle ilgili bilginin kontrolünü Google, Facebook ve benzerlerine devretmeyi özgürce kabul ederler” (Andrejevic, 2014b: 75). İşte bu durum kişilerin verileri üzerinde olan kontrolü kaybetmesine neden olmaktadır ve yüksek etkileşim beklentisi, kullanıcı bilgilerinin şirketlere teslimiyetiyle sonuçlanmaktadır. Bireyleri önce nicelleştiren ve ardından bireyleri kendi ürettikleri verilerden yoksun bırakan bu düzen, sermaye ile birey arasında yeni bir ilişki rejimine işaret etmektedir (Thatcher, vd., 2016: 998).

Dijital ağ kullanıcıları çevrimiçi olur olmaz veri yaratmaya başlamaktadır. Bu veriler, “profillerine ve çevrimiçi davranışlarına atıf yapan” verilerdir ve reklamverenlere satılmaktadır. Kullanıcılar, ağ ekosistemi içerisinde değer üretmekte, dolayısıyla onlarsız kâr elde edilememektedir (Fuchs, 2014a: 25-26). Bu nedenle Fuchs, ağlardaki kullanıcıları *üretketici* olarak tanımlar ve dijital ağların metalaştırıldığına vurgu yapar: Özellikle sosyal medya platformları “... ağları metalaştırma üzerine kurulu bir üretketici metalaşma sistemi

geliştirmektedir” (Fuchs, 2014a: 351) ve “Ağ bağlantılı dijital teknolojiler, yeni metalaştırma ve sömürü biçimleri ile birikime ilişkin yeni sorunlar” yaratmaktadır (Fuchs ve Chandler, 2021: 79). Bugün, kişileri dijital ağlara bağlamak şirketler için zorunluluk haline gelmiştir. Artık dijital ağlar, ciddi derecede önemli bir pazar konumundadır. Bu nedenle bu pazarda pay sahibi olmak, özellikle medya şirketlerinin hayatta kalmasına olanak sağlayan kaynaklardan biri haline gelmiştir. Milyarlarca insan da bu ağlara bağlanmak için oldukça isteklidir. Bu isteği memnuniyetle kabul eden şirketler, kullanıcıların yarattığı değeri kullanarak zenginleşmektedir.

1.3.2. Veri Sermayedarları: Sosyal Nicelleştirme Sektörü

Verilerin toplanması ve dolaşımı, çağdaş kapitalizmin merkezi bir unsuru haline gelmiştir. Veri toplama, sürekli sermaye birikimi döngüsü tarafından yönlendirilmektedir ve bu da sermayeyi her şeyin veriden oluştuğu bir evren inşa etmeye zorlamaktadır. Dünyanın en zengin şirketleri veri sermayesi üzerine kuruludur (Sadowski, 2019: 1) ve sosyal hayatımızdan sürekli veri çıkarılmasıyla yeni bir düzen inşa edilmektedir. Bu düzen, ekonomik değer yaratmak için optimize edilmiştir (Couldry ve Mejias, 2019: 1). Veri sermayedarı şirketler, toplumsal hayatı, yani sosyalliği nicelleştirmektedir. Sosyal nicelleştirme, toplumdan sosyal verilerin (tutumlar, davranışlar, etkileşimler vb.) çıkarılmasına ve işlenmesine dayanmaktadır. Aslında herhangi bir pazarda bireyin davranışını tahmin etmek için niceliksel veri setlerini kullanmak pek de yeni bir fikir değildir; örneğin, bireylerin kredi puanları (verileri) uzun süredir kredi veya sigorta riski prim oranlarını belirlemek için kullanılmaktadır. Ancak bugün büyük veri, “sosyal nicelleştirme sektörü”¹⁸ için daha fazlasını ifade etmektedir (Thatcher, vd., 2016: 997-998). Van Dijck (2014: 198)’ın deyişiyle “yaşam madenciliği”, sosyal davranışı anlamak için kabul gören bir paradigma haline gelmiştir. Veri madenciliği veya makine öğrenmesi gibi yöntemler kullanılarak sosyal hayat ölçülmekte ve değerlendirilmektedir. Öte yandan Couldry vd. (2016: 118) de “sosyal analitik”¹⁹ teriminden bahsetmektedir. Sosyal analitik, özellikle sosyal medya arayüzleri aracılığıyla “sosyal aktörler” tarafından toplanan bu tür verilerin kullanımını ifade etmektedir. Burada sosyal aktörlerden kasıt ise veri üretme ve analiz etme (genellikle kâr amaçlı) temel

¹⁸ Andrejevic, bu şirketleri “büyük veri zengini” şirketleri olarak tanımlar. Büyük Veri zengini şirketler, büyük veri setleri oluşturabilen veya satın alabilen ve depolayabilen şirketlerdir (bkz. Andrejevic 2014a: 1675).

¹⁹ Sosyal analitik yaklaşımı ise analitiğin bir dizi sosyal aktör tarafından nasıl kullanıldığının sosyolojik olarak ele alınmasıdır. Sosyal analitik yaklaşımı, analitiğin bir dizi sosyal aktör tarafından sosyal amaçlarına ulaşmak için nasıl kullanıldığına dair çıkarımlar yapan sosyolojik bir yaklaşımdır (Couldry ve Powell 2014: 2; Couldry, vd., 2016: 119).

amacının ötesinde ve üstünde sosyal amaçları olan bireyler veya gruplardır (Couldry ve Powell, 2014: 2). Bu aktörler, sosyal hayata dair verileri pazarlama faaliyetlerinin dışında, toplumsal araştırmalar, kamu yönetimi veya insan kaynakları gibi alanlarda da kullanabilmektedir.

Couldry ve Mejias, (2019: 4)'a göre sosyal nicelleştirme sektörü, dijital cihaz üreticileri (Amazon, Apple, Microsoft, Samsung vb.), bilgisayar tabanlı ortamların ve bağlantı kurmamızı sağlayan araçların yaratıcıları (Alibaba, Baidu, Facebook, Google, Tencent, WeChat vb.) ve hizmetlerini kişiselleştirmek durumunda olan (Netflix, Spotify, Airbnb, Uber vb.), "... güncel toplumsal eylemleri yakalayarak onları analiz eden ve niceliksel verilere dönüştüren" (Couldry ve Mejias, 2020: 21) organizasyonlardır. Faaliyet alanı ne olursa olsun tüm bu şirketler, sosyal hayattan veri işlemeye bağımlıdır. Verisiz soluk alamaz, operasyonlarını yönetemezler. Dijital ekonomide platform şirketleri, platformlarındaki kullanıcılar hakkında veri toplamakta ve bu verileri ticari faaliyetlerini daha rekabetçi hale getirmek için kullanmaktadır (West, 2019: 28). Örneğin Netflix'in kullanıcılarına sunduğu temel hizmet modeli, onlara kişiselleştirilmiş öneriler sunmak ve ilgi duyduğu içerikleri bulmasına yardımcı olmaktır. Bu nedenle kullanıcının davranışlarına ve tarama geçmişine dayalı verileri toplayıp analiz etmektedir. Ancak topladığı verilerden kullanıcısının kim olduğunun kesin hatlarını çizebilir ve bu bilgileri başkalarıyla da paylaşabilir (Nielsen, 2020: 28). Bu durum, Amazon içinde geçerlidir; Amazon, ürünlerini ve hizmetlerini tüketiciler için daha da karşı konulmaz hale getirmek için büyük miktarda veri toplamaktadır. Ve bu nedenden ötürü Amazon, amacı tüketiciler hakkında veri toplamak olan araçları/hizmetleri giderek daha fazla tasarlamaktadır (West, 2019: 27-28).

Sosyal medya platformlarının da kendine özgü yöntemleri vardır ve bu yöntemler, kullanıcıların gönüllü olarak paylaşmaktan imtina ettiği veriler de dâhil olmak üzere kişilerin davranışsal verilerini ele geçirme ve üzerinde hak iddia etmesine olanak tanımaktadır (Zuboff, 2021: 107). Örneğin Facebook hem veri toplayıcı hem de dijital pazarlama platformu olarak işlev gören ve çok çeşitli endüstri ortaklarına hitap eden çok sayıda özel ortak programı işleten birkaç baskın aktörden biri olarak özellikle semboliktir. Ayrıca Facebook, 2 milyara yaklaşan aktif kullanıcının gerçek zamanlı, konum tabanlı sosyal verisini toplama yeteneğine sahiptir (Helmond, vd., 2017: 1). Diğer taraftan Facebook, aynı zamanda bir iş platformudur. Facebook'un gelirleri dâhili büyüme (platforma ait uygulama ve web gelirleri), satın almaların (mülksüzleştirme) yanı sıra web ve uygulama alanının platformlaştırılmasıyla da artmıştır. Milyonlarca işletme ve kurum, reklam yayıncısı, reklam aracı, üçüncü taraf içerik geliştiricisi ve kullanıcısı için arayüz oluşturmaktadır. Facebook, sosyal eklentiler gibi

platform özelliklerini üçüncü taraf web sitelerine ve uygulamalara genişleterek pazarın her iki tarafını da giderek daha fazla kontrol etmektedir (Helmond, vd., 2017: 1-2; Nieborg ve Helmond, 2019: 211).

Öte yandan kişisel veriyi toplayarak ve bu verileri satarak para kazanan “veri komisyoncusu” şirketler de sosyal nicelleştirme sektörünün bir başka aktörüdür. Veri komisyoncusu kesin olmayan bir terim olsa da genellikle, kişisel bilgilerin toplanması ve değiş tokuşunda uzmanlaşmış şirketleri ifade eder ve büyük ölçekli veri operasyonlarıyla ilişkilendirilir. Acxiom ve Experian gibi “bilgi satıcıları” olarak da adlandırılan büyük veri komisyoncularının kökleri doğrudan pazarlama ve kredi raporlaması gibi yerleşik iş sektörlerinde bulunmaktadır. Veri komisyoncuları, ağ bağlantılı iletişim ve bilgi işlem tarafından oluşturulan veri toplama ve analiz olanaklarından yararlanmakta; genişleyen ticari gözetim endüstrisinin kalbinde faaliyet göstermektedir. Veri komisyoncuları, kişisel verilerin metalaştırılması ve kapitalist genişlemenin tarihsel süreçlerine derinden kök salmıştır ve kontrol edilmezlerse daha yaygın ve istilacı olmaya devam edecekleri öngörülmektedir (Crain, 2018: 90-100).

1.3.3. Verilerin Sermayeleştirilmesinde Emek

Ekonomi biliminin temel sorunlarından biri, meta üretiminde emeğin kullanılmasıdır. Meta üretimi esnasında emeğin nasıl harcandığı ve sonrasında ortaya çıkan değerın nasıl bölüşüldüğü de bağlantılı sorunlardandır (Eaton, 1996: 31). Bu nedenle emek kuramları, geçmişten beri ekonomi çerçevesinde emek bağlantılı sorunsalların çözümlemesinde kullanılmıştır. Özellikle Marksist kuramda emek, değer ve sınıf temel kavramlardır. Marx, birbiriyle ilişkili bu üç kavramı, “kapitalist toplum analizinde” kullanmıştır (Amorim, 2018: 69). Öte yandan günümüz kapitalizmde çalışma koşullarının değiştiği, “emek ve yaşamın karmaşık şekillerde iç içe geçtiği” (Jarret, 2021: 153) dile getirilmektedir. Marx’ın emek kuramı, kapitalizmin eleştirisi için halen önemli bir kuram olmakla birlikte, iş ve gündelik yaşamın giriftliği, Marx’ın emek kuramını sorgulanır hale getirmiştir:

Marx’ın problematiğinin yapısını oluşturan bu kavramsal üçayağın (emek, değer ve sınıfın) geçerliliği bir süredir sorgulanmakta. Bu eleştirinin merkezinde çağdaş kapitalist toplumun merkezinin, bir şekilde üretim ve fabrika emeğinin ötesine taşındığı tezi bulunmaktadır. Bu tezin iddiası, meta üretiminin ve emeğin ortadan kalktığı değildir. İddia edilen daha ziyade, meta üretiminin yerini yeni toplumsal etkinlik türlerinin aldığı ve bunların da birlikte ya da ayrı olarak, yeni toplumsal örgütlenme ve siyaset biçimlerini meydana getirdiğidir (Amorim, 2018: 70).

Hardt ve Negri (2018: 287)'ye göre bu bir süreçtir ve buna "... endüstrinin hakimiyetinden hizmetler ve enformasyon hakimiyetine geçişe bir ekonomik *postmodernleşme*, daha doğrusu *enformatikleşme* süreci"²⁰ denilebilir. Özellikle enformasyon teknolojilerinin giderek daha fazla kullanılması ve buna bağlı olarak hizmet sektörünün gelişmesi sonucu post-endüstriyel bir çağa adım atıldığı ve dolayısıyla günümüz kapitalizmini açıklayabilecek yeni bir emek anlayışına ihtiyaç bulunduğu dair söylemler giderek daha da dillendirilmektedir (Sayers, 2018: 23). Endüstriyel kapitalizm evresinden, kapitalizmin yeni evresi olarak lanse edilen bilişsel kapitalizme doğru geçişte, endüstriyel emek biçimleri hegemonyasını yitirmiştir. Kas gücüne dayalı işçi emeğinin etkisi kaybolmaya başlamış, maddi olmayan emek, ücretsiz emek ve dijital emek gibi kavramlar gündeme gelmeye başlamıştır (Hardt ve Negri, 2004: 122; Uca, 2016: 45; Koşar, 2017: 83). Maddi olmayan emek, literatürde kullanılan diğer emek tanımlamalarını kapsayacak şekilde şemsiye bir kavram olarak kullanılabilir. Ancak aşağıda da belirtildiği üzere farklı tanımlamalar da söz konusudur. Özellikle dijital ağlardaki kullanıcılar üzerine yoğunlaşan bu emek türleri, yalnızca emek sömürsüne değil, dijital ağlardaki veri sömürsüne de dikkat çekmektedir; yani kullanıcı emeğinin kullanılarak verilerin sermayeleştirilmesine.

1.3.3.1. Maddi Olmayan Emek Üzerine

Fizyokratlardan, Adam Smith ve David Ricardo'ya uzanan ve Marx tarafından değiştirilen ve geliştirilen klasik gelenek, toplumdaki ekonomik değerin kaynağı olarak emeğe odaklanmıştır (Gandy, 1993: 71). Smith (2014: 357-358), üretken emek ile üretken-olmayan emek arasında ayrım yapmıştır: "Bir çeşit emek vardır ki, harcadığı nesnenin değerine değer katar. Bir başkası vardır, öyle bir etkisi olmaz. Birinciye, bir değer hâsıl ettiği için, üretken emek; ötekine, üretken-olmayan emek denilebilir". Bu ayrım aslında şu şekilde özetlenebilir: Emek, sermayeye gelir kazandırıyor, yani artı-değer üretiyorsa üretken, sermayeye para kazandırmıyor, yani artı-değer üretmiyorsa ve emeğin ücreti sermayenin gelirinden ödeniyorsa üretken olmayan emektir (Uca, 2016: 54; Wittel, 2019: 404). Marx, (2019: 332), "emek gücünün kapitalist tarafından mümkün olduğu kadar çok sömürüldüğünü" belirtmektedir. Kapitalist üretim ilişkileri bağlamında Marx'ın kuramı, "... malların üretimi için gereken toplam emek zamanının analizinden sonuca varan bir emek değer kuramıdır" (Fuchs, 2014b: 156-157). Yani malların değeri, toplumsal olarak harcanan emek zamanına

²⁰ "Modernleşme süreci emeğin tarım ve madencilikten (birinci sektör) endüstriye (ikinci sektör) göçüyle tanımlanırken, postmodernleşme ya da enformatikleşme süreci emeğin endüstriden hizmet alanına (üçüncü sektör) göçüyle tanımlanır" (Hardt ve Negri, 2018: 291).

bağlıdır. Mallar/hizmetler üretilirken, harcanan emek zamanı ne kadar fazlaysa o kadar değerli hale gelmektedir. Marx (2019), çalışma süresinin uzatılmasının kapitalist artı değer birikimi için önemli bir unsur olduğunu ileri sürer. Ona göre kapitalist birikim, emeğin yaratıcı gücü üzerindeki kapitalist kontrol ve sömürü ile gerçekleşir (Gandy, 1993: 71).

Marx (2019), kuramında emek zamanına büyük önem atfedilmektedir. Ancak bugün, "... bilginin yayılması ve itici gücüne dayalı bir ekonominin ortaya çıkışından sonra, entelektüel emek stratejik bir etmene dönüşür ve doğrudan emek zamanı ekonomik açıdan anlamlı bir ölçü birimi olmaktan çıkar" (Vercellone, 2015: 268). Sürekli değişip dönüşen dünyada emek de kaçınılmaz olarak dönüşmektedir. Yeni çalışma biçimlerinin ortaya çıktığı, maddi olmayan emeğin öne çıktığı bir dönem işaret edilmektedir: Kitleli işçilerin emeği ile çarkları dönen endüstriyel fabrikaların yerini başka şeyler alıyor ve F. Hegel ve K. Marx'tan beri yeni çalışma biçimleri yaratılıyor (Sayers, 2018: 36). Henri Lefebvre (2019: 55)'ye göre de bu biçimler "özellikle maddi olan ve maddi olmayan (yönetme, komuta etme gibi idari işlevler; düşünsel işlevler vb.) emek arasındaki bölünme" kendini göstermektedir. "Gorz, Lazzarato ve Negri'nin çalışmalarında maddi olmayan emek, esasen, fiziksel varlığa sahip olmayan emektir. Negri, maddi olmayan emeği; 'enformasyon, bilgi, fikirler, imajlar, ilişkiler ve duygulanımlar gibi maddi olmayan metalar üreten' emek olarak tanımlar" (Amorim, 2018: 75-77). "Sanayi sonrası ekonominin tüm özellikleri (hem sanayide hem de bir bütün olarak toplumda) görsel-işitsel üretim, reklam, moda, bilgisayar yazılımları, fotoğrafçılık, kültürel etkinlikler vb. gibi "maddi olmayan" üretimin klasik biçimlerinde büyük oranda mevcuttur" (Lazzarato, 2016: 38). Burada maddi olmayan emeğin üretimi ile ilgili bir kafa karışıklığı söz konusudur. Maddi olmayan şey emek midir, yoksa emeğin çıktısı mıdır? Hardt ve Negri (2004: 123) bu karışıklığı şu şekilde giderir: "Maddi olmayan üretimin tamamında kullanılan emeğin maddi kalmaya devam ettiğini vurgulayalım: Bu emek, bütün emek türleri gibi, bedenimizi ve beynimizi içerir. Maddi olmayan şey *emeğin ürünüdür*"

Bugün, tüketimle ilişkili olmayan zamansal bir kategori neredeyse yoktur. İş zamanını (üretim) boş zamandan ayırmak giderek zorlaşmaktadır. Hayat, işten ayrılmaz bir biçimde kesişmekte, iç içe geçmekte ve bulanıklaşmaktadır (Lazzarato, 2016: 233; Uca, 2016: 70; Jarret, 2021: 139). Fuchs (2014b: 163-164)'a göre toplumsal yapıdaki faaliyetler, örneğin eğitim, kültür ve sanat -boş zaman da buna dâhildir- sermaye tarafından karşılığının ödenmesi gerekmeyen etkinlikler olarak görülmektedir:

Bu tartışmanın sonucu, doğadan, miras alınan bilgiden, pratik bilgiden, teknolojik bilgiden ve kamusal altyapılardan (sağlık, eğitim, tıbbi hizmetler, sosyal hizmetler, kültür, medya, siyaset vb. alanlardaki emek) oluşan toplumun müştereklerini şirketlerin bedavaya tükettiğidir. Dolayısıyla bilgi toplumunda

sömürünün önemli biçimlerinden biri, aynı zamanda çokluğun ve bir bütün olarak sömürülmesi olan müştereklerin sermaye tarafından sömürülmesidir (Fuchs, 2014b: 173).

Wittel (2019: 408)’de ücretsiz emeğin üç özelliği olduğundan bahsetmektedir: Bunlardan ilki ücretsiz emeğin bedava olmasıdır; çünkü karşılığında ödeme yapılmaz. Yukarıda belirtildiği üzere sermaye, ücretsiz emeği karşılığı ödenecek bir emek biçimi olarak görmemektedir. Bu nedenle gönüllü olarak yapıldığı varsayılır. İkincisi, ücretli emekle karşılaştırıldığında daha özgür hissettirebilir ve nispeten yabancılaşma oranı daha azdır. Bu durumun nedeni de ücretsiz emeğin eğlenceli olmasıdır ve icra edildiği yerin “Fabrika değil de daha çok bir oyun alanı gibi” olmasından kaynaklanır. Lazzarato (2016: 34), bu alanları “neoliberalizmin aygıtları” olarak görür ve “ilk kez hayata geçirildikleri alanlardan biri olan fabrikanın çok daha ötesine” uzandığından bahseder. Ona göre toplumsal makineler yalnızca emek süreçlerini değil, gündelik hayatın işlerliğini, yani en insani eylemleri (davranışları) de esir almıştır. Ücretsiz emeğin üçüncü ve son özelliği ise malumun ilanıdır: Ücretsiz emek sermayenin boyunduruğu altındadır ve sömürülmektedir.

Üretici güçler, işçilere ürettikleri malların değerinin altında ödeme yapmakta ve onları sömürerek kapitalist gelişmenin zeminini hazırlamaktadır. “Marksist kuramda hem kapitalizme neden olan gelişmenin hem de kapitalist gelişmenin temel kavramı üretici güçlerin genişlemesidir. Üretici güçlerin gelişmişlik düzeyi ise üretim için kullanılan teknoloji ve emek gücünün niteliği ile tanımlanmaktadır” (Başaran, 2016: 68). Meta üretiminde emek zamanı kadar mekânda önemli bir yer tutmaktadır ki Fuchs, bunu şu şekilde açıklar:

Emeğin, ekonominin merkezinde yer aldığını düşünürsek hem zaman hem de mekân, emeği anlamak için çok önemlidir. Belirli bir metanın üretimi için gereken emek, çoğu durumda tek bir mekânla sınırlanmamıştır ve yerkürenin etrafına yayılmış birbiriyle bağlantılı birçok mekânda gerçekleşir. Böylece sermaye, emek ve kaynaklar için yatırım maliyetlerini azaltmaya ve karları artırmaya çalışır (Fuchs, 2015: 24).

Fuchs’un vurguladığı nokta, meta üretiminde ve emek sömürüsünde mekân sınırının ortadan kalktığıdır. Kısacası artık dijital alanlarda sınır bulunmamaktadır ve emek metalaşmaktadır: “Neoliberal kapitalizm, iletişim dâhil neredeyse her şeyin metalaşmasına yol açmıştır. Dijital meta dünyasında, dijital emek gücünün, dijital içeriğin, dijital teknolojilerin ve çevrimiçi izleyicilerin metalaştığı”na şahit olunmaktadır (Fuchs, 2021b: 76). Buna her şeyin metalaşması da denilebilir ve bu durum, dijitalleşme sayesinde olanaklı hale gelmiştir. Sömürülme sırası dijital emektedir. Dijital emek için boş zamanda gerçekleştirilen, karşılığı ücret olarak ödenmeyen, bir nevi gündelik işlere benzetilen bir emek biçimi algısı

vardır. Sendikalaşma ya da çalışma hakları gibi konular bu emek türünde yer almaz. Dolayısıyla dijital emeğin algılanması zordur (Fuchs, 2015: 357). Ancak bugün kişilerin emek gücünün yanında dijital emeğinin de sömürüldüğü göz ardı edilemez. Bu nedenle son yıllarda gündeme gelen dijital emek çalışmaları, günümüz dijital ortamında gerçekleşen emek sömürüsünü açıklamada kullanılan önemli bir kuram olarak görülmektedir: “Dijital Emek çalışmaları, sosyal medya kullanıcılarını, sosyal medya fenomenlerini ve çeşitli iş pratiklerinin dijital teknolojiler tarafından yeniden şekillendirilme yollarını bünyesinde toplayarak hızla kendi başına bir alan haline geliyor” (Jarret, 2021: 139).

1.3.3.2. Dijital Ağlardaki Emek Biçimi: Kullanıcı/Ağ Emeği

Sanal dijital ağlar, giderek dijital tabanlı politik, ekonomik ve kültürel faaliyetlerin merkezi haline gelmektedir (Schuler, 2002: 71). Dijital ağların kullanıcılarının kimler olduğu sorusunun yanıtı açık bir ifadeyle çevrimiçi platformlarda etkileşime giren, dijital ürünü/hizmeti kullanan kişilerdir. Bu kişiler, ilgi alanlarına göre ya da bir nedeni olmaksızın etkileşen (iletişim kuran, bilgi arayan, eğitim alan, eğlenen vb.), bir anlamda dijital ağları var edenlerdir. Dijital ağlardaki her hareket, şirketler için değer üretmektedir. Bunlardan bazıları e-posta gönderme/alma, fotoğraf yükleme, blog yazma, yorum yazma vb.’dir. Aynı zamanda kullanıcılar hem fiziki hayattaki hem de sanal dünyadaki istek ve ihtiyaçlarını karşılamak için mal veya hizmet satın almaktadır; dolayısıyla kullanıcılar birer tüketicidir. Ancak kullanıcılar, ürün ya da hizmet tüketmenin yanında kimi zaman bunların üreticisi konumundadır. Tüketim mallarının ya da hizmetlerinin yaratılmasına aktif rol oynamaktadır. Tüketici her iki nedenden ötürü, ister üretim ister tüketim faaliyetinde bulunsun, dijital ağlarda yer alan bir “tüketici emeği”nin varlığından bahsetmek yanlış olmayacaktır.

Jarret (2021: 140), tüketici emeğinden bahsederken “kültürel ürünlerimizin onları platformlara yüklediğimiz anda el konularak yabancılaştırılmasının sayısız yolunu, fakat bunun yanında verilerimizin dijital medya şirketleri için artı değer üretmenin temel taşı haline gelmesini” vurgulamaktadır. Fuchs (2014a: 152)’a göre de ticari sosyal medyada kullanıcılara ödeme yapılmamaktadır. Dolayısıyla kullanıcıların tüm çevrimiçi zamanı, artı emek zamanı haline gelmektedir. Fuchs, kullanıcılara ödeme yapılmadığını ileri sürmekte haklıdır. Çünkü çoğu dijital medya şirketi, kullanıcın onlar için değer ürettiğini inkâr ederek, çoğu ücretsiz olan ürünlerinin bedava kullanılmasını ön plana çıkarmaktadır. Örneğin, “Facebook, enformasyonel kapitalizm çağında yükselen bu yeni bedava-hizmet modelinin tipik örneğidir. Bu yolla, bu yeni trendin parçası olma yoluyla, bizim internet etkinliklerimiz kapitalistler tarafından kara dönüştürülür” (Netchitailova, 2021: 6). Kullanıcılar emeğinin karşılığında

ödeme alamadığı gibi, ücretsiz kullanım bahanesiyle kişisel verilerini şirketlere teslim etmektedir.

Marx (2019)'a göre üretim araçlarına sahip olanlarla olmayanlar arasında çelişki vardır. Bu çelişki, geçmişten günümüze sınıf kavramının anlaşılmasına yardımcı olmaktadır. Örneğin eski dünyada köle sahibi, kölenin üretimde kullanmış olduğu ilkel aletlerin sahibiydi. Bugün de kapitalist sınıf üretim araçlarını elinde bulundurmaktadır. “O halde kapitalist üretim tarzının ve kapitalist sınıfın ayırıcı özelliği nedir?” sorusunun cevabı önem kazanmaktadır. Kapitalist üretim tarzı ile köleci üretim tarzının ayrıldığı nokta ücret karşılığı meta üreten işçilerdir (Eaton, 1996: 52). Çünkü eskiden köle, aynı zamanda sahibinin mülküydü ve kölenin çalışması zorunluydu; köle sahibi isterse onu öldürebilirdi (Fuchs, 2014a: 25). Ancak kapitalizmde işçi kapitalistin mülkü değildir ve emek gücü kiralanır; dolayısıyla işçi sınıfı var olmadıkça kapitalist üretim olamaz (Eaton, 1996: 52), dolayısıyla kapitalist sınıf da olmaz.

Kölelik, 1860'lı yıllarda dünyanın çoğunda resmi olarak kaldırılmış olmasına rağmen günümüzde tekrar ortaya çıktığına dair görüşler bulunmaktadır. Yaklaşık 167 ülkede 40,3 milyon insanın zorla çalıştırıldığı tahmin edilmektedir. Bu durum, kölelik mücadelesinin hala devam ettiğini göstermektedir. Dolayısıyla kölelik geçmişte kalmış bir olgu değildir; mücadele bugün farklı alanlarda sürdürülmektedir (Chomsky ve Waterstone, 2023: 321-322). Fuchs (2014b: 179)'a göre ise bugün sermaye için çalışan ücretsiz işçiler vardır ve artık “geleneksel sınıf kavrayışının ötesine geçmek” gerekmektedir. Qiu (2021: 207), dijital işçi, modern kölelik veya imal edilmiş kölelik gibi kavramlarının bugün farklı bir sınıfı temsilen sıklıkla kullanılmasının nedeninin, kapitalist şirketlerin kölelik anlayışı “dijital alanlara nasıl yayarız” düşüncesinde yattığını ileri sürer. Qiu (2021: 207, 212)'ya göre eski kölelik tipi ile yirmi birinci yüzyılın modern köleliği arasında paralellik bulunmaktadır. Eski tip kölelikteki sömürüyle dijital alandaki maddi olmayan ücretsiz emek, dijital emek ya da kullanıcı emeğinin sömürüsü benzer tiptedir. Kölelikte, tüm gün iş zamanıdır ve sömürü sınırsızdır; ayrıca hem köle emeğinde hem dijital emekte “oyun zamanı, çalışma zamanıdır” (Fuchs, 2015: 395). Aynı şekilde dijital ortamlarda günün her saati çalışmayı ve sömürüyü olanaklı kılmaktadır. Bir başka benzerlik ise emek gücü ile alakalıdır: “Her ikisi de emek piyasasında emek gücünü bir meta olarak satmazlar” (Fuchs, 2015: 395).

Öte yandan iki tip kölelik tarzında mevcut olan benzerliklerin yanında bazı farklar da bulunmaktadır. Emeğin niteliği bakımından fiziksel ve zihinsel çalışmanın farkları vardır: “Köle çalışması, fiziksel olarak yorucu ve oyun gibi hissettirmeyen, zahmetli ve elle yapılan bir çalışma iken, dijital emek, neredeyse sırf veya yüksek düzeyde oyun gibi hissettiren enformasyon çalışmasıdır” (Fuchs, 2015: 395). Yine önemli farklardan biri baskı biçimidir.

Fuchs'un yukarıda verilen alıntısında köle sahibinin kölesini baskıyla/zorla çalıştırdığından ve onu istediğinde öldürebildiğinden bahsedilmişti. Lazzarato (2016: 38-39), modern köleliğin baskı veya ideoloji ile çalışmadığını vurgular ve insanı “bilinçaltı imal ederek” ele geçirdiğini ileri sürer. *Dijital kölelikte görünürde bir baskı yoktur; baskı zihinlerdedir.*



İKİNCİ BÖLÜM

SÖMÜRGEÇİLİĞİN DİJİTAL BİR FORMU OLARAK MOBİL UYGULAMA ARACILI VERİ SÖMÜRGEÇİLİĞİ

Bu bölüm öncelikle, yeni bir sömürgecilik türüne; “veri sömürgeçiliği” olarak adlandırılan bir sömürgecilik formuna odaklanmaktadır. Bu bağlamda mobil iletişimde kritik öneme sahip olan mobil uygulamalar ve mobil uygulamalar aracılığıyla gerçekleşen veri sömürgeçiliği incelenmiştir. Bölüm, merkeziyetçi bir yapılanmaya sahip olan mobil uygulamalardan, merkezi olmayan uygulamalara doğru evrilen, blok zinciri tabanlı sistemin çeşitli boyutları, çalışma konusu kapsamında incelenmiştir.

2.1. Dijital Dünyanın Verimli Toprakları: Kişisel Veriler ve Veri Hâkimiyetinde Sömürgeçiliğin İzleri

Bu başlık altında, tarihsel olarak sömürgeçiliğin tüm yönlerini derinlemesine ortaya koymak gibi bir amaç bulunmamaktadır. Amaç, sömürgeçiliğin etkilerinin tamamen yok olmadığını, dijital bir formunun ortaya çıktığını ve sömürgeçiliğin bıraktığı mirasın istilacı şirketler tarafından devam ettirildiğini göstermektir. Bunun en önemli göstergesi ise günümüz sömürgecilik tarzının, tarihsel sömürgecilikte uygulanan sömürü taktiklerine benzer bazı yöntemleri kullanmasıdır. Eskiden olduğu gibi bugün de sömürgeci güçler, sömürgeleştirdiği bölgelerden çıkardığı kaynakları kullanarak zenginleşmektedir. Eski sömürgeci güçler, tarihsel olarak bakıldığında bazı ulus devletler, sömürgeleştirilenler ise savunmasız kabileler, halklardır. Günümüz sömürgeci güçleri de bazı teknoloji şirketleridir ve bugünün sömürgeleştirilenleri de sömürgeci şirketlerin ürünlerini kullananlardır.

Üretim ilişkileri bakımından tarihsel sömürgecilikte, sömürgeleştirilen ülkelerden çıkarılan kaynaklar nasıl sanayileşme için –ve dolayısıyla daha fazla güçlenmek için- kullanıldıysa, bugün de kişilerden çıkarılan veriler, teknoloji şirketleri tarafından daha fazla teknolojik yatırım için ve bu yatırımlarla daha fazla alana yayılmak için kullanılmaktadır. Tüketim ve bölüşüm ilişkileri bağlamında değerlendirme yapılacak olunursa tarihsel sömürgecilikle günümüz veri sömürgeçiliği arasında benzerlikler göze çarpmaktadır. Sömürgeleştirilen ülkelerden çıkarılan hammaddeleri, ülkelere ihraç edip üretilen malları yeniden sömürdüğü ülkelere satan sömürgeci devletlerin rolünü, günümüzde şirketler üstlenmektedir. Dünyanın dört bir yanındaki kullanıcılardan veri çıkaran şirketler, bunları kendi sunucularında depolamakta ve işlemektedir. Ve yine tarihsel sömürgecilikte olduğu gibi

veri sömürgecilğinde de bölüşüm dengesizdir. Sömürülenler üzerinde egemen olan sömürgeci güçler, hammaddelelerin üzerinde olduğu gibi veriler üzerinde de kontrol sahibidir.

Veri, enformasyon ve bilginin yapı taşlarını oluşturan materyal olarak kabul edilmektedir (Kitchin, 2014: 3). Couldry ve Mejias (2022: 13), veriyi yalın ve anlaşılır bir şekilde açıklamışlardır: “*Veri* derken neyi kastediyoruz? Kastettiğimiz şey bir kâğıt parçasına bir alışveriş listesi karalanması değil. Ancak liste eğer bir cep telefonuna, belki de Google’ın Keep [not alma] uygulamasına girilmişse, kastettiğimiz şey odur”. Genellikle dijital dünyanın hammaddesi olarak görülen veriler, sayı, metin, fotoğraf ve video gibi birçok farklı formda bulunabilmekte (Pandare vd., 2022: 16) ve bu veriler insan hayatına dair bilgiler içerebilmektedir. Veriler bir bakıma “İnsan yaşamının bütün biçimlerinden toplama ve işleme altyapılarında geçen enformasyon akışlarıdır” (Couldry ve Mejias 2022: 13); dolayısıyla bireyi tanımlayabilecek her veri de kişisel veri haline gelmektedir. Sonuç olarak kişisel veri de “... kişilerle gerçek ya da potansiyel bağlantıları olan ve onlardan ya da başka kişi veya şeylerden toplanan veriler” (Couldry ve Mejias, 2020: 19) olarak tanımlanabilir.

Günümüzde kişisel veriler, ekonomik bir kaynak olarak görülmektedir. Bu değer, *yeni kapitalizmin* hayati bir bileşenidir: Verilerin geç kapitalizm ekonomisi içinde teorik bir değeri vardır; bu veriler, birçok endüstrinin sosyal, ekonomik ve politik yönetim teknolojisi için çok önemli hale gelmiştir (Gandy, 1993: 92). Jathan Sadowski (2019: 2) de verilerin sosyal, politik ve ekonomik boyutlarına ilişkin mevcut literatürün, verileri meta olarak ele almakta olduğunu ifade eder. İster örtük ister açık bir biçimde hem akademide hem de medya kuruluşlarındaki analizler, tipik olarak bu analitik çerçeveyi verili kabul etmektedir. Örneğin Fuchs (2021b: 84-85)’a göre “Kişisel veri, kullanıcıların profillerine hedefli reklamlar gösterme yetkisine sahip reklamcı müşterilere satılan, kullanıcıların dijital emeği tarafından üretilmiş bir metadır”. Ancak Sadowski (2019: 1), sermaye ile meta arasında ayrım yapar ve verilerin her zaman meta olarak varsayılamayacağını söyler: *Veriler artık bir sermaye biçimi haline gelmiştir*. Andrew Iliadis ve Federica Russo (2016) da veriyi metadan daha fazlası olarak görür; onlara göre *veri, bir iktidar biçimidir*. Iliadis ve Russo’nun bu değerlendirmelerinde vurguladıkları veri iktidarı, dijital alanda ekonomik, sosyal ve kültürel iktidarın sahibi olmanın anahtarı konumundadır. Tarihçi ve yazar Yuval Noah Harari’nin 2018 Dünya Ekonomik Forumu’ndaki konuşması da bu savı destekler niteliktedir. Harari, konuşmasında verilerin dünyadaki en önemli varlık haline geldiğini söylemiş; veriye sahip olan ve onu kontrol edenlerin sadece insanlığı değil, yaşamın geleceğini de şekillendireceğini iddia etmiştir (Harari, 2018). Patrik Hummel vd. (2021: 1) de verilerin dünyamızın büyük bir kısmına yön verdiğini ileri sürerken; son yıllarda yeni veri güdümlü teknolojilerin ve bunların

altyapılarının geliştirilmesi ve uygulanmasına ilişkin tartışmalarda Veri Egemenliği (Data Sovereignty) kavramının ortaya çıkışına tanık olduğunu söylemektedir.

Bireylerin, belirli grupların veya toplulukların verilerinin işlenmesi üzerindeki kontrolü ellerinde tutması gerektiğine dair az çok fikir birliği vardır (Hummel vd., 2021: 1). Bu inancın bu denli başarılı olmasının nedeni, kitlelerin -safça ya da farkında olmadan- kişisel bilgilerini kurumsal platformlara emanet etmesidir. Böylelikle *güven* kavramı da tartışılır hale gelmektedir. Dolayısıyla kişilerin bilgilerini teslim etmede bir sorun görmediği bu medya ekosistemine daha eleştirel bir gözle bakılması gerekmektedir (Dijck, 2014: 198). Kullanıcılar, verileri üzerindeki haklarından feragat ettikçe -ya da hak talep etmedikçe- kendine ait verilerin sömürüsüne maruz kalmaya devam edeceklerdir.

Veri egemenliği kavramı, bireyin başkalarıyla bağlantı kurma ve bilgi paylaşma haklarını kapsamaktadır (Hummel, vd., 2018: 7). Dolayısıyla veri egemenliği, veri özneleri üzerindeki kontrol ve sahiplik ile doğrudan ilişkilidir. Günümüzde, kişisel verilerin kontrolünün büyük teknoloji şirketlerinin elinde olduğu bilinmektedir. Bu şirketler, sahip oldukları yaygın ve etkin yazılım ürünleri sayesinde kimi zaman yasal olmayan kimi zaman da mevcut yasalardaki boşlukları kullanarak -lehine çevirerek- giderek daha fazla veriye erişme imkânı elde etmektedir. Bu durum, kişisel veri istismarı ile sonuçlanabilmektedir: “Dijital ortamlarda kişiler kendilerine ait mahremiyet bölgelerini koruyamamakta ve kişisel verileri üzerindeki kontrolü kaybetmektedir. Böylelikle kişisel verilerin korunması özel hayatın gizliliği bağlamında daha da önemli bir konuma gelmektedir” (Taşkaya ve Talay, 2019: 372). Bu nedenle, veri öznelerinin egemenliğini korumak için, kişisel hakların yanı sıra özgürlük haklarının da yasalaştırılabilmesini, saygı gösterilmesini ve bunların uygulanabilir hale getirilmesini sağlamak için ek yasal mekanizmalara ihtiyaç duyulmaktadır (Hummel, vd., 2018: 5).

Öte yandan, veriler üzerinde kontrolü bulunan şirketlerin günümüz kuralsızlaştırma (deregulation) ortamında ek yasal mekanizmalar bir tarafta dursun, mevcut yasalara ne ölçüde uydukları tartışmalı bir konudur. Örneğin 2016 yılında Avrupa Birliği (AB)’nin Genel Veri Koruma Yönetmeliği (GDPR- General Data Protection Regulation), dünya çapında birincil kapsamı veri gizliliği olan bir yasa olarak kabul edilmiştir. Bu yasa, AB vatandaşlarına geniş bir haklar yelpazesi tanımıştır. Bunlar arasında, şirketlerin kişiler hakkında topladığı verileri silme hakkı, kişisel bilgilerin satılmaması hakkı ve kişisel veriler üzerinde bireysel özerklik sağlama gibi bir dizi hak bulunmaktadır. Ancak bu süreçte Meta, Apple ve Amazon gibi şirketler, veri gizliliğini düzenlemeye yönelik tasarlanmış olan yasaları aşmak için kullanılan bir olgu olan deregülasyondan faydalanmışlardır. Şirketler, özellikle gizlilikle ilgili söylemleri

kendi lehlerine çevirerek ve kişisel verileri korumak için güvenilmesi gerekenin kendi sistemleri olduğunu savunmuşlardır (Krupp, 2022: 875).

Helen Nissenbaum (2017), “Deregulating Collection: Must Privacy Give Way to Use Regulation?” adlı çalışmasında yasal düzenlemelerin yeterliliğini sorgulamıştır. Veri gizliliği konusundaki deregülasyonun kişisel verileri toplayan ve kullanan şirketler tarafından hesap verebilirliğin azalmasına yol açabileceğini belirtirken, tüketicinin korunmasını etkileyebileceğini, aynı zamanda şirket birleşmelerini, satın almaları ve devralmaları motive edebileceğini belirtmekte ve bu durumun oldukça olumsuz sonuçları beraberinde getirebileceğini savunmaktadır. Nissenbaum veri mahremiyetini korumak için veri toplamının düzenlemelere tabi olmasını da yeterli bulmamaktadır. Ona göre yasal düzenlemeler, verilerin toplandıktan sonra kötüye kullanımını göz ardı etmektedir. Nissenbaum ayrıca veri mahremiyetini korumak ve verilerin kötüye kullanıma karşı korunmak için veriye erişimin seçici olarak azaltılmasının gerekebileceğini öne sürmektedir. Ancak hem ek yasal mekanizmaların devre alınması hem de veriye erişimin azaltılması, gittikçe daha fazla veri talep eden şirket sayısının artması ve bu şirketlerin yasal düzenlemelerle mücadele halinde olmaları nedeniyle kişilerin değil de şirketlerin verilere egemen olmaya devam edeceğinin göstermektedir. Alexander F. Krupp (2022: 918), yine de verilerin sorumlu bir şekilde işlenmesine yönelik kapsamlı ve düşünceli bir yaklaşımın olması gerektiğini ileri sürmektedir. Günümüzde mahremiyetin zor olabileceğini ancak imkânsız da olmadığını vurgularken, şirketlerden korunmanın yine hukukun işlevlerinden yararlanılması gerektiğini ifade etmektedir.

2.1.1. Sınır Tanımayan Sömürgecilik: Veri Sömürgeciliği

Tarihsel olarak egemenlik, bir alana ilişkin mutlak gücü, örneğin egemen bir ulus devletin kendi topraklarındaki gücünü ifade etmektedir (Hummel, vd., 2018: 1). Sömürgecilik ise güç ya da zorlama ile bir ülkenin veya grubun bir başka ülke veya insan grubu üzerinde hâkimiyet sağladığı bir sistemi tanımlar. Sömürgecilik kavramının farklı coğrafyalarda farklı karşılıkları bulunmaktadır. Örneğin, “Rusya’da toprak genişlemesiyle sömürgeleştirme hareketleri neredeyse eş anlamlıdır. Oysa Batı dünyasında bu iki sözcük titizlikle birbirinden ayrılır; toprak genişlemesi ulusal bir konu, denizaşırı hareketler sömürgecilik olarak adlandırılır” (Ferro, 2017: 21). Ancak sömürgecilik hakkındaki bu iki farklı bakış açısı, 16. yüzyıldan başlayarak, 20. yüzyıla kadar bir kişinin ya da bir zümrenin zenginleşmesi için milyonlarca yerlinin katledilmesi ve doğal kaynakların yok edilmesi gerçeğini değiştirmemektedir (Couldry ve Mejias, 2020: 19). Günümüzde de benzer bir durumla karşı

karşıya kaldığımız söylenebilir. Kişileri etkileme gücü ve ekonomik değeri karşısında verilere egemen olmak isteyen ulus-aşırı şirketler, dünyanın her yanında verileri çıkarma ve sunucularında depolama yarışına girmişlerdir. Emperyalist taktikler bugün de devam etmekte, dijital çağa göre güncellenen hamlelerle tekrar edilmektedir (Sadowski, 2019: 3).

Bugün, dijital dünyanın veri savaşlarında sömürgeciliğin izlerini görmek mümkündür ve *Veri Sömürgeciliği (Data Colonialism)* olarak adlandırılan bir kavram ortaya çıkmıştır. Couldry ve Mejias (2020: 11), global bir veri çıkarma sürecine atıfta bulunur ve veriyle sömürgeleştirmeye vurgu yapar:

“İnsan deneyimi, imkân dahilinde bu deneyimin her bir katmanı ve yönü karlı çıkarmanın [extraction] hedefi haline geliyor. Bu duruma *veriyle sömürgeleştirme* diyoruz. Veriyle sömürgeleştirme, kapitalizmin kendisinin bugün nasıl evrimleştiğinin önemli bir boyutunu ortaya koyuyor” (Couldry ve Mejias 2022: 11).

Couldry ve Mejias (2020: 19), veri sömürgeciliği kavramını kullanırken, tarihsel sömürgeciliğin kullandığı fiziksel şiddetle ilişkili bağlantılardan ya da birebir benzetmelerden ziyade “kaynak düzenleme konusunda yaptığı normalleştirmeleri ve kamulaştırmayı doğalmış gibi gösterecek biçimde, toplumsal ilişkileri yeniden tanımlayışı ile ilgili paralellikleri keşfetmeyi” amaçlamışlardır. Veri sömürgeciliği, yağmacı ve çıkarımcı tarihsel sömürgecilik pratiklerini bünyesinde barındırmaktadır. Sömürgecilik nasıl endüstriyel kapitalizmin doğuşunu sağlayan koşulları yarattıysa, veri sömürgeciliği de yeni bir kapitalizm biçiminin ön koşullarını sağlamıştır (Couldry ve Mejias, 2020: 16). Yine Couldry ve Mejias (2022: 48)’a göre “Veri sömürgeciliğinin kendine özgü bir coğrafyası vardır”. Veri sömürgeciliğinin de tarihsel sömürgeciliğe benzer şekilde global emelleri bulunmaktadır; ancak veri sömürgeciliği tarihsel sömürgecilikten farklı olarak bireylerin yaşam koşullarına her nerede olurlarsa olsun nüfuz edebilir. Veri sömürgeciliğinin bir farkı da genişlemedir. Tarihsel sömürgecilik, coğrafi bölgelerin kaynaklarını sahiplenerek genişlerken, veri sömürgeciliği insan yaşamını sahiplenerek genişlemektedir (Couldry ve Mejias 2022: 31-48). Burada vurgulanan nokta, insan yaşamından (sosyalitelerinden) çıkarılan kaynaklara; insandan çıkarılan davranış verilerine sınırsızca el konulmasıdır; “Buradaki ideal, her zaman, neticede dünya ve içindeki her şeyi tarif eden, sürekli genişleyen sınırlardır” (Zuboff, 2021: 170). Veri sömürgeciliği, sınırlarını sosyal ilişkilerin içine doğru genişletirken, giderek “yeni toplumsal ilişkilerin (bilgi işlemesine ham girdiler oluşturan veri ilişkileri), yeni ekonomik değerlerin yaratıldığı anahtar bir araç halini” almaktadır (Couldry ve Mejias, 2020: 26).

Söz konusu mobil uygulamalar olduğunda veri sömürgeciliği, başlıkta da yazıldığı üzere adeta sınır tanımamaktadır. Mobil uygulamalar aracılığı ile gerçekleştirilen veri sömürüsü, giderek daha fazla verinin gözetimini gerekli kılmaktadır. Kullanıcının her türden verisi izlenmekte, bilgisi dâhilinde veya dışında toplanmakta ve sömürülmektedir. Örneğin, bazı uygulamalar kullanıcılarından hem *aktif* hem de *pasif veri*²¹ toplamak üzere üretilmiş gibidir. Google Opinion Rewards (GOR)’da bu uygulamalardan biridir ve kullanıcılarından anket verisi toplamaktadır. Uygulama, gönüllü veri paylaşımını ödüllendiren bir mekanizmaya sahiptir ve kullanıcı, uygulamanın kendisine ilettiği anketleri doldurarak değişen miktarlarda para ödülü kazanmaktadır (Talay ve Çelik 2023: 93-96). GOR, birçok uygulama gibi kullanıcının aktif verisini toplarken aynı zamanda pasif verisini de toplamaktadır. Kişilerin açık rızasının alınarak, bilerek ve isteyerek paylaşılan verilerin (aktif veri), kullanıcı iradesi açısından özgür bir eylem olduğu gibi görülse de ödül kazanmanın yarattığı cazibe kullanıcıların kişisel veri paylaşımını teşvik ve motive etmektedir. Neticede gündelik hayatın nicelleştirilmesi karşılığında, bireylere bazı avantajlar ya da onlara göre zevkli olabilecek bazı deneyimler sunulmakta (Thatcher, vd., 2016: 997-998), bu deneyimin karşılığında inşa edilen göstermelik rıza sayesinde kişisel verilere el konulmaktadır. Ayrıca GOR uygulamasının kullanıcının rızası dışındaki (pasif veri) verileri de toplayabilmesi, açıkça veri istismarıdır. Öte yandan anket yanıtlarını toplayan GOR, verileri anket için para ödeyen üçüncü taraf şirketlere/araştırmacılara -bazı veriler Google ürünlerini geliştirmek için kullanmaktadır- aktarmaktadır (Talay ve Çelik 2023). Google, hem üçüncü taraf şirketler/araştırmacılardan anket yayınlama karşılığında gelir elde etmekte, hem üçüncü tarafların topladığı verilere erişmekte, hem de kendi ürünlerini geliştirmek için kişilerin aktif ve pasif derin verilerini sömürmektedir.

Veri sömürgeciliği, insan yaşamının ticari amaçlarla kullanılması amacıyla ortaya çıkan bir düzenin uzantısıdır. Bu düzen içinde insan yaşamından sürekli olarak veri çıkarılır. “Bu çıkarma, *veri ilişkileri* aracılığıyla, bunların birbirleriyle ve dijital araçların imkân tanıdığı bu dünya ile etkileşim yolları aracılığıyla, işlevsel hale getirilir” (Couldry ve Mejias 2022: 14). Veri sömürgeciliğinin temelinde, veri ilişkileri adı verilen yeni bir sosyal ilişki

²¹ Kullanıcıların bilgisi doğrultusunda toplanan veriler aktif veri (örneğin, anketler, formlar), bilgisi doğrultusunda olmadan toplanan veriler pasif veri (örneğin, konum, sağlık verisi) olarak adlandırılmaktadır (Maher vd., 2019: 242; Jäcke, vd. 2019: 899). Ancak bu tanımlar karışıklığa neden olabilmektedir. Bu nedenle aktif verinin, kullanıcının bilgisi dahilinde geri bildirimde bulunduğu veriler olarak tanımlanması daha doğru olacaktır. Çünkü günümüzde pasif veriler de kullanıcının bilgisi dahilinde toplanabilmektedir. Dolayısıyla pasif veriler için kullanıcının aksiyonda bulunmadığı, yani herhangi bir geri bildirime gerek olmadan toplanan veri olarak tanımlanması daha doğru olacaktır.

türünün yaratılması vardır. Veri ilişkileri, verilerin ticari olarak kullanılabilmesini sağlayan beşerî bir ilişki olarak tanımlanabilir. Bu ilişkiler aracılığıyla dünyanın her yerindeki toplumsal yaşam, sermaye için bir kaynak haline gelmekte ve veri çıkarımına açık bir kaynak olarak görülmektedir. Veriler, insan yaşamının soyutlaştırılmasıdır. Bu soyutlaştırma, kişilerin toplumsal ilişkiler aracılığıyla rıza gösterdiği noktalarda gerçekleşir, hatta geçmişe dönük bile olabilir. Bu süreçte veriler giderek artan bir şekilde ticarileştirilmiştir. Endüstriyel kapitalizm, emeği soyut bir boyuta dönüştürerek (emeğin ticarileşmesi) evrensel bir insan aktivitesi olan emeği bir sosyal forma dönüştürerek toplumu değiştirmiştir. Bugün de veri sömürgeciliği, insan yaşamını ticarileştirmek için olgunlaşmış bir soyutlanmış sosyal biçim olan verilere dönüşerek toplumu değiştirmektedir. Bu değişim, toplumsal yaşamdaki ilişkileri de dönüşüme uğratmaktadır. Yukarıda da bahsedildiği üzere üretim ve tüketim ilişkilerinin dönüşüme uğraması gibi emek ilişkileri de dönüşüme uğramıştır: Emek ilişkileri giderek veri ilişkilerine evrilmektedir. Ve dolayısıyla zamanla, gündelik yaşama tam olarak yerleştiğinde veri ilişkilerinin emek ilişkileri kadar doğallaşması muhtemeldir (Couldry ve Mejias, 2019: 2; Couldry ve Mejias, 2020: 16-41, 61).

Veri ilişkileri, mobil uygulamalar ekseninde değerlendirildiğinde şirket ve kullanıcı arasında bir veri ilişkisinin olduğu ortaya çıkmaktadır ve bu ilişkinin emek ilişkisine benzer bir biçim aldığı söylenebilir. Neticede uygulamalarla etkileşime giren kullanıcılar, içerik paylaşım yaparak, geri bildirimde bulunarak veya uygulamanın gelişimi ve daha iyi çalışabilmesi için katkıda bulunarak, uygulama geliştiricisi ile bir emek ilişkisi içerisine girmektedir. Ayrıca kullanıcıların kişisel verilerinin şirketler tarafından pazarlama ve reklamcılık faaliyetlerinde kullanılması sonucu da bir değer üretiminden bahsedilebilir. Kullanıcılar uygulamayı kullanmanın karşılığı olarak şirket için değer üreten bir uygulama işçisi/emekçisi gibi bir konumlanmaktadır. Örneğin yukarıda bahsedildiği üzere GOR uygulaması kullanıcılarının Google'ın bizzat kendisine çalışan, onun marka değerine ve ürünlerine görece düşük miktarlarda ödül karşılığında kişisel verilerini aldırış etmeden teslim eden bir uygulama işçisi gibi hizmet ettiği gösterilmiştir (Talay ve Çelik, 2023: 96).

Öte yandan birçok uygulama kullanıcılar için giderek vazgeçilmez hale gelmektedir. Bu uygulamaların bazıları Facebook, YouTube, TikTok, X (Twitter) ve Instagram'dır. Bu uygulamaların iş modelleri, içerik üretimine ve dağıtımına dayalıdır ve ortak noktalarından biri kullanıcıların uygulama içeriklerine erişerek iletişim kurmasıyken kullanıcılarından bazılarının aynı zamanda içerik üreticisi olmalarıdır. Bu uygulamaların içerik üreticileri uygulamanın bir nevi çalışanı, geliştiricisi ise işveren konumunda gibi görünmektedir. Ayrıca içerik üreticisinin ürettiği değer karşılığının genel kabul gören herhangi bir ölçütü

bulunmamaktadır. Bu nedenle geliştirici-içerik üretici arasında uzlaşılan bir ücret söz konusu değildir. İçerik üreticilerin de kabul etmiş olduğu iş ortağı sözleşmeleri de dolayısıyla tek taraflıdır. Bu durum, bir bakıma emek biçimlerindeki değişimin, yani maddi olmayan emek biçimlerinin mobil uygulamalarda da var olduğunun göstergesi olarak görülebilir.

Bir olguyu verileştirmek, onun tablolastırılabilmesi ve analiz edilebilmesi için sayısallaştırılmış bir forma sokmak demektir. Ancak verileştirme, salt dijitalleşme ile açıklanabilecek bir süreç değildir. Verileştirme (Datafication) ile insan yaşamının geniş alanları, büyük ölçekte otomatikleştirilebilen analiz biçimleriyle işlenmeye açık hale gelmiştir (Mayer-Schönberger ve Cukier, 2013: 78). Verileştirme teriminin analitik değeri, insan yaşamına yönelik verilere el konulması yoluyla günümüzde yeni bir veri çıkarma biçiminin ortaya çıktığı süreçleri ve çerçeveleri isimlendirme yeteneğinde yatmaktadır. Verileştirme süreci ise çok katmanlı ve globaldir; çoğunlukla şirketler ve devletler tarafından sahip olunan veya kontrol edilen dağıtım, erişim, depolama, analiz ve gözetim mekanizmalarını içermektedir (Mejias ve Couldry, 2019: 3-7).

Verileştirme paradigmasını destekleyen araştırmacılar, verilerin doğal izler olarak görüldüğü ve platformlar için iş akışlarını kolaylaştırdığı iddialarını tekrarlama eğilimindedir (Dijck, 2014: 198). Ancak verileştirme, iki süreci birleştirmektedir: İnsan hayatının nicelleştirme süreçleri yoluyla veriye dönüştürülmesini ve veriden farklı türlerde değer üretilmesini (Mejias ve Couldry, 2019: 3). Verilerde olup bitenleri sömürgeci bir hamle olarak kabul etmek, bugün verileştirme yoluyla yapılmakta olan kaynak sahiplenmesinin tam kapsamını kabul etmek anlamına gelmektedir. Toplumsal deneyim alanlarının yeniden inşasının bir parçası olarak doğrudan sermayeye ilhak edilebilmesi için sahiplenilen şey insan yaşamının kendisidir. Ekonomik sömürü için mevcut kaynaklarda böylesi bir değişimin tek bir tarihi emsali vardır, o da 15. yüzyılın sonları ve 16. yüzyılın başlarında sömürgeciliğin ortaya çıkışıdır (Couldry ve Mejias, 2019: 2). Verileştirme de tarihsel sömürgeciliğe benzer biçimde doğal kaynak olarak görülen insan hayatının ve deneyiminin sömürsünü doğallaştıran oldukça kritik bir sürecin bir parçasıdır.

Mobil uygulamalardaki verileştirme pratikleri de kullanıcı verilerinin doğrudan sermayeye aktarılmasını doğallaştıran taktiklerle işler hale getirilmektedir. Bu taktikler, kullanıcı deneyimini iyileştirme, kişiselleştirme, ödül mekanizmaları ve oyunlaştırma (gamification) olarak gösterilebilir. Bu taktikler sayesinde uygulamanın kullanıcıya daha iyi bir deneyim sunacağı vaadi verilmekte ya da kullanıcıya bir amaç sunularak ve oyun hissiyatı verilerek veri toplama doğallaştırılmaktadır. Örnek verilecek olursa, kullanıcı için daha işlevsel bir uygulama kullanabilmesi için, uygulama içerisindeki hareketleri

verileştirilmektedir. Kullanıcı, uygulamayı kullanırken veya oyun oynarken oyunlaştırma taktiği kullanılarak uygulamayla/oyunla ilgili kişiye herhangi bir ayrıcalık tanınmaktadır. Bu taktik sayesinde kullanıcının ilgi alanları belirlenerek verileştirilmektedir.

Vericilik (Dataism) terimi, insan faaliyetleri hakkında veri toplama, harmanlama ve analiz etmenin yeni yollarını içeren büyük verinin, insan hayatının tüm alanlarında ilerlemeye önemli bir katkı sağlayacağını öne süren bir ideolojiyi tanımlamak için kullanılmaktadır (Devlieghere vd., 2022: 328). Vericilik, büyük veri teknolojilerinin kullanımını destekleyen ve verilerin bilgelik ve değere sahip olduğunu varsayan bir ideolojidir ve büyük veri teknolojileri için faydalı terimlerle -genellikle de tekno-liberal bir tatla- yeniden yorumlanan bir *büyük veri zihniyeti* yaratmaktadır (Adamczyk, 2023: 4-7). Bu tekno-liberal görüşe göre vericilik, bilinçli kararlar almak ve sorunları çözmek için veri kullanımına dayanan bir felsefedir. Verilerin, daha iyi kararlar almak için kullanılabilir olacak eğilimler ve kalıplar hakkında içgörüler sağlayabileceği fikrine dayanmaktadır. Kalıpları ve içgörülerini ortaya çıkarmak için verileri analiz etmeyi ve bu içgörülerini karar vermek için kullanmayı içeren bir veri odaklı karar verme biçimi olarak da görülmektedir (Pandare vd., 2022: 17). “Dataizm [Vericilik], olan ve olacak olan her şeyi hesaplamak ister” (Han, 2022: 14).

Vericiliği bir iletişim süreci olarak yorumlamak, vericiliğin büyük veriyle ortaya çıkan deneyimleri adlandırma gücünü merkeze almak demektir. Bu açıdan bakıldığında, son yirmi yılda vericiliğin yükselişinin itici gücü, ortaya çıkan büyük veri teknolojileriyle ilgili yeni deneyimlerden insan soyutlamasının ve bu deneyimler hakkında iletişim kurma ihtiyacının bir işlevi olarak kolayca tanımlanabilir (Adamczyk, 2023: 10). Verileştirilmiş izler, pazarlamayı hedeflemek, sağlığı yorumlamak, siyasi tutumu ölçmek ve insan davranışını ölçen, manipüle eden veya diğer herhangi bir şekilde kullanılabilir. Büyük veri zihniyeti ve onun verileştirme dürtüsü, nicelleştirmenin nesnelliğine olan inancı açığa çıkarmakta ve sadece nicelleştirme yapan kurum ve kuruluşlara değil, aynı zamanda verileri yorumlamak için kullandıkları algoritmaların öngörüselle doğruluğuna olan güveni de sarsmaktadır. Büyük veri zihniyetinden doğan retoriğe duyulan kamu güveni, büyük verinin mantığı, kuralları ve açık işleyişi kullanıcıların yaşamlarına ilişkin olasılıkları belirlemeye çalışan bir sosyal sistem içine gömülmesine neden olmaktadır. Bu sistemin belki de en yaygın örneği, Google’ın kapitalist yaşam biçimlerini teşvik eden algoritmalar oluşturmak için toplanan verileri nasıl kullandığıdır (Adamczyk, 2023: 7).

Veriyi yücelten bu ideoloji, verinin üstün özelliklerini vurgulamakta ve veriyi teknolojik ilerlemenin anahtarı olarak sunmaktadır. Bu ılımlı bir yaklaşımdır ve toplumda yol açabilecek potansiyel olumsuzlukları göz ardı etmektedir. Başta veri mahremiyet kaygıları

olmak üzere, kişisel hak ve özgürlüklerin sınırlandırılmasına ve eşitsizliklere neden olabilmektedir. Baştan beri vurgulanan ve özellikle verilerin belirli çevreler elinde toplanması ve toplumları kontrol edebilecek düzeyde bir manipülasyon aracı olarak kullanılması, buradan elde edilen gücün yine belli sınıfların/zümrelerin çıkarlarına hizmet etmesiyle sonuçlanmasına neden olmaktadır. Bu durum, güç dengelerini sarsarak sosyal adaletsizliğe ve eşitsizliğe mal olabilmektedir. Sonuçta bu ideoloji, görünürde demokratik mekanizmalarla donatılı; ama totaliter rejim benzeri karaktere -bireysel özgürlük ve baskıcı bir karakter- bürünebilecek tehlikeli bir ideoloji olarak görülmelidir.

Veri Gözetimi (Dataveillance), ilk olarak Roger Clarke (1988) tarafından ortaya atılan bir kavramdır; insanların ya da grupların, davranışlarını düzenlemek ya da yönetmek amacıyla kişisel veri sistemleri aracılığıyla sistematik olarak izlenmesi anlamına gelmektedir (Esposti, 2014: 209-210). Geleneksel gözetim, bir veya daha fazla kişinin eylemlerinin veya iletişimlerinin sistematik olarak araştırılması veya izlenmesi; birincil amacı genellikle bu kişilerin, faaliyetleri hakkında bilgi toplamaktır. Temel biçimi fiziksel gözetimdir; izleme ve dinlemeyi (görsel ve işitsel gözetim) içerir. Veri gözetimi ise bir ya da daha fazla kişinin eylemlerinin ya da iletişimlerinin araştırılması ya da izlenmesinde kişisel veri sistemlerinin sistematik olarak kullanılmasıdır. Veri gözetimi, görece teknik ve ekonomik olarak daha üstündür. Ayrıca, veri gözetimi geleneksel yöntemlerden daha ucuz olduğu için, daha fazla kuruluşun daha fazla kişiyi izlemesi yönünde bir eğilim vardır: *Hem kişisel hem de kitlesel gözetim rutin hale gelmektedir* (Clarke, 1988: 499-511). Bu nedenledir ki veri gözetimi giderek geleneksel gözetim tekniklerinin yerini almaktadır. Bu eğilimle birlikte, daha etkili koruma önlemleri ve resmi bir politika çerçevesi gerektiren kişisel veri izleme ve kitlesel veri izleme gibi yeni izleme yöntemleri ortaya çıkmaktadır (Clarke, 1988: 498). Dijck (2014: 205)'a göre de veri gözetimi (kişilerin, çevrimiçi verileri temelinde izlenmesi) en az bir önemli konuda geleneksel gözetimden farklıdır: Gözetim belirli amaçlar için (kamu güvenliği, terörle mücadele, nüfusun yönetimi veya salgın hastalık kontrolü) izlemeyi varsayarken, veri gözetimi önceden belirtilmemiş amaçlar için meta verilerin sürekli izlenmesini gerektirir. Veri gözetimi, sosyal dokunun her zerresine nüfuz ettiği için bireyleri izlemenin çok ötesine geçmektedir. Örneğin, veri gözetimi sonucunda kişilerin oy verme davranışları etkilenecek eğilimleri değiştirilebilir. Bu salt izleme sürecinin ötesine geçer ve gözetim, bir bakıma eyleme dönüşmüş olur. Bu nedenle veri gözetimi, bir yanda kurumsal platformlar ve devlet kurumları ve diğer yanda vatandaşlar-tüketiciler arasındaki sosyal sözleşme için derin sonuçları olan geniş, kapsamlı bir önermedir (Dijck, 2014: 198).

“Hem geleneksel gözetim hem de verilere dayalı izleme, özgürlük kavramlarıyla çatışır, çünkü her ikisi de bir dış güç adına benliğin temel alanını istila eder. Asıl sorun, gözetim ve veri toplama süreçlerinin bireyin asgari bütünlüğüne uyguladığı zorlayıcı ve baskıcı karakterdedir” (Couldry ve Mejias 2022: 221-222). Couldry ve Mejias’ın vurguladığı nokta, her iki gözetim türünün kişilerin asgari düzeyde hayatını sürdürmesini sağlayan koşulları (güvenlik, sağlık, mahremiyet vb.) temelden sarsmasıdır. Ancak belirtilen bu koşullar yalnızca fiziksel koşullar değildir. Örneğin tarihsel olarak, başlangıçta fiziksel mahremiyet kavramına odaklanılsa da son zamanlarda iletişim teknolojilerinin yaygınlığı –ve dolayısıyla veri gözetimi- ile bilgi mahremiyeti kavramı da büyük önem kazanmış, bilgi mahremiyetine ilişkin endişeler, günümüz çağının başlıca kaygılarından biri haline gelmiştir (Connolly ve McParland, 2012: 32). Öte yandan veri gözetimi, kişiler üzerindeki baskısını giderek daha fazla hissettirmektedir. Verinin kontrolü, toplumların da kontrolüyle sonuçlanmakta, kişilerin ifade özgürlüğü sınırlanabilmektedir. Kişiler davranış değiştirebilmekte veya görüşlerini özgürce ifade etmekten çekinebilmektedirler. Neticede veri gözetimi, etik standartlara uygun bir yapılanımda değildir. İnsana dair pek çok özerk alan her daim tehlike altındadır.

2.1.2. Veri Sömürgeciliğinde Büyük Verinin Önemi

Veri sömürgeciliği, büyük verinin gözetimiyle yakından ilişkilidir. Büyük veri denildiğinde tahayyül edilen şey, verilerin depolandığı devasa bir veri havuzudur. Oysaki büyük veri, son derece kapsamlı veri gruplarının toplanmasını, saklanması, işlenmesini, analiz edilmesini ifade eden bir terimdir (Register ve McIlroy, 2014: 87; Pandare vd., 2022: 16). Bu nedenle büyük veri, yalnızca bu dijital veri koleksiyonuna değil, aynı zamanda bu verileri toplamanın ve analiz etmenin yeni yollarına atıfta bulunmak için kullanılan bir ifadedir (Devlieghere vd., 2022: 328). Fuchs ve Chandler (2021: 13)’a göre “Büyük Veri, farklı alanlardaki bilme yöntemlerimizi dönüştürdü ve algoritmik bilgi günlük uygulamaları ve süreçleri”ni derinden etkiledi. Bu etkiye, 2017 yılında The Economist dergisi tarafından yayımlanan, “Dünyanın en değerli kaynağı artık petrol değil, veri” başlıklı makale ile dikkat çekilmiştir. Bu makalede, verinin yeni bir ekonomik kaynak olarak görüldüğü ve yirminci yüzyılda petrolün yaptığı gibi, yirmi birinci yüzyılda da verinin ekonomiyi ve toplumu dönüştüreceği öne sürülmüştür. Ayrıca büyük verinin inovasyon ve yaratıcılığa olanak sağlayarak yeni bilgi üretme yöntemlerine yol açacağına dair popüler düşünceler de bu makalede yer almıştır (The Economist, 2017). Ancak büyük verinin eleştiri alan yönleri de vardır. Bunlardan biri yine verinin doğal bir kaynak olarak lanse edilmesine benzer şekilde

büyük verinin de bu şekilde görülmesidir. Oysaki büyük veri de doğal bir kaynak değildir ve veri yığını da olsa, insandan izler taşımaktadır. Dolayısıyla büyük veri de özeldir ve sömürüye açılması için doğallaştırma taktiği uygulanmaktadır.

Öte yandan büyük veri konusunda dikkat çeken bir başka fikir, dijital verilerin kuruluşların rekabet avantajı elde etmek için kullanması gereken en yeni önemli varlığı temsil ettiğidir. Veriler satılabilir, diğer verilerle eşleştirilebilir, çıkarılabilir ve insanların davranışlarından hava koşullarına kadar her şey hakkında çıkarımlar yapmak için kullanılabilir. Özellikle, büyük veri analitiği (BDA- Big Data Analytics) olarak bilinen şey -yani büyük verinin modellenmesi ve analizi- başarılı şirketleri, pazarın geri kalanından farklılaştıran bir yetenek haline gelmiştir (Esposti, 2014: 209). Büyük veriyi yetenek olarak görmek yine neoliberal bir ifadedir. Bu ifade, büyük veriyi kullanan şirketlerin başarılı, kullanamayanların başarısız olduğu anlamını taşımaktadır. Burada sorulması gereken soru “Her şirketin büyük veriye yeteri kadar erişimi var mıdır?” Sorusudur ve burada büyük veri eşitsizliğinden bahsedilebilir. Dolayısıyla bu eşitsizlik ortamında rekabet avantajı sağlamak hiç de adil olmayacaktır. Birleşmiş Milletler (BM) ise büyük veri analitiğinin önemine dikkat çekerek dünyadaki gıda kıtlığı ve çevre krizlerinin çözümünde rol oynayabileceğini belirtmiştir. Örneğin “akıllı şehir” konsepti çerçevesinde kentlerin daha verimli yönetilmesini sağlayabileceği (trafik, atık yönetimi vb.) vurgulamıştır (Fuchs ve Chandler, 2021: 12). Büyük verinin bu amaçlar için kullanılması elbette olumludur; ancak Thatcher vd. (2016: 997)’ne göre büyük verinin asıl amacı, öngörülemeyen bireysel tüketici davranışlarını, tahmin edilebilir tüketim istatistiklerine dönüştürmektir. Aynı zamanda büyük teknoloji şirketleri, kullanıcılarına “... önerilerde bulunmak için büyük veriyi kullanır. Bu öneriler bir dizi unsura dayanır; örneğin bir kişinin profiline tıkladıysanız, aynı dönemde aynı şirkette çalıştıysanız, bazı ortak kişilerle bağlantıdaysanız” (Marr, 2021: 98) şirket tarafından belirlenen bir kalıba girilmiş olunur. Bu durum bir bakıma dijital dünyanın bir sonucudur: “Nasıl ki, küresel ısınma bireylerin ve şirketlerin gaz salınımlarının bir sonucu ise, büyük veri de bireysel eylemlerin, algısal verilerin ve gerçekliğimizin dijital görüntüsünü oluşturan diğer gerçek dünya ölçütlerinin bir sonucudur” (Zwitter, 2019: 166-167). Aslında amaç yine tüketim ve bir kalıba sokulmuş kullanıcı verilerinin tüketim için sömürülmesidir.

2.1.2.1. Veri Yığınlarının Ayıklanma Süreci ve Bir İçgörü Mekanizması Olarak Veri Madenciliği

Gözetim ve veri izleme kabiliyetleri, tüketim mallarından sivil altyapıya kadar geniş bir yelpazeye entegre edilmiştir. İşletmeler için, *akıllı* teknolojilerin oluşturduğu değerin çoğu,

ürünün satın alınmasından ziyade kullanım (Aynı zamanda, birçok akıllı teknoloji sürekli duyuşal ve kayıt modunda olduğundan, sadece etrafımızda bulunsa bile veri üretirler.) aşamasından gelmektedir. Ayrıca gündelik hayata entegre edilen akıllı teknolojilerle etkileşim kurmak, şirketlere büyük veri yığınları üretmektedir (Sadowski, 2019: 6). Veri madenciliği tam da burada devreye girmektedir. Veri madenciliği, veri yığınlarının incelendiği özellikle geniş hacimli verilerde keşfedici bir anlam bulma sürecini ifade eder (Maryville University, t.y.). Daha spesifik olarak, veri madenciliği bir halkın genel görüşü, parti tercihleri ve diğer siyasi olmayan özellikleri hakkında bilgi toplanmasını sağlar. Veri yoğun algoritmaların uygulanmasıyla, kullanıcıların ortak niteliklere göre kümelenmesi ve profil çıkarılması mümkün hale gelmektedir. Böylece kimin ve nasıl etkileneceğini belirlemek kolaylaşmaktadır (Papakyriakopoulos vd., 2018: 1). Örneğin sosyal medya, bu verileri analiz etmek için çok uygundur ve kişilerin söylediklerini ve yaptıklarını yakalamak için güçlü bir ortam sağlamaktadır (Kennedy ve Moss, 2015: 1). Sosyal medya içeriğinin ötesinde, meta veriler geniş çapta incelenir ve bazı uzmanlar tarafından içeriğin kendisinden daha değerli olarak kabul edilir. Bu tür meta veriler, içerik üreticilerinin kim olduğu ve paylaştığı, konum bilgileri, bağlantıları, etkileşim düzeyleri ve aktiflik durumları gibi bilgileri içerir. Ayrıca, önceki faaliyet kalıpları incelenir ve bunun gelecekteki eğilimlere ve tercihlere dair öngörüler sağlayabileceği düşünülmektedir. Bu meta veriler, sosyal medya platformlarının kullanıcı davranışlarını anlama, etkileşimleri ölçme ve içgörüler elde etme süreçlerinde kritik bir rol oynamaktadır (Kennedy vd., 2015: 1).

Veri bilimcileri, büyük miktardaki veriyi analiz etmek için çeşitli yöntemler kullanmaktadır. Bu veri hacmi daha önce de belirtildiği gibi insanlar tarafından doğrudan işlenemez, bu nedenle algoritmalar kullanılarak kalıplar ve önemli noktalar belirlenir. Bu analiz sonuçları, örneğin bir şirketin pazarlama ekibine iletilir ve veri madenciliği yöntemleriyle müşteri davranışlarındaki eğilimler keşfedilir. Bu keşif, şirketlere hedef kitlelerini daha iyi anlama, pazarlamalarını uyarlama ve gelecekteki müşteri davranışlarını tahmin etme imkânı verir. Örnek olarak, trafik yönetimi girişimleri, farklı şehirlerdeki trafik modellerini veri madenciliği ile analiz ederek, şehir yöneticilerine trafik sıkışıklığını azaltmak için kentsel altyapıyı daha iyi tasarlama fırsatı sunmaktadır. Veri madenciliği yoluyla bir endüstri, ürünlerini ve hizmetlerini kullanan insanlar hakkında çok daha fazla şey öğrenebilir ve onları iyileştirmek ve tüketicilerin ihtiyaçlarını tahmin etmek için çalışabilir (Maryville University, t.y.). Veri madenciliği, örüntü tanıma ve tahmin algoritmaları gibi teknolojik yardımlara dayanan yeni sosyal kontrol biçimlerinin ortaya çıkmasıyla birlikte, *geleneksel izleyici tahmini* kavramına bir alternatif olarak ortaya çıkmıştır (Bolin ve Anderson Schwarz,

2015: 4). Çünkü büyük verinin önemli noktalarından biri keşiftir. Geleneksel izleyici tahmini (veritabanı sorgulaması), bir düzeyde hipotez gerektirirken, büyük veri madenciliği, aramayı bile bilmediğimiz ilişkileri ve kalıpları ortaya çıkarma potansiyeline sahiptir (Dyche, 2012). Elbette yukarıda verilenler, iyimser yaklaşımları temsil etmektedir. Ancak veri madenciliğine eleştirel açıdan da yaklaşılması gerekmektedir. Daha önce de belirtildiği gibi veriye doğal bir kaynak gibi yaklaşılması akademik çevrelerce eleştiri konusu olmaktadır. Dolayısıyla verinin analiz edilerek anlamlı hale getirilme sürecinin de *madencilik faaliyeti* olarak adlandırılması da benzer şekilde eleştirilmelidir. Bu nedenlerle eleştirel yaklaşımlar, veri madenciliği ve analitiğin baskın kullanımlarının toplum üzerindeki etkileri ile ilgili bir dizi endişeyi dile getirmektedir: Veri Madenciliği daha az mahremiyet, daha fazla gözetim ve sosyal ayrımcılığa yol açmaktadır (Kennedy ve Moss, 2015: 1).

Veri madenciliği, algoritmik iyileştirme ve otomasyonun etik ve sosyal etkileri, son yıllarda dijital medyaya ilgi duyan akademisyenler için artan bir endişe kaynağı olmuştur (Albury vd., 2017: 1). Andrejevic (2014a: 1675)'e göre veri madenciliği, dijital medyanın demokratikleştirici/güçlendirici vadinin altını oyacak şekilde, açıklama ve anlama yerine korelasyon ve tahmine öncelik vermektedir. Veri madenciliğiyle ilişkilendirilen kişiselleştirme retoriğine rağmen, olasılıksal karakterde tahminler ortaya çıkarmaya ve zaman içinde karar vermeye ayrıcalık tanımaktadır. Dahası, *bireylerin ve grupların yaşam şanslarını etkileyen* kararlar almak için kullanılabilecek, öngörülemeyen; ancak kalıcı kalıpları ayırt etme yeteneği olan “sosyal sınıflandırma” çağını başlatmaktadır. Böylelikle veri madenciliği mantığı “açık rıza” ya da “bilgilendirilmiş rıza” gibi kavramları büyük ölçüde anlamsız kılmıştır.

Wouter Weerkamp ve Maarten de Rijke (2012)'ya göre veri madenciliği bir anlamda “hayat madenciliği”dir. Söz konusu hayat madenciliği olduğunda, yine liberal söylemle veri madenciliği için verimli maden sahalarına sahip olan mobil uygulamalar akla gelmektedir. Kullanıcının hayatına dair derin veriler elde edilebileceği gibi Andrejevic'in ileri sürdüğü “sosyal sınıflandırma” için de uygun zemini sağlar. Bu uygun zemin de veri madenciliği başlığı altında yeni sorunların filizlenmesine neden olur. Bunlardan bazıları sosyal ayrımcılık, temsil ve eşitsizlik gibi konulardır. Örneğin, yapay zekâ algoritmalarını oluşturmak için kullanılan verilerin altında yatan önyargı, “algoritmik önyargı” olarak bilinir ve sosyal ayrımcılığa ve başkaca sosyal etkilere yol açabilir (Hamza, 2022), toplumdaki gruplar veya bireyler arasında var olan eşitsizlikleri derinleştirebilir, yeni eşitsizlikler yaratabilir. Ayrıca ön yargılı tasarlanmış algoritmalar veri setlerindeki ön yargı ve ayrımcılığı kopyalayarak veriyi temsil ettiği düşünülen grupların ayrımcılığa maruz kalmasına neden olabilir (Hamza, 2022).

Bütün bunlar, veri madenciliğini sürecinde önemli rol oynayan algoritma, yapay zekâ ve makine öğrenmesi gibi yöntemlere yönelik endişeleri de beraberinde getirmektedir. Helen Kennedy ve Giles Moss (2015: 2) ise bu endişelerin ortadan kaldırılması ve veri madenciliğinin demokratikleştirilmesi için üç temel adım önermektedir. İlk olarak, veri madenciliğinin olası olumsuz etkilerini ele almak için daha fazla kamu denetimi ve düzenlemeye ihtiyaç duyulmaktadır. İkinci olarak veri madenciliği teknolojileri, çeşitli amaçlar için kamuya açık ve erişilebilir hale getirilmelidir, böylece dijital uçurum riski en aza indirilebilir. Üçüncü olarak da veri madenciliği, halkın birbirini daha iyi anlamasını, ortak konularda düşünmeyi ve kolektif kararlar almalarını teşvik ederek, kamusal meselelerin temsilinde etkili bir araç olarak kullanılabilir. Ayrıca algoritma önyargısıyla mücadele etmek için de yalnızca yapay zekâ ve algoritma konusunda teknik bilgiye sahip veri bilimcilerinin değil, farklı geçmişlere ve bakış açılarına sahip profesyonellerin de mücadele alanına dâhil edilmesi gerekmektedir (Hamza, 2022).

2.1.2.2. Veri Madenciliğinin Düşünsel Tasarımı: Algoritmalar

Günümüzde sıklıkla kullandığımız teknolojik araçlar sayesinde toplanan kullanıcı verileri, büyük veri olarak adlandırılan büyük bilgi yığınlarına dönüştürülmekte ve analiz edilmektedir. Degli Esposti (2014)'ye göre büyük veri, muazzam miktarda verinin hızla üretilip dolaşıma girdiği ve gerçek zamanlı olarak işlendiği bir alanı ifade etmektedir. Bu veriler, yalnızca makineler ve algoritmalar tarafından işlenebilir ve analiz edilebilir düzeyde büyük ve karmaşıktır. Büyük verinin hacmi, insanların el yordamıyla işleyebileceği bir boyuttan çok daha büyük olup, bu veri kümelerinin insan müdahalesi olmadan makineler tarafından yönetilmesi gerektiğini vurgular. Bu nedenle, büyük verinin işlenmesi ve analizi için özel algoritmalar ve otomasyon yazılımları gerekmektedir (Fuchs ve Chandler, 2021: 13; Esposti, 2014: 209).

Algoritma tasarımları, büyük miktarda veriyi anlamlı bilgilere dönüştürmek amacıyla programlama diliyle kodlanmış yazılımlardır. Algoritmalar, veri toplama, analiz ve içgörü elde etme süreçlerinde, özellikle büyük veri analitiği, yapay zekâ (AI- Artificial Intelligence) ve makine öğrenimi (ML- Machine Learning) gibi veri odaklı teknolojilerde kritik rol oynamaktadır. Bu yazılımlar, çeşitli kaynaklardan gelen verileri yakalama, depolama ve analiz etme işlevlerini yerine getirmek amacıyla kullanılmaktadır (Bolin ve Anderson Schwarz, 2015: 1; Pandare vd., 2022: 17). Geçmişte, algoritmalarından daha ilkel olan teknolojiler genellikle yaş, cinsiyet, etnik köken, eğitim gibi sosyo-ekonomik değişkenlere dayalı kategoriler üzerine inşa edilmekteydi. Bu kategoriler medya kullanıcıları ve sektör

temsilcileri tarafından kolayca anlaşılabilir. Ancak büyük veri teknolojileri, tüketici tercihlerini, coğrafi konumu, web hareketlerini ve davranışsal bilgileri içeren daha soyut ve teknik olarak karmaşık veri yollarıyla kaydetmeye başladı. Bu veriler, genellikle tam anlamıyla çözümlenemeyen teknik detayları içerirken, özellikle örüntü tanıma amacıyla çıkartılan veriler, demografik özellikler yerine ilişkisel niteliklere odaklanma eğilimindedir. Bu, geleneksel kategorilerin ötesinde, verilerin birbiriyle nasıl ilişkilendiği ve etkileşimde bulunduğu konularına odaklanmayı gerektirmektedir. Büyük veri analizindeki bu yaklaşım, daha derinlemesine bakış açıları elde etmek ve daha önce fark edilmemiş örüntüleri keşfetmek için önemlidir (Bolin ve Anderson Schwarz, 2015: 1).

Algoritmalar, dijital medya ve enformasyon teknolojilerinin giderek ayrılmaz bir parçası olmuştur (Velkova ve Kaun, 2021: 525). Bu nedenle algoritmalara yönelik eleştirel yaklaşımlar da giderek daha sorunlu alanlara dikkat çekmektedir. Örneğin sosyal medyadaki kişiselleştirme algoritmaları bireyleri ve toplumu, kar etmek için hesaplamaya indirgeyebilecek varlıklar olarak temsil etme eğilimindedir. Algoritmalarındaki riskler, bireysel ve toplumsal uyumu temelden tehdit etmektedir (Reviglio ve Agosti, 2020: 9). Öte yandan YouTube'un, önemli ölçüde somutlaşmış sosyal ve kültürel sermayeye sahip güzellik Vlogger'ları tarafından yaratılan hegemonik, kadınsılaştırılmış kültürel çıktıları, aktif olarak desteklediğini iddia edilmiş (Bishop, 2018: 69), Google'ın görsel arama sonuçlarında ırksal önyargının bulunduğu dile getirilmiştir (Velkova ve Kaun, 2021: 523).

Algoritmalar, yapay zekâ ve makine öğrenmesi gibi yöntemler sayesinde büyük miktarda veriyi analiz etmek kolaylaşmaktadır. Ancak verilerin sistematik hale getirilmesinde hem de anlamlandırılmasında önemli bir konuma gelen bu yöntemler, doğrudan deneyimleri şekillendirilmekte veya bunlara aracılık etmektedir. Dolayısıyla algoritmalar, veri sömürsünü kolaylaştıran ve veri madenciliği süreçlerinin kilit noktasında yer alan potansiyel bir tehlike olarak görülmelidir. Çünkü algoritmalar her zamankinden daha büyük veri kümelerini seçtikçe, birbirine bağladıkça ve analiz ettikçe, günlük yaşamın daha önce özel olan, ölçülmemiş anlarını kâr kaynaklarına dönüştürmeye devam edecektir (Thatcher vd., 2016).

2.2. Mobil Uygulama Aracılı Veri Sömürgeciliği

Günümüzde veri sömürgeciliği, özellikle sosyal nicelleştirme sektörünün ve sosyal medya platformlarının kişisel veri çıkarma faaliyetleri nedeniyle giderek daha belirgin hale gelmektedir (Couldry ve Mejias, 2022: 21-22). Bu süreç, mobil uygulamaların veri sömürgeciliği pratiğinin merkezine yerleştirilmesiyle daha da güçlenmiştir. Hemen hemen her

mobil cihazda bulunan uygulamalar, büyük teknoloji şirketleri tarafından faaliyet alanlarına entegre edilerek neredeyse kişisel veri toplama amacıyla kullanılan bir tür ajan yazılım haline gelmiştir. Bu yazılımlar, mobil cihazlarda kimi zaman arka planda çalışarak ya da açıkça bilgilendirerek kullanıcıya ait birçok veri toplamaktadır. Bu veriler özellikle konum bilgileri, sosyal etkileşim ve satın alma davranışlarıdır. Uzun yıllar web’den toplanan veriler günümüzde yoğun olarak *mobil ortamdan* toplanmaya başlamıştır: Mobil cihazlar artık daha kişisel bir alandır ve en derin kişisel veriler de mobil ortamdadır ve veri toplamada *mobil uygulama çağı* başlamıştır.

Bu çağdaki yenilik, büyük veri akışlarının otomatik olarak toplanması, özellikle davranış ve sağlık bilgilerinin diğer birçok veri türüyle birleştirilebilme potansiyelidir. Bireysel platformlar, daha hacimli veri setlerini toplamak ve takas etmek için artan bir güce sahiptir ve baskın veri simsarlarının (data brokers) ortaya çıkması, bireysel platformları, veri odaklı ekosistemin tutsakları haline getirmektedir (Van Dijck ve Poell, 2016: 8). Bu tutsaklık durumu, veri sömürsünde sınırların zorlanmasına (her türden hassas verinin elde edilmesi), iş modellerinin bu sömürü düzeni üzerine kurulmasına neden olmaktadır. Mobil uygulamalar da adeta bu düzenin sağlıklı bir şekilde çalışmasına aracılık etmesi için yaratılmıştır. Mobil uygulamalar bir bakıma kullanıcıdan veri toplayan ve geliştiricisine aktaran bir araçtır. Mobil uygulamaların giderek daha fazla kişisel veri toplama kapasitesine sahip hale gelmesiyle birlikte kullanıcı mahremiyetine ilişkin endişeler de artmaya başlamıştır. Mahremiyetin ihlali toplumsal, hukuki ve etik açıdan kişinin temel hak ve özgürlüklerini sınırlamaktadır. Bu nedenle mobil uygulamalardaki veri kaynaklı sorunlar, akademik çevrelerce daha fazla gündeme getirilmelidir.

2.2.1. Mobil Uygulama Ekolojisi

Medya ve iletişim çalışmaları akademisyeni Carlos A. Scolari (2012: 204), medya ekolojisi metaforunun, iletişim çalışmaları için yenilikçi ve kullanışlı bir kuramsal çerçeve olarak sıklıkla kullanıldığını ileri sürer. Medya ekolojisi metaforuyla ilgili olarak Neil Postman (1970: 161)’ın *medyanın ortamlar olarak incelenmesi* gerektiğini savunduğu, Marshall McLuhan’ (2004: 71)’ın 1977’de *medyanın, balıkların suda yaşadığı gibi bireylerin yaşadığı ortamlar olduğunu* dile getirdiği yıllardan itibaren günümüze kadar medya ekolojisi metaforunun sıklıkla kullanıldığı akademik çevrelerce dile getirilmiştir (Logan, 2004: 2; Scolari 2012: 204). Medya ekosistemleri, doğal ekosistemlere benzer şekilde, içinde yaşadıkları aktörlerin faaliyetleri ve stratejileri kadar maddi koşullarıyla da tanımlanmaktadır. Bu nedenle medya ekolojisi metaforunun mobil uygulamaların ve bu uygulamaların dijital

iletiřim ortamında giderek daha önemli hale gelen rolüne iliřkin anlayıřın geliřtirilebilmesi iin olduka uygun kuramsal bir hareket noktası olacađını söylemek yanlıř olmayacaktır (Lai ve Flensburg, 2021: 2303).

Mobil uygulamalar, mobil cihazların üretilmesinden itibaren bu cihazlardaki eřitli iřlevleri yerine getiren yazılımlar olarak ortaya ıkmıřtır. 1990'ların bařından itibaren, saat, takvim ve hesap makinesi gibi bazı temel fonksiyonların alıřması iin kullanılmıřtır. 2000'li yıllardan itibaren eřitlenmeye bařlayan uygulamalar, mesajlařma ve oyun gibi kategorilere ayrılmaya bařlamıř ve grece daha eđlenceli hale gelmeye bařlamıřtır. Ancak bu yazılımların ortak noktası, cihaza entegre olarak sunulmaları ve sınırlı iřlevlere sahip olmalarıdır. 2007'de iPhone'un piyasaya sürölmesi, mobil uygulama endüstrisinin büyüme sürecini tetiklemiřtir. Bu süreç kullanıcılara, kiřisel bilgisayar benzeri bir iřlevselliđi, tařınabilir cihazlarda deneyimleyebilme fırsatını sunarak bařlamıřtır. Bu iřlevselliđe sahip olan akıllı telefonlar ve onlarla gelen uygulamalar, günlük yařantımızda giderek daha yaygın bir konum elde etmiřtir (Rakestraw, 2013: 1-2). Günümüz mobil uygulamaları, akıllı telefonlarda alıřmak üzere geliřtirilmiř pratik yazılımlardır (Flora vd., 2014: 21) ve kullanıcının belirli bir görevi gerekleřtirmek iin bu yazılımlara ihtiyaı vardır (Rakestraw, 2013: 3). Mobil uygulamalar, zaman zaman masaüstü uygulamalarla karıřtırılabilmektedir. Oysaki bu uygulamalar, geleneksel masaüstü (web tabanlı) uygulamalardan farklıdır (Zhang vd., 2013: 1). Masaüstü uygulamalar halen kullanılmaya devam etse de popölaritesini yavaş yavaş kaybetmekte, gün getike tahtını mobil uygulamalara kaptırmaktadır. Lai ve Flensburg (2021: 2307)'a göre de mobil uygulama ekosistemi, bazı yönleriyle web tabanlı sistemlerden avantajlı konuma gemektedir. Mobil uygulama ekosistemi, altyapı özelliklerine bađlı olarak mobildir ve kullanıcının günlük yařamda her yerde bulunmasına imkân tanımaktadır. Bu nedenledir ki kullanıcıların faaliyetleri veya nerede oldukları hakkında da web tabanlı sistemlere göre daha ayrıntılı veriler barındırmaktadır. Mobil uygulama ekosisteminin bir bařka avantajı ise web tabanlı uygulamaların mobil uygulamalara entegre edilebilmesidir. Örneđin web etkinlikleri iin kullanılan tarayıcılar halen kilit önemde olsalar da bunlar mobil cihazlarda da alıřmaktadır. Günün sonunda tarayıcılar da aslında birer mobil uygulamaya dönuřmüřlerdir (Talay, 2018: 66; Lai ve Flensburg, 2021: 2307). Ayrıca mobil uygulamalar web tabanlı uygulamalara göre kullanımı grece kolay olan interaktif uygulamalardır. Bütün bunlar bize web tabanlı sistemlerin hem ekonomik hem de pazar düzeyinde uygulama ekosisteminde bir alt sistem haline geldiđini göstermektedir (Cheng, 2017: 49; Lai ve Flensburg, 2021: 2307).

Mobil medya arařtırmacıları mobil uygulamaları, iletiřimi, sosyalliđi, kamu biimlerini dönuřtüren ve üreten konumsal bir medya biimi olarak görmektedir. Evrensel

hizmetlere ve yardımcı programlara (çoğunlukla ücretsiz) erişim sağlayan uygulamalar ceplerimizde, ofislerimizde, evlerimizde ve arabalarımızda bulunan kültürel, sosyal ve ekonomik açıdan da önemli bir yazılım biçimi halini almakta, nesnelere, cihazlara, yapılara ve sosyal ortamlara yerleşerek giderek daha fazla gündelik hayatın bir parçası haline gelmektedir (La Polla vd., 2013: 446; Razaghpanah vd., 2018: 1; Gerlitz vd., 2019: 2-7). Hatta mobil uygulamaların *internetin düzenleyici mantığı* haline geldiği iddia edilmekte, ekonomi politik perspektifinden bakıldığında *yazılım metasının belirli bir tezahürü* olarak da görülmektedir (Gerlitz vd., 2019: 2-7). Bu ifade, mobil uygulamaların geniş bir ekonomik sistemin önemli bir parçası olduğunu göstermektedir. Dolayısıyla mobil uygulamaların şirketlerin ekonomik olarak büyümesine de katkıda bulunduğu/bulunacağı söylenebilir. Ancak bu büyümeyi salt finansal terimlerle ifade etmek yeterli değildir. Giderek altyapısal özelliklere sahip olan yeni hizmetlerin ve uygulamaların geliştirilmesine ve ardından kurumsal ortaklıkların yaratılmasına ve pazarların ele geçirilmesine işaret ederek ekonomik merceğin genişletilmesi gerekmektedir (Nieborg, ve Helmond, 2019: 200). Bu nedenle, mobil uygulamaları tanımlayan temel özellikleri anlamak son derece önemlidir (Flora vd., 2014: 21). Ayrıca mobil uygulama ekosisteminin anlaşılması, veri odaklı gözetime karşı politikalar ve düzenleyici araçlar geliştirmesi için gereklidir. Uygulama ekolojisi ve veri ekonomisi hakkındaki bilgi ve bilgi edinme yeteneğini geliştirmek, kullanıcı sömürüsü ve yabancılaşma senaryosundan uzaklaşarak özgürleşmenin geleceğine doğru atılan önemli bir adım olacaktır (Lai ve Flensburg, 2020: 18).

2.2.1.1. Mobil İşletim Sistemlerine Veri Gizliliği Düzleminden Bakış

Mobil işletim sistemleri, mobil cihazlar için özel olarak tasarlanmış yazılım programlarıdır ve masaüstü işletim sistemlerine kıyasla, genellikle düşük depolama alanı ve bellek ihtiyacıyla karakterize edilmektedir. Bu nedenle mobil işletim sistemleri, tabletler, akıllı telefonlar ve giyilebilir teknolojiler gibi cihazlarda kullanılabilir. Mobil işletim sistemleri, kişisel bilgisayarların sunduğu temel işlevleri de bünyesinde barındırmaktadır. Bunlar arasında dokunmatik ekran, hücreli bağlantı, kablosuz bağlantı (Bluetooth, Wi-Fi vb.), konum (GPS), kamera, konuşma tanıma, müzik çalar ve ses kaydedici gibi bileşenler bulunmaktadır. Mobil işletim sistemleri, çoklu kullanıcı, çoklu işlem ve çoklu görev gibi özelliklere sahiptir ve en önemlisi mobil iletişim yetenekleri sunarlar. İlk mobil işletim sistemi olan Palm OS 1.0, 1996 yılında tanıtılmış ve cep bilgisayarları (PDA- Personal Digital Assistant) için kullanılmıştır. Günümüz işletim sistemleri, bazı farklı (örneğin, kalem ve dokunmatik ekran) yeteneklerin yanı sıra gelişmiş kullanıcı arayüzleri sunmaktadır.

Günümüzde en popüler mobil işletim sistemleri arasında Android, iOS ve Windows bulunmaktadır. Bazı eski işletim sistemleri, örneğin Web OS ve Palm OS, artık üretimi durdurulmuş veya kullanımı oldukça seyrelemiştir (Wukkadada vd., 2015: 273).

Tezin giriş bölümünde bahsedildiği üzere Android ve iOS işletim sistemlerinin, mobil işletim sistemleri pazar payının %99'undan fazlasına sahip olması nedeniyle yalnızca bu iki işletim sistemi üzerinde durulmuştur. Diğer işletim sistemleri bu tezde kapsam dışı bırakılmıştır. Mobil işletim sistemlerinin mobil uygulamalar ile doğrudan ilişkisi bulunmaktadır. İşletim sistemleri mobil cihazların temel işlevlerini yönetirken, cihazın donanımını da kontrol etmektedir. Mobil uygulamalar da uyumlu işletim sistemi üzerinde çalışmaktadır. Sonuç olarak işletim sistemleri mobil uygulamalarla veri alışverişinde bulunmakta ve veri gözetimini olanaklı kılan donanım (örneğin, sensörler) ve uygulamalar arasında köprü kurmaktadır.

Android, mobil cihazlar için bir üretilen bir platformdur ve tıpkı gerçek bir çalışma platformu gibi uygulamalar için bir temel sağlamaktadır (Speckman, 2008: 11). Öte yandan Android, bir yazılım platformu olarak anılmasının yanı sıra bir işletim sistemi olarak da kabul edilmektedir ve temel uygulamaları da içeren bir yazılım yığındır. Android ilk olarak 23 Eylül 2008 tarihinde piyasaya sürülmüş ve Google tarafından geliştirilmiştir (Wukkadada vd., 2015: 273). Android, dünya çapında mobil işletim pazarında ilk sırada yer almaktadır. 2022 itibarıyla, 59 milyardan fazla aktif Android cihaz bulunmaktadır. Ayrıca, 2022 yılının verilerin göre dünya çapında 5 milyondan fazla aktif Android geliştiricisi bulunmaktadır, bu da onu sektördeki önde gelen işletim sistemi konumuna getirmektedir (Aishwar, 2023).

Android, açık kaynak kodlu, ücretsiz bir yazılımdır (Wukkadada vd., 2015: 273) ve geliştiricilerin onu kullanmasına ve geliştirmesine olanak tanımaktadır. Açık kaynak sistemi aynı zamanda Google'ın geliştiricilerin yaptığı katkıları da kullanmasını sağlamaktadır (Spreeuwenberg ve Poell, 2012). Android'in açık kaynak kodlu olup olmadığı konusu ise tartışmalıdır. Kimi yazarlar bunun bir reklam taktiği olduğunu öne sürmektedir: Android, açık kaynaklı bir proje olarak pazarlanmakta ve reklamı da şu şekilde yapılmaktadır: *Mobil cihazlar için açık kaynaklı bir yazılım yığını ve Google tarafından yönetilen açık kaynaklı bir proje* (Spreeuwenberg ve Poell, 2012). Kimberley Spreeuwenberg ve Thomas Poell (2012)'un çalışması, Android'in açık kaynak modelinin, Google hizmetlerini teşvik etmek ve Android cihazlarının donanım gelişimini yönlendirmek amacıyla kullanıldığını ortaya koymaktadır. Ayrıca açık kaynak modeli, Google'ın kendi hizmetlerini Android platformunda yaygınlaştırmak ve diğer donanım üreticilerini belirli standartlara uymaya teşvik etmek için kullanılmaktadır. Bu durum, Android ekosistemini Google'ın hizmetlerine daha fazla entegre

etmek ve cihazların uyumluluğunu artırmak için kullanılan bir stratejiyi yansıtmaktadır. Spreeuwenberg ve Poell (2012) bu stratejiyi detaylandırmaktadır: Örneğin, Microsoft'un her şeyden önce lisans ücretleri yoluyla gelir elde ettiğini, buna karşılık Google'ın lisanslama veya donanım satışları yoluyla değil kullanıcıların meta verilerinin toplanması ve hedefli reklamların görüntülenmesi için bir platform oluşturarak gelir elde ettiğini söylemektedir. Bu platformlaştırma süreci, açık kaynak yazılım gelişimine yönelik gerçek potansiyeli sınırlayabilen uygulama mağazaları ve platform araçları tarafından işletilen bir mantığı temsil etmektedir. Bu mantık, uygulamaların özgür ve inovasyon dolu gibi görünse de aslında büyük global şirketlerin etkisi altında olduğu anlamını taşımaktadır. İş modelleri, global platformların yoğun sermaye odaklı uygulamalarıyla tam entegre olmasa da bu platformlarla uyumlu hale getirilmiştir (Nieborg, 2021: 314).

Zuboff (2021: 172)'a göre de Google, Android'i mobil cihazlarda hızla davranışsal artı değer elde etmek için kritik bir stratejik araç olarak kullanmıştır. Google, Android'i mobil cihaz üreticilerine ücretsiz olarak dağıtarak, kullanıcıları Google'ın hizmetlerine çekmeyi ve davranışsal artı değeri artırmayı amaçlamıştır. Zuboff (2021: 172), bunu Google'ın reklamcılık ve hizmetler alanlarında büyüme potansiyelini artırmak için kullandığını ve Android'in bu amaç doğrultusunda kritik bir tedarik noktası haline geldiğini ileri sürmektedir. Google için Android'in mümkün olduğunca çok sayıda mobil cihazda çalışması ve hizmetlerinin kullanıcı seviyesini en üst düzeye çıkarması oldukça önemli görünmektedir (Spreeuwenberg ve Poell, 2012).

Sonuç olarak Google'ın Android'i işletim sistemi olarak piyasaya sürmesiyle, mobil uygulama ekosisteminde çeşitlilik meydana gelmiş, üçüncü taraf geliştiriciler için de ulaşılabilir, geliştirilebilir ve özelleştirilebilir bir işletim sistemi meydana gelmiştir. Android'in mobil pazarda güçlü konumunu koruyacağı ve gelecekte büyümesini sürdüreceği beklenmektedir. Büyük bir kullanıcı veri tabanı, yüksek etkileşimli kullanıcılar ve geliştiricilerle Android'in, işletmelerin ürün ve hizmetlerini hedeflemeleri açısından önemli bir platform olmaya devam edeceği söylenebilir (Aishwar, 2023). Öte yandan Android'in bu güçlü yönleri bazı sorunları da beraberinde getirmiştir. Android'in aşırı şekilde büyümesi mobil pazarda tekel olmasıyla sonuçlanmıştır. Android'in ücretsiz olarak dağıtılması da rekabeti sınırlayıcı bir etken olmuştur. Apple haricindeki diğer işletim sistemleri neredeyse mobil uygulama piyasasından silinmiştir. Bir başka problemli konu da veri bağlantılı sorunlardır. Aşırı şekilde büyüyen Android pazarı sayesinde çok geniş kitlelerin verileri Google'da toplanmaktadır. Bu, Google için daha fazla davranışsal veri ve daha fazla reklam

geliri demekken; kullanıcılar için mahremiyet endişelerinin artarak devam etmesi ve yoğun reklam maruziyeti demektir.

Mobil işletim sistemi pazarının Android'den sonra ikinci büyük oyuncusu olan iOS, Apple Inc. tarafından iPhone için geliştirilen bir mobil işletim sistemidir. İlk olarak 29 Haziran 2007'de piyasaya sürülen iOS, şirketin yine kendi işletim sistemi olan Mac OS X'ten türetilmiştir (Wukkadada vd., 2015: 273). IOS mimarisinin, uygulama geliştirme ve yürütme için güvenli, stabil ve verimli bir platform sunmak amacıyla tasarlandığı iddia edilmektedir. Bu iddiaya göre söz konusu mimari, esas işlevselliği ve destek sağlayan net tanımlı katmanlara sahiptir. IOS'un önemli avantajlarından birisi olarak kullanıcılara sağladığı güvenlik düzeyine işaret edilmektedir. Gaurav Singh (2023)'e göre birden fazla şifreleme katmanı bulunması, Apple cihazlarına izinsiz erişimi oldukça zorlaştırmaktadır. Öte yandan iOS, geniş bir uygulama yelpazesi, verimli pil kullanımı ve kullanıcı odaklı tasarımlar gibi avantajlar sunmasına rağmen, Android işletim sistemiyle kıyaslandığında daha az özelleştirme ve dosya aktarımı seçeneğine sahip olması nedeniyle eleştirilmiştir (Wolfel, 2022).

IOS işletim sistemine yöneltilen bir eleştiri de kapalı bir sistem kullanıyor olmasıdır. Örneğin yukarıda da bahsedilen Google'ın açık kaynak uygulamaları, Apple'ın iOS'u ile karşıt durumdadır. Apple, iOS'u öncelikle Apple donanımını satmak için geliştirmiştir (Spreeuwenberg ve Poell, 2012; Wukkadada vd., 2015: 273). Görüldüğü üzere iOS işletim sistemi yalnızca Apple'ın kendi ürünlerine hizmet etmektedir. Bu konuda Android işletim sistemiyle taban tabana zıttır. Android'de gelir, öncelikle fikri mülkiyetin metalaştırılması yoluyla değil, *ortak aklın ağ değerine* dönüştürülmesi yoluyla elde edilirken (Spreeuwenberg ve Poell, 2012), iOS da gelir etmede ilk hedef kendi ürettiği cihazların lisanslanmasıdır. Bu, yukarıda da belirtildiği üzere Microsoft'un yürüttüğü mantığa benzer şekilde işlemektedir. Diğer taraftan Apple'ın öncelikli hedefinde, reklam yoluyla gelir de bulunmamaktadır. Dolayısıyla işletim sistemi açısından değerlendirilirse kişisel veri toplamaya odaklı çalışan bir yapılanmanın bulunmadığı söylenebilir.

2.2.1.2. Dijital Dünyanın AVM'leri: Mobil Uygulama Mağazaları

Mobil uygulama mağazaları, milyonlarca geliştirici²² tarafından geliştirilen, milyonlarca uygulama ile mobil uygulama ekolojisinin önemli bir bileşeni haline gelmiştir

²² Orr, A. (2022). "Apple'ın 34 milyondan fazla kayıtlı geliştiricisi var". 2022 yılı itibariyle yalnızca iOS'a kayıtlı 34 milyon geliştirici bulunmaktadır. (Android'e kayıtlı resmi geliştirici sayısı ise bilinmemektedir.) <https://appleinsider.com/articles/22/06/06/apple-now-has-over-34-million-registered-developers> (erişim tarihi: 11.11.2023).

(Wang vd., 2017: 163). Mobil uygulama mağazaları, kullanıcının akıllı telefonu için mobil uygulamalar indirmesine izin veren bir yazılımdır (Rakestraw, 2013: 5). Bu yazılım bir bakıma geliştiriciler ve geliştirdikleri uygulamaları kullanıcılarla buluşturmaktadır. Mobil işletim sistemlerinin de önemli bir parçası olan uygulama mağazaları, bir yandan kullanıcıların uygulamalara erişme, indirme, satın alma, inceleme ve derecelendirme koşullarını belirlerken, diğer yandan uygulama geliştiricilerine uygulamalarını dağıtmak, tanıtmak ve bunlardan para kazanmak için bir araç sağlamaktadır (Gerlitz vd., 2019: 4). Bu mağazalarda satışa sunulan ücretli uygulamaların yanı sıra ücretsiz uygulamalar da bulunmaktadır. Çoğu durumda uygulamalar, mevcut ürünlerinin reklamını yapmayı veya yeni uygulama geliştirmek isteyen şirketler gibi üçüncü taraf geliştiriciler veya uygulamalarını gelir için satan serbest yazılımcılar tarafından geliştirilmektedir.

Apple ve Google, günümüzün en önde gelen uygulama mağazalarına sahiptir ve bu şirketler, uygulama endüstrisindeki en önemli rakip olarak kabul edilmektedir. Bu iki şirket, uygulama geliştiricileriyle olan ilişkileri, mevcut uygulama sayısı ve uygulamaların mağazadaki özellikleri konularında kendilerini rakiplerinden ayırmak için büyük bir çaba harcamaktadır (Rakestraw, 2013: 1-5). Mobil uygulama endüstrisi, mobil pazarda önemli bir oyuncu haline gelmiştir ve bunun bazı belirgin göstergeleri vardır. İlk olarak, uygulama endüstrisi, yatırım çekme ve bilgi paylaşma yeteneğine sahiptir. Uygulama ekonomisinin ikinci önemli göstergesi ise “indirme sayısı”dır (Cheng, 2017: 49). Mobil uygulama mağazasının sonuç sayfasında ilk sıralarda yer almak, gösterimleri iyileştirdiği ve indirme şansını arttırdığı için uygulamanın başarısının anahtarıdır. Kullanıcı memnuniyeti ve iyi deneyimler de her zaman olduğu gibi uygulamaların popülerliğini belirleyen en önemli değişkenlerden biridir ve marka bilinirliğini artırmaktadır (Statista, 2023c).

Google Play Store, global Android kullanıcılarının başlıca uygulama dağıtıcısı olmasının yanı sıra sektördeki en önemli mobil uygulama mağazalarından biridir (Statista, 2023c). Google Play, Apple’ın App Store’u açmasından birkaç ay sonra, 2008 yılında “Android Mağaza” adı altında faaliyete geçmiştir. İlk başta Google Play Store’da App Store’dan daha az uygulama varken, 2011 yılına gelindiğinde Play Store, App Store’u geride bırakmıştır (Priori Data, 2023). Google Play Store, Android cihazların artan popüleritesiyle beraber Haziran 2023 itibariyle indirilebilen yaklaşık 2,6 milyon uygulama ile dünyanın en büyük uygulama mağazasıdır (Statista, 2023b).

Google Play Store, mobil uygulama endüstrisinin önemli bir parçasıdır ve geliştiriciler için ciddi bir ekonomik kaynak oluşturmaktadır. Google Play uygulamalarının yıllık geliri, zaman içinde istikrarlı bir artış sergilemiştir. 2016’da 15 milyar dolar seviyelerinde

gerçekleşen gelir, sonraki yıllarda önemli bir artış göstermiş, 2017’de 21,21 milyar dolarlık gelir, 2018’de 24,82 milyar dolara yükselmiştir. Bu artış eğilimi devam ederek 2021’de 47,94 milyar dolara ulaşmıştır. 2022’de ise gelirde hafif bir düşüş yaşanmış ve toplam gelir 42,32 milyar dolar seviyesine gerilemiştir. 2023’te ise bu rakamın 45,63 milyar dolara ulaşması beklenmektedir (Priori Data, 2023). Ayrıca uygulama mağazalarındaki abonelikler, uygulama geliştiricileri için önemlidir. Çünkü birçok Google Play’deki abonelik uygulamalarından elde edilen yıllık gelir, 2016 yılında 0,5 milyar dolardan başlayıp her yıl istikrarlı bir şekilde artmıştır. Bu trend devam ederek gelirin 2019’da 1,9 milyar dolara yükselmiştir. Büyüme oranı 2021’de daha da hızlanmış ve gelir 2,7 milyar dolara, ardından 2022 yılında güçlü büyüme ile 3,9 milyar dolara ulaşmıştır. Uygulama abonelik gelirlerinin ise 2023’te 4,3 milyar dolara çıkacağı tahmin edilmektedir (Priori Data, 2023).

Apple App Store, iOS için yaklaşık 1,6 milyon mevcut uygulamanın bulunduğu ikinci en büyük uygulama mağazasıdır. App Store, iPhone 3G ile birlikte Temmuz 2008’de hizmete açılmıştır (Curry, 2023). Uygulama mağazası, 2008’den bu yana büyük bir hızla büyümüş ve en büyük uygulama platformlarından biri haline gelmiştir (Ahuja, 2023). App Store’da Google Play Store’a benzer şekilde milyonlarca uygulama barındırmaktadır. 500 uygulama ile başlayan serüven, 2013 yılının sonlarına doğru 1 milyon civarına yükselmiştir (Ahuja, 2023). 2023 yılı itibarıyla indirilebilir uygulama sayısı 1,8 milyon civarındadır (Statista, 2023e). Uygulama mağazasındaki indirme sayılarındaki artış da dikkat çekicidir. 2015 yılında 22 milyon olan indirme sayısı 2020’ye kadar istikrarlı bir şekilde artmış, 34,4 milyon indirme seviyesine gelmiştir. 2021 yılında hafif bir düşüş yaşasa da (32,3 milyon) 2022’de 32,6 milyon indirmeyle yeniden yükseliş trendine girmiştir (Ahuja, 2023). Apple App Store uygulamalarının yıllık geliri de Google Play’de olduğu gibi ciddi rakamlardır. 2016 yılında 28,6 milyar olan yıllık gelir 2022’ye gelindiğinde 86,8 milyar dolar seviyesine ulaşmıştır (Curry, 2023). 2021’nin üçüncü çeyreğinde, Apple App Store aracılığıyla mobil uygulamalara yapılan global tüketici harcaması 21,5 milyar ABD dolarına ulaşmış ve Google Play platformunun 12,1 milyar ABD dolar olan harcamasını geride bırakmıştır (Statista, 2023d).

2.2.1.3. Tüketici Olmanın Ötesine Geçen Mobil Uygulama Kullanıcıları

Kullanıcı, bir ürün/hizmeti kullanan veya tüketen kişi olarak tanımlanabilir. Ancak, teknolojinin hâkim olduğu günümüz dünyasında, kullanıcı kavramı yeni bir anlam kazanmıştır. Kullanıcı, artık sadece ürün satın alan bir kişiyi tanımlayan basit bir terim değildir. Kullanıcılar artık ürün/hizmet ile etkileşime giren, aynı zamanda modern iş dünyasının kalbinde yer alan karmaşık ve çok yönlü bir fikri ifade etmektedir. Günümüzde

kullanıcıların isteklerini/beklentilerini/vb. anlamak çok önemli hale gelmiştir. Bunun nedenlerinden biri, kullanıcıların, şirketlerin ihtiyaç ve tercihlerine uygun ürün ve hizmetler yaratmalarına yardımcı olmalarıdır. Şirketler, kullanıcılarını anlayarak, kullanımı kolay ve görsel olarak çekici ürün ve hizmetler tasarlayabilirler, onları anlayarak hedef pazarlarını belirleyebilir ve belirli kullanıcı segmentlerine hitap eden mesajlar ve reklamlar oluşturabilirler. Bu çabalar, pazarlama çalışmalarının etkinliğini artırılabilir ve daha fazla potansiyel müşteri ve dönüşüm sağlayabilir. Ayrıca, kullanıcıları anlamak, işletmelerin inovasyon alanlarını belirlemesine ve kullanıcılarının ihtiyaçlarına yönelik yeni ürün ve hizmet geliştirmesine yardımcı olabilir, kullanıcılarının sorunlu noktalarına ve isteklerine uyum sağlayarak kendilerini rakiplerinden farklılaştıran yeni ürünler ve hizmetler yaratmasına yardımcı olabilir. Kullanıcı merkezli tasarım olarak bilinen bu yaklaşım, daha iyi kullanıcı deneyimlerine ve daha yüksek katılım ve memnuniyet seviyelerine yol açabilir. Bu nedenle kullanıcıları anlamak, işletmelerin günümüzün rekabetçi pazarında başarılı olması için kritik önem taşımaktadır (Chisel Labs, 2023).

Mobil uygulama kullanıcıları da yukarıda bahsedilen ve “basit” olarak yansıtılan kullanıcı profilinin dışında çıkmıştır. Mobil uygulamaların yaygınlaşması, insanların günlük yaşamlarında evrimsel bir değişikliğe neden olurken (Li vd., 2016: 1351), kullanıcılar da mobil uygulama endüstrisinde çeşitli değişikliklere neden olmuştur. Özellikle kullanıcıların etkileşim faaliyetleri, giderek daha önemli hale gelmekte, uygulama kullanım tercihleri ve geri bildirimler geliştiriciler için hayati önem taşımaktadır. Uygulama mağazaları 100 milyardan fazla kez indirilen milyonlarca uygulamaya ev sahipliği yapmaktadır. Bu nedenle kullanıcıların günlük yaşamlarında mobil uygulamaları nasıl yönettiklerini araştırmak, mobil kullanıcıların davranışlarını ve tercihlerini anlamak, uygulamaların kalitesini çıkarmak ve kullanıcı deneyimini iyileştirmek için bir fırsat yaratmaktadır (Li vd., 2016: 1351). Uygulama mağazaları, kullanıcıların mobil uygulamaları aramasına, satın almasına ve yüklemesine ve ardından inceleme ve derecelendirme şeklinde geri bildirimde bulunmasına olanak tanımaktadır. İnceleme, kullanıcının uygulamayla ilgili deneyimi ve uygulamayla ilgili görüşleri, özellik istekleri ve hata raporları hakkında bilgiler içerebilir. Dolayısıyla incelemeler, yalnızca başkalarının bir uygulama hakkında ne düşündüğünü öğrenmek isteyen kullanıcılar için değil, aynı zamanda müşteri geri bildirimleriyle ilgilenen geliştiriciler ve yazılım şirketleri için de değerlidir (Genc-Nayebi ve Abran, 2017: 207). Derecelendirme ve incelemeler, uygulama kalitesinin kitle kaynaklı bir göstergesi olarak hem geliştiriciye hem de potansiyel yeni kullanıcılara değer katmaktadır. Bu nedenle, geliştiriciler için olumlu yorumlar ve yüksek puanlar almak, uygulamaların görünürlüğünü artıran bir faktördür (Daha

sonra da değinileceği üzere uygulamaların üst sıralarda yer alması önemlidir.) ve bir uygulamanın sürdürülebilir bir geleceğe sahip olmasını sağlamak için önemlidir (Vasa vd., 2012: 241).

2.2.1.4. Bağımsız Geliştiricilerin Bağımsızlığı Üzerine

Uygulama geliştiriciler, mobil uygulama ekolojisinin temel yapı taşlarından biridir. Google ve Facebook gibi büyük geliştiricilerin yanı sıra, bağımsız geliştiriciler ve küçük ölçekli şirketler de uygulama geliştirme alanında önemli rol oynamaktadır. Ancak çok az sayıda çalışma uygulama geliştiricilere odaklanmıştır ve mobil uygulama ekolojisinin bu kısmı hakkında çok az şey bilinmektedir (Wang vd., 2017: 163). Son yıllarda, bir oyunun ya da uygulamanın indie olup olmadığı konusunda çeşitli tartışmaların olduğu bilinmektedir. Buna ilaveten çoğu yazar/akademisyen de indie terimi hakkında net bir ifadede bulunamamaktadır. Ancak hem oyun odaklı çalışmalar yürüten akademisyenlerinin hem de bazı uygulama geliştiricilerinin bağımsızlık terimi hakkında uzlaştığı ortak bir nokta vardır: Ana akım olmamak. Nadav Lipkin (2012: 9-10)'e göre ana akım oyun geliştirme, doğası gereği kurumsal ve kapitalisttir. Evrensel olarak adil olmasa da ana akım, yaratıcılık ve sanattan ziyade kâr ve popüleriteyi vurgulamakla karakterize edilir ve ana akım oyunlar çok sayıda farklı şirketteki büyük ekipler tarafından milyonlarca dolarlık bütçelerle geliştirilmektedir. Öte yandan en basit haliyle indie medya, ana akım olmayan şeylerle tanımlanırken, film yapımları üzerinden bir analogi yapılacak olursa, Hollywood filmleri “çok katlı sinemalar” için; bağımsız filmler “film festivalleri ve sanat sinemaları” içindir (Newman, 2011: 15). Ancak diğer bağımsız kültürel üretim biçimlerinde olduğu gibi, bağımsızlık konusunda net bir kategorizasyon yapmak zordur (Parker, 2013: 1).

Maria B. Garda ve Pawel Grabarczyk (2016: 1), “indie”²³ teriminin etimolojisine rağmen yalnızca “bağımsız” teriminin bir kısaltması olmadığını iddia etmektedir. Onlara göre tam olarak bağımsızlık diye bir şey yoktur ve bağımsızlık kavramı özünde ilişkisel bir kavramdır. Örneğin, bir ülkenin bağımsız olduğundan bahsedildiğinde, onun diğer ülkelerden bağımsız olduğunu eklemek gerekmez. İlişkisel bir kavramın anlamı, parametrelerinden biri değiştiğinde farklılaşmaktadır. Bir ülkenin finansal veya kültürel bağımsızlığından bahsedilmek isteniyorsa, karışıklığı önlemek için bunun doğrudan belirtilmesi gereklidir.

²³ “Independent” kelimesinin kökeni Latince’ye dayanmakta “dependent” (bağlı, bağımlı) ve “in” (değil, olmadan) kelimelerinin birleşiminden oluşmaktadır (Online Etymology Dictionary, t.y.) <https://www.etymonline.com/word/independent> (erişim tarihi: 10.08.2023). “Indie” kelimesi ise bu birleşimin kısaltılmış halidir (Online Etymology Dictionary, t.y.) <https://www.etymonline.com/word/indie> (erişim tarihi: 10.08.2023).

Yazarlar buradan hareketle, oyun bağımsızlığı kavramının anlamını yakalamak için, oyun bağımsızlığı parametreleri olarak işlev görebilecek üç tür bağımsızlık arasında ayırım yapmanın faydalı olacağını ifade etmektedir. Bunlar: Finansal bağımsızlık, yaratıcı bağımsızlık ve yayıncı bağımsızlığıdır (Garda ve Grabarczyk, 2016: 7) ve birbirleriyle doğrudan ilişkilidir.

Finansal bağımsızlık, yazılım ürünlerinin herhangi bir finansman desteği olmaksızın geliştirici tarafından üretilmesini ifade eder. Garda ve Grabarczyk (2016: 8), finansman desteğini detaylandırır: Yalnızca kâr elde etmek amacıyla geliştiricilere finansman sağlayan özel şirket ve bireyleri (örneğin, bankalar, risk sermayesi veya start-up finansörleri) değil, aynı zamanda devlet kurumlarını (örneğin, ulusal fon kuruluşları) ve ticari olmayan projeleri finanse eden diğer kurumları da ifade etmektedir. Yaratıcı bağımsızlığı ise çoğu zaman finansal bağımsızlık belirler; çünkü genellikle hedef kitle yatırımcı tarafından belirlenir (Garda ve Grabarczyk, 2016: 9). Bu nedenle yaratıcı bağımsızlıktan söz edilebilmesi için hedef kitlenin belirlenmesinden, yaratıcı fikrin uygulanmasına kadarki sürecin yine geliştirici tarafından belirlenmesi gerekmektedir. Garda ve Grabarczyk (2016: 10-11)'e göre yayıncı bağımsızlığından, ancak yayıncının aynı zamanda geliştirici olduğu durumda bahsedilebilir. Ancak şunu da belirtmek gerekir ki bir oyunun ilk yayınlandığı andaki bağlamı önemlidir. Çünkü çoğu oyun ilk yayınından sonra başarılı olursa, harici bir yayıncı edinir (örneğin, ürünü başka bir platforma taşımak veya geleneksel perakende sürecine sokmak için). Birçok durumda finansal ve yayıncılık bağımlılığı örtüşmektedir (sıklıkla dış yatırımcı aynı zamanda yayıncıdır). Sonuç olarak yazarlar bağımsız oyun kavramını çevreleyen kafa karışıklığının bu üç bağımsızlık türünün de düzgün bir şekilde ayırt edilmemesi olduğunu dile getirmektedir. Yazarların iddiası, “bağımsız oyun” kavramının üç farklı bağımsızlık türünün kesişimi ile açıklanabileceğidir. Belirli bir oyun bu türlerden herhangi birine, hepsine veya ikisinin herhangi bir alt kümesine ait olabilir. Ancak, bağımsız olarak sınıflandırılabilmesi için bunlardan en az birine ait olması gerekmektedir (Garda ve Grabarczyk, 2016: 11).

Bağımsız yazılım kavramında yaşanan belirsizlik, bağımsız geliştiriciler içinde benzer şekilde belirsizdir. *Indie developers* tanımında yaşanan muğlaklık, kafalarda giderek daha fazla soru işareti uyandırmakta, kavramın ifade edilmesini zorlaştırmaktadır. Geliştiricilerin kendilerine sorulduğunda kimi geliştirici, herhangi bir şirkette çalışmayan kişileri “indie developers” olarak tanımlarken, kimileri ise tek ya da küçük gruplar halinde çalışanları, yani “büyük şirketlerde” istihdam edilmeyen geliştiricileri de “indie developers” olarak görmektedir (Çalışmanın veri toplama aşamasında X platformunda yer alan ‘iOS Dev Community’deki yazışmalardan elde edilen bir sonuç). Bazı geliştiriciler ise yazmış olduğu

kodun kime hizmet ettiğinin geliştiricinin indie olup olmadığını belirlediğini iddia etmektedir. Kod eğer bir şirkete hizmet ediyorsa geliştirici indie olarak görülmezken; kod bir şirkete hizmet etmiyor, bireysel kullanıma açıksa veya herhangi bir topluluğa hizmet ediyorsa geliştirici indie olarak kabul edilmektedir (Çalışmanın veri toplama aşamasında elde edilen geliştirici görüşleri).

Garda ve Grabarczyk'in yukarıdaki sınıflandırması oyunlardan geliştiricilere genişletilecek olursa bir indie geliştiricisini, indie yazılımın türevi olarak tanımlamak gerekmektedir: Eğer bir geliştirici *indie yazılım* yaratıyorsa *bağımsız geliştirici* olmaktadır. Garda ve Grabarczyk'in bu sınıflandırmasının pratikteki etkisi, belirli bir geliştiricinin üzerinde çalıştığı projeden ayrı olarak *indie* veya *ana akım* olmamasıdır. Aslında, odaklanılan projeye bağlı olarak aynı geliştirici, her ikisi olarak da değerlendirilebilir. Bir şirkette çalışan ve ana akım bir oyun geliştiren kişinin boş zamanlarında başka bir proje geliştirdiği düşünüldüğünde bu durumda o kişi hem ana akım hem de indie geliştiricidir (Grabarczyk P., kişisel iletişim, 18.07.2023). En nihayetinde yazılım üretim sürecinde Garda ve Grabarczyk'in bağımsızlık sınıflandırmasından herhangi birinin varlığı halinde geliştirici indie olarak değerlendirilebilir. Sonuç olarak, bağımsızlık terimi ile indie terimi tam olarak birbirini karşılamamaktadır. Ayrıca hem yazılım hem de geliştirici açısından tam bir bağımsızlıktan söz edilememektedir. Paolo Pedercini (2012)'nin de dediği gibi *mutlak bağımsızlık yoktur; çünkü her zaman teknolojik platformlar, protokoller, donanım veya altyapılar tarafından kısıtlanmaya devam edeceğiz*.

2.2.1.5. Mobil Uygulamaların Baskın (İstilacı) Aktörleri

Mobil pazar, sıklıkla güçlü şirketlerin sürekli olarak veri toplayıp dağıtarak değer ürettiği bir ekosistem olarak tanımlanmaktadır (Lai ve Flensburg, 2021: 2301). Bugün, kullanıcı olarak ihtiyaç duyduğumuz cihaz veya hizmetlere Google gibi verilerimizi talep eden şirketler tarafından cevap verilmektedir. Bu şirketler, bazen bize hizmeti satan, bazen de ücretsiz hizmetler sağlayan tekellerdir. Google gibi veri toplayıcı şirketler, ürettiğimiz verilerin tek alıcısı gibi hareket ederler (Couldry ve Mejias 2022: 80). Öte yandan yukarıda da ifade edildiği gibi mobil uygulamalar, günümüz dijital temelli ekonomik sistemin önemli bir parçası haline gelmiştir. Uygulamaların üretilmesi, dağıtılması, tanıtılması ve regülasyonu üzerinde doğrudan hâkimiyeti bulunan şirketler giderek daha fazla uygulama geliştirme/dağıtma gücüne sahip olmaya başlamıştır. Örneğin Google, internet altyapısının inşasında ve yönetiminde merkezi rol oynayan birkaç global teknoloji şirketinden biridir (Lai ve Flensburg, 2021: 2301) ve uygulama mağazalarını adeta işgal etmiştir. Kişisel verilerin

toplanması ve işlenmesi, dijital yaşamın neredeyse her yerde bulunan bir parçası haline gelmiştir ve az sayıda güçlü teknoloji şirketi tarafından domine edilmektedir: Apple ve Google hem işletim sistemlerine hem de uygulama dağıtım kanallarına hakimdir (Kollnig, vd., 2022: 1).

Google LLC'nin 2023'ün son çeyreği tarihi itibarıyla Google Play Store'da 143 adet uygulaması vardır. Bu uygulamalar tarayıcı uygulamalarından sağlık uygulamalarına, eğlenceden yardımcı araçlara kadar pek çok farklı kategoridedir ve kullanıcıların bu uygulamalara ulaşması çok kolaydır; çünkü Google'ın uygulamaları indirme sayıları ve kendi uygulamalarını optimize etmesi sayesinde üst sıralarda yerini almaktadır. 2023 yılının son çeyreği itibarıyla Apple App Store'da yapılan Google uygulamaları taramasına göre (iPhone, iPad, Apple Watch ve Apple TV) Google'a ait 59 uygulama olduğu görülmüştür. App Store'da "Apple Inc." olarak yapılan taramada ise 102 adet uygulamanın olduğu görülmüş (iPhone, iPad, Apple Watch ve Apple TV ürünleri dâhil edilmiş, Mac ürünleri hariç tutulmuştur), uygulama kategorilerinde Google'a benzer şekilde bir çeşitlilik olduğu tespit edilmiştir. Apple'ın Google Play Store'daki uygulama sayısını ise 7'dir ve oldukça sınırlıdır.

Meta Inc, kullanıcılar ve kullanıcı katılımı açısından gelir ve erişimdeki büyüme nedeniyle, özellikle mobil pazarlama ve uygulama ekonomisinde en görünür ve baskın aktörlerden biri haline gelmiştir. (Helmond ve Nieborg, 2016: 8; Helmond, vd., 2017: 2). Play Store'da "Meta Platforms Inc." olarak yapılan taramada toplam Meta'nın toplam 15 adet uygulaması olduğu görülmüştür. Meta'nın yan kuruluşları olan Whatsapp ve Instagram'ın da 6 adet uygulaması bulunduğu tespit edilmiş olup toplamda 21 uygulaması bulunmaktadır. Meta'nın App Store'daki (iPhone, iPad ve Apple TV) taramasında ise 14 adet uygulamasının bulunduğu görülmektedir. Meta'nın yan kuruluşları olan Whatsapp ve Instagram'ın da 5 adet uygulaması bulunduğu tespit edilmiş olup toplamda 19 uygulamasının mağazada yer aldığı görülmüştür. Meta'nın her iki uygulama mağazasında genellikle eğlence ve mesajlaşma uygulamalarının olduğu da dikkat çekmektedir. Ayrıca 2023'ün ikinci çeyreğinin sonunda Meta'nın Instagram, Facebook ve WhatsApp uygulamaları en çok indirilen Android uygulamaları olurken (Statista, 2023b), Instagram, dünya çapında 70 milyon, Facebook ise 38,5 milyon indirmeyle ikinci en popüler uygulama olmuştur. (Statista, 2023c).

MAANG şirketlerinden Netflix, Microsoft ve Amazon'un da mobil uygulama mağazalarında ciddi derecede üstünlüğü bulunmaktadır. Play Store'da "Netflix Inc." olarak yapılan taramada Netflix'e ait 84, App Store'da yapılan taramada ise 83 uygulaması (iPhone, iPad ve Apple TV) olduğu tespit edilmiş olup bunların çoğunun eğlence ve oyun uygulaması olduğu görülmüştür. Play Store'da "Microsoft Corp." olarak yapılan taramada Microsoft'a ait

83, App Store’da yapılan taramada ise 90 adet (iPhone, iPad, iMessage ve Apple TV) uygulama tespit edilmiş, bunların çoğunun yardımcı araç uygulaması olduğu görülmüştür. Play Store’da “Amazon Mobile LLC.” olarak yapılan taramada Amazon’a ait 48, App Store’da yapılan taramada ise 40 (iPhone, iPad, Apple Watch ve Apple TV) uygulama bulunmaktadır ve bunlar, video, müzik ve alışveriş uygulamalarıdır.

Sonuç olarak MAANG şirketleri, mobil uygulama mağazalarını istila etmiştir. Bu durum, küçük ölçekli şirketlerin veya bağımsız geliştiricilerin uygulamalarına yeteri kadar ulaşamamasına neden olmaktadır. Çünkü çoğunlukla kullanıcılar üst sıralardaki oyun ve uygulamalara ilgi göstermektedir. Özetle, çoğu zaman kullanıcılar alternatifsiz bırakılmaktadır. Alternatif uygulamalar, mevcut şirket uygulamalarına göre daha iyi performans gösterse, daha işlevsel ve hatta daha az veri toplama eğiliminde olsalar bile, bu uygulamalar genellikle görünürlük açısından yeterince erişilebilir değildir.

2.2.2. Mobil Uygulamalarda Gözetim Altyapısı

Yakın tarihli bir konferans konuşmasında, AB Komisyonu Başkan Yardımcısı Margrethe Vestager, katılımcılara *akıllı telefonunuzun anneniz olduğunu hayal edin* demiştir. *Ne de olsa her sabah gördüğünüz ilk ve uyumadan önce gördüğünüz son şey* diye devam etmiş, *onun onaylamayacağı bir şey yapmıyorsunuz, sonuçta sizi büyüttü* diyerek alegorik bir ifadeye bulunmuştur. Vestager, konuşmasında akıllı telefonlarımızın yaptığı kapsamda, her hareketimizi izleyen başka biri olsaydı buna direneceğimizin de altını çizmiştir (Vestager, 2019’dan Akt. Lai ve Flensburg, 2020: 1). Yukarıdaki ifadelere bakıldığında Vestager’in akıllı telefon üzerinden kurduğu alegori, mobil uygulamaları da kapsamaktadır. Neticede kullanıcıyı takip etmek için yalnızca sensörlerin varlığı yeterli değildir. Mobil uygulamalar, akıllı telefonların sensörlerini fonksiyonel hale getirmektedir.

Mobil uygulamaların yaygınlaşmasıyla, zengin bir gözetim ekosistemi gelişmiştir. Geliştirici uygulamaları, kullanıcıların hareketlerini takip edebilirken, reklam şirketleri (örneğin, AdMob), hedefli reklamlar sunmak için geliştiricilere destek sağlamaktadır. Analiz şirketleri (örneğin, Flurry Analytics) de uygulama geliştiricilere, ürünlerini geliştirmek üzere kullanım verilerini toplamaları için kütüphaneler sunmaktadır. Mobil cihazlarda izleme, web tabanlı izlemeye göre de daha karmaşık ve kullanıcılar için daha az şeffaf bir süreçtir. Web izleme, genellikle üçüncü taraf çerezler (cookies)²⁴ aracılığıyla gerçekleştirilirken (Kullanıcılar istediklerinde üçüncü taraf çerezlerini inceleyebilir veya engelleyebilir.), mobil

²⁴ Çerezler, kullanıcılara ait verilerin veya dijital izlerin takibini sağlayan ve bu verilerin pazarlama amaçlı kullanılmasına yardımcı olan veri depolama mekanizmalarıdır (Taşkaya ve Talay, 2019: 357).

cihazlarda izleme, kullanıcılar tarafından uygulama yükleme ve izinleri kabul etme kararının ötesine geçebilir, bu da potansiyel gizlilik ve mahremiyet ihlali riskini artırabilir. Ayrıca erişim izinleriyle toplanabilen çok çeşitli bilgiler, kullanıcıların konumlarını, telefon numaralarını, arama ve e-posta geçmişlerini, fotoğraflarını ve takvim etkinliklerini içerebilir (University of Washington, 2012: 2).

Yukarıda bahsedilen web tabanlı gözetimin aksine, mobil uygulamalarda gözetim, birçok yazılım ve aracı yardımıyla gerçekleştirilebilir. Örneğin, çeşitli platformlar geliştiricilerin ilgisini çekmek ve daha fazla uygulama üretilmesine yardımcı olmak için giderek artan sayıda Uygulama Programlama Arayüzü (API- Application Programming Interface)²⁵ sunmaktadır. Bu API'ler gözetimi olanaklı kılan birer aracı konumundadır. Akıllı telefon işlevlerine (örneğin, GPS, ivmeölçer, kamera) ve çoğu gizliliğe duyarlı olan kullanıcı verilerine (örneğin, benzersiz tanımlayıcılar, konum, sosyal medya hesapları) erişim sağlamaktadır (Liu vd., 2016: 27). Uygulama takibini kolaylaştıran bu yazılımlar tek başına bir yazılım ya da aracının değil, daha geniş perspektifte bir gözetim alt yapısının varlığına işaret etmektedir. Mobil uygulamalarda var olan gözetim altyapısını da üç başlık altında toplamak mümkündür. Bunlar Tanımlayıcılar (Identifiers), Uygulama İzinleri (Mobile Permissions) ve Çevrimiçi İzleyiciler (Online Trackers)'dir ve veri gözetimini olanaklı kılmaktadır.

2.2.2.1. Mobil Uygulamaların Kimlik Tanımlayıcıları

Mobil cihaz tanımlayıcıları (Mobil Cihaz/Uygulama Kimlikleri), mobil cihazı benzersiz bir şekilde tanımlayan bir kimlik numarası veya karakter dizisidir. Bu tanımlayıcılar, cihazın donanımı veya yazılımıyla ilişkili olabilir ve kullanıcı doğrulama işlemlerinde önemli bir rol oynar. Mobil cihazlarda Uluslararası Mobil Cihaz Kimliği (IMEI- International Mobile Equipment Identity), Uluslararası Mobil Abone Kimliği (IMSI- International Mobile Subscriber Identity) ve Android ID gibi bazı yaygın tanımlayıcıların kullanıldığı bilinmektedir (Wu vd., 2016: 8073-8081). IOS ekosisteminin en bilinen tanımlayıcısı ise Apple ID'dir ve bu kimlik, kullanıcının cihazının özelliklerini tanımlayan bir parmak izi olarak kullanılabilir. Bu parmak izi, kullanıcının gerçek dünyadaki kimliğiyle ilişkilendirilebilir (Kurtz vd., 2016: 13-17). Yine iOS'un *Reklamverenler için Tanımlayıcı* (IDFA- Identifier for Advertisers) olarak da adlandırılan bir tanımlayıcısı da bulunmaktadır. Android'de ise Google Reklam Tanımlayıcı (GAID- Google Advertising ID) bulunmaktadır.

²⁵ API'ler uygulama yazılımları arasında verilerin biçimlendirilmiş şekilde aktarılmasını sağlayan bir protokoldür (Apple Support, t.y.).

Bir diğerk tanımlayıcı ise *Reklam Tanımlayıcısı* (AdID)'dir. AdID, hem iOS hem de Android'de bulunan benzersiz bir tanımlayıcıdır. Bu tanımlayıcılar, çerezlerin özellikle web tarayıcılarda etkili, mobil uygulamalarda ise etkisiz olması üzerine devreye alınan hamlelerdir ve reklamverenlerin kullanıcılara daha alakalı reklamlar göstermesini sağlamaktadır (örneğin, aynı reklamı iki farklı uygulamada iki kez göstermekten kaçınarak), ancak aynı zamanda uygulama kullanıcıları hakkında detaylı profiller oluşturmak için de kullanılabilmekte, potansiyel veri ihlallerine yol açabilmektedir (Kollnig vd., 2021: 181; Kollnig, vd., 2022: 6-7). Öte yandan geliştiriciler de bireysel uygulama kurulumlarını tanımlamak veya sadece ek izinler istemekten kaçınmak için kullanıcılara kimlik atamayı da seçebilirler. Bu tür tanımlayıcılara da uygulama tarafından atanan kimlikler denilmektedir (Vanrykel vd., 2017: 3).

Wenjia Wu vd. (2016: 8073-8074)'nin çalışmasına göre tanımlayıcılar kötüye kullanılabilir. Yine bir diğerk çalışma, kullanıcıların yapılandırma profillerinin parmak izi oluşturmak için yeterli bilgi sağladığını göstermiştir. Wu vd. (8073-8074)'nin çalışmasındaki bazı testlerde, kullanıcılara ait verilerin %90'ın üzerinde doğruluk oranıyla eşleştirildiği görülmüştür. Bu bilgiler, kullanıcının cihazını diğerk kullanıcılardan ayırt etmek için kullanılabilir. Apple kimlik bilgileri bir kullanıcının kimliğini belirlemek veya takip etmek için kullanılabilir. Ayrıca araştırmada, kullanıcı mahremiyeti konusunda bazı endişelerin olduğu bulgular arasındadır. Çalışmada, kullanıcılardan habersiz veri toplamanın ve parmak izinin gerçek kimlikleriyle ilişkilendirilebilmesinin önemli bir sorun olduğu da ifade edilmektedir (Kurtz, vd., 2016: 13-17). Bu tanımlayıcıların kullanıcıların gerçek kimlikleriyle eşleştirilebilme ihtimali bir bakıma Apple'ın da kabul etmiş olduğu bir durumdur. Apple, 2019 geliştirme konferansında, özellikle hassas bir uygulama kullanıcısı grubu olan çocuk uygulamalarının üçüncü taraflarca izlenmesinin yasaklandığını duyurmuştur. 2021'de ise iOS 14.5 sürümünden başlayarak Apple, geliştiricilerin AdID'ye erişmeden veya reklamla ilgili izleme yapmadan önce kullanıcılardan izin istemelerini zorunlu kılmıştır. Google ise henüz Android kullanıcılarının AdID'ye erişimin engellenmesine izin vermemektedir (Kollnig vd., 2022: 2).

Konrad Kollnig vd. (2022: 10)'nin araştırmasında AdID'ye potansiyel erişimin iOS uygulamalarına göre Android uygulamaları arasında daha yaygın olduğu görülmüştür. İncelenen uygulamalar arasında, Android uygulamalarının %86,1'i AdID'ye erişebilirken, iOS'ta bu oran %42,7'dir. AdID erişimindeki farklılıkların nedeni platformlar tarafından belirlenen kısıtlamalardır. Apple, genellikle reklamla bağlantılı olan AdID'nin kullanımına karşı adımlar atmaktadır. Uygulama yayıncıları, App Store'a uygulama gönderirken,

uygulamalarının AdID'yi yalnızca reklamcılıkla ilgili belirli ve özel nedenlerle kullandığını beyan etmek zorundadır. Buna ek olarak Apple, iOS kullanıcılarının tüm uygulamaların AdID'ye erişmesini engellemesine izin vermekte ve açık bir onay istemektedir. Kollnig vd. (2022)'nin bu çalışması, AdID'ye erişimin iOS'a kıyasla Android'de daha yaygın olduğunu gösterse de iOS uygulamalarındaki %42,7'lik oran da azımsanmayacak bir oran olduğu söylenebilir. Apple'ın geliştiriciler üzerindeki düzenlemeleri ve AdID'ye erişimin kullanıcıların iznine bağlı olması gibi uygulamalar olumlu olsa da bu durum, atılan bu adımların etkisinin sınırlı olduğuna işaret etmektedir. Ayrıca üçüncü tarafların AdID'ye erişimi engellenmiş olsa bile bu tür tanımlayıcılara Apple'ın ulaşip ulaşmadığı da tam olarak bilinmemektedir.

2.2.2.2. Veri Gizliliğinde Son Kale: Uygulama İzinleri

Mobil uygulama izinleri (Mobile App Permissions), mobil cihazdaki hassas bilgileri korudukları için Android ve iOS'un güvenlik modellerinin önemli bir parçasını oluşturmaktadır (Kollnig vd., 2022: 7). Mobil uygulama platformları, kişilerin hassas kaynaklarına erişimi düzenlemek için izin sistemlerini kullanmakta, üçüncü taraf bir uygulamaya veri ve kaynaklara erişim izni verilip verilmeyeceğini belirlemek için kullanıcı istemlerine güvenmektedir (Wijesekera vd., 2017: 1078) ki izinler, uygulamalar için önemli bir rol oynamaktadır; çünkü uygulamalara izin vermek, veri sızıntılarına yol açabilmektedir (Kern ve Semetinger, 2012: 148). Bu nedenle mobil uygulama izinleri, deyim yerindeyse kullanıcının mahremiyeti için *son kaleyi* temsil etmektedir (Lai ve Flensburg, 2020: 3). Lai ve Flensburg'un *son kale* vurgusu, bu güvenli alana (kale) gelene kadar bazı önlemlerin alınarak belli ölçülerde düşmanın bertaraf edilebildiği (Örneğin, çerezlerin engellenmesi, reklam tercihlerinin pasif hale getirilmesi, alternatif uygulamaların kullanılması veya uygulama kullanımından vazgeçilmesi), tüm çareler tüketildiğinde -veya hiçbir şekilde karşı koymaksızın olduğu gibi- kullanıcıların, verilerini kendi elleriyle geliştiricilere açtığı son adım olarak değerlendirilebilir. Çünkü uygulama izinleri, cihazın geçmişini ve mevcut durumunu okuma olanağı sağlamakta, cihaz ve uygulama geçmişine erişimle birlikte hassas veri günlüklerini okuma ve anlık mesajları inceleme yeteneklerini de içermektedir (Lai ve Flensburg, 2021: 2310). Öyle ki, yapılan bazı çalışmalar, bu erişim sonucu, mobil uygulamaların güvenli olmayan arka uç veri tabanlarının, kullanıcı adları, şifreler gibi kişisel olarak tanımlanabilen bilgiler dahil olmak üzere tahmini 280 milyon hassas kullanıcı kaydını açığa çıkarabileceğini göstermiştir (Zuo vd., 2019: 1296).

Uygulama izinleri, herhangi bir uygulamanın yazılım kodunda tanımlandığı ve uygulama sahipleri tarafından eklendiği için, veri erişimi üzerindeki kontrolü, doğal olarak uygulama sahiplerinin verir ve onların taleplerini yansıtır. Başka bir ifadeyle, dünya genelinde en fazla indirilen uygulamalara sahip olmanın bir sonucu olarak, en büyük uygulama sahipleri genellikle kullanıcı verilerine en geniş erişimi elde ederler (Lai ve Flensburg, 2021: 2310). Android ve iOS platformlarının her ikisi de izin tabanlı mekanizmalara dayanmaktadır. Bu platformlar, kullanıcıların hassas verilere ve işlemlere erişimi kontrol etmelerine izin veriyor olsa da sonuçta, bu da sorunlu bir durumdur; çünkü kullanıcıdan vermesi beklenen çok sayıda uygulama izni kararı ortaya çıkmaktadır (Liu vd., 2016: 27). Kullanıcılar da genellikle bu izinlerin müdahaleci olabileceğini fark etmemektedir. Share Labs (2015a)'ın araştırmasına göre bu durum, kullanıcıların bu izinlerin anlamını kavrayamadıkları için değil, genelde bunu anlama konusundaki ihmalleri nedeniyle olduğunu göstermiştir. Android kullanıcılarının izin kavramını nasıl anladıklarını araştıran bir çalışma da kullanıcıların büyük bir kısmının temel erişim haklarını ve bunların ne gibi sonuçlara yol açabileceğini anlamadıklarını ortaya koymuştur. Ancak, katılımcıların çoğunluğu, telefonlarının çok fazla kaynağına erişim izni olan uygulamaların farkında olmaları halinde bunları kaldırmaya istekli olduklarını belirtmiştir (Struse vd., 2012: 66).

2.2.2.3. Uygulamanın Derinliklerine Gömülen Yazılımlar: Çevrimiçi İzleyiciler

İzleme faaliyeti, kullanıcı etkinliklerinin zaman içinde oluşturulan bir profil ile ilişkilendirilmesi olarak tanımlanabilir. Kullanıcıyı benzersiz şekilde tanımlamak için bir tür istemci durumu gereklidir. En temel izleme profili, kullanıcının belirli bir uygulamayı ne zaman kullandığına dair bir dizi gözleme dayanır. Bu asgari profil, kullanıcının konumu gibi belirli zaman dilimlerindeki konum bilgisi, telefon numarası ve hatta kullanıcının kişisel içerikleri gibi kişisel verilere kadar çeşitli ek bilgiler içerebilir (University of Washington, 2012: 2). Bir çevrimiçi izleyici (Online Trackers) -Çevrimiçi izleyiciler, üçüncü taraf hizmetleri (izleyicileri) olarak da adlandırılmaktadır- genellikle şirketler tarafından, uygulama geliştiricilerinin işini kolaylaştırmayı amaçlayan bir tür hazır araç seti olan Yazılım Geliştirme Kiti (SDK- Software Development Kit) olarak dağıtılmaktadır (Exodus Privacy, t.y.). Kâr amacı gütmeyen bir kuruluş olan Exodus Privacy, çevrimiçi izleyicilerin hangi amaçla uygulamalara gömüldüğünü altı başlık altında toplamıştır bunlar: Çökme Raporlayıcıları, Analitik, Profil Oluşturma, Kimlik Belirleme, Reklamlar ve Konum'dur. Çökme Raporlayıcıları'nın görevi, uygulamanın nasıl bir sorunla karşılaştığını geliştiricisine bildirmektir. Uygulama çöktüğü anda toplanan bilgiler, geliştiricinin hatayı düzeltmesine

olanak tanımaktadır. Analitik ise geliştiricinin hedef kitlesi hakkında daha iyi bilgi sahibi olmasını (Kullanıcının hangi sayfayı ziyaret ettiğini veya sayfanın belirli bir alanında ne kadar süre kaldığını öğrenebilir.) sağlamak içindir. Profil Oluşturma izleyicilerinin amacı, sanal bir profil oluşturmak için uygulama kullanıcısı hakkında mümkün olduğunca fazla bilgi toplamaktır. Bu amaçla, izleyici örneğin tarama geçmişine veya yüklü uygulamaların listesine vb. bileşenlere odaklanmaktadır. Kimlik Belirleme izleyicileri de dijital kimlikleri belirlemekten sorumludur. Bu kimlik, resmi bir kimliğe veya soyut tanımlayıcılara (takma ad vb.) atıfta bulunabilir. Amaç, bir bireyin çevrimiçi ve çevrimdışı faaliyetlerini ilişkilendirebilmektir. Reklam izleyicileri de hedeflenen reklamları sunmak için uygulama kullanıcısını tanımlamayı amaçlamaktadır. Bu yalnızca kullanıcının hâlihazırda oluşturulmuş bir dijital profili varsa mümkün ve geçerli olmaktadır. Geliştiricinin böyle bir izleyiciyi uygulamaya yerleştirmesinin amacı, genellikle uygulamalardan reklam yoluyla para kazanmaktır. Konum izleyicileri ise mobil cihazın coğrafi konumunu belirlemek için tasarlanmıştır. Bunu yapmak için, bu tür bir izleyici çeşitli sensörlerden yararlanmaktadır: Bunlardan bazıları GPS çipleri, çevredeki hücresel antenler, bölgede bulunan Wi-Fi ağları, yakındaki Bluetooth işaretçileri ve hatta hoparlörler tarafından iletilen belirli seslerdir (Exodus Privacy, t.y.).

Üçüncü taraf takibi geniş anlamda kişisel verilerin bir çevrimiçi hizmetten bu hizmetin sağlayıcısı dışındaki bir kuruluşa aktarılması olarak tanımlanabilir (Binns vd., 2018: 51). Üçüncü taraf hizmetleri gözetim ekosisteminin ayrılmaz bir parçasını oluşturmaktadır: Uygulama geliştiricilerinin performans analizi ve sosyal ağ entegrasyonu gibi özellikler eklemelerine ve kullanıcı takibi ve hedefli reklam dağıtımını mümkün kılarak uygulamalarından para kazanmalarına olanak sağlamaktadırlar (Vallina-Rodriguez vd., 2016: 1). Ancak, mobil sistemlerin genel opaklığı nedeniyle, bu tür hizmetler kullanıcılar tarafından büyük ölçüde görünmezdir. Bu durum kullanıcı mahremiyeti açısından olumsuz sonuçlar doğurmaktadır, zira üçüncü taraf hizmetler kullanıcıları rızaları olmadan, hatta birden fazla uygulama üzerinden takip edebilmektedir (Razaghpanah vd., 2018: 1). Share Labs (2015b)'ın araştırma sonuçlarına göre web ortamında en sık kullanılan izleyici Google Analytics (Google Analiz/Analitik)'dir. Bir diğer izleyici ise yine Google'a ait olan DoubleClick'dir. DoubleClick, Google'ın tamamlayıcısıdır. Müşterilerin işlem yapmalarını, hedeflemelerini, dağıtım yapmalarını ve reklam kampanyalarına rapor vermelerini sağlamaktadır. İzleyicilerde en sık görülen bir başka şirket ise Facebook'tur. Web ortamına benzer şekilde bu izleyiciler mobil uygulamalarda da yoğun olarak kullanılmaktadır. Kollnig vd. (2021: 21)'nin analizi, izleme pazarında yüksek düzeyde bir yoğunlaşma olduğuna işaret etmektedir:

Alphabet/Google ve Meta/Facebook, uygulama takibine de hâkimdir. Aynı zamanda, nispeten daha küçük ölçekli birçok şirket de uygulama takibine dâhil olmaktadır. Bunlardan bazıları uygulama yüklemeleri açısından oldukça yüksek pazar paylarına ulaşmayı başarmıştır (AppLovin, AdColony ve Chartboost). Bu küçük şirketler Alphabet/Google, Meta/Facebook veya Verizon gibi geniş bir dijital hizmet portföyüne sahip olmak yerine genellikle yalnızca mobil reklamcılığa odaklanmaktadır (Kollnig vd., 2021: 21). Daha küçük şirketlerin daha az uygulamaya erişimi olabilir, ancak yine de bireylerin yaşamları hakkında, özellikle de toplu düzeyde, derin bilgiler edinebilirler. Bir izleme şirketi yalnızca küçük bir kullanıcı alt kümesine erişebilse bile, kalıcı kullanıcı tanımlayıcılarının kullanılması bu şirketlerin veri araçları gibi diğer izleme şirketleriyle veri alışverişinde bulunmasını ve daha fazla sayıda kullanıcı hakkında bilgi edinmesini sağlayabilir (Kollnig vd., 2021: 22).

Mobil uygulama geliştiricilerinin önemli bir bölümü, genellikle uygulama çökmesi, hata raporlama ve sosyal ağ entegrasyonu gibi kullanıcı deneyimini geliştiren hizmetlerin yanı sıra kullanıcı takibi ve reklam entegrasyonu ile uygulamalarından para kazanmak için üçüncü taraf sağlayıcılara güvenmekte ve uygulamalarına bu yazılımları entegre etmektedir. Üçüncü taraf izleyiciler, hizmetlerini sağlamak için kullanıcı hakkında bilgi toplamaktadır. Dahası, üçüncü taraf etki alanları uygulama içi reklamlar sağlamasalar bile izleme bilgilerini toplayabilmektedir (Vallina-Rodriguez vd., 2016: 1; Razaghpanah vd., 2018: 1-3). Bu bilgileri toplamak için kullanıcı tarafından verilen uygulama izinleri kullanılır. Mobil platformlar genellikle kullanıcıların her uygulama için izin vermesine veya izinleri devre dışı bırakmasına olanak tanısa da bu modelin çeşitli eksiklikleri vardır. İlk olarak, kullanıcılar genellikle bir uygulamaya izin vererek bilgilerinin üçüncü taraf hizmetler tarafından toplanabileceğinden habersiz kalmaktadır. İkincisi, kullanıcılar hangi uygulamaların aynı üçüncü taraf hizmetlerini paylaştığı konusunda bilgilendirilmemekte, bu da onları üçüncü taraf hizmetlerinin topladığı potansiyel olarak zengin verilerden (uygulamalar arasında bir izinler süper kümesini kapsayan) habersiz kılmaktadır. Bu şeffaflık eksikliği, üçüncü taraf hizmet ekosisteminin kullanıcılar, araştırmacılar ve düzenleyiciler için temelde gizemli kaldığı anlamına gelmektedir (Vallina-Rodriguez vd., 2016: 1). Bunun kullanıcı mahremiyeti açısından doğrudan sonuçları vardır. Mobil sistemlerdeki genel şeffaflık eksikliği, kullanıcıların uygulamaları tarafından kullanılan üçüncü taraf hizmetlerini tanımlayamamasına ve bu hizmetlerin kişisel verilerini ve çevrimiçi etkinliklerini uygulamalar ve platformlar arasında ne ölçüde toplayabildiğini, ilişkilendirebildiğini ve bir araya getirebildiğini bilememesine neden olmaktadır. Sonuç olarak hem kullanıcılar hem de geliştiriciler bu hizmetlerin ağ düzeyinde nasıl çalıştığına, hassas verileri işleyip işlemediğine

veya nasıl işlediğine ve veriler cihazdan çıktıktan sonra, bağlı reklam hizmetleri ve hatta veri araçları da dahil olmak üzere diğer üçüncü taraflarla paylaşıp paylaşmadığına (veya satıp satmadığına) dair tam veya doğru bilgilere sahip değildir (Razaghpanah vd., 2018: 1).

2.3. Merkezi Uygulamalardan Merkezi Olmayan Uygulamalara

Büyük çoğunluğu ticari olan mobil uygulamalar, genellikle kontrol, yönetim ve denetim sürecinin tek merkezden (sunucu) yürütüldüğü, merkezi (centralized) bir alt yapı kullanmaktadır. Merkezi uygulamaların tüm verileri, merkezi uygulamaya ait sunucularda depolanmaktadır. Kullanıcıların verilere erişimi, uygulamanın güncellenmesi ve kontrolleri bu sunucu aracılığıyla gerçekleştirilmektedir. Öte yandan merkezi alt yapıyı kullanmayan, herhangi bir otoritenin kontrolüne olmayan Blok Zinciri (Blockchain) tabanlı uygulamalar, dağıtık (distributed) merkezi olmayan (decentralized) sunucularda -ağ üzerinde çeşitli düğümlere (node) dağıtılmış- depolanmaktadır. Bu uygulamalar merkeziyetsiz uygulama (DApp- Decentralized Application) olarak adlandırılmaktadır.

Son yıllarda blok zincir teknolojisi ve uygulamaları oldukça popülerlik kazanmıştır. Bu teknolojinin etkinliği ve erişilebilirliği, geniş çapta kabul gören bir teknoloji haline gelmesini sağlamış (Rajasekaran vd., 2022: 1), Blok Zinciri mantığı günümüzdeki merkezileşme kavramının sorgulanmasına neden olmuştur. Öte yandan Blok Zinciri henüz çok yeni bir teknolojidir ve bazı akademisyenlere göre siber saldırılara karşı kırılgan olması ve merkezi uygulamaların yıllardır süregelen otoritesi nedeniyle bu teknolojiye temkinli yaklaşılmaktadır. Ancak bu teknoloji üzerinde çalışan uygulamalarının vadetmiş olduğu güvenlik, şeffaflık, mahremiyet ve özgürlük gibi kavramların, tek merkezden yönetilen mobil uygulamalardaki problemlerin üstesinden gelebilecek ve çözümler üretebilecek potansiyele sahip olduğu da göz ardı edilmemelidir. Bu nedenle merkezi uygulamalardan merkezi olmayan uygulamalara doğru evrilebileceği varsayılan -merkezi uygulamalar tamamen yok olmasa bile- uygulama ekosisteminin, blok zinciri tabanlı ve merkezi olmayan uygulamalarını kullanıcı mahremiyeti, veri gizliliği ve güvenliği açısından sorgulamayı gerektirmektedir.

2.3.1. Blok Zinciri Teknolojisi

Blok zinciri teknolojisi, dijital para birimi olarak adlandırılan Bitcoin'in işleyişini destekleyen tasarıma verilen isimdir. Bitcoin, blok zinciri olarak bilinen yapı üzerine kuruludur. Bu sistem, iki ağ üyesi arasında gerçekleşen işlemlerin tüm ağ üyeleri (düğümler) tarafından duyurulması ve sınırlı bir kapasiteye sahip olan bloklara kaydedilmesiyle çalışmaktadır. Bir blok dolunca, düğümler karmaşık; ancak kolay doğrulanabilir birtakım matematiksel işlem gerçekleştirilmektedir. Bir düğüm, problemi çözdiğünde, çözümü diğer

düğömlere duyurur. Düğömler, bu çözümleri ve işlemleri hızlı ve uygun maliyetle doğrular. Ağın işlem gücünün çoğunluğu (%51'i) bir bloğı onayladığında, düğömler yeni işlemleri mevcut bloklarda değıştirilmiş yeni bir blokta kaydetmeye başlamaktadır. Problemini çözen ilk düğüm, ağın para birimiyle ödüllendirilmektedir. Bu ödöl, işlemlerin doğrulanmasını teşvik etmekte ve genellikle madencilik (mining) olarak adlandırılan süreci tetiklemektedir. Ancak, aslında bu süreç, işlemleri doğrulama sürecidir ve bu, terim olarak daha doğru bir tanımlamaya olanak vermektedir (Nakamoto, 2008: 1).

Kavramsal olarak blok zinciri, katılımcı üyeler arasında paylaşılan işlemlerin kayıtlarını içeren dağıtılmış bir veri tabanıdır. Her bir işlem, üyelerin çoğunluğunun mutabakatı ile onaylanır ve böylece hileli işlemlerin toplu onaydan geçmesi mümkün olmaz. Bir kayıt oluşturulduktan ve blok zinciri tarafından kabul edildikten sonra, asla değıştirilemez veya kaybolmaz (Efanov ve Roschin, 2018: 116). Blok zinciri teknolojisi güvenlik, şeffaflık, merkezi olmayan yönetim, değışmezlik ve programlanabilirlik gibi kendine has temel özellikleri içermektedir. Üstelik herhangi bir merkezi güvenilir otoriteye bağılı değildir. Ayrıca işlemlerinin doğrulanması için herhangi bir aracı tarafa ihtiyaç duyulmamaktadır. Bu olgu, kullanıcıların işlemleri bağımsız ve ucuz bir şekilde kolayca doğrulamasına ve incelemesine olanak tanımaktadır (Rajasekaran vd., 2022: 1). Blok zinciri teknolojisi, kripto para birimi kavramından öte bir teknolojidir. Genel anlamda her türlü mal, hizmet veya işlemin güvenli bir şekilde gerçekleştirilmesini sağlayan bir yapı sunmaktadır. Bu teknoloji, gelecekte endüstride farklı türdeki sorunların üstesinden gelmede önemli bir rol oynayabilir. Özellikle veri işleme süreçlerinde, güvenlik, şeffaflık ve güvenilirlik gibi endüstriyel zorluklara çözüm sağlayabilir, eşler arası veya eşten eşe (P2P- Peer-to-peer) ağ, kriptografi (cryptography) ve şifreleme algoritmaları (hash) ile güven sorunu çözülebilir. Blok zinciri, hali hazırda sağladığı şeffaflık ve güvenlik ile çeşitli sektörlerde adeta devrim yaratmış ve işlemlerin güvenilirliğine yeni bir boyut getirmiştir (Ahram vd., 2017: 1; Efanov ve Roschin, 2018: 116; Golosova ve Romanovs, 2018: 1).

Blok zinciri teknolojisi ve geleceğı hakkında iki farklı görüş bulunmaktadır. Bir bölüm akademisyen ve araştırmacı, blok zincirinin internetten sonraki en önemli buluş olarak kabul etmektedir (Efanov ve Roschin, 2018: 116). Geliştiriciler, girişimciler ve teknoloji meraklıları gibi paydaşlar da blok zincirinin çağdaş, ekonomik, yasal, politik ve kültürel manzarayı yeniden yapılandırma potansiyeline sahip olduğunu iddia etmektedir. Şüpheciler ise bu teknoloji ve uygulamalarının yukarıda belirtilen -ekonomik, yasal, politik ve kültürel- yapıları değıştirme potansiyelinin muğlak ve belirsiz olduğunu iddia etmektedir (Frizzo-Barker vd., 2020: 1). Hatta bazı yazarlar, sistemin güvenliğinin bazı kriterlere bağılı olduğunu ve tamamen

güvenli olamayabileceğinden bahsetmektedir. Örneğin Wang vd., (2020: 108767)'ye göre de blok zinciri ağları çoğunlukla müdahaleye/manipülasyona karşı dayanıklı olsa da bazı ağ saldırılarına karşı savunmasızdır. İşlemler anonim olsa da işlem grafiğini analiz edilerek işlemin iki tarafı arasındaki ilişki hesaplanabilir. Bu nedenle blok zincirinin kamuya açık olan şeffaf özellikleri, işlem gizliliğini ve güvenliğini tehdit edebilmektedir. Saifedean Ammous (2016:3)'a göre de blok zinciri, sağlam ve değiştirilemez bir veri tabanı ve varlık kayıdır. Ancak, blok zinciri yalnızca yerel para birimi için yeterince değerli olduğunda ve para birimi ağının saldırılara karşı dayanıklı olması için yeterli işlem gücüne sahip olduğunda geçerlidir (Ammous, 2016: 3). Neticede blok zincirinde de tam anlamıyla bir gizlilik ve güvenlik söz konusu değildir ki daha önce yaşanan bazı olaylar bu sonucu kanıtlar niteliktedir. Blok zincire yapılan bazı saldırılar sonucunda yalnızca 2022 yılı içerisinde 3 milyar ABD doları üzerinde bir varlık çalınmış, sistemin gizlilik ve güvenlik söylemi sorgulanmaya başlamıştır (bkz. Bambysheva, 2022; Howcroft ve Satter, 2023; Korn, 2023). Ancak bazı çalışmalar da veri, kimlik ve işlem gizliliğinin bazı ek önlemlerle korunabileceğini, kullanıcıların verilerinin kontrolünü sağlayabilecek blok zincir modellerinin yaratabileceğini de göstermiştir (bkz. Zyskind ve Nathan, 2015; Bernabe vd., 2019; Chanson vd., 2017; Li vd., 2020; Feng vd., 2022)

2.3.2. Blok Zincirinde Gizlilik ve Güvenlik

Bireylerin verilerini toplama ve analiz etme yeteneklerinin giderek arttığı günümüzde, ağ tarafından üretilen *verinin mülkiyeti* giderek daha önemli hale gelirken (Mohanta vd., 2019: 14), insanlara ürettikleri verilerin sahipliğini vermek de çok önemli bir konu haline gelmektedir (Chanson vd., 2017: 13). Son zamanlarda kullanıcıların mahremiyetini tehlikeye atan gözetim ve veri ihlalleri vakalarındaki artış, üçüncü tarafların büyük miktarlarda kişisel veri topladığı ve kontrol ettiği mevcut modelin sorgulanmasına da neden olmaktadır (Zyskind ve Nathan, 2015: 180). Özellikle merkezi uygulamaların yaratmış olduğu veri gözetimi ve veri sömürsünün önüne geçebilecek çözümler aranmaya başlanmıştır. Blok zinciri de bu teknoloji çözümlerinden biri olarak görülmektedir.

Blok zinciri, anonim kullanıcılar arasında güven oluşturmada ve herhangi bir üçüncü taraf aracı olmadan işlem yapmalarına olanak tanımaktadır. Böylelikle merkezi sunucuya ihtiyaç kalmamaktadır. Diğer yandan blok zinciri teknolojisinin büyük veri ile entegrasyonu, gizli veya hassas verilerin, sırların ve telif hakkı formlarının güvenli kriptografik katmanda tutulmasına yardımcı olmaktadır. Ayrıca, blok zincirinin değişmez doğası nedeniyle tamamen güvenli olan büyük hacimli verilerin depolanmasına da yardımcı olmaktadır (Rajasekaran vd.,

2022: 11). Blok zincirde kişiler, verileri üzerinde kontrol sahibidir; veriler eksiksiz, tutarlı, zamanında, doğru ve kolayca dağıtılabilmekte, zincirde yapılan değişiklikler ağın tüm üyeleri tarafından görülebilmektedir (Esposito, 2018: 35). Blok zincirindeki varlıkların güvenliği de bir tür dijital kimlik olan özel anahtarın korunmasına bağlıdır. Eğer bir kişinin özel anahtarı ele geçirilir ya da çalınırsa, hiçbir üçüncü taraf bu anahtarı geri alamaz. Sonuç olarak, bu kişinin blok zincirinde sahip olduğu tüm varlıklar ortadan kaybolacaktır (Efanov ve Roschin, 2018: 119). Bu durum bir bakıma *merkeziyetsiz mantığın* bir sonucudur. Merkezi bir uygulamanın ya da organizasyonun varlığı, o sistem üzerindeki regülasyonu merkezi yönetime bırakmaktadır. Blok zinciri üzerine inşa edilen uygulamalarda ise varlığın (Kripto para, NFT- None-Fungible Token vb.) güvenliği, sistem tarafından yaratılan kriptografik anahtarların kullanıcı tarafından korunmasına bağlıdır. Ancak bu koruma yalnızca varlıklar için değil aynı zamanda kimlik ve veri gizliliği için de geçerlidir. Neticede kimlik bilgilerinin veya kişisel verilerin merkezi sunucularda depolanması demek, merkezi otoritenin tüm bunlar üzerinde hak iddia etmesi demektir. Diğer taraftan merkezi otorite, verilerin gizliliği ve güvenliğinden de sorumludur. Blok zincir tabanlı merkeziyetsiz uygulama ya da organizasyonlarda böyle bir sorumluluk (ağın geliştiricileri ve gönüllü kullanıcılar hariç) bulunmamaktadır. Bu nedenle blok zinciri sistemin gizliliği ve güvenliği daha da önemli hale gelmektedir. Blok zincir, merkezi sistemlere göre daha güvenli olarak görülsede sistem üzerindeki işlemler saldırıya uğrayabilmekte, kimlik veya veri gizliliği tehlikeye girebilmektedir.

Kimlik gizliliği ile ifade edilmek istenen, kullanıcının gerçek kimliği ile blok zinciri adresi arasındaki ilişkidir. Blok zincirindeki bilgiler değiştirilemez, zincir üzerinde dağıtılmış defter şeklinde saklanmaktadır ve herhangi bir düğüm zincirden tüm bilgileri elde edinilebilir. Blok zincirindeki işlemler belirli bir anonimliğe sahip olsa da hesaplama teknolojisinin gelişmesiyle birlikte anonimlik, kullanıcı kimliğinin gizliliğini tam olarak koruyamamaktadır. Kötü niyetli kişiler, global defterdeki herkese açık verilerin alaka düzeyini izleyerek ve analiz ederek hassas bilgileri bulabilir (Wang vd., 2020: 108767). İşlem gizliliği ise blok zincirinde saklanan işlem kayıtlarını ve işlemin arkasındaki potansiyel bilgileri ifade etmektedir.

Geleneksel bilgi koruma önlemi, bilgilerin şifrelenerek kötü niyetli kişilerin eline geçmesini veya tahrif edilmesini önlemekten ibarettir. Ancak, blok zincirinde işlem bilgilerinin şifrenmesi sürecinde, bir yandan işlem bilgilerinin yetkisiz düğümler tarafından çalınmamasını da sağlamak gerekmektedir. Öte yandan, hassas bilgileri ifşa etmeden işlemin gerçekliğini de doğrulamak gerekmektedir. Dolayısıyla işlem içeriği tamamen şifrelenemez. Tüm bunlar, gizliliği sağlamadaki güçlüklerdir. Özetle, blok zincir teknolojisi kullanıcıların

gizliliği için mutlak koruma sağlayamamaktadır (Wang vd., 2020: 108767). Bu nedenle gizliliği sağlamak için bazı ek algoritmik önlemler alınmaktadır. Bunlarda bazıları, Akıllı Sözleşmeler (Smart Contracts), Gizli Adresler (Stealth Address), Halka İmza (Ring Signature), Grup İmzaları (Group Signatures) ve Sıfır Bilgi Kanıtı (Zero-Knowledge Proof)'dır (University College London, 2016; Lee ve Song, 2021; Devidas vd., 2021).

Akıllı sözleşmeler, önceden tanımlanmış süreçlerin şeffaf bir şekilde yürütülmesini sağlayan blok zinciri veya benzer altyapılar üzerinde merkezi olmayan bir şekilde sabitlenmiş komut dosyalarıdır. Akıllı sözleşmeler kullanılarak iş mantığı otomatikleştirilebilir ve para gibi varlıklar programlanabilir hale gelmektedir. Bugüne kadar, akıllı sözleşmeler milyarlarca değeri kontrol etmektedir (Ante, 2021: 1). Bu sözleşmeler, kullanıcı verilerini kontrol etmek ve blok zincirdeki erişim haklarını izlemek gibi ek güvenlik özellikleri sağlayan, önceden tanımlanmış sözleşme politikasına sahip, kendi kendine çalışan bir programdır ve önceden tanımlanmış koşullar karşılandığında otonom olarak yürütülmektedir (Singh ve Kim, 2019: 136). Akıllı sözleşmeler, güvenli bir şekilde veri paylaşmayı ve şeffaflığı misyon edindiği için özellikle veri sahteciliğini önlemek için kullanılabilir (Lee ve Song, 2021: 158124).

Gizli adresler, blok zincirinde kullanıcıların gizliliğini koruyan ve anonim olmayı sağlayan için etkili bir teknolojidir (Fan vd., 2019: 1; Kovács ve Seres, 2023: 1). Blok zincirinde dağıtık defter teknolojisi kullanılır. Ancak, bu aynı zamanda ağdaki tüm düğümlerin defterde görünenlere erişimi olduğu anlamına gelir (Fan vd., 2019: 1). Gizli adresler, bir göndericinin varlıklarını alıcıya anonim bir şekilde etkileşimsiz olarak aktarmasına olanak tanımaktadır. Bu teknoloji, alıcının adresini gizli tutmakta ve böylelikle alıcı anonim kalmaktadır (Kovács ve Seres, 2023: 1). Grup imzaları da bir mesajı imzalayan bir grup üyesinin, kimlik gizliliğinin korunmasında hayati bir rol oynamaktadır. Bu nedenle merkezi grup yöneticileriyle ilgili güven sorunlarının üstesinden gelmek ve kullanıcı gizliliğini iyileştirmek için grup yöneticisinin rolünü merkezsizleştirerek, merkezi olmayan grup imzasının kullanılması önerilmektedir (Devidas, 2021: 353). Halka imzalar da bir işlemi gerçekleştiren kişinin anonim olmasını sağlamaktadır. Örneğin, bir e-postanın yalnızca hedef alıcı tarafından doğrulanabilecek şekilde imzalanmasını mümkün kılar. İmza, halka içinde bulunan diğer kullanıcıların imzaları sayesinde atan kişinin kimliğini gizler; bu durum, imzayı atan kişinin izlenememesi ve dolayısıyla kullanıcı gizliliğinin artması anlamına gelmektedir (Rivest vd., 2001: 553-554). Sıfır bilgi kanıtı sisteminde ise kanıtlayıcı, doğrulayıcıya herhangi bir geçerli bilgi sağlamadan doğrulayıcıyı bir mesajın doğru olduğuna inandırabilir. Sıfır bilgi kanıtı, esasen iki veya daha fazla tarafı içeren bir protokoldür, yani iki veya daha fazla tarafın bir görevi tamamlamak için atması gereken bir dizi adımdır (Wang vd., 2020:

108767). Sıfır bilgi kanıtı protokolü ise zk-SNARK olarak adlandırılır. Bu protokol, bir tarafın, yani kanıtlayıcının diğer tarafa, yani doğrulayıcıya, özel olarak tutulan bazı bilgiler hakkındaki bir beyanın, bilginin kendisini ifşa etmeden doğru olduğunu kanıtlamasına olanak tanımaktadır (Chen vd., 2022: 1) Neticede sıfır bilgi kanıtı teknolojisi kullanılarak blok zincirinin gizliliği önemli ölçüde artırılabilir. Bu doğrulama yöntemi, kanıtlanan mesajın başka hiçbir bilgisini ifşa etmemektedir. Dolayısıyla sıfır bilgi kanıtı, mesajları doğrulamak için kullanılabilirse birçok sorun etkili bir şekilde çözülebilecektir (Wang vd., 2020: 108769).

2.3.3. Merkezi Olmayan Organizasyonlar

Merkezi olmayan organizasyonlar (DAO- Decentralized Autonomous Organization), insanların halka açık bir blok zincirine yerleştirilen ve kendi kendini yürüten bir dizi kural aracılığıyla koordine olmalarını ve kendi kendilerini yönetmelerini sağlayan ve yönetişimi merkezi olmayan blok zinciri tabanlı bir sistemdir (Hassan ve De Filippi, 2021: 2). Son yıllarda, blok zincir teknolojisinin hızlı gelişimi, yönetim ve operasyonel kuralların tipik olarak belirlendiği yeni bir organizasyon biçimi olan merkezi olmayan otonom organizasyonun -bazen merkezi olmayan otonom şirket (DAC- Decentralized Autonomous Cooperative) olarak da adlandırılır- ortaya çıkmasına neden olmuştur (Wang vd., 2019: 870). DAO'lar, günümüzün geleneksel tüzel kişilikleri ve diğer iş birliklerinin çoğundan farklı varsayımlarla çalışmaktadır. DAO'lar kurullar ya da yöneticiler tarafından yönetilmemekte, bunun yerine demokratik ya da yüksek katılımlı süreçler ya da algoritmalarla yönetilmeyi amaçlamaktadır. DAO'lar fiziksel konumları, geçmişleri ya da inançları ne olursa olsun binlerce, hatta on binlerce ya da yüz binlerce üyeyi bir araya getirerek tüm dünyaya yayılmaya çalışırlar (Wright, 2021: 2). DAO'ların blok zinciri tabanlı doğasının, DAO'ları geleneksel organizasyonlardan ayıran bazı özellikleri varır. Birincisi örgütsel yönetişim, örgütlerdeki, daha geleneksel yönetişim biçimlerinden önemli ölçüde farklıdır. Geleneksel organizasyonlar yukarıdan aşağıya, özel ve merkezi karar alma mekanizmasıyla yönlendirilirken, DAO'lar herhangi bir DAO üyesinin genellikle her tür kurumsal karar için teklif sunabildiği ve bunlara oy verebileceği kamusal ve dağıtılmış karar alma yoluyla çalışmaktadır. Bu çerçevede, DAO'nun ortak hedefleri ve idealleri paylaşan tüm üyeleri arasında iş birliğini ve topluluk katılımını kolaylaştırmaktadır (Bellavitis vd., 2023: 188). DAO'ların hiyerarşik bir yapısı yoktur ve konuşlandırıldıktan sonra yaratıcısından bağımsızdır. Tek bir varlık tarafından sansürlenemez, ancak önceden tanımlanmış bir çoğunluk tarafından sansürlenebilir. Bu çoğunluk kuralları, fikir birliği protokolünde veya akıllı sözleşmede belirlenir ve kullanım senaryosuna bağlı olarak değişebilir. Örneğin, bazı

ülkeler, Avusturya gibi, hukuk literatüründe DAO'ları medeni hukuk ortaklığı olarak değerlendirmeye eğilimlidir (Blockchainhub, 2019)

DAO'ların önemi giderek artmaktadır ve blok zinciri tabanlı yönetişimin hem geleneksel yönetim mekanizmalarını dijitalleştirerek hem de ticari işletmeleri organize etmenin temelde yeni yollarını sunarak firmaların yönetilme şekli üzerinde önemli bir etkiye sahip olacağına dair erken aşama göstergeler bulunmaktadır (Wright, 2021: 175). DAO'lar açık kaynaklıdır, dolayısıyla şeffaftır ve teorik olarak bozulmaz. Kuruluşun tüm işlemleri bir blok zinciri üzerinde kaydedilir ve muhafaza edilir (Blockchainhub, 2019). Blok zinciri üzerinde akıllı sözleşmeler şeklinde kodlanır ve merkezi kontrol veya üçüncü taraf müdahalesi olmadan otonom olarak çalışabilir. DAO'lar ayrıca bireylerin anonimliklerini ya da takma adlarını koruyarak hızlı ve güvenli bir şekilde organize olmaları, fon toplamaları ve kendilerini yönetmeleri için fırsatlar yaratır. Bu avantajlar DAO'ların yeni nesil çevrimiçi topluluklar ve forumlar haline gelmesine neden olabilir. Bugüne kadar birçok DAO, Web3 uygulamalarının geliştirilmesi ve yönetilmesine yönelik ortak bir ilgi temelinde kurulmuştur (Murray vd., 2023: 197). Bu organizasyonların geleneksel hiyerarşik yönetim modelini tersine çevirmesi ve kuruluşların iletişim, yönetim ve iş birliği maliyetlerini önemli ölçüde azaltması beklenmektedir. Ancak bu organizasyonlar, hala güvenlik ve gizlilik sorunu, belirsiz yasal durum vb. gibi birçok zorlukla karşı karşıyadır (Wang vd., 2019: 870).

2.3.4. Merkezi Olmayan Uygulamalar

Merkezi olmayan bir uygulama (DApp- Decentralized Application), merkezi olmayan bir ağ üzerinden²⁶ birden fazla kullanıcı tarafından yürütülen bir uygulamayı ifade etmektedir. Son yıllarda, özellikle blok zinciri teknolojisinin popüleritesiyle, hızla geliştirilmeye başlanan DApp'ler, yaygın olarak benimsenmiş ve uygulama pazarı milyarlarca dolarlık ve milyonlarca kullanıcıyla bir pazar haline gelmiştir (Wu, 2019: 1; Wu vd., 2021: 2033). Aynı şekilde blok zinciri kullanımının benimsenmesini teşvik edeceği varsayılan bir uygulama türü olan merkezi olmayan uygulamaların artan önemine rağmen, bu uygulamaların pratikte nasıl ve ne kadar iyi kullanıldığı hakkında çok az şey bilinmektedir (Wu, 2019: 1).

Merkezi olmayan uygulamalar, blok zincir gibi dağıtılmış bir bilgi işlem sisteminde çalışan yazılımlardır. Çoğu internet uygulamasına güç veren istemci ve sunucu mimarisinin aksine, blok zincire entegre olan uygulamalar şeffaf, doğrulanabilir ve değişmez olduğu garanti edilen uygulama mantığını yürütebilir (Johnson vd., 2019: 1). Bu uygulamalar, mobil

²⁶ Örneğin Ethereum, akıllı sözleşmeler ve merkezi olmayan uygulamalar oluşturma ve çalıştırma imkânı sağlayan özel bir blok zinciri tabanlı yazılım platformudur (Rouhani ve Deters, 2017).

merkezi uygulamalar gibi istemcilere, sunuculara sahip olabilirler, ancak temel veriler ve işlemler blok zincirindeki akıllı sözleşmelerde tutulmaktadır (Wu, 2019: 2). Buradaki mantık, eşler arası bilgisayar ağında çalışmasıdır. Örneğin, dosya paylaşımı için BitTorrent, anlık mesajlaşma için BitMessage ve video akışı için Popcorn Time gibi birçok ünlü uygulama geliştirilmiş ve geniş çapta yayılmıştır (Wu vd., 2021: 2033). Blok zinciri tabanlı merkezi olmayan uygulamalar, blok zinciri teknolojilerinin giderek gelişmesi ve geniş uygulama alanı bulmasıyla birlikte daha fazla dikkat çekmektedir. Ağustos 2022 itibarıyla günlük 1,67 milyondan fazla benzersiz aktif cüzdan (kullanıcı) ile 5.000’den fazla DApp bulunmaktadır (Zheng vd., 2023: 121). Virtue Market Research (2023)’ün araştırmasına göre merkezi DApp pazarı, 2022 yılında 25,63 milyar dolardır ve 2030 yılına kadar yüzde 56,1’lik bir büyüme oranıyla 70,82 milyar dolara ulaşacağı tahmin edilmektedir. Geleneksel uygulamalardan farklı olarak, uygulamaları dağıtmak için Play Store/App Store gibi merkezi bir uygulama mağazası bulunmamaktadır. Bununla birlikte, DApp’ler hakkında bilgi veren ve kategorilere ayıran “DAppRadar” gibi bazı DApp mağazaları vardır (Zheng vd., 2023: 124).

DApp’ler anonim olarak kabul edilebilir çünkü blok zincir teknolojisi doğal olarak anonimdir. Yani bir şekilde DApp’ler kullanıcıların mahremiyetini koruyabilir (Zheng vd., 2023: 126). DApp’ler ayrıca veri manipülasyonunu, dolandırıcılık risklerini ve araçlara olan bağımlılığı azaltabilir; merkezi olmayan ve değişmez bir işlem defteri sağlayarak paydaşlar arasında güveni teşvik edebilir (Akhil, vd., 2023: 348-351). Araştırmalarda veri gizliliği genellikle güvenilir bir üçüncü tarafça yönetilse de bu merkezi yaklaşımın yetersiz kaldığı önemli alanlar vardır. Katılımcılar, verilerini uygun şekilde kullanmaları için üçüncü taraflara/araştırmacılara güvenmek zorundadır. Aynı zamanda verilerinin, verileri kötüye kullanabilecek diğer kişilere karşı korunduğuna ve güvende olduğuna da güvenmelidir. Blok zinciri, veri yönetimi ve uygulama mantığı için güvenilir bir üçüncü tarafa dayanmayan alternatif bir yöntem sunduğundan, merkeziyetsiz veri gizliliğini korumak için alternatif bir yöntem olarak keşfedilebileceği bir fırsat vardır (Johnson vd., 2019: 10). Bununla birlikte, sistemin bazı sınırlamalarını ve potansiyel dezavantajlarını kabul etmek önemlidir (Akhil, vd., 2023: 348-351). Örneğin geliştiricilerin, DApp’lerin yazılım mühendisliği sürecinin birçok aşamasında karşılaştığı pek çok zorluk vardır. Kritik aşama, geleneksel merkezi uygulamalarla karşılaştırıldığında DApp bakımındır (Samreen ve Alalfi, 2023: 2). Örneğin düşük verim alınan veya güvenlik açığı fark edilen bir uygulama, hızlı bir şekilde güncellenememektedir. Bu da ciddi problemlere yol açabilir. Bir başka dezavantaj da yasaların ihlal edilebilme ihtimalidir. Örneğin Monero, kişilerin, hükümetin sansürüne rağmen para transfer etmelerini sağlamaktadır. Bu aynı zamanda potansiyel suçluların para

elde etmesine yardımcı olacaktır. Bu nedenle DApp'lerde hukuk ve mahremiyet arasında bir denge kurmak zor olduğu gibi denetim de eksiktir. Diğer bir zorluk da gizli işlem oluşturmak için kullanılan algoritmalar, her zaman çok fazla bilgi işlem kaynağı tüketmektedir (Zheng vd., 2023: 126). Blok zinciri tabanlı ürünlere yöneltilen en büyük eleştirilerden biri de enerji tüketimidir. Bu sistemin çalışabilmesi için, her düğümün ağı katılması ve işlemleri onaylaması için belli bir donanım ve elektrik enerjisi gereklidir. Bazı araştırmacılar ise merkezi ve merkezi olmayan sistemler arasındaki tartışmanın büyük ölçüde önyargılı olduğuna inanmaktadır. Bu sistemlerin hiçbirinin makul düzeyde bir gizlilik koruması sunmadığını, bazı hibrit yöntemlerin kullanılarak iki dünyanın en iyisini elde etmek için daha fazla çalışmaya ihtiyaç olduğunu dile getirmektedir (Vaudenay, 2020: 29). Ayrıca merkezi sistemlerde hâlihazırda var olan denetim veya yasal uygulamalar ne ölçüde yeterli olduğu tartışmalıdır. Kaynak tüketiminde de blok zinciri aratmayacak düzeyde algoritma ve yapay zekâ kullanılmaya devam edilmektedir. Özellikle yapay zekâ gün geçtikçe çok daha fazla ekran kartı ve bilgisayar işlemcisi (GPU- Graphics Processing Unit veya CPU- Central Process Unit) kullanmakta, enerji tüketimi giderek daha fazla artmaktadır. Neticede iki yöntemin de verimli yönlerini kullanarak daha çevreci, daha verimli, yasal, denetlenebilir gizliliğe ve güvenliğe önem veren yapıların oluşturulması gerekliliği giderek gün yüzüne çıkmaktadır.

ÜÇÜNCÜ BÖLÜM

VERİ SÖMÜRGEÇİLİĞİ VE VERİ GÖZETİMİ EKSENİNDE BAĞIMSIZ MOBİL UYGULAMA GELİŞTİRİCİLERİNE YÖNELİK SAHA ÇALIŞMASI

3.1. Araştırmanın Yöntemi

Tezin giriş bölümünde de belirtildiği gibi bu araştırmada, bağımsız mobil uygulama geliştiricilerinin veri sömürgeçiliği ve veri gözetimine karşı bir direniş gösterip göstermediğini anlamak ve olası karşı-gözetim hamlelerini ortaya çıkarmak için nitel bir yaklaşım kullanılmıştır. Geliştiricilerin görüşlerinden ve ilgili literatürden yola çıkarak kavram haritaları (MAXMaps)²⁷ çıkarılmış; derinlemesine görüşmelerle toplanan veriler, *tematik analiz* kullanılarak analiz edilmiştir. Tematik analizi desteklemek için Apple ve Google’ın Gizlilik Politikaları *doküman analiziyle* incelenmiştir. Bu veri toplama yöntemlerine ek olarak topluluk gözlemleri de araştırmaya eklenmiştir. Çalışmada, *kuram çeşitlemesinin* yanı sıra *veri çeşitlemesi*²⁸ de kullanılmış, farklı veri kaynaklarından yararlanılmıştır. Ayrıca *akran değerlendirmesi* ve *katılımcı teyidi* ile araştırmanın geçerliği ve güvenilirliği artırılmıştır.

Birçok meslek grubunda olduğu gibi mobil uygulama geliştiricileri de internette çeşitli ağlar oluşturarak, diğer geliştiricilerle ya da yayıncılarla iletişim kurmakta, kaynak/bilgi paylaşımında bulunmakta ya da iş birliği içerisine girebilmektedir. Ağ oluşturma, giderek bağımsız geliştiricilerin yazılım geliştirme ve yayınlama hedeflerine ulaşmalarını kolaylaştıran önemli unsur haline gelmektedir (Wu, 2017: 31). Öte yandan çevrimiçi forumlar, kullanıcıların farklı konular hakkında soru ve yorum gönderebilecekleri zengin ortamlar sağlamaktadır. Forumlara benzer şekilde belirli bir konu etrafında oluşturulan topluluklar da kullanıcılar için oldukça verimli olabilmektedir. Kişilerin çevrimiçi forum/topluluklarda nasıl davrandığını anlamak, bir grup bireyde kolektif düşüncenin ortaya

²⁷ MAXMaps, belgeleri, notları ve kodları, görsel bir çalışma alanında temsil etmek ve bu unsurları birbirleriyle ilişkilendirmek amacıyla tasarlanmış bir araçtır. MAXMaps, araştırmacılara kodlar arasında karmaşık ilişkileri daha anlaşılır bir şekilde görselleştirmelerini ve analiz etmelerini sağlar (MAXQDA, t.y). <https://www.maxqda.com/help-mx24/maxmaps/what-does-maxmaps-do> (erişim tarihi: 24.09.2023).

²⁸ “... *veri çeşitlemesi*, farklı zamanlarda, yerlerde ve kişilerde incelenen farklı veri kaynaklarının birleşimini ifade eder. *Teori çeşitlemesi*, ‘verilere çoklu bakış açıları ve hipotezler göz önünde bulundurularak yaklaşma’ anlamına gelir” (Denzin 1970, 1978’den akt. Flick, 2021: 455). “Farklı yöntemlerle (görüşme, gözlem ve doküman analizi gibi) elde edilen verilerin birbirlerini teyit amacıyla kullanılması, ulaşılan sonuçların geçerliliğini ve güvenilirliğini artırır” (Yıldırım ve Şimşek, 2016: 279).

çıkacağı temel mekanizmalara ışık tutabilir, kullanıcı deneyimini geliştirebilecek önemli uygulamalara da sahip olabilir (Medvedev vd., 2018: 183). Ayrıca James C. Scott (2021: 22), “İdeolojik direniş en iyi, doğrudan gözetimden korunduğu zaman gelişebildiği için, bu direnişin filizlenebileceği toplumsal mekânları incelememiz gerekiyor” demiştir. Dolayısıyla geliştiricileri anlamanın ve anlamlandırmanın en iyi yolu, onları kendi ortamlarında gözlemlemekten, onlarla aynı havayı solumaktan geçmektedir. Buradan hareketle çeşitli geliştirici topluluklarına internet ortamında dâhil olunmuş, konuyla ilgili yazışmaları üzerinden veri gözetimine karşı direniş kültürü oluşturup oluşturmadıkları ve gözetime mukavemet biçimleri konusunda bilgi edinilmeye çalışılmıştır. Araştırmanın çalışma grubu, geliştiricilerin sıklıkla kullandığı ve bilgi alışverişinde bulundukları Discord Platformu “Ünög Geliştirici Topluluğu” sunucusunda; Slack platformu “NSİstanbul” kanalında ve X’te “iOS Development TR” ve “Android Türkiye” topluluğunda, profilinde “developer” ibaresi geçen kişiler arasından belirlenmiştir. Araştırmanın temsil çeşitliliğini artırabilmek amacıyla, katılımcılar farklı platformlardaki topluluklar arasından seçilmiştir. Platformlar, ilgi alanları nedeniyle birbirinden farklılaşmaktadır: Örneğin Discord, daha fazla oyuncuların tercih ettiği topluluklara sahipken, X daha çok uygulamalara odaklanan geliştiricilerin yer aldığı toplulukları barındırmaktadır. Slack ise daha çok profesyonel iş platformu olarak bilinmekte, oyunculara kıyasla uygulama geliştiricilerinin bilgi alışverişinde bulunduğu topluluklara ev sahipliği yapmaktadır. Topluluklar aracılığıyla belirlenen profiller taranarak, iOS ve Android geliştiriciler haricindeki geliştiriciler ve platformu belirsiz olan geliştiriciler elenmiştir. Bu tarama sonrasında 54 geliştirici ile direkt mesaj ve topluluk gönderileri yoluyla iletişime geçilmiş ve bunlardan 11’i derinlemesine görüşme talebini kabul etmiştir. Yedinci görüşmeden sonra veri doygunluğuna ulaşıldığı görülse de doygunluk noktasının netleştirilmesi amacıyla geri kalan dört katılımcıyla görüşülmeye devam edilmiş ve böylece toplam 11 katılımcıyla görüşme gerçekleştirilmiştir.

Katılımcılar, ortalama yedi yılın üzerinde yazılım deneyimi olan, alanında uzman olarak değerlendirilebilecek Android ve iOS geliştiricilerden oluşmaktadır. Katılımcıların çoğu kendini tanımlayabilecek verilerin paylaşılmasını kabul etmediğinden demografik bazı bilgilere yer verilememiştir. Bunlardan bazıları yaş (18 yaşından büyük oldukları teyit edilmiştir), eğitim durumu ve gelir bilgileridir. Örneğin ortalama gelirleri sorulduğunda yıllık ortalama kazançlarının çoğunlukla değişkenlik gösterdiği ifadeleriyle karşılaşmış, gelir durumlarının belirsiz olduğu anlaşılmıştır. Öte yandan katılımcıların aldıkları eğitimin yaptıkları iş üzerinde belirleyici olmadığı yönündeki düşünceleri, konuşmaların seyrinden anlaşılmış, saha çalışması kısmında katılımcıların perspektifine odaklanılması nedeniyle bu

konularda bilgi alma çabasında ısrarcı olunmamıştır. Katılımcıların tümü erkektir. Katılımcılar belirlenirken, cinsiyet eşitliğinin sağlanması adına profiller incelenerek, kadın geliştiricilerle de iletişim kurulmaya çalışılmış, ancak bu girişim olumsuz sonuçlanmıştır. Katılımcıların vermiş olduğu bilgilerden ve literatürde yer alan bağımsız geliştirici tanımlamalarından yararlanılarak katılımcıların organizasyon tipi/çalışma durumları da kategorilendirilmiştir.

Tablo 3.1 Katılımcıların Kodlama ve Profil Tablosu

<i>Kodlama</i>	<i>Platform</i>	<i>Mobil Yazılım Türü</i>	<i>Yazılım Deneyimi-Yıl</i>	<i>Organizasyon Türü</i>
1	Android	Uygulama	4	Serbest Çalışan*
2	iOS/Android	Oyun	8	Ücretli Çalışan**
3	iOS	Uygulama/Oyun	7	Kurucu Ortak***
4	iOS/Android	Uygulama/Oyun	9	Ücretli Çalışan
5	iOS	Uygulama	8	Ücretli Çalışan
6	Android	Uygulama	8	Serbest Çalışan
7	iOS/Android	Uygulama	11	Serbest Çalışan
8	iOS	Uygulama	5	Serbest Çalışan
9	iOS/Android	Oyun	10	Ücretli Çalışan
10	iOS/Android	Uygulama	13	Kurucu Ortak
11	Android	Uygulama	9	Serbest Çalışan

* Bir yazılım şirketinde ücretli olarak çalışmayan geliştiriciler.

** Uluslararası olmayan bir yazılım şirketinde (yerel) ücretli olarak çalışan geliştiriciler.

*** Uluslararası olmayan bir yazılım şirketinde (start-up) yazılımcı ekibin üyesi olan geliştiriciler.

3.1.1. Görüşme Protokolü

Derinlemesine görüşme öncesinde; gözlem aşamasında belirlenen araştırma soruları rehberliğinde oluşturulan çalışma odakları ve alt odaklara paralel olarak hazırlanan görüşme

soruları, katılımcı protokolü²⁹ haline getirilerek aşağıdaki tabloda verilmiştir:

Tablo 3.2 Derinlemesine Görüşme Protokolü

Araştırma Odağı	Alt Odak	Görüşme Soruları
Veri Toplama ve Veri Sömürgeciliği Süreci	Verilerin önemi ve geleceği Veri toplama süreçleri Veriler üzerinde istilacı şirketlerin rolü	Veri, kişisel verilerin önemi ve geleceği hakkında söyleyecekleriniz nelerdir? Şirketlerin kişisel veri elde etme süreçlerini açıklar mısınız? Uygulama mağazalarında tekelleşen şirketler hakkındaki düşünceleriniz nelerdir?
Mobil Uygulamalarda Gizlilik, Veri Gözetimi ve Güvenlik	Mobil uygulamalardaki gözetim mekanizmaları İşletim sistemlerine göre veri toplama ve veri ihlalleri İstilacı şirketlerin veri politikaları	Mobil uygulamalarda dijital gözetim ve veri gözetiminin nasıl işlediğini geliştirici gözüyle açıklar mısınız? Android ve iOS işletim sistemlerini karşılaştırsanız, veri toplama hangi işletim sisteminde daha kolay gerçekleştirilebilir? Apple, kullanıcıların gizliliğini sağladığını iddia eden reklamlar yayınlıyor sizce de kullanıcı mahremiyetini koruyabilir mi? Apple'ın veri izleme politikası nasıl işliyor? Android uygulama gizliliği ve güvenliği hakkındaki düşünceleriniz nelerdir?

²⁹ Protokol, daha önce yapılmış herhangi bir çalışmadan alınmamış, odaklar, alt odaklar ve görüşme soruları tarafımızca oluşturulmuştur.

	Gizlilik ve güvenlik ilişkisi Geliştiricilerin veri konusundaki hassasiyetleri Merkezi olmayan uygulamalar ve gizlilik	Bağımsız geliştirici olarak mobil uygulama geliştirme/yayınla ma sürecinde kişisel verilerin güvenliğine ilişkin hassasiyetiniz nelerdir? Daha güvenli bir uygulama deneyimi için neler yapılabilir? Web 3.0 hakkında düşünceleriniz nedir? Blok zinciri ile kişisel veriler korunabilir mi? Merkezi olmayan uygulamalar (DApps) ve merkezi olmayan organizasyonlar (DAO) hakkında söylemek istedikleriniz nelerdir? Merkezi olmayan uygulamalar, merkezi uygulamaların hâkimiyetine son verebilir mi?
Gözetimden Kaçınma ve Gizlilik Stratejileri	Geliştiricilerin gizlilik kaygıları Karşı-gözetim stratejileri ve gözetim hamleleri Gözetimden ve veri sömürsünden kaçınma yolları	Mobil uygulama kullanırken kendinizi gizleme ihtiyacı duyuyor musunuz? Mobil uygulamalardaki veri gözetiminde, çeşitli yazılım (çerez, eklenti vb.) ve algoritmalar kullanılmaktadır. Bu yazılım ve algoritmaları yanıltmanın bir yolu var mı? Mobil uygulamalardaki veri gözetim mekanizmaları, herhangi bir ek yazılımla ya da bir müdahale ile (kod ya da eklenti gibi) engellenebilir mi? Gözetimden kaçınma/korunma stratejileriniz var mı? Kullanıcılar gözetimden kaçınmak için hangi yolları izlemeli?

3.1.2. Veri Toplama ve Analiz Süreci

Veriler, çevrimiçi yarı yapılandırılmış video görüşmelerle 01/02/2023-23/06/2023 tarihleri arasında toplanmıştır³⁰. Katılımcılara çalışmanın amacı hakkında bilgi verilmiş ve her katılımcıdan açık rızası alınmıştır. Katılımcılar, 18 yaşından büyük olduklarını teyit etmişlerdir. Katılımcılara görüşme protokolüne göre sorular yöneltilmiş, görüşmeler 45-60 dakika arası sürmüştür. Görüşmeler boyunca analitik notlar alınarak tematik analiz için ön bilgiler elde edilmiştir. Görüşme kayıtları deşifre edilmiş ve görüşme başı 3000-5000 kelime arasında veri elde edilmiştir. Ayrıca doküman analizi için Apple ve Google'ın internet sitesinde yer alan gizlilik politikaları, "MAXQDA Web Collector" kullanılarak taranmış ve 9358 kelimelik veri elde edilmiştir.

Görüşmelerden toplanan veriler, "tematik analiz" kullanılarak analiz edilmiştir. Veri seti MAXQDA 20 nitel veri analizi programına aktararak kod oluşturma aşamasına geçilmiş, her bir görüşme metni okunarak önemli olduğuna karar verilen kelime ve paragraflara kodlar atanmıştır. Ayrıca doküman analiziyle Apple ve Google'ın Gizlilik Politikalarından elde edilen veriler MAXQDA 20 nitel veri analizi programına aktararak analiz edilmiştir. Temalar, tümevarımcı bir yaklaşımla, görüşmeler esnasında tutulan analitik notlar ve doküman analizi yardımıyla keşfedilmiştir. İlişkili kodlar temalar halinde gruplandırılmış, dört kapsayıcı kategori altında konumlandırılmış ve rapor haline getirilmiştir.

3.1.3. Araştırmanın Kısıtları

Araştırma sırasında yapılan alan gözlemleri doğrultusunda toplumsal cinsiyet eşitsizliğinin yazılım alanında da yoğun olarak var olduğu görülmüştür. Kadın geliştiriciler, seyrek de olsa topluluklarda yer almaktadır; ancak kadın yazılımcılardan derinlemesine görüşmeye katılım talebine olumlu yanıt alınamamıştır. Bu durum, çalışma için toplumsal cinsiyet eşitliği açısından bir kısıttır. Öte yandan çalışma, yapay zekâ konusundaki farkındalığı yansıtmakla birlikte, temel aldığı tarihsel süreç ve tezin sorunsalı kapması nedeniyle tezde merkezi bir konuma oturtulmamıştır. Dijital teknolojilerin oldukça hızlı dönüşüm geçirdiği zamanlara denk düşen araştırma tasarımı sürecinde, yapay zekâya ilişkin konuların görece daha az sıklıkta görünür olması da bu durumun gerekçelerinden birisidir. Yine de gerek görüşmeci ifadeleri gerekse hızla yenilenen literatür desteği ile, teze konu olan araştırma alanındaki dinamizmle uyumlu hareket etmeye çalışılmıştır.

³⁰ Araştırma öncesinde Akdeniz Üniversitesi Bilimsel Araştırma ve Yayın Etiği Kurulu'ndan Etik Kurul Onayı (25.01.2023 tarih ve 47-3 sayılı karar) alınmıştır.

3.1.4. Araştırma Soruları

Aşağıda belirtilen araştırma soruları, görüşülen bağımsız geliştiricilerin ifadeleri doğrultusunda araştırmanın veri toplama ve veri analizi sürecinde yol gösterici olmuş, araştırma boyunca bu sorulara yanıt aranmıştır.

- 1- Bağımsız mobil uygulama geliştiricilerinin dijital gözetim, veri gözetimi ve veri sömürüsüne yönelik yaklaşımları nasıldır?
- 2- Bağımsız mobil uygulama geliştiricilerinin uygulama geliştirme/yayınlama aşamalarında veri mahremiyeti ve gizliliği konusundaki hassasiyetleri nasıldır?
- 3- Bağımsız mobil uygulama geliştiricilerinin kişisel mahremiyetlerine ilişkin kaygı durumlarını ifade etme biçimleri nasıldır?
- 4- Bağımsız mobil uygulama geliştiricilerinin gözetime tepki ve karşı-gözetim hamleleri nasıldır?
- 5- Bağımsız mobil uygulama geliştiricilerinin uygulama kullanım tercihleri nasıldır ve güvenli bir uygulama deneyimi için nasıl bir strateji izlenmelidir?

3.2. Araştırmanın Bulguları

Çevrimiçi topluluklarda çokça vakit geçiren bağımsız geliştiriciler, genellikle yazılımla ilgili konular çerçevesinde diğer yazılımcılarla bilgi alışverişinde bulunmaktadır. Tezin birinci bölümünde de belirtildiği gibi, Netnografik yöntemle bağımsız geliştiricilerden bireysel olarak araştırma kapsamında yeteri kadar veri elde edilemeyeceği anlaşılmıştır. Geliştiricilerin, veri gözetimi ve veri sömürgeciliği gibi konuları topluluğun genel sohbet/kanal kısmında konuşma eğiliminde olmadıkları, bu konularla ilgili gönderilere de çoğunlukla cevap vermedikleri tespit edilmiştir. Bu nedenle topluluklar, geliştiricilerle iletişim kurmak için kullanılmış, veri toplama odağı derinlemesine görüşmelere yoğunlaştırılmıştır. Bağımsız geliştiricilerle yapılan görüşmeler sonucunda tüm katılımcıların, veri hakkında yeteri kadar bilgi sahibi olduğu, veri ihlali, veri sızıntısı ve veri istismarı gibi veri kaynaklı sorunlara ve mobil uygulamalardaki gözetim mekanizmalarına hâkim oldukları anlaşılmıştır. Buradan hareketle geliştiricilerin, gözetime tepki verip vermediklerini ve karşı-gözetim hamlelerinin olup olmadığı araştırılmış, veri gözetimine karşı direniş kültürü geliştirip geliştirmedikleri ortaya çıkarılmaya çalışılmış, bulgular ilgili literatür ışığında yorumlanmıştır.

3.2.1. Saha Gözlemleri

Derinlemesine görüşmeler gerçekleştirilmeden önce ve görüşmeler sırasında, söz konusu toplulukların sohbet odası niteliğindeki alanlara iletilen sorular aracılığıyla katılımcı gözlem yürütülmüştür, alınan yanıtlar çalışmanın önemli kavramsal odaklarından biri olan bağımsız geliştiricilerin bağımsızlığı tartışması yürütülmesi noktasında destekleyici veri olarak kullanılmıştır. Bu noktada Türkiye’de yazılım sektörünün son yıllarda oldukça ivme kazanan bir sektör olduğu ve gelişime oldukça açık karakteriyle bağımsız geliştiricilerin de kendilerine zemin bulduğu yönündeki ifadeler yol gösterici olmuştur. Dünya çapında mobil uygulamalara olan ilginin artışına paralel olarak ülkemizde de mobil uygulamalara olan ilginin -özellikle mobil oyunlara- gün geçtikçe arttığı ifade edilmiştir. Topluluklarda uygulama geliştiricilerle yapılan yazışmalarda, bu alandaki gelişmelerin rüzgarını değerlendirmeye hevesli geliştiriciler bulunsa bile Türkiye’nin halen mobil uygulama sektöründe tüketici konumunda bulunduğu, yazılım konusunda gelişmiş ülkelere kıyasla mobil uygulama geliştirme ve mobil yazılım yatırımları açısından gerilerde kaldığı ifade edilmiştir. Mobil uygulama pazarına Amerika Birleşik Devletleri hâkim olsa da mobil uygulama geliştirmede Çin, Hindistan ve Filipinler gibi ülkelerin giderek ağırlıklarını hissettirdikleri dile getirilmiştir. Ayrıca Orta Avrupa ülkelerinin, özellikle Polonya ve Ukrayna’nın giderek uygulama geliştirmede söz sahibi oldukları da ileri sürülmüştür. Geliştiricilerin büyük bölümü, bu ülkelerin bilgisayar teknolojilerine olan yatırımları ve bu alandaki eğitime verilen önem sayesinde yazılım sektöründe söz sahibi olduklarını vurgulamışlardır.

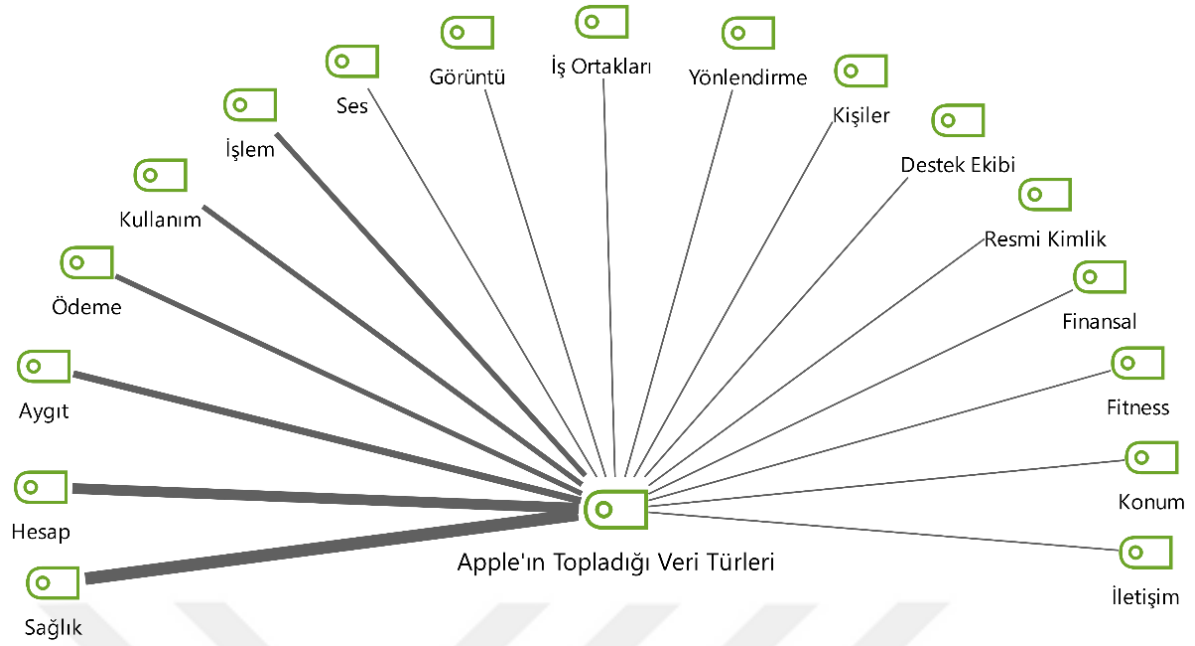
Topluluk gözlemlerine göre geliştiriciler, genellikle yazılımlarla ilgili bilgi alışverişinde bulunmak, ağ oluşturmak ve topluluk etkinliklerinden haberdar olmak için bu ortamlarda yer almaktadır. Geliştiriciler, çeşitli yazılım dillerine hâkim olmaları nedeniyle aslında ortak bir dil konuşmaktadır. Yazılım dünyasının vatandaşları olarak değerlendirebileceğimiz geliştiriciler, topluluklara ait kültürleri de paylaşmaktadır. Örneğin bazı topluluklarda iş birliği, dayanışma ve katkı kültürünün oldukça yerleşik olduğu anlaşılmaktadır. Öte yandan geliştiricilerin deneyimlerini toplulukla paylaşması da dikkat çeken bir başka önemli konudur. Topluluklar, geliştiricilerin yazılım konularında kendilerini geliştirmeleri ve teknik becerilerini iyileştirmeleri için fırsatlar sunarken aynı zamanda sosyalleşmelerini -yüz yüze olan etkinliklere de katılmaktadırlar- de sağlayabilmektedir.

3.2.2. Apple ve Google’ın Gizlilik Politikası Belgelerine İlişkin Doküman Analizi

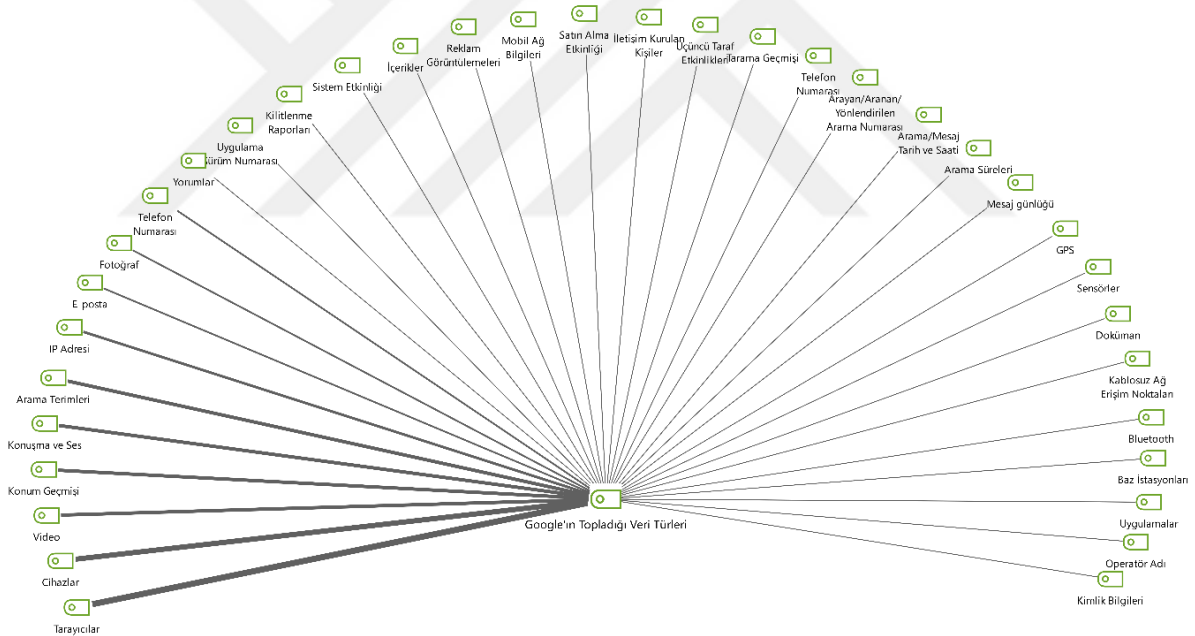
Doküman analizi, çeşitli dokümanların incelenmesi ve sistematik hale getirilerek anlamlandırılmasıdır. Bu bağlamda tezin başından itibaren irdelenen, mobil uygulama ekolojisinin baş aktörleri olan Apple ve Google’ın Gizlilik Politikaları, sık kullanılan kavramların neler olduğu ve söz konusu kavramların kullanım sıklıkları katılımcı ifadelerini birlikte değerlendirmek amacıyla MAXQDA 2020 nitel veri analizi programıyla analiz edilmiştir. Google Gizlilik Politikasından 6159, Apple Gizlilik Politikasından 3199 kelimelik veri elde edilmiş, veriler “Kişisel Veri”, “Veri Toplama Teknolojileri” ve “Yasal Yükümlülükler” kategorileri altında incelenmiştir. Bu kategorilendirme, belgelerin sistematik hale getirilmesi sırasında şirketler tarafından en fazla dikkat çekilen başlıkların tespit edilmesiyle belirlenmiştir. Daha sonra veri setine ait veriler grafikler ve şekillerle görselleştirilmiş, kavram haritalarıyla kavramlar arasındaki ilişkiler ve bağlar analiz edilmiştir.



Grafik 3.1 Apple Gizlilik Politikası - Kelime Bulutu



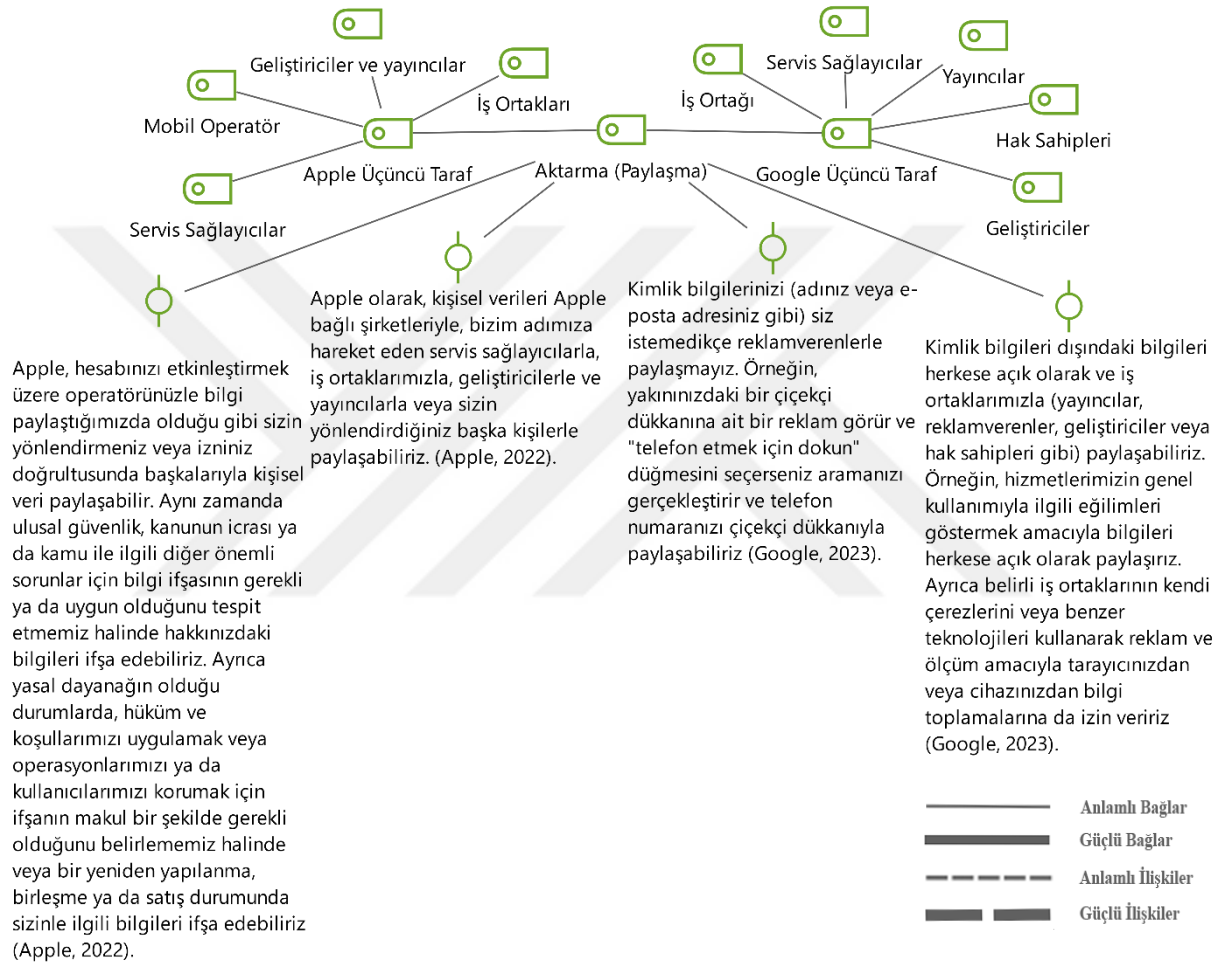
Şekil 3.1 Apple'ın Topladığı Veri Türleri - Hiyerarşik Kod-Alt Kod Modeli



Şekil 3.2 Google'ın Topladığı Veri Türleri - Hiyerarşik Kod-Alt Kod Modeli

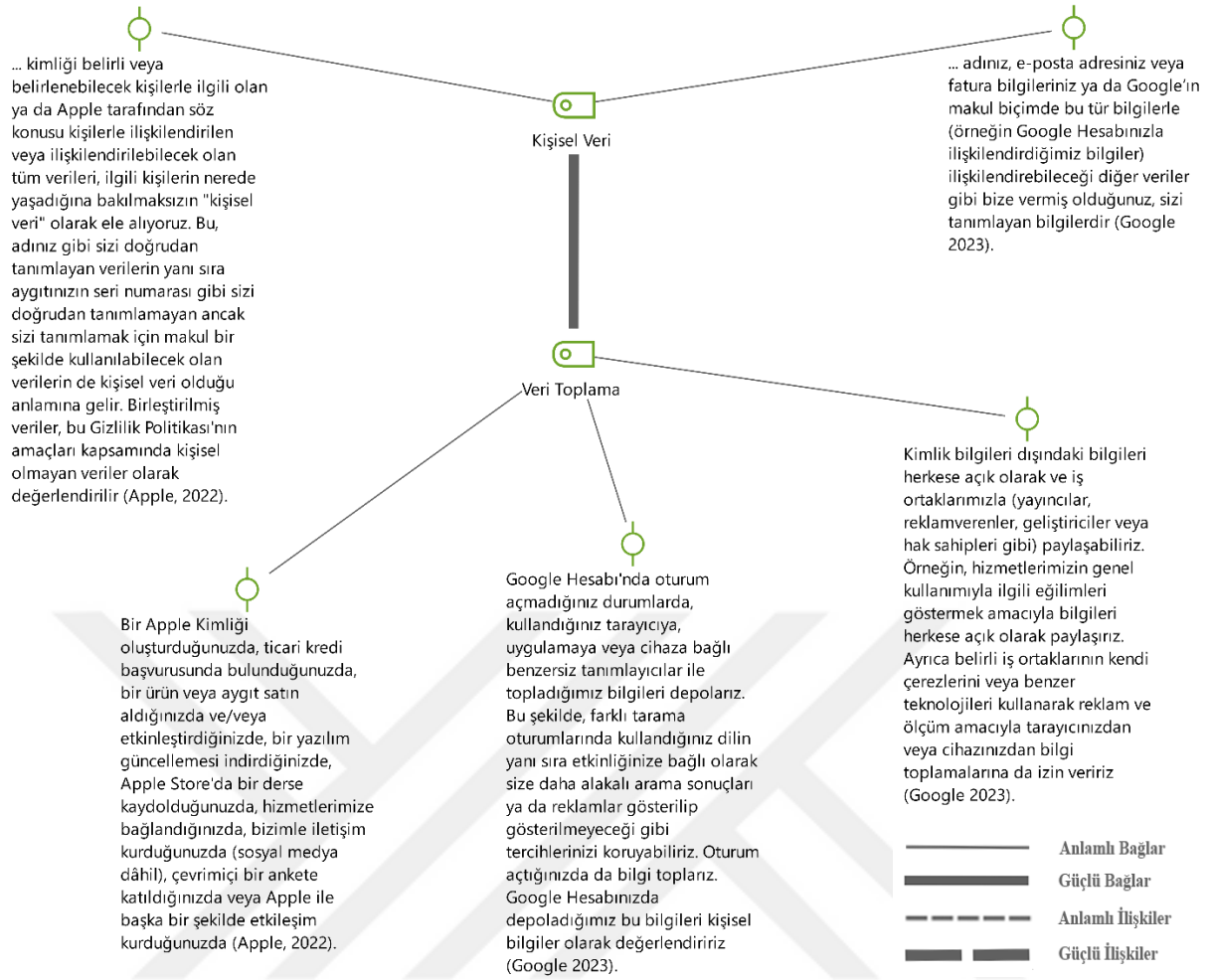
Şekil 3.1'te Apple'ın, 3.2'de ise Google'ın topladığı veri türleri yer almaktadır. Apple'ın topladığı veri türlerinden “Sağlık”, “Hesap Bilgileri”, “Aygıt”, “Ödeme”, “Kullanım” ve “İşlem” verilerinin bu dokümanda daha sık geçtiği görülmektedir. Bu veriye göre Apple, sağlık verileriyle daha fazla ilgilenmektedir. Diğer veri türleri ise (Aygıt, Hesap, Ödeme, Kullanım ve İşlem) daha çok kullanıcıların uygulamalardaki hesap hareketlerini takip eden verilerdir. Google'ın topladığı veri türleri ise Apple'a kıyasla daha fazladır. Bu veri türlerinden “Tarayıcılar”, “Cihazlar”, “Video”, “Konum Geçmişi”, “Konuşma ve Ses”,

“Arama Terimleri”, “İp Adresi”, “E-Posta”, “Fotoğraf” ve “Telefon Numarası” gibi veri türleri bu dokümanda daha sık geçmektedir. Burada görüldüğü üzere Google, Apple’a göre daha fazla davranış verisi talep etmektedir. “Tarayıcılar” ve “Arama Terimleri” verisi, Google’ın en önemli ürününün arama motoru olduğu göz önüne alındığında belli ölçülerde kabul edilebilirdir; ancak, diğer veri türlerine bakıldığında neredeyse kullanıcının dijital ortamlardaki her hareketinden elde ettiği veriyi toplayabilmesi de düşündürücüdür.



Şekil 3.3 Üçüncü Taraflara Veri Aktarımı - Kod Teori Modeli

Şekil 3.3'te her iki dokümanda yer alan “Veri Aktarma” kelimesi kod teori modeliyle görselleştirilmiş, veri aktarma ile ilgili paragraflara yer verilmiştir. Şekilde görüldüğü üzere her iki şirket de kullanıcılarından topladığı veriyi üçüncü taraflarla paylaşmaktadır. Burada dikkat çeken nokta ise yukarıda Google politikasına ait kelime bulutunda (bkz. Grafik 3.2) verilen “bilgi” kelimesinin Google tarafından doğrudan “kişinin kimlik bilgisi” olarak lanse edildiğidir. “Kimlik bilgilerinizi (adınız veya e-posta adresiniz gibi) siz istemedikçe reklam verenlerle paylaşmayız” (Google, 2023) ifadesi, Google’ın topladığı verilerin, aslında kişilere ait kimlik bilgilerinden oluştuğu açık bir şekilde politikada yer almaktadır.

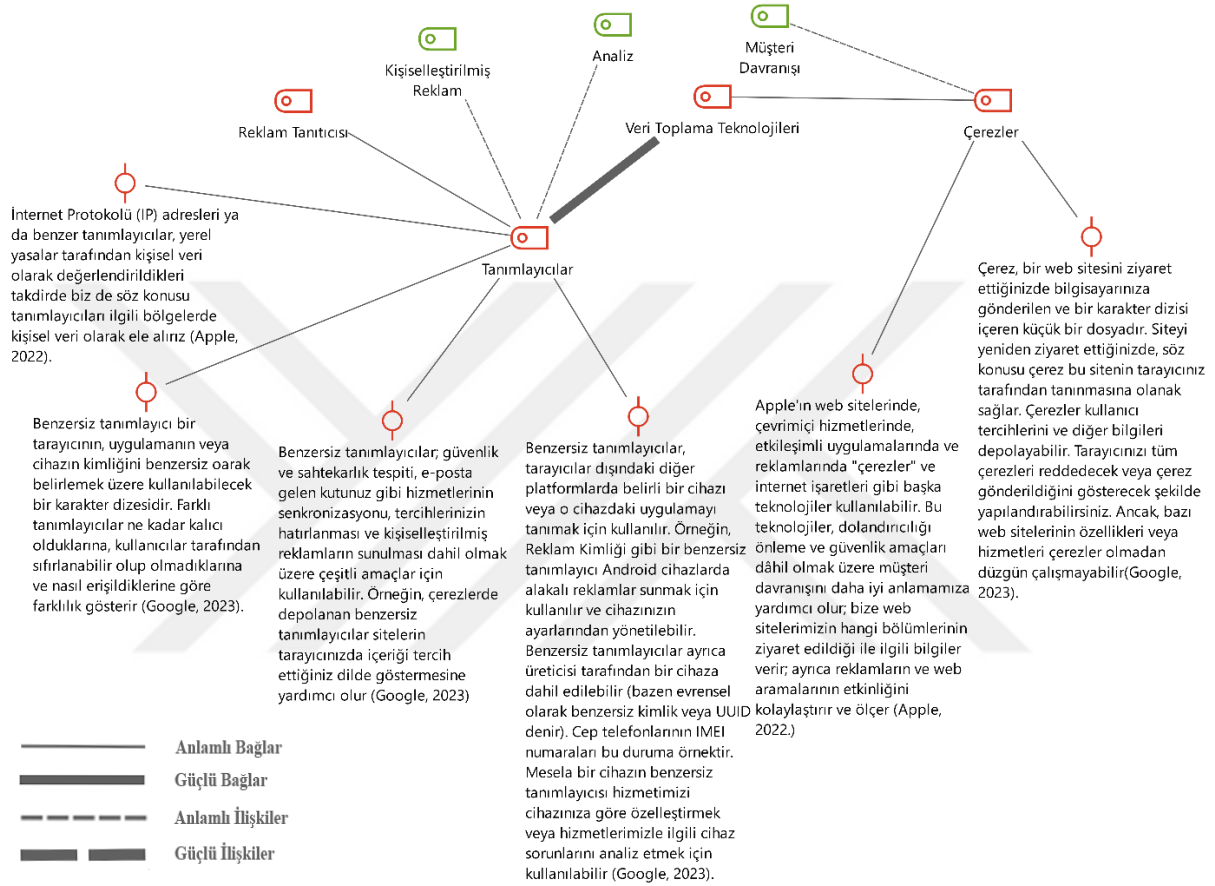


Şekil 3.4 Kişisel Veri Tanımları ve Veri Toplama - Kod-Alt Kod-Bölümler Modeli

Şekil 3.4'te gösterildiği üzere “Kişisel Veri” kategorisi ile “Veri Toplama” kelimesi arasında güçlü bir bağ (kalın çizgi) oluşmuştur. “Kişiler Veri” ile ilişkili paragraflara bakıldığında da kişisel verilerin, kişilere ait bilgilerle ilişkilendirilebileceği görülmüştür. “Veri Toplama” ile ilgili paragraflarda ise Apple’ın, kullanıcının kendi ürünleriyle ilişki içerisinde olduğu zaman (cihaz alma, oturum açma, yazılım indirme vb.) veri topladığı, Google’ın ise ürünleriyle ilişkili olup olmamasına bakılmaksızın kullanıcıdan veri topladığı görülmektedir. Burada Apple’ın daha az veri toplama eğiliminde olduğu anlaşılırken, Google’ın daha fazla veri toplama eğiliminde olduğu söylenebilir. Ancak Apple kullanıcılarının çoğu, hesaplarında oturum açmadan neredeyse hareket dahi (Apple ürünlerine erişememe) edememektedir. Dolayısıyla Apple’a ait herhangi bir uygulamada oturum açıldığında veri toplamanın *startu* verilmiş olacaktır. Google ise her durumda veri toplarken, iş ortaklarına da veri toplama imkânı tanımaktadır. Sonuç olarak Google, Apple’a oranla daha fazla veri talep etmektedir. Üçüncü tarafların Google kullanıcılarından veri toplamasına izin vermesi, Google’ın adeta bir veri toplama mekanizması olarak işlev gördüğünü göstermektedir.

2. Veri Toplama Teknolojileri (Gözetim Alt Yapısı)

Bu kategori altında, gizlilik politikalarında geçen veri toplama yöntemleri ve gözetim mekanizmalarına ilişkin ifadeler yer verilmiştir. Apple ve Google’ın Gizlilik Politikalarında yer alan ve veri toplama yöntem ve yazılımlara ilişkin dağılım aşağıdaki şekil aracılığı ile görselleştirilmiştir:



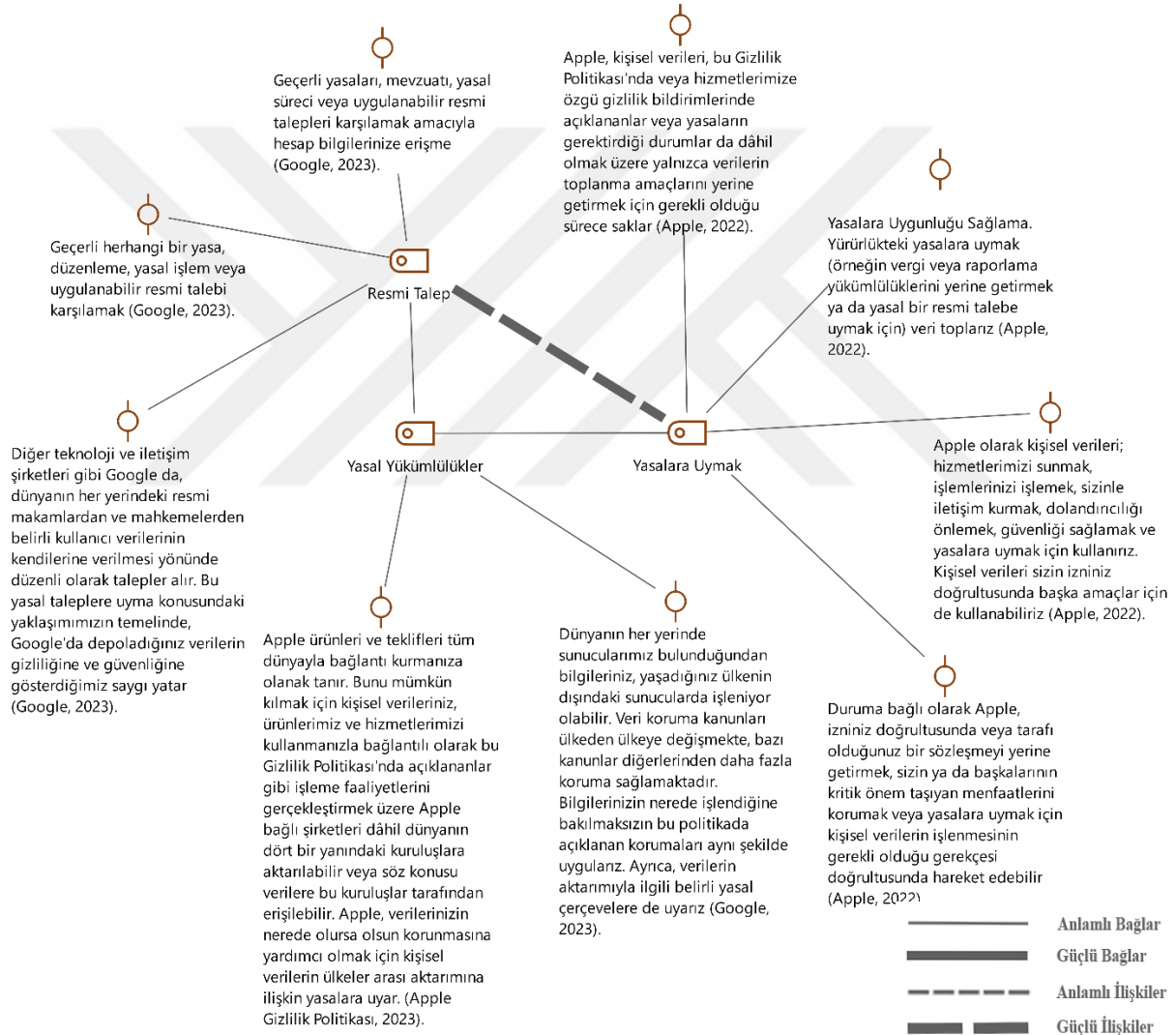
Şekil 3.5 Veri Toplama Yöntem ve Yazılımları - Kod Teori Modeli

Şekil 3.5’te gösterildiği üzere “Veri Toplama Teknolojileri” kategorisi ile “Tanımlayıcılar” arasında güçlü, “Veri Toplama Teknolojileri” ile “Çerezler” arasında anlamlı bir bağ (normal çizgi) bulunmaktadır. Veri toplama amacıyla oluşturulan yazılımlar her iki politikada yer alsa da Apple’ın politikasında tanımlayıcıların ne için kullanıldıkları açıkça belirtilmemiştir. Google’da ise tanımlayıcıların hangi amaçlar doğrultusunda kullanıldığı açıklanmıştır. Apple’ın dokümanında “Tanımlayıcılar” bölümü altındaki paragrafta yer alan ve benzersiz tanımlayıcılar hakkında verilen “... yerel yasalar tarafından kişisel veri olarak değerlendirildikleri takdirde” şeklindeki ifade, tanımlayıcılardan elde edilen verilerin de kişisel veri olarak görülmesi gerektiğinin kanıtı sayılabilir. Apple, bu ifadeyle, politikasında yer verdiği “... kimliği belirli veya belirlenebilecek kişilerle ilgili olan ya da Apple tarafından söz konusu kişilerle ilişkilendirilen veya ilişkilendirilebilecek olan tüm

verileri, ilgili kişilerin nerede yaşadığına bakılmaksızın “kişisel veri” olarak ele alıyoruz” ifadesiyle çelişmektedir. Dolayısıyla tanımlayıcıların, yalnızca yasalar tarafından değerlendirildiği zaman değil, her zaman kişisel veri olarak kabul edilmesi gerekmektedir.

3. Yasal Yükümlülükler

Bu kategori altında, gizlilik politikalarında geçen yasal yükümlülüklerle ilgili ifadelere yer verilmiştir. Apple ve Google’ın Gizlilik Politikalarında yer alan ve yasal yükümlülüklerle ilişkin şekil aşağıda verilmiştir:



Şekil 3.6 Yasal Yükümlülükler - Kod-Alt Kod-Bölümler Modeli

Şekil 3.6’da gösterildiği üzere “Yasal Yükümlülükler” kategorisi ile “Yasalara Uymak” ve “Resmi Talep” kelimeleri arasında anlamlı bir bağ vardır. “Resmi Talep” ve “Yasalara Uymak” kelimeleri arasında ise çok güçlü bir ilişki (kesikli kalın çizgi) bulunmaktadır. Bu veri, resmi bir talep olduğunda yasalar çerçevesinde kişisel verilerin resmi makamlarla paylaşılacağını ifade eden paragrafların sıklıkla ilişkilendirildiğini

göstermektedir. Her iki şirketin politikasında yer alan yasal yükümlülüklerle bağlantılı ifadeler, kişisel verilerin korunmasında yasaların veya yönetmeliklerin önemli bir yerde konumlandığını göstermektedir. Bu türden düzenlemelerin varlığı, yasal caydırıcılık açısından da olumlu olarak değerlendirilebilir; ancak daha da önemli olan nokta bu yasa ve yönetmeliklerin etkili bir şekilde uygulanmasıdır. Örneğin ülkemizde mevcut olan KVKK'daki bazı belirsizliklere/eksikliklere dikkat çekmek gerekmektedir. 6698 sayılı KVKK'nın 1. maddesinin birinci fıkrasına göre 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". Kanun aynı zamanda kişisel verilerin nasıl tanımlandığı konusuna açıklık getirmektedir. KVKK'nın 6. Maddesinin birinci fıkrasında belirtildiği üzere "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir." ve yine kanunun ikinci maddesine göre özel nitelikli verilerin işlenmesi "açık rıza" şartı ile yasaklanmıştır: "Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır". Öte yandan KVKK, belirli durumlarda kişisel verilerin işlenmesine istisnalar getirmektedir. Örneğin "... resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi" veya "millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi" istisnalar kapsamındadır. Bir başka istisna, kanunun 6. Maddesinin üçüncü fıkrasında şu şekilde belirtilmektedir: "Birinci fıkrada sayılan sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir." Bu istisna, Apple ve Google gizlilik politikalarında yer alan "yasal yükümlülükler" başlığı altındaki istisnalara benzerdir. İlgili kanunun 6. Maddesinin üçüncü fıkrasında belirtildiği üzere "Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir". Görüldüğü üzere KVKK'ya göre özel nitelikli veri olarak adlandırılan ve işlenmesi yasak olan veriler, yine aynı kanundaki bazı maddelere göre istisnalara dahilinde işlenebilmektedir. Ancak burada bazı belirsizlikler bulunmaktadır. Örneğin özel nitelikli

verilerin “suç teşkil etmemek” kaydıyla işlenebilmesi ifadesinde suçun nasıl tanımlandığı ya da hangi durumun suç olup olmadığına ilişkin açıklama/tanımlama bulunmamaktadır. Ayrıca gözetimi meşrulaştıran güvenlik söylemleri ve terör önlemlerine benzer şekilde KVKK’nın bazı maddelerinde, örneğin “kamu güvenliğinin” nasıl değerlendirileceği konusunda belirsizlik vardır. Öte yandan bu istisnalar, temel hak ve özgürlükleri orantısız veya eşit olmayan bir biçimde sınırlandırabilir. Bu nedenle, temel hak ve özgürlükleri koruma adına oluşturulan bu türden kanunların dengeli, meşru ve demokratik bir temele dayandırılması gerekmektedir.

3.2.3. Derinlemesine Görüşmelerden Elde Edilen Katılımcı İfadelerinin Tematik Analizi

Nitel araştırmaların doğası gereği çalışma grubundan, değişen miktarlarda ham veri elde edilmektedir. Nicel araştırmalara kıyasla nitel araştırmadan elde edilen veriler düşünceler, deneyimler ve inançlardır. Dolayısıyla nitel araştırmalarla elde edilen bu bilgileri organize etmek zorlaşmaktadır. Tematik analiz de veri içindeki örüntüleri (temaları) belirlemeye, analiz etmeye ve raporlamaya yönelik bir yöntemdir. Bu yöntem, veri setini asgari düzeyde düzenlemeye ve zengin ayrıntılarla tanımlaya yardımcı olmakta hem *gerçekliği* yansıtmak hem de *gerçekliği* ortaya çıkarmak ve çözmek amacıyla kullanılmaktadır (Braun ve Clarke, 2006: 79). Tüm bu nedenlerle hem veri setinin organize edilmesi hem de verilerin derinlemesine analiz edilmesi için tematik analiz tercih edilmiştir. Tematik analizde yer alan kategori, tema ve alt temaları gösteren tablo aşağıdaki gibidir:

Tablo 3.3 Kategori, Tema ve Alt Temaları Gösterir Tematik Analiz Kapsamı

Kategori	Tema	Alt Tema
1. Katılımcıların Kişisel Veri ve Veri Bağlantılı Süreçlere İlişkin İfadelerinin Analizi	Veriye Atfedilenler	<i>Veri Gücü</i>
	Kişisel Veri Mahremiyeti ve Gizlilik	
	Regülasyonların Etkililiği	
	Veri Mahremiyeti ve Gizliliğinde Geliştirici Hassasiyeti	
	Verinin Gözetimi	
	Veri Toplama Süreçleri	
	Veri-Reklam İlişkisi	<i>Kişiselleştirme ve Hedefli Reklam</i>
2. Katılımcıların Mobil Uygulamalarda Gizlilik, Güvenlik ve Gözetime İlişkin Yaklaşımlarının Analizi	Verilerin Hâkimiyetinde İstilacı Şirketler	
	Mobil İşletim Sistemlerinde Gizlilik ve Güvenlik	
	Mobil Uygulamalar ve Gizlilik	<i>Erişim İzinleri ve Çevrimiçi İzleyiciler</i>
	Google ve Gizlilik	

	Apple ve Gizlilik	<i>Alternatifsizliğin İtirafı</i>
	Blok Zinciri ve Merkezi Olmayan Uygulamalar	
	Blok Zincirinde Veri Gizliliği	
3. Katılımcıların Veri Gözetimine Karşı (Mukavemet) Tepki Hamlelerinin Analizi	Engelleme Hamleleri	<i>Maskeleme ve Algoritmalar</i>
	Maskeleme Hamleleri	
	Kırma Hamleleri	
	Karşı-Gözetim Hamleleri	
4. Katılımcıların Deneyimleri Perspektifinden Kullanıcılara Mukavemet Önerilerinin Analizi	Anonimlik	
	Güvenlik	
	Veri Paylaşmama / Dijital Ayak İzi	
	Uygulama Özelinde Önlemler	

Tematik analiz için MAXQDA 2020 Nitel Veri Analizi Programı yardımıyla kategoriler, temalar ve alt temalar³² oluşturulmuş, katılımcıların ifadeleri bu temalara kodlanarak analiz edilmiştir. MAXQDA üzerinde oluşturulan temalar ve alt temalar, “Kişisel Veri”, “Uygulama Ekosistemi”, “Gözetime Tepki” ve “Direniş Önerileri” kategorileri altında *sadeleştirilerek*³³ kodlanmıştır. Katılımcı ifadelerinin kodlandığı kategorilere ait grafik aşağıda verilmiştir:

Kod Sistemi	K.1	K.2	K.3	K.4	K.5	K.6	K.7	K.8	K.9	K.10	K.11	TOPLAM
> KİŞİSEL VERİ	•	•	•	•	•	•	•	•	•	•	•	428
> UYGULAMA EKOSİSTEMİ	•	•	•	•	•	•	•	•	•	•	•	573
> GÖZETİME TEPKİ	•	•	•	•	•	•	•	•	•	•	•	87
> DİRENİŞ ÖNERİLERİ	•	•	•	•	•	•	•	•	•	•	•	32
Σ TOPLAM	108	117	108	103	170	116	82	70	91	73	82	1.120

Grafik 3.3 Kod Matrisi Tarayıcısı - Kategoriler

Grafik 3.3’te gösterildiği üzere katılımcıların ifadeleri, en çok “Uygulama Ekosistemi” kategorisindeki tema ve alt temalarda yoğunlaşmıştır. En çok kodlanan ikinci kategori “Kişisel Veri” kategorisidir. “Gözetime Tepki” ve “Direniş Önerileri” kategorisine ise daha az sayıda kodlama yapılmıştır. Bu veri, katılımcıların uygulama ekosistemi, veri ve veri bağlantılı konular hakkında çok daha fazla görüş bildirdiklerini gösterirken, veri gözetimine

³² Tüm tema ve alt temaları gösterir kod sistemi Ek-1 de sunulmuştur. Yukarıda belirtilen dört kategoriye ek olarak “Duygular” kategorisi, katılımcıların diğer kategori ve temalara karşı duygu durumlarını ortaya koyabilmek için analize en son eklenmiş; ancak ayrı bir başlık altında incelenmemiştir. Bu kategori altında yer alan temalar, diğer kategoriler altında yer alan temalarla birlikte değerlendirilmiştir.

³³ Tematik analiz kategorileri, temaları ve alt temaları, görselleştirmeyi zorlaştırması nedeniyle sadeleştirilerek verilmiştir.

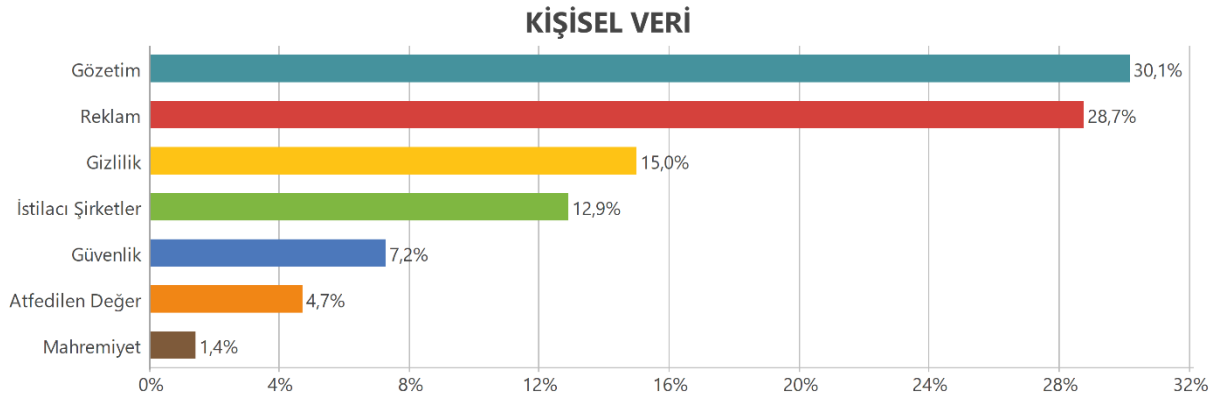
gösterilen tepki, karşı-gözetim ve gözetime karşı geliştirilebilecek stratejiler hakkında daha seyrek görüş bildirdiklerini göstermektedir.

3.2.3.1. Katılımcıların Kişisel Veri ve Veri Bağlantılı Süreçlere İlişkin İfadelerinin Analizi

Kimse kendi verisini şirketlere kaptırmamalı.

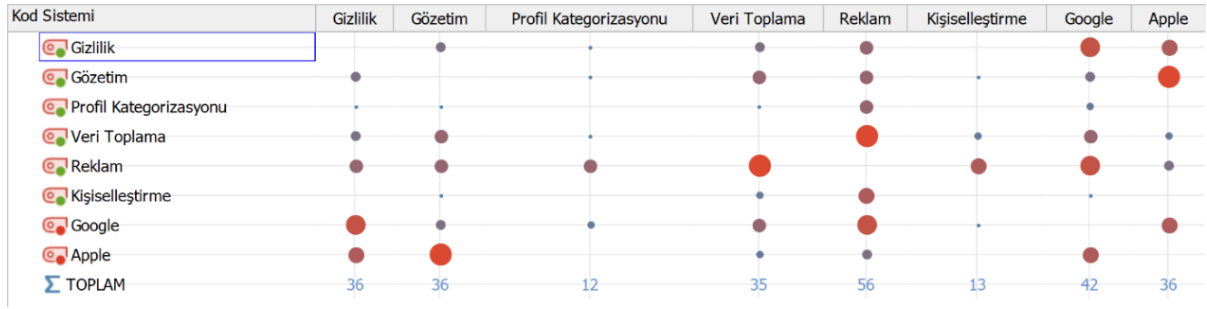
Çünkü önümüzdeki dönemlerde bunlarla neler yapılabileceğini hiç bilmiyoruz (K.6).

Bu kategori altında katılımcıların kişisel veri ve bağlantılı konulara ilişkin görüşlerine yer verilmiştir. Geliştiricilerin verinin önemi ve veriye atfedilen değer hakkında neler düşündüğü, veri mahremiyeti, veri gizliliği ve veri toplama süreçlerinin onlar için ne ifade ettiği ve mobil uygulamalardaki istilacı şirketlere bakış açıları resmedilmeye çalışılmıştır.



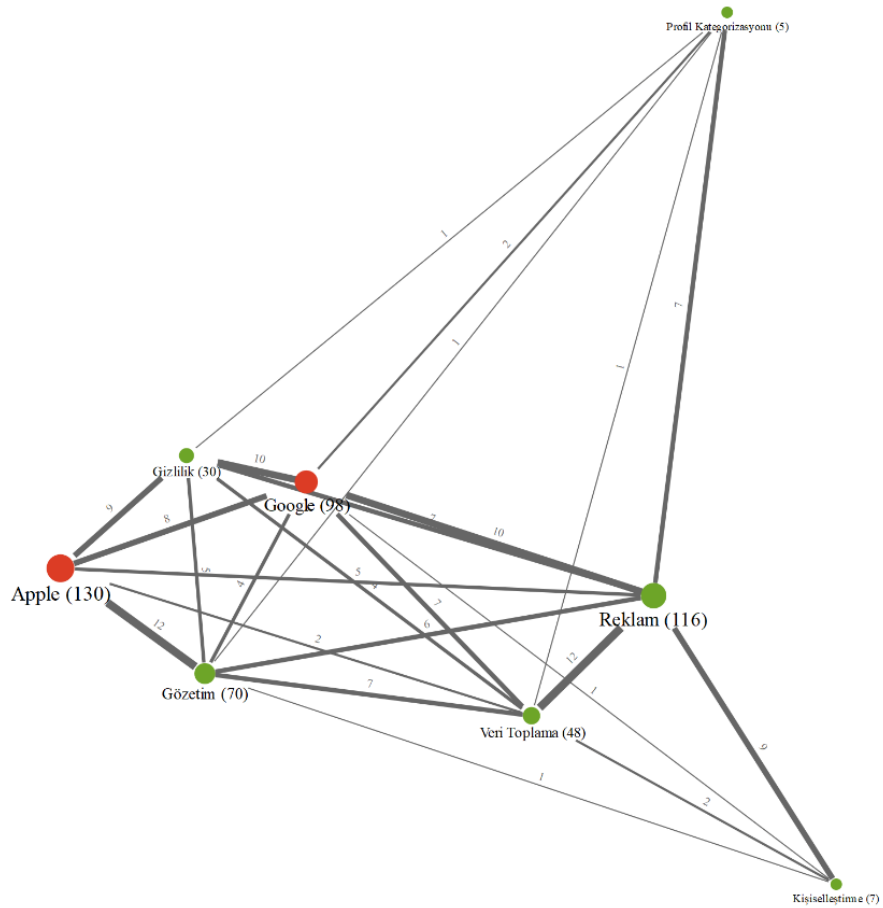
Grafik 3.4 Kişisel Veri Kategorisinde Yer Alan Temaların Kod İstatistiği

Grafik 3.4'te gösterildiği üzere “Kişisel Veri” kategorisi altındaki kodlamalar en çok “Gözetim”, “Reklam” ve “Gizlilik” temalarına yapılmıştır. Katılımcılar, kişisel veri ve bağlantılı konulardan bahsederken aynı zamanda sıklıkla gözetim ve reklamlardan bahsetmişlerdir. “Kişisel Veri” kategorisinde birlikte daha sık kodlanan temalar da aşağıda verilmiştir:



Grafik 3.5 Kişisel Veri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri

Grafik 3.5’te gösterildiği üzere katılımcıların ifadeleri, en çok “Veri Toplama” ve “Reklam” temasıyla birlikte kodlanmıştır. “Gizlilik” ve “Gözetim” temalarının da “Google” ve “Apple” temalarıyla ilişkili olduğu görülmektedir. Aşağıda verilen şekilde ise bu temalara ait kod haritası verilmiştir:



Şekil 3.7 Kişisel Veri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası

Şekil 3.7’ de görüldüğü üzere “Kişisel Veri” kategorisi altındaki “Reklam”, “Gizlilik”, “Veri Toplama”, “Google” ve “Apple” temaları birbirleriyle yakın ilişki içerisinde olup sık bir biçimde kodlanmıştır. “Kişiselleştirme” ve “Profil Kategorizasyonu” alt temaları “Reklam”

Teması ile sık kodlanırken diğer temalara göre daha uzak bir ilişki içerisinde. Buradan çıkarılacak en önemli sonuç ise Google’ın Apple’a kıyasla reklam ekosistemi için çok daha fazla veri topladığıdır. Diğer önemli bir sonuç ise kullanıcılara kişiselleştirilmiş reklam göstermek için profil kategorizasyonu yapılmasıdır. Profil kategorizasyonu yapılırken de kullanıcıların *hedef* ve *çöp* gibi kategorilerde sınıflandırdığı (bkz. Turow, 2015: 21) bilinmektedir. Böylelikle kullanıcıların profillerine göre reklam gösterilmekte, kategoriye dâhil olan kullanıcıya ilişkili reklamlar gösterilirken kategori dışı bırakılanlara gösterilmemektedir.

Veriye Atfedilenler

Araştırma kapsamında görüşülen tüm geliştiriciler, kişisel verilerin oldukça önemli olduğunu dile getirirken bazı katılımcılar da verinin öneminin kavranamadığını ifade etmişlerdir. Dijitalleşmeyle birlikte giderek daha fazla veri yığınları ürettiğimizi, daha fazla veri işleme ve anlamlandırma sürecinin içerisine çekildiğimizi söylemişlerdir. Ayrıca katılımcılar, verinin geliştirici açısından da önemini vurgulamışlardır. Katılımcıların veriye atfettiği değer de kimi zaman para birimi, kimi zaman şirketlere kaptırmaması gereken kişisel bilgi cüzdanı olduğu, verilerin kişilere ait bir değer olduğunu özellikle vurguladıkları görülmüştür. Ayrıca kişiler hakkında birçok bilgiyi barındıran verilerin, gelecekte nasıl kullanılacağı bilinmediğini, bu nedenle kişisel verilerin koruma noktasında temkinli olunması gerektiğini ifade etmişlerdir:

“Aslında bizim için çok fazla öneme sahip. Kişisel veri dediğimiz şey aslında bir para birimi gibi bir şey şu anda. İnsanlar buna böyle hitap ediyor artık. Kişisel veriler daha önceleri kâr amacı gütmeyen şekillerde kullanılırken günümüzde kâr etmek için kullanılmaya başladı” (K.1).

“Önemini henüz kavrayabilmiş değiliz” (K.2).

“Veriler çok önemli bizim için. Geliştirdiğimiz uygulamalar ve oyunlar için. Mesela bir oyun geliştirdiğim zaman oradan kişinin verisini mutlaka almam gerekiyor ki o oyunun daha sonrasında nasıl geliştireceğim, onlarla ne yapacağıma dair bir benim için bir yol gösterici oluyor” (K.9).

“Kişisel veriler artık çok önemli. Veriler bizim hakkımızda birçok bilgi barındırıyor” (K.11).

“Kimse kendi verisini kimse şirketlere kaptırmamalı. Çünkü önümüzdeki dönemlerde bunlarla neler yapılabileceğini hiç bilmiyoruz. Yapay zekayla da zaten birçok şey artık belki on kat hızlandı... Yüz kat hızlanıyor. O yüzden dikkat edilmeli” (K.6).

Hem katılımcı ifadeleri hem de alan gözlemlerine dayanılarak, katılımcıların önemli bir bölümünün veriye bakış açısı, verilerin çok önemli olduğu, korunması gerektiği ve kişisel veri mahremiyetinin oldukça hassas bir konu olduğu yönündedir. Ancak katılımcıların bir bölümü de veriyi, yazılımlarını daha da geliştirmek için elde edilmesi gereken, doğrudan toplanmasa bile analitik olarak fayda sağlaması beklenen bir *çıkar nesnesi* olarak görmektedir. Buradaki *çıkar* ifadesi olumsuz olarak algılanabilir; ancak büyük şirketlerle/yayıncılarla rekabet etmekte zorlanan geliştiricilerin verilerden mümkün olduğunca yararlanmak istemesi beklenen bir durum olarak görülebilir. Onlar için verilerden yararlanmak sorun değildir, sorun, kişisel veriler üzerinde büyük şirketlerin hegemonya kurmaya çalışmasıdır. Verilere erişimin eşitsiz olması, veri hâkimiyetine sahip olmayan bağımsız geliştiricilerin gelişimine engeldir. Bağımsız geliştiriciler veriye, yalnızca verilere hâkim olan şirketlerin istediği kadar ulaşabilmektedir. Şirketlerin buradaki amacı, bağımsız geliştiricilerin kendileriyle rekabet edecek düzeye gelmemesi ve bağımsız olarak kalmasıdır. Verinin güç olarak kabul edildiği dijital kapitalist sistemde, geliştiricilerin veriye ulaşma fırsatlarındaki eşitsizlik, gücün dağılımında da eşitsizlik yaratmaktadır.



Şekil 3.8 Veriye Atfedilen Değer - Kod Teori Modeli

Şekil 3.8’de “Veriye Atfedilen Değer” teması ile “Güç” alt teması arasında oluşan bağlar gösterilmiştir. “Veriye Atfedilen Değer” ve “Güç” alt teması arasında anlamlı bir bağ varken, “Veriye Atfedilen Değer” temasıyla “Reklam”, “Güvenlik” ve “Gizlilik” temaları arasında anlamlı bir ilişki (kesikli normal çizgi) olduğu görülmektedir. “Güç” alt teması ile birlikte oluşan kodlarda en ilişkili kod “Kişisel Veri” kategorisi ile oluşmuştur. Veriye atfedilen

değerin katılımcılar tarafından çoğunlukla güç olarak lanse edilmesi, “Veri Gücü” alt temasını oluşturmuş ve katılımcıların veri gücüne dair ifadelerine aşağıda yer verilmiştir.

Veri Gücü

Veri gücü, veriye atfedilen en önemli değerlerden biri olarak görülmektedir. Bu nedenle katılımcılar, veriye sahip olmanın önemini sık sık vurgularken, veri gücünü örneklerle ifade etmeye çalışmışlardır. Buna ilaveten büyük teknoloji şirketlerinin veri gücünü ellerinde bulundurduklarını ve bu gücü kullanarak insanlar üzerinde tahakküm kurduklarını belirtmektedirler:

“Veri ile ilgili Netflix belgeselleri bile yapıldı. Veri çok büyük bir güç şirketler için ve çoğumuzda biliyoruz bu kadar ücretsiz ürün olmasının sebebi aslında insanların verisini toplayıp oralardan bir anlamlandırma çıkartmak. “Big Data” dediğimiz mevzu. O yüzden de aslında veriye sahip olmak çok çok önemli dipnot da söyleyeyim” (K.5).

“Şu anda bütün dünya veriler üzerinden dönüyor. Veriler ve bu verilerin işlenmesi üzerinden. Yani verinin gücüyle. Bugün siyasi partilerin hangi adayı çıkaracağından tut, Suudi Arabistan’ın ne kadar petrol ihraç etmesi gerektiğine kadar veriler üzerinden dönen bir sistem var” (K.4).

“Verilerimiz sayesinde ve daha doğrusu alışkanlıklarımız sayesinde büyük şirketler bizi neredeyse yönetebilecek seviyede” (K.2).

Katılımcı ifadelerinin literatürle uyumlu olduğu görülmektedir. Günümüzde veriler, “insan yaşamındaki enformasyon akışlarıdır” (Couldry ve Mejias 2022: 13) ve kişisel verilere para, petrol veya ekonomik kaynak olarak bakılmaktadır (Salek, 2008; Share Lab, 2015b; Zuboff, 2021; Couldry ve Mejias 2022). Ayrıca Avrupa veri koruma süpervizörü Peter Hustinx (European Data Protection Supervisor, 2014: 28)’in ifade ettiği gibi dijital ekonomideki güç, belirli bir girişimin gerçekten, potansiyel veya hipotetik olarak kişisel bilgileri toplama ve yayma yeteneği tarafından kısmen belirlenmektedir ki bu yetenek, günümüz teknoloji şirketlerinin en büyük kozu hale gelmektedir.

Kişisel Veri Mahremiyeti ve Gizlilik

Kişisel veri mahremiyeti ve gizlilik konusu çalışmanın önemli odak noktalarından biridir. Mahremiyet ve gizlilik katılımcılar için de kilit noktadır ve katılımcıların bu konuda iyimser ifadelerinin oldukça sınırlı olması beklenen bir sonuçtur; günümüzde veri mahremiyetini korumanın kişisel tercihe indirgenmesi nedeniyle kullanıcıların verilerini şirketlere açıp açmama konusundaki özgürlüğü bir anlamda askıya alınmaktadır. Bu nedenle katılımcılar, kişisel verilerin mahremiyetinden pek de bahsedilemeyeceğini dile getirmektedir.

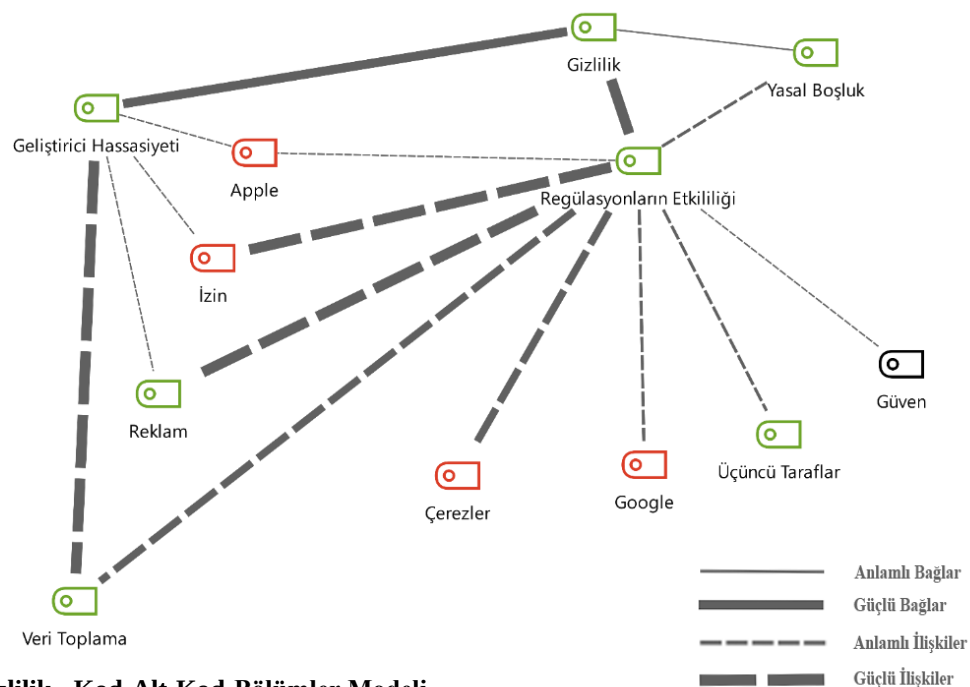
Onlara göre internete girdiğimiz andan itibaren verilerimiz talep edilmektedir ve bu veriler kişileri tanımlayabilecek özelliktedir. Öte yandan katılımcıların tamamının, verilerin şirketlerce nasıl kullanılabileceği konusunda yeteri kadar bilgi sahibi olduğu anlaşılmaktadır. Bu nedenle bazı kullanıcıların veri mahremiyetine önem gösterdiği ve veri paylaşımını mümkün olduğunca sınırladığı da görülmüştür:

“Her platformu kullanmamız için o platformda bizden bir kendimizi tanımlamamızı istiyorlar. Bu tanımın içinde de birçok veri oluyor, kişisel veri oluyor. Bunların bir kısmı her yerde bulabileceğimiz, yani bulunsada problem oluşturmayacak veriler olsa da bazıları o platformu kullanabilmemiz için özel bilgiler oluyor. Öncelikle bize bir hizmet sunmak için veri topluyorlar; ama aynı zamanda bunu gelir elde etmek için de topluyorlar” (K.8).

“Kişisel verilerle ilgili konu özellikle son zamanlarda gizlilik ve güvenlik kaygısı ile gündeme çok fazla geldi. Çünkü veriler bizim satın alma davranışlarımız internet alışkanlıklarımız ve daha akla gelebilecek birçok şeyi bizim hakkımızdaki birçok şeyi barındırıyor” (K.11).

“Günümüz sosyal medya dünyasında, herkesin bir şeyler paylaştığı bir dönemde verilerin gizliliği çok önemli. Ben o sebeple çok büyük bir sosyal medya kullanıcısı değilim. Çocuğumun fotoğraflarını vesaire paylaşmıyorum. Bir sürü sebep var arkasında yatan. Bunların hepsi de tabii bu verilerin nasıl kullanılabileceğini bilmekle alakalı” (K.5).

Burada özellikle Katılımcı 5’in ifadesi dikkat çekicidir. Geliştiricinin ailesine ait herhangi bir fotoğrafı dahi paylaşmaktan imtina etmesi, internet ortamındaki kişisel veri gizlilik riskini açıkça göstermektedir. Bilindiği üzere bugün, özellikle mobil uygulamalar aracılığıyla, deyim yerindeyse tek bir tıkla ve her an, sosyal medyada en özel anlar paylaşılabilen, fotoğraflara konum bile eklenebilmekte -ki bu sayede kişinin hareketleri takip edilebiliyor- gizlilik riski gün geçtikçe daha da artmaktadır.



Şekil 3.9 Gizlilik - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.9’da gösterildiği üzere “Gizlilik” temasıyla “Geliştirici Hassasiyeti” ve “Regülasyonların Etkililiği” alt temaları arasında güçlü bir bağ bulunurken, “Gizlilik” temasıyla “Yasal Boşluk” alt teması arasında bir anlamı bir bağ bulunmaktadır. “Geliştirici Hassasiyeti” alt temasıyla “Veri Toplama” alt teması arasında çok güçlü, “Veri Toplama” alt teması ve “Regülasyonların Etkililiği” alt teması arasında güçlü bir ilişki bulunmaktadır. Ayrıca “Regülasyonların Etkililiği” alt temasıyla “İzin” ve “Reklam” alt temaları arasında da çok güçlü bir ilişki bulunmaktadır. Buradan çıkarılabilecek sonuç ise kişisel veri mahremiyeti ve gizliliğinde geliştiricilerin de rolü bulunduğu, geliştiricilerin veri toplarken veri gizliliğine dikkat etmesi gerektiği ve yasal düzenlemelerle bunun kontrol altına alınabileceğidir. Katılımcılar, regülasyonların etkili şekilde işletilmesi halinde kişisel veri gizliliğinin mümkün olabileceğine işaret etmişlerdir. Ayrıca katılımcılarda bu düzenlemelere ilişkin güven de söz konusudur. “Regülasyonların Etkililiği” ve “Geliştirici Hassasiyeti” temalarına ilişkin detaylı analize de aşağıda yer verilmiştir.

Regülasyonların Etkililiği

Dijital teknolojilerin kullanıldığı birçok ürün ve hizmette kişisel verilerin korunmasıyla ilgili bazı regülasyonlar mevcuttur. Bunlardan bazıları AB ülkelerinde uygulanan Genel Veri Koruma Yönetmeliği (GDPR- General Data Protection Regulation), ABD’de (Genel bir koruma yasası bulunmamaktadır.) uygulanan Çocukların Çevrimiçi Gizliliğini Koruma Kanunu (COPPA- Children’s Online Privacy Protection Rule) ve Türkiye’de de Kişisel Verilerin Korunması Kanunu (KVKK)’dur. Katılımcılar, bu kanunların şirketlerdeki veri toplama iştahını dizginlemek için çıkarıldığını, aynı zamanda bu düzenlemelerin uygulanabilirliği konusunda sorunlar olduğunu; ancak yine de bu düzenlemelere ihtiyaç olduğunu, mevcut yasaların daha da iyileştirilerek yaptırımların ve uygulanabilirliğinin artırılması gerektiğini bildirmektedir:

“Bu konuda karışık duygular besliyorum. Çünkü bir yandan Avrupa ve Avrupa Birliği başta olmak üzere birtakım kanunlar, birtakım regülasyonlar devreye sokmaya başladı. Bir şeyler yapmaya başladı. Öte yandan çok da işe yarıyor gibi durmuyor. Şu anda bir süre önümüzde pop-up [İnternet sitelerinde ve mobil uygulamalarda aniden belirlen bir reklam türü] çıkıyor ama yine bütün çerezleri kapatamıyoruz web sitelerinde. Uygulamalarda zaten ne olduğu belli değil ne aldığı belli değil. Mesela Facebook’un kendi uygulamasında muhtemelen çok daha fazla veri alıyordur ve haberimiz olmuyordur. O yüzden bir yandan iyi adımlar, güzel adımlar atılmaya başlandıysa da daha iyiye gideceğinden çok emin değilim” (K2).

“Kullanıcıdan çok fazla veri toplanıyor. Bunun biraz daha yönetilebilir, denetlenebilir bir şekilde ilerlemesi lazım bence. Şu an çok doğru bir şekilde yönetildiğini, denetlendiğini düşünmüyorum açıkçası” (K.10).

“Şu ana kadar çok fazla veri istismarı problemiyle karşılaşıldı. Dolayısıyla bunun regüle edilmesi gerekiyordu. Avrupa’daki GDPR, Türkiye’deki KVKK gibi regülasyonlarda aslında biraz bunun sonucu. O kadar fazla veri toplanabilir ki bu artık insanların mahremiyetini tehlikeye atacak derecede sonuçlar doğurabilir. Regülasyonlarla bunun kontrolden çıkmaması sağlanmaya çalışılıyor. GDPR gibi yasalar, regülasyonlar yokken veri toplama daha korkunçtu. Kullanıcının izin verdiği, o sırada fark etmeden veya fark ederek izin verdiği her türlü şey kullanılarak kullanıcıyla ilgili veri toplanıyordu. Mesela kullanıcı galeri izni vermiş olsun... Uygulama açık değilken bile eskiden galerisi kullanıcının gözden geçirilerek, o fotoğraftaki konum bilgileri gözden geçirilerek o kullanıcının nerelere seyahat etmiş olduğunun verisi alınıp işlenebilir, depolanabilir, sunucularda saklanabilirdi. Böylece o kullanıcıya yönelik mesela ucuz uçak bileti önerisi yapmak üzere bu reklam toplayıcılara verilebilir gibi şeyler vardı. Regülasyonlardan sonra biraz daha bu işte dizginlenmeye çalışıyor” (K7).

“Kişisel verilerin günümüzde korunması çok zor bence. Birçok büyük firmalar bile milyonlarca insanın verilerini sızdırabiliyor. Verilerin korunması için özellikle buraya çok büyük kaynak ayrılması gerektiğini düşünüyorum. Bir de hiç görmediğimiz yani ulaşamadığımız şirketlerin, insanların kişisel verilerinizi alıp onlarla bir ton işlem yaptığını düşündüğümde işin içinden çıkılmaz bir duruma geliyor. Yani çok güvene dayalı bir ekosistem var burada. O güveni sağlamak da tabii ki karşı tarafa düşmüş durumda. Şirketlerin ve devletlerin bayağı bir önem vermeleri gerekiyor” (K8).

Kişisel verilerin korunması için çıkarılan kanunlar, mahremiyetin korunması ve verilerin kötüye kullanımın önlenmesi açısından çok önemlidir. Ancak Katılımcı 8’in de işaret ettiği “*güvene dayalı*” olan bu sistemin, yalnızca şirketler tarafından regüle edilmesi çeşitli sorunlara yol açabilir. Şirketlerin gizlilik politikaları çerçevesinde kullanıcı gizliliğini korumak için uygulamaya sokabileceği düzenlemeler elbette önemlidir; fakat bu düzenlemelerin de denetime tabi olması, devletler veya hükümetler tarafından çıkarılacak kanunlarla regüle edilmesi gereklidir. Örneğin mahremiyet endişeleri ile çevrimiçi bilgi paylaşımı arasındaki ilişkiyi inceleyen bir araştırma, hükümetlerce yapılan düzenlemelerin çevrimiçi bilgi paylaşımı üzerinde önemli bir etkisi olduğunu bulmuştur (Chaudhuri vd., 2023: 467). Öte yandan bir başka çalışma mahremiyetle ilgili endişelerin tüketicilerdeki risk algısını artırdığını (Gurung ve Raja, 2016: 1), bir başka çalışma da bu endişelerin tüketicileri alışveriş yapmaktan caydıran bir faktör olarak göstermiştir (Bowie ve Jamal, 2006: 323). Bu endişeler, mobil uygulama ekosistemi için de geçerlidir. Mobil uygulamalar özelinde denetim ve düzenleme eksikliği, kullanıcıların uygulama kullanımını etkileyebilir (Leong, 2017: 155), mobil uygulamalara ve geliştiricilere güvenin zedelenmesine neden olabilir, mobil uygulama ekosistemine ve ekonomisine ciddi zararlar verebilir.

Veri Mahremiyeti ve Gizliliğinde Geliştirici Hassasiyeti

Araştırma süresince veri mahremiyeti için kullanıcı gizliliğinin sağlanması ve kişisel verilerin korunmasının önemli olduğu, hükümetler ve şirketler tarafından atılması gereken adımların yanında geliştiricilerin de bu konuda aktif bir rol üstlenmeleri gerektiği sonucuna

ulaşılmıştır. Katılımcıların bir bölümü geliştirdikleri uygulamalarda mümkün olduğunca az veri toplamaya çalıştıklarını -ihtiyaçları doğrultusunda- belirtmişlerdir. Veri toplarken de kullanıcıların hangi bilgilerini ve nasıl toplayacakları konusunda bilgilendirdiklerini ifade etmişlerdir. Bazı katılımcılar da kimi kullanıcının uygulama izinlerini dikkate alabileceğini, böylelikle uygulamasının tercih edilebilmesi açısından kullanıcıdan talep edilecek olan veri miktarını sınırlandığı görülmüştür:

“Mesela benim kendi kişisel web sitemde kullandığım bütün teknolojiler kullanıcı verisini toplamayan teknolojiler. Ve kullanıcı verisini toplamadıkları için de aslında ücretli teknolojiler. Çünkü bir şekilde o maliyeti çıkartması lazım. Satamıyor çünkü veri toplamadığı için. O yüzden de benim yorum mekanizmamdan tutun da analitik araçlarıma kadar hepsi kişisel veriye erişmeyecek şekilde planlandı, yapıldı. Bunun için de yaklaşık ayda seksen-doksan dolar gibi bir para ödüyorum bu servislere. Böyle bir hassasiyetim var. Veri konusunda biraz hassas birisine denk geldin” (K5).

“Özellikle şöyle bir vebal hissediyorum. Kendi web sitem, sonuçta orası benim tabiri caizse çöplüğüm olduğu için oraya gelenlere o şekilde davranmayı biraz kendi boynumun borcu olarak gördüğümünden dolayı biraz hassasım; ama kullanıcı olarak takıldığım yerlerde bu kadar aşırı katı değilim açıkçası” (K.5).

“Sınırlı kalıyoruz açıkçası. Uygulama marketinden geçmeme riskini almak istemiyoruz. Açıkçası sadece analitik bilgilere ihtiyacımız var. Ne kadar oyun içinde kalmış, hangi ürünleri almış, uygulama içi satın alma varsa hangi ürünleri daha çok satın almış, hangi ürünleri almak için reklamı daha çok izlemiş? Onlara bakıyoruz ki çok fazla bir veri toplamaya ihtiyaç kalmıyor bizim genele bakmamız yeterli. Yani bireysel de bir harekete bile bakmıyoruz. Oyunumu daha iyi geliştirmem için neye ihtiyacım varsa sadece onu topluyorum” (K.9).

“Ben birkaç ay önce bir uygulama yayınlamıştım Play Store’da. Ve orada kişisel verilerin işte ben uygulamada hangi verileri topladığıma dair geliştirici olarak kullanıcılara bilgi vermek durumundayım. Vermeyenler de oluyor tabii ki. Toplamıyorum diyenler de oluyor. Ama ben kendi etik kurallarım gereği bunları sağlıyorum. Hangi verileri topladıysam kullanıcıları bilgilendiriyorum ve bunlara düzgün bir şekilde mağaza sayfasında yer veriyorum” (K.6).

“Veri toplama konusunda işime yaramayan veriyi toplamıyorum diyebilirim. Bu zaten irrite edici bir durum. Öyle elzem bir uygulamam olmadığı için, yani benim uygulamamı kullanıcının yüklemesi için arayıp bulması gerekir açıkçası. Zaten zor indirileceği için de dikkat etmem gerekir. Ama toplanan verilerde çoğunlukla Google Analytics’e gittiği için dikkat etseniz de veriyi Google çeker” (K11).

Öte yandan, Katılımcı 7, mümkün olduğunca fazla veri toplamak için uygulama mağazasının veri toplama sınırını zorlayacak kadar veri talep etmektedir. Uygulama mağazasının izin verdiği sürece veri toplamaya imkân sağladığını, veri toplarken geliştiricilere değil, uygulama mağazasının politika ve regülasyonuna güvenilmesi konusunda görüş bildirmektedir:

“Markette şu an yüklü iki tane uygulamam var. Onlar da genelde veri toplayan uygulamalar

değiller. Ama ben doğruyu söylemek gerekirse market ne kadarını zorluyorsa o kadarını almaya çalışıyorum. Mesela bana diyor ki eğer analitiği kullanıyorsan bunu ana ekrandan ulaşılabilir bir gizlilik sözleşmesi metniyle açıklamalısın. Yoksa geçemezsin incelemeyi diyor. Gidip bir tane gizlilik sözleşmesi bulup yerleştiriyorum. Ve ona bir tuş koyup oraya ekliyorum. Çünkü bunu yapmasam yükleyemem. Yani böyle bir zorunluluk olduğu için bunu yapıyorum. O yüzden bireysel geliştiricilerin vicdanına değil, marketlerin, platformların, sağlayıcıların regülasyonlarına bu iş bırakılmalı zaten” (K.7).

Öte yandan bağımsız geliştiriciler en nihayetinde platformların düzenlemeleri çerçevesinde bu verileri toplayabilir. Katılımcı 7’nin *“doğruyu söylemek gerekirse market ne kadarını zorluyorsa o kadarını almaya çalışıyorum”* ifadesi de veri toplamanın maksimize edildiğini göstermektedir. Bağımsız geliştiricilerin bu konuda hassas davranıp davranamaması, tıpkı Katılımcı 7’nin veri toplama konusundaki davranışına bakıldığında oldukça vicdanidir. Katılımcı 4 ise bağımsız bir geliştirici olarak bu verileri her şekilde toplayabileceğini, hatta kötüye de kullanılabileceğini söylemiş; ancak bunun bağımsız geliştiricilere bir faydasının olmadığını, daha çok şirketlerin bu verilerle ilgileneneğini dile getirmiştir:

“İstesek gerçekten bunları toplarız. Gözetleriz, kötüye de kullanabiliriz yazılımcılar olarak. Ama bunun yapmanın bize bir faydası olmadığını düşünüyorum. Büyük şirketler nezdinde bunun çok faydası var. Tabii ki de bunu kullanıyorlar. Manipüle etmeye açık ama bağımsız geliştiricilerin çok manipüle etmediğine inanıyorum” (K.4).

Katılımcı 9 ise veri toplamada herhangi bir sakınca görmezken, uygulamanın nasıl kullanıldığı konusunda verilere ihtiyacı olduğunu, kullanıcıyı tanımlayan herhangi bir bilginin işine yaramayacağını ve bu bilgilerle ilgilenmediğini dile getirmektedir:

“Ben bir geliştiriciyim ve bu veriyi ne için topladığımı biliyorum. Senin kişisel olarak ne olduğunun benim çok bir önemi yok. Yani benim veri toplama sebepim uygulamayı nasıl kullandığın. Kim olduğun yani umurumda değil” (K.9).

Ancak tezin ikinci bölümündeki gözetim alt yapısı kısmında da belirtildiği üzere çevrimiçi izleyicilerin kişileri tanımladığı, yani kullanıcının dijital kimliğinin gerçek kimliği ile ilişkilendirilebileceği gösterilmiştir. Katılımcı 9, kullanıcısının uygulamayı nasıl kullandığı ile ilgili analitik verileri elde etmek için Google’a bu verileri göndermektedir. Dolayısıyla geliştiricinin, kullanıcının kim olduğuyla ilgilenip ilgilenmemesi, hiçbir şey değiştirmemektedir. Veriler hem Google ürünleri yoluyla hem de Google’ın analitik araçlarını kullanan geliştiriciler tarafından yine Google’a akmaktadır.

Verinin Gözetimi

Veri sömürgeciliğini mümkün kılan bir yöntem olan veri gözetimi, çalışmanın temel

odağı olarak konumlandırılmıştır. Buradan hareketle veri üzerindeki gözetime ilişkin katılımcı ifadeleri alınmış, mobil uygulamalar çerçevesinde görüşleri aktarılmıştır. Katılımcıların tamamının gözetim kavramı hakkında bilgisi olduğu, kimi zaman gözetim olarak ifade etmeseler bile, bu kavramı izleme veya takip olarak adlandırdıkları görülmüştür. Katılımcı 6, gözetim hissini ürkütücü bulduğunu, veri gözetimine dikkat edilmesi gerektiğini ifade ederken, Katılımcı 4, veri gözetiminin oldukça kolay olduğunu, istenilen birçok veriye rahatlıkla ulaşılabildiğini belirtirken, uygulama kullanımı öncesinde verilere erişim için istenen bazı izinlerin reddi halinde hizmetin kullanılamayacağını dile getirmiştir. Katılımcı 1 ise bazı uygulamaların fark ettirmeden kullanıcıları izleyebileceğini ve buna yapılacak pek de bir şeyin bulunmadığını ifade etmiştir:

“Big Brother [Büyük Birader] hissiyatı bazen bende de oluşuyor. Bence çok hoş bir hissiyat değil. Çünkü baktığımız zaman çok büyük şirketler var ve birkaç tane var. Bunlar çok fazla veriyi ellerinde tutuyorlar. Ve bu, günün sonunda çok kötü şeylere yol açabilir. Bu yüzden de aslında veri gözetimine kullanıcıların dikkat etmesi gerekiyor” (K6).

“Verinin gözetimi çok kolay. Gerçekten de ben istediğim her veriye ulaşabiliyorum bir noktada. Sen izin verdiğin sürece, ki sen de benim hizmetimden yararlanmak için bunu kabul ediyorsun ister istemez. Yoksa benim hizmetimi alamazsın zaten. O uygulamayı yüklemene ya da o yazılıma girmene izin vermem. Bir noktada sen giriş yaparak bütün o yazılanları kabul etmiş oluyorsun. Okumadan ya da okuyarak fark etmez” (K.4).

“Mesela Pegasus diye bir mobil uygulama vardı. Casus uygulama... Hiçbir şekilde fark ettirmeden sizi izleyebiliyor. Bir sürü siyasetçi üzerinde kullanıldı diye biliyorum. İsrail merkezli bir uygulama bu. Uygulamanın genel olarak içerisine entegre edilmiş bazı parametrelerle, uygulamanın sizin telefonunuzla olan bağlantısı, direkt izin kısmını geçiyor. Yani bypass ediyor, atlıyor üzerinden. Şimdi bu da kırılmış mesela. Kırılabilir. Biz fark etmesek de aslında bizi gerçekten de izleyebilirler ve bunun için yapacak pek bir şeyimiz de yok” (K.1).

Katılımcı 3 ve 4 ise akıllı telefonların sensörlerinin veri gözetiminde kullanıldığını, bazı uygulamaların bizi gizlice takip ettiğini ve verileri üçüncü kişilere/şirketlere/hükümetlere sızdırdığını, kullanıcıların mobil uygulama kullanırken yaptığı bazı aksiyonların da veri gözetimine sebep olabileceğini dile getirmiştir:

“Ben konuştuğum bir konuyu, arkadaşım ile konuştuğum bir konu bu. Instagram’da bana reklam olarak düşüyor. Bu çok net bir şekilde bir gerçek. Sadece Instagram’da değil, büyük ihtimal Facebook’ta da düşüyordur. Çok net bir şekilde gözlemledim ben bunu. En az altı-yedi defa kendimce kanıtladım. Çünkü hiçbir şekilde aratmadığım bir şey sadece konusunu geçirdiğim anda benim karşıma çıkabiliyorsa burada sesli bir biçimde de bir veri gözetimi olduğu aşikâr. O yüzden izleniyoruz...” (K.4).

“Hatırladığım kadarıyla geçtiğimiz yıllarda TikTok’la ilgili bir olay açığa çıkmıştı. Kullanıcılarının verilerini gizlice topladığı ve bunları Çinli bazı şirketlerle paylaştığı ortaya çıktı. Hatta Çin hükümetiyle paylaştığıyla ilgili bazı haberler ortaya çıktı. ABD, bazı Çinli

şirketlere yaptırım bile uyguladı. Yani bu noktada mesela WhatsApp'tan örnek verecek olursam böyle ücretsiz uygulamalar, hizmetler aslında bir yerden para kazanmak zorunda. Mesela WhatsApp mesajlarınızı toplamıyor sizin. Mesajlarınızı paylaşmıyor ama metadata [üst veri]³⁴ dediğimiz verinin verisini paylaşıyor. Büyük şirketlerin topladığı verilerden bahsedecek olursak bunlar bizim gizlice kameramızı açıp veri toplamıyor. Zaten bu çok büyük bir skandal olur. Bunlar ne yapıyor? Bizim gönderdiğimiz mesajdaki metadatayı alıyor. Mesela siz bir kullanıcı olarak hangi saatlerde aktıfsınız? Ya da hangi konumlarda bulunuyorsunuz? Bunları topluyor ve bunları reklam amacıyla farklı şirketlere, Google, Facebook veya Meta'ya bunları satabiliyor. Yani aslında bu da bir gelir modeli. Ama yasal mı? Biliyorsunuz Mark Zuckerberg'in bir davası vardı. Uzun süre sürdü; ama ne oldu bu davada? Aslında sıyrıldı denebilir, çok da bir şey olmadı. Tabii ki bunu bir şekilde yasal zemine oturtuyorlar. Kullanıcılar ne kadar da biz onay vermedik deseler de kullanıcı sözleşmelerinin bir yerlerinde o yazıyor oluyor aslında. Ve biz kendi elimizle verilerimizi vermiş oluyoruz" (K.6).

"WhatsApp uygulamasında uçtan uca şifreleme var. Yazışmalar hiçbir şekilde bilinmiyor. Ama yazışmaların bilinmemesine rağmen yazışma sırasında uygulama açıkken konumlara izin veriyorsanız her yazdığınız kelime, her "enter" tuşuna basıp yolladığınız gönderi, sizin bulunduğunuz yerle ve saatle işaretleniyor. Ve bulunduğunuz yerleri ve saatleri kullanarak bile bu şirketler sizin neye yönelik ihtiyacınız olduğunu tespit edebiliyor veya bir çıkarımda bulunabiliyorlar" (K.3).

"Zettabaytlarca veri tutuluyor, kullanıcılara ait geçmişe dönük cihaz bazlı kullanıcı verileri. Ulusal güvenliği tehdit altına girdiğinde bununla ilgili veriler ilgili kanallara sunuluyordur diye düşünüyorum" (K.10).

Katılımcıların ifadeleri özetlenecek olursa, şirketlerin veri gözetimi için mobil uygulamaları etkin bir şekilde kullandığı ortaya çıkmaktadır. Birçok aleni, hassas ve gizli veriye erişimi olan şirketler, bu verileri çıkarları doğrultusunda üçüncü taraflarla paylaşmaktadır. İfadelerden de anlaşılacağı üzere, bu üçüncü taraflar zaman zaman reklam verenler, zaman zaman hükümetler veya devletler olabilmektedir. Bu durum gözetim literatüründe bunu sıklıkla dile getirilmiştir: Anthony Giddens (1981) gözetimi, örgütlenme için gerekli olan temel bir bilgi toplama süreci olarak tanımlamaktadır. Ayrıca şirketlerin ve devletlerin merkezi gözetim aktörleri olduğu, Oscar Gandy Jr. (1993)'ın ve Toshimaru Ogura (2006)'nın eserlerinde bulunabilir. Sonuç olarak gözetim, doğası gereği bilgi toplamaya bağlıdır (Fuchs, 2010a: 2-5) ve günümüzde çıkar gruplarının hedefinde kişisel veriler bulunmaktadır.

³⁴ Kullanıcı verilerinin büyük veriden farklı olarak daha spesifik olan (örneğin konum verisi) verileridir.

hangi verileri hangi şekillerde topladığını açıklamışlardır:

“Süreç aslında siz bir uygulamaya girdiğiniz zaman az çok başlıyor” (K1).

“Şirketler kişisel verileri genellikle web sitelerinden ve mobil uygulamalardan topluyorlar. Önceden nasıl topluyorlardı, bir form dolduruyordun veriyordun ve dosyalama sistemleri ile bunu fiziksel olarak topluyorlardı. Şimdi dijital yollardan alıyorlar ve çok daha hızlı, basit hesaplanabilir bir şekilde alıyorlar” (K.11).

“Çevrimiçi olduğumuz sürece, çevrimiçi bir hizmetten faydalandığımız sürece geliştirici tıkladığımız her ekranı, yani neye baktığımızı görebilir rahatlıkla. Ve bunun meta verilerini kaydedebilir. Şu reklama tıkladı, bu reklama çok baktı şu vakitte gibi. Neyle ilgilendi, kimi aradı gibi verileri kaydedebilir, kaydediyor da...”(K.2).

“YouTube’den konuşursak YouTube verileri nasıl topluyor? Önce YouTube’un Play Store’daki uygulamasına girip bizden istediği izinlere bakmamız lazım. Mikrofonunu kullanmak istiyorsa ve buna izin veriyorsa O zaman sesli data da topluyordur. Gün içinde telefonun yanında olduğu sürece o oradan da veri toplayacaktır. Ama eğer izinlerinde böyle bir şey yoksa öyle bir şey kullanamaz. Mağazada uygulamanın detaylarında o izin senden istenmiyorsa onu zaten uygulamanın içinde kullanamazlar. Biz kullanamıyoruz. Belki çok büyük yazılımcı ya da çok büyük şirketler bunu kullanabiliyordur” (K.4).

“Biz bir uygulamayı indirip kullanmaya başladıktan itibaren bizim hakkımızda her türlü veriyi geliştiricisine gönderir; çünkü geliştirici zaten veriyi almak zorundadır. Başlangıçta örneğin kullanıcı adı girersin, şifre girersin ya da e-posta girersin. Buradan itibaren kişisel verilerin toplamaya başlar. Klavye kullanırsın buradan senin yazma alışkanlıklarını öğrenebilir. Kamerayı kullanır. Buradaki veriyi zaten sunucuya göndermiş olursun. Senin nerede olduğunu bilgisini GSM operatörü de gönderir ama konumdan da nerede olduğunu bilir. Dolayısıyla yaptığın her işlem bir bakıma gözetim altındadır” (K.11).

Katılımcı 11’in “*her hareket bir bakıma gözetim altındadır*” ifadesi gerçekten de veri toplamanın ürkütücü tarafını gözler önüne sermektedir. Ayrıca geliştiricilerin bu verilere gerçekten de bu kadar kolay ulaşabilmesi başka bir problemliliğe işaret etmektedir. Katılımcı 10’un ifadesi de literatürde de yer aldığı şekliyle veri sömürgeciliğinin en temel özelliğine atıfta bulunmaktadır: “*Verileri toplamanın doğal bir hak gibi görülmesine.*”

“Teknolojinin daha da ilerlemesiyle aslında bu konu önem arz etmeye başladı. Mağazalarda, bunu görüyoruz. Bu kişisel verileri almak, sanki buna doğal bir hakmış gibi davranılıyor. Biz sizin hakkınızı yemiyoruz der gibiler ama aslında bütün izinleri onaylatıyorlar” (K.10).

Katılımcı 10’un “*bütün izinleri onaylatıyorlar*” ifadesi de şirketlerin, mobil uygulamalar aracılığıyla verilerden yararlanmanın ötesine geçerek, veri ile sömürgeleştirme yolunu izlediğini gösterirken, kişileri kullanıcı sözleşmelerini onaylamaya zorunlu veya mecbur bırakarak, tarihsel sömürgeciliğin taktiklerinin kullanıldığını da göstermektedir. Diğer yandan Katılımcı 4 ve 9, veri toplamanın küçük şirketler ve geliştiriciler için önemine vurgu yapmış ve veri toplama süreçlerinin nasıl işlediğini ve nasıl kullanıldığını belirtmişlerdir:

“Benim gibi ufak şirketlerde çalışanlar için bu veriler, kullanılan yazılımın ya da bir uygulamanın hizmet kalitesinin artırılması ile alakalı. Biz verileri birilerini manipüle etmek için ya da bunu satmak için kullanmıyoruz. Örneğin senin konum bilgini alıyorsam adresini kullanmak için alıyorumdur. Senin kişilerine ulaşmak istiyorsam amacım senin arkadaşını daha rahat bulmanı sağlamaktır. (...) Ama büyük şirketlerde paraya dönüştürülüyor. Bir çıktıya dönüştürülüyor. (...) ben bir geliştirici olarak ve çevremdekiler de bu verileri manipüle etmek için kullanmıyor. Çünkü bize getirisi olmayan bir şey. Bana ve firmama bir getirisi yok. Ben sadece hizmetim kadar varım” (K.4).

“Bu süreç şöyle ilerliyor. Biz oyunun reklamlarını verdiğimiz zaman örneğin Facebook üzerinden veriliyor. Bu reklamlar kullanıcının karşısına reklam çıktığı zaman tıklıyor mu? Tıkladıktan sonra uygulama marketine gittikten sonra oyunu yüklüyor mu? Bunun gibi verilerini almaya çalışıyoruz. Bu birinci aşaması. İkinci aşamada bu sefer oyun içi veriler gelmeye başlıyor. Bunun işte bazı araçlar kullanıyoruz. Oyuna ne zaman girdi. Oyuna girdikten sonra hangi seviyeye kadar ilerledi, kaçınıcı seviyeden sonra oyundan çıktı, ne kadar para harcadı, reklamları izledim mi, izlemedim mi? Onun gibi verilerini toplamaya çalışıyoruz. O gelen verilere göre de işte reklam sayısını arttırıyoruz ya da azaltıyoruz ya da diyoruz ki ikinci gün, üçüncü gün oyuna tekrar girişler az kalmış. O zaman diyoruz ki oyuncuyu oyunda tutacak bir şeyler daha eklememiz lazım? Orası eksik kalmış. Ya da ilk baştan çıkıyor. Demek ki oyunu anlamamış. O zaman tutorial [öğretici] kısmı birazcık güçlendirelim. Bu tarz veriler alıyoruz genelde. Bu da şu an bizim kullandığımız genelde analitik üzerinden isim gibi bir şey de gözüküyor bir ID olarak geliyor” (K.9).

Katılımcılardan bazılarının ifadelerine göre geliştiricilerin veri toplama amacının uygulamalarının daha da geliştirilmesi olsa da bu amaç, büyük şirketlerin de veri toplamak için en temel gerekçelerinden biridir. Ürün ya da hizmetleri iyileştirmek için kullanıcılardan toplanan veriler hem bunlar için kullanılmakta hem de üçüncü taraflara satılmaktadır. Fiziki gözetimi meşrulaştıran en temel neden nasıl savunma önlemleri ise şirketlerin ürün ve hizmetlerinin kalitesinin artırılması veri gözetimi ve sömürsünü meşru hale getiren en önde gelen nedenlerdendir.

Veri-Reklam İlişkisi

Alan gözlemlerine ve araştırma boyu alınan analitik notlara göre, katılımcıların tamamı, veri sömürsünün başlıca sorumlularından biri olarak reklamverenleri görmektedir. Katılımcı 1 ve 5’in ifadeleri dikkate değerdir ve onlara göre reklam sektörü, en fazla veri talep eden devasa sektörlerden biri haline gelmiştir:

“Veri, genelde reklam için kullanılıyor. Veri, alınıp satılan bir şey. Toplu bir şekilde alınıp satılan ve şirketler tarafından reklamcılara satılan bir şey” (K.1).

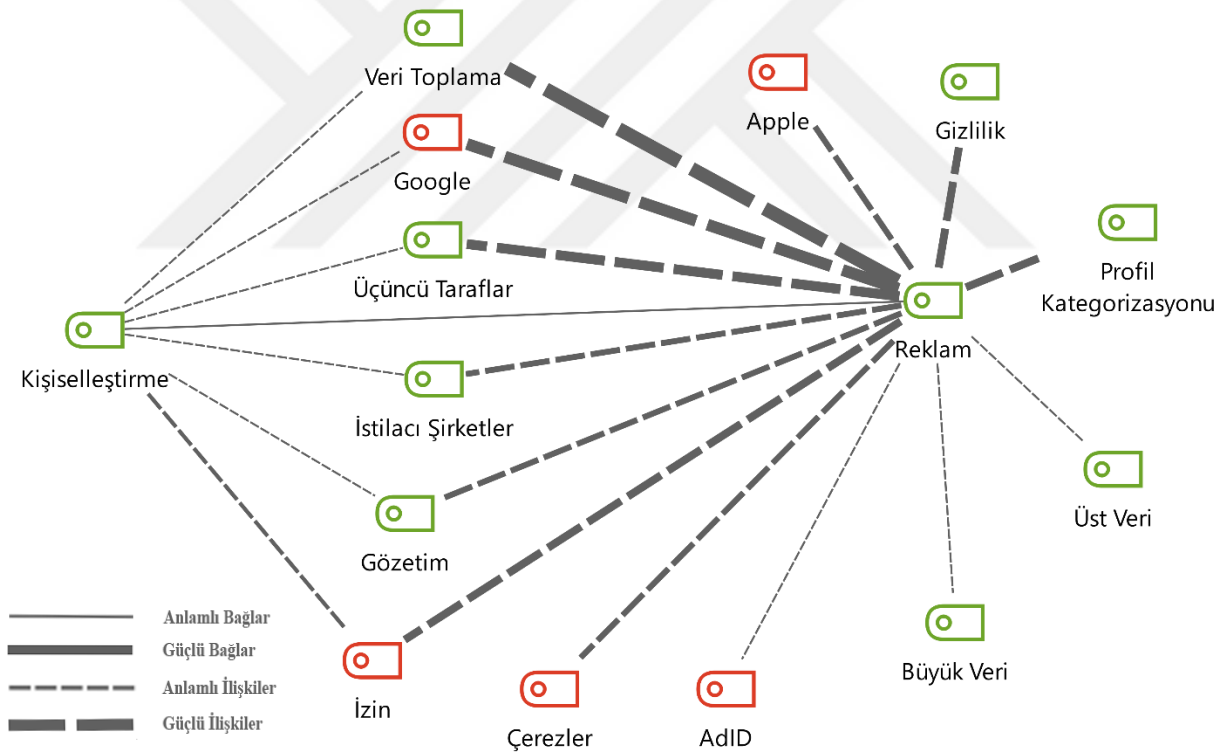
“Çok büyük pazar reklam sektörü. Google’ın gelirinin yüzde sekseni reklamlardan ki milyarlarca dolar paradan bahsediyoruz. Böyle bir geliri kimse bırakmak istemez. Bu şirketler böyle ayakta duruyorlar. O yüzden her türlü arkadan dolaşmayı yapacaklardır” (K.5).

Katılımcı 2 ise üçüncü taraf şirketlerin (özellikle reklamcılık sektörü ve analitik

şirketlerinden bahsediyor) toplumun yönelimlerini etkileyebilecek bir düzeyde olduğunu belirtirken bu durumun büyük bir problem olduğunu ifade etmektedir:

“Tekel şirketler ve bunların verdiği reklamlar bütün toplumun yönelimlerini etkileyebilir. Böyle ufak ufak doğru zamanda doğru şey göstererek. İstedikleri bir politik figürü seçtirebilir seçimlerde. Propaganda... Savaş propagandası yapıp toplumun yönelimini değiştirebilir, toplumu istediği gibi yönlendirebilir. Bu büyük bir problem” (K.2).

Buradaki ifadeler de yukarıda verilen *veri gücü* hakkındaki ifadelere benzer niteliktedir. Veriye sahip olmanın veya veriyi doğru kullanmanın önemi katılımcılar tarafından bir kez daha dile getirilmiştir. Reklam yoluyla kullanıcıların manipüle edilmesi, eğilimlerinin ya da tercihlerinin değiştirilebilir hale gelmesiyle reklam etiği tartışmaları da giderek daha fazla gündeme taşınmakta (bkz. Aral ve Eckles, 2019; Saura vd., 2021), veri-reklam ilişkisi bakımından tüketicilerin mahremiyetinin korunması, tüketici hakları bağlamında da tüketiciye doğru ve dürüst içeriklerin sunulması zorunlu olmalıdır.



Şekil 3.11 Reklam ve Kişiselleştirme - Kod Teori Modeli

Şekil 3.11’de “Reklam” temasıyla “Kişiselleştirme” alt teması arasında anlamlı bir ilişki bulunduğu görülürken, “Reklam” temasıyla “Veri Toplama”, “Google” ve “Üçüncü Taraflar” arasında çok güçlü bir ilişki vardır ve sıklıkla birlikte kodlanmışlardır. Ayrıca “İzin” alt teması, “Reklam” teması ve “Kişiselleştirme” alt teması ile güçlü şekilde ilişkilidir. Bu şekle göre yukarıda da belirtildiği gibi (bkz. şekil 3.10) veri toplama, reklamlarla

ilişkilendirilmekte, uygulama izinlerinin reklam göstermeyi ve kişiselleştirmeyi olanaklı kıldığını göstermektedir. Şekilde dikkat çeken bir diğer unsur ise hem Apple'ın hem de Google'ın reklamlarla ilişkilendirilmesidir. Ancak Google'ın reklam ile ilişkisi çok daha güçlüdür ve kişiselleştirme ile de ilişkisi bulunmaktadır. Apple ise kişiselleştirme ile ilişkili şekilde kodlanmamıştır. Bu veri, daha önce de gösterildiği (bkz. şekil 3.7) ve daha sonra da detaylı olarak değinileceği üzere Google'ın iş modelinin reklam temelli olmasıdır.

Kişiselleştirme ve Hedefli Reklam

Herhangi bir ürün veya hizmeti kullananların tercih ve ihtiyaçlarının belirlenerek tüketici memnuniyetini artırmaya dayalı bir yöntem olan kişiselleştirme, kullanıcı verilerinin kullanılarak kişileri hedef haline getiren ve kullanıcıya *daha alakalı* reklam göstermek için kategorize eden bir yapılanmaya sahiptir. Bu yöntemin kullanılabilmesi için kişisel verilere ihtiyaç vardır ve araştırma sonucuna göre kişisel verinin sömürüsü sıklıkla reklamlarla ilişkilendirilmiştir. Katılımcılardan veri-reklam ilişkisini detaylandırmaları istendiğinde, kişiselleştirmenin önemli bir unsur olduğu ve hedefli reklamlar aracılığıyla kullanıcıların ilgi alanlarına göre nasıl reklam gösterildiğini ifade etmişlerdir. Katılımcılar ayrıca sosyal medya şirketlerinin reklam ağına göndermede bulunarak, kişiselleştirilen verileri reklam ekosisteminde kullandıklarını dile getirmektedirler:

“Eskiden beri aslında zaten ticari anlamda insanların özellikle alışveriş verisi işlenmeye çalışılıyordu. Bankalar, süpermarketler, AVM’ler hep bunları toplamaya ve buna göre daha iyi satış yapabilmek ve satış pazarlama süreçlerini optimize edebilmek için bu verileri kullanıyordu. Şimdi iş bunun da ötesinde artık hayatımızın her alanında nasıl daha kişiselleştirilmiş, reklam gösterilebilir? Nasıl daha çok o kullanıcıya hitap eden içerik gösterilip o da daha çok angaje edilebilir o platformlar buna döndü” (K.7).

“Bir makine öğrenmesi algoritması tarafından senin kategorizasyonun yapılıyor. Hatta o kategorizasyonlara bu GDPR yasasından sonra Avrupa Birliği’nin o kanunundan sonra ulaşabiliyorsun. Biraz diplere saklamışlar; ama mesela senin profilin içinde mesela Fenerbahçe taraftarı diyor, metal müzik dinliyor diyor gibi böyle farklı farklı klasmanlar var. Senin hakkında arka tarafta o verileri tutuyor. Niye? Çünkü daha sonra reklam vermek isteyen birileri olursa, Facebook’tur, Instagram’dır, WhatsApp’tır. Google gibi platformlarda bu kullandıkları veriyi hedeflemek için koyuyorlar. Çünkü ben Fenerbahçe taraftarına yönelik bir ürün yapıyor olabilirim, tasarlıyor olabilirim. O reklamı o ilgi alanına sahip insanları direkt olarak gösterebiliyorum ve aslında para buradan dönüyor” (K.5).

“Örneğin Facebook örneği var önümüzde. Bizim kişisel verilerimizi alıp kişiselleştirilmiş reklamlar üzerinden gelir elde edebiliyorlar. Bunları da nasıl alıyorlar? Bizim isteğimizle alıyorlar öncelikle. En kolay yolu. Biz kendimiz isteyerek veriyoruz. Yani kullanıcı sözleşmelerini önceden okuyup onaylayarak veriyoruz. Eğer zaten öyle almıyorlarsa zaten yasal bir durum olmuyor” (K.8).

“Biz uygulamalarımızda Google’ın Admob ağını kullanıyoruz. Yani reklamlarımızı Google

sağlıyor bizim. Gösterdiği reklam üzerine büyük payı o alıyor ama bize de bir miktar reklamını gösterdiğimiz için para veriyor. (...) Kullanıcılar izin vermezse rastgele reklamlar gösteriyor. Yani yine reklam gösteriyor ama kullanıcının neye ihtiyacı olduğunu veya neyle ilgilendiğini bilmeden reklam gösteriyor. Eğer izin verirse büyük ihtimalle kullanıcı Chrome kullanıyorsa, Chrome'daki bilgilerini veya işte başka uygulamalarda reklamları varsa o tarzda bilgilerini, izin verdiği yerler varsa o bilgilerini meta dataları kullanarak kullanıcının ilgi alanını tahmin etmeye çalışıyor” (K.3).

Katılımcı 3'ün kullandığı *“Kullanıcılar izin vermezse rastgele reklamlar gösteriyor.”* şeklindeki ifade, kullanıcıların kişiselleştirilmiş reklam görmesinin onların lehine olabileceği anlamına gelmektedir. Kullanıcı, ilgisiz reklamlardan ziyade daha ilgili/ilişkili reklamlar görerek satın alma niyeti varsa ya da sonraki aramaları için ön bilgi edinebilir. Ancak kullanıcı, ilgisiz reklamlarla karşılaşlıyorsa kullanıcının mahremiyeti de bir anlamda korunmuş olur. Aksi takdirde davranış verileri, hâlihazırda dolaşımdadır ve mahremiyeti tehlike altındadır.

Verilerin Hâkimiyetinde İstilacı Şirketler

Veriye bağımlı birçok şirkette olduğu gibi uygulama mağazalarını istila eden ve mobil uygulama ekolojisinin en önemli aktörlerinden olan şirketler, kişisel verilere hâkim olmak için ürünlerini öyle bir noktaya taşımıştır ki bugün, sıklıkla kullanılan hatta gün geçtikçe neredeyse zorunluk haline gelen yazılımlar birçok insan için vazgeçilmez olmuştur. Ancak, katılımcılardan bazıları bu durum farkındadır ve bazı katılımcılar bu ürünleri kullanmaktan imtina etmektedir. Katılımcıların bu yazılımları kullanmama tercihlerine ilişkin ifadelerine aşağıda yer verilmiştir. Ayrıca katılımcıların istilacı şirketlerden bahsederken, tekelleşme, rekabet ve mülksüzleştirme kavramlarına atıf yaptıkları görülmüş, Katılımcı 2 ve 4, kullanım zorunluluğunu alternatifsizlikle bağdaştırmıştır:

“Google'dan uzak durmaya çalışıyorum ama bir yere kadar durabilirsin. Çünkü YouTube'un bir alternatifi yok. Bu tekel şirketler sadece bir takım devlet müdahaleleriyle durdurulabilir. Tasmaları böyle birazcık daha kısa tutulabilir. Muhtemelen bu aşamada kimse çıkıp da ben de kendi işletim sistemimi yapıyorum diyemez artık. Zaten en büyük problem de işletim sistemine bağlı. Problem bu ekosisteme mecbur kalıyor olmamız” (K.2).

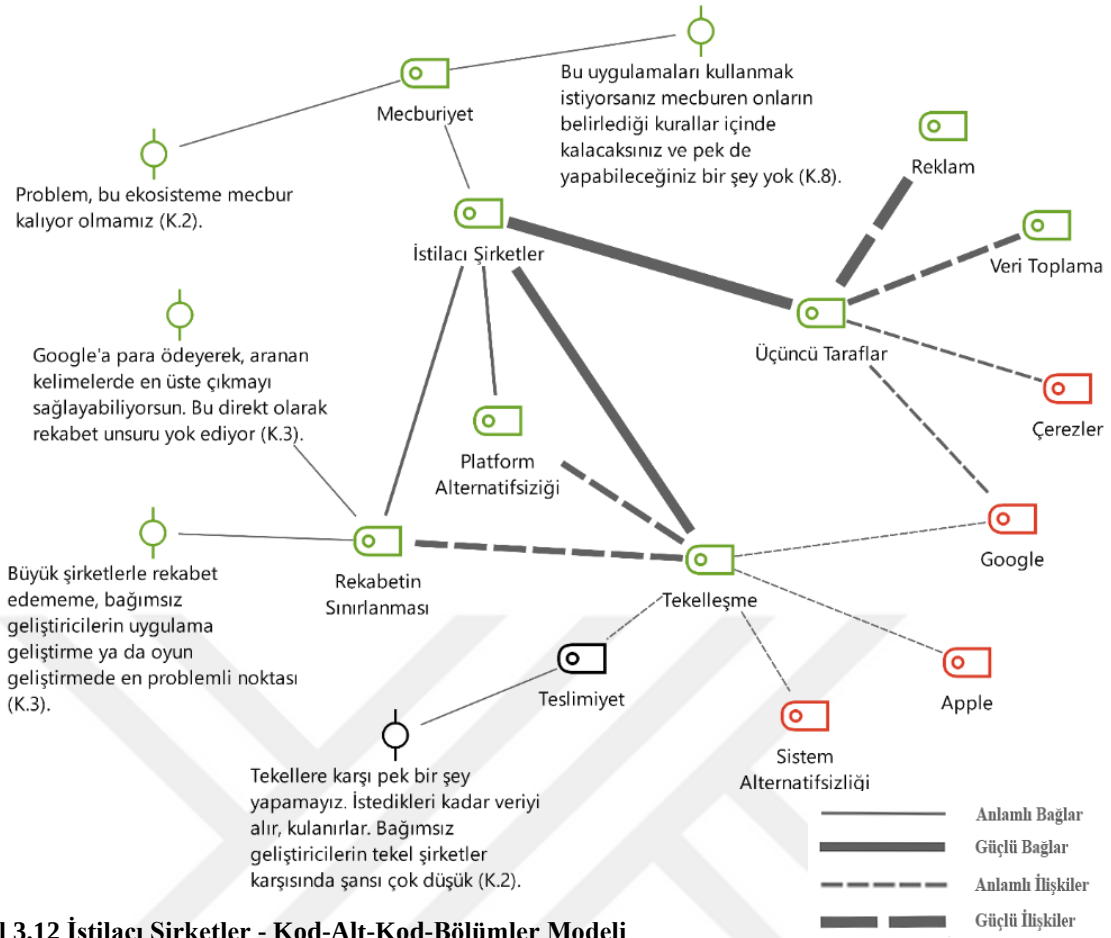
“Büyük yazılımlarla donanım üreticileri bunlar. Tekeller bu konuda. Muadilleri yok. Tercih edilmek zorundalar. Bunu da bir faydaya dönüştürüyorlar. Bu tekel şirketler rekabet unsurunu ortadan kaldırıyor. Apple bunu yapıyor son zamanlarda. Mevcutta olan uygulamayı yeni iOS sürümünde kendi içine dâhil ediyor ve o uygulamayı bitiriyor. Bir araç var mesela örnek veriyorum klavye olsun bu, klavyeyi farklı temalarda kullanmanızı sağlayan bir uygulama olduğunu düşünün. Apple bir dahaki iOS sürümünde bunu telefonun içine gömüp seni bitiriyor. Ya da AdJust var bir ödeme yöntemi. Apple diyor ki kardeşim içeride sen sadece uygulama içi satın almayı Apple Cüzdanınla yapabilirsin. Bu sefer ne oldu? Adjust gibi RevonueCat gibi dışarıdan sana ödeme hizmeti sağlayan şirketlerin değeri bir anda yüzde yirmi düştü. Hemen kendi yararına kullanabiliyor, tekelleşebiliyor. Yasa dışı bir iş de yapmış

oluyor burada. Aynı şekilde Google’da hizmetlerinde kendi hizmetlerini öne çıkaracak şeylere gidiyor. (...) örneğin haritalarını kullanıyorsam ben, beni her zaman engelleyecek unsurlar koyuyor. Kendi istediği hizmetleri daha fazla öne çıkarabiliyor yani. Bunu oldukça kullanıyorlar diyebilirim hem uygulama marketlerinde olsun hem de hizmetlerinde” (K.4).

“Aslında şöyle bir örnek vermek isterim. Mobil uygulamalar özelinde değil ama onu kapsayan bir konu. Baktığımızda biraz da şirketlerin rekabet etmesi gerekir. Örneğin Microsoft Activision Blizzard’ı satın almaya çalışıyordu ve rekabet kurumu Microsoft’u mahkemeye verdi. Oyun yapım şirketi Activision. Burada tekel olmasının önüne geçmeye çalışıldı. Mobil uygulamalarda da aynı şekilde. Uygulama mağazalarında da tekel olan şirketler var. Çok fazla uygulaması olan işte Clash of Clans var. Bunun mesela çatı şirketi olan Tencent var. Bir sürü oyun şirketinin sahibi. Oyunlardan örnek vermemin sebebi genellikle oyunlar en çok indirilen uygulamalar oluyor. Ve en çok kullanılan. Aslında bu hoş bir durum değil. Çünkü öncelikle rekabetin önüne geçiyor. Ayrıca veri güvenliği noktasında da sıkıntılar yaratıyor. Bu şirketlerin veri güvenliğiyle ilgili konuya nasıl baktığı da önemli. O şirketler mesela etik kurallarını ne kadar önemsiyor? Açıkçası bu benim tamamen şahsi düşüncem, Tencent Çin merkezli bir şirket. Merkezi Çin’de olan şirketlere hiç güvenmiyorum. Özellikle TikTok’a. Bunların sürekli gizlice verileri topladığı ortaya çıkıyor. Geçtiğimiz yıllarda zaten bir sürü bunlarla ilgili olay oldu. O yüzden açıkçası ben mobil uygulama yayınlanan mağazalarda bu şekildeki baskın şirketlerin olmasına karşıyım. Bununla ilgili kim ne yapabilir dersek bununla ilgili en fazla bu mağazaların sahibi olan şirketler işte Google ya da Apple bazı adımlar atabilir. Bağımsız geliştiricilerin geliştirdiği uygulamaları daha çok öne çıkarmak olabilir ki bu daha çok uygulamanın geliştirilmesinin de aslında önünü açar” (K.6).

“Bu şirketler olmasaydı ne olurdu bunu düşünüyorum da birçok yerel uygulama ya da bireysel uygulama olurdu ve bu kadar genişleyemezdi bu piyasa diye düşünüyorum. Bir yandan da bu şirketlerin aşırı derecede büyümesi ile her şeyin ele geçirilmesi, pazarın tamamı ile kontrol altına tutmasıyla işte bireysel start-uplar diyelim bunların önünü kesiyor açıkçası. Bu büyük teknoloji şirketleri çok daha fazla yatırım yapabiliyor sonuçta ve argeleri ciddi rakamlarda yatırım oluyor. Dolayısıyla bu şirketlerle kapışmak çok zor hale geliyor” (K.11).

Katılımcı 6’nın “... mobil uygulama yayınlanan mağazalarda bu şekildeki baskın şirketlerin olmasına karşıyım.” ifadesi “... Google ya da Apple bazı adımlar atabilir” ifadesiyle çelişkilidir; çünkü bu iki şirket de Tencent gibi istilacıdır. Katılımcı 6’nın regülasyonu bu iki şirketin yürütmesi gerektiği belirtmesi, Katılımcı 7’nin benzer şekildeki “marketlerin, platformların, sağlayıcıların regülasyonlarına bu iş bırakılmalı zaten.” ifadesine benzer bir ifadedir. Burada sorulması gereken soru şudur: Mobil uygulama mağazalarını istila eden şirketler, istila ettiği alanları mobil uygulama ekosisteminin tüm aktörleri için aynı eşitlikte düzenleyebilir mi? Öte yandan Katılımcı 11’in ifadeleri de bir yandan bu şirketlere olan ihtiyacı vurgularken, bir yandan da bu alanı kontrol etmesiyle yaşanan problemleri dile getirmiştir. Görüldüğü üzere, bağımsız geliştiriciler de aslında çelişki içerisinde.



Şekil 3.12 İstilacı Şirketler - Kod-Alt-Kod-Bölümler Modeli

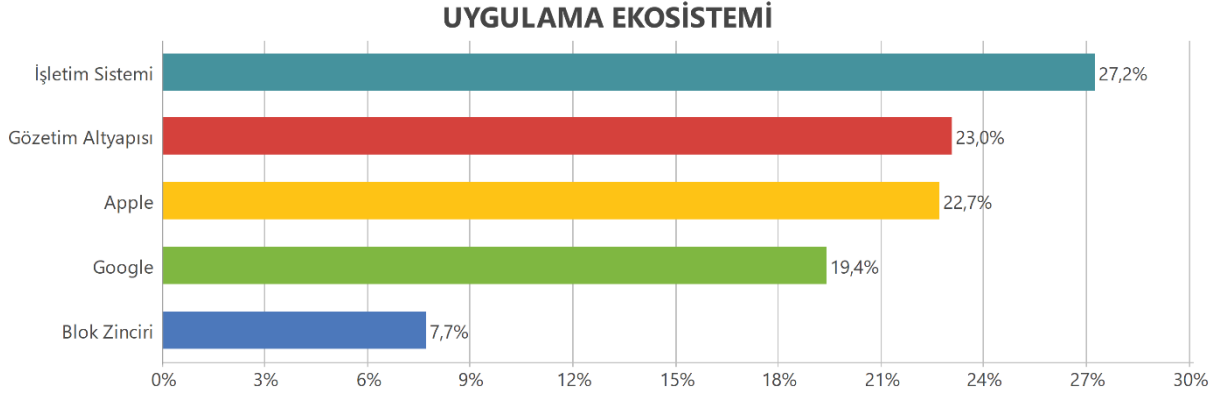
Şekil 3.12’de gösterildiği üzere “İstilacı Şirketler” temasıyla “Üçüncü Taraflar” ve “Tekelleşme” alt temaları arasında güçlü bağlar vardır ve katılımcı ifadeleri bu temalara sıklıkla kodlanmıştır. “Üçüncü Taraflar” alt teması, “Reklam” ve “Veri Toplama” ile güçlü şekilde ilişkilendirilmiştir. Ayrıca şekil 3.17’de “Tekelleşme” “Rekabetin Sınırlanması” ve “Mecburiyet” temalarına ilişkin katılımcı ifadelerine yer verilmiştir. Şekle göre istilacı şirketler katılımcılar tarafından tekelleşmiş, rekabeti sınırlayan ve kullanıcıları alternatifsiz bırakan -ürünlerine bağımlı hale getiren-yapılanmalar olarak görülmektedirler.

3.2.3.2. Katılımcıların Mobil Uygulamalarda Gizlilik, Güvenlik ve Gözetime İlişkin Yaklaşımlarının Analizi

Apple ya da Google kullanıcılarının gizliliklerini koruyabilir. Peki biz kendimizi Apple veya Google’dan koruyabilir miyiz? (K.6).

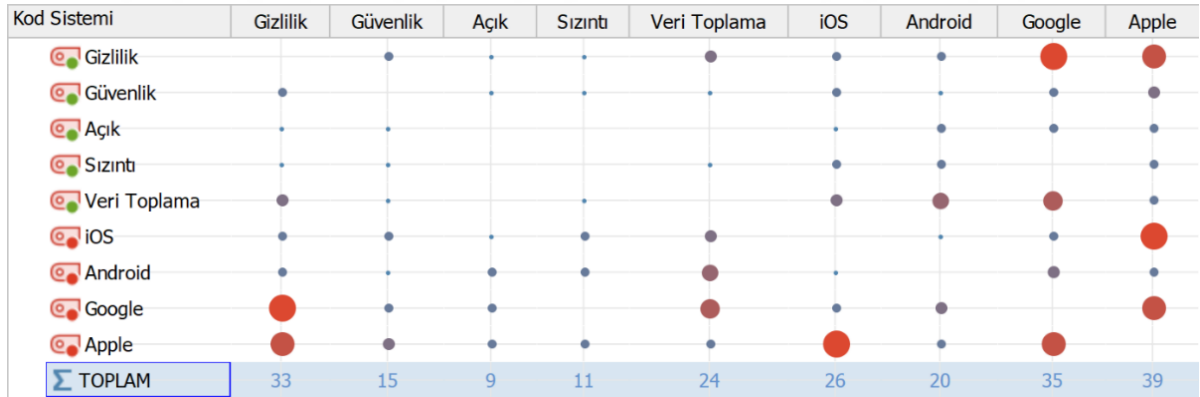
Bu kategori altında katılımcıların mobil uygulama ekolojisinde var olan gözetim alt yapısına dair detaylı bilgiler elde edilmiştir. Ayrıca katılımcıların merkezi uygulamalar

karşısında merkezi olmayan uygulamaların nasıl konumlandığı konusundaki düşüncelerine yer verilmiştir.



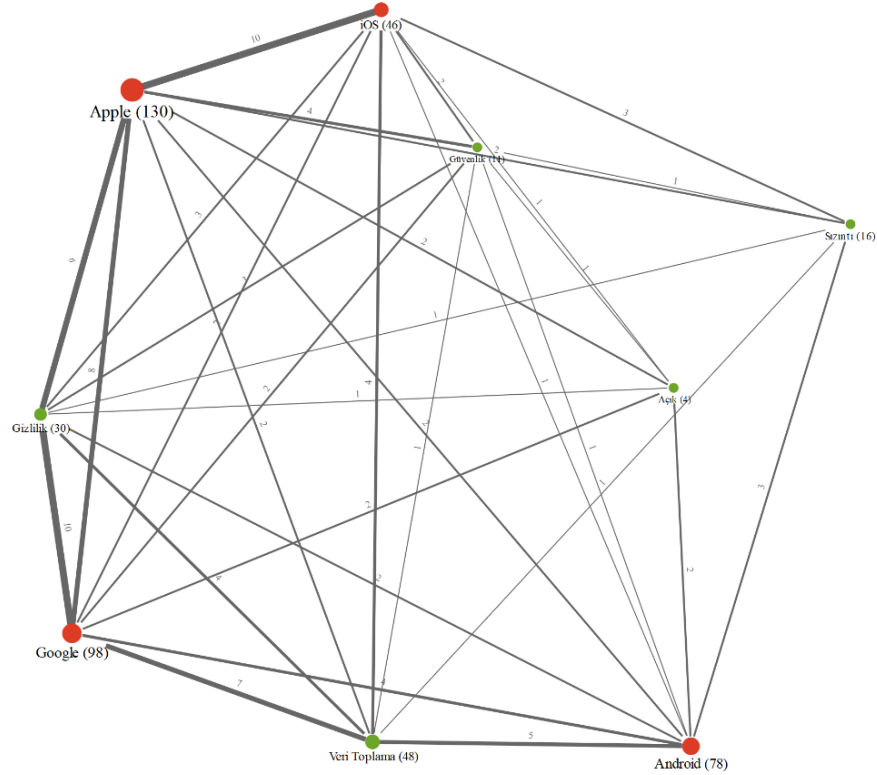
Grafik 3.6 Uygulama Ekosistemi Kategorisinde Yer Alan Temaların Kod İstatistiği

Grafik 3.6’da gösterildiği üzere “Uygulama Ekosistemi” kategorisi altındaki kodlamalar en çok “İşletim Sistemi” ve “Gözetim Alt Yapısı” temalarına yapılmıştır. Katılımcılar, işletim sistemleri ve uygulamaların gözetim alt yapılarından bahsederken aynı zamanda sıklıkla Apple ve Google’dan bahsetmişlerdir. “Uygulama Ekosistemi” kategorisinde sıklıkla birlikte kodlanan temalar da aşağıda verilmiştir:



Grafik 3.7 Uygulama Ekosistemi Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri

Şekil 3.7’de gösterildiği üzere katılımcıların ifadeleri, en çok “Apple” ve “Google” temasıyla ilişkilendirilmiştir. “Gizlilik” teması ve “Veri Toplama” alt temasının da “Google” ve “Apple” temalarıyla ilişkili olduğu görülmektedir. Aşağıda verilen şekilde ise bu temalara ait kod haritası verilmiştir:



Şekil 3.13 Uygulama Ekosistemi Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası

Şekil 3.20’ de görüldüğü üzere “Uygulama” kategorisi altındaki “Apple”, “Google” ve “Gizlilik”, temaları birbirleriyle yakın ilişki içerisinde olup sık bir biçimde kodlanmıştır. “Android” ve “iOS” temaları ise “Veri Toplama” alt teması ile sık kodlanırken, “Sızıntı” ve “Açık” alt temaları diğer temalarla daha uzak bir ilişki içerisinde. Ayrıca şekle bakıldığında temalar arasındaki ilişkilerin nispeten dengeli dağıldığı görülmektedir. Ancak katılımcılar, konu güvenlik olduğunda Apple ve iOS işletim sisteminin Google ve Android işletim sistemine kıyasla güvenlikle daha fazla ilişkilendirdikleri anlaşılmaktadır.

Mobil İşletim Sistemlerinde Gizlilik ve Güvenlik

Mobil işletim sistemleri, mobil uygulama ekolojisi için büyük önem taşımaktadır. Cep telefonların üretilmesinden bu yana birçok işletim sistemi üretilmiş, akıllı telefonların ortaya çıkışıyla birlikte bu trende ayak uydurabilen mobil işletim sistemleri hayatta kalmıştır. Günümüzde ise mobil işletim pazarı iOS ve Android işletim sistemlerinin hakimiyetindedir. Bu durum mobil işletim sistemlerinin kişisel veri gizliliği ve güvenliği zemininde incelenmesini gerekli kılmıştır. Katılımcılardan kullanıcı verilerinin korunması bağlamında (sızıntı, veri toplama ve veri koruma) Android-iOS işletim sistemleri arasında karşılaştırma yapmaları istemiş ve ağırlıklı olarak Android işletim sistemi kullanan uygulamaların daha fazla veri sızdırabileceği ve bu uygulamalardan daha fazla veri toplanabileceği ifade

edilmiştir. Android işletim sisteminin açık kaynak kodlu olduğuna dikkat çeken katılımcılar, iOS'un kapalı bir sistemini olduğuna ve kendi ekosistemi içerisinde hareket etğine dikkat çekmişlerdir:

“Şu anda baktığımız zaman Android eskiye göre daha da gelişti. Yani kapalı bir sistemi yok. Bu zaten Android'in bir özelliği aslında. IOS'da uygulamanın kendi tarafları korunuyor” (K.1).

“Muhtemelen Android'de daha kolaydır. Ama Apple da pek farklı değil artık. Apple eskiden mahremiyete oldukça önem veren bir markaydı ve şöyle diyebiliyordu, paran varsa al ben senin verinle ilgilenmiyorum. Sende diyordun Apple alayım ki birazcık daha mahremiyetim korunsun. Şimdi Apple'da da öyle bir şey yok. Öte yandan Android'in birçok farklı sürümü var. Bu yüzden muhtemelen çok daha fazla açığı vardır. O yüzden muhtemelen Android'den veri toplamak daha kolay olabilir” (K.2).

“IOS yıllardır güvenlik üzerine, işletim sistemi güvenliği üzerine çalışan bir işletim sistemi. Apple bu konuda çok sert. Mağazadaki uygulamalarını çok sıkı denetliyor. Herhangi bir hata da kaldırılabiliyor uygulamaları. Google tarafında bu uzun süredir böyle değildi, gizliliğe, kullanıcı verilerine bu kadar dikkat edilmiyordu; ama son işte iki üç yılda Google'da bu noktalara dikkat etmeye başladı. Google'da burada katı önlemler almaya başladı. Yani aslında baktığımızda iOS'un biraz daha güvenilir olduğunu söylemek bence yanlış olmaz. Hem kendi cihazları, Apple'ın geliştirdiği cihazlar, sınırlı sayıda cihazlar. Ama Android tarafında öyle değil. Milyonlarca cihaz var bir işletim sistemi üzerinde. Android daha esnek bir işletim sistemi. Veri sızıntısı da muhtemelen daha çok olacaktır diye düşünüyorum” (K.6).

“Şu an artık çok yakın birbirine; ama belki bir tık daha Apple için daha güvenli diyebiliriz. Gitgide Google'da bunu engellemek üzere adımları attı. Ama Android'in yapısı, doğası gereği yani açık kaynak kodlu bir işletim sistemi olması, özelleştirmeye açık olması, kullanıcıya özgürlük alanı vermesi, geliştiricilere özgürlük alanı vermesi aslında böyle bir sonucu doğurdu. Kötü niyetli yazılımcıların, kötü niyetli geliştiricilerin kullanıcıların farkında olmadan bir şeyler yapabilmesine aslında yol açtı. Mesela eskiden bazı virüsler ve kötü yazılımlar vardı. Kullanıcı o sırada telefonun başında değilse; ama ekran açıksa mesela, belli ekranda reklamlar gösterip sanki kullanınca ona bakıyormuş gibi oradan para kazanan veya kullanıcının telefonunu bir nevi zombi cihaza çevirip istediği gibi ele geçirebildiği bir dönem vardı. Daha kolaydı çünkü arka planda uygulama çalıştırmak izne tabi değildi. Ama son birkaç senedir artık bu tarz konuların gündeme gelmesiyle Apple'ı yakaladı diyebiliriz. Şu anda benim bildiğim Apple'daki ekstra bir fark, kişiselleştirilmiş reklamın artık ayarlardan yönetilebiliyor olması. Yani ben işte kişiselleştirilmiş reklam istiyorum ya da istemiyorum gibi ayarlardan yönetilebiliyor ve böylece uygulamalara aslında bayağı zorluk çıkarıyor. Kişiselleştirilmiş reklam göstermek isteyen uygulamalara ya da bununla ilgili veri toplamak isteyen uygulamalara zorluk çıkarıyor. Yani şu an Apple bir tık daha önde gidiyor. Bu kullanıcı tarafına daha yakın gidiyor Google'a göre” (K.7).

“Apple gizliliği koruyabilir evet, zaten geliştirdiği cihazlar belli. Hani habitatı belli öyle diyeyim. Sınırlarını biliyor, cihazın sınırlarını biliyor, platformun sınırlarını biliyor, kendisi kontrol ediyor zaten. O yüzden bunu sağlayabilmesi, koruyabilmesi çok mümkün. Android tarafına baktığın zaman binlerce cihazda çalışan bir sistemi var. O yüzden şunları sınırlayın, bunları sınırlayın diyebilmek çok mümkün değil. Yani çok geniş bir skala var orada mühendislik açısından. Bu yüzden gizliliği koruyabilmek çok zor olsa gerek diye düşünüyorum; ama Apple tarafında evet bunu yapması gayet mümkün. Zaten her şeye izin vermiyor, bütün dosyalara erişimine bile izin vermiyor. Yani Apple tarafın izin verdiği kadar yerlere erişebiliyorsun. Sınırlar çok net olduğu için bilgiyi koruması da dahil mümkün” (K.9).

Yukarıda verilen ifadelerle göre platform yönetimleri arasında farklılık bulunmaktadır ve mobil uygulama platformlarını araştıran bazı çalışmalarda da bu farklılık gösterilmiştir. Örneğin, Google'ın Android platformunun kurallarının Apple'inkinden daha az katı görüldüğü belirtilmiştir (bkz. Nieborg, 2016). Ayrıca, Android'in iOS'a kıyasla güvenlik ihlallerine ve kötü amaçlı yazılım saldırılarına daha fazla yatkın olduğu (bkz. Garg ve Baliyan, 2021), Google'ın platformunun Android kullanıcılarının meta verilerinin toplanmasını kolaylaştırdığı ve özellikle konum hizmetlerinin meta verilerin toplanmasına olanak sağladığı gösterilmiştir (bkz. Spreeuwenberg ve Poell, 2012). Öte yandan Katılımcı 4 tam tersi görüş bildirerek iOS'a kıyasla, Android işletim sisteminin veri toplamayı kolaylaştıran bir sistem olduğunu ifade ederken, Katılımcı 11, Katılımcı 4'ün tersi görüş bildirmiştir:

“Mobil cihazlarda iOS önerir misin desen? iOS daha sıkıntılı bence baktığın zaman. Apple daha kapalı kutu çalışıyor. Örneğin Android'de Google hizmetlerini kurmak zorunda değilsin. Veri toplayan hizmetlerini. Haritaları bugün silebiliyorsun telefonundan; ama Apple'da öyle bir şey mümkün de değil. Güvenlik olarak daha güvenli olabilir. Mesela iCloud'una sızılması - ki bu da oldu defalarca- Android telefonuna sızılmasından daha zor olabilir. Bu konuda iOS daha güvenli olabilir, hackerların eline geçmesi konusunda. Ama veri toplanması açısından ben iOS'u daha zararlı buluyorum açıkçası” (K.4).

“Android ve iOS işletim sistemleri birbirinin zıttı gibi gözükse de benzer şekilde çalışıyor. Birisi daha kapalı bir sistem o kadar. Ben de bir Android geliştirici olarak Android daha iyi diyebilirim. Şu yönden elbette Android kullanan kullanıcı sayısı Apple'a göre daha fazla dolayısıyla onun için yazılabilecek zararlı yazılımlar da daha fazla. Önceden denirdi Microsoft ürünlerine yani Windows'a çok virüs bulaşır ama Mac bilgisayarlara bulaşmaz. Bunun da bir nedeni biraz önce dediğim gibi çok daha fazla kullanılmasıdır. Ancak biz Apple'ın bu kapalı sisteminin ileride nasıl kullanılacağını bilmiyoruz. İki işletim sisteminde de veri bir şekilde toplanıyor ama Android uygulamalar daha fazla veri topluyor diyebiliriz. Biraz önceki nedenlerden dolayı da aynı zamanda çünkü çok daha fazla uygulama hem uygulama marketinde var hem de daha fazla yazılıyor” (K.11).

Katılımcı 4, iOS'un Android'e kıyasla güvenlik açısından daha güvenilir olsa bile, veri toplama açısından daha zararlı olduğunu dile getirmiştir. Katılımcı 11'de benzer düşündedir; fakat Android'den daha fazla veri toplandığını kabul etmekte, bunun nedenini de Android uygulamaların iOS'a göre daha fazla olmasından kaynaklı olmasıyla açıklamaktadır. Buna göre katılımcıların herhangi bir platforma tam olarak güvenmedikleri ortaya çıkmaktadır. Hem Google hem de Apple veri konusunda katılımcıların güvenini kazanamamıştır.

Mobil Uygulamalar ve Gizlilik

Mobil uygulamalar, kullanıcıların internet ortamına veya sosyal medya platformlarına ulaşması için kullanılan basit yazılımlar değildir. Mobil uygulamalar, kullanıcılarını tanıyan, onun hakkına birçok bilgiyi barındıran ve bu bilgileri aktarmayı olanaklı kılan oldukça etkili

ve önemli yazılımlardır. Bu yazılımlardan bazıları kişisel verileri sızdırabilmekte, kullanıcının gizliliğini ve kişisel veri mahremiyetini tehlikeye atabilmektedir. Bu nedenle Katılımcılar, uygulama ve gizlilik sorularına farklı açılardan yaklaşmışlar, bazı katılımcılar gizliliği veri toplamayla, bazıları ise bırakılan dijital izlerin kullanılmasıyla ilişkilendirmişlerdir. Katılımcı 3, mobil uygulamalardaki gizliliği tehlikeye atan en önemli şeyin kullanıcıların arkasında bıraktığı dijital izler olduğunu vurgulamış, bu izler sayesinde hangi saatte nerede olduğu öğrenilen kullanıcılara reklam gösterildiğini ifade etmiştir:

“Uygulama ile fotoğraf çektiğinizde o fotoğraf belirli etiketlerle kaydediliyor. Yani şurada şu saatte çekildi gibi bilgiler oluyor verinin içinde. Yazışmalar da böyle, her attığınız post bir şekilde etiketleniyor. Yazının içeriğinin bir önemi yok. Ama siz o yazıyı saat öğlen on ikide bir AVM’de attıysanız ve siz bunu belki üç beş gün boyunca sürekli yaptıysanız sizin öğlen vakti her gün AVM’ye gittiğinizi öğrenmiş oluyor. Belki yemek yediniz, oradan çıkarım yapıyor ve size o saatlerde ve oynadığınız oyun varsa veya kullandığınız uygulamada reklam gösterimi varsa yemekle ilgili reklamlar gösteriyor. Mesela Facebook sayfanızı açtığınızda uygulamanızda önünüze reklam olarak yemekle ilgili reklamlar gelebilir. Sadece belirli yerde, belirli saatte sürekli mesaj attığınız için veya arkadaşlarınıza mesajlaştığınız için” (K.3).

“Benim gördüğüm ve okuduğum kadarıyla ve haberlerde de görmüştüm TikTok, kullanıcısının batarya seviyesinden tutun da yani telefonunun her şeyini alıp yani Çin’e yollayabiliyor. Devasa büyüklükte ve güçte. Bunları rahatça depolayabiliyor en önemlisi bu. Bunları almak bir mesele bir de depolamak var. Depolayabiliyor. O güçte uygulamalar var” (K.8).

Katılımcı 8 ise gizliliğin, veri toplama ve depolama yoluyla tehlikeye atıldığını ileri sürmüştür. Katılımcı 8’in veri gizliliği konusunda Çin merkezli şirketlere gönderme yaparak sunduğu bu yaklaşım, global ölçekte rekabet halinde olan iki ülkenin –Çin ve Abd-veri toplama ve depolama konusunda da rekabet içerisinde olduklarını göstermektedir. Katılımcı 5 ve 11 ise mobil uygulamalardaki reklam kimliklendirme sistemine dikkat çekmiş, Katılımcı 5 AdID’nin nasıl kullanıldığını açıklamıştır:

“AdID diye bir şey var. Reklam kimliğini, yani senin verilerini o ID ile eşleştirip gönderiyor şirkete” (K.11).

“Mobil uygulamalarda şöyle bir sistem vardı. Apple’ın her kullanıcı için özel olarak oluşturduğu AdID dediğimiz bir sistemi vardı. Cihaza ve kullanıcıya göre özeldi. Ve mesela eşlemek için yine Google Analytics vb. gibi araçlar kullanıyorlardı. Mesela bir uygulamada analitik yüklüyse veriyi oradan alıyordu. Senin mobil uygulamadaki ilgi alanlarında, web’deki ilgi alanlarını birleştirebiliyordu bir havuzda. Ama Apple yakın zamanda bir izin sistemi getirdi iOS’ta. Beni takip etme! Takip etme iznini soruyor size. Üçüncü parti şirketler ayrıca takip edebilir mi diye. Birçok uygulama artık bunu gösteriyor. Söylemek zorunda, yoksa kabul etmiyorlar. Ona izin vermediğiniz takdirde o verilen ID “sıfır sıfır” olarak geliyor. Bir sürü sıfır olarak giriyor. Böylece senin kim olduğunu tam olarak algılayamıyorlar. O noktada işte o senin takibin bir anda kopmuş oluyor uygulama içerisinde. Yani Cookies yerine bir ID var. Onun üzerinden gidiyor her şey. Teknik olarak söyleyecek olursam böyle” (K.5).

Erişim İzinleri ve Çevrimiçi İzleyiciler

Mobil uygulamalarda gizlilik ve mahremiyet kaynaklı sorunların genellikle uygulamaların daha iyi çalışabilmesi için entegre edilen gözetim araçlarıyla mümkün olduğu bilinmektedir. Buradan hareketle katılımcıların mobil uygulamalardaki erişim izinleri ve çevrimiçi izleyiciler hakkında görüşleri alınmıştır. Uygulama izinleri ile ilgili Katılımcı 4'ün ifadesine göre bu izinlere karşı olumsuz bir bakış açısı söz konusudur. Oysaki Katılımcı 4'e göre erişim izinleri, uygulamanın çalışması için ya da bir işlevi yerine getirebilmesi için gereklidir:

“Mesela telefonun ekranını açık tutma, uykuya dalmasını engelleme. Burada aslında biz her şeye öcü gibi bakıyoruz. Bu noktada örnek vereyim. Çünkü ben de yaptığım bir uygulamada bunu kullandım. Ama kullanma sebebim oyun oynarken ekranın kapanmasını engellemek. Çünkü anlık olarak tepki vermesi gereken bir oyun. Soruyu bilirse cevaplıyor ve otuz saniye boyunca durduğu zaman ekranı kapanıyor. Çünkü zaman aşımına uğruyor ve bunu engellemek için koydum” (K.4).

Katılımcı 4'ün ifadesi geçerli olabilir; ancak önemli olan uygulama izninin geliştirici tarafından nasıl kullanıldığıdır. Katılımcı 10, bunu net bir şekilde ifade etmektedir:

“Siz konum servisinin bilgisini veriyorsunuz, iznini veriyorsunuz. Servis kullanım hizmetini açtığınız zaman orda geliştirici özgür. Siz bu özgürlüğü kaybetmiş oluyorsunuz aslında. Orada artık konum servislerinden açtıktan sonra belki arkada bir servis başlatarak full bir takipte yapılabilir. Ya da başka verilere erişebilir” (K.10).

Mobil uygulamalardaki AdID'nin hem Google'da hem de Apple'da kullanıldığı, tezin ikinci bölümünde dile getirilmiş, ayrıca “Mobil Uygulamalar ve Gizlilik” başlığı altında Katılımcı 5'in AdID'nin nasıl çalıştığı konusundaki ifadelerine yer verilmişti. Bu tanımlayıcıların veri toplama ve dijital iz takibinin dışında, uygulamalar arası kullanıcı gizliliğini etkileyebilecek bir uygulama olduğu yine Katılımcı 5'in detaylı ifadesiyle ortaya çıkmıştır:

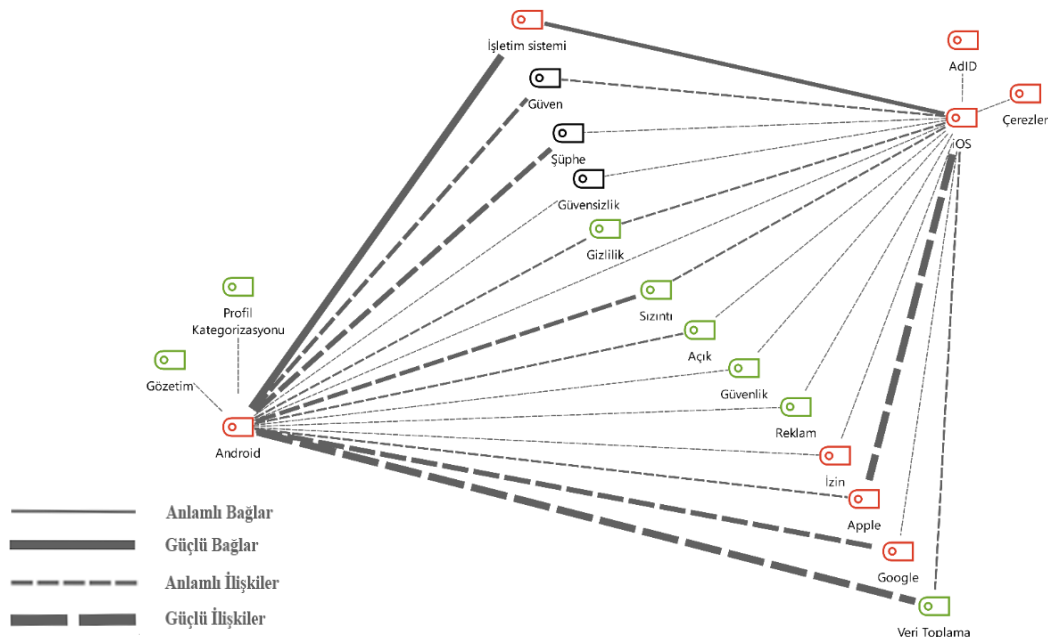
“Uygulamalarda bir ID'si var herkesin. Kimlik numarası gibi düşünebiliriz. O kimlik numarası, uygulamalar arasında hep aynı kalıyor, hiç değişmiyor. Senin hangi uygulamayı açtığına, o kimlik numarasını kaydederek bakıyor sistemler. O kimlik numarasını paylaşmadığınız zaman sen uygulamalar arasına geçiş yaptığın zaman senin o olduğunu anlayamıyor diğer uygulamalar. Çünkü o kimlik numarasına erişemiyorlar. Erişemediği için bir eşleştirme yapamıyor arka tarafta. Ama tabii sen şimdi Instagram'a üye oldun. Hesap açtın, fotoğraf yükledin. O veri Instagram'ın sunucularında duruyor. Senin profilinin altında ve Instagram bir veri sızıntısı yaşadığı zaman aslında o veri sızıntısı senin verilerini de sızdırmış oluyor. Yani bizim sonuçta verilerimiz o ürünlerin sunucularında duruyor. Buradaki olay sadece senin reklam amacıyla yaptığın davranışları takip edip sana ona göre reklam göstermemesini sağlamak. Bu Instagram için de geçerli değil. Çünkü Instagram içerisinde yine veri, kendi makinesine logladığı için ve uygulama kartında zaten bu verileri okuyorum diye beyan ettiği için onda bir sakınca yok. Ama sen Instagram'daki kullanıcı adını

Hepsiburada'daki kullanıcı adıyla eşleştiremiyorsun. Bu sefer Hepsiburada sana reklam gösterirken Instagram'daki ilanlarına göre reklam gösteremiyor” (K.5).

Katılımcı 7 ise analitik araç olarak kullanılan çevrimiçi izleyicilerin ne için ve nasıl kullanıldığını açıklamış, bu yöntemin pek çok geliştirici ve şirket tarafından kullanıldığını, bu yolla toplanan verilerin ise anonim olduğundan bahsetmiştir:

“Mesela biz mobil uygulama geliştirirken bir yazılımın doğru çalışıp çalışmadığını anlayabilmek için belli analitik araçlar kullanıyoruz. Bu araç gereçler belli ölçüde kullanıcının davranışlarını ve uygulamanın onların cihazlarına nasıl çalıştığını, hayati verilerini, mesela çöküyor mu? Veya çöküyorsa hangi model telefonlarda çöküyor? Hangi işletim sistemi olanlarda çöküyor? Hangi ekran büyüklüklerinde düzgün görüntülenemiyor? Bunları anlayabilmek için belli veriler toplarız. Bu verileri GDPR gereği ve diğer yasalar gereği zaten yani gizlilik sözleşmelerinde söylüyoruz. Google Play Store gibi Apple Store gibi marketlerde ne kadar verinin alındığına dair belli sorular soruyor ve bunları cevaplayarak markete yüklüyoruz. Eğer yanlış cevap verdiğimiz anlaşılırsa risk olarak algılanır, uygulamanın kaldırılması veya o geliştirici hesabının yasaklanması gibi durumlar söz konusu olabilir. O yüzden geliştiriciler genelde doğru cevap vermeye çalışıyor. Bu en temelde bu kadar yapılıyor. Yani hiç kişisel veri toplamak istemeyen yazılımcılar ve şirketler bile en azından uygulamanın hayati verilerini kontrol etmek için toplar. Kaç kişi yüklemiş? Kaç kişi indirmiş? Hangi coğrafyalarda daha çok indiriliyor gibi temel verilerinin toplanması gerekiyor ki bu artık zaten ana akım olmuş bir yöntem. Yani anonimleştirilmiş bir şekilde. Bunun daha da ötesine gitmek isteyen şirketler illaki var bildiğimiz kadarıyla. Bir de bilmediğimiz şeylerin de çok fazla olduğu söyleniliyor ve düşünülüyor” (K.7).

Katılımcı 7'nin uygulamaların sağlıklı çalışması açısından topladığı verilerin anonim olduğunu söylese de daha önce açıklandığı üzere kullanıcıların mobil uygulamalardaki kimliklerinin gerçek hayattaki kimlikleriyle ilişkilendirilebileceği gösterilmiştir. Bu nedenle uygulamanın kararlı çalışması için toplanan verilerin de diğer veriler gibi kişisel olarak nitelendirilmesi gerekmektedir.



Şekil 3.14 İşletim Sistemi Veri Toplama İlişkileri - Kod-Alt Kod-Bölümler Modeli

Şekil 3.14'te gösterildiği üzere “İşletim Sistemi” temasıyla “Android” ve “iOS” alt temaları arasında güçlü bir bağ vardır. “Android” alt teması ile “Veri Toplama” alt teması arasında yakın bir ilişki varken, “iOS” alt temasıyla en güçlü ilişki “Apple” teması arasındadır. Ayrıca “Android” ile “Sızıntı” arasında güçlü bir ilişki varken, aynı ilişki “iOS” ve “Sızıntı” arasındaki ilişki daha az güçlüdür. “Android” temasıyla “gözetim” teması ve “Profil Kategorizasyonu” alt teması birlikte kodlanırken, “iOS” temasıyla, “AdID” ve “Çerezler” alt temalarıyla birlikte kodlanmıştır. Bu şekilden çıkan en önemli sonuç, katılımcılardan bir bölümünün Android’e şüpheyile yaklaşması, bir bölümünün ise güvenilir bulmasıdır. Android’in daha fazla veri sızdırdığına ilişkin katılımcı ifadeleri de bu işletim sistemi üzerindeki şüpheyile dair bulguları destekler niteliktedir. Diğer bir önemli sonuç ise iOS’a daha az şüpheyile yaklaşıldığıdır. Veri sızıntısı konusunda ise katılımcıların Android’den daha az veri sızdırabileceği görüşü de bu veriyi desteklemektedir.

Google ve Gizlilik

Google, son yıllarda kullanıcı gizliliğini sağlamak çeşitli adımlar atmıştır. Bu girişimlere, uygulama izinlerinde sunmuş olduğu seçenekler, -özellikle yalnızca uygulama kullanırken erişim izinlerinin aktif edilmesi- kamera kullanımı sırasında sensörler yardımıyla kullanıcı dikkatinin çekilmesi ve uygulama izinlerinin değiştiğinde³⁵ kullanıcılara bu değişim hakkında bildirim gitmesi gibi örnekler verilebilir. Ancak katılımcılar, çoğunlukla Google ve gizlilik kavramının yan yana kullanılmasını yadırgamışlardır. Katılımcı 3 ve 4, Google’ın analitik ve reklam altyapısını kullandıklarını, ancak derinlerde neler yaptığını bilmediğinden şüpheli bir şirket olduğunu ifade etmiştir. Katılımcı 5 ise daha da ileri giderek Google’ı zararlı yazılım (spyware) olarak tanımlamıştır:

“Reklam göstermek için Google’ın altyapısını kullanıyoruz. O altyapıda bir yere kadar biz Google’ın neler talep ettiğini biliyoruz. Yani çok daha derinlerde farklı şeyler yapıyorsa Google, o kadar derin altyapısını bilmiyoruz çoğu zaman. Biz diyoruz ki bunları hiçbir şekilde kullanıcıdan alamazsın, kendin saklayamazsın. Google’da ben zaten o bilgilere ihtiyacım yok diyor. Ama daha derinde kodlar sıkıştırdıysa oraya bir şeyler yaptıysa o bilgi bizde yok. Burada şuna güveniyoruz. Google’ın reklam ağını birçok uygulama kullanıyor. Eğer böyle bir sıkıntı olsa illaki dünyada milyonlarca kullanıcısı olduğu için bir yerden patlar ve bu Google’a büyük sıkıntı çıkartır. Bu bilgidenden dolayı biraz güvenimiz var” (K.3).

“Firebase kullanıyoruz biz. Tabii başka şeyler kullanıyoruz. Ama onlarda kendi belirlediğimiz

³⁵ Mobil uygulamaların cihazlara ilk yüklendiğinde istediği erişim izinleri, sonradan değişebilir. Örneğin bir uygulama konum verileri ile ilgili bir değişiklik yaptığında “bu uygulama konum verilerini artık 3. taraflarla paylaşıyor” uyarısıyla karşılaşabilmektedir.

ölçüde bize bilgi topluyor. Benim bilmediğim şekilde entegre ettiğim zaman onların hizmetine yazılımımı eğer başka bir şey kullanıyorsa bunun farkında değilim” (K.4).

“Android Google’ın bir ürünü ve aslında Android’in yapılış amacı insanların telefonlarına girelim ve orada ne yapıyorlarsa her şeyi okuyalım. Çünkü Google ne kadar seninle ilgili şey bilirse o kadar iyi hedefleme yapabiliyor sana. Ve ne kadar iyi hedefleme yaparsa da o kadar iyi para kazanıyor. Bu yüzden de Google’ın çıkardığı bütün ürünler yani Google Chrome, Google Maps işte Android zaten kendi başlı başına... Gmail vesaire, bunlar tamamen senin kişisel verini okuyup senin profilini çıkartmak üzerine kurgulanmış sistemler. O yüzden de Android zaten başlı başına bir spyware bana sorarsan. Tamamen bütün kullanıcıların bütün hareketlerini, hangi uygulamayı açtı, hangi uygulamayı kapattı, nereye girdi çıktı? Her şeyi çok rahatlıkla Google’a gönderebildiği bir işletim sistemi. Benim için Android bu sebeplerden dolayı bir opsiyon değil; çünkü tamamen her şeyi Google’a açyorsun” (K.5).

Google ve Android’in mobil uygulama ekosistemindeki rolüne bakıldığında, Google’ın her şeyden önce bir reklam ağı olduğunu görmek önemlidir (Spreeuwenberg ve Poell, 2012). Yukarıda verilen ifadeler de Spreeuwenberg ve Poell’i kanıtlar niteliktedir. Google’ın oldukça geniş bir analitik ve reklam ağı bulunmaktadır ve geliştiricilerin büyük bir kısmı bu altyapıyı kullanmaktadır. Dolayısıyla bu alt yapıları kullanan geliştiricilerin topladığı veriyi Google’a teslim ettiği sonucuna ulaşılmaktadır. Katılımcı 2 ve 5 özellikle Google Analytics’in ücretsiz olmasına vurgu yapmışlar ve bunun sonucunda verilerin Google’a aktığını dile getirmişlerdir:

“Google Analytics ve benzeri uygulamalar bedava. Geliştirici buna para vermiyor. Nereden para geliyor? Yine bu kullanıcı verilerinden” (K.2).

“Ücretsiz alternatif diye bir şey pek yok. Google bu hizmeti bedavaya veriyor. Ne için yapıyorsun? Kullanıcılar nereye basmış? Nereye gitmiş? Hangi ülkelerden gelmiş? Hangi ekranlarda daha çok gezmiş? Bunları öğrenebilmek adına Google Analytics’in Kütüphanesi var. Onu kendi uygulamanın içerisinde gömüyorsun, gömünce de oradan verileri kendisi almaya başlıyor. Kullanmayan neredeyse yok gibi bir şey” (K.5).

Google, özellikle ücretsiz olarak sunduğu bu alt yapı sayesinde devasa bir veri madeni bulmuş, bu değerli madenin verimli bir şekilde çalışmasını sağlamak ve sürdürülebilir olması için kaynaklarını adeta seferber etmiştir: Bu nedenle Android analitik araçları, Google’ın kullanıcıların kontrolünü elinde tutmaya ve meta verilerini toplayabildiğinden emin olmaya çalıştığı bir araç olarak görülmelidir (Spreeuwenberg ve Poell, 2012). Katılımcı 6 ise Android işletim sistemi ve gizlilik konusunu ön plana çıkararak Google’ın gizlilik konusunda çok geç adımlar attığını, Android’in önceki sürümlerinin oldukça gizlilik riski barındırdığını, giderek gizlilik ve güvenlikle ilgili adımların atıldığını; ancak özellikle gizlilik açısından Google’a kıyasla Apple ürünlerinin kullanılmasını önermiştir:

“Google biraz geç kaldı gizlilikle ilgili adımları atmak için. Geçtiğimiz yıllarda burada büyük

bir güncelleme aldık gizlilik ve güvenlikle ilgili. Tabii bu yıllar içinde yaygınlaşacaktır. Çünkü hep yeni yeni Android sürümlerine geliyor bunlar. Eski Android sürümleri hala o kadar güvenilir değil. Ama bence yine de bir kişi eğer gizliliğini önemsiyorsa günümüzde bence Apple çok daha iyi bir seçenek” (K.6).

Apple ve Gizlilik

Apple, kullanıcı gizliliğini koruma konusundaki kararlılığını, kullanıcılarına bir açıklama mektubu yazarak açıklamıştır. Şirket, kişisel verilerin gizliliğini ve güvenliğini koruma amacını vurgulayarak, gizliliği sağlama hedefini sıkı bir şekilde sürdürmek istediğini belirtmiştir. Apple, verilerin kontrolünün kaybedilmesi durumunda, kullanıcıların hem gizlilikleri hem de güvenlikleri açısından büyük bir riskle karşı karşıya kalabileceğini belirtilmektedir. Apple’ın bu çerçevedeki kararlılığı, kullanıcıların gizliliği ve güvenliği konusunda önemli bir güvence olarak kabul edilebilmektedir (Martin ve Murphy, 2017: 151). Ayrıca Apple ve Google karşılaştırması, bir bakıma iş modellerinin karşılaştırılması anlamına da gelmektedir. Bu iki iş modeli arasındaki fark (açık kaynak-kapalı sistem) ve Apple’ın gizliliğe daha fazla önem veren açıklama ve attığı adımlar göz önüne alındığında, iOS ekosisteminin paylaşılabilecek veri türleri ve üçüncü taraf paylaşımının kapsamı açısından genel olarak gizliliği daha fazla koruyacağı varsayımını güçlendirmektedir (Kollnig, vd., 2022: 2).

Yukarıda Katılımcı 6’nın belirttiği üzere Apple’ın veri mahremiyeti koruduğuna dair bazı emareler bulunmaktadır. Katılımcı 3 ve 8’in aşağıdaki ifadeleri de yukarıda belirtilen Apple’ın açıklama mektubundaki kullanıcı gizliliğini koruma konusundaki duruşunu destekler niteliktedir:

“Apple gizlilik konusunda iyi. Biz her uygulamayı markete yüklerken sekiz-on tane soruyla karşılaşıyoruz. Bu veriyi alıyor musunuz? Bu veriyi alıyorsanız nerelerde kullanıyorsunuz? Hangi amaçla alıyorsunuz? Üçüncü parti şirketlere bu verileri aktarıyor musunuz? Gibi soruları cevaplayarak biz uygulamaları yüklüyoruz uygulama marketine” (K.3).

“Çok fazla iOS geliştiriciden duyduğum şöyle bir olay var. Uzun süredir yıllardır güncelleme yaptığı bir uygulama mesela. Güvenliğe önem vermediği için uygulamalar marketten kaldırılabilir. Bunları çok duydum. Güvenliğe yeterince önem vermediği için, bir şeyi atladığı için” (K.8).

Yukarıda verilen katılımcı ifadelerine ek olarak Apple’ın yalnızca kendi uygulama marketinden uygulama indirmeye izin vermesi, Apple’ın veri güvenliği ve gizliliği ile ilgili en önemli duruşlardan biri olarak görülebilir. Ancak Apple’ın 2024 yılının başında yaptığı açıklamayla AB’deki yeni dijital yasanın zorlayıcı maddeleri nedeniyle politikasını

gevşettiği (AB ülkesi kullanıcıların App Store dışından uygulama indirmeye izin vermiştir.)³⁶ Kendi uygulama mağazasından uygulama indirerek güvenliği sağladığı yönündeki bu duruşla ters düştüğü görülmüştür. Katılımcı 3'ün bir başka ifadesi ise kullanıcı-geliştirici kimliği açısından bir çelişkiye işaret etmektedir. Kullanıcı mahremiyetinin korunurken aynı zamanda geliştiricilerin reklam gelirine darbe vurulması bu çelişik durumu yaratmaktadır:

“Kullanıcılar tüm verilerini sakladığı zaman biz mesela reklam verenlere çok iyi bilgi sunamıyoruz. Sunamadığımız için reklam kaynağımız aşırı düşüyor. Neyden bahsediyorum? Bu son Apple'ın beni takip etme özelliğinden bahsediyorum. Evet kullanıcılar için güzel bir özellik katılıyorum. Ama bir yazılımcı olarak diyorum ki keşke bizim uygulamada izin verseler de ilgili alanlarda reklamlar göstersem daha iyi bir maddi kazanç sağlayabilsem. Kullanıcı tarafından baktığımda da diyorum ki benim Google'dan aradığım bir şeyi takip etmeyi versin. Başka uygulamalarımı müdahale etmesin diyorum. Biraz çelişki içerisindeyim aslına bakarsanız” (K.3).

Öte yandan Katılımcı 3'ün bir başka ifadesi yine çelişik bir duruma işaret etmektedir. Katılımcı 3'ün “*Apple gizlilik konusunda iyi*” ifadesinden yola çıkarak, Apple'ın kullanıcı gizliliği açısından taşıdığı sorumluluğu değerlendirmesi istendiğindeki verdiği ifade, adeta Apple'ın sorumluluk reddini göstermektedir:

“Kullanıcılar o uygulamayı kullanmak istiyorsa, uygulamanın altında yazan kişisel özellikler kısmındaki verileri kabul etmiş oluyor. Ondan sonra konu zaten Apple'ın üzerinden çıkmış oluyor bir bakıma. Apple telefon olarak, cihaz olarak ben sizin bu bilgilerinizi koruyorum. Hiç kimseye de vermiyorum. Bunu diyebilir. Ama işin içine başka uygulamalar, başka konular girdiği zaman zaten diyor ki konu benim dışımda. Senin problemin... o uygulamayla senin aranda, sen oraya izin vermişsin veya o yapmış. Bu biraz da Apple'ın kendisini sıyırmasıyla da alakalı bir durum. Apple'ın buradaki çözümü, konuyu uygulama geliştiricilerle uygulama kullananlar arasına bırakmak. Kendisi aradan çıkıyor, sorumluluğu üstüne almıyor noktasına getiriyor” (K.3).

Diğer taraftan katılımcı 1, 2 ve 8, Apple'a kesin bir dille güvenmediklerini dile getirmişlerdir:

“Veriler üzerinde öyle yüksek paralar dönüyor ki bu işin içerisinde... Apple'ın gizlilik ile ilgili girişiminin sadece reklam amaçlı olduğunu düşünüyorum. Gizliliği koruduğunu düşünmüyorum; çünkü Apple'a inanmıyorum” (K.1).

“Geçen sene bir haber görmüştüm. Apple senin telefonunu tarayıp çocuk istismarı görüntüsü var mı diye bakacağız, biz çocuk istismarına karşıyız gibi bir iddiayla bütün fotoğraflarını inceleyeceğini söylemişti. Çok fazla tepki alınca vazgeçtiler. Mesela bunu yapıp da sana söylemeyebilirler. Bu yüzden çok da fazla güvenim yok açıkçası” (K.2).

³⁶ The New York Times, “Apple, Yeni Dijital Yasaya Yanıt Olarak Avrupa'daki Uygulama Mağazasını Elden Geçiriyor” <https://www.nytimes.com/2024/01/25/technology/apple-app-store-europe.html> (erişim tarihi: 28.01.2024).

“Benim kişisel görüşüm, dijital ortamda hiçbir şey yüzde yüz güvenlidir diyemeyiz. Yani Apple da olsa yüzde yüz güvenli bir sistem yoktur” (K8).

Yukarıda kullanıcı gizliliğini koruması ile ilgili bazı olumlu ifadeler karşı, Apple’ın kullanıcı gizliliğini korumadığını ve özellikle *beni takip etme* özelliğinin bir pazarlama veya reklam taktiği olarak kullanıldığını öne süren katılımcıların daha ağır bastığı görülmektedir:

“Apple bir reklam engellemeye falan çalışıyor başladı gibi ama öte yandan kendisiyle reklam işine girmek istiyor gibi şu anda. Apple her cihazda hangi reklamın oynatıldığını biliyor. Bazı ayarlar var. Onları engelleyebiliyorsun spesifik olarak birtakım şeyler engellenebiliyor. Kişiselleştirilmiş reklam daha az geliyor sana. O ayarlar sayesinde. Ama öte yandan Apple kendi reklamını kullanıyor burada bir çelişki var” (K.2).

“Şöyle bir zorunluluk var mesela Apple’da daha önce yoktu. “Hesabımı sil” gibi bir buton koymak zorundasın. Eğer bunu koymazsan uygulamayı geçmiyor. Yayına alınmıyor asla. Ve bu butonu görmezse Apple uygulamayı kabul etmiyor. Böyle bir gerçek de var. Ve o butonu kontrol ediyor hesabını gerçekten siliniyor mu diye. Yani aslında görünürde gerçekten de senin tarafında gibiler. Baktığın zaman kullanıcı olarak senin arkasını kolluyor gibiler. Ama ben inanıyorum ki kesinlikle büyük şirketler arasında bir transfer var. Karşılıklı bir kazanç var. Gerçekten de tek tuşla her şeyi silebilirsin bu mümkün. Ama böyle bir şey olmaz, kendilerinin kazancına, doğasına aykırı bir kere. Elindeki veriyi silmek istemez yani. Birine karşı elinizde bir koz olduğunu düşünün. Bu kozu kaybetmek istemezsiniz. İllaki bir yerde işinize yarar. O yüzden mümkün ama bunu bilerek yapmıyorlar diyebilirim” (K.4).

“Onlar bu işin pazarlaması, kullanıcının konumunu takip edip etmemek sadece bir butonla olmaz. Yani oradaki butonu açıp kapatmak değil. Orada tekelleşme var. Her istediğini yapar, istediği veriye ulaşır, yapabilir. Biz sizin özgürlüğünüze saygı duyuyoruz gibi bir pazarlama var. Ama onun dışında ben sanmıyorum ki herhangi bir veri takibi yapılmasın. Kaldı ki şöyle teknoloji, özellikle telefonlar, mobil uygulamalar, dünyada 7 milyar insan var ve 7 milyar insan hakkında bilgi sahibi olabileceğimiz en temel iletişim araçları aslında. Ve buna en çok ihtiyaç duyan tabii ki ülkeler ve siyasi yönetimler oluyor. Tabii ki ilk başta ya da devlet bunları talep ediyor. En nihayetinde Amerikan ulusal güvenliğimiz deyip verileri Facebook’tan da Apple’dan da veya Google’dan da talep ediyordur” (K.10).

“Apple, bu gizlilik olayını özellikle kendisi bir pazarlama aracı olarak da kullanıyor. Sizin veri gizliliğinize çok önem veriyor diye, bunun reklamını yapıyorlar. Apple Facebook’a çok büyük darbe vurdu bu AdID’yi paylaşmama mevzusundan sonra. Çünkü Facebook her türlü veriyi topluyordu. Hem kartlarda göstermek zorunda kaldılar ne topladıklarını. Hem de artık insanları takip edemiyorlar uygulamalar arasında. Şimdi tam rakamını hatırlamıyorum ama baya değer kaybetti Facebook bu yüzden. Ama daha sonra Apple kendi reklam sistemine ağırlık vermeye başladı ve kendilerine böyle işletim sistemi düzeyinde bazı imtiyazlar tanımaya başladı AdID paylaşma konusunda. Tabii acaba Apple bunu aslında kullanıcıların gizliliğini düşündüğü için değil de kendi reklam modeli daha çok para kazansın diye mi yaptı diye bir soru işareti oluştu. Haklı da bir endişe onu söyleyebilirim. İlerleyen zamanlarda neler olur bilmiyorum ama şu an pek iç açıcı gözüküyor açıkçası” (K.5).

“İşin görünür tarafında verilerinizi koruyoruz, bak buna değer verdiğimiz için bunu yapıyoruz gibi gözüküyor ama arka planda açıkçası için öyle olduğunu sanmıyorum. Çünkü şu an veri takibi çok önemli bir kaynak, yani o veri geliştiriciler için şirketler için çok ciddi bir kaynak. Ben bir tane oyun analiz aracı ile ücretsiz şekilde bunlara erişebiliyorum ve Facebook mesela

Facebook analiz gibi araçlar bunu kendileri satıyorlar. Açıkçası ben Apple'ın artık bu ücretsiz olan tarafı kesip kendi sistemine hazırlık yaptığını düşünüyorum. Zaten bu veriyi kendileri satmak gibi bir hazırlıkları var. Sanırım hâlâ beta aşamasında daha kesin bir şey yok. Yani ben Apple'ın yine bir ürün ortaya çıkartabilmek için bunu yaptığını düşünüyorum. Evet şu an net bir şekilde bana vermiyor ama verebilecek kanallara... Bana biraz para ver bunun bir ücreti olsun ondan sonra sen bunu kullanabilirsin demek için yapıldığını düşünüyorum açıkçası. Aslında benim fikrim de değil, araştırıp gördüğüm tarafı da var. Apple'ı düşünürsek çoğu şeyi bedava vermez. Yani bir şekilde elindeki bir veriyi, bu kadar değerli bir veriyi bedava vermez. O yüzden şimdi onun altyapısını hazırlıyor. Daha sonra bu verileri ben Apple'ın izin verdiği kadar ücretini ödeyerek alabiliyor olacağım. Bırakmazlar mümkün değil! Bir oyun geliştiricisi olarak düzgün oyun geliştiremeyeceğim demek bu. Apple'ın oyun ekosistemine çok ciddi bir zarar verir. Ben oradaki kullanıcıların verilerini bilmiyorum, nasıl davrandıklarını bilmiyorum. Yani bana bir şekilde o veriyi verecek. Mutlaka benim o veriye erişmem lazım ama sadece bunu dediğim gibi Apple'ın izniyle, Apple'ın bittiği bir değerle olacağını düşünüyorum” (K.9).

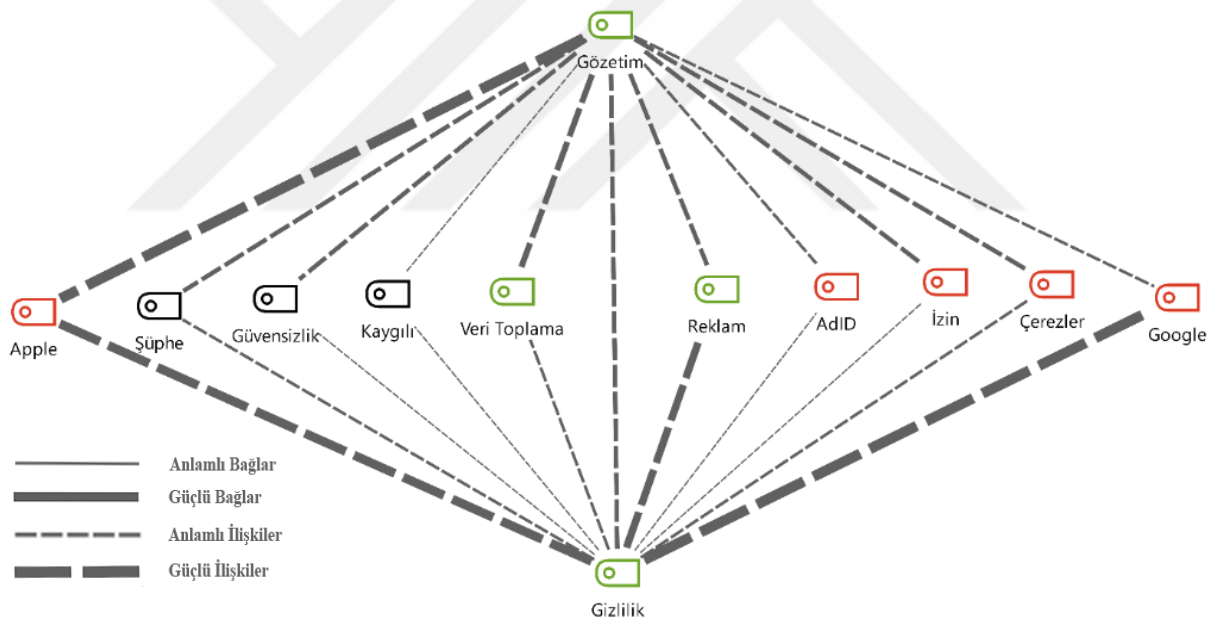
Katılımcıların ifadeleri özetlenecek olursa Apple, kullanıcılarına uygulama takibi izinlerini denetleme imkânını vermiştir. Bu ilk bakışta kullanıcı gizliliğini önemseyen olumlu bir yaklaşım gibi görünmektedir. Hatta Apple, diğer şirketlere göre genellikle ücretsiz değil ücretli uygulama politikası güden bir şirkettir. Ücretsiz uygulamaların çok daha fazla veri talep ettiği göz önüne alınırsa Apple'ın bu ücret politikasının gizliliği bir ölçüde koruyacağı da düşünülebilir. Öyle ki Zuboff (2021: 38), Apple'ın bu konuda kendine has bir çizgi oluşturduğunu ve aşırı veri talep eden uygulamalardan uzak durduğunu söylemiştir. Ancak Zuboff, Apple'ın tamamen güvenilir ve kusursuz bir kullanıcı gizliliği sağladığını da iddia etmemiştir. Ona göre “... çizgi çoğu zaman bulanıktır ve Apple da yönelimini değiştirebilir ya da bununla çelişebilir” (Zuboff 2021: 38). Ayrıca “Myske” takma adını kullanan iki geliştirici, Apple'ın gizlilikle ilgili vermiş olduğu vaatlerin tamamen yanlış olduğunu, Apple'ın kullanıcıların her hareketini izlediğini, gizlilik için işlev gördüğü iddia edilen mekanizmaları devre dışı bırakmanın hiçbir yolunun olmadığını ileri sürerek Apple hakkında dava açıldığını duyurmuşlardır (The Economic Times, 2022). Öte yandan uygulama içerisindeki bu izinlerin devre dışı bırakılması, çoğunlukla hizmetin kullanamama durumuyla karşılaşılmasına neden olmaktadır. Zuboff'un bahsettiği çelişki 2023 itibarıyla yürürlükte olan Gizlilik Politikası'nda bulunmaktadır. Politikada, verilerin işlenmesini istemeyen kullanıcıların Apple'dan düşük bir hizmet almama garantisi sunulurken hemen sonrasında veri sağlanmadığında taleplerin yerine getirilemeyeceğinden bahsedilmektedir:

“Apple olarak kişisel verilerinizi öğrenme, düzeltme, aktarma, silme, söz konusu verilere erişme ve verilerin işlenmesini kısıtlama tercihlerinize saygı duyuyoruz. Bu hakları küresel müşteri tabanımıza sağlamış durumdayız ve söz konusu gizlilik haklarını kullanmayı tercih etmeniz halinde ayrımcı bir muamele görmeme veya Apple'dan daha düşük dereceli bir hizmet almama hakkına sahipsiniz” (Apple, 2022).

Talep ettiğimiz kişisel verileri sağlamanız zorunlu değildir. Ancak kişisel verilerinizi

paylaşmamayı seçerseniz çoğu durumda size ürünlerimizi veya hizmetlerimizi sağlayamaz ya da taleplerinizi yerine getiremeyiz (Apple, 2022).

Öte yandan katılımcıların, Apple'ın, uygulama veri takibini denetleme imkanını kullanıcılara veren bu uygulamasını, reklam ya da pazarlama amacı olarak görmeleri ve Apple'ın da kendi reklam ekosistemini yaratmak istiyor olma ihtimali, göstermelik kullanıcı gizliliğini lehine kullanacağına işaret etmektedir. Kendi ekosisteminde istediği uygulama veya şirkete uygulayacağı imtiyazlarla verinin kime, nasıl ve ne şekilde gönderileceğinin kontrolünü ele geçirmeye çalışacağı öngörülmektedir. Tüm bunlar elbette şu an için varsayımdır. Ancak daha önce de belirtildiği gibi Apple kapalı bir sistem üzerine inşa edilmiştir. Birçok çalışma Android ekosistemindeki gizliliği analiz etmiş olsa da iOS hakkında nispeten daha az şey bilinmektedir. Bunun bir nedeni, Apple'ın özel programlama dilleri ve derleyicilerin kullanımı da dahil olmak üzere kullandığı kapalı kaynak yapısı, analiz çabalarını zorlaştırmaktadır (Kollnig, vd., 2022: 3).



Şekil 3.15 Google - Apple Gizlilik ve Gözetim Bağları - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.15’te gösterildiği üzere “Apple” temasıyla “Gizlilik” ve “Gözetim” temaları arasında güçlü bir ilişki vardır. “Google” temasıyla ise “Gizlilik” teması arasında güçlü bir ilişki varken, “Gözetim” temasıyla daha az güçlü bir ilişki vardır. Ayrıca “Android” ile “Sızıntı” arasında güçlü bir ilişki varken, aynı ilişki “iOS” ve “Sızıntı” arasındaki ilişki daha az güçlüdür. Ayrıca “Gizlilik” ve “Gözetim” teması arasında da güçlü bir ilişki bulunmaktadır. Şekilden anlaşılabacağı üzere Apple daha fazla veri gözetimiyle, Google ise gizliliğin tehlikeye atılmasıyla ilişkilendirilmektedir. Google ile gözetimin daha az

ilişkilendirilmesi ise Google tarafından uygulanan veri gözetiminin sıradanlaşmış olabileceğine işaret etmektedir.

Blok Zinciri ve Merkezi Olmayan Uygulamalar

Son dönemlerde blok zinciri teknolojisinin veri mahremiyeti koruyabileceği, blok zinciri tabanlı merkeziyetsiz uygulamaların kullanıcı gizliliğini mümkün kılabileceği yönündeki söylemler giderek daha fazla dillendirilmektedir. Bu nedenle tez konusu kapsamında mobil uygulamalara alternatif olabilme ihtimali bulunan ve merkeziyetsiz bir yapılanması olan merkezi olmayan uygulamalara ilişkin olarak katılımcıların görüşlerine ihtiyaç duyulmuştur. Katılımcıların tamamı, mobil uygulama geliştiricisi olsa da çoğu katılımcının blok zinciri ve üzerinde çalışan merkezi olmayan uygulamalar hakkında bilgi sahibi olduğu görülmüştür. Teknik açıdan bu yazılım diline ve merkezi olmayan uygulama geliştirmeye çok fazla hâkim olmasalar da sistemin işleyiş mantığı konusunda değerli görüşler sunmuşlardır. Katılımcı 6 ve 11, blok zinciri hakkında olumlu görüş bildirmişlerdir:

“Blok zinciri aslında çok güzel bir teknoloji. Blok zincirinin gelecekte kullanımı çok daha fazla artacak” (K.6).

“Elbette güzel ve yeni bir sistem blok zinciri. Ancak eksikleri var. Bunlar tamamlandıktan sonra veya daha da geliştirildikten sonra iyi şeyler yapılabilir diye düşünüyorum. Geleceğin interneti olarak lanse ediliyor blok zinciri. İnternetin geleceği olur mu olmaz mı bilmiyorum; ancak birçok çözüm için etkili olabileceğini düşünüyorum. Mesela bankacılık sistemi üzerinde etkilerinin olacağı söyleniyor. Aracı bir kuruma ihtiyaç olmadan karşılıklı transfer yapabiliyorsunuz ki bu yalnızca para için değil veri için de olabilir veya haberleşme olabilir” (K.11).

Katılımcı 1, 3 ve 6, merkeziyetsizlik konusunda bazı çelişkilerin bulunduğunu dile getirmiştir. Katılımcı 3 ve 6 da merkeziyetsiz iddiasında bulunan sistemlerin de merkezi hale geldiği çelişik bir durumu dile getirmişlerdir:

“Merkeziyetsizlik diyoruz ama kime göre merkeziyetsizlik? Ne kadar merkeziyetsiz de olsa kâr amacı güden bir oluşum olduğu için herhangi bir şekilde güvenilir olduğunu düşünmüyorum” (K.1).

“DAO diyoruz, vakıf tarzı kurulan veya işte demokratik oylama sistemiyle kurulan ve güç tabanlı merkezi olmayan dağıtık sistemler diyoruz. Ama benim gördüğüm hepsi bir şekilde bir noktada merkezileşiyorlar. Henüz tamamen merkezi olmayan herhalde bir Bitcoin [kripto para] var; çünkü sahibi yok” (K.3).

“Mesela diye bir Mastodon diye sosyal medya platformu var ve şöyle çalışıyor. Siz orada bir sosyal medya hesabı oluşturabiliyorsunuz, profil oluşturabiliyorsunuz. Sizin profiliniz orada tutuluyor. Ancak orada paylaştığınız gönderileri sizin bir yerde tutmanız gerekiyor. Bu da aslında merkeziyetsiz oluyor. Siz burada kendi bilgisayarınızı kullanabilirsiniz. Gönderileriniz

kendi bilgisayarınızda olur ve insanlar sizin gönderilerinizi ve ulaşmak istediğinde, profilinize girdiğinde eğer bilgisayarınız açık değilse gönderilerinizi göremezler. Ya da bunun için bir sunucu kiralayabilir, burada depolayabilirsiniz. Ya da aslında popüler olan şu an Mastodon’un üzerinde, Mastodon sunucularından herhangi birini seçip bunlara katılabilirsiniz ve verilerinizin oralarda tutulmasını sağlayabilirsiniz. Aslında merkeziyetsiz ama kendi adı altında merkezi olmuş versiyonu bu. Çünkü günün sonunda binlerce kişi yine bir yerlere depolamış oluyor... yani ortak bir alana. Ama bunun çıkış noktası kullanıcıların kendi sunucularında ya da kendi bilgisayarlarında bunu depolamasıydı ama bu şekilde yürümedi işler” (K.6).

Katılımcı 6’nın ifadesindeki verileri depolama durumu, Mastodon sosyal medya platformunda (Mastodon uygulaması web tabanlıdır ve blok zincir üzerine inşa edilmemiştir. Ancak merkeziyetsiz bir platformdur.) isteyen herkesin bir sunucu yaratmasıdır. Bu merkeziyetsiz sosyal ağ uygulaması, kullanıcılarının sunucu kurmasına izin vermekte, kullanıcı verileri bu sunucularda depolanmaktadır. Neticede bu uygulama bir sosyal medya uygulamasıdır ve kullanıcı adı, şifre, fotoğraf ve hatta takipçi etkileşimi gibi veriler sunucuya teslim edilmektedir. Mastodon, sunucularında tutulan verinin çeşitli güvenlik önlemleriyle korunduğunu ileri sürülmekte, kullanıcıyı tanımlayabilecek herhangi bir verinin üçüncü taraflara satılmadığını veya başka bir yolla aktarılmadığını da iddia etmektedir. Öte yandan Google Play Store’da yer alan Mastodon veri güvenliği bölümünde “Geliştirici, bu uygulamanın kullanıcı verilerini toplamadığını söylüyor” ifadesi bulunmaktadır. Ancak yine aynı bölümde “kişinin adı ve e-posta adresinin” üçüncü taraflarla paylaşıldığı ibaresi bulunmaktadır.³⁷ Bu ifadeler, Mastodon uygulamasının toplamadığı veriyi paylaştığını iddia ederek çelişkili bir duruma neden olmaktadır.

Katılımcı 5 ise merkezi olmayan uygulamalardaki çelişkiyi dile getirmiş, merkezi sistemlerin merkeziyetsiz sistemlere göre daha sürdürülebilir bir sistem olduğunu, merkeziyetsizliğin gelip geçici bir heves olduğunu ve dezavantajlarının merkezi sistemlere göre daha fazla olduğunu dile getirmektedir:

“Zaten web merkeziyetsiz bir ortamdı. İlk internet çıktığında bir siteye girdiğiniz zaman aslında bir kişinin evindeki bilgisayara giryordunuz. Herkesin kendi kurduğu bir sunucu vardı. Böyle bir merkezi bir veri sistemi, Cloud gibi şeyler yoktu. Daha sonra zamanla bu büyük platformların çıkması Google’ı, ortaya çıktı. Herkes kendi hesabını bu merkezi sistemlerde açmaya başladı. Yani bir merkezileşme oldu. Bu kötü bir şey değil bu arada, iyi bir şey. Tekrardan bunu dağıtmaya çalışıyorlar. Şimdi baktığımız zaman mesela Fikri Nitelikli Tapu’ya merkeziyetsiz bir olay dediler ama insanlar merkezi platformda satışlarını gerçekleştiriyorlar. Yine tamamen merkeziyetsizlik dışı bir ortam oluştu. Ben bunun gelip geçici bir heves olduğunu düşünüyorum. Bu konuda tabii birçok insanla farklı düşünüyorum

³⁷ Google Play Store, Mastodon Veri Güvenliği > Paylaşılan Veriler > Toplanan Veriler ve Kişisel Bilgiler <https://play.google.com/store/apps/datasafety?id=org.joinmastodon.android&hl=tr&gl=US> (erişim tarihi: 02/12/2023).

olabiliriz. Metaverse'ün de insani olmadığını ve geri tepeceğini düşünüyorum ben. Bir noktada insanların kabul etmeyeceğini düşünüyorum. Şu ana kadar çok iyi bir uygulama diyebileceğimiz bir uygulama olmadı. İşte Bitcoin'ler vesaire söyleniyor ama Bitcoin'in de hali ortada. Şu an insanlar onu bir para birimi olarak kullanmıyor. Al-sat bir yatırım aracı olarak kullanıyorlar. Ve tükettiği kaynaklara baktığımızda Afrika'da üç ülkenin toplamı kadar elektrik yakıyor bir günde. O yüzden çok büyük bir geleceği olduğunu düşünmüyorum yani mevcut şartlara bakarak. Ama birisi çok böyle acayip inovatif bir kullanım alanı bulur. Der ki bu böyle yapılacak, hayatımıza yerleşir. O zaman bir şey diyemem ama kalıcı bir teknoloji olacağını düşünmüyorum" (K.5).

Katılımcı 5'in işaret ettiği üzere Bitcoin gibi kripto varlık ediniminde blok zinciri ve merkezi olmayan uygulamaların mantığına aykırı bazı durumlar bulunmaktadır. Örneğin bazı kripto para borsaları, bu mantığa ters düşmektedir. Merkezi borsalarda ya da NFT pazarlarında bu varlıklar alınıp satılabilmektedir. Merkezi sistemler bugün, merkeziyetsiz sistemleri de merkezi hale getirmiştir. Öte yandan Metaverse konusunda henüz başlangıç aşamasında olması, kullanıcı deneyimi açısından da bazı sorunlar barındırmaktadır. Sanal gerçeklik gözlükleri ile girilebilen bu evrenlerde regülasyon eksikliği, mahremiyet sorunları ve fiziksel bazı sorunlar (baş, göz ağrısı ve cilt sorunları) gündeme gelmektedir. Katılımcı 5'in ifade ettiği bir başka problemlili alan ise bu sistemin aşırı enerji tüketiyor olmasıdır. Ancak bu blok zincire özgü bir durum değildir. Günümüzde kullanılan birçok yazılım ve teknoloji ürünü aşırı elektrik tüketmektedir. Örneğin yapay zekâ bunlardan biridir ve çok güçlü GPU'lara ihtiyacı vardır ve elektrik sarfıyatı had safhadadır.

Katılımcı 6 ve 7, yukarıda bahsedilen Metaverse uygulamalarında olduğu gibi merkeziyetsiz pek çok uygulamada veya DAO'larda kuralların konulmasından kuralların uygulanmasına ve denetlenmesine dek pek çok sürecin baltalanmaya müsait olması nedeniyle endişelerini dile getirmektedirler:

"Merkeziyetsiz uygulamalarda şöyle bir problem olabilir. Kuralları kim koyacak? Veya bu düzenlemeleri kim yerine getirecek?" (K.6).

"Fikir olarak güzel bir fikir. Merkeziyetsizleştirme. Ama pratikte hem henüz karşılığını göremedik hem de karşılığını görme konusunda çok ciddi endişelerim var. Çünkü mesela onu denetleyen bir mekanizma yok. Dolayısıyla çok güçlü veya çok zengin olan hükümetler, belli ağların büyük bir kısmını ele geçirip yine bu şeyi tekelleştirebilir. Hatta merkeziyetsizleştirmeyi ortadan kaldırabilir. Blok zinciri olmadan bunu yapıyoruz ve merkeziyetsiz hale geliyor. Ama birçok şey yavaşlıyor, birçok şey daha kötü kullanıcı deneyimine sebep oluyor. Mesela Mastodon çıktı Twitter alternatifi, merkeziyetsiz. Ben hiç sevmedim. Özellikle birden fazla sunucunun olma fikrini hiç sevmedim. Blue Sky çıktı. Bekliyoruz bakalım nasıl olacak?" (K.7).

Katılımcı 7'nin "güçlü veya çok zengin olan hükümetler, belli ağların büyük bir kısmını ele geçirip yine bu şeyi tekelleştirebilir" ifadesi merkezi uygulamalardaki mülksüzleştirme politikalarının merkezi olmayan uygulamalarda da söz konusu olabileceğini

düşündürmektedir. Örneğin bu alanda baskın olmak isteyen şirketler, satın alma yoluyla olmasa bile, ağır/organizasyonun yönetimini ele geçirebilir ve uygulamaları merkezileştirebilir. Bu durum, anonimliği ortadan kaldırabilir ve kullanıcıların mahremiyeti tehditlere açık hale gelebilir. Katılımcı 8 ise bu sistemin tekelleşmeyi engelleyebileceğini dile getirmiştir. Böylelikle bireylerin, baskı altına girmeden veya bir otorite altında olmaksızın kendilerine ait özel alanlar yaratabileceğine dikkat çekmiştir:

“Muazzam bir yenilik, ben destekliyorum açıkçası ve bayağı bir şeyi değiştirebileceğini düşünüyorum. Tekel bir ortam olmaktan ziyade her insanın kendine özel bir ortamı olabilir. Yani dayatmalar azalır, insanlar abone olmak istedikleri platformlara sadece abone olur ve bir şey görmek için bir çatının altına girmesi gerekmez. Bunun gibi çok güzel avantajlar olduğunu düşünüyorum” (K.8).

Katılımcı 8’in yukarıdaki ifadesinin tam tersi yönde görüş bildiren Katılımcı 10, blok zinciri ve uygulamalarında bir tekelleşme ihtiyacı doğduğundan bahsetmiştir. Katılımcı 10’un ifadesinde dikkat çeken nokta blok zincir ve uygulamalarındaki verilerin kimin tekeline gireceğidir:

“Ben çok sağlıklı bulmuyorum açıkçası. Şundan kaynaklı, orada da bir tekelleşme ihtiyacı var. Mesela veriler, her yerden geliyor ama biz bunları alalım ihtiyacı gibi geliyor bana. O yüzden çok sağlıklı bulmuyorum” (K.10).

Tezin giriş bölümünde daha ayrıntılı olarak değinildiği üzere kapitalizm sürekli genişleme eğilimindedir ve şirketler de blok zincir tabanlı bazı uygulamalara -özellikle de Metaverse evrenine- dahil olmuştur. Katılımcı 5, blok zincir tabanlı bu sistemin yeni sömürü alanları yaratmasına atıfta bulunarak, sistemin bazı uygulamalarını tüketim bağlamında ifade etmeye çalışmıştır:

“Bir dünya yetmedi. Dediler ki biz bir sanal dünya yapalım. Örneğin bir lüks moda tüketim markası, bin beş yüz dolara kol çantası satıyor. Şimdi bunu alabilecek insan sayısı dünya nüfusuna oranla yüzde bir, yüzde iki. Ama diyor ki ben bunun dijitalini yaparım, üç dolara mal eder seksen dolara satarım diyor. Metaverse de satacağım, markanın ürününü sanal avatarında kullanılacak diyor. Bu sefer ne oluyor? Satabileceği insan sayısını, skalasını arttırmış oluyor, genişletmiş oluyor. Tamamen kapitalizmin uydurduğu bir şey. İnşallah başarılı olmaz. Diyecek ki adam işte bak böyle bir hayatın var. Sen bak Metaverse de şöylesin, kralsın bir sürü üçkağıt algoritması yapacaklar. Sana orada sahte bir mutluluk verecek. Herkes seni burada tanıyor, gel sen bundan sonra burada takıl diyecek. Sonra senin asgari ücretinin yarısını Metaverse de harcamanı sağlayacak” (K.5).

Görüldüğü üzere Katılımcı 5’in ifadesi, kapitalizmin sürekli genişleme mantığına işaret etmektedir. Katılımcı 5, şirketlerin bu ortamlarda sahte mutluluklar yaratarak -veya manipüle ederek- kişileri daha fazla tüketime yönlendireceğini öngörmektedir. Bu yalnızca

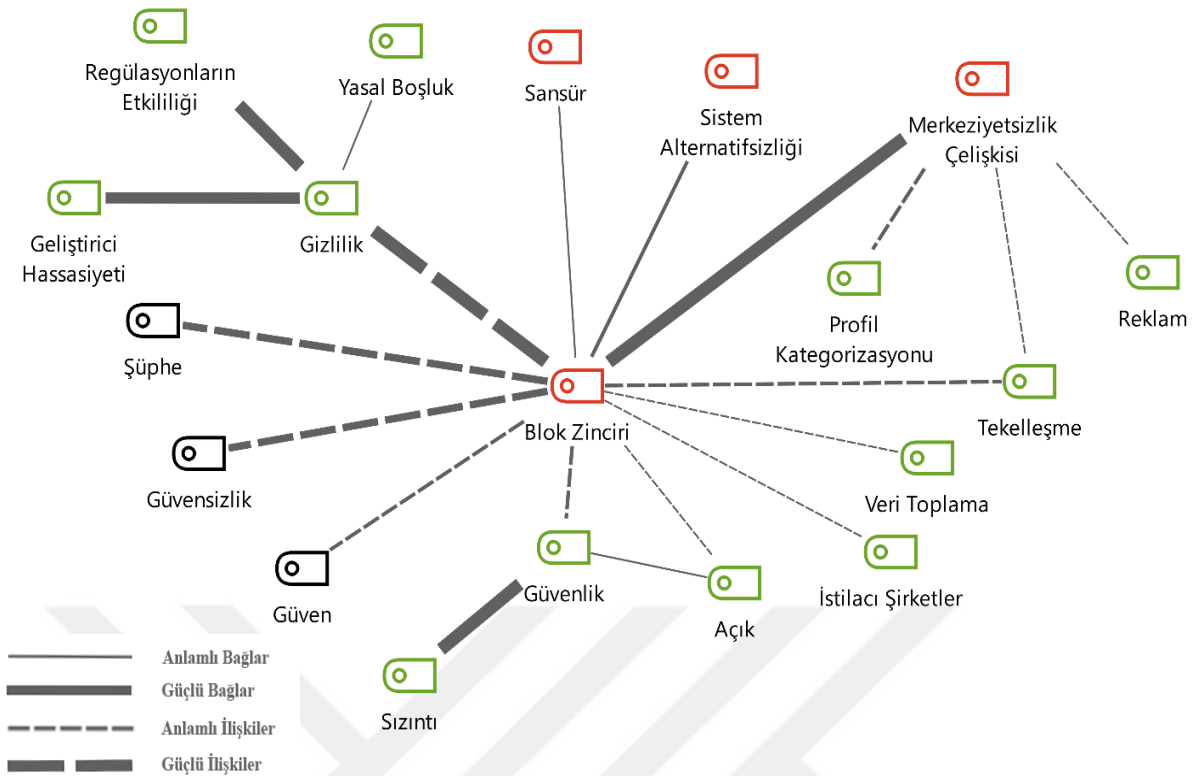
merkezi şirketlerin değil, merkeziyetsiz yapıların da hedefidir. Merkezi şirketlerden arta kalan ya da bu şirketlerin henüz giremediği alanları/boşlukları doldurmanın peşine düşülmüş olduğu şüphesini uyandırmaktadır. Daha fazla teknoloji ürünü satılmadığında ya da mevcut ürünlerin yetersiz kaldığı ya da popüleritesini yitirdiği durumlarda yenilerine ihtiyacın yaratılmasına benzer bir sistem işletilmektedir.

Katılımcılar, merkeziyetsiz yapılardaki güven sorunundan da sıklıkla bahsetmektedir. Özellikle regülasyonların eksikliği ya da nasıl uygulanacağı konusu giderek daha tartışmalı hale gelmektedir. Katılımcı 3, bu sisteme güvenilmesi için henüz erken olduğunu ifade ederken, asıl önemli olanın uygulamaları/organizasyonları geliştirecek olan yazılımcıların güvenilir olması gerektiğini belirtmektedir:

“Blok Zinciri ve merkeziyetsiz sistem için şu anda büyük firmalardan daha güvenilir demek çok erken. Bence şu anda çok açıkları var. Birçok şey duyuyoruz koca koca sistemlerin, milyon dolarların içeride yatırılmış olan sistemlerin hacklendiğini veya bir anda değerlerinin sıfırlara düştüğünü falan duyuyoruz, okuyoruz. Burada önemli olan o sistemi geliştirecek olan yazılımcıların çok güvenilir olması. İnsanların onlara çok güveniyor olması lazım. Veya öyle bir noktaya gelecek ki işte o yazılım, o merkeziyetsiz dediğimiz uygulamalar, milyonlar tarafından kullanılacak ve sistemin çekirdeğini yazan yazılımcılar biz burada bir yanlış yaparsak milyonlar üzerimize çöker diye düşünüp yapmamaya yönelecek. Ama şu andaki ortamda hackerlar için çok daha güzel bir yer. Şu an için öyle. Belki ileride çok daha böyle stabil yazılımlar olacak. Şu an için yine bir merkezden yazılıyor. Yazılan şey merkeziyetsiz hale geliyor; ama temelde yapı birileri tarafından yazılıyor” (K.3).

Burada Katılımcı 3’ün ifade etmeye çalıştığı, uygulamaları/organizasyonları geliştiren ekibin -bu ekip kurucudan araştırmacılara, pazarlamacılardan reklamcılara geniş bir ekiptir- güvenilir olmaları ve sistemin sürdürülebilir olması için çalışıyor olmalarıdır. Katılımcı 4’e göre bu sistem, toplumsal olarak bir sorumluluk bilinci içinde davranılırsa ancak başarılı olabilir. Ona göre bu sistemde yer alanların, uygulamaların/organizasyonların istila edilmemesi ve sürdürülebilir olmaları için organize olunarak aktif rol alınmasını ve toplumsal bir görev bilinci içerisinde davranılmasını gerektirmektedir:

“Bu sistemin devam etmesi için birilerinin rol alması lazım. Açık kaynak kodu mantığı, yani bizim verilerimiz, büyük tekeller tarafından kullanılmasın deyip böyle bir Reddit topluluğu gibi ortaya çıkıp bir şeyler yapılırsa bunun mümkün olduğunu düşünüyorum ama onun dışında gerçekten ben zamanımı ayırıp bir iş yapıyorsam ondan bir fayda bekliyorumdur. Bu şekilde bir toplumsal görev olarak görülüp yapılabilir, mümkün. Gerçekten olabileceğine inanıyorum. Ama bunun içinde büyük kitlelerin bir şekilde organize olması lazım” (K.4).



Şekil 3.16 Blok Zinciri - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.16’da gösterildiği üzere “Blok Zinciri” temasıyla “Merkeziyetsizlik Çelişkisi” alt teması arasında oldukça güçlü bir bağ bulunurken bu iki temanın “Tekelleşme” ile ilişkisi bulunmaktadır. Ayrıca “Blok Zinciri” temasıyla “Gizlilik” teması arasında güçlü bir ilişki bulunmaktadır. “Gizlilik” temasının da “Geliştirici Hassasiyeti” ve “Regülasyonların Etkililiği” alt teması arasında güçlü bağlar vardır. Blok zinciri ve merkeziyetsizlik arasındaki bağlar katılımcıların merkezi olmayan uygulamaların da bir süre sonra merkezileşebileceği ya da merkeziyetsiz platformların merkezi platformların karşısında pek de bir şansının bulunmadığı yönündeki baskın görüşleri nedeniyle oluşmuştur. Şekle bakıldığında blok zinciri tabanlı uygulamalara güvensizliğin olduğu ve şüpheyle yaklaşıldığı görülmektedir. Öte yandan blok zinciri tabanlı uygulamalarda da mobil uygulamalara benzer şekilde gizlilik, geliştirici hassasiyeti ve regülasyon konularının ilişkilendirildiği görülmüştür. Şüpheyle yaklaşılan ve henüz tam anlamıyla güvenilmeyen bu uygulamaların da yine alternatifsizlikle nitelendirilmesi de dikkat çekici bir sonuçtur. Merkezi uygulamalara kıyasla alternatifi olsa da özellikle popüleritelerinin düşük olması nedeniyle bu tür uygulamalarda bulunan sistem alternatifsizliği de bir başka unsur olarak göze çarpmaktadır.

Alternatifsizliğin İtirafı

Katılımcı 2 ve 11, merkezi uygulamalara alternatif olabilecek pek fazla merkeziyetsiz

uygulamanın olmadığından bahsederken, merkezi uygulamaların cazibesinin hala kuvvetli olduğunu belirtmişlerdir. Merkezi uygulamaların işlerliğinin merkezi olmayan uygulamalara göre daha verimli olduğunu ve merkezi uygulamaların kullanıcılara verdiği güvenin merkezi olmayan uygulamalardan daha yüksek olduğunu dile getirmişlerdir. Ayrıca katılımcı 11, merkezi olmayan uygulamaların merkezi uygulamaların hakimiyetine en azından şimdilik son veremeyeceğini söylerken, iki sistemin beraber yürütülebileceği konusunda görüş bildirmiştir:

“Alışkanlık... Birde doğru yazılımlar doğru anda oradalar. Merkeziyetsiz uygulamaların tekellerle savaşması çok çok zor. Mesela YouTube’un alternatifleri yok mu? Var. Ama niye kimse kullanmıyor? Çünkü YouTube daha iyi yapıyor her şeyi. Bir diğer problem de sansür problemi oluyor aslında uygulamalarda. Mesela hep sansürden şikayetçiyiz biz. Facebook sansürlüyor, Twitter sansürlüyor diyoruz. Facebook’un alternatifleri var. Giriyorsun sadece faşistler var orada, aşırı sağcılar var. Çünkü niye? Banlanmış oraya gitmiş. Orada takılıyor şu anda. Herkes gelsin... Herkes gelmiyor niye? Çünkü o muhabbetlere katılmak istemiyorlar” (K.2).

“Merkezi olmayan uygulamalar blok zincir üzerinde olan uygulamalar. Haberleşme uygulaması olan WhatsApp ile değil de Merkezi olmayan bir uygulama ile yazıyorsun. YouTube değil de onun alternatifi olan merkeziyetsiz bir uygulama aracılığıyla videolarını yayınlıyorsun. Bunun bazı avantajları da var dezavantajları da. Avantajlarından bazıları örneğin bazı uygulamalar yayıncısına ya da merkeziyetsiz uygulamasını kullanan kişiye ödeme yapabiliyor ya da bu bir reklam yayıncısıysa indirim yapabiliyor. Tabii bazı sorunlar da var. Bunlardan bazıları güncellenme. Örneğin, herhangi bir açık varsa uygulamada bunu düzeltmesi zaman alıyor ve bu bazı ihlallere neden olabiliyor mesela birçok kripto para hırsızlığı oldu. Merkezi, yani anında müdahale edebileceği bir ekip yoksa bu ciddi sıkıntılar doğurabilir. Merkezi olmayan organizasyonlar da gönüllüğü esas alıyorlar veya topluluklar var ve bu topluluk o organizasyonu yönetiyor; ama sonuçta maaşlı bir çalışan değil bu kişiler. O oluşumun kripto parasına sahip olan kişiler olabilir; ama zorlayıcı veya itici bir güç olmadığından kurallar konusunda da geride kaldığını düşünüyorum. Mastodon gibi uygulamalar var mesela buralarda gördük çok da fazla ilgi görmedi açıkçası ama bu geliştirilmeyeceği anlamına da gelmez. Merkezi uygulamalarla merkeziyetsiz uygulamaların birlikteliği bence daha önemli. Merkeziyetsiz uygulamalar mevcut merkezi uygulamaları yok eder diye bir şey söyleyemeyiz bence, İnternetin televizyonu nasıl tamamen ortadan kaldırmadysa aynı durum” (K.11).

Blok Zincirinde Veri Gizliliği

Blok zinciri, verilerin dağıtık bir ağ üzerinde birden fazla cihazda paylaşılarak depolanmasına imkân tanıyan bir teknolojidir. Bu nedenle merkezi sunucuların karşısında konumlanan ve kişisel verilerin gizliliği açısından dikkate alınması gereken bir sistem olarak görülmektedir. Katılımcılardan 1, 4 ve 11, blok zinciri ve uygulamalarının bazı güvenlik mekanizmaları sayesinde veri sızıntılarının engellenebileceğini ve veri gizliliğinin korunabileceğini iddia etmişlerdir:

“İmkânsız diyemem ama imkânsıza yakın çok zor yani. Çünkü bir şifrelemeden geçiyor. Ayrı bir filtreden geçiyor ve sadece siz uygun şifreyi açabiliyorsunuz. Şifreleme anahtarı sizde” (K.1).

“Blok zincir teknolojisiyle, iki faktörlü şifrelemelerle mümkün gibi gözüküyor” (K.4).

“Gizlilik konusuna geldiğimizde verileri koruyabilir. Merkeziyetsizliğin mantığı bu. Şu an bu sistemin iddiası verileri koruduğu yönünde. Doğası gereği merkezi bir yapı olmadığı için veriye ihtiyaç duymayabilir, veriyi de zaten merkezi bir sunucuda tutmuyorsa gizlilik ve güvenlik açısından olumlu” (K.11).

Katılımcı 4, bu sistemlerle korunabileceğini düşünse de manipüle edilebileceğini dile getirmiş, merkeziyetsiz sistemlerle merkezi sistemlerin hibrit bir şekilde kullanılmasının gizliliği ortadan kaldıracabileceğini ifade etmektedir. Örneğin, benzersiz kimliğe sahip kripto varlık cüzdanlarıyla merkezi sistemlere yapılan varlık aktarımında bu izler takip edilebilir ve kişinin kimliği anonim olmaktan çıkabilir. Bu durum varlıkların tehlikeye atılması ve dolayısıyla da veri gizliliğinin sağlanamayacağı anlamına gelmektedir:

“Ama bence bir noktada yine şirketler bunu manipüle edebilirler. Çünkü sonuçta sen kimliğinle bir şekilde Binance’a giriyorsun. Bir şekilde swap sitelerine [kripto varlık değişimi] sitelerine kaydoluyorsun. Yine senin bir kimliğin olmuş oluyor gün sonunda. Yeteri kadar merkeziyetsiz gelmiyor bana. Yine belli kitlelerin altında toplanıyor, belli varlıklar, belli bilgiler. Bunun olması için belki zaman gerekli diyebilirim. Şu an ona uygun bir düzen olmadığını düşünüyorum” (K.4).

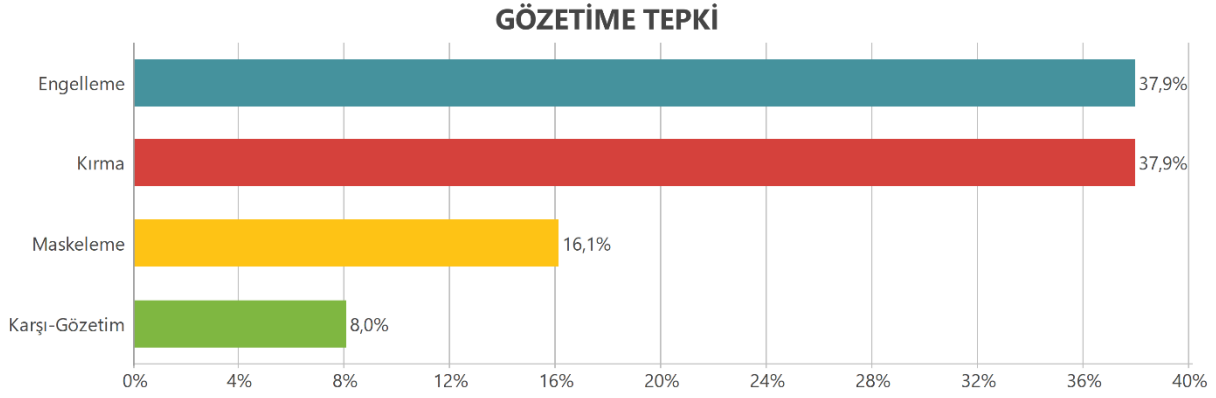
Katılımcı 9 ise blok zinciri ve uygulamalarında mevcut durumda dahi verilerin tamamen anonim olmadığını dile getirirken, veri toplayabilecek mekanizmaların bulunduğunu ileri sürmektedir:

“Veriyi anonim haline getirdiler mi? Çok sanmıyorum. Arka taraftan yine o veriyi toplayabilirim açıkçası. Bunu yapabileceğim kanallar var” (K.9).

3.2.3.3. Katılımcıların Veri Gözetimine Karşı (Mukavemet) Tepki Hamlelerinin Analizi

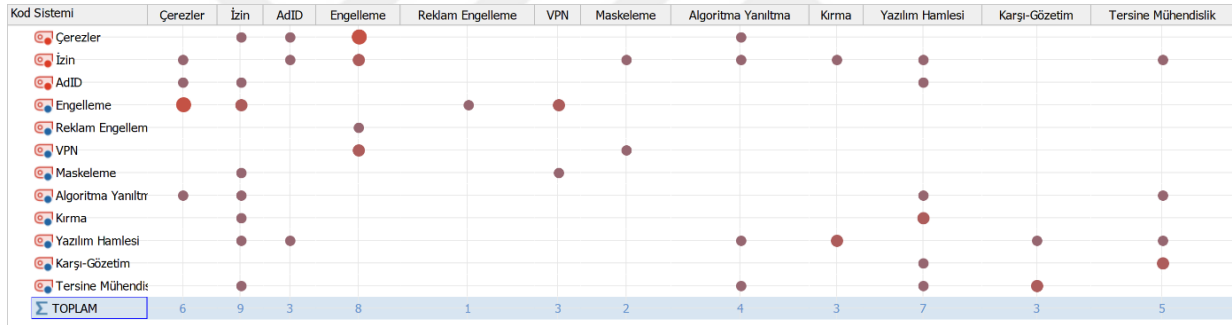
*Evin kapısını kilitlemek her zaman hırsızlıktan
korumaz seni. Ama açık bırakmıyorsun (K.2).*

Bu kategori altında katılımcıların gözetime karşı direniş gösterip göstermediği, gözetimden kaçınma ve karşı koyma stratejilerinin olup olmadığı ortaya çıkarılmaya çalışılmıştır. Geliştiricilerin ifadeleri G. T. Marx (2018)’in karşı-gözetim hamleleri çerçevesinde analiz edilmiştir.



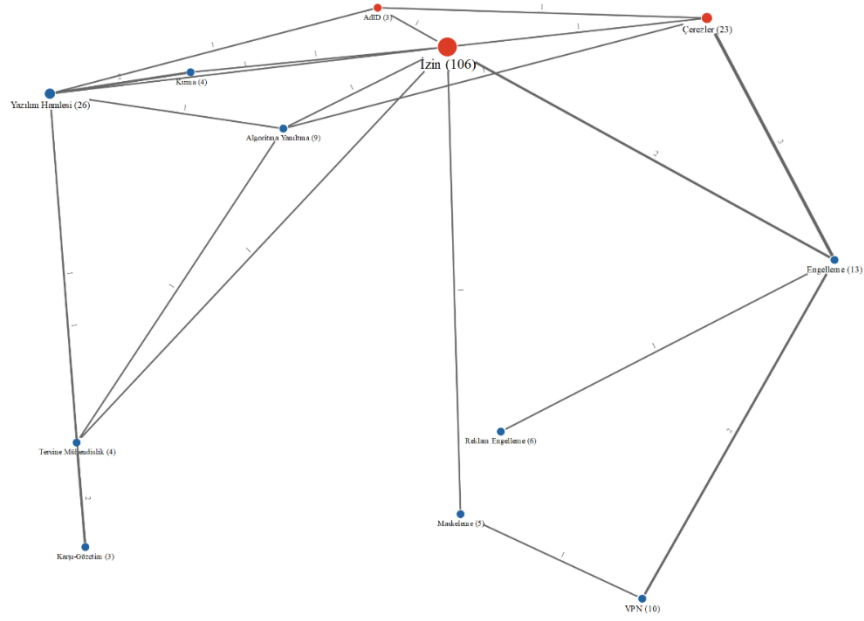
Grafik 3.8 Gözetime Tepki Kategorisinde Yer Alan Temaların Kod İstatistiği

Grafik 3.8’de gösterildiği üzere “Gözetime Tepki” kategorisi altındaki kodlamalar en çok “Engelleme” ve “Kırma” temalarına yapılmıştır. “Maskeleye” ve “Karşı-Gözetim” temalarına ise daha az sayıda kodlama yapılmıştır. “Gözetime Tepki” kategorisinde sıklıkla birlikte kodlanan temalar da aşağıda verilmiştir:



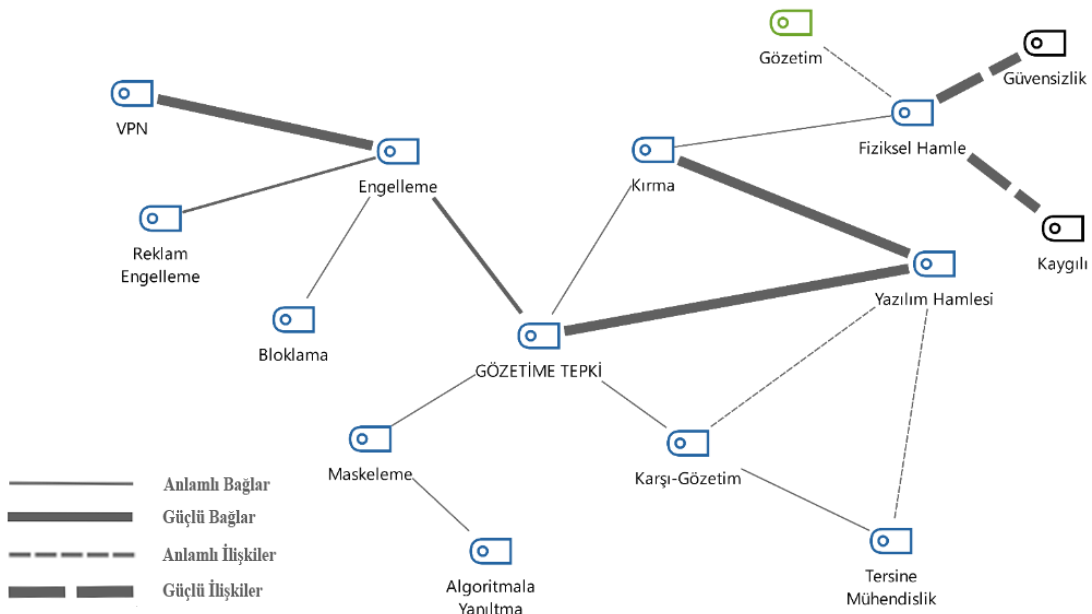
Grafik 3.9 Gözetime Tepki Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri

Grafik 3.9’da gösterildiği üzere katılımcıların ifadeleri, en çok “Engelleme” ve “Çerezler” temasıyla ilişkilendirilmiştir. Ayrıca “İzin” ve “Engelleme” temalarına daha fazla kodlama yapıldığı da görülmektedir. Aşağıda verilen şekilde ise bu temalara ait kod haritası verilmiştir:



Şekil 3.17 Gözetime Tepki Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası

Şekil 3.17’de gösterildiği üzere “Gözetime Tepki” kategorisi altındaki “Kırma” teması “Yazılım Hamlesi”, “Algoritma Yanıltma” ve “İzin” temaları ile yakın ilişki içerisinde olup sık bir biçimde kodlanmıştır. “Engelleme” teması da “İzin” ve “Çerezler” temaları ile yakın ilişki içerisinde olup sık bir biçimde kodlanmıştır. Bu kategori altına kodlanan ifadeler diğer kategorilere göre daha seyrek. Bu veri, katılımcıların gözetime tepki hamlelerinin var olduğunu gösterse de gözetime direniş biçimlerinin mukavemet şeklinde olduğu ortaya koymaktadır.



Şekil 3.18 Gözetime Tepki - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.18’de gösterildiği üzere “Gözetime Tepki” kategorisiyle “Yazılım Hamlesi” alt teması arasında, “Yazılım Hamlesi” alt temasıyla “Kırma” teması arasında çok güçlü bir bağ vardır. “Engelleme” teması ile “VPN” alt teması arasında güçlü bir bağ vardır. “Fiziksel Hamle” alt temasıyla ise “Güvensizlik” ve “Kaygılı” duygu temalarıyla çok güçlü bir ilişki vardır. Veri gözetimine karşı gösterilen tepki, doğrudan yazılımla alakalıdır. Hem engelleme hem de kırma hamleleri tamamen yazılım veya mevcut yazılım uygulamalarıyla gerçekleştirilmektedir. Yalnızca kırma hamlesi fiziksel hamleyle ilişkilendirilmiştir. Burada katılımcıların dijital gözetimden rahatsızlıkları ön plana çıkmaktadır. Kendilerini güvende hissetmeyen bazı katılımcılar, gözetlendikleri kaygısını taşımaktadır. Bu nedenle bazı katılımcılar cihazlarının kameralarını bantla kapattıklarını ifade etmişlerdir. Sıklıkla engelleme hamlesine başvuran katılımcılar VPN kullanımını öne çıkarırken, reklam engelleme ve çeşitli kodlarla veri akışını engelleme gibi yöntemlere de başvurdukları anlaşılmaktadır.

Engelleme Hamleleri

Veri gizliliğine ve gözetime dikkat eden katılımcılar, veri toplamayı olanaklı kılan mekanizmaların mümkün olduğu kadar engellenmesi gerekliliğini dile getirmişlerdir. Katılımcı 2, reklam engelleyicileri kullanarak reklam verilerini, Katılımcı 5 ise yardımcı uygulamalarla analitik verileri engellediğini belirtmiştir:

“Bir geliştirici senin bilgilerini topluyor. Bir de reklamı sana veren kişi topluyor. Uygulamaya üçüncü bir sağlayıcıdan reklam alınıyor çünkü. Bir de üçüncü beşinci kişilere falan da gidiyor ve ne kadar çok reklam varsa o kadar çok kişiye gidiyor bilgiler. O yüzden de reklamları sadece reklamları engellersek bile bunun büyük önemi var. Etkisi olacaktır şu anda. AdBlock’u komple ağına da kurabiliyorsun. Ancak hepsini engellemek mümkün değil. Çünkü zaten sitenin çalışabilmesi için neyi tıkladığını bilmesi gerekiyor. Bunları tutacak yani en azından” (K.2).

“IOS’ta “1 Blocker” diye mesela bir tane uygulama var. Analitik verilerinin nereye gönderildiğini görüp onları network seviyesinde blokluyor. Yani göndermeye çalışırken göndermesini engelliyor. O zaman ne oluyor? Sen analitik verin gitmiyor. Böyle mekanizmalar var” (K.5).

G. T. Marx (2018: 30), engelleme hamlelerinden bahsederken, kişinin herhangi bir mesaj ya da ileti gönderirken gönderici bilgilerini gizleyen anonim e-postalar kullandığı durumlarda, bu girişimin belirlenmeyi önleyerek gönderenin izini kaybetme olanağı sağladığını dile getirmiştir. Katılımcı 2 ve 5 de IP adreslerini gizleyen VPN uygulamalarının karşı sunuculara gönderilen verileri anonim hale getirdiğini ve böylelikle kullanıcının da anonim kalabileceğini ifade etmiştir:

“Mümkün olduğunca kadar gizlenmeye, mümkün olduğunca anonim kalmaya çalışıyorum. Bir analogi olarak çok güzel bir önermeye denk gelmişim. Tuvalette ne yaptığınızı herkes biliyor; ama yine de kapıyı kapatıyorsunuz. Böyle bir şey bu da sanırım. VPN kullanıyorum bu yüzden” (K2).

“Tor [The Online Router] gibi tarayıcılardan internete girdiğiniz zaman anonim bir şekilde maskelenerek gezinebiliyorsun. Mobil uygulamalarda da VPN uygulamaları var. İyi VPN’lerden bahsediyorum. Bunları kullanarak olabildiğince takip edilmeyi minimuma indirebilirsin. Bu uygulamalar büyük oranda seni maskeleyiş oluyor yani” (K.5).

VPN kullanılarak gözetime verilen bu tepki hamlesi aşağıda da belirtilecek olan maskeleyme hamlesi (enformasyonun yanıltıcı olması) ile benzerdir. Çünkü VPN kullanımında sahte IP adresleri kullanılmakta, dolayısıyla karşıya giden enformasyon da sahte olmaktadır. Ancak bazı durumlarda VPN kullanımı açığa çıkabilir. Katılımcı 8, VPN kullanımında kendini anonim hissetmemektedir:

“VPN kullandığımda yetkisi olan insanların o oradan yani bir şekilde beni bulabileceklerini biliyorum. O yüzden VPN kullanarak güvendeyim hissini almıyorum” (K.8).

Birçok VPN uygulamasının kullandığı IP adresleri standarttır ve bu gözetleyen tarafından belirlenebilir. Bu adresler tespit edildiğinde kullanıcının VPN kullandığı ortaya çıkabilir. Bu nedenle VPN kullanımı, engelleme hamlesi olarak değerlendirilmelidir.

Maskeleyme Hamleleri

Maskeleyme hamlesinde ise toplanan veriler, gözetleyen için bir şey ifade etmemektedir: Maskeleymenin bir sonucu olarak, gözetim düzeneği istenildiği şekilde işlese de toplanan enformasyon yanıltıcı ve yararsızdır. Gözetleyenler bunun gerçekleştiğinin farkına bile varmayabilirler (G. T. Marx, 2018: 32). Katılımcıların maskeleyme hamlelerinin var olup olmadığı araştırıldığında, katılımcıların zaman zaman böyle yöntemleri kullandıkları; ancak özellikle bu hamlelere başvurmadıklarını –zorunda kalmadıkça- dile getirmişlerdir. Teknik açıdan maskeleymenin olanaklılığı sorgulandığında, bazı yöntemlerin kullanılabileceğini ifade etmişlerdir:

“Savunma amaçlı kendimde belirli şeyler bırakabilirim. Eğer onlar kullanılırsa, eğer o verileri benden almaya çalışırlarsa eğer, ben o verileri boş gönderirim. Yani orada bir veri yine döner, dönmek zorunda çünkü uygulama çalışmaz. Ama boş döner. Sanki ben de hiç yokmuş gibi veya oradaki yazılım yokmuş gibi ben o veriyi boş olarak döndürürüm” (K.1).

“Arka planda başka videolar izliyormuş gibi gösterebiliriz. Örneğin ben bir Vlog [video blog] izliyorumdur. Ama izlediğim Vlog’un kaynağını [URL- Uniform Resource Loader] arka planda başka bir URL gibi gösterip YouTube’u bu şekilde kandırabilirim, aslında bir anonimleşebilirim” (K.4).

“Bazı uygulamalarla kendimizi maskeleyebiliriz. Diyelim ki bir uygulama konum izni istiyor. Konum izni vereyim mi? Konum izni vermeyeyim mi? Yoksa da sahte bir konum mu vereyim? Böylece uygulamadaki kısıtlamayı geçebiliyoruz. Çünkü mesela uygulama diyor ki konum iznini verirsem bu ekrana ulaşabilirsin diyor. Vermezsen geri gidiyor. O ekrana illa konum izni vererek ulaşmamız lazım. Vermemek bizim seçeneğimiz ama vermesek de uygulamanın bize sunduğu şeyi kullanamıyoruz. Sahte veriler gönderiyoruz mesela, konum istiyorsa sahte bir konum. Galeri izni istiyorsa boş bir galeri verisi vererek izin isteyen uygulamaların o kısıtlamalarını geçmeyi sağlıyor. Hem de sizin verilerinizi korunmuş oluyor” (K.7).

Görüldüğü üzere geliştiriciler, sıradan kullanıcılardan farklı olarak gözetime direnmenin veya etkisiz hale getirmenin teknik açıdan olanaklı olduğunu göstermişlerdir. Sıradan kullanıcılar, teknik açıdan bilgisi olan veya yazılım alanıyla ilgisi olan kullanıcılar da çeşitli yardımcı uygulamaları kullanarak gözetime karşı koyabilirken; alanında uzman geliştiriciler, uygulanması görece zor olan hamlelerle (örneğin kod veya teknik birtakım yazılım imkânlarını kullanarak) gözetimi bertaraf etmeyi başarabilirler. Bu nedenle geliştiricilerin uzmanlığından yararlanılarak gözetimi etkisiz hale getiren TOR³⁸ gibi projelerin yaratılması için çeşitli girişimlerde bulunulabilir.

Maskeleme ve Algoritmalar

Algoritmalar, bilindiği üzere verilerin analizinde kullanılan, kullanıcıyı tanıyan, öğrenen ve ilgi alanlarına göre onlara sonuçlar çıkartan yazılımlardır. Buradan hareketle algoritmaları yanıltmanın kullanıcıyı maskeleyerek anonim olmasını sağlayabileceği düşünülmüş, bu şekilde bir hamlenin kullanıp kullanılamayacağı sorusu katılımcılara yöneltilmiştir. Katılımcı 2 ve 5, algoritmaların yanıltmanın çok zor olduğunu, bir yerde ona yakalanma ihtimalinin olduğunu dile getirmişlerdir:

“Yanıltmanın bir yolu olduğunu düşünmüyorum. Çünkü özellikle bir uygulama indirip içine girdiysek zaten büyük ihtimal üyelik açmışızdır” (K.2).

“Çok zor; çünkü senin her davranışın kaydediliyor. Mesela Instagram’daki bir gönderide kaç saniye durdun, baktın o görsele... Onların hepsinin kaydını tutuyor ve senin orada bulunduğun ağırlıklı ortalamaya bakarak senin tercihlerini gösteriyor. Ona göre karar veriyor. Yani her hareketin kaydı tutulduğu için bundan kaçınmak, kandırmak çok kolay bir şey değil açıkçası” (K.5).

Bazı katılımcılar ise teknik olarak algoritmaların yanıltılabileceğini; başkası gibi davranarak veya sahte bir profil oluşturarak algoritmanın kullanıcı hakkında yanlış veri

³⁸ Tor Projesi, Tor ağını geliştiren ve sürdüren kâr amacı gütmeyen bir kuruluştur. Açılımı “The Onion Router” olan Tor, kullanıcıların internette anonim ve güvenli bir şekilde gezinmelerini sağlayan ücretsiz ve açık kaynaklı bir yazılımdır <https://www.torproject.org/about/history/> (erişim tarihi: 24.09.2023).

toplamasının sağlanabileceğini dile getirmişlerdir. Katılımcı 5, algoritmaları yanıltmanın zor olduğunu söylese de algoritmanın sahte ilgi alanları yaratılarak yanıltılabileceğini dile getirmiştir:

“Ama tabii ne yapabilirsin? İşte hiç senin ilgi alanın olmayan, farklı şeylere gidip algoritmanın kafasını karıştırabilirsin. Bu sefer de sana tavsiye edilen şeyler senin ihtiyacın olan ya da istediğin, görmek istediğin şeyler olmaz. Böyle bir durum var. Onun dışında da başka bir seçenek yok” (K.5).

Katılımcı 4 de yeni bir cihazda, yeni bir hesap ve profile, algoritmaya sahte bir profil çizilebileceğini ve teknik açıdan anonim kalınabileceğini belirtmiştir:

“Evet aslında kandırabilirsin. Sonuçta senin izlediğin videolardan yola çıkıyor. Ya da senin beğendiklerinden, yorum yaptıklarından yola çıktığı için tertemiz bir hesap açıp orada bu algoritmayı yanıltabilirsin” (K.4).

Katılımcı 3 ve 11 ise her ne kadar algoritmalar yanıltılsa bile algoritmaların kullanıcıyı yanıltıldığı şekliyle tanıyacağı ve bunun pek de sürdürülebilir bir şey olmayacağını ifade etmektedirler:

“Belirli algoritmaları çözebilirsiniz ama benim tahminimce arka tarafta mümkün olan en insancıl varyasyonda düşünebilen yazılımlar çalışıyor ve sizin hareketlerinizi takip ediyor. Yani bir iki kere yanılttıktan sonra o düzeni de kavrayıp size uygun sonuçlarla dönebilirler. Burada önemli olan ne kadar kurtulmak istiyoruz? Ne kadar istemiyoruz?” (K.3).

“Algoritmaları yanıltabilirsiniz ama yanılttığınız şekilde de sizi tanımaya başlar. Bir süre sonra yanılttığınız şekilde size bazı geri dönüşler yapar. Evet böylece gizlenebilirsiniz; ama bu ne kadar sürdürülebilir bilmiyorum bir şekilde bir yerden patlak verilecektir. Kimsenin sürekli anonim kalmak isteyeceğini düşünmüyorum” (K.11).

Katılımcıların ifadeleri özetlenecek olursa, algoritmaların yanıltılmasıyla anonimliğin kısmen sağlanabileceğini; ancak bunun sürdürülebilir olmayacağını ve özellikle Google veya Apple gibi şirketlerin hesaplarına giriş yapıldığında tekrar başa dönebileceğini dile getirmişlerdir. Sonuç olarak algoritmalar kullanıcı gizliliği tehlikeye atabilecek yazılımlardır. Çünkü kullanıcıları tanıyarak davranış verileri hakkında derin bilgiler elde etmekte ve bu verilere göre sonuçlarla onları yönlendirmektedir. Dolayısıyla algoritmalar gözetim sürecinin ve veri sömürsünün bir parçası olarak görülmelidir.

Kırma Hamleleri

G. T. Marx (2018: 33)’a göre kırma hamlelerinin kullanılma amacı, gözetleyen aygıtı çalışmaz hale getirmektir. G. T. Marx, bunun fark edilebilir olacağını özellikle dile getirirken,

bu hamleyi aynı zamanda en kaba etkisizleştirme biçimi olarak görmektedir. Bu hamleyi örneklendirirken, elektronik cihazlara verilen çeşitli zararlardan bahsetmektedir. Bunlar arasında iletişimi etkisiz hale getirmek veya video kameralara spreya boyası sıkılması gibi bazı girişimler bulunmaktadır. G. T. Marx, bu hamlelerin tıpkı engelleme hamlesinde olduğu gibi gözetleyenler tarafından tespit edileceğini de ekler. Katılımcıların bazı ifadeleri, tam da bu hamlelerle doğrudan bağdaşmaktadır. Katılımcı 4 ve 8, cihazlarındaki donanımların bazılarını fiziksel veya yazılımsal olarak devre dışı bırakmaktadır:

“Kişisel bilgilerimle ilgili bir kaygım yok. Zaten buna ulaşabildiklerini biliyorum. Ve bu beni rahatsız etmiyor; ama rahatsız ediyor olsaydı bundan kaçınma yöntemlerini biliyorum ve kullanabilirdim. Maksimum yaptığım şu an kameramı kapatıyorum. İşte ses mikrofونlarının alıcılarını kapatıyorum bilgisayarımda” (K4).

“Genel olarak kamerasını bantla kapatan bir kullanıcıyım. Yani herhangi bir uygulama beni takip etmese de kameranın karşısında eğer diyelim ki kameranın görmesini istemediğim bir şey bir durum varsa kendi önlemimi daha önceden alırım” (K.8).

Burada Katılımcı 4’ün ifadesi dikkat çekicidir. Kişisel verilerine erişilmesi veya sızdırılmasının kendisini rahatsız etmediğini ifade ettikten sonra kamera ve mikrofونunun alıcılarını kapattığını dile getirmiştir. Bu çelişik ifade, aslında derinlerde bir kaygının olduğu ancak geliştirici kimliğinin yarattığı bir özgüven duygusu ile davranmış olabileceğini göstermektedir.

Katılımcılar mobil uygulamalarda bazı kırma hamlelerinin kullanılabileceğini dile getirmişlerdir; ancak bu hamlenin uygulamanın karasız çalışmasına sebep olabileceğini dile getirmişlerdir. Katılımcı 3, veri toplamayı engelleyen kodların yazılabileceğini, Katılımcı 8 ise veri akışının durdurulabileceğini ifade etmiştir. Katılımcı 10 ise genellikle tanıtım ve pazarlama amaçlı olarak kullanılan “0850”³⁹ kodu ile başlayan numaraları bloke eden bir mobil uygulama yazdığını dile getirmiştir:

“Veri toplamayı engelleyen kodlar yazılabilir. Ama öyle bir yazılım kullandıktan sonra büyük ihtimal Google Chrome kullanamazsınız. Instagram kullanamazsınız, Twitter kullanamazsınız veya telefonu kullanamazsınız gibi bir noktaya gidebilir konu” (K.3).

“Bir uygulamanın içindeki kodları geçersiz kılamayız. Ama o anki akışı durdurabiliriz. Mesela internet akışını, o an bir şey indirmesi gerekiyorsa indirmemesini sağlayabiliriz belki. Ama bu da muhtemelen gerekli şeyleri de yapmamasına yol açar. O yüzden pek bana olası gelmedi açıkçası” (K.8).

³⁹ Bu alan kodu genellikle çağrı merkezleri için kullanılan bir koddur. Gözetimle doğrudan olmasa da dolaylı bir bağlantısı vardır. Örneğin gizlilik sözleşmelerinde/politikalarında yer alan üçüncü taraf bir pazarlama şirketine aktarılan telefon verisi, bu şirketten gelen aramayla sonuçlanmaktadır.

“Şöyle bir uygulama ihtiyacı olmuştu bende. Telefon numaralarını bloklama gibi bir şey yazdım. O zamanlar da çok yoktu. 8-9 sene önce yazmıştım. Benim verime bir şekilde ulaşılmış, yani telefon numarama. Bir liste şeklinde kara liste şeklinde 0850’li numaraların aramasını engelleyen bir uygulamaydı” (K.10).

Bazı katılımcılar ise G. T. Marx’ın yukarıda da değindiği üzere bu kırma hamlesinin - kod yazarak veya eklentilerle gözetimi etkisiz kılmaya çalışmanın- gözetleyen tarafından fark edilecek bir hamle olduğunu, geliştiricilerin hamleyi görüp karşı bir hamlede bulunabileceğinden bahsetmişlerdir:

“Spesifik olarak her uygulama için çalışman gerekir. Çünkü uygulama için de yöntemler hep değişiyor. Instagram farklı toplar, YouTube farklı toplar. Burada o yüzden önce onun kişisel verilerini hangi kanallardan takip ettiği, hangi izinlerini manipüle ettiği kötüye kullandığını bildikten sonra bunu bir şekilde kırmayı başarabilirsin. Ama burada şöyle de bir gerçek var. Sen bunu yaptığın zaman bu büyük şirket bunun farkına varacak ve senin metoduna karşılık yeni bir veri toplama yöntemiyle tekrar senin aslında önüne geçmiş olacak. Bu şirketlerin büyüklüğü bence göz ardı edilmemeli. Arka planda inanılmaz bir veri akışı var. O yüzden en büyük gelir kaynaklarını da böyle hafife almazlar diye düşünüyorum. Sana karşı yine bir sıfır, iki sıfır öne geçebilirler. O yüzden bu biraz da aslında yarışa döner” (K.4).

“Mobil uygulamalarda biraz zor olabilir bu iş. Ama muhtemelen yapılabilir. Çünkü baktığımızda o da bir yazılım. Belki işletim sisteminin derinlerine inerek telefonlarda hani bu verilerin toplanması engellenebilir. Uygulamaların veri toplamasını, engelleyebilmek için o uygulamanın kodlarının tekrar geri dönüştürülerek kodlarda çeşitli değişiklikler yapılması ve fonksiyonların iptal edilmesi gerekiyor. Teknik olarak mümkün olduğunu düşünüyorum. Şimdiye kadar bir örneğini görmedim. Çünkü genellikle bu çok dert edilen bir mesele değil günümüzde. Mobil taraftaki verilerin toplanması çok dert edilmiyor. Ve bunu da aslında sürekli olarak yapmak zor. Çünkü mesela Instagram. Sürekli güncelleme alıyor bu uygulama. Belki her hafta güncelleme alıyor. Şimdi bu kodu değiştirdiğinizde bir hafta sonra uygulama değişti. Ne yapalım? Bir daha yapalım aynısını; ama işte biz zaten bunu bir ayda yapmıştık. Böyle olunca aslında hiçbir anlamı kalmıyor. O yüzden de muhtemelen örneklerini görmüyoruz. Çünkü dediğim gibi bu işlem çok kolay bir işlem değil. Belki işte der ki uygulamanız güncel değil, yeni sürümü indirin ya da uygulama kapanabilir. Kullanamayabilirsiniz. O şekilde şeyler olabilir. Yani aslında bunu engellemek açıkçası bence zor” (K.6).

“Evet engellenebilir ancak sürdürülebilir olmayacaktır. Siz mobil uygulamaya müdahale etmek için bir yazılım atacaksınız Google Play’de bu net bir şekilde engellenecektir ya da bir sonrakinde güncelleme almayacaktır ya da geliştirici bunu fark edecek nasıl engellediğini anlayıp, hemen o açığı kapatıp ya da kodu değiştirip sizin bunu yapmanızı yine bertaraf edecektir” (K.11).

Karşı-Gözetim Hamleleri

Katılımcılar, kırma hamleleri ile ilgili görüş bildirirken uygulamaların kodlarıyla oynayarak ya da ek bir yazılım kullanarak, uygulamadan veri toplanmasının engellenebileceğini dile getirmişlerdir. Katılımcı 1 ve 10 da benzer şekilde görüş bildirmiştir. Ancak bu görüşleri dile getirirken kullandıkları “tersine mühendislik” ifadesi karşı-gözetim hamlesinde bulunabileceklerini göstermektedir. Çünkü G. T. Marx (2018: 36), karşı-gözetim

hamlelerinin gözetime verilen diğer on tepkiden farklı olduğunu belirtmektedir: Bu hamle, “... işleri tersine çevirmeyi ve gözetim yapanları gözetlemeyi içerir.” ifadesi bu görüşlerle uyumludur:

“Tersine mühendislik kullanabiliriz. Kodlarla oynayabiliriz, verisini silebiliriz, yeni bir veri seti kurabiliriz. Arkada kontrollerini devre dışı bırakabiliriz. Bunu bozmanın yolları var. Veri paketini bozabilirim. Örneğin Instagram’ın veri akışına karşı ayrı bir uygulama da yazabilirim. Fakat herhangi bir anlamı olacağını düşünmüyorum. Çünkü uygulamanın içerisinde kullanılan servisleri kapatmış olurum ve bu da uygulamayı kullanırken belirli hatalara yol açabilir” (K.1).

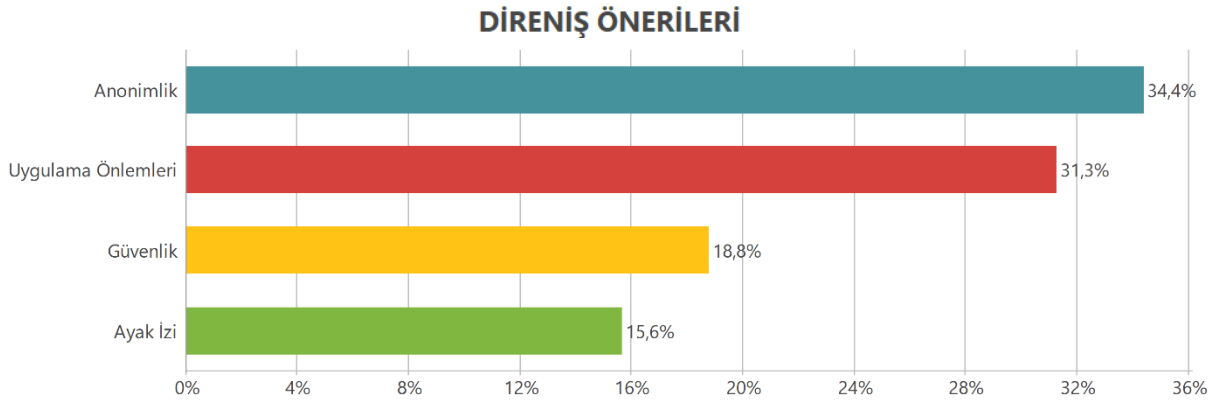
“Öncelikle uygulamanın ne tarz verileri eriştiğini incelemek lazım. Tersin mühendislik dediğimiz bir işlem sürecinden geçirip orada nasıl veri takip ettiğini anlamak lazım. Paketleri inceleyip ne tarz veriler gidiyor, hangi sunucuyla haberleşiyor bu tarz yapılar sunucu üzerinden bloklanabilir en azından ekstra eklentilerle” (K.10).

Yazılım alanında kullanılan tersine mühendislik; bir sistemi veya sistem bileşenlerini çıkarma, işlevselliğini ve tasarımını analiz etme sürecini ifade eder. Bir sistemin bileşenlerini analiz edilmesini veya yeniden yapılandırılmasını sağlar. Ancak, tersine mühendislik yalnızca bu amaca hizmet etmez. Örneğin, zararlı bir yazılım türünün ortaya çıktığı düşünülürse, bu durumda, kaynak kodu bilinmeyen bu tehdide karşı önlemler alabilmek, yazılımın içeriğini anlamak ve aynı zamanda fikri mülkiyeti kötü niyetli kişilere karşı korumak amacıyla da kullanılabilir. Tersine mühendislik, teknikleri ve becerileri gerekmektedir. Bu süreç, kötü amaçlı yazılım dosyasını bir hata ayıklayıcı aracılığıyla açıp iç yapısını kontrol etmekten daha karmaşık işlemlere (örneğin, sanal makine anlık görüntü karşılaştırmaları, ağ izleme vb.) kadar geniş bir yelpazede değişebilir (Uğurlu, 2022: 2). Dolayısıyla Katılımcı 1 ve 10’un kırma hamleleri için tersine mühendisliği yazılım üstünde uygulama düşünceleri, gözetleyenlerin de gözetlenebileceği bir sürece göndermede bulunmaktadır. (Bu da bağımsız geliştiricilere gözetim sorununa karşı proaktif davranma olanağı verebilir.)

3.2.3.4. Katılımcıların Deneyimleri Perspektifinden Kullanıcılara Mukavemet Önerilerinin Analizi

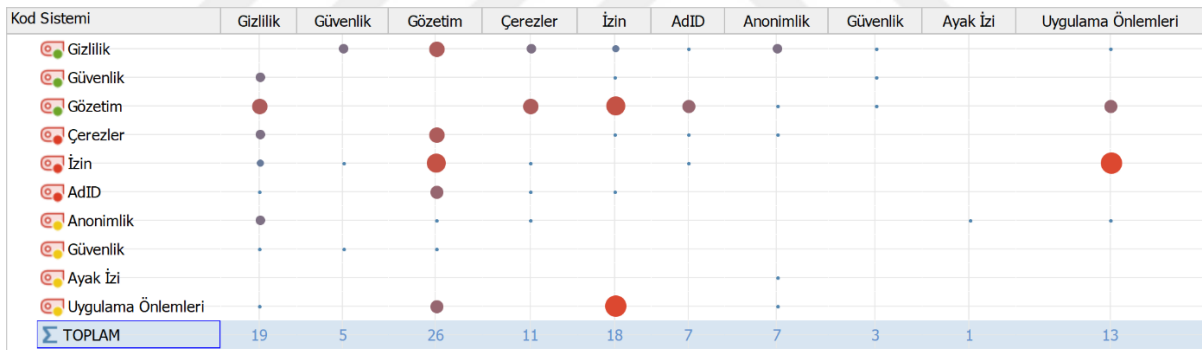
Bence sosyal medya kullanmasınlar. Kesin çözüm (K.5).

Bu kategori altında katılımcıların gizlilik ve güvenlikle ilgili görüşlerine yer verilmiştir. Geliştiricilerin önerileri ve deneyimlerinden yola çıkılarak veri gözetimine karşı sıradan bir kullanıcının bile uygulayabileceği yöntemlere değinilmiş, anonim olmak isteyen kişilerin yararlanabileceği ve onlara yol gösterebilecek bilgilerin verilmesi amaçlanmıştır.



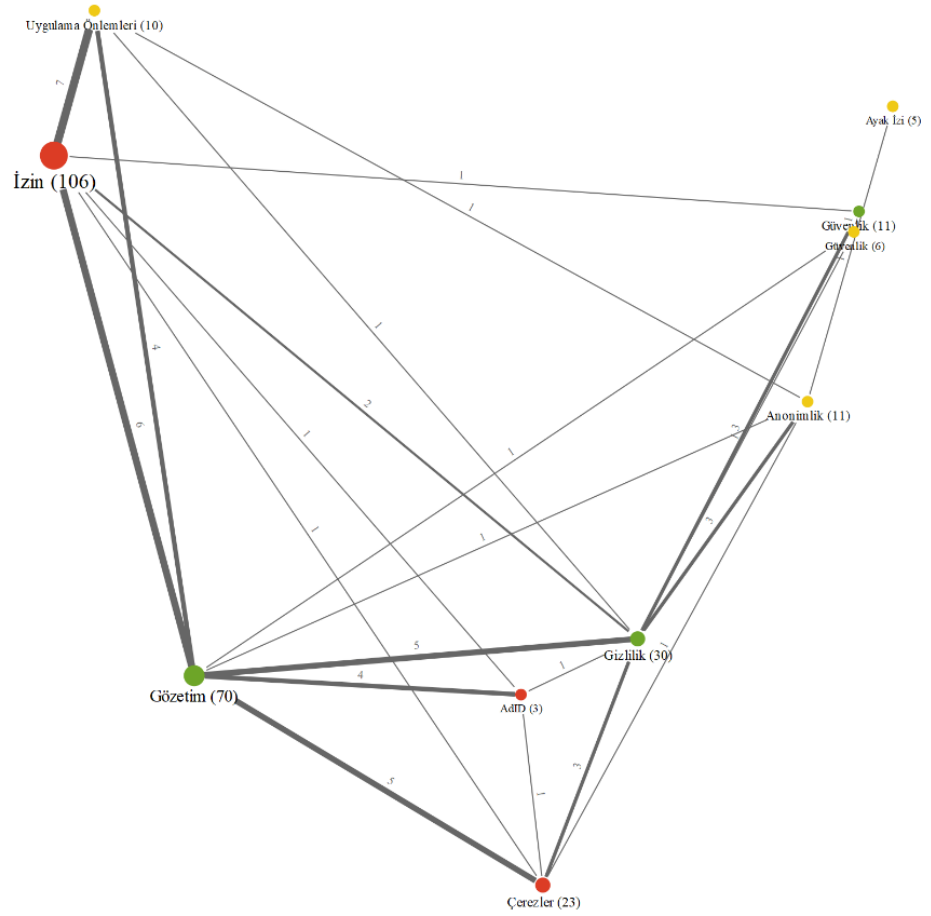
Grafik 3.10 Direniş Önerileri Kategorisinde Yer Alan Temaların Kod İstatistiği

Grafik 3.10’da gösterildiği üzere “Direniş Önerileri” kategorisi altındaki kodlamalar en çok “Anonimlik” ve “Uygulama Önlemleri” temalarına yapılmıştır. Katılımcılar, gizlilik için kullanıcıların neler yapabileceği konusunda önerilerde bulunurken gözetim ve ayak izi gözetim ve reklamlardan bahsetmişlerdir. “Direniş Önerileri” kategorisinde sıklıkla birlikte kodlanan temalar da aşağıda verilmiştir:



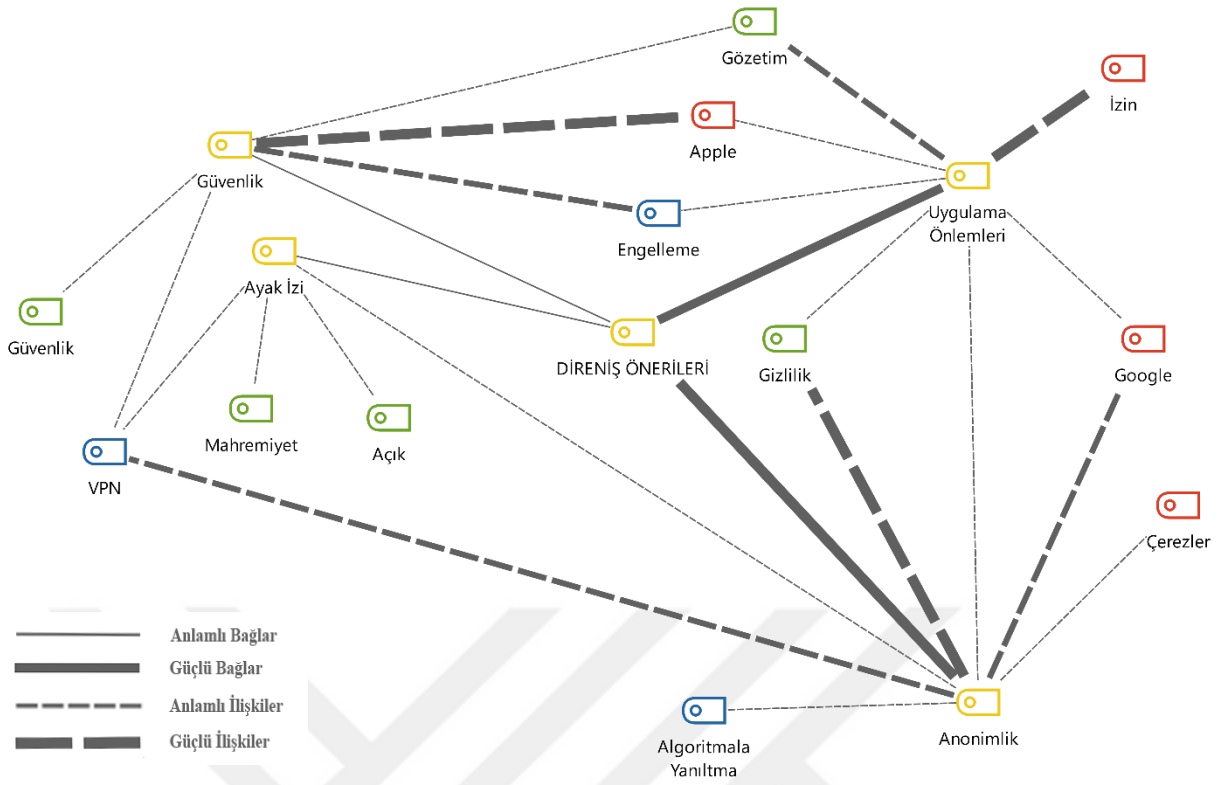
Grafik 3.11 Direniş Önerileri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri

Grafik 3.11’de gösterildiği üzere katılımcıların ifadeleri, en çok “Gözetim”, “Gizlilik” ve “İzin” temasıyla ilişkilendirilmiştir. Aşağıda verilen şekilde ise bu temalara ait kod haritası verilmiştir:



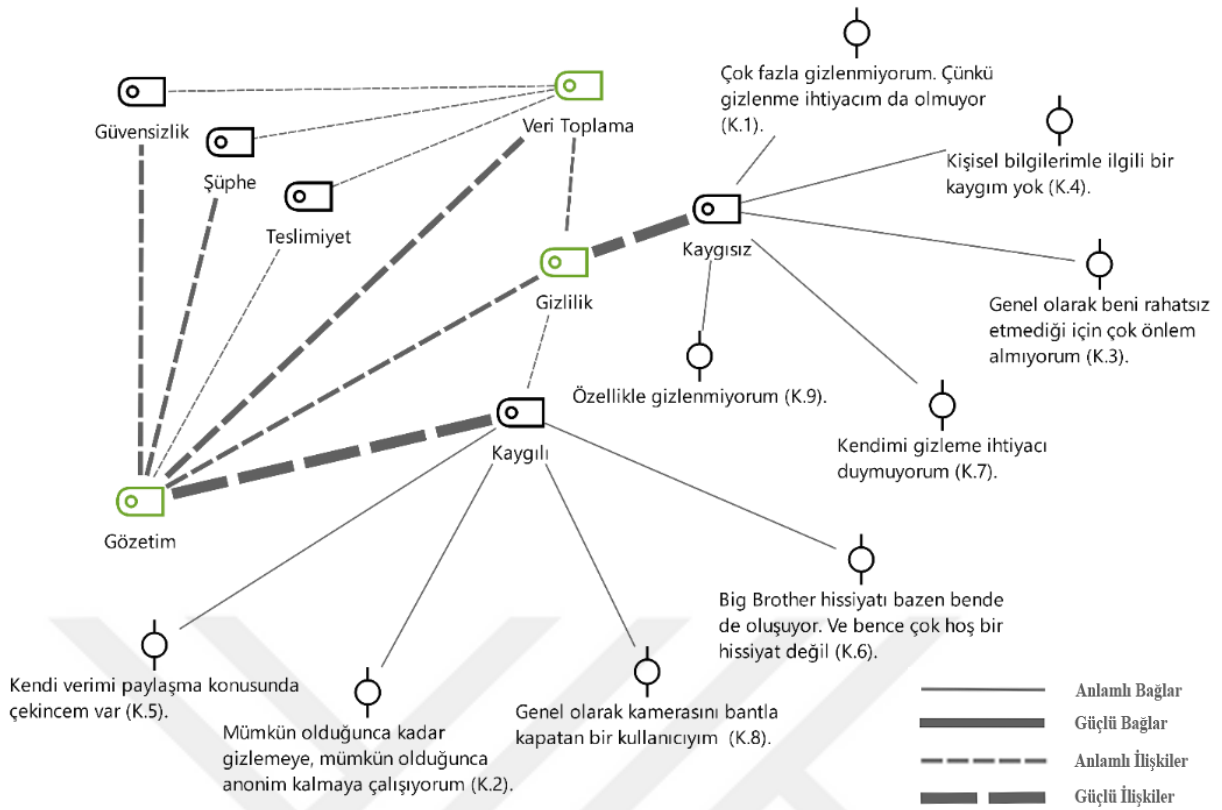
Şekil 3.19 Direniş Önerileri Kategorisinde En Sık Kodlanan Temaların Kod İlişkileri Haritası

Şekil 3.19’da görüldüğü üzere “Direniş Önerileri” kategorisi altındaki “İzin”, “Gözetim” ve “Uygulama Önlemleri” temaları birbirleriyle yakın ilişki içerisinde olup sık bir biçimde kodlanmıştır. “Gizlilik” teması ise “Anonimlik” ve “Güvenlik” teması ile sık kodlanırken yakın ilişki içerisinde. Katılımcılar, deneyimleri çerçevesinde uygulama kullanıcılarına gözetimden kaçınma önerilerinde bulunurken uygulama önlemlerini ön plana çıkarmışlardır. Uygulama izinleri, yukarıda değinildiği üzere kullanıcı mahremiyetinin son kalesi olarak lanse edilmiştir. Bu nedenle uygulama önlemleri katılımcıların oldukça üzerinde durduğu, gözetimden kaçınmanın en önemli yöntemlerden biri olmuştur.



Şekil 3.20 Direniş Önerileri - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.20’de gösterildiği üzere “Direniş Önerileri” kategorisiyle “Anonimlik” ve “Uygulama Önlemleri” temaları arasında güçlü bir bağ vardır. Yine “Direniş Önerileri” kategorisiyle “Ayak İzi” ve “Güvenlik” arasında anlamli bir bağ bulunmaktadır. “Anonimlik” temasıyla “Gizlilik” teması arasında çok güçlü bir ilişki bulunurken, “Google” temasıyla ve “VPN” alt temasıyla güçlü bir ilişki bulunmaktadır. “Güvenlik” teması ise “Apple” temasıyla güçlü bir ilişki içerisindeyken, “Engelleme” temasıyla da güçlü bir ilişki içerisinde olup, sıklıkla birlikte kodlanmıştır. “Uygulama Önlemleri” temasıyla da “İzin” alt teması arasındaki çok güçlü ilişki dikkat çekicidir. Katılımcılar, anonim olmak için VPN kullanılmasını önerirken, anonimliğin aynı zamanda veri gizliliğini ve kullanıcının mahremiyetini kısmen de olsa sağlayabileceğini ifade etmişlerdir. Veri gözetiminden kaçınmak için uygulama özelinde alınacak önlemlerin de aynı şekilde gizliliği sağlayabilecek bir öneri olduğu görülmektedir. Öte yandan güvenlikle Apple’ı ilişkilendiren bazı katılımcılar, veri güvenliği sağlamanın bir yolu olarak Apple cihazlarını önermişlerdir. IOS işletim sisteminde kullanılan bazı yazılımlarla veri güvenliğinin sağlanabileceğini iddia etmişlerdir. Katılımcılar ayrıca dijital ayak izinin minimuma indirilmesiyle, olası veri sızıntısı durumunda kullanıcı mahremiyetinin belli ölçülerde korunabileceğini dile getirmişlerdir.



Şekil 3.21 Duygular - Kod-Alt-Kod-Bölümler Modeli

Şekil 3.21’de gösterildiği üzere “Duygular” kategorisi altında yer alan “Kaygılı” temasıyla “Gözetim” teması arasında, “Kaygısız” temasıyla “Gizlilik” teması arasında çok güçlü bir ilişki vardır. Ayrıca “Güvensizlik”, “Şüphe” ve “Teslimiyet” temaları ile “Gözetim” ve “Veri Toplama” temaları arasında güçlü ilişkiler bulunmaktadır. Şekil 3.32 aynı zamanda “Kaygılı” ve “Kaygısız” temalarına ilişkin katılımcı ifadelerine de yer verilmiştir. Katılımcılar veri toplama süreçlerine şüpheyile yaklaştıklarını, veri gözetimi nedeniyle güvensiz hissettiklerini, ancak bu durum için aynı zamanda bir teslimiyet duygusu içerisinde olduklarını belirtmişlerdir. Katılımcıların bir bölümü veri gözetimine karşı kaygı taşıırken bir bölümü ise herhangi bir kaygı taşımamaktadır. Ancak bu durum aşağıda detaylı olarak verildiği üzere değişkenlik göstermektedir.

Anonimlik

Görüşmelerin başından itibaren katılımcıların internet ortamında anonim kalma konusunda oldukça umutsuz oldukları kanaatine varılmıştır. Katılımcı 1, anonim olabilmek için cihazların kapatılması veya internete hiçbir şekilde bağlanılmaması konusunda görüş bildirmiştir. Katılımcı 5 ise özellikle sosyal medyaya vurgu yaparak sosyal medyanın kullanılmamasının anonim olmaya yardımcı olabileceğini belirtmiştir:

“Ne yapabiliriz en fazla? Telefonumuzu kapatabiliriz kullanmadığımız zamanlarda ya da hiçbir şekilde internet kullanmayın desem?” (K1).

“Bence sosyal medya kullanmasınlar. Kesin çözüm” (K.5).

Katılımcı 1 ise Wi-Fi ağlarının gizliliği ifşa edebileceğini bu nedenle kullanıcıların tanımadığı ağlara erişim yaptığında Sanal Özel Ağ (VPN- Virtual Private Network) kullanmaları gerektiğini söylemiştir. Ayrıca Katılımcı 1, güvenilmeyen Wi-Fi ağlarına bağlanan kişilerin şifrelerinin çalınabileceğini de eklemiştir:

“Mesela ben dışarıda bir Wi-Fi ağına bağlandığım zaman VPN servisi kullanırım. Çünkü Wi-Fi ağında gizlenemezsiniz. Wi-Fi ayağına bağlanıp şifresi çalınan kişiler var. Hatta çoğu zaman tarayıcıda gizli sekmeden giriyorum. Ne kadar gizli olduğu şüphelidir ama tabii belirli araçlar kullanarak onu da halledebiliyorum” (K.1).

Katılımcı 2, 6 ve 11, Google ürünlerine temkinli yaklaşılmasını, mümkün olduğunca bu ürünlerin az kullanılmasını veya gizliliği engelleyen uygulamaların devre dışı bırakılması gerektiği konusunda görüş bildirmişlerdir:

“Google’ın servislerini mümkün olduğu kadar az kullanmaya, kaçınmaya çalışıyorum” (K.2).

“Google Chrome kullanmıyorum. Farklı bir tarayıcı kullanıyorum. Biraz daha gizliliğimi sağlayabilecek şeylere dikkat ediyorum” (K6).

“Google ve ürünlerine temkinlilaşıyorum. Kişiselleştirilmiş reklam ve gizlilik seçeneklerine hep bakar ve kapatırım. Konum geçmiş ve “nereleri ziyaret ettiniz” gibi bu tarz uygulamalar hep devre dışıdır bende” (K.11).

Araştırmanın başlangıcından itibaren geliştiricilerin Google ve ürünlerine karşı olan olumsuz tavrı dikkatten kaçmamıştır. Geliştiriciler Google’dan uzak durarak kullanıcı mahremiyetinin korunabileceğini dile getirmişlerdir. Ancak Share Lab (2015b)’ın araştırmasına göre kullanıcılar, Google servislerini kullanmaktan kaçınıyor olsalar bile internette gezinme davranışlarının %90’ı yine Google tarafından takip edilebilmektedir (Share Lab, 2015b). Ayrıca Google ürünlerini kullanmamak günümüzde oldukça zordur. Geniş uygulama yelpazesi nedeniyle birçok uygulama kategorisinde kullanıcıyı cezbedecek ürünlere sahiptir. Google ürünlerinin tamamına yakını ücretsizdir ve bu da bir çekicilik unsurudur. Katılımcı 2 ise anonim olabilmek için “*Parasını verdiğiniz ürünleri kullanabilirsiniz*” şeklinde bir ifade kullanmıştır. Bu ifade ücretsiz uygulamaların ücretli uygulamalara göre daha fazla veri topladığı dikkate alındığında bir gizlilik önlemi sayılabilir. Öyle ki ücretsiz uygulamaların ücretli uygulamalara göre daha fazla internet erişim, ve konum verisi talep

ettiği tespit edilmiştir (Felt vd., 2011: 5; Chia vd., 2012: 319). Ancak bu ifade daha önce de belirtilen “Hizmet bedavaysa ürün sizsiniz” söylemine atıfta bulunur. Oysaki Zuboff (2021)’un bakış açısına göre üründen çok daha fazlasıyız. Teknoloji şirketlerinin kâr elde etmesi için hammaddelerin çıkarıldığı veri madenleriyiz. Dolayısıyla uygulama ücretsiz olsun veya olmasın, şirketler kullanıcıları veri madeni gibi gördükçe, kullanıcılarından veriyi çıkarabilmek için yine ve yeniden alternatif yollar aramaya, veriyi çıkarmak için farklı gözetim ve sömürü mekanizmalarını denemeye devam edecektir.

Öte yandan kullanıcıların bir bölümü internette anonim kalabilmek için VPN veya çeşitli anonim ağ sağlayıcı projelerin kullanımını önermiştir. Bu öneriler aynı zamanda engelleme hamlesidir:

“En basitinden VPN kullanarak internet sağlayıcınızdan gizlenebilirsiniz. Yani internet sağlayıcınızda ayak izi oluşturmada BTK’ya [Bilgi Teknolojileri Kurumu] veri göndermeden gezinebilirsiniz internet üzerinde” (K.1).

“Benim de kendi çapımda bir gizlilik önlemlerim var. Güvenli olduğunu düşündüğüm VPN şirketlerinin ürünleri kullanırım” (K.11).

“VPN’ler veya işte Tor gibi sistemler kullanılırsa internet anonimliği sağlanabilir. Ama mobilde bu o kadar şu an kolay değil. Bunu yapmak bir mobil telefonda yapmak çok kolay değil. Çünkü genelde Apple’a iCloud [Apple’ın depolama ve bulut bilişim servisi] hesabını bağlayarak, Android cihazlarda da Google hesabını bağlayarak başlıyoruz. Anonimlik orada kırılıyor zaten. Yani o telefon bizim kim olduğumuzu bilerek başlıyor işe. Akıllı telefonumuzla çektiğimiz fotoğraf, kaydettiğimiz ses, izlediğimiz video ve aslında çok kişisel bir şey. O yüzden anonim kalmak aykırı gibi geliyor. Çünkü zaten verilerimizle sürekli besliyoruz ki o verileri kullanarak bize akıllı bir şeyler getiriyor. Araba kullanırken Google Asistan’a “Start Navigation Home” diyorum evime o anda konum rotasını başlatıyor. Telefonuma dokunmadan yapabiliyorum. Şimdi benim evimi bilmeseydi, benim o sırada mikrofonum açık olmasaydı ve dediğimi duymasaydı zaten ben işlevselliği kaybediyordum. O zaman tamamen anonim kalmak istiyorsam, onun bana sunacağı faydalardan yararlanamıyorum demek. Belli bir taviz var yani ortada o hizmeti alabilmek için” (K.7).

Yukarıda verildiği üzere güvenilir VPN’lerin kullanımıyla veya kâr amacı gütmeyen kuruluşların projeleri ile mobilde ortamda anonim kalınabilmektedir. Ancak Katılımcı 7’nin “... anonim kalmak aykırı gibi geliyor.” ifadesi dikkat çekicidir. Bu ifade, mobil uygulamaların işlevselliğine atıfta bulunmaktadır. Taviz vermeden mobil uygulamaların sunduğu özelliklerden yararlanılamamaktadır. Katılımcı 2 ise anonimliğe farklı bir açıdan yaklaşmış, anonimliğin sisteme zarar vereceğini dile getirmiştir:

“Şöyle bir tarafı da var herkes önlemini alırsa, o zaman çok büyük ölçüde bu sisteme zarar verecektir ve sistem hayatta kalmak adına çok daha alternatif yollar aranmak zorunda kalacaktır” (K.2).

Katılımcı 2'nin ifadesi liberal görüşe denk düşmektedir. Sistemin hayatta kalmak adına insan hayatının özgürlüğünün rafa kaldırılması kapitalizmin yayılmacı politikasıyla örtüşmektedir. Bu türden bir yaklaşım, şirketlerin veri sömürgeciliği faaliyetlerinin meşrulaşması anlamına gelmektedir.

Güvenlik

Araştırmanın başından itibaren, güvenlik önlemlerinin gözetimden kaçınmanın ve direnişin bir parçası olduğu kanaatine varılmıştır. Katılımcılar genellikle gizlilik ve güvenliği ilişkilendirmişler ve kullanıcıların almış olduğu güvenlik önlemlerinin veri gizliliği için önemli bir unsur olduğunu belirtmişlerdir. Bu nedenle daha önce deneyimledikleri güvenlik önlemlerini ve uygulamaları paylaşmışlardır:

“Bazı password yöneticileri var. Bunlar bütün şifreleri tutan uygulamalar. Lastpass kullanıyorum ben şahsen. Bütün şifreniz orada duruyor. Senin sadece tek bir şifren var. O da Lastpass'a girmen için. Kalan her şeyi o kendisi tutuyor, bilgileri kendisi dolduruyor önüne bir şifre çıktığı zaman. Her sitede böylece farklı bir şifren olmuş oluyor. (...) genelde bu şöyle çalışıyor. Sen bir tane foruma e-mail ve her zamanki şifreni girdin. O forumun, sitenin veri tabanı patladı. Şifren ve mailin dark web'e düştü. İnsanların yüzde doksanı aynı şifreyi kullandığı için... Ve böylece bütün hesapların tehlikede olmuş oluyor. Bu banka hesabında olabilir, Amazon hesabın da olabilir. Ama password manager kullandığımız zaman her sitedeki şifre farklı olduğu için sadece formdaki hesabın patlıyor” (K.2).

“Sign with in Apple'da sahte bir e-posta ile güvenliğini sağlayabilirsin. Sana sahte bir e-posta veriyor ve posta senin asıl e-posta'a yönlenecek. Ama sen karşı tarafa o sahte e-posta'yı veriyorsun. O zaman ne oluyor? Oraya karmakarışık rakamların olduğu bir e-posta ile kaydoluyorsun. Sign with in Apple butonuna bastığın zaman Apple onu hatırlıyor hangi e-posta ile kaydolduğunu ve otomatik girişini yapıyor. Ama karşı taraftaki servisin sahibi olan kişi senin asıl e-posta'nı göremiyor ve istediğin zaman da mesela bu kişi artık bana erişemesin diye o bağlantıyı kopartabiliyorsun. Böylece sana posta göndermeyi de durdurmuş oluyor. Yine Apple'ın kendi içinde olan bir aracı var iCloud Keychain diye. İşletim sistemi düzeyinde bütün cihazlar arasında senkronlanıyor şifreler. Senin bir ana şifren oluyor. Her kaydolma formunda Apple diyor ki ben senin için bir şifre uydurabilirim. Kompleks bir şifreyi kaydediyorum ben arka tarafta diyor. O şifreyi hatırlamana gerek yok. Sonra o siteye ya da uygulamaya girdiğin zaman Apple diyor ki senin şifren benle kayıtlıydı doldurayım mı formu diye soruyor. Hangi kullanıcının için doldurayım diye soruyor. Doldurup devam ediyorsun. Güzel bir şey, ben hep kullanıyorum onu” (K.5).

Katılımcı 2 ve 5'in önerileri, çeşitli güvenlik uygulamaları sayesinde mobil uygulamalarca toplanan verilerin herhangi bir şekilde ele geçirilmesi ya da sızdırılması sonucu ortaya çıkabilecek güvenlik açığı problemlerine yöneliktir. Öte yandan katılımcıların bu önerileri, engelleme hamlesi olarak da değerlendirilebilir. Uygulamalar, sahte e-posta ya da şifre üreterek, veri gizliliğini ve güvenliğini sağlamaya yardımcı olabilir.

Veri Paylaşmama

Günümüzde gönüllü veri paylaşma eğilimi oldukça yaygındır. Özellikle sosyal medya uygulamaları aracılığıyla istemsizce veya bile isteye kişisel bilgiler, e-posta adresleri veya fotoğraflar paylaşılmaktadır. Katılımcı 11, veri paylaşımı konusundaki bu eğilime dikkat çeken ifadelerde bulunmuştur. Katılımcı 5 ise veri paylaşımı konusundaki çekincelerini dile getirdiği ifadesinde anonim kalma konusunda katı bir tutum sergilemese de veri paylaşımını sınırlandırdığı görülmüştür. Katılımcı 8 de paylaştığı verilerin güvenliğinden endişe etmesi sonucunda arkasında bıraktığı dijital izlerine dahi dikkat etmekte, yaşamını bu yönde biçimlendirmektedir:

“Bugün biliyoruz ki herkes her şeyini paylaşma eğiliminde. Instagram’a fotoğraf koymaktan yediğimiz yemeğin görselinde paylaşmaktan hiç çekinmiyoruz. Evimize, tatilimize, partnerimize ve evcil hayvanlarımıza kadar paylaşıyoruz. Sonra gizlilik endişesinden bahsediyoruz ki zaten gizlilik bitti herkes her şeyi yayınlıyor. Ama ben mesela paylaşmam, ilk günden beri. İnternette beni aratsanız bir iki görsel çıkar onlar da bana benzemiyor artık. Değiştim çünkü. Bir süre sonra da silinir gider. Mümkün merteye de ismimi vermemeye çalışırım, avatar kullanırım, takma ad kullanırım” (K.11).

“Gönüllü olarak kendi verimi paylaşma işinden birazcık imtina ediyorum. Instagram’da falan paylaşım yapan bir insan değilim. En son 2016’da bir fotoğraf attım, altı sene olmuş. Altı senedir bir şey göndermiyorum. Özetle kendi verimi paylaşma konusunda çekincem var. Ama böyle çok katı bir işte tamamen incognito [anonim] bir şekilde takılayım internette gibi bir obsesyonum yok açıkçası” (K.5).

“Birçok şeye erişimi olduğundan dolayı özel gösteriyorum. Dijital ortamlarda artık herhangi yazdığınız bir şeyin çok yüzde yüz güvenli şekilde tutulamayacağını bildiğim için ona göre davranıyorum. Dijital izimi ona göre bırakıyorum diyebilirim yani. Hayatımı ona göre yaşıyorum” (K.8).

Katılımcı 6 ise, kullanıcıların fikirlerini beyan ettiği platformlarda anonim kalmak isteyebileceğini belirtmiştir. Katılımcı 6’nın bu ifadesi aslında ifade özgürlüğü konusundaki kaygıya işaret etmektedir:

“Belki bazı platformlarda işte belki ekşi sözlük gibi platformlarda olabilir. Anonim kalmak isteyebilir insan. Fikirlerini belki biraz daha iyi ifade edebilmek için; ama benim öyle bir ihtiyacım olmadı” (K.6).

Kişilerin sosyal ağlarda kimi zaman fikirlerini özgürce dile getirememesi, sürekli gözetim altında olmasının bir sonucudur. Düşünce ve ifade özgürlüğünü kısıtlayan veri gözetimi, kişilerin kendi kendilerini sansürlemelerine de neden olmaktadır. Kişiler, kimi zaman fikirlerini özgürce beyan edemezken kimi zaman da fikirlerini açıklarken seçici davranabilir. Sonuç olarak bu durum, kişinin özgürlüğünün ve ifade hakkının gaspıdır.

Uygulama Özelinde Önlemler

Mobil uygulama izinleri, daha önce de belirtildiği üzere kullanıcı verilerine erişimin kapısını aralayan son eşikte konumlanmaktadır. Bu nedenle katılımcıların uygulama kullanım deneyimlerinden yola çıkarak uygulama özelinde gizliliğe ilişkin alınabilecek önlemler aşağıda verilmiştir:

“Birçok uygulamayı da işim bittikten sonra hiçbir şekilde arka tarafta çalışır halde bırakmıyorum. Sürekli kapatıyorum. Biliyorum ki onlar arka tarafta da benim konumumu izlemeye devam edeceklerdir. O yüzden kullanıp konumla işim varsa o konum işimi halledip uygulamayı hemen kapatıyorum. Bu uygulamalar devlet kontrolünde uygulamalar olsa dahi hiç fark etmiyor benim için. Uygulamanın ne tarzı olduğunun bir önemi yok” (K.3).

“Benim bütün mobil uygulama izinlerim kapalıdır. Her zaman yeni bir uygulama kurduğumda da kapatırım. İzinlerden hepsini kapatıyorum. Paylaşım yapacağım zaman izinlerini açıyorum. Paylaşımı yaptıktan sonra izinlerin hepsini tek tek kapatıyorum aslında. Konum servisi, galeriye ulaşma izni vb. hepsini kapatıyorum. Bunun da bilinçli olduğum için her seferinde yaparım. Suiistimal edilebilir. Bir geliştirici olarak bunun farkındayım çünkü” (K.10).

“Aslında dikkat ettiğim birkaç şey var. Öyle çok fazla dikkat etmiyorum. Mesela bir uygulamayı yüklediğim zaman bazı uygulamalar bir sürü izin istiyor. İndirdiğim uygulamaya bakıyorum. Mesela dil öğrenme uygulaması olsun. Sizden ne izin isteyebilir? Mikrofon izni ister, konuşmak için belki fotoğraf çekeceksiniz, bir şey paylaşacaksınız uygulama içinde. Onun için kamera izni isteyebilir. Ama böyle absürt izinler istiyorsa, bunun ne işi var diyorsam o uygulamayı siliyorum. Yani yüklemem o tarz şeyler. Açıkçası yani biraz da kullanıcının dikkat etmesi lazım. Ne kullandığına...” (K.6).

“Kendimi gizleme ihtiyacı duymuyorum o kadar fazla; ama rastgele bir uygulama ya da izin de vermiyorum. Çünkü neler yapılabileceğini biliyorum. Özellikle kamera izni mikrofon izni, galeri izni gibi şeyleri sadece güvendiğim büyük şirketlerin uygulamalarına veriyorum. Tek seferlik bir şey kullanıp deneyeceksem, o tek sefer onu deneyip uygulamadan o izni kaldırıyorum veya uygulamayı siliyorum eğer hiç bilmediğim bir uygulamaysa. Çünkü biliyorum ki o sırada telefon açıkken benim fotoğraflarım peyderpey bir sunucuya yüklenebilir. Bunun önünde herhangi bir engel yok. Yani böyle bir şey yapıldı mı yapılmadı mı ben tespit edemem. Mesela Twitter benden kamera izni istediği zaman, galeri izni istediği zaman bunu çok önemsemiyorum. Ama ilk defa ismini duyduğum küçük ve daha işte bir iki aydır piyasada olan bir uygulama, benden bir anda mikrofon izni isterse mesela sorarım ne yapacak bu mikrofon iznini ve reddederim. Bildirimlerden de çok rahatsız olduğum için genelde kapatırım” (K7).

“Mobil uygulama kullanırken özellikle gizlenmiyorum ama dikkat etmiş olduğum şeyler var. Örneğin uygulamaların izinleri konusunda bayağı hassasım çünkü işin arka planını bildiğim için neler toplayabileceğini biliyorum” (K.11).

Katılımcı 6, 7 ve 11’in ifadelerinin hemen başında mobil uygulama kullanırken özellikle gizlenme ihtiyacı duymadıklarını dile getirmişlerdir. Ancak hemen ardından dikkat ettikleri hususlar ise gayet titiz ve uğraş gerektiren işlemlerdir. Bunların bazıları, uygulamaların izinlerini incelemek ve kapatmak, yalnızca uygulama kullanırken izinleri açıp kapatmak (İşletim sistemlerinin yeni sürümleri, izinlerin uygulama kullanılırken açılıp açılmaması ile ilgili kullanıcıya seçenek sunmaktadır.) bildirimleri kapatmak veya arka planda

alıřan uygulamaları temizlemek gibi grece meřakkatli iřlemlerdir. Literatrde de gizliliğın korunması iin katılımcıların ifadeleri doğrultusunda neriler bulunmaktadır: Uygulama izinlerinin devre dıřı bırakılabileceğı ve gereksiz izinlerin kaldırılması nerilmektedir (Dovd., 2014: 5073). te yandan Katılımcı 7, “gvendiğı byk řirketlerin uygulamalarına” eriřim izni verdiğini dile getirmiřtir. Bu ifade, “kullanıcıların” gzetime tepki hamlelerini arařtıran bir alıřmada da dile getirilmiřtir. Kullanıcılar, “Instagram gibi bilindik uygulamalarda ise diğerk uygulamalara nazaran daha gvende hissettiklerini ve zellikle bu bilindik platformların mobil uygulamaları sz konusu olduğunda daha tereddtsz bir řekilde her trl eriřim iznini verdiklerini belirtmiřlerdir” (Bulur, 2021: 498). Ayrıca belirtilmelidir ki geliřtiricilerin uyguladıkları gizlilik nlemleri, sıradan kullanıcılara kıyasla daha eřitlidir ve istediklerinde gzetimi bertaraf edebilecek yazılım bilgisine sahiptirler. nk kullanıcılar grece daha “basit nlemler almaya alıřmaktadırlar” (Bulur, 2021: 497). Geliřtiricilere gre temel olarak adlandırılabilcek nlemler, onlara gre oğuzaman nemsiz ya da olağandır. Oysaki sıradan kullanıcıların oğuz yukarıda verilen nlemlerin oğundan habersizdir.

DEĞERLENDİRME VE SONUÇ

Veriye giderek bağımlı hale gelen büyük sermaye çevreleri, dijital ortamlardaki varlıklarını sürdürebilmek için kişisel verilere egemen olmak istemekte, verileri ve dolayısıyla bireyleri gözetim altında tutarak, ürünlerini kullanan kişilerin verilerini sömürmektedir. Veriye bağımlı olan şirketler, veriler üzerindeki gözetimi ve sömürüyü de çeşitli taktiklerle doğallaştırmaya çalışmakta, özellikle verilere, doğal kaynak niteliği atfederek sömürüyü haklı gösterme çabası içerisine girmektedirler. Madencilik faaliyetlerinde kullanılan terminolojiye benzer bir biçimde, teknoloji ürünlerini kullanan bireyler maden sahası gibi görülürken, onlara ait davranış verileri de henüz işlenmemiş olan değerli bir maden cevheri olarak görülmektedir. Ancak bu metaforik benzetme oldukça sorunludur ve literatürde seyrek de olsa eleştirilmektedir. Örneğin Dijck (2014: 201)'a göre verilerin, sosyal yaşamın hammaddesi olarak lanse edilmesi yanlış bir yönlendirmedir. Sadowski (2019: 2-6) için de veri işleme faaliyeti için kullanılan veri madenciliği kavramı uygun değildir; daha uygun bir kullanım biçimi *veri üretimi* olabilir. Çünkü verilerden *toplanmış* ve hatta *çıkarılmış* olarak bahsedildiğinde, sanki veriler kişilerden hasat edilmeye hazır bir ürünmüş gibi bir görüntü ortaya çıkmaktadır. Sonuç olarak verinin her yerde bulunan ve elde edilebilen doğal bir kaynak olarak çerçevelenmesi, veri biriktirme rejimini güçlendirmektedir. Çalışma, bu farkındalık içerisinde yürütülse de araştırmanın doğası ve kavramların yoğun olarak bu şekilde kullanılıyor olması kavramların politik doğruculuk gözetilerek kullanılmasını zorlaştırmıştır. Bu nedenle bu kavramlar, dokümanlarda ve kullanıcıların ifadelerinde verildiği şekliyle; yani veri biriktirme rejiminin ideolojik seçimlerine paralel biçimde kullanılmıştır.

Mobil iletişimin kritik bir noktasında konumlanan mobil uygulamalar ise, kullanıcı verilerine açılan kapının kilidi haline gelmiştir. Mobil uygulamalardaki kişisel veri ve kullanıcı mahremiyeti konusu giderek daha fazla araştırma konusu haline gelirken, uygulama ekolojisinde yer alan ve uygulama mağazalarına sahip olan şirketlerin veri gizliliğini koruma adına attığı bazı adımlar da özellikle Apple'ın "gizliliğini koruyoruz" sloganıyla yayınladığı reklamlar yoluyla gündeme taşınmıştır. Burada sorgulanması gereken, zaten veriye bağımlı olan şirketlerin veri gizliliğini ve kullanıcı mahremiyetini sağlayıp sağlayamayacağıdır. Çalışmanın araştırma bölümünde de gösterildiği üzere katılımcılardan bazıları, mobil uygulamalarda veri gizliliği konusundaki regülasyonların uygulanmasında veya veri gizliliği ile ilgili yasal düzenlemelere uyulması konusunda uygulama mağazalarının daha fazla sorumluluk almaları gerektiğini ve uygulama mağazalarını bu şirketlerin regüle etmesi

gerektiğini dile getirmişlerdir. Bu tür bir yaklaşım, bir ölçüde kabul edilebilir olsa da -bu, uygulama geliştiricilerinin ve uygulama mağazalarını düzenleyen şirketlerin, kullanıcılarına verileri üzerinde şeffaflık ve kontrol olanağı sağlama sorumluluğuna (Razaghpanah vd., 2018: 13) işaret etmektedir- veri egemenliği konusu başta olmak üzere birçok problemlili duruma neden olabilir. Örneğin, Kollnig vd. (2021: 22)'ye de göre verilerin yalnızca birkaç şirketin elinde toplanması, veri işlemedeki şeffaflığı ve veri koruma ve gizlilik yasalarına uyumu artırabilir; ancak bu durum aynı zamanda veri gücünü bu şirketlerin eline daha fazla verebilir. Kollnig vd. (2021)'nin bu ifadesi, çok daha fazla şirket tarafından yönetildiğinde bu verilerin, hem şirketler hem de kamu tarafından denetlenmesinin çok daha zor hale getirebileceğinden yola çıkmaktadır. Ancak bu varsayım veri biriktirme rejimlerini güçlendiren bir noktada durmaktadır. Araştırma bulgularında verildiği üzere bazı katılımcılar, veri gizliliği için atılan bu adımların, diğer şirketler tarafından talep edilen veri miktarını sınırlayacağını, ancak uygulama mağazalarına sahip olan şirketlerin kendi çıkarları doğrultusunda kullanmak isteyebileceklerini ileri sürmüşlerdir. Dolayısıyla şirketler yine burada bir taktik yürütmekte göstermelik veri ve kullanıcı gizliliği vaadiyle diğer şirketlerin veri talebini sınırlarken, kendi ekosistemi için daha fazla veri talep eder hale gelmektedir. Sonuç olarak verilerin dengesiz dağılımının ve sömürsünün önüne geçilememektedir. Öte yandan yasal caydırıcılığın sağlanması adına veri odaklı kanunların/yönetmeliklerin dünya çapında yaygınlaşması önemli, ancak tek başına yeterli değildir. Couldry ve Mejias (2022: 259)'ın da ifade ettiği gibi “Daha ileri giden yol, hukuki düzenlemelerin ayrıntılarından çok, yüzyıllardır sömürgecilığe ve kapitalizme direnenlerin vizyonu ile bağlantılı bir insanca yaşama ekolojisini savunmaktan geçer”. Bu da ancak hükümet, akademisyen/bilim insanı, yayıncı ve geliştirici gibi paydaşların ortak çabalarıyla gerçekleştirilebilir.

Gündelik hayatta sıklıkla kullanılan dijital araçlara entegre edilmiş olan mobil uygulamalar aracılığıyla birçok dijital medya platformuna erişilebilmekte veya oyun uygulamalarıyla dijital oyunlar oynanabilmektedir. Kullanıcıların, bu araçları kullanması sonucunda iletişim ihtiyacını tatmin etmesinin, haber almasının veya eğlenmesinin yanında, yazılımın geliştiricisi için meta ürettiği ve maddi olmayan emeğin sömürüldüğü ortaya çıkmaktadır. Örneğin mobil oyun oynayan bir kullanıcının oyun oynama zamanı da dâhil olmak üzere (Talay, 2022: 306) oyun içinde yaptığı her faaliyet (reklam izleme, oylama, yorum yapma vb.) dijital emeğin sömürülmesidir. Ancak “... bu sömürü, sosyal medyada bir sömürü değilmiş gibi algılanmaya meyillidir, çünkü dijital emek, sömürü gerçeğini diğer kullanıcılarla bağlantı kurma ve tanışma eğlencesinin arkasına gizleyen oyun emeğidir” (Fuchs, 2015: 407). Burada şirketlerin emek sömürsünü gizlediği taktiklerle

karşılaşılmaktadır. Bir başka taktik yine verilerle ilgilidir. Kullanıcıların bu yazılımları kullandığında -zaman zaman kullanmadığında da- her etkinliği dijital veri üretmektedir. Dolayısıyla üretilen veri, dijital emekle doğrudan bağlantılıdır. Fuchs (2015: 357)’un da dediği gibi “Metaları yaratan üreticiler vardır; aksi halde var olamazlardı. Bu yüzden eğer internet platformlarında zikredilen meta, kullanıcı verisi ise, o zaman bu veriyi yaratma süreci de değer üreten emek olarak değerlendirilmelidir”. Öte yandan mobil uygulamaları kullananların, adeta bir uygulama işçisi veya kölesi gibi davranış sergiledikleri literatürde yer almaktadır. Burada dikkat edilmesi gereken nokta, şirketlerin kullanıcılarına köle gibi davranması değil, kullanıcıların köleleştirilme taktikleriyle dijital araçlara bağımlı hale getirilmesidir. Bir kere bağımlı hale gelen kullanıcılar, fiziksel olarak değil, zihinsel olarak köleye dönüşmekte, özne olmaktan çıkarak nesne haline gelmektedir. Qiu, (2021: 205-208)’ya göre “Sonuçta, kölelik, insan öznelerin insanlık dışı nesnelere indirgenmesidir, nihai bir nesneleştirme ve yabancılaştırma biçimidir”; ancak dijital kapitalizm köleliği diriltirken köleliği tarihsel olarak revize etmiş olur ve kölelik karşıtı hareketleri tetikleyebilir ve insan öznelerini köleliğe karşı direnişe teşvik edebilir. Buradaki yaratıcı motivasyon ise “... aynı dijital araçları birer kölelik karşıtlığı aracı olarak kullanmak, insan öznelerini kurtarıp yeniden icat etmektir” (Qiu, 2021: 214).

“21. yüzyılda insanlar, Kapitalizm uğruna yaşamlarının veriler aracılığıyla durmaksızın temellük edildiği bir dünyayı kabul etmeli midir?”. Couldry ve Mejias (2022: 18)’ın sorduğu bu soru, gözetim kapitalistlerinin kişilerin dijital verilerine el koymasına karşı gösterilmesi gereken direnişin fitilini ateşleyebilecek türde bir sorudur. Tarihsel sömürgeciliğin yöntemlerine gösterilen dirençle, veri sömürgeciliği yöntemlerine gösterilmesi gereken direnç aslında benzerdir. Kendi toprakları üzerinde hak sahibi olmak isteyen halklarla, kendi verileri üzerinde hak sahibi olması gerekenlerin benzer olduğu gibi. Ayrıca bu iki sömürgecilik türünde de toplumlar denetim ve gözetim altında tutulmakta, insan hayatı sömürüye uğratılmaktadır. Peki, veri sömürgeciliğine karşı direnişe nereden başlamak gerekir? Couldry ve Mejias (2020: 28)’a göre veri sömürgeciliğine karşı gösterilmesi gereken direniş, gözetimin ifşasıyla başlamalıdır: “... sürekli olarak iz sürülebilen bir yaşam, ifşa edilen bir yaşamdır. Bu ifşanın farkına varmak, veri sömürgeciliğine karşı yapılacak direnişin başlangıcıdır”. Bu bağlamda, veri gözetimi ve sömürü mekanizmalarını ortaya koyan bu çalışma da veri sömürgeciliğine karşı gösterilen direnişin bir parçası olarak görülebilir.

Kullanıcı ve veri gizliliğini koruduğu yönünde bir iddia ile ortaya çıkan blok zinciri tabanlı merkezi olmayan uygulamalar ve organizasyonlar ise 2015 yılından itibaren özellikle Ethereum Ana Ağının (Ethereum Mainnet) başlatılmasıyla birlikte nispeten yaygınlaşmaya

başlamıştır. Hem ilgili literatüre göre hem de çalışmanın araştırma sonuçlarına dayanılarak bu uygulamaların merkezi uygulamalara alternatif olarak kullanılabileceği, kişisel veri ve kullanıcı mahremiyetini koruyabilecek potansiyeli olduğu, ancak henüz bu tür platform ve uygulamaların başlangıç evresinde olduğu anlaşılmıştır. Bu uygulamaların en önemli vaatleri arasında ise merkezi otoritenin bulunmaması, kararların topluluk kararıyla hızlı bir biçimde uygulanabilir olması ve kullanıcıların verileri üzerinde kontrol sahibi olabilmesine olanak tanınmasıdır. Blok zinciri, kullanıcıların kişisel verilerinin sahibi olarak tanınmasını sağlayabilir. Merkezi olmayan bir platformlarda hassas verilerin toplanması, saklanması ve paylaşılmasıyla ilgili yasal ve düzenleyici kararlar daha hızlı bir şekilde alınabilir. Ayrıca, blok zinciri üzerinde programlanabilir hale getirilen yasalar ve düzenlemeler otomatik olarak uygulanabilir. Blok zinciri, manipülasyona karşı dayanıklı olması nedeniyle, verilere erişim veya depolama konusunda yasal kanıt olarak kullanılabilir (Zyskind ve Nathan, 2015: 181). Couldry'nın görüşüne göre ise (Mejias'ın da böyle düşündüğünü ekliyor.) her şeyden veri elde eden, nesnelerin internetine dayalı bir internet türevi olarak görülen blok zinciri tabanlı bazı ortamlar; örneğin Metaverse evrenleri, sömürgeciliğin sanal gerçeklik alanlarına uygulanmış bir tekrarıdır. Ancak gelecekte veri sömürgeciliği ile ilgili bazı sorunları potansiyel olarak çözebilecek bazı gelişmelerin (Bu gelişmeler muğlak olduğu için belki bazıları web 3.0 olarak adlandırılabilir.) olabileceği ihtimali de göz önünde bulundurulmalıdır. Örneğin, Facebook ve X gibi büyük platformların yerini Mastodon gibi merkezi olmayan ve yerel sosyal medyanın alması gibi. Couldry'a göre bu türden uygulamalar genellikle veri talep etmiyor ve kitlesel fonlama ile finanse ediliyor. Ancak Mastodon ve benzeri platformlar başarılı olsa bile bu sadece sosyal medyada yer alan veri sömürgeciliğini kapsayacak ve diğer yönleri ele almayacaktır: Sağlık ve eğitim verilerinin elde edilmesi, sosyal refah verileri, finans verileri, işyerinde veri sağlama gibi. Dolayısıyla Couldry, merkezi olmayan uygulamaların veri mahremiyetinde yaşanan problemlerin çözümü konusunda kısmen iyimser olabileceğini aktarmıştır (Couldry N., kişisel iletişim, 24.01.2023). Tezin araştırma bölümünden elde edilen sonuçlar da Couldry'nın bu ifadelerini destekler niteliktedir. Merkezi uygulamaların veri biriktirme odaklı yapısına karşı veri mahremiyetini ve özel hayatın gizliliğini önemseyen merkeziyetsiz uygulama projelerinden bazılarının, veri bağımlısı şirketlere ve onların merkezi uygulamalarına gösterilen, direniş odaklı ve kâr amacı gütmeyen projeler olduğu anlaşılırken, bazı projelerin, kapitalistlerin sızamadığı ya da henüz yayılma imkânı bulamadığı blok zinciri tabanlı dijital alanların hâkimi olmak isteyen alternatif bir aktör olma çabası içinde olduğu anlaşılmaktadır.

Araştırma soruları, çalışma boyunca bağımsız geliştiricilerdeki direniş kültürünü keşfetmeye, gözetim ve veri sömürüsüne karşı gösterilen tepki hamlelerine ilişkin derinlemesine bir anlayış geliştirilmesine yardımcı olmuştur. Araştırma sorularına aranan yanıtlar, hem genel bir bakış sunmak hem de çalışmanın başlangıcında verilen amaca ulaşıp ulaşılmadığını belirlemek amacıyla değerlendirilmiştir. Bağımsız mobil uygulama geliştiricilerinin dijital gözetim, veri gözetimi ve veri sömürüsüne ilişkin yaklaşımlarının niteliğini belirlemek amacı taşıyan ilk araştırma sorusunu yanıtlayan bulgulara göre araştırmaya dâhil edilen bağımsız mobil uygulama geliştiricilerinin, kişisel veri ve veri bağlantılı konular/sorunlar hakkında genel olarak bilgi sahibi oldukları görülmüştür. Katılımcılar, daha önce yaşanan veri sızıntısı/ihlalleri konularında da görüşlerini dile getirmişler, kişisel verinin hem şirketler hem geliştiriciler hem de kullanıcılar için çok önemli olduğunu iddia etmişlerdir. Bazı katılımcılar, kullanıcıların kişisel verilerini şirketlere teslim etmemesi gerektiğini söylerken bazı katılımcılar, kullanıcıların verilere erişim izni vermelerinde bir sakınca görmediklerini ifade etmişlerdir. Katılımcıların veriyi güç ile ilişkilendirmeleri beklenen bir durumdur. Çünkü veriler, şirketler için önemli bir güç unsuru olsa da aynı zamanda geliştiriciler için de büyük bir güç olma potansiyeli taşımaktadır. Veriyi kontrol etme imkanına sahip olanların dijital alanları da kontrol etme yeteneğini elde etme olasılığı, tam da kapitalistlerin sermaye birikimine benzer bir yapının işlediği bir duruma işaret etmektedir: Nasıl ki kapitalistlerin toplumsal konumu, ekonomik ve siyasi gücü, kontrol ettiği sermayenin büyüklüğü ile ölçülmekteyse (Hunt ve Lautzenheiser, 2019: 351) dijital alanlardaki gücün göstergesi de gözetim kapitalistlerinin sahip olduğu ve kontrol ettiği verinin büyüklüğü ile ölçülmektedir. İnternet ortamında muazzam bir veri büyüklüğünden bahsedilmektedir. Geliştiricilerin bu denli büyük bir veri yığınınına hâkim olmalarının neredeyse imkânsız olduğu görülmektedir; çünkü büyük miktardaki bu veri yığınlarını depolayabilecek, aktarabilecek ve işleyebilecek olanaklara sahip olmadıkları anlaşılmaktadır. Bu nedenle veriler, git gide bu veriyi elde edebilen, işleyebilen ve depolayabilen istilacı şirketlerin hakimiyetine girmektedir. Böylece şirketler rekabet avantajı elde etmekte, veriler üzerinden değer elde etmekte ve giderek gözetim kapitalistleri olmaktan çıkarak veri kapitalistleri haline dönüşmekte, global olarak bireyleri etkileme ve kontrol etme gücüne daha fazla sahip olmaktadır.

Çalışmada ikinci sırada yer alan araştırma sorusu, bağımsız mobil uygulama geliştiricilerinin uygulama geliştirme/yayınlama aşamalarında veri mahremiyeti ve gizliliği konusundaki hassasiyetlerine odaklanmakta, bu hassasiyetlerin yol açtığı davranış örüntülerini ortaya koymayı amaçlamaktadır. Mobil uygulama geliştirme, tamamen veri elde

etmeye bağımlı bir eylem değilken, uygulama hizmetinin geliştirilmesi ve iyileştirilmesi gibi işlemler verinin elde edilmesine bağlıdır. Bu nedenle kullanıcıdan veri elde etmek her geliştirici için daha da önemli hale gelmektedir. Katılımcıların, uygulama geliştirme/yayınlama aşamalarında veri gizliliğine ve kullanıcı mahremiyetine kısmen önem gösterdikleri görülmüştür. Katılımcıların bazılarının, kullanıcılardan mümkün olduğunca az veri elde ederek bu konuda oldukça hassas davranırken, bazılarının mevcut regülasyonlar ve uygulama mağazalarının izin verdiği ölçüde veri elde ettikleri ve daha az hassas davrandıkları anlaşılmıştır. Katılımcıların bağımsız geliştirici oldukları ve veriye erişimin eşitsiz olduğu göz önüne alındığında veri bağımlısı istilacı şirketlere kıyasla çok daha fazla hassasiyet gösterdikleri söylenebilir. Uygulamalardaki gizlilik risklerini araştıran, 320 binden fazla uygulama geliştiricisi ve geliştirdikleri 1,5 milyondan fazla Android uygulamasının incelendiği çalışmada, ciddi gizlilik risklerine sahip uygulamaların %70'inden fazlasının uygulama geliştiricilerinin %1'i tarafından oluşturulduğu görülmüştür. Bu bulgu, bazı geliştiricilerin düşük gizlilik derecelerine sahip uygulamalar oluşturma alışkanlığına sahip olduğunu gösterse de (Wang vd., 2017: 164), aynı zamanda sınırlı sayıda geliştiricinin aşırı veri elde etme eğiliminde olduğunu göstermektedir. Geliştiriciler, mobil uygulama ekosisteminin en önemli aktörlerindendir; bu nedenle kullanıcının veri mahremiyetini korumak için gizlilikle ilgili önlemleri alma ve etik kurallara uyma zorunlulukları bulunmaktadır.

Çalışmanın diğer araştırma sorusu, bağımsız mobil uygulama geliştiricilerinin kişisel mahremiyetlerine ilişkin kaygı durumlarını ifade etme biçimlerine odaklanmış, katılımcıların ifadeleri duygu analizi için veri olarak değerlendirilerek bulgulara dönüştürülmüş ve tematik olarak yorumlanmıştır. Veri gizliliği ve mahremiyetine ilişkin duygu ifadelerinin değerlendirilmesi sonucunda, katılımcıların duygu durumlarında çeşitlilik olduğu ortaya konmuştur. Katılımcı söylemlerine bakıldığında katılımcıların bir kısmı mahremiyet kaygısı taşıırken diğer bir kısmı bu kaygıyı taşımamaktadır. Ancak kaygı taşımayan geliştiricilerin gözetimden kaçınmak için çeşitli stratejiler geliştirdikleri de görülmüştür. Geliştiricilerin kaygı durumlarını ifade etme biçimleri çoğu zaman muğlaktır. Araştırmanın bulgularında detaylı olarak gösterildiği üzere oldukça çelişik ifadeler göze çarpmaktadır. Bazı katılımcılar, veri mahremiyetinin sağlanamayacağını iddia ederek teslimiyet duygularını ön plana çıkarmışlardır. Bu durum, geliştiricilerin deneyimlerinden yola çıkarak verilerin korunmasında çoğu zaman çaresiz kalınmasıyla açıklanabilir. Bu çaresizliğin nedeni ise verilerin tam anlamıyla kullanıcı tarafından kontrol edilemeyeceğini düşünmelerinden kaynaklanmaktadır. Bazı katılımcılar ise veri üzerindeki kontrolün sağlanabileceğini dile

getirmişlerdir. Ancak bu kontrol tamamen bireysel eylemleri içermektedir. Geliştiricilerin veri paylaşmaktan imtina etmek, mümkün olduğunca anonim kalarak veya cihazlarının kameralarını kapatarak kaygılarını azaltmaya çalıştıkları anlaşılmıştır. Ancak yine de özel hayatın gizliliği bağlamında kaygılarını ifade etmekten çoğunlukla çekindikleri yine bulgular arasındadır.

Bağımsız mobil uygulama geliştiricilerinin gözetime verdikleri tepki ve karşı-gözetim hamlelerinin niteliğini ortaya koymayı amaçlayan bir diğer araştırma sorusu, bu alandaki direniş biçimlerini keşfetmeye odaklanmıştır. Araştırmanın çalışma grubunu oluşturan bağımsız mobil uygulama geliştiricilerinin, mobil uygulamalardaki gözetim alt yapıları hakkındaki tecrübeleri ve veri elde etme mekanizmalarının yazılım boyutuna hâkim olmaları sayesinde, gözetime ve dolayısıyla veri sömürüsüne direnebilme kabiliyetlerinin sıradan kullanıcılara kıyasla daha fazla olduğu sonucuna ulaşılmıştır. Dolayısıyla bağımsız geliştiriciler, çeşitli yazılım veya yazılım araçlarını kullanarak gözetimi tersine çevirebilecek ve karşı-gözetim olanaklarını var edebilecek yazılım profesyonelleri olarak görülmeleri gerektiği iddiası da güçlenmiştir. Geliştiricilerin veri gözetimine ve veri sömürüsüne direniş biçimlerinin zaman zaman kullanıcıların da uyguladıkları direniş biçimleriyle örtüştüğü görülmüştür. Bağımsız geliştiricilerin geliştirici ve kullanıcı kimliği girift haldedir. Bu durum geliştiricilerin kullanıcı kimliğine özgüdür; ancak sıradan kullanıcılara göre uygulayıcı olarak daha profesyonel davranmaktadırlar. Örneğin, VPN kullanımı birçok kullanıcının anonim kalmak için kullandığı bir hamledir. Oysaki geliştiriciler, kullandıkları VPN'lerin de güvenli olanlarını tercih etmektedir. VPN kullanımına ek olarak başka önlemlerde (örneğin DuckDuckGo gibi, Tor gibi arama motorlarını kullanıyorlar) almaktadırlar. Geliştiriciler sıradan kullanıcılara göre yazılım bilgisine sahip oldukları için, tersine mühendislik yoluyla, şirketlerin gözetim mekanizmalarını çözebileceği, gözetimi tersine çevirebileceği ve veri sömürüsünü engelleyebilecekleri ortaya çıkmıştır. En nihayetinde, görüşülen geliştiricilerin veri gözetimine direniş gösterdikleri, bu direniş biçiminin toplu eylemleri içermeyen, bireysel bir mukavemet şeklinde olduğu bulgular arasındadır. Katılımcılar, şirketlerin gözetim araçlarına direnmek ve gözetimden kaçınmak için yine şirketlerin araçlarını kullanmakta ve gözetimden kaçınmak için taktikler geliştirmektedir. Bu durum, tehdit altındayken bile güvenliği geri kazanmak için aynı teknolojileri kullanma fırsatlarını arayan bir direniş (Kafer, 2016: 238) olarak anlaşılabilmektedir. Yasmin Jiwanı (2011: 350)'nin de dediği gibi anti-kolonyal taktikler, *efendinin araçlarını* kullanmak durumundadır, ancak bunu yaratıcı yollarla yaparlar. Gerçekten de bağımsız geliştiriciler, gözetimi tersine çevirebilmek için yaratıcı taktikler uygulayabilecek, gelecekte veri sömürgeciliğine karşı çıkabilecek yeni yollar

keşfeden önemli aktörler olabilirler.

Çalışmada yanıt aranan son soru, bağımsız mobil uygulama geliştiricilerinin uygulama kullanım tercihlerinin ve güvenli bir uygulama deneyimi için kullandıkları stratejileri ortaya koymaya yöneliktir. Yukarıda bahsedildiği üzere katılımcılar, zaman zaman kullanıcı kimlikleriyle de hareket etmektedir. Dolayısıyla katılımcıların çoğunluğu, sıradan kullanıcıların yeterliliklerini gözeterek, kendi kullanıcı kimlikleri perspektifinden direniş önerilerinde bulunmuşlardır. Katılımcıların bu davranışı anlaşılır bir durumdur; çünkü katılımcılar geliştirici kimlikleriyle sıradan kullanıcılara direniş önerilerinde bulunsalar bile sıradan kullanıcılar tarafından bu öneriler alımlanamazlar. Bu nedenle katılımcılar, sıradan kullanıcıların da uygulayabileceği, gözetime ve veri sömürüsüne direnişin basit ve bireysel yollarına göndermede bulunmuşlardır. Katılımcılar, uygulama seçimlerinde güvenliğe odaklanarak hareket etmektedirler. Bir uygulama edinirken, kaynağına, geliştiricisine dikkat etmekte ve uygulama izinlerini incelemektedirler. Geliştiricisi ya da kaynağı bilinmeyen uygulamaları telefonlarına dahi indirmemektedirler. Öte yandan geliştiricilerin bir bölümü, gizliliği güvenlikle bağdaştırmıştır. Bu sonuç, hem veri hem de cihaz güvenliği bakımından alınacak önlemlerin de veri gözetimine ve sömürüsüne direnişin bir parçası olduğunu göstermektedir. Sonuç olarak alanında uzman olarak nitelendirilmesi gereken bağımsız geliştiricilerin, gözetimden kaçınma stratejileri ve direniş önerilerinin, sıradan kullanıcılar için uygulanabilir ve yol gösterici olduğu ortaya çıkmıştır.

Gelecek Çalışmalar İçin Öneriler

Günümüz eleştirel veri çalışmaları, veri odaklı süreçlerin eleştirel biçimde incelenmesini gerektiren, verinin yarattığı gücü sorgulayan, bu gücü elde etmede yaşanan eşitsizlikleri ortaya koyan, bireysel mahremiyetin korunmasını ve özel hayatın gizliliği konusunda yaşanan/yaşanması muhtemel sorunların çözümüne katkıda bulunabilecek potansiyeli oldukça yüksek bir çalışma alanıdır. Gelecekte kişisel veri ve veri bağlantılı konulara/sorunlara eleştirel veri çalışmaları alanı çerçevesinde eleştirel olarak yaklaşmak isteyen yazarlara/akademisyenlere, veri odaklı kavramları kullanırken veri biriktirme rejiminin kullanmış olduğu sömürü dilinden uzaklaşmaları, veri sömürüsünü haklı çıkarmaya çalışan taktikleri boşa çıkaracak tanımlarla çalışmalarını kurgulamaları önerilmektedir. Belki de veri sömürgeciliğine direnmenin ilk adımı bu tür bir kullanımı reddetmek olacaktır.

Geliştirici toplulukları ise geliştiricilerin bilgi alışverişinde bulunmak veya iletişim kurmak için dahil oldukları uğraklardır. Topluluklar, kullanıcı mahremiyetine önem veren, veri elde etme konusunda etik ilke ve önerileri, üyelerine benimsetebilecek ve farkındalık

yaratabilecek oluşumlar olarak görülebilir. Bu geliştirici topluluklarına üye olan geliştiriciler, topluluğun bilinçlendirme ve teşvikleri ile veri mahremiyeti ve gizliliği konusunda daha fazla sorumlu davranabilirler. Bu bağlamda geliştirici topluluklarının kültürel çalışmalar perspektifinden geliştiricilerin iletişim pratikleri, geliştirici rolleri ve kullanıcı kimlik oluşturma süreçleri, topluluk etkileşimleri, etik ve kültürel kodların nasıl alımlandığı araştırılabilir. Katılımcı gözlem ve derinlemesine görüşmeler yoluyla topluluk dinamikleri derinlemesine anlaşılabilir; geliştirici topluluklarının niteliksel çalışmalarla araştırılması, literatüre zenginlik katabilir. Başlangıçta dile getirildiği gibi merkezi olmayan uygulama ve organizasyonların henüz yolun başında olmaları, bu alana özgü veri gizliliği ve mahremiyeti çerçevesinde daha fazla araştırma yapılmasını gerektirmektedir. Gelecekte, bu uygulamalara veri odaklı yaklaşan, merkezi olmayan uygulama geliştiricilerinin de dâhil edildiği, merkezi ve merkezi olmayan uygulamaların veri politikalarını karşılaştıran çalışmaların yapılması, merkezi ve merkezi olmayan uygulama çalışmaları alanının gelişmesine katkıda bulunacaktır.

Araştırmanın kısıtlarında da belirtildiği gibi, katılımcıların tamamının cinsiyeti erkektir ve kadın geliştiricilere araştırmaya dâhil olmaları için ulaşılsa da yanıt alınamamıştır. Gelecekte, kadın yazılımcıların da yer aldığı ya da yalnızca kadın geliştiricilere odaklanan çalışmalar yürütebilir, farklılıklar veya benzerlikler ortaya koyulabilir. Öte yandan çalışma, yapay zekâ konusundaki farkındalığı yansıtmakla birlikte, temel aldığı tarihsel süreç nedeniyle tezde merkezi bir konuma oturmamaktadır. Ancak gelecekte, bu tür bir çalışmanın yapay zekâ konusu kapsamına alınmaksızın gerçekleştirilemeyeceğinin de göz önünde bulundurulması gereklidir. Çalışmanın daha sonra yapılacak olan çalışmalara önemli bir alt yapı oluşturacağı düşünülmektedir. Yapay zekânın iş ve emek biçimlerinde yaratmış olduğu ve henüz tam olarak gerçekleşmeyen; ancak başladığı düşünülen dönüşüm süreciyle birlikte, yeni iş ve emek biçimlerinin yeniden tanımlanmasının ve dolayısıyla yapay zekânın, ilerleyen dönemlerde bu alandaki çalışmalara dâhil edilmesinin bir zorunluluk haline geleceği öngörülmektedir.

Son Söz

Bu tez, gelecekte yazılımcıların katılımcı olarak dahil edileceği çalışmalar için temel oluşturabilir. Hem akademisyenler hem de yazılımcılar, bu çalışmayı temel alarak veri gözetimine ve veri sömürüsüne direnmenin çok daha başka yollarının mümkün olabileceğini görebilir, çalışmadaki eksiklikleri tespit edebilir ve bu eksiklikleri gidererek yeni direniş yollarını var edebilir. Çalışma, veri sömürgeciliği ile verilerin ve dolayısıyla insan hayatının sömürüye uğratılmasını engelleyebilecek aktivist girişimlerin filizlenmesini de sağlayabilir.

Gelecekte yapılacak arařtırmalar bu dūřünceleri ilerletebilir, veri gözetimine bařkaldırın farklı yollar bulunabilir ve veri sömürgeciliğini ortadan kaldırarak çözümler üretilebilir. En nihayetinde bu sömürü düzeninin yerine daha řeffaf, insan hayatının mahrem alanlarına müdahale etmeyen, demokratik bir düzen inřa edilebilir.



KAYNAKLAR

- Adamczyk, C. L. (2023). "Communicating Dataism". *Review of Communication*, 23(1), 4-20.
- Adorno, T. (2008). *Kültür Endüstrisi Kültür Yönetimi*. (Çev. N. Ülner, M. Tüzel ve E. Gen), İletişim Yayınları, İstanbul.
- Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J. ve Amaba, B. (2017). "Blockchain Technology Innovations". *IEEE Technology & Engineering Management Conference (TEMSCON)*. Santa Clara, 8-10 Haziran 2017, 137-141.
- Akçoraoğlu, A. (2019). "'Yeni Kapitalizm' Teorileri, Dijital Devrim ve Türkiye Kapitalizmi". *Mülkiye Dergisi*, 43(3), 525-575.
- Akhil R, Athul K., Athira S., Gayathri J. ve Nair R. R. (2023). "Blockchain-Enabled Supply Chain: A Review of Decentralized Application (Dapp) Implementations". *International Journal Of Progressive Research in Engineering Management And Science (Ijprems)*. Haziran 2023, 348-351.
- Albury, K., Burgess, J., Light, B., Race, K. ve Wilken, R. (2017). "Data Cultures of Mobile Dating and Hook-Up Apps: Emerging Issues for Critical Social Science Research". *Big Data & Society*. 4(2), 1-11.
- Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J. ve Agarwal, Y. (2015). "Your Location Has Been Shared 5,398 Times! A Field Study On Mobile App Privacy Nudging." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. Nisan 2015, 787-796.
- Amatriain, X. (2013). "Big & Personal: Data and Models behind netflix recommendations". In *Proceedings of the 2nd International Workshop on Big Data, Streams and Heterogeneous Source Mining: Algorithms, Systems, Programming Models and Applications*. Ağustos 2013, 1-6.
- Amorim, H. (2018). "Maddi Olmayan Emek Teorileri: Marx'a Dayanan Eleştirel Bir Bakış" *Maddi Olmayan Emek Teorisi: Kuramsal Bir Eleştiri*. A. Koşar (hızl.). Kor Kitap, İstanbul.
- Ammous, S. (2016). "Blockchain Technology: What is it Good for?". *SSRN*, 1-5.
- Andrejevic, M. (2014a). "Big Data, Big Questions the Big Data Divide". *International Journal of Communication*, 8(17), 1673-1689.
- Andrejevic, M. (2014b). "Eleştirel Medya Çalışmaları 2.0: Etkileşimli Bir Sürüm". M. Çakır (Ed.). *Yeni Medyaya Eleştirel Yaklaşımlar*, Doğu Kitabevi, İstanbul.

- Andrejevic, M., Hearn, A. ve Kennedy, H. (2015). "Cultural Studies Of Data Mining: Introduction". *European Journal of Cultural Studies*, 18(4-5), 379-394.
- Ante, L. (2021). "Smart Contracts on the Blockchain-A Bibliometric Analysis and Review". *Telematics and Informatics*, (57), 1-29.
- Aral, S. ve Eckles, D. (2019). "Protecting Elections from Social Media Manipulation". *Science*, 365(6456), 858-861.
- Arıkan, R. (2017). *Araştırma Yöntem ve Teknikleri*. Nobel Akademik Yayıncılık, Ankara.
- Barnes, S. B. (2006). "A Privacy Paradox: Social Networking in the United States". *First Monday*. <https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312> (erişim tarihi: 30.04.2022).
- Barth, S., De Jong, M. D., Junger, M., Hartel, P. H. ve Roppelt, J. C. (2019). "Putting the Privacy Paradox to the Test: Online Privacy and Security Behaviors among Users with Technical Knowledge, Privacy Awareness, and Financial Resources". *Telematics and Informatics*, (41), 55-69.
- Başaran, F. (2014). *İletişim ve Emperyalizm: Türkiye’de Telekomünikasyonun Ekonomi-Politiği*. Ütopya Yayınevi, Ankara.
- Başaran, F. (2016). "Uzun Dalgalar ve Bilgi ve İletişim Teknolojileri Paradigması". F. Başaran ve H. Geray (Ed.). *İletişim Ağlarının Ekonomisi*. Ütopya Yayınevi, Ankara.
- Bauman, Z. ve Lyon, D. (2013). *Akışkan Gözetim*. (Çev. E. Yılmaz), Ayrıntı Yayınları, İstanbul.
- Bellanova, R., ve González Fuster, G. (2018). "No (Big) Data, No fiction? Thinking Surveillance with/against Netflix. A. R. Saetnan, I. Schneider ve N. Green (Ed.). *The Politics and Policies of Big Data: Big Data Big Brother?* Routledge, London.
- Bellavitis, C., Fisch, C. ve Momtaz, P. P. (2023). "The Rise of Decentralized Autonomous Organizations (DAOs): A First Empirical Glimpse". *Venture Capital*, 25(2), 187-203.
- Berardi, F. (2014). *Gelecekte Sonra*. (Çev. O. Şişman ve S. Özer), Otonom Yayıncılık, İstanbul.
- Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T. ve Skarmeta, A. (2019). "Privacy-Preserving Solutions for Blockchain: Review and Challenges". *IEEE Access*, (7), 164908-164940.
- Binns, R., Zhao, J., Kleek, M. V. ve Shadbolt, N. (2018). "Measuring Third-Party Tracker Power Across Web and Mobile". *ACM Transactions on Internet Technology (TOIT)*, 18(4), 1-22.

- Bishop, S. (2018). "Anxiety, Panic and Self-Optimization: Inequalities and the Youtube Algorithm". *Convergence*, 24(1), 69-84.
- Bolin, G. ve Andersson Schwarz, J. (2015). "Heuristics of the Algorithm: Big Data, User Interpretation and Institutional Translation". *Big Data & Society*, 2(2), 1-12.
- Bowie, N. E. ve Jamal, K. (2006). "Privacy Rights on the Internet: Self-Regulation or Government Regulation?". *Business Ethics Quarterly*, 16(3), 323-342.
- Braun, V. ve Clarke, V. (2006). "Using Thematic Analysis in Psychology". *Qualitative Research in Psychology*, 3(2), 77-101.
- Brophy, E. (2011). "Language Put to Work: Cognitive Capitalism, Call Center Labor, and Worker Inquiry". *Journal of Communication Inquiry*, 35(4), 410-416.
- Brophy, E. ve De Peuter, G. (2015). "Labors of Mobility: Communicative Capitalism and the Smartphone Cybertariat". A. Herman, J. Hadlaw ve T. Swiss (Ed.). *Theories of the Mobile Internet*, Routledge, London.
- Bulur, N. (2021). "Covid-19 Sürecinde Sosyal Medya Uygulamaları ve Karşı Gözetim Stratejileri: Nitel Bir Araştırma". *İletişim Çalışmaları Dergisi*, 7(3), 487-501.
- Calzati, S. (2021). "Decolonising "Data Colonialism" Propositions for Investigating the Realpolitik of Today's Networked Ecology". *Television & New Media*, 22(8), 914-929.
- Cangızbay, K. (2001). "İnsan Hakkı Değil, İnsan Olma Hakkı", *Birikim Dergisi*, 150(10): 106-112.
- Castells, M. (2013). *Enformasyon Çağı: Ekonomi, Toplum ve Kültür: Ağ Toplumu'nun Yükselişi*. (Çev. E. Kılıç), Bilgi Üniversitesi Yayınları, İstanbul.
- Castells, M. (2016). *İletişim Gücü*. (Çev. Ebru Kılıç). İstanbul: Bilgi Üniversitesi Yayınları.
- Cecere, G., Le Guel, F. ve Soulié, N. (2015). Perceived Internet Privacy Concerns on Social Networks in Europe. *Technological Forecasting and Social Change*, (96), 277-287.
- Chanson, M., Bogner, A., Wortmann, F. ve Fleisch, E. (2017). "Blockchain As A Privacy Enabler: An Odometer Fraud Prevention System". *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*. Eylül 2017, 13-16.
- Chaudhuri, R., Chatterjee, S. ve Vrontis, D. (2023). "Antecedents of Privacy Concerns and Online Information Disclosure: Moderating Role of Government Regulation". *EuroMed Journal of Business*, 18(3), 467-486.

- Chen, T., Lu, H., Kunpittaya, T. ve Luo, A. (2022). "A review of Zk-snarks". *ArXiv Preprint arXiv:2202.06877* 1-34.
- Cheng C. W. (2017) "The System and Self-Reference of the App Economy: The Case of Angry Birds". *Communication & Culture* 9(1): 47-66.
- Chia, P. H., Yamamoto, Y. ve Asokan, N. (2012). "Is This App Safe? A Large Scale Study on Application Permissions and Risk Signals". *Proceedings of the 21st International Conference on World Wide Web*, 16-20 Nisan, Lyon, 311-320.
- Chomsky, N. ve Waterstone, M. (2023). *Kapitalizmin Sonuçları: Üretimden Hoşnutsuzluk ve Direniş*. (Çev. M. K. Coşkun), Scala Yayıncılık, İstanbul.
- Connolly, R. ve McParland, C. (2012). "Dataveillance: Employee Monitoring & Information Privacy Concerns in the Workplace". *Journal of Information Technology Research (JITR)*, 5(2), 31-45.
- Chou, C. H., Chiu, C. H., Ho, C. Y., ve Lee, J. C. (2013). "Understanding Mobile Apps Continuance Usage Behavior and Habit: An Expectance-Confirmation Theory". *PACIS* (132), 1-10.
- Clarke, R. (1988). "Information Technology and Dataveillance". *Communications of the ACM*, 31(5), 498-512.
- Clarke, K. V. D. (2023). *Amending Amendments: Digital Colonialism, Bill C-11, and Assessing the Call for Improvement* (Yüksek Lisans Tezi). University of Windsor, Windsor.
- Couldry, N. ve Powell, A. (2014). "Big Data from the Bottom Up". *Big Data & Society*, 1(2), 1-5.
- Couldry, N., Fotopoulou, A. ve Dickens, L. (2016). "Real Social Analytics: A Contribution Towards a Phenomenology of a Digital World". *The British Journal of Sociology*, 67(1), 118-137.
- Couldry, N., ve Mejias, U. (2019). "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?". *Internet Policy Review*, 8(2), 1-16.
- Couldry, N. ve Mejias U. A. (2020). "Veri Sömürgeciliği: Büyük Verinin Modern Özne İle İlişisini Yeniden Düşünmek". F. Aydoğan (Ed.). *Yeni Medya Kuramları II*. Der Yayınları, İstanbul.
- Couldry, N. ve Mejias U. A. (2022). *Bağlantının Bedelleri: Veri Sömürgeciliği Tartışmalarına Bir Giriş*. NotaBene Yayınları, İstanbul.

- Couldry, N., ve Mejias, U. A. (2023). "The Decolonial Turn in Data and Technology Research: What is at Stake and Where is it Heading?". *Information, Communication & Society*, 26(4), 786-802.
- Couldry, N. (2023). [Elektronik Posta Yoluyla Kişisel İletişim, 24.01.2023].
- Crain, M. (2018). "The Limits of Transparency: Data Brokers and Commodification". *New Media & Society*, 20(1), 88-104.
- Creps, D. (2020). "Sosyal Ağlar ve Uluslararası Kapitalizm". F. Aydoğan (Ed.). *Yeni Medya Kuramları II. Der Yayınları*, İstanbul.
- Creswell, J. W. (2014). *A Concise Introduction to Mixed Methods Research*. SAGE Publications, London.
- Creswell, J. W. (2018). *Nitel Araştırma Yöntemleri: Beş Yaklaşım Göre Nitel Araştırma ve Araştırma Deseni*. (Çev. M. Bütün ve S. B. Demir), Siyasal Kitabevi, Ankara.
- Çakır, M. (2015). *İnternette Gösteri ve Gözetim. Eleştirel Bir Okuma*. Ütopya Yayınevi, Ankara.
- Çoban, B. (2016). "Gözün İktidarı Üzerine", (Çev. ve hzl. B. Çoban ve Z. Özarlan), *Panoptikon: Gözün İktidarı*. Su Yayınları, İstanbul.
- De Bustos, J. C. M. ve Izquierdo-Castillo, J. (2019). "Who Will Control the Media? The Impact of Gafam on the Media Industries in the Digital Economy". *Revista Latina de Comunicación Social*, (74), 803-821.
- De Certeau, M. (2005). "Making do": Uses and Tactics". Gabrielle M. Spiegel (Ed.). *Practicing History: New Directions in Historical Writing After The Linguistic Turn*. Routledge, Londra.
- De Certeau, M. (2008). *Gündelik Hayatın Keşfi-I: Eylem, Uygulama, Üretim Sanatları*. (Çev. L. Arslan Özcan), Dost Kitabevi Yayınları, Ankara.
- Dean, J. (2005). "Communicative Capitalism: Circulation and the Foreclosure of Politics". *Cultural Politics*, 1(1), 51-74.
- Dean, J. (2014). "Communicative Capitalism and Class Struggle". *Spheres: Journal for Digital Cultures*, (1), 1-16.
- Dean, J. (2015). "Apps and Drive". A. Herman, J. Hadlaw ve T. Swiss (Ed.). *Theories of the Mobile Internet*, Routledge, New York.
- Degli Esposti, S. 2014. "When Big Data Meets Dataveillance: The Hidden Side of Analytics". *Surveillance & Society*, 12(2): 209-225.

- Devidas, S., Rao YV, S. ve Rekha, N. R. (2021). "A Decentralized Group Signature Scheme for Privacy Protection in a Blockchain". *International Journal of Applied Mathematics and Computer Science*, 31(2), 1-12.
- Devlieghere, J., Gillingham, P. ve Roose, R. (2022). Dataism Versus Relationshipism: A Social Work Perspective. *Nordic Social Work Research*, 12(3), 328-338.
- Do, Q., Martini, B. ve Choo, K. K. R. (2014). "Enhancing User Privacy on Android Mobile Devices via Permissions Removal". *IEEE 47th International Conference on System Sciences*, Hawaii, 5070-5079.
- Dörndorfer, J., ve Seel, C. (2016). "The Impact of Mobile Devices and Applications on Business Process Management". *Prozesse, Technologie, Anwendungen, Systeme und Management*, Heide, 10-19.
- Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., Vlist, F. V. D. ve Weltevrede, E. (2018). *Store, Interface, Package, Connection: Methods and Propositions for Multi-Situated App Studies*, Publikationen aus der Universität Siegen, Siegen.
- Dieter, M., Gerlitz, C., Helmond, A., Tkacz, N., van Der Vlist, F. N., ve Weltevrede, E. (2019). "Multi-Situated App Studies: Methods and Propositions". *Social Media+ Society*, 5(2), 1-15.
- Dinner, I. M., Van Heerde, H. J. ve Neslin, S. (2015). "Creating Customer Engagement Via Mobile Apps: How App Usage Drives Purchase Behavior". *Tuck School of Business Working Paper*, 5 Ekim 2015, 1-47.
- Dwyer, C., Hiltz, S. ve Passerini, K. (2007). "Trust And Privacy Concern within Social Networking Sites: A comparison of Facebook and MySpace". *Proceedings of the 13th Americas Conference on Information Systems (AMCIS)*, 9 Ağustos 2007, Keystone, 1-13.
- Eaton, J. (1996). *Ekonomi Politik Bir Marksist El Kitabı*. (Çev. Ş. Yalçın), Bilim ve Sosyalizm Yayınları, Ankara.
- Efanov, D. ve Roschin, P. (2018). "The All-Pervasiveness of the Blockchain Technology". *Procedia Computer Science*, (123), 116-121.
- Emirgil, B. F. (2010), "Yeni Kapitalizmde Emeği Sorunsallaştırmak: Emeğin Maddi-Olmayan Görünümleri". *Çalışma ve Toplum*, 24 (1), 221-237.
- Esposito, C., De Santis, A., Tortora, G., Chang, H. ve Choo, K. K. R. (2018). "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?". *IEEE Cloud Computing*, 5(1), 31-37.
- European Data Protection Supervisor (2014). "Privacy and Competitiveness in the Age of Big

- Data". Hustinx, P. (Supervisor). European Data Protection Supervisor Online Report, Brussels. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf (erişim tarihi: 10.08.2023).
- Fan, J., Wang, Z., Luo, Y., Bai, J., Li, Y. ve Hao, Y. (2019). "A New Stealth Address Scheme for Blockchain". *Proceedings of the ACM Turing Celebration Conference*, Çin, Mayıs 2019, 1-7.
- Felt, A. P., Greenwood, K. ve Wagner, D. (2011). "The Effectiveness of Application Permissions". *2nd USENIX Conference on Web Application Development*, 15-16 Haziran 2011, Portland, 1-12.
- Feng, T., Yang, P., Liu, C., Fang, J. ve Ma, R. (2022). "Blockchain Data Privacy Protection and Sharing Scheme Based on Zero-Knowledge Proof". *Wireless Communications and Mobile Computing*, 1040662, 1-11.
- Ferro, M. (2017). *Sömürgecilik Tarihi: Fetihlerden Bağımsızlık Hareketlerine Kadar 13.-20. Yüzyıl*. (Çev. M. Cedden), İmge Kitabevi, Ankara.
- Flick, Uwe (2021). "Çeşitleme (Triangulation)" N. K. Denzin ve Y. S. Lincoln (Ed.). *Nitel Araştırmalar Kılavuz Kitabı*. (Çev. Ed. G. Ekici ve S. Yeşilçınar), Vizetek Yayıncılık, Ankara.
- Flora, H. K., Wang, X. ve Chande, S. V. (2014). "An Investigation on the Characteristics of Mobile Applications: A Survey Study". *International Journal of Modern Education and Computer Science*, 6(11), 21-27.
- Fraser, A. (2019). "Curating Digital Geographies in an Era of Data Colonialism". *Geoforum*, (104), 193-200.
- Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D. ve Green, S. (2020). Blockchain as a Disruptive Technology for Business: A Systematic Review. *International Journal of Information Management*, (51), 1-14.
- Foucault, M. (1992). *Hapishanenin Doğuşu*. (Çev. M. A. Kılıçbay), İmge Kitabevi, Ankara.
- Fuchs, C. (2010a). "How Can Surveillance be Defined? Remarks on Theoretical Foundations of Surveillance Studies". *The Internet & Surveillance-Research Paper Series*. <http://www.sns3.uti.at/wp-content/uploads/2010/10/The-Internet-Surveillance-Research-Paper-Series-1-Christian-Fuchs-How-Surveillance-Can-Be-Defined.pdf> (erişim tarihi: 23/03/2023).
- Fuchs, C. (2010b). "Labor in Informational Capitalism And on the Internet". *The Information Society*, 26(3), 179-196.

- Fuchs, C. (2014a). *Sosyal Medya: Eleştirel Bir Giriş*. (Çev. D. Saraçoğlu ve İ. Kalaycı), NotaBene Yayınları, İstanbul.
- Fuchs, C. (2014b). “Bilişsel Kapitalizm ya da Enformasyonel Kapitalizm? Enformasyonel Ekonomide Sınıfın Rolü”. M. A. Peters ve E. Bulut (Ed.). *Bilişsel Kapitalizm: Eğitim ve Dijital Emek*. (Çev. K. Özdi), NotaBene Yayınları, İstanbul.
- Fuchs, C. (2015). *Dijital Emek ve Karl Marx*. (Çev. T. E. Kalaycı ve S. Oğuz), NotaBene Yayınları, İstanbul.
- Fuchs, C. (2021a). *Dijital Kapitalizm Çağında Marx'ı Yeniden Okumak*, (Çev. D. Saraçoğlu). NotaBene Yayınları, İstanbul.
- Fuchs, C. (2021b). “Büyük Veri Kapitalizmi Çağında Karl Marx”. D. Chandler ve C. Fuchs (Ed.). *Dijital Nesneler, Dijital Özneler: Büyük Veri Çağında Kapitalizm, Emek ve Siyaset Üzerine Disiplinlerarası Yaklaşımlar*. NotaBene Yayınları, İstanbul.
- Fuchs, C. (2021c). “Google Kapitalizmi”. F. Aydoğan (Ed.). *Yeni Medya Kuramları I*. Der Yayınları, İstanbul, 71-83.
- Fuchs, C. ve Chandler D. (2021). “Büyük Veri Kapitalizmi Siyaset, Eylemcilik ve Kuram”. D. Chandler ve C. Fuchs (Ed.). *Dijital Nesneler, Dijital Özneler: Büyük Veri Çağında Kapitalizm, Emek ve Siyaset Üzerine Disiplinlerarası Yaklaşımlar*. NotaBene Yayınları, İstanbul.
- Grabarczyk, P. (2023). [Elektronik Posta Yoluyla Kişisel İletişim, 18.07.2023].
- Gandy Jr., O. H. (1993). “Toward a Political Economy of Personal Information”. *Critical Studies in Media Communication*, 10(1), 70-97.
- Garda M. B. ve Grabarczyk P. (2016). “Is Every Indie Game Independent? Towards the Concept of Independent Game. *Game Studies*, 16(1), 1-26.
- Garg, S. ve Baliyan, N. (2021). “Comparative Analysis of Android and IOS from Security Viewpoint”. *Computer Science Review*, (40), 100372, 1-13.
- Genc-Nayebi, N., & Abran, A. (2017). “A Systematic Literature Review: Opinion Mining Studies from Mobile App Store User Reviews”. *Journal of Systems and Software*, (125), 207-219.
- Geray, H. (2016). “İletişim Ağları ve Masaüstü Sömürgecilik”, *İletişim Ağlarının Ekonomisi*. F. Başaran ve H. Geray (Ed.). Ütopya Yayınevi, Ankara.
- Gerlitz, C., Helmond, A., van der Vlist, F.N. ve Weltevrede, E. (2016). “App Studies: Platform Rules and Methodological Challenges”. *The 17th Annual Meeting of the Association of Internet Researchers*. 5-8 Ekim 2016, Berlin, 1-3.

- Gerlitz, C., Nieborg, D. B., van der Vlist, F. N. ve Helmond, A. (2019). “Apps and Infrastructures: A Research Agenda”. *Computational Culture: A Journal of Software Studies*, (7). 1-28.
- Giddens, A. (1981). “A Contemporary Critique of Historical Materialism (Vol. 1)”. University of California Press, Berkeley and Los Angeles.
- Goettke, R. ve Christiana, J. (2007). “Privacy and Online Social Networking Websites”. *Computer Science 199r: Special Topics in Computer Science Computation and Society: Privacy and Technology*. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=85ac0c9d9ec424a501d22187893857165b6606b0> (erişim tarihi: 14.10.2023).
- Golosova, J. ve Romanovs, A. (2018). “The Advantages and Disadvantages of the Blockchain Technology”. *6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE)*, Eylül 2018, 1-6.
- Goodwin, P. (2021). “Köleler Değil, Ücretli İşçiler: Jack Qiu’nun Bölümü Üzerine Düşünceler”. D. Chandler ve C. Fuchs (Ed.). *Dijital Nesneler, Dijital Özneler: Büyük Veri Çağında Kapitalizm, Emek ve Siyaset Üzerine Disiplinlerarası Yaklaşımlar*. NotaBene Yayınları, İstanbul.
- Gurung, A. ve Raja, M. K. (2016). “Online Privacy and Security Concerns of Consumers”. *Information & Computer Security*, 24(4), 348-371.
- Han, B. C. (2022). *Enfokrasi: Dijitalleşme ve Demokrasinin Krizi* (Çev. M. Özdemir). Ketebe Yayınları, İstanbul.
- Hardt, M. ve Negri A. (2004). *Çokluk: İmparatorluk Çağında Savaş ve Demokrasi*. (Çev. B. Yıldırım), Ayrıntı Yayınları, İstanbul.
- Hardt, M. ve Negri, A. (2018). *İmparatorluk*. (Çev. A. Yılmaz). Ayrıntı Yayınları, İstanbul.
- Harvey, D. (2022). *Anti-Kapitalist Günlükler*. (Çev. U. Özmakas), Sel Yayıncılık, İstanbul.
- Hassan, S. ve De Filippi, P. (2021). Decentralized Autonomous Organization. *Internet Policy Review*, 10(2), 1-10.
- Hassandoust, F., Akhlaghpour, S. ve Johnston, A. C. (2021). “Individuals’ Privacy Concerns and Adoption of Contact Tracing Mobile Applications in a Pandemic: A Situational Privacy Calculus Perspective”. *Journal of the American Medical Informatics Association*, 28(3), 463-471.
- Helmond ve Nieborg (2016). “Facebook in the App Economy: From Web to App(s)”. *AoIR Selected Papers of Internet Research*. 5-8 Ekim 2016, Berlin, 8-11.

- Helmond, A., Nieborg, D. B. ve Van Der Vlist, F. N. (2017). "The Political Economy of Social Data: A Historical Analysis of Platform-Industry Partnerships". *Proceedings of The 8th International Conference on Social Media & Society*, (38), Temmuz, 1-5.
- Hepp, A., Jarke, J. ve Kramp, L. (2022). "New Perspectives in Critical Data Studies: The Ambivalences of Data Power-An Introduction". Hepp, A., Jarke, J. ve Kramp, L. (Ed.). *New Perspectives in Critical Data Studies: The Ambivalences of Data Power. Transforming Communications – Studies in Cross-Media Research*. Palgrave Macmillan, Bremen.
- Hill, D. W. (2019). "Goodbye iSlave: A Manifesto for Digital Abolition". *Information, Communication & Society*, 22(8), 1186-1188.
- Ho, K. K., Chiu, D. K. ve Sayama, K. L. (2023). "When Privacy, Distrust, and Misinformation Cause Worry about Using Covid-19 Contact-Tracing Apps". *IEEE Internet Computing*, Mart-Nisan 2023, 27(2), 7-12.
- Hudson, S. ve Liu, Y. (2023). "Mobile App Users' Privacy Concerns: Different Heuristics for Privacy Assurance Statements in the Eu And China". *Information Technology & People*, 36(1), 245-262.
- Hummel, P., Braun, M., Augsberg, S. ve Dabrock, P. (2018). "Sovereignty and Data Sharing". *ITU Journal: ICT Discoveries*, 25(8), 1-10.
- Hummel, P., Braun, M., Tretter, M. ve Dabrock, P. (2021). "Data Sovereignty: a Review". *Big Data & Society*, 8(1), 1-17.
- Hunt E. K. ve Lautzenheiser M. (2019). *İktisadi Düşünce Tarihi: Eleştirel Bir Perspektif*. (Çev. V. U. Aslan). Siyasal Kitabevi, Ankara.
- Ichiba, T. (2022). "Is Tax Payment a Part of Corporate Social Responsibility?". *Business and Accounting Review*, 29(1), 1-21.
- Iliadis, A. ve Russo, F. (2016). "Critical Data Studies: An Introduction". *Big Data & Society*, 3(2), 1-7.
- Jäckle, Annette., Wenz, Alexander., Burton, Jonathan. ve Couper, Mick. P. (2019). "Increasing Participation in a Mobile App Study: The Effects of a Sequential Mixed-Mode Design and in-Interview Invitation". *Journal of Survey Statistics and Methodology*, 10(4), 898-922.
- Jakobsson, P. ve Stiernstedt, F. (2010). "Pirates of Silicon Valley: State of Exception and Dispossession in Web 2.0". *First Monday*. <https://journals.uic.edu/ojs/index.php/fm/article/view/2799/2577> (erişim tarihi: 17.03.2023).

- Jarret, K. (2021). “Yeniden Üretim Merceğinden: Kültür ve Ekonominin Kesişiminde Emek ve Mücadele”. D. Chandler ve C. Fuchs (Ed.). *Dijital Nesneler, Dijital Özneler: Büyük Veri Çağında Kapitalizm, Emek ve Siyaset Üzerine Disiplinlerarası Yaklaşımlar*. NotaBene Yayınları, İstanbul.
- Jenkins, H. (2021). “Medya Yöndeşmesinin Kültürel Mantığı”. F. Aydoğan (Ed.). *Yeni Medya Kuramları I*. Der Yayınları, İstanbul, 33-45.
- Jiwani, Y. (2011). “Pedagogies of Hope: Counter Narratives and Anti-Disciplinary Tactics”. *Review of Education, Pedagogy, and Cultural Studies*, 33(4), 333-353.
- Johnson, M., Jones, M., Shervey, M., Dudley, J. T. ve Zimmerman, N. (2019). “Building a Secure Biomedical Data Sharing Decentralized App (Dapp): Tutorial”. *Journal of Medical Internet Research*, 21(10), 1-36.
- Joseph, D. J. (2018). “The Discourse of Digital Dispossession: Paid Modifications and Community Crisis on Steam”. *Games and Culture*, 13(7), 690-707.
- Kadivar, J. (2018) “Sosyal ve Mobil Ağlarda Hükümet Gözetimi ve Karşı Gözetim: İran Örneği (2009)” *Panoptikon 2.0 Alternatif Medya ve Karşı-Gözetim*, B. Çoban ve B. Ataman (Ed.). Kafka Epsilon Yayınevi, İstanbul.
- Kafer, G. (2016). “Reimagining Resistance: Performing Transparency and Anonymity in Surveillance Art”. *Surveillance & Society*, 14(2), 227-239.
- Kennedy, H. ve Moss, G. (2015). “Known or Knowing Publics? Social Media Data Mining and the Question of Public Agency”. *Big Data & Society*, 2(2), 1-11.
- Kern, M. ve Sametinger, J. (2012). “Permission Tracking in Android”. *The Sixth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, 48-155. <https://se.jku.at/wp-content/uploads/2012/09/2012.permission-tracking.pdf> (erişim tarihi: 06.02.2023).
- Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. SAGE Publications, London.
- Kim, S. J., Wang, R. J. H. ve Malthouse, E. C. (2015). “The Effects of Adopting and Using a Brand’s Mobile Application on Customers’ Subsequent Purchase Behavior”. *Journal of Interactive Marketing*, 31(1), 28-41.
- Kişisel Verilerin Korunması Kanunu, (6698 sayılı kanun). *T.C. Resmî Gazete*, Sayı: 29677, Cilt: 57, 07/04/2016.
- Kollnig, K., Binns, R., Van Kleek, M., Lyngs, U., Zhao, J., Tinsman, C. ve Shadbolt, N. (2021). “Before and After GDPR: Tracking in Mobile Apps”. *Internet Policy Review*

- 10(4), 1-30. <https://arxiv.org/ftp/arxiv/papers/2112/2112.11117.pdf> (erişim tarihi: 01.05.2023).
- Kollnig, K., Shuba, A., Binns, R., Van Kleek, M. ve Shadbolt, N. (2022). “Are Iphones Really Better for Privacy? A Comparative Study Of Ios and Android Apps”. *Proceedings on Privacy Enhancing Technologies*, (2), 6-24.
- Kovács, A. ve Seres, I. A. (2023). “Anonymity Analysis of the Umbra Stealth Address Scheme on Ethereum”. *ACM Trans. Graph.* 37(4), 1-7. <https://arxiv.org/pdf/2308.01703.pdf> (erişim tarihi: 04.10.2023).
- Koşar, A. (2017). *Negri, Sınıf ve Çokluk: Postmodern Özne Arayışının Eleştirisi*. Kor Kitap, İstanbul
- Koşar, A. (hızl.) (2018). *Maddi Olmayan Emek Teorisi: Kuramsal Bir Eleştiri*. Kor Kitap, İstanbul.
- König, P. D. (2017). “The Place of Conditionality and Individual Responsibility in a “Data-Driven Economy””. *Big Data & Society*, 4(2), 1-14.
- Krupp, A. F. (2022). “Privacy is Not Dead: Expressively Using Law to Push Back against Corporate Deregulators and Meaningfully Protect Data Privacy Rights”. *Georgia Law Review*, (57), 875-918.
- Kurtz, A., Gascon, H., Becker, T., Rieck, K. ve Freiling, F. C. (2016). “Fingerprinting Mobile Devices Using Personalized Configurations”. *Proceedings on Privacy Enhancing Technologies*, (1), 4-19.
- La Polla, M., Martinelli, F. ve Sgandurra, D. (2013). A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials*, 15(1), 446-471.
- Lai, S. S. ve Flensburg, S. (2020). “A Proxy for Privacy Uncovering the Surveillance Ecology of Mobile Apps”. *Big Data & Society*, 7(2), 1-20.
- Lai, S. S. ve Flensburg, S. (2021). “Invasive Species of the App Ecosystem: Exploring the Political Economy of Mobile Communication”. *International Journal of Communication*, 15, 18. 2301-2318.
- Lazzarato, M. (2005). “Maddi Olmayan Emek”, (Çev. S. Özer ve S. Göbelez), *İtalya’da Radikal Düşünce ve Kurucu Politika*. Otonom Yayıncılık, İstanbul.
- Lazzarato, M. (2016). *Göstergeler ve Makineler*. (Çev. F. N. Demirci). Otonom Yayıncılık, İstanbul.

- Lee, D. ve Song, M. (2021). "Mexchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address". *IEEE Access*, (9), 158122-158139.
- Lefebvre, H. (2019). *Marksizm*. (Çev. V. Günyol), Sel Yayıncılık, İstanbul.
- Lebert, D. ve Vercellone, C. (2015). "Kapitalizmin Uzun Vadeli Dinamiği İçinde Bilginin Rolü: Bilişsel Kapitalizm Varsayımı", (Çev. D. Kundakçı), *Bilişsel Kapitalizm: Post-Fordist Dönemde Bilgi ve Finans*, Otonom Yayıncılık, İstanbul.
- Lehuedé, S. (2023). "The Coloniality of Collaboration: Sources of Epistemic Obedience in Data-Intensive Astronomy in Chile". *Information, Communication & Society*, 26(2), 425-440.
- Logan, R. (2004). *The Sixth Language: Learning a Living in The Internet Age*. Blackburn Press, New Jersey.
- Li, H., Ai, W., Liu, X., Tang, J., Huang, G., Feng, F. ve Mei, Q. (2016). "Voting with Their Feet: Inferring User Preferences from App Management Activities". *Proceedings of the 25th International Conference on World Wide Web*, Nisan 2016, 1351-1362.
- Li, C. Y. (2018). "Consumer Behavior in Switching Between Membership Cards and Mobile Applications: The Case of Starbucks". *Computers in Human Behavior*, (84), 171-184.
- Li, W., Guo, H., Nejad, M. ve Shen, C. C. (2020). "Privacy-Preserving Traffic Management: A Blockchain and Zero-Knowledge Proof Inspired Approach". *IEEE Access*, (8), 181733-181743.
- Lipkin, N. (2013). "Examining Indie's Independence: The Meaning of "Indie" Games, The Politics of Production, and Mainstream Cooptation". *Loading...*, 7(11): 8-24.
- Liu, B., Andersen, M. S., Schaub, F., Almuhiemedi, H., Zhang, S. A., Sadeh, N. ve Acquisti, A. (2016). "Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions". *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, 22-24 Haziran 2016, Denver, 27-41.
- Liao, S. H. ve Ho, C. H. (2021). "Mobile Payment and Mobile Application (App) Behavior for Online Recommendations". *Journal of Organizational and End User Computing (JOEUC)*, 33(6), 1-26.
- Leong, L. (2017). "Mobile Myanmar: The Development of a Mobile App Culture in Yangon". *Mobile Media & Communication*, 5(2), 139-160.
- Lynch, R., Young, J. C., Jowaisas, C., Sam, J., Boakye-Achampong, S., Garrido, M. ve Rothschild, C. (2023). "'The Tears don't Give You Funding': Data Neocolonialism in Development in The Global South". *Third World Quarterly*, 44(5), 911-929.

- Lyon, D. (1997). *Elektronik Göz*. (Çev. D. Hattatoğlu), Sarmal Yayınevi, İstanbul.
- Lyon, D. (2006). *Gözetlenen Toplum: Günlük Hayatı Kontrol Etmek*. (Çev. G. Soykan), Kalkedon Yayıncılık, İstanbul.
- Lyon, D. (2013). *Gözetim Çalışmaları*. (Çev. A. Toprak), Kalkedon Yayıncılık, İstanbul.
- Lupton, D. Ve Michael, M. (2017). “‘Depends on Who’s Got the Data’: Public Understandings of Personal Digital Dataveillance”. *Surveillance & Society* 15(2): 254-268.
- Maher, N. A., Senders, J. T., Hulsbergen, A. F., Lamba, N., Parker, M., Onnela, J. P. ve Broekman, M. L. (2019). “Passive Data Collection and Use in Healthcare: A Systematic Review of Ethical Issues”. *International Journal of Medical Informatics*, (129), 242-247.
- Martin, K. D. ve Murphy, P. E. (2017). “The Role of Data Privacy in Marketing”. *Journal of the Academy of Marketing Science*, (45), 135-155.
- Marx, G. T. (2018) “Ayakkabıdaki Çivi: Yeni Gözetime Direnme ve Onu Etkisizleştirme” *Panoptikon 2.0 Alternatif Medya ve Karşı-Gözetim*. B. Çoban ve B. Ataman (Ed.). Kafka Epsilon Yayınevi, İstanbul.
- Marx, K. (2019). *Kapital Cilt: I: Ekonomi Politiğin Eleştirisi*. (Çev. M. Selik ve N. Satılğan), Yordam Kitap, İstanbul.
- Marazzi, C. (2014). *Sermayenin Komünizmi: Finansallaşma, Biyopolitik Emek ve Küresel Kriz*. (Çev. D. Kundakçı), Otonom Yayıncılık, İstanbul.
- Marr, B. (2021). *Büyük Veri İş Başında: 45 Yıldız Şirket Büyük Veriyi Nasıl Kullandı?* (Çev. B. Gündüz), MediaCat Kitapları, İstanbul.
- Mayer-Schönberger, V. ve Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work and Think*. Houghton Mifflin Harcourt, New York.
- McLuhan, M. 2004. *Understanding Me: Lectures and Interviews*. S. McLuhan and D. Staines (Ed.). MIT Press Cambridge.
- Medvedev, A. N., Lambiotte, R. ve Delvenne, J. C. (2019). The Anatomy of Reddit: An Overview of Academic Research. *Dynamics On and Of Complex Networks III: Machine Learning and Statistical Physics Approaches*, (10), 183-204.
- University College London (2016). “Privacy on the Blockchain: Unique Ring Signatures”. R. Mercer, Supervised by N. T. Courtois. MSc in Information Security at University College London. <https://arxiv.org/pdf/1612.01188.pdf> (erişim tarihi 16.08.2023).
- Mejias, U. A. ve Couldry, N. (2019). “Datafication”. *Internet Policy Review*, 8(4), 1-10.

- Meng, W. Ding R., Chung S. P., Han S. ve Lee W. (2016:) “The Price of Free: Privacy Leakage in Personalized Mobile in-Apps Ads”. *23rd Annual Network and Distributed System Security Symposium (NDSS)*, Şubat, San Diego, 1-15.
- Melo, J. F. (2023). “Intercultural Information Ethics Applied to the Data Colonialism Concept”. *International Conference on Computer Ethics* 1(1). <https://soremo.library.iit.edu/index.php/CEPE2023/article/view/295/303> (erişim tarihi 14.11.2023).
- Miller, T. (2014). “Bütün Ülkelerin Siberözgürlükçüleri Birleşin: Tube’larınızdan Başka Kaybedecek Bir Şeyiniz Yok!”. M. Çakır (Ed.). *Yeni Medyaya Eleştirel Yaklaşımlar*. Doğu Kitabevi, İstanbul.
- Mohanta, B. K., Jena, D., Panda, S. S. ve Sobhanayak, S. (2019). “Blockchain Technology: A Survey on Applications and Security Privacy Challenges”. *Internet of Things*, (8), 100107, 1-19.
- Montgomery, A. L. ve Smith, M. D. (2009). “Prospects for Personalization on the Internet”. *Journal of Interactive Marketing*, 23(2), 130-137.
- Moore, M. ve Tambini, D. (2018). *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*. Oxford University Press, New York.
- Moroney, L. ve Moroney, L. (2017). *Using AdMob. The Definitive Guide to Firebase: Build Android Apps on Google’s Mobile Platform*, Apress, Berkeley.
- Morley, D. ve Robins, K. (2011). *Kimlik Mekânları: Küresel Medya, Elektronik Ortamlar ve Kültürel Sınırlar*. (Çev. E. Zeybekoğlu), Ayrıntı Yayınları, İstanbul.
- Mosco, V. (2009). *The Political Economy of Communication*. SAGE Publications, London.
- Murray, A., Kim, D. ve Combs, J. (2023). The Promise of a Decentralized Internet: What is Web3 and How Can Firms Prepare? *Business Horizons*, 66(2), 191-202.
- Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System”. *Decentralized Business Review*. <https://assets.pubpub.org/d8wct41f/31611263538139.pdf> (erişim tarihi: 01.12.2022).
- Postman, N. (1970). “The Reformed English Curriculum”. *High School 1980: The Shape of the Future in American Secondary Education*. A.C. Eurich (Ed.). Pitman Publishing, New York.
- Negri, A. (2023). Marx’ın Hareketi: Tarihsel ve Güncel Bağlamıyla Operaismo. (Çev. E. Eser ve M. Çelik), Otonom Yayıncılık, İstanbul.
- Netchitailova, E. (2021). “Flaneur, Aylak ve Empatik İşçi”. F. Aydoğan (Ed.). *Yeni Medya Kuramları I. Der Yayınları*, İstanbul, 33-45.

- Newman, M. Z. (2011). *Indie: An American Film Culture*. Columbia University Press, New York.
- Nieborg, D. B. (2016). "From Premium to Freemium: The Political Economy of the App". T. Leaver ve M. Willson (Ed.). *Social, Casual and Mobile Games: The Changing Gaming Landscape*, Bloomsbury Academic, New York.
- Nieborg, D. B. ve Helmond, A. (2019). "The Political Economy of Facebook's Platformization in the Mobile Ecosystem: Facebook Messenger as a Platform Instance". *Media, Culture & Society*, 41(2), 196-218.
- Nieborg, D. B., Young, C. J. ve Joseph, D. (2020). "App Imperialism: The Political Economy of the Canadian App Store". *Social Media+ Society*, 6(2), 1-11.
- Nieborg, D. B. (2021). "Apps of Empire: Global Capitalism and the App Economy". *Games and Culture*, 16(3), 305-316.
- Niedzviecki, H. (2019). *Dikizleme Günlüğü: Kendimizi ve Komşularımızı Gözetlemeyi Niçin Bu Kadar Sevdik?* (Çev. G. Gündüç), Ayrıntı Yayınları, İstanbul.
- Nielsen, M. B. C. (2020). "Data Privacy Challenges of Contractual Consent to Process Personal Data: The Example of Netflix". *European Journal of Privacy Law & Technologies*, (1), 20-33.
- Nissenbaum, H. (2017). "Deregulating Collection: Must Privacy Give Way To Use Regulation?". SSRN, 1-42. <https://ssrn.com/abstract=3092282> (erişim tarihi: 12.11.2023).
- Ogura, T. (2006). "Electronic Government and Surveillance-Oriented Society". *Theorizing Surveillance: The Panopticon on Beyond*. D. Lyon (Ed.). Routledge, London.
- Pandare, M. P., Rumao, M. P., Bari, M. P. ve Katkar, M. A. (2022). "Datafication, Dataism and Dataveillance: The Age of Big Data". *Journal Of Engineering And Sciences (SJES)*, 4(1): 16-17.
- Pang, H., Ruan, Y. ve Wang, Y. (2023). "Unpacking Detrimental Effects of Network Externalities on Privacy Invasion, Communication Overload and Mobile App Discontinued Intentions: A Cognition-Affect-Conation Perspective". *Behavioral Sciences*, 13(1), 47.
- Papakyriakopoulos, O., Hegelich, S., Shahrezaye, M. ve Serrano, J. C. M. (2018). "Social Media and Microtargeting: Political Data Processing and the Consequences for Germany". *Big Data & Society*, 5(2). 1-15.

- Peters, M. A. ve Bulut, E. (2014). “Giriş: Bilişsel Kapitalizm, Eğitim ve Dijital Emek”. M. A. Peters ve E. Bulut (Ed.). *Bilişsel Kapitalizm: Eğitim ve Dijital Emek*. (Çev. B. Yıldırım), NotaBene Yayınları, İstanbul.
- Qiu, J. L. (2021). “Hoşçakal iKöle: Dijital Nesnelerle Alternatif Özneler Oluşturmak”. D. Chandler ve C. Fuchs (Ed.). *Dijital Nesneler, Dijital Özneler: Büyük Veri Çağında Kapitalizm, Emek ve Siyaset Üzerine Disiplinlerarası Yaklaşımlar*. NotaBene Yayınları, İstanbul.
- Rajasekaran, A. S., Azees, M. ve Al-Turjman, F. (2022). “A Comprehensive Survey nn Blockchain Technology”. *Sustainable Energy Technologies and Assessments*, (52), 102039, 1-13.
- Rakestraw, T. L., Eunni, R. V. ve Kasuganti, R. R. (2013). “The Mobile Apps Industry: A Case Study”. *Journal of Business Cases and Applications*, 1(1), 1-26.
- Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C. ve Gill, P. (2018). “Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem”. *The 25th Annual Network and Distributed System Security Symposium (NDSS 2018)*, 18-21 Şubat, San Diego.
- Register R. ve McIlroy T. (2014). *Meta Data: Üst Veri El Kitabı*, (Çev. T. Çolak), Profil Yayıncılık, İstanbul.
- Reviglio, U. ve Agosti, C. (2020). “Thinking Outside the Black-Box: The Case for “Algorithmic Sovereignty” in Social Media”. *Social Media+ Society*, 6(2), 1-12.
- Ricaurte, P. (2019). “Data Epistemologies, The Coloniality of Power, and Resistance”. *Television & New Media*, 20(4), 350-365.
- Rivest, R. L., Shamir, A. ve Tauman, Y. (2001). “How to Leak a Secret”. *Advances in Cryptology—ASIACRYPT 2001: 7th International Conference on the Theory and Application of Cryptology and Information Security*, 9-13 Aralık, Berlin, 552-565.
- Rouhani S. ve Deters R. (2017). “Performance Analysis of Ethereum Transactions in Private Blockchain”. *8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 24-26 Kasım, Beijing.
- Sadowski, J. (2019). “When Data is Capital: Datafication, Accumulation, and Extraction”. *Big Data & Society*, 6(1), 1-12.

- Samreen, N. F. ve Alalfi, M. H. (2023). “An Empirical Study on the Complexity, Security and Maintainability of Ethereum-Based Decentralized Applications (Dapps)”. *Blockchain: Research and Applications*, 4(2), 100120, 1-13.
- Sayers, S. (2018). “Emek Kavramı: Marx ve Eleştirmenleri”, A. Koşar (hızl.). *Maddi Olmayan Emek Teorisi: Kuramsal Bir Eleştiri*. Kor Kitap, İstanbul.
- Saura, J. R., Palacios-Marqués, D. ve Iturricha-Fernández, A. (2021). “Ethical Design in Social Media: Assessing the Main Performance Measurements of User Online Behavior Modification”. *Journal of Business Research*, (129), 271-281.
- Schiller, H.I. (1976). *Communication and Cultural Domination*. White Plains Press, New York.
- Scolari, C. A. (2012). Media Ecology: Exploring the Metaphor to Expand the Theory. *Communication Theory*, 22(2), 204-225.
- Scholz, T. (2010). “Facebook as Playground and Factory”. D. E. Wittkower (Ed.). *Facebook and Philosophy: What’s on Your Mind?* Open Court, Illinois.
- Scott, J. C. (2021). *Tahakküm ve Direniş Sanatları: Gizli Senaryolar*. (Çev. A. Türker), Ayrıntı Yayınları, İstanbul.
- Schuler, D. (2002). “Digital Cities and Digital Citizens”. Tanabe, M., van den Besselaar, P., Ishida, T.(Ed.). *Digital Cities II: Computational and Sociological Approaches, Lecture Notes in Computer Science*, 2362, 71-85.
- Smith, A. (2014). *Milletlerin Zenginliği*. (Çev. H. Derin), Türkiye İş Bankası Kültür Yayınları, İstanbul.
- Smythe, D. (2006). “Batı Marksizminin Kör Noktası”, L. Yaylagül (drl.). *Kitle İletişiminin Ekonomi Politikası*. Dalbaz Yayıncılık, Ankara.
- Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H. ve Borgthorsson, H. (2014). “Leakiness And Creepiness in App Space: Perceptions Of Privacy And Mobile App Use”. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2347-2356.
- Singh, M. ve Kim, S. (2019). “Blockchain Technology for Decentralized Autonomous Organizations”. *Advances in Computers* (115), 115-140.
- Singh, R. (2023). “The Decolonial Turn is on the Road to Contingency”. *Information, Communication & Society*, 26(4), 803-806.
- Speckmann, B. (2008). *The Android mobile platform*. (Yüksek Lisans Tezi). Eastern Michigan University, Michigan.

- Spreeuwenberg, K. ve Poell, T. (2012). "Android and the Political Economy of the Mobile Internet: A Renewal of Open Source Critique". *First Monday*. <http://firstmonday.org/ojs/index.php/fm/article/view/4050/3271#author> (erişim tarihi: 09.10.2023).
- Srnicek, N. (2017). *Platform Capitalism*. Polity Press, Cambridge.
- Stevenson, N. (2008). *Medya Kültürleri. Sosyal Teori ve Kitle İletişimi*. (Çev. G. Orhon ve B. E. Aksoy), Ütopya Yayınevi, Ankara.
- Struse, E., Seifert, J., Üllenbeck, S., Rukzio, E. ve Wolf, C. (2012). "Permission Watcher: Creating User Awareness of Application Permissions in Mobile Systems". *Ambient Intelligence: Third International Joint Conference*, 13-15 Eylül, Pisa, 65-80.
- Sunio, V. ve Schmöcker, J. D. (2017). "Can we Promote Sustainable Travel Behavior through Mobile Apps? Evaluation and Review of Evidence". *International Journal of Sustainable Transportation*, 11(8), 553-566.
- Swirsky J. ve Pajot L. (Yapımcı-Yönetmen), *Indie Game: The Movie* [Film], BlinkWorks Media, Kanada.
- Taffel, S. (2023). Data and Oil: Metaphor, Materiality and Metabolic Rifts. *New Media & Society*, 25(5), 980-998.
- Talay, Ö. (2018) *Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi*. (Yayımlanmamış Yüksek Lisans Tezi). Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya.
- Talay, Ö. (2022). "Dijital Oyunlarda Başarının Kestirme Yolu: Oyun İçi Ekonomik Etkinliklerde Güç ve Statü Alışverişi". *Ankara Üniversitesi İletişim Fakültesi Dergisi*, 9(2), 286-311.
- Talay, Ö. ve Çelik, H. C. (2023). "What Does Google Opinion Rewards Require and Get from Users?". *Central European Journal of Communication*, 16(1), 79-100.
- Taşkaya, M. ve Talay, Ö. (2019). Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza". *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, (31), 356-376.
- Thatcher, J., O'Sullivan, D. ve Mahmoudi, D. (2016). "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data". *Environment and Planning D: Society and Space*, 34(6), 990-1006.
- Timisi, N. (2016). "Teknoloji ve Toplum, Ağlar ve Aktörler". *Dijital Kavramlar, Olanaklar, Deneyimler*. N. Timisi (hızl.). Kalkedon Yayınları, İstanbul.

- Torlak, Ö. (2000). *Tüketim: Bireysel Eylemin Toplumsal Dönüşümü*. İnkılâb Basım Yayım, İstanbul.
- Turow, J. (2015). *İzleniyoruz*. (Çev. M. Benveniste), Hil Yayın, İstanbul.
- Uca, O. (2016). *Türkiye’de Orta Sınıfın Fotoğrafı: Akışlar ve İlişkiler: Maddi Olmayan Emeğe Sahanın Eleştirisi*. NotaBene Yayınları, İstanbul.
- University of Washington (2012) “A Study of Third-Party Tracking by Mobile Apps in The Wild”. (UW-CSE-12-03-01). Han, S., Jung, J. ve Wetherall, D. University of Washington Technical Report, Washington. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4834a5e2f55d194fa0e28f03b7d87759697de545> (erişim tarihi 6.7.2023).
- Uğurlu, G. (2022). *Tersine Mühendislik Yöntemleri ve Bilgisayar Uygulamaları Analizi*. (Yüksek Lisans Tezi). Başkent Üniversitesi Fen Bilimler Enstitüsü, Ankara.
- Vallina-Rodriguez, N., Sundaresan, S., Razaghpanah, A., Nithyanand, R., Allman, M., Kreibich, C. ve Gill, P. (2016). “Tracking The Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem”. *arXiv*, arXiv:1609.07190, 1-6.
- Van Dijk, J. (2016). *Ağ Toplumu*. (Çev. Ö. Sakin), Kafka Yayınevi, İstanbul.
- Van Dijck, J. (2014). “Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology”. *Surveillance & Society*, 12(2), 197-208.
- Van Dijck, J. ve Poell, T. (2016). “Understanding the Promises and Premises of Online Health Platforms”. *Big Data & Society*, 3(1), 1-11.
- Vanrykel, E., Acar, G., Herrmann, M. ve Diaz, C. (2017). “Leaky Birds: Exploiting Mobile Application Traffic for Surveillance”. *Financial Cryptography and Data Security: 20th International Conference*, Şubat, Barbados, 367-384.
- Vasa, R., Hoon, L., Mouzakis, K. ve Noguchi, A. (2012). “A Preliminary Analysis of Mobile App User Reviews”. *Proceedings of the 24th Australian Computer-Human Interaction Conference*, 26-30 Eylül, Melbourne, 241-244.
- Vaudenay, S. (2020). “Centralized or Decentralized? The Contact Tracing Dilemma”. *IACR Cryptology ePrint Archive*, 531, 1-31.
- Velkova, J. ve Kaun, A. (2021). “Algorithmic Resistance: Media Practices and the Politics of Repair”. *Information, Communication & Society*, 24(4), 523-540.
- Vercellone, C. (2015). “Üretken Emek Kavramının Dönüşümü ve Yeni Bölüşüm Kuralları”, (Çev. D. Kundakçı), *Bilişsel Kapitalizm: Post-Fordist Dönemde Bilgi ve Finans*, Otonom Yayıncılık, İstanbul.

- Viera Magalhães, J. ve Couldry, N. (2021). “Giving by Taking Away: Big Tech, Data Colonialism and the Reconfiguration of Social Good”. *International Journal of Communication*, 15, 343-362.
- Wagner, S. ve Fernandez-Ardevol, M. (2016). “Local Content Production and the Political Economy of the Mobile App Industries in Argentina And Bolivia”. *New Media & Society*, 18(8), 1768-1786.
- Wallerstein, I. (2021). *Tarihsel Kapitalizm ve Kapitalist Uygarlık*. (Çev. N. Alpay), Metis Yayınları, İstanbul.
- Wang, H., Liu, Z., Guo, Y., Chen, X., Zhang, M., Xu, G. ve Hong, J. (2017). “An Explorative Study of the Mobile App Ecosystem from App Developers’ Perspective”. *Proceedings of the 26th International Conference on World Wide Web*, 3-7 Nisan, Perth, 163-172.
- Wang, S., Ding, W., Li, J., Yuan, Y., Ouyang, L. ve Wang, F. Y. (2019). “Decentralized Autonomous Organizations: Concept, Model, And Applications”. *IEEE Transactions on Computational Social Systems*, 6(5), 870-878.
- Wang, D., Zhao, J. ve Wang, Y. (2020). “A Survey on Privacy Protection Blockchain: The Technology and Application”. *IEEE Access*, (8), 108766-108781.
- Wasko, J. (2006). “Hollywood’daki ‘Yeni’ Teknolojiler Hakkında Bu Kadar ‘Yeni’ Olan Nedir? İletişimin Ekonomi Politığının İncelenmesinin Bir Örneği”. L. Yaylagül (drl.). *Kitle İletişiminin Ekonomi Politığı*. Dalbaz Yayıncılık, Ankara.
- Wayne, M. (2015). *Marksizm ve Medya Araştırmaları: Anahtar Kavramlar, Çağdaş Eğilimler*. (Çev. B. Cezar), Yordam Kitap, İstanbul.
- Weerkamp, W. ve De Rijke, M. (2012). “Activity Prediction: A Twitter-Based Exploration”. *SIGIR Workshop on Time-Aware Information Access*, Ağustos, Portland, (16), 1-4.
- West, S. M. (2019). “Data Capitalism: Redefining The Logics of Surveillance and Privacy”. *Business & Society*, 58(1), 20-41.
- Wetherall, D., Choffnes, D. R., Greenstein, B., Han, S., Hornyack, P., Jung, J. ve Wang, X. S. (2011). “Privacy Revelations for Web and Mobile Apps”. *13th Workshop on Hot Topics in Operating Systems*, 9-11 Mayıs, Napa, 1-5.
- Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D. ve Beznosov, K. (2017). “The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences”. *2017 IEEE Symposium on Security and Privacy (SP)*, 22-26 Mayıs, San Jose, 1077-1093.
- Wilken, R., Burgess, J. ve Albury, K. (2019). “Dating Apps and Data Markets: A Political Economy of Communication Approach”. *Computational Culture*, (7), 1-26.

- Wittel, A. (2019). “Sayısal Marx: Dağıtık Medyanın Ekonomi Politğine Doğru”. V. Mosco ve C. Fuchs (drl.). *Marx Geri Döndü. Medya, Meta ve Sermaye Birikimi*. NotaBene Yayınları, Ankara.
- Wood, M. A. and Thompson C. (2018). “Crowdsourced Countersurveillance: A Countersurveillant Assemblage?”. *Surveillance & Society*, 16(1), 20-38.
- Wright, A. J. (2021). “The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges”. *Stanford Journal of Blockchain Law & Policy*, 4(2), 152–176.
- Wu, W., Wu, J., Wang, Y., Ling, Z. ve Yang, M. (2016). “Efficient Fingerprinting-Based Android Device Identification With Zero-Permission Identifiers”. *IEEE Access*, (49), 8073-8083.
- Wu, M. (2017). *Case Study the Indie Game Industry and Help Indie Developers Achieve Their Success in Digital Marketing*. (Yüksek Lisans Tezi). Northeastern University, Boston.
- Wu, K. (2019). “An Empirical Study of Blockchain-Based Decentralized Applications”. *arXiv preprint arXiv:1902.04969*, 1-11.
- Wu, K., Ma, Y., Huang, G. ve Liu, X. (2021). A First Look at Blockchain-Based Decentralized Applications. *Software: Practice and Experience*, 51(10), 2033-2050.
- Wukkadada, B., Nambiar, R. ve Nair, A. (2015). Mobile Operating System: Analysis and Comparison of Android and iOS. *International Journal of Computing and Technology*, 2(7), 273-276.
- Yıldırım A. ve Şimşek H. (2016). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri*. Seçkin Yayıncılık, Ankara.
- Zhang, J., Sagar, S. ve Shihab, E. (2013). “The Evolution of Mobile Apps: An Exploratory Study”. *Proceedings of the 2013 International Workshop on Software Development Lifecycle for Mobile*, 19 Ağustos, Saint Petersburg, 1-8.
- Zhang, Y. ve Zhang, J. (2021). “Catch Them All: Impacts of Location-Based Augmented Reality Mobile Applications on Local Businesses”. *Information & Management*, 58(8), 103550, 1-17.
- Zheng, P., Jiang, Z., Wu, J. ve Zheng, Z. (2023). “Blockchain-Based Decentralized Application: A Survey”. *IEEE Open Journal of the Computer Society*, (4), 121-133.
- Zorlu, A. (2006). *Üretim Kapitalizminden Tüketim Kapitalizmine: Üretim ve Tüketim Teorileri*. Glocal Yayınları, Ankara.

- Zuo, C., Lin, Z. ve Zhang, Y. (2019). “Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps”. *IEEE Symposium on Security and Privacy (SP)*, Mayıs, San Francisco, 1296-1310.
- Zuboff, S. (2015). “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization”. *Journal of Information Technology*, 30(1), 75-89.
- Zuboff, S. (2021). Gözetleme Kapitalizmi Çağı. Gücün Yeni Sınırında İnsan Geleceği İçin Savaş. (Çev. T.Uzunoğlu), Okuyan Us Yayınevi, İstanbul.
- Zvarikova, K., Gajanova, L. ve Higgins, M. (2022). “Adoption of Delivery Apps During The COVID-19 Crisis: Consumer Perceived Value, Behavioral Choices, and Purchase Intentions”. *Journal of Self-Governance and Management Economics*, 10(1), 69-81.
- Zyskind, G. ve Nathan, O. (2015). “Decentralizing Privacy: Using Blockchain to Protect Personal Data”. *IEEE Security and Privacy Workshops*, Mayıs, San Jose, 180-184.
- Zwitter, A. (2019). “Büyük Veri Etiği” *İletişim Hakkı ve Yeni Medya: Tehditler ve Olanaklar*, Durna T., Binark M. ve Bayraktutan G. (drl.). Um: Ag Vakfı Yayınları, Ankara.

İnternet Kaynakları

- Ahuja, S., (2023). “Apple App Store Statistics 2023 – Trends And Figures”. <https://bigohitech.com/apple-app-store-statistics> (erişim tarihi: 05.11.2023).
- Aishwar, (2023). “Android Statistics 2023: Exciting Approach to Keep Your Eyes On”. <https://jitendra.co/android-statistics> (erişim tarihi: 04.11.2023).
- Apple, (2022). “Apple Privacy Policy”. <https://www.apple.com/legal/privacy/en-ww/> (erişim tarihi: 12.09.2023).
- Apple Support, (t.y.). <https://support.apple.com/tr-tr/guide/shortcuts-mac/apd2e30c9d45/mac#:~:text=An%20API%2C%20or%20application%20programming,receive%20content%20from%20the%20service> (erişim tarihi: 16.08.2023).
- Bambysheva, N., (2022) “Over \$3 Billion Stolen in Crypto Heists: Here Are The Eight Biggest”. <https://www.forbes.com/sites/ninabambysheva/2022/12/28/over-3-billion-stolen-in-crypto-heists-here-are-the-eight-biggest/?sh=57a942aa699f> (erişim tarihi 06.11.2023).
- Blockchainhub, (2019). “What is a DAO”. <https://blockchainhub.net/dao-decentralized-autonomous-organization> (erişim tarihi: 03.11.2023).
- Burton, F., “The Secrets of Countersurveillance”. <https://telluric.us/the-secrets-of-countersurveillance> (erişim Tarihi: 05.02.2023).

- Chisel Labs, (2023). What Is User? Definition, Types and Role <https://chisellabs.com/glossary/what-is-user/> (erişim tarihi: 15.06.2023).
- BBC News, “Chinese Factory Asks for ‘No Suicide’ Vow”. <https://www.nbcnews.com/id/wbna37354853> (erişim tarihi: 15.05.2022).
- Covello, L., (2021). “Why Personalization is the Holy Grail of Loyalty”. <https://www.forbes.com/sites/forbestechcouncil/2021/11/09/why-personalization-is-the-holy-grail-of-loyalty/?sh=7320ae5fe77c> (erişim tarihi: 24.11.2022).
- Curry, D., (2023). “Apple App Store Statistics (2023)”. <https://www.businessofapps.com/data/apple-app-store-statistics> (erişim tarihi: 05.11.2023).
- Dyche, J., (2012). “Big Data “Eurekas!” Don’t Just Happen”. <https://hbr.org/2012/11/eureka-doesnt-just-happen> (erişim tarihi: 02.10.2023).
- Exodus Privacy, (t.y.). “Trackers”. <https://reports.exodus-privacy.eu.org/en/info/trackers/> (erişim tarihi: 02.10.2023).
- Ferranti, M., (2000). “Bezos: Net Personalization is Key”. <https://www.computerworld.com/article/2596081/bezos-net-personalization-is-key.html> (erişim tarihi: 02.10.2023).
- Google, (2023). “Google Privacy Policy”. <https://policies.google.com/privacy?hl=en-US> (erişim tarihi: 12.09.2023).
- Google Play Store, “Mastodon Data Security”. <https://play.google.com/store/apps/datasafety?id=org.joinmastodon.android&hl=tr&gl=US> (erişim tarihi: 02.12.2023).
- Hamza, (2022). “What is Algorithmic Bias? And Why You Should Be Aware about It”. <https://medium.com/institute-for-ethics-and-emerging-technologies/what-is-algorithmic-bias-2f9d5a018f> (erişim tarihi: 02.12.2023).
- Harari Y. N., (2018). “Will the Future Be Human?”. *Davos: World Economic Forum 2018*. https://www.youtube.com/watch?time_continue=202&v=hL9uk4hKyg4 (erişim tarihi: 9 Mayıs).
- Howcroft, E. ve Satter R., (2023) “Blockchain Analysts Suspect North Korea-Linked Hackers behind \$70 Million Crypto Theft”. <https://www.reuters.com/technology/blockchain-analysts-suspect-n-korea-linked-hackers-behind-70m-crypto-theft-2023-09-15> (erişim tarihi: 06.11.2023).

- King, M., “A Working Life: The App Developer”. <https://www.theguardian.com/money/2011/mar/05/working-life-app-developer> (erişim tarihi: 05.02.2023).
- Korn, J., (2023). “Record \$3.8 Billion Stolen in Crypto Hacks Last Year, Report Says”. <https://edition.cnn.com/2023/02/01/tech/crypto-hacks-2022/index.html> (erişim tarihi: 06.11.2023).
- Maryville University, (t.y.). “Big Data and Data Mining: The Role Data Mining Plays in Big Data”. <https://online.maryville.edu/blog/big-data-and-data-mining-the-role-data-mining-plays-in-big-data/> (erişim tarihi: 10.10.2023).
- MAXQDA, (2023). “What Does MAXMaps Do?”. <https://www.maxqda.com/help-mx24/maxmaps/what-does-maxmaps-do> (erişim tarihi: 24.09.2023).
- Online Etymology Dictionary, (t.y.). <https://www.etymonline.com/word/indie> (erişim tarihi: 10.08.2023).
- Online Etymology Dictionary, (t.y.). <https://www.etymonline.com/word/independent> (erişim tarihi: 10.08.2023).
- Orr, A., (2022). “Apple Now Has over 34 Million Registered Developers”. <https://appleinsider.com/articles/22/06/06/apple-now-has-over-34-million-registered-developers> (erişim tarihi: 11.11.2023).
- Pedercini, P., (2012). “Toward Independence”. <https://www.molleindustria.org/blog/toward-independence-indiecade-2012-microtalk/> (erişim tarihi: 26.03.2023).
- Priori Data, (2023). “Google Play Store Revenue, Ratings & Subscription Stats 2023”. https://prioridata.com/data/google-play-revenue-statistics/#Annual_Google_Play_revenue_apps_games (erişim tarihi: 05.11.2023).
- Salek, N., (2008). “Secure the Internet, to Secure the Economy: OECD”. <https://www.crn.com.au/news/secure-the-internet-to-secure-the-economy-oecd-114605> (erişim tarihi: 10.10.2023).
- Share Lab, (2015a). “Invisible Infrastructures : Mobile Permissions”. <https://labs.rs/en/invisible-infrastructures-mobile-permissions> (erişim tarihi: 10.10.2023).
- Share Lab, (2015b). “Invisible Infrastructures : Online Trackers”. <https://labs.rs/en/invisible-infrastructures-online-trackers> (erişim tarihi: 10.10.2023).
- Singh, G., (2023). “iOS Operating System”. <https://www.codingninjas.com/studio/library/ios-operating-system> (erişim tarihi: 10.10.2023).

- Statista, (2023a). “Global Market Share Held by Mobile Operating Systems from 2009 to 2023, By Quarter”. <https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since2009/#:~:text=Android%20maintained%20its%20position%20as,the%20mobile%20operating%20system%20market> (erişim tarihi: 04.02.2023).
- Statista, (2023b). “Technology & Telecommunications Software Android - Statistics & Facts”. <https://www.statista.com/topics/876/android/#topicOverview> (erişim tarihi: 04.11.2023).
- Statista, (2023c) “Leading Android Apps in the Google Play Store Worldwide in June 2023, by Number of Downloads”. <https://www.statista.com/statistics/693944/leading-android-apps-worldwide-by-downloads> (erişim tarihi: 04.11.2023).
- Statista, (2023d). “Mobile Android Operating System Market Share Worldwide from January 2018 to July 2023, by Version”. <https://www.statista.com/statistics/921152/mobile-android-version-share-worldwide> (erişim Tarihi: 04.11.2023).
- Statista, (2023e). “Number of Apps Available in Leading App Stores As of 3rd Quarter 2022”. <https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/> (erişim Tarihi: 04.11.2023).
- The Economist, (2017). “The World’s Most Valuable Resource is No Longer Oil, But Data”.<https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> (erişim tarihi: 3 Mart 202).
- The Economic Times, (2022). “Apple Faces Critics over its Privacy Policies”. <https://economictimes.indiatimes.com/tech/technology/apple-faces-critics-over-its-privacy-policies/articleshow/96028085.cms> (erişim tarihi: 11 Mart 2023).
- The New York Times, (2024). “Apple Overhauls App Store in Europe, in Response to New Digital Law”. <https://www.nytimes.com/2024/01/25/technology/apple-app-store-europe.html> (erişim tarihi: 28.01.2024).
- Virtue Market Research, (2023). “Decentralized Application Development (DApps) Market Size (2023-2030)”. [https://virtuemarketresearch.com/report/decentralized-application-development-\(dapps\)-market](https://virtuemarketresearch.com/report/decentralized-application-development-(dapps)-market) (erişim tarihi: 11 Kasım 2023).
- Wolfel, E., (2022). “Apple iOS Operating System: History, Origin, and More”. <https://history-computer.com/apple-ios-operating-system-guide> (Erişim Tarihi: 4 Kasım 2023).

EK 1- MAXQDA KOD SİSTEMİ

Araştırmada kullanılan tematik analiz ve doküman analizine ait MAXQDA kod sistemleri aşağıdaki karekodda verilmiştir. Kod sistemleri, MAXQDA programına yüklenerek gelecek çalışmalarda kullanılabilir.



ÖZGEÇMİŞ

Adı ve SOYADI	Ömür TALAY
EĞİTİM DURUMU	
Mezun Olduğu Lise	Dikmen Lisesi, Ankara, 2000.
Lisans Diploması	Anadolu Üniversitesi, İktisat Fakültesi, İktisat, 2009.
Lisans Diploması	Akdeniz Üniversitesi İletişim Fakültesi, Halkla İlişkiler ve Tanıtım, Antalya, 2015.
Yan Dal	Akdeniz Üniversitesi İletişim Fakültesi, Radyo, Televizyon ve Sinema, Antalya, 2015.
Tezli Yüksek Lisans Diploması	Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Halkla İlişkiler ve Tanıtım Anabilim Dalı, Antalya, 2018.
Tezli Yüksek Lisans Tez Konusu	Mobil Ortam Reklamlarında Dijital Gözetim Algısı: Dijital Göçmenler ve Dijital Yerlilerin Karşılaştırmalı Analizi
Yabancı Dil	İngilizce
BİLİMSEL FAALİYETLER	
Araştırma Makaleleri Talay, Ö. ve Çelik, H. C. (2023). "What Does Google Opinion Rewards Require and Get from Users?". <i>Central European Journal of Communication</i> , 16(1), 79-100. Talay, Ö. (2022). "Dijital Oyunlarda Başarının Kestirme Yolu: Oyun İçerik Ekonomik Etkinliklerde Güç ve Statü Alışverişi". <i>Ankara Üniversitesi İletişim Fakültesi Dergisi</i> , 9(2), 286-311. Taşkaya, M. ve Talay, Ö. (2019). "Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza" ". <i>Akdeniz Üniversitesi İletişim Fakültesi Dergisi</i> , (31), 356-376. Kitap İncelemesi Talay, Ö. (2022). "Gözetleme Kapitalizmi Çağı: Gücün Yeni Sınırında İnsan Geleceği İçin Savaş". <i>Galatasaray Üniversitesi İletişim Dergisi</i> , (36), 165-170.	
İŞ DENEYİMİ	
Çalıştığı Kurumlar	Akdeniz Üniversitesi İletişim Fakültesi, 2007-...