Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Sosyoloji Anabilim Dalı

BÜYÜK VERİNİN BÜYÜK BİRADERE DÖNÜŞÜMÜ: DİJİTAL SOSYOLOJİ PERSPEKTİFİNDEN BİREYİN VERİLEŞMESİ VE VERİ GÖZETİMİ

Elif ÖZUZ DAĞDELEN

Doktora Tezi

Ankara, 2023

BÜYÜK VERİNİN BÜYÜK BİRADERE DÖNÜŞÜMÜ:
DİJİTAL SOSYOLOJİ PERSPEKTİFİNDEN
BİREYİN VERİLEŞMESİ VE VERİ GÖZETİMİ

Elif ÖZUZ DAĞDELEN

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü

Sosyoloji Anabilim Dalı

Doktora Tezi

Ankara, 2023

KABUL VE ONAY

Elif Özuz Dağdelen tarafından hazırlanan "Büyük Verinin Büyük Biradere Dönüşümü: Dijital Sosyoloji Perspektifinden Bireyin Verileşmesi ve Veri Gözetimi" başlıklı bu çalışma, 27.11.2023 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından doktora tezi olarak kabul edilmiştir.

[redacted]

Doç. Dr. Çiçek COŞKUN (Başkan)

[redacted]

Prof. Dr. Tuğça POYRAZ (Danışman)

[redacted]

Doç. Dr. Aslıhan ÖĞÜN BOYACIOĞLU (Üye)

[redacted]

Doç. Dr. Ceyda KULOĞLU (Üye)

[redacted]

Doç. Dr. Emek Barış KEPENEK (Üye)

Yukarıdaki imzaların adı geçen öğretim üyelerine ait olduğunu onaylarım.

Prof. Dr. Uğur ÖMÜRGÖNÜLŞEN

Enstitü Müdürü

YAYİMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin tamamını veya herhangi bir kısmını, basılı (kâğıt) ve elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kitap, lisans ve patent vb.) kullanım hakları bana ait olacaktır.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihlal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanılması zorunlu metinleri yazılı izin alınarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan ***"Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge"*** kapsamında tezim aşağıda belirtilen koşullar haricince YÖK Ulusal Tez Merkezi / H.Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- Enstitü / Fakülte yönetim kurulu kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren 2 yıl ertelenmiştir. (1)
- Enstitü / Fakülte yönetim kurulunun gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihimden itibaren ..... ay ertelenmiştir. (2)
- Tezimle ilgili gizlilik kararı verilmiştir. (3)

12/12/2023

[redacted]

Elif ÖZUZ DAĞDELEN

1"*Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge*"

(1) *Madde 6. 1. Lisansüstü tezle ilgili patent başvurusu yapılması veya patent alma sürecinin devam etmesi durumunda, tez* ***danışmanının*** *önerisi ve* ***enstitü anabilim dalının*** *uygun görüşü üzerine* ***enstitü*** *veya* ***fakülte yönetim kurulu*** *iki yıl süre ile tezin erişime açılmasının ertelenmesine karar verebilir.*

(2) *Madde 6. 2. Yeni teknik, materyal ve metotların kullanıldığı, henüz makaleye dönüşmemiş veya patent gibi yöntemlerle korunmamış ve internetten paylaşılması durumunda 3. şahıslara veya kurumlara haksız kazanç imkanı oluşturabilecek bilgi ve bulguları içeren tezler hakkında tez* ***danışmanının*** *önerisi ve* ***enstitü anabilim dalının*** *uygun görüşü üzerine* ***enstitü*** *veya* ***fakülte*** *yönetim* ***kurulunun*** *gerekçeli kararı ile altı ayı aşmamak üzere tezin erişime açılması engellenebilir.*

(3) *Madde 7. 1. Ulusal çıkarları veya güvenliği ilgilendiren, emniyet, istihbarat, savunma ve güvenlik, sağlık vb. konulara ilişkin lisansüstü tezlerle ilgili gizlilik kararı,* ***tezin yapıldığı kurum*** *tarafından verilir *. Kurum ve kuruluşlarla yapılan işbirliği protokolü çerçevesinde hazırlanan lisansüstü tezlere ilişkin gizlilik kararı ise,* ***ilgili kurum ve kuruluşun önerisi*** *ile* ***enstitü*** *veya* ***fakülte****nin uygun görüşü üzerine* ***üniversite yönetim kurulu*** *tarafından verilir. Gizlilik kararı verilen tezler Yükseköğretim Kuruluna bildirilir.*
Madde 7.2. Gizlilik kararı verilen tezler gizlilik süresince enstitü veya fakülte tarafından gizlilik kuralları çerçevesinde muhafaza edilir, gizlilik kararının kaldırılması halinde Tez Otomasyon Sistemine yüklenir.

** Tez* ***danışmanının*** *önerisi ve* ***enstitü anabilim dalının*** *uygun görüşü üzerine* ***enstitü*** *veya* ***fakülte yönetim kurulu tarafından*** *karar* ***verilir.***

ETİK BEYAN

Bu çalışmadaki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi, görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu, kullandığım verilerde herhangi bir tahrifat yapmadığımı, yararlandığım kaynaklara bilimsel normlara uygun olarak atıfta bulunduğumu, tezimin kaynak gösterilen durumlar dışında özgün olduğunu, **Prof. Dr. Tuğça POYRAZ** danışmanlığında tarafımdan üretildiğini ve Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesine göre yazıldığını beyan ederim.

[redacted]

Arş. Gör. Elif ÖZUZ DAĞDELEN

Kızım Defne’ye

TEŞEKKÜR

Hem yüksek lisans hem de doktora eğitim sürecim boyunca bana akademik anlamda sonsuz desteği ve katkısı olan, çalışkanlığını, sabrını ve güler yüzünü hep kendime örnek aldığım ve alacağım saygıdeğer danışmanım Prof. Dr. Tuğça Poyraz'a sonsuz teşekkürlerimi sunarım. Doktora tezim sürecinde Tez İzleme Kurullarında beni dinleyen ve tezime çokça katkı sağlayan Doç. Dr. Aslıhan Öğün Boyacıoğlu ve Doç. Dr. Ceyda Kuloğlu'na çok teşekkür ederim. Tez savunma sınavımda yer alan Doç. Dr. Emek Barış Kepenek ve Doç. Dr. Çiçek Coşkun'a önerileri ve destekleri için çok minnettarım.

Senelerce Başkent Üniversitesi'nde araştırma görevliliğim süresince aynı odayı paylaştığım, her konuda bana destek olan, akademik anlamda görüşleri ve gerçek dostluğuyla yanımda olan Arş. Gör. Melike Bozdoğan'a varlığı, desteği ve dostluğu için sonsuz teşekkürler. Orta Doğu Teknik Üniversitesi'nde tanışıp en yakın arkadaşlarımdan olan, Hacettepe Üniversitesi'ne birlikte geçip, birlikte araştırma görevliliği yolculuğuna başladığım, her zaman beni kendisi gibi düşünen, destek olan, benimle stres olup benimle mutlu olan canım arkadaşım Arş. Gör. Leyla Bakacak Karabenli'ye de çok teşekkür ederim. Yine bu süreçte desteklerini esirgemeyen sevgili çalışma arkadaşlarım Arş. Gör. Ayçe İdil Ataoğlu ve Arş. Gör. Ezgi Hazal Turhan'a teşekkür ederim.

Hayatım boyunca her zaman bana destek olan, başarılarımda büyük emekleri ve katkıları olan aileme minnettarım. Yanımda huzur ve neşe kaynağı olan babam Suat Özuz, annem Emel Özuz ve ablam Sevcan Özuz Achakzai'ye çok teşekkür ederim. Doktora sürecim boyunca, benimle hayatı ve sorumlulukları paylaşan, akademik ideallerim için her zaman beni yüreklendiren sevgili eşim Barış Can Dağdelen'e ve zor günlerde varlığıyla ve gülümsemesiyle beni mutlu eden canım kızım Defne Dağdelen'e de çok teşekkür ederim. Ayrıca enerjisiyle ve tatlılığıyla beni neşelendiren yeğenim Kayla Su Achakzai'ye de teşekkür ederim. Aynı şekilde her zaman bana destek olan Ali Dağdelen, Hanife Dağdelen ve Yağmur Gülsün Dağdelen'e de teşekkürlerimi sunarım.

Son olarak, bu araştırmayı yapmamı sağlayan, vakitlerini ayırıp benimle değerli bilgilerini ve deneyimlerini paylaşan tüm katılımcılara çok teşekkür ederim.

ÖZET

DAĞDELEN ÖZUZ, Elif. *Büyük Verinin Büyük Biradere Dönüşümü: Dijital Sosyoloji Perspektifinden Bireyin Verileşmesi ve Veri Gözetimi*, Doktora Tezi, Ankara, 2023.

Bu çalışmada bilgi ve iletişim teknolojilerinin ve gözetim sistemlerinin gelişimiyle birlikte bireyler hakkında toplanan verilerin toplumsal, kültürel, ekonomik, siyasi amaçlarla kullanıldığı ve kullanılabileceği potansiyeli düşünülerek büyük verinin artan etkisinin değerlendirilmesi hedeflenmektedir. Bu hedefle özellikle verileştirme ve veri gözetimi temel alınarak, büyük veri ve yeni gözetim pratiklerinin yol açtığı toplumsal değişimler incelenmektedir. Araştırma, 16 veri bilimcisi (bu sistemleri ve onların yol açabileceği sonuçları öngörebilen ve aynı zamanda deneyimleyen bireyler oldukları için) ile uzman mülakatları ve derinlemesine mülakatlar yapılarak gerçekleştirilmiştir. Mülakatlar ile onların ontolojik güvenlik (bireylerin değişimler dolayısıyla ortaya çıkan tepkiler, korkular ve endişelere karşı ne tür bir başa çıkma stratejisi geliştirdikleri incelendiği için) anlamında ne tür bir strateji geliştirdiği, bu strateji ve çözüm önerilerinin toplumda da nasıl fayda sağlar hale gelebileceği inşacı bir bakış açısı ve nitel analiz yöntemiyle analiz edilmektedir. Değerlendirmeler sonucunda, veri bilimcilerin gözünden bakıldığında, büyük verinin tanımının ve içeriğinin değiştiği ve bunun tamamen yeni bir dijital gözetim pratiği oluşturduğu görülmektedir. Bu çerçevede büyük veri karar verme mekanizmalarının temel öğesi, bir tür sermaye ve sınıflandırma aracı olarak ele alınmaktadır. Büyük veri ve yeni gözetim pratikleri, unutulma hakkı, kontrol amaçlı yaptırım, veri güvenliği ve manipülasyonu, güvenlik ihlali, bozulmuş veri, ayrımcılık, panoptik sınıflandırma, anonimliğin kalmaması, güç dengesizliği ya da gücün tekelleşmesi, yankı odası, sosyal ilişkilerde ön yargı gibi pek çok sorunla ilişkilendirilmektedir. Çalışmada yeni gözetim pratiklerinin özellikle güvenlik, risk ve ötekinin tanımlanması ile ilişkilendirildiği; sosyal ilişkiler ve sorumluluklar alanında da "mikro düzeyde gözetim pratiklerinin" uygulandığı görülmektedir. Katılımcıların ontolojik güvenlik anlamında özellikle kendi ülkelerindeki veri ihlallerinin onlarda "kendi güvenliğine ilişkin şüphe" yarattığı görülmekte; sosyal fayda için büyük veri ile bu sistemlerin ontolojik güvenliğe katkısı incelenirken; sosyal zarar için büyük veri kavramsallaştırmasıyla ontolojik güvensizliğin daha belirgin hale geldiği anlaşılmaktadır. Katılımcıların ontolojik güvenlik/güvensizlik anlamında daha çok pragmatik bir kabulleniş (örtülü bir kötümserlik) stratejisine başvurdukları, ama sürekli iyimserlik, alaycı kötümserlik ve radikal katılım anlamında değerlendirilebilecek stratejilere de sahip olduklarına dair bulgular olduğu da görülmekte ve açıklanmaktadır. Bu stratejiler bağlamında veri bilimcilerin görüşleri doğrultusunda farklı alanlarda çözüm önerileri sunulmaktadır.

Anahtar Sözcükler

Büyük Veri, Dijital Gözetim, Verileşme, Veri Gözetimi, Ontolojik Güvenlik

ABSTRACT

DAĞDELEN ÖZUZ, Elif. *Transformation of Big Data to Big Brother: Datafication and Dataveillance from the Perspective of Digital Sociology*, PhD Thesis, Ankara, 2023.

This study aims to evaluate the increasing impact of big data, considering the potential that data collected about individuals can be used for social, cultural, economic, and political purposes with the development of information and communication technologies and surveillance systems. With this aim, social changes caused by big data and new surveillance practices are examined, especially based on datafication and data surveillance. The research was carried out by conducting expert interviews and in-depth interviews with 16 data scientists (as they are individuals who experience these systems and can predict the consequences they may cause). Through the interviews it is examined with a constructivist perspective and the qualitative analysis method what kind of strategy individuals have developed in terms of ontological security (what kind of coping strategy they develop against reactions, fears and anxieties that arise due to changes) and how these strategies and solution suggestions can become beneficial in society. As a result of the evaluations, when viewed from the eyes of data scientists, it is seen that the definition and content of big data has changed, and this creates a completely new digital surveillance practice. In this context, big data is considered as the basic element of decision-making mechanisms and as a type of capital and classification tool. Big data and new surveillance practices are associated with a variety of problems, such as the right to be forgotten, sanctions for control purposes, data security and manipulation, security breach, rotted data, discrimination, panoptic classification, lack of anonymity, power imbalance or monopolization of power, echo chamber, prejudice in social relations. In the study, new surveillance practices are particularly associated with security, risk, and identification of the other; it is seen that "micro-level surveillance practices" are also applied in the field of social relations and responsibilities. In terms of ontological security, it is seen that data breaches in the participants' own countries raise "doubt about their own security" in them; while examining the contribution of big data and ontological security of these systems for social benefit; it is understood that ontological insecurity becomes more evident with the conceptualization of big data for social harm. It is also seen and explained that there are findings that the participants mostly resort to a pragmatic acceptance (implicit pessimism) strategy in the sense of ontological security/insecurity, but they also have strategies that can be evaluated in the sense of constant optimism, cynical pessimism, and radical participation. In the context of these strategies, solution suggestions are offered in different areas in line with the opinions of data scientists.

Keywords

Big Data, Digital Surveillance, Datafication, Dataveillance, Ontological Security

İÇİNDEKİLER

KISALTMALAR DİZİNİ

AB: Avrupa Birliği

AI: Yapay Zekâ (Artificial Intelligence)

AKP: Adalet ve Kalkınma Partisi

ATM: Bankamatik (Automated Teller Machine)

AVM: Alışveriş Merkezi

BİLGEM: Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

BİT: Bilgi ve İletişim Teknolojileri

B3LAB: Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı

CEO: Yönetim Kurulu Başkanı (Chief Executive Officer)

CHP: Cumhuriyet Halk Partisi

EYT: Emeklilikte Yaşa Takılanlar

FBI: Federal Soruşturma Bürosu (Federal Bureau of Investigation)

G20: Yirmiler Grubu

GDPR: Genel Veri Koruma Yönetmeliği (General Data Protection Regulation)

IMF: Uluslararası Para Fonu (International Monetary Fund)

IP: İnternet Protokolü (Internet Protocol Adress)

IT: Bilişim Teknolojisi (Information Technology)

KKB: Kredi Kayıt Bürosu

KVKK: Kişisel Verileri Koruma Kanunu

MHRS: Merkezi Hekim Randevu Sistemi

MİT: Millî İstihbarat Teşkilâtı

NASA: ABD Ulusal Havacılık ve Uzay Dairesi (National Aeronautics and Space Administration)

NFC: Yakın Saha İletişimi (Near Field Communication)

NVI: Nüfus ve Vatandaşlık İşleri

PET: Mahremiyet Artırıcı Teknolojiler (Privacy Enhancing Technologies)

QR: Kare Kod (Quick Response)

SD: Standart Çözünürlük (Secure Digital)

TC: Türkiye Cumhuriyeti

TÜİK: Türkiye İstatistik Kurumu

TÜBİTAK: Türkiye Bilimsel ve Teknik Araştırma Kurumu

UN: Birleşmiş Milletler (United Nations)

VPN: Sanal Özel Ağ (Virtual Private Network)

VR: Sanal Gerçeklik (Virtual Reality)

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

GİRİŞ

> *"Herkesi her an izliyor da olabilirlerdi. Ama size istedikleri zaman bağlanabildikleri açıktı. Çıkardığınız her sesin duyulduğunu, karanlıkta olmadığınız sürece her hareketinizin gözetlendiğini varsayarak yaşamak zorundaydınız; zorunda olmak ne söz, artık içgüdüye dönüşmüş bir alışkanlıkla yaşıyordunuz."* (Orwell, 1984, s. 13)

Devamlı olarak gözetlendiğini düşünerek yaşamak ve bir tür sosyal kontrol mekanizmasının altında olduğunu hissetmek, küreselleşme ve dijitalleşme teknolojilerinin bireysel ve toplumsal temelde yaptığı en büyük değişimlerden bir tanesidir. Özellikle Nesnelerin İnterneti, Yapay Zekâ Teknolojisi, Blokzincir gibi değişim ve dönüşümlerin büyük veriyi desteklemesi, gözetimin dijital gözetime evrilmesini hızlandırmış, dijital gözetim ise bireyleri hem kamusal hem mahrem alanlarda sarmalamıştır. Bir mesajlaşma uygulamasına dahil olabilmek için telefona gelen kodla onay vermek, bir sosyal medya platformuna katılabilmek için istenen tüm verileri paylaşmak ve sanal avatar ya da gerçek kimlikle oraya dahil olunsa da bir şeyleri feda etmek, başka bir uygulama için telefondaki tüm görsellere erişim hakkı vermek, indirim hakkı kazanabilmek için e-posta hesabına gelen herhangi bir linke tıklamak ve çeşitli alışveriş sitelerine üye olmak gibi durumlar bireylerin tüm hayatlarının büyük veriyle sarmalandığını gösteren bazı örneklerdir. Dahası gezilen, satın alınan, favorilere eklenen ya da tedarik edilince haber verilmesi istenen ürünlerle yine birçok veriyi ve tüketim pratiklerini, bilinen ve bilinmeyen kurumlar, şirketler, kuruluşlar, kişilerle paylaşmak büyük veriye dâhiliyetin görünen kısmıdır. Gündelik hayatta sorgulamadan "parantez içine alarak" ya da sorgulansa da dijital okuryazarlık, dijital beceriler ya da genel olarak bu sistemin işleyişi hakkında yeterli bilgiye sahip olunmadığı halde, çeşitli faydalar uğruna (sosyalleşebilmek, paylaşmak, alışveriş yapmak, ödeme yapmak, indirim kazanmak, iş ilanlarını takip edebilmek, iş hayatındaki bağlantılarını dijital ortamda da sürdürebilmek gibi) büyük veriye dahil olunmaktadır. Dijital sosyoloji alanının bilinen isimlerinden bir tanesi olan Lupton, kitabının giriş kısmında, artık dijital toplumda yaşadığımızı, bu toplumda yeni dijital teknolojilerin, günlük yaşantımızda, sosyal

ilişkilerimizde, yönetimde, ticarette, ekonomide, üretimde ve bilginin yayılımında ciddi bir etkiye sahip olduğunu belirtmektedir. Bu etkinin yanı sıra, bireylerin hareketleri, satın alma alışkanlıkları ve çevrimiçi iletişim pratiklerinin de dijital teknolojiler tarafından izlendiği ve istesek de istemesek de seçsek de seçmesek de bireylerin birer dijital veri öznesi haline geldiği yeni bir düzenden bahsetmektedir (2014).

Büyük veri bu anlamda, dijital toplumlarda, Durkheim'ın kavramsallaştırmasıyla dışsal ve zorlayıcı bir olgu haline gelmektedir. Bir toplumsal olguyu, onun bireyler üzerinde uyguladığı ya da uygulayabileceği dış zorlama gücüyle ilişkilendiren Durkheim, bu gücün varlığının herhangi bir yaptırımın olması ya da olgunun kendisini çiğnemeye yönelen bireysel girişime karşı gösterdiği dirençle tanımlanabileceğini söylemektedir (2019, s. 35). Bu tanımda olguları her şeyi yapma biçimi olarak değerlendiren Durkheim, bunların aynı zamanda toplu olma biçimleri olduğunu söylemekte ve ikisinin de kendini bireye kabul ettirdiğinden bahsetmektedir (age, s.36). Durkheim'ın toplumsal olguyla ilgili olarak ulaştığı son kısa tanım ise şu şekildedir: "Yerleşmiş olsun olmasın, birey üzerinde bir dış baskı uygulayabilecek her yapma biçimi toplumsal olgudur; ya da bireysel tezahürlerinden bağımsızca kendine özgü bir varlığı olup, verili bir toplumun yayılım alanında ola gelen her şey toplumsal olgudur" (s. 37).

Büyük veri ve onun temelini oluşturduğu gözetim sistemlerinin, toplumsal olgu olarak ele alınması sürecinde, bilgi ve iletişim teknolojilerindeki dönüşümler önemli bir rol oynamaktadır. Bu dönüşüm sürecine bakıldığında Toplum 1.0'dan Toplum 5.0'a uzanan büyük bir farklılaşma görülmektedir. Toplum 1.0 (insanların doğa ile uyumlu bir şekilde avlama ve toplama faaliyetleri gerçekleştirdiği toplum), Toplum 2.0 (tarımsal üretim, artan örgütlenme ve millet inşasının meydana geldiği toplum), Toplum 3.0 (Endüstri Devrimi ile endüstrileşmeyi destekleyen ve kitle üretimi ile makineleşmeyi mümkün kılan toplum), Toplum 4.0 (maddi olmayan varlıkları bilgi ağları olarak birbirine bağlayarak katma değeri artıran bir bilgi toplumu) ve son olarak Toplum 5.0 (Toplum 4.0 üzerine kurulan ve refah insan-merkezli toplum fikrini savunan bir

bilgi toplumu) olarak birbirini takip etmektedir (Fukuyama, 2018). Refah insan-merkezli bir bilgi toplumu düşünüldüğünde, Toplum 5.0, teknolojik değişimlerin toplumsal değerlere uyması ve insan-merkezli olmaktan çıkmasını engellemek amacıyla ortaya çıkan bir felsefe olarak da tanımlanmaktadır. Endüstri 4.0'ın temelde üretim alanında getirdiği değişikliklerin insanların yaşam tarzına olan etkilerini kontrol altına alarak, dijital teknolojilerin toplumsal fayda ile ilerlemesi felsefesini öne sürmektedir (a.g.e., 2018). Süper Akıllı Toplum olarak literatürde değerlendirilen bu kavram, Akıllı Evler, Akıllı Şehir, Akıllı Park Sistemleri, Akıllı Ulaşım ve Enerji Sistemleri gibi birçok yeni sistemi içinde barındıran toplumsal dönüşüme işaret etmektedir. Bahsi geçen tüm bu sistemler, bir yandan bireylerin hayatlarına teknolojik değişim ve dönüşümleri entegre etmesini sağlarken bir yandan bireysel ve kitlesel bir veri toplama sistemine imkân sağlamaktadır. Yaşam tarzında refahı temel alan bu sistemlerin vurgulanan en önemli noktalarından bir tanesi "gerçek hayattan elde edilen kişilerin ve toplumun davranış verilerinin, bilgilerinin bilgisayarlar tarafından işlenip tekrar gerçek hayatta kişilerin ve toplumun yönlendirilmesinde kullanılmasıdır" (Cem, 2020). Bu yönlendirmenin nasıl ve kim tarafından olacağı ise ülkeler ve toplumlar temelinde düşünüldüğünde dijitalleşen dünyanın en önemli sorunlarından biri haline gelmektedir.

Akıllı sistemlerin, bireysel ve kitlesel veri toplama sürecine dahil olmasına ek olarak, dünyadaki diğer örneklere bakıldığında dijital medya teknolojilerinin desteğiyle birlikte, sosyal medya araçları devletlerin vatandaşlarını değerlendirmesine, kontrol etmesine ve hatta bazı durumlarda yönlendirmesine imkân sağlamaktadır. Büyük verinin nasıl kullanıldığı ve kullanılabileceğinin, en güncel örneklerinden bir tanesi Çin Devlet Konseyi'nin 2014 senesinde "Sosyal Güven Sisteminin İnşası Taslak Programı" doğrultusunda sosyal güven kavramını yeniden tanımlayarak, dijitalin sağladığı tüm yeniliklerden faydalanarak "Sosyal Kredi Sistemi"[1] ismini verdiği yeni bir sistem oluşturmasıdır (Liang, Das, Kostyuk ve Hussain, 2018). Bu sistemle birlikte,

[1] Daha fazla bilgi için bknz. Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, *10*(4), 415-453.

insanların fiziksel olarak bulundukları mekanlardaki tavır alışları ve davranışları ile dijital sosyolojinin önerdiği gibi artık birer gerçek “mekân” anlamı kazanmakta, sosyal medya alanlarında, araçlarında veya platformlarındaki her bir hareketi, oluşturulan algoritmalar sayesinde her bir birey -devlet ile düşünüldüğünde- her bir vatandaş birer veri öznesi haline gelmektedir. Bireylerin puanları belirlenirken, sosyal habitusları, sosyal medya kullanımları, toplumsal sorumluluk projelerine katılımları, toplumda uygun görülen norm, değer ve yasalara uyup uymamaları gibi birçok etken bir araya getirilmekte ve puanlama bu şekilde gerçekleştirilmektedir. Bu şekilde bir sistemin kurulabilmesine imkân veren şey, dijital sosyolojinin de en temel konularından biri olan dijital gözetim sistemleridir.

Dijital gözetim kavramı, sadece Çin’in yaptığı gibi Sosyal Kredi Sistemi’ni kurabilmek için uygulama yapılan alanda kamera gibi fiziksel gözetim teknolojisi aletlerini kullanmayı değil; gözetim temelinde toplumsal ve bireysel anlamda arka planda işleyen düşünce sistemlerini de kapsamaktadır. Bu anlamda “Yapay Zekâ Destekli Sosyal Puanlama Sistemi” olarak değerlendirebileceğimiz “Sosyal Kredi Sistemi” yüz tanıma teknolojileri, sosyal medya kullanımı, yapay zekâ teknolojileri ve robot kuşların kullanımıyla toplumlarda sosyal güven kavramının yeniden sorgulanmasına neden olmaktadır. Çin bu anlamda ekstrem bir örnek olarak gösterilse de dijital toplumlarda dijital platformlar ile sosyal medya ve e-posta hesaplarındaki bireysel veriler, hangi internet sitelerinde dolaşıldığı, internette ne gibi aramalar yapıldığı, telefon konuşmaları, mesajlaşma uygulamalarındaki konuşmalar gibi birçok şekilde hem uluslararası şirketler hem de devletler tarafından bireysel verilerin toplanabileceği ve bu verilerin algoritmalar sayesinde kullanılabileceği görülmektedir. Almanya’da sırf bunun için NetzDG Yasası’nın konması, Avustralya’da e-Güvenlik Komiserliği’nin kurulması, Fransa’da nefret söylemlerine yönelik dijital ortamlar için özel yasa çıkarılması, Rusya’da kendi vatandaşlarının verilerinin ülke sınırlarındaki sunucularda tutulma zorunluluğu konması, Çin’de WhatsApp, Google, Twitter’ın yasak olması ve “milli” Weibo, Baidu, Wechat gibi uygulamaların kullanılmasının zorunlu kılınması da konunun ne kadar güncel ve

önemli olduğunun göstergelerindendir. Çin menşeili olarak görülen sosyal medya platformu olan TikTok'un ise ABD, Kanada ve bazı Avrupa ülkeleri tarafından kısıtlamalara tabii olduğu ve "ABD Meclis Dış İlişkiler Komitesi verilerini güvende tutmak amacıyla Başkan Biden'a uygulamayı yasaklama yetkisi verecek bir yasa çıkardığı bilinmektedir" (Kalsın, 2023). Almanya, Kanada, İngiltere ve Estonya[2] gibi ülkelerde ise kamu kurumlarında ya da devletin verdiği mobil cihazlarda uygulamanın kullanımında kısıtlamaya gidildiği görülmektedir (age, 2023). Bu durumun sadece veri güvenliğiyle alakalı olmadığı, aynı zamanda genellikle ABD temelli sosyal medya platformlarının güç sahibi olduğu bir düzende Çin'in ürettiği TikTok'un kullanımının diğer ülkeler ve özellikle ABD için bir sorun teşkil ettiği de belirtilmektedir. "Özellikle Çin kaynaklı olması ve ilk defa ABD ile sosyal medya alanındaki rekabete Çin'in güçlü bir şekilde girebilmesi, TikTok'u siyasi alanda da tartışılır hale getirmiştir" (Aras, 2022).

Tüm bu gelişmelerle bakıldığında, verileşme (datafication) ile toplumsal kontrolün sağlanmasının hedeflenebileceği ve bunun da gözetim teknolojileriyle, veri gözetimi (dataveillence) ile yapılabileceği görülmektedir. Bu kavramlar sosyal güven kavramıyla birlikte de ele alınmakta, bireylerin içselleştirmiş oldukları gözetimle nasıl kategorize edilebilecekleri, zorunlu ya da gönüllü bir şekilde sistemlere ve yaptırımlara uyabileceklerinden bahsedilmektedir. Bu kavramlarla bağlantılı olarak kullanılan güvenin oyunlaştırılmasıyla (gamification of trust) ise durumun bireyleri belli bir kredi sistemi temelinde değerlendirebilecek bir hale gelebileceği ifade edilmektedir.

Sosyal güven kavramı, dijitalleşmenin toplumda meydana getirdiği dijital kültür içerisinde şekillenirken, güç ve öznelleştirme teknolojilerinin kullanımı, itibar puantajı (reputation scoring), profil çıkarma (profiling) gibi tamamen yeni olan sosyolojik olgularla bir anlamda "toplum mühendisliği"nin ortaya çıkabileceği düşünülmektedir. Bu süreç, veri-güdümlü yönetim ve izlenebilirlik ya da

[2] Daha fazla bilgi için bknz. Kalsın, B. (2023). TikTok Yasaklarının Arka Planı: Veri Güvenliği mi? Siyasi İlişkiler mi?. *TheJournal of SocialSciences*, *64*(64), 148-159.

hesaplanabilirlik temelli düzenleyici sistemlerin de ortaya çıkabileceğini işaret etmektedir. Dijital sosyoloji alanında birer distopya olarak değerlendirilebilecek senaryolarıyla dikkat çeken birçok bölüme sahip Black Mirror dizisinin "Nosedive" bölümünde de seneler önce konu alındığı gibi, mobil cihazların giderek bireyin bir parçası haline gelmesi "teknolojik habitusların" oluşması, bedenin ve kimliğin nicelikleştirilmesi (quantification), bireylerin sosyal habituslarının etki küresi ve iç halka gibi terimlerle ayırt edilerek sosyal parametrelerin analizlerinin yapılması ve hatta sosyal parametreleri düşük olan bireylerin puanlarını yükseltebilme sorumluluğu olan yeni meslek dallarının ortaya çıkması gibi düşüncelerin hiçbirinin ütopya olmadığını ortaya koymaktadır. Çin örneğinde olduğu gibi, sosyal medya araçları gözetim ve değerlendirme süreçlerinde planlamayı belirleyen en etkin araçlar haline gelmiştir. Bu araçlar, bireyler arasında "sosyal medya hiyerarşisi" temelinde etkileşim ritüellerini doğrudan etkilemektedir.

Dijital gözetim insan hayatına bu derece dahil olmuşken, devletler, kurumlar, şirketler, bireyler, ulusal ve uluslararası farklı ölçekteki güçler farklı hedeflerle bireyleri gözetim altında tutmaktadır. Bu kapsamda, bu tezde büyük verinin ve dijital gözetimin boyutlarının ne durumda olduğu, teknik, siyasi, teknolojik, sosyolojik, kültürel ve ekonomik anlamda ne tür öngörülere ulaşılabileceği anlaşılmaya çalışılmaktadır. Tezin amacı, bu doğrultuda, sorgulamadan yaptığımız şeyleri, gündelik hayatta parantez içine aldıklarımızı, büyük verinin dışsal ve zorlayıcı olmasının sonuçlarını ortaya çıkarmaktır. Özellikle kendini izleme, denetim, gözetim, mahremiyet algısı ve tanımı, farkındalıklar, riskler ve ontolojik güvenlik temelinde bu durumun açıklanması gerektiği düşünülmektedir.

Büyük verinin büyük biradere dönüşümünü görebilmek ve dijital gözetim kuramları ile değerlendirebilmek amacıyla bu tezde: Bu sistemleri tasarlayan ve dijital okuryazarlığı, dijital becerileri en yüksek olan grupta kişisel güven ya da ontolojik güven inşasında büyük verinin rolü nedir? Başkalarına güven duymak için onları gözetlememiz gerekir mi? Büyük veri ve dijital gözetim sistemlerinin güvenin oyunlaştırılmasındaki rolü nedir? Dijital gözetim sistemlerinin ve

temelde büyük verinin güven inşasındaki rolü nedir? Niçin çoğu insan, çoğu zaman, üzerinde kendi teknik bilgilerinin pek az olduğu ya da hiç bulunmadığı uygulamalara ve toplumsal düzeneklere güvenir? (Anthony Giddens'ın Modernliğin Sonuçları kitabında sorduğu temel sorulardan bir tanesi) Güven inşası aşamalarında hangi araçlar ve hangi platformlar daha çok kullanılmaktadır? Büyük verinin güven inşası kullanımında ve büyük veri sistemlerine dâhiliyette tanıdıklık ve yabancılık arasında ne tür farklılıklar vardır? Büyük veriye dahil olmak insanları daha güvende hissettirir mi? Güven ilişkisi kurmak için mahremiyetten vazgeçmek gerekli midir? Büyük verinin mahremiyeti aşındırması ve güven inşasında kullanılması, gerçekten kişisel olarak da itibar puantajı, profil çıkarma gibi durumlara yol açar mı? Gelecekte büyük veri kullanılarak oluşturulan kartografiler ne gibi sonuçlara yol açabilir? Sosyal parametrelerden sorumlu yeni meslek dalları ortaya çıkabilir mi? Bireyler verilerine göre puanlanabilir mi? Arkadaşlık, dostluk, iş arkadaşlığı, akrabalık ilişkileri, evlilik, sevgililik gibi sayılabilecek tüm ilişkilerde bu puanlamanın etkisi ne yönde olabilir? Büyük verinin gelecekte sağlayabileceği olumlu ve olumsuz durumlar neler olabilir? Devlet ve vatandaş arasındaki güven ilişkisinde büyük veri nasıl bir rol oynayabilir? Büyük verinin sebep olduğu yeni dijital gözetim pratiklerinin sosyolojik olarak ortaya çıkaracağı değişimler nelerdir? sorularına cevap aranmaktadır.

Çalışmada amaçlı örneklem ile belirlenmiş, büyük veriyi kendi mesleğinde aktif olarak kullanan, büyük verinin işleyişi konusunda bilgi sahibi olan ve büyük verinin geleceği hakkında fikir yürütebilecek 16 veri bilimci ile derinlemesine mülakatlar ve uzman mülakatları gerçekleştirilmiştir.

Çalışma 4 bölümden oluşmaktadır. İlk bölümde araştırmanın konusu, amacı ve önemi ve problem cümleleri net bir şekilde belirtildikten sonra uygulamalı bir çalışma olan bu çalışmanın yöntemi başlığı altında ne tür bir ontolojik epistemolojik bakış açısıyla konuya yaklaşıldığı, veri toplama aracı, veri toplama ve veri değerlendirme süreciyle ilgili bilgilendirmeler yapılmaktadır.

İkinci bölümde ise araştırmanın kavramsal çerçevesi başlığı altında büyük verinin kavramsal olarak ne ifade ettiği ve onunla ilgili kavramların literatür yardımıyla tanımlamaları yapılmaya ve açıklanmaya çalışılmaktadır. Öncelikli olarak kavramsal olarak büyük veri, büyük verinin ortaya çıkışı ve gelişimi, büyük veriyi destekleyen sistemler, büyük veri analizi, verinin değeri, metaveri, sayısallaştırma, işlevsel fayda, veriyi ikincil konuma tabii tutma, büyük veri ayrımı, algoritmik manipülasyon kavramları ve bu kavramlarla ilişkili kavramlar açıklanmakta daha sonra dijital sosyolojide büyük veriyi açıklayan temel iki kavram olan verileştirme ve veri gözetimine odaklanılmaktadır. Özellikle kişisel ve kitlesel veri gözetimi de açıklanmaya çalışılmakta, konuyla ilgili en güncel ve en önemli örneklerden bir tanesi olduğu için kısaca yapay zekâ destekli sosyal puanlama sistemi de bu kısma dahil edilmektedir.

Üçüncü bölümde araştırmanın kuramsal çerçevesi başlığı altında dijital sosyoloji temelinde gözetimden dijital gözetime başlığı altında daha pek çok sayıda kavram olsa da (bunların da isimleri belirtilmektedir) literatürde en çok tartışılan ve kullanılan panoptikon, sinoptikon, panspektron, süperpanoptikon ve oligoptikon üzerinde durulmaktadır. Daha sonra dijital gözetim sosyolojisi kuramlarında da geniş bir çerçeve olduğu için sosyal bir tasnif olarak, panoptik tasnif olarak, gözetim simülasyonu formunda, akışkan, rizomatik, içselleştirilmiş, risk önleme aracı olarak, prostetik gözetim ile yeni gözetim ve gözetim kapitalizmi başlıkları altında, bu alandaki en önemli kuramların her birine yer verilmeye çalışılmaktadır.

Dördüncü bölümde ise nitel yöntemle elde edilen verilerin analizi doğrultusunda ortaya çıkan sonuçları açıklama amacıyla “Veri Bilimcilerin Gözünden Büyük Veri”, “Veri Gözetimi ve Toplumsal Değişimler”, “Sosyal İlişkiler ve Sorumluluklar Alanında Büyük Veri” ve “Büyük Verinin Geleceği: Veri Bilimciler ve Ontolojik Güvenlik” başlıkları altında araştırmanın sonuçları paylaşılmaktadır.

BİRİNCİ BÖLÜM

ARAŞTIRMANIN KAPSAMI VE YÖNTEMİ

1.1. ARAŞTIRMANIN KONUSU AMACI VE ÖNEMİ

1.1.1. Araştırmanın Konusu

Bu araştırmanın konusu, dijital gözetim sosyolojisi perspektifinden, büyük verinin ve dijital gözetim sistemlerinin veri analistlerinin ontolojik güvenlik algısında ve dolayısıyla toplumda yarattığı/yaratabileceği değişimlerdir. Büyük veri, bireyler hakkında toplanan veriler bütünüdür ve eskiden daha çok "suçlu" ya da "sapkın" bireyleri tespit etmek için kullanılan gözetim, sadece belirli bireyleri kapsarken, günümüzde dijitalleşmenin de etkisiyle kitlesel hale gelerek kapsamı, hedefi ve etkileri de genişlemiştir. Bireylerin sosyal dünyada var olabilmek için, dijital ortamda da aktif bir şekilde yaptıkları veri paylaşımının giderek bu verilerin toplanması ve işlenmesiyle farklı bir boyuta taşındığı bilinmektedir. Geçmişten bu yana, kişisel verilerin çeşitli sebeplerle toplanarak, farklı amaçlarla ve özellikle de gözetim pratiklerinde kullanılması olağan bir durum olarak görülmeye başlanmıştır. Tarihteki birçok güvenlik açığına ve bireysel verilerin çok daha farklı amaçlarla kullanıldığı ve kullanılabileceği tehlikesinin bilinmesine rağmen, büyük veri onu çevreleyen sistemlerle daha da güçlenmiş ve toplumsal sınıflandırma pratiklerinde aktif olarak kullanılabilecek bir gözetim aracı haline gelmiştir.

Modern öncesi, modern, post-modern ya da Bauman'ın kavramlarıyla panoptik ve akışkan modernitenin post-panoptik güçlerinin odaklandığı nokta, genellikle mahremiyet kaybı olsa da gözetim yalnızca bu durumla değil, "tarafsızlık ve adalet, temel özgürlükler ve insan hakları" ile de ilişkilidir (Bauman ve Lyon, 2020, s. 24). Bireylerin gündelik hayatlarında bıraktıkları dijital izlerin onların farkında olarak ya da olmayarak kullanılması, günümüz dünyasının bir gerçeği haline gelmiş, büyük veri karar verme mekanizmalarının da temeline oturmuştur. Bu karar verme mekanizmalarında, büyük veri yığınları içerisinden,

gelişmiş yazılım sistemleriyle analiz edilen veriler, bireylerin, grupların ya da toplumların manipüle edilmesi ya da çeşitli alanlarda onlar hakkında öngörü sağlamak için kullanılan bir sistem haline gelmiştir. Bu çalışmada, büyük verinin bu kapsamda görülen avantaj ve dezavantajları düşünülerek, büyük verinin özellikle veri bilimcilerin ontolojik güvenlik durumlarını nasıl etkilediği anlaşılmaya çalışılmakta ve ne tür sosyal politika önerileri olabileceği tartışılmaktadır. Büyük veri alanında çalışan uzmanların ontolojik güvenlik konusunda farkındalıklarının olup olmadığının keşfi, bireylerin gündelik hayatlarında sorgulamadan içine dahil oldukları, dijital dünyada güvenlik ve mahremiyet konularını yeniden sorgulamaya yol açmaktadır.

Araştırmada katılımcılar olarak veri bilimcilerin seçilme sebebi, günümüzde veri analisti, veri mühendisi, veri sorumlusu gibi pek çok farklı konumda çalışan genel olarak algoritmaların, kodlamanın mantığını, veri analizi ile neler yapabileceğini bilen, veri destekli karar verme mekanizmalarının nasıl işlediği ve nasıl kullanılabileceğini öngörebilecek bireyler olmalarıdır. Bunun dışında ne kadar bilinçli olunursa olunsun, sistemlere dahil olmak ve çeşitli uygulamalara erişmek için bireyler karşılarına çıkan uzun sözleşmeleri, izin formlarını genel olarak tam okumadan onaylamakta, kişisel bilgilerini paylaşmakta ve böylece dijital gözetime dahil olmaktadırlar. Yakın zamanda WhatsApp'ın veri ihlali ile ilişkili olarak ortaya çıkan haberlerden yola çıkan bir araştırma, sonuçları şu şekilde ifade etmektedir: "(Bu durum) Kişisel verilerin ticari kaygılar ile kullanılması gibi etik bir problemin ne kadar yaygın olduğu yönünde değerlendirilebilir ve pek çok kullanıcı tarafından gizlilik sözleşmelerinin okunmadan onaylanması, kullanıcının neye izin verdiğini bilmemesi sonucunu doğurmaktadır. Okunmadan onaylanan sözleşmeler, kişisel verilerin ekonomik bir değer olarak kullanımını kolaylaştırmaktadır" (Turancı, 2021). Okunmadan onaylanan sözleşmelerin yanısıra, Türkiye'de Kişisel Verileri Koruma Kanunu'na yönelik tehditlere karşı yasal bildirimlere bakıldığında bu sayının çok düşük olduğu görülmektedir. "Kişisel Verileri Koruma Kurumu Başkanı tarafından Anadolu Ajansı'na yapılan açıklamaya göre, Ağustos 2019 tarihi itibarı ile kuruma yapılan şikâyet sayısı 691, ihbar sayısı 83, veri ihlal bildirimi sayısı ise

108 olup toplam 882 başvurudan 439'u sonuçlandırılmıştır (Anadolu Ajansı, 2019 akt. Özdemir, 2020). Bu açıdan bakıldığında bireylerin verilerini bilinçli bir şekilde paylaşmama durumunun çok yüksek olmasının yanı sıra, aynı zamanda kendi verilerine yönelik ihlallerle karşılaştıklarında da bunla ilgili hukuki beyanda bulunmadıkları görülmektedir. Bu durum da bireyleri yeni gözetim sistemleri anlamında daha korumasız bir konuma itmekte, belki de hem ulusal hem uluslararası kurumlar hem de devletler tarafından verilerini, özellikle kişisel verilerini tehlikeye atmaktadır.

Bu tehlikeli durumun bu araştırmayı yapmanın temel sebeplerinden biri olmasının yanı sıra, araştırmanın amacı ve önemi ise bir sonraki kısımda güncel örneklerle gösterilerek açıklanmaktadır. Aynı zamanda ontolojik güvenlik kavramının neden dahil edildiği ve neden bu kavramın tercih edildiğinden de bahsedilmektedir.

1.1.2. Araştırmanın Amacı ve Önemi

Bu çalışmanın giriş kısmında Orwell'in kitabından alıntılanan "Herkesi her an izliyor da olabilirlerdi. Ama size istedikleri zaman bağlanabildikleri açıktı. Çıkardığınız her sesin duyulduğunu, karanlıkta olmadığınız sürece her hareketinizin gözetlendiğini varsayarak yaşamak zorundaydınız; zorunda olmak ne söz, artık içgüdüye dönüşmüş bir alışkanlıkla yaşıyordunuz." (Orwell, 1984, s. 13) cümlesi bu çalışmanın ve araştırmacının temel endişesini (amacını) göstermekte ve bu çalışmanın neden gerçekleştirildiğine dair temel bir başlangıç noktası sağlamaktadır. Lyon ve Bauman'ın da vurguladığı gibi, "Zamyatin, Orwell, Aldous Huxley gibi geçmişteki en büyük distopya yazarları... kırmızı alarm veriyor, mezbahaya uysalca yürüyen koyun uyuşukluğunda bir bilinmeyene doğru giderken yol arkadaşlarını bu tasavvurlarla sarmayı umuyorlardı" (Lyon ve Bauman, 2020, s. 123). Sosyal hayata dahil olabilmek için sürekli veri paylaşımı yapmanın bir rutin haline gelmesi, vatandaşlık bilgilerinden, finansal kayıtlara, kişisel bilgilere dijital sistemler vasıtasıyla ulaşmanın kolaylaşması fakat bu verileri korumanın gittikçe zorlaşması, bu

paylaşımın sorgusuz bir alışkanlık haline gelmesi ve hatta giriş kısmında da vurgulandığı gibi büyük verinin dışsal ve zorlayıcı bir olgu haline gelmesi bu çalışmanın neden yapılması gerektiğine dair önemli unsurlar olarak görülmektedir. Çalışma, bu sistemleri en iyi bilen bireylerden bilgi alarak bir uyarı niteliği taşımakta, bu sistemlerin dijital gözetim anlamında ne tür bir noktaya ulaşabileceğini, toplumsal değişime dair bir öngörüde bulunabilmeyi, bu değişimleri ortaya çıkarmayı amaçlamaktadır. Bu kapsamda veri bilimcilerin ontolojik güvenliklerine bakarak bu sistemlere hâkim bireylerin içinde bulunduğu durumu görmek, toplumun geri kalanı ile ilgili endişeleri ve öngörüleri dile getirmek de hedeflenmektedir. Bu amaç, araştırmanın bir genelleme amacı olduğu anlamına gelmemekte, tamamen bu konuda en bilgili kesimin bilgisine başvurarak, toplumdaki diğer bireyler için de çözüm önerileri ortaya koyma ve farkındalık yaratma hedefini ifade etmektedir.

Ontolojik güvenlik, Giddens'ın "Modernliğin Sonuçları" kitabında "Güvenlik duygularının bir biçimi, kendi öz kimliklerimizin sürekliliğine ve çevredeki toplumsal ve nesnel eylem ortamlarının sabitliğine duyulan itimat. Kişi ve şeylerin güvenilir oldukları duygusu, ontolojik güvenlik duygularının temelini oluşturur" şeklinde açıklanmaktadır (Giddens, 2021, s. 93). Giddens, ontolojik güvenlik kavramıyla günümüzdeki güven ve mahremiyet ilişkilerini sorgularken, büyük veri gibi sistemlerin de bu anlamda tekrar düşünülmesine imkân sağlamakta ve gözetim, verileştirme ve veri gözetiminin kişisel güven sağlama anlamındaki rolüne teorik bir zemin sunmaktadır. Çünkü büyük verinin gittikçe gelişmesi ve bunların dijital gözetim ve kitlesel gözetim için kullanılmasının arkasındaki en büyük tehlike giriş kısmında da bahsedildiği gibi "gerçek hayattan elde edilen kişilerin ve toplumun davranış verilerinin/bilgilerinin bilgisayarlar tarafından işlenip tekrar gerçek hayattaki kişilerin ve toplumun yönlendirilmesinde kullanılmasıdır" (Cem, 2020).

Çalışmanın amacı bu temelde tekrar düşünüldüğünde, dijitalleşme ile kişilere, sistemlere, gruplara ve kurumlara duyulan güvenin nasıl oluştuğunu kuramsal olarak sorgulamayı, mahremiyetin gözetim ile dönüşümünü göz önünde

bulundurarak, ontolojik güvenlik ve büyük veri arasındaki bağlantı üzerine düşünmeyi hedeflemektedir. Büyük verinin, tıpkı para gibi simgesel bir işaret sistemi olup olmadığı, büyük veri temelli sistemlerin de bir tür uzmanlık sistemi olarak kabul edilip edilemeyeceği tartışılmaktadır. Bu temelde büyük veri ve büyük veri sistemleri, yerinden çıkarma düzeneği olarak günümüz dijital toplumlarında yer almakta ve Giddens'ın da öngördüğü şekilde bu yerinden çıkarma düzenekleri ile olanaklı/beklenen/elverişli geleceklerin listelenmesi yapılmaktadır. Yerinden çıkarma düzenekleri, ilişkileri yeniden yerleştirme ile başka bir boyuta taşımakta, güven örtülü ya da görünür bağlılıklar kavramlarıyla tekrar düşünülmektedir.

Araştırmanın önemi ve güncelliği ise, çalışmada sürekli bahsi geçen Yapay Zekâ Destekli Sosyal Puanlama Sistemi dışında, dijital gözetimin hem Türkiye'de hem uluslararası anlamda çok ciddi bir veri ihlaliyle ve ciddi bir güç olarak ilerleyebileceğiyle ilgilidir. İran'ın başörtüsü takmayanları yüz tanıma teknolojisiyle tespit etmeye başlaması, Tesla'da araçların içindeki kameralar aracılığıyla veri ihlalleri yaşanması, Thodex Skandalı gibi haberler gibi bunun pek çok örneği vardır. Bunların dışında, kuramsal kısımda da bahsedileceği gibi Cambridge Analytica, Snowden Olayı gibi gözetim ve sosyoloji kuramlarında sıklıkla bahsedilen, büyük veriyle neler yapılabileceğine dair örnekler de bu araştırmanın önemini gözler önüne sermektedir. Cambridge Analytica olayına bakıldığında "Cambridge Analytica veya Cambridge Analytica ile bağlantılı şirketler, 87 milyon kadar Facebook kullanıcısının ayrıntılı psikolojik profillerini oluşturmak için yaklaşık 200.000 Facebook kullanıcısının kişisel verilerini kullanmıştır. İlk 200.000 kullanıcı gönüllü olarak bir kişilik testini tamamlamış olsa da yanıtlarının nasıl kullanılacağını bilmiyorlardı ve profili çıkarılan 87 milyon kullanıcı da kesinlikle bunun için bilgilendirilmiş onaylarını vermemiştir" (Cadwalladr, 2018 akt. Heawood, 2018). Cambridge Analytica, bu devasa veri tabanını Birleşik Krallık, ABD ve diğer ülkelerdeki siyasi kampanyacıların Facebook kullanıcılarını son derece spesifik mesajlarla hedeflemesine yardımcı olmak için kullanılmıştır. Snowden Olayı'nda ise, Haziran 2013'te, eski bir NSA (National Security Agency- Ulusal Güvenlik Kurumu) çalışanı olan Edward

Snowden, ABD gözetimi hakkında çok sayıda gizli belge yayınlamıştır. NSA'yı vatandaşların haklarını ihlal etmek ve yasa dışı hareket etmekle suçlamıştır. Snowden'ın sızıntıları dünyanın dört bir yanından ilgi görmüştür. Örneğin, 29 Ekim 2015'te Avrupa Birliği, Snowden'a 'üye devletler dahilinde siyasi haklar' verilmesi lehinde oy kullanmıştır (Chen, 2017).

Çalışmanın temel amacından bir tanesi bireylerin kişisel verilerini bu kadar kolay paylaşma konusunda farkındalık yaratmasıdır. Lokke'un bu alandaki çok önemli bir kitabı olan "Mahremiyet ve Dijital Toplumda Özel Hayat" örneğine bakıldığında bireylerin çoğunlukla hiçbir bilgilendirmeyi okumadıkları görülmektedir: "İngiltere merkezli Game Station internet şirketinin 2010 yılında yaptığı 1 Nisan şakasında internet sitelerinde alışveriş yapmanın şartlarından biri, müşterinin ruhunu satmasıydı. Game Station, 10 kişiden 8'inin, sitede alışveriş yapmak için gerekli şartları okumadığını belirtti, bu da vatandaşların internetteki koşullar ve şartlar karşısındaki tutumunu gözler önüne seren bir olaydır" (Lokke, 2020, s. 75).

Bu durumun ne gibi bir sonucu olacağına dair çok önemli görüşleri olan Bridle da bu konunun neden acilen araştırılması ve konuya neden önem verilmesi gerektiği konusunda büyük veri ve işlemlemenin sonuçlarına dair değerlendirmelerde bulunmaktadır:

> *"İşlemleme önce kültürün haritasını çıkarıp modeller, sonra da onun kontrolünü devralır. Google önce insanlığın bildiği her şeyi kataloglamaya koyulup, sonra bu bilginin kaynağına, belirleyicisine dönüştü: İnsanların fiilen düşündüğü şey haline geldi. Facebook önce insanlar arasındaki bağlantıların haritasını -sosyal grafik- çıkarmaya girişip, sonra bu bağlantıların kurulduğu platform haline geldi ve toplumsal ilişkileri geri dönülmez biçimde yeniden şekillendirdi. Tıpkı göçmen kuş sürülerini bombardıman filoları zanneden bir hava kontrol sistemi gibi, yazılım da kendi dünya modeli ile gerçekliği birbirinden ayırt edemez ve bir kez şartlandığımızda aynı şey bizim için de geçerli hale geli*r" (Bridle, 2020, s. 49).

Aynı şekilde hem büyük arama motorlarının hem de büyük veriyi elinde tutan uluslararası büyük şirketlerin mahremiyet ilkelerini sürekli belirli çıkarlara göre

değiştirmesi ve genellikle bunlardan kullanıcılarının haberinin olmaması ve genellikle bu değişikliklerin bireylere çıkar sağlayacağı ifadesiyle daha çok veri istemi ve kullanımı doğrultusunda yönlendiği görülmektedir. Bu cümlelere çok net bir örnek ise büyük verinin temel kaynaklarından biri olan Google'ın mahremiyet ilkelerinde yaptığı değişikliktir. Google 2001 yılında mahremiyet ilkelerini doğrudan değiştirmiştir. 2000 senesinde doğrudan anonimlik garanti edilirken, 2001 senesinde aynı bilgisayarların daha önce Google'ı ziyaret eden bilgisayar olup olmama kaydını tutmasının yanı sıra, kişilerin kim olduğu ve hangi ülkede olduğu gibi bilgilere de erişim sağlamıştır. 2001 yılındaki değişim, mahremiyeti koruma ilkeleri şu şekilde değişmiştir: "İhtiyaç duyulduğunda, Google yalnızca, sizin kim olduğunuzu tanımlamakla kalmayıp üçüncü kişilerle bu bilgiyi paylaşabilecektir" (Lokke, 2020, s. 80).

Dijital sosyolojinin temel hedeflerinden bir tanesi, dijitalleşme ve toplumun birbirlerine uyum sağlayarak gelişmesidir. Dijital sistemler gelişirken, bireylerin ve toplumların haklarının korunması ve var olan toplumsal düzenin sosyal fayda gözetilerek etkilenmesi bu açıdan önemlidir. Dijital medya teknolojilerinin gelişiminin ya da dijital gözetimin birey özgürlüğünü, haklarını ya da toplum hayatını "insan-merkezli" bir anlayışı temel alarak ilerlemesi bu anlamda sosyolojik bakış açısı kazandırılması bilimsel birikim ve üretime katkı sağlayacaktır. Büyük veri, yapay zekâ, Nesnelerin İnterneti, Robotik, Blokzincir teknolojisinin birey ve teknoloji arasındaki ilişkiye nasıl bir etki yaptığı ve verileşme (datafication) ve veri gözetimi (dataveillance) gibi toplumda yer alabilecek düzenleyici sistemlerin analiz edilmesinin önemi küresel anlamda tartışılmaktadır. Belirtilen bu önemli durum, araştırmanın amacının büyük veri ve onu destekleyen sistemlerin, nasıl ilerlediğini gözetim temelinde inceleyerek bu alanda gerekli önlemlerin alınması ve düzenlemelerin yapılması olarak belirlenmesine sebep olmuştur.

Konunun küresel anlamda önem arz etmekle birlikte, özellikle Türkiye temelinde ayrıca önemli olduğu görülmüştür. Türkiye'de de bu alanın gelişimi için çeşitli önlemler alınmış, 2013 senesinde Türkiye İstatistik Kurumu (TÜİK) bünyesinde

Büyük Veri İleri Analitik Projesi başlatılmış, TÜBİTAK BİLGEM'e bağlı B3LAB (Bulut Bilişim ve Büyük Veri Araştırma Laboratuvarı) kurulmuştur. Bu kuruluşun temel aldığı projelerden birisi Avrupa Birliği projelerinden biri olan "Humane AI Net" olmuştur. Bu kapsamda, insan yeterliliklerini iyileştirebilecek ve hem vatandaşları hem de toplumu küreselleşen dünyada güçlendirebilecek güvenilir ve etik yapay zekâ sağlamak amaç olarak belirtilmektedir. 2016 senesinde ise Kişisel Verileri Koruma Kanun'u kabul edilmiş ve Kişisel Verileri Koruma Kurul'u kurulmuştur. Başta büyük veri olmak üzere, diğer tüm teknolojiler için önem teşkil eden şeylerden bir tanesi toplumdaki insanların dijital ortamları kullanım oranları ve sıklıklarıdır. Bu anlamda Türkiye, araştırılması gereken bir ülke olarak göze çarpmaktadır. Sosyal Medya Platformları kullanım oranlarını gösteren, "We are Social 2020" raporuna göre, Türkiye'nin en fazla Facebook kullanan Avrupa ülkesi olması, Instagram kullanımında dünyada 6. sırada yer alması, Twitter için dünyada 6. Avrupa'da 2. sırada yer alması, LinkedIn için 15. sırada yer alması, sadece son bir yılda 100 bin yeni kullanıcı olması ve dünya genelinde en pahalı internete sahip ülkelerden biri olması araştırmanın neden Türkiye'de çok önemli olduğunu da gözler önüne sermektedir (2020). We are Social 2022 Raporu'na göre Türkiye, dünyada kripto para satın alan ülkeler arasında ilk sıralarda yer almaktadır, Türkiye, akıllı ev aleti satın alan ülkeler arasında Birleşik Krallık, İrlanda, Kanada, ABD ve Çin'den sonra 6. sırada yer almakla birlikte sosyal medyayı en aktif kullanan ülkelere bakıldığında Brezilya, Hindistan, Endonezya, Filipinler, Malezya, Türkiye ve Çin şeklinde sıralama olduğu görülmektedir (2022). Türkiye büyük veri anlamında sürekli veri üretmeye devam eden ve bu anlamda dünya sıralamalarında da üst konumlarda yer alan ülkelerden bir tanesidir. Bu sebeple büyük veri kaynaklı yeni dijital gözetim pratikleri ve onun yol açacağı toplumsal değişimlerin incelenmesi gereken ülkelerden bir tanesidir.

Bu çalışma aynı zamanda büyük veriyi tek başına ele almaktansa Nesnelerin İnterneti, Yapay Zekâ, Robotik ve Blokzincir Teknolojisi ile işlediği düşünülen verileştirme, veri gözetimi, güvenin oyunlaştırılması, veri güdümlü yönetim, izlenebilirlik ve hesaplanabilirlik düzenleyici sistemleri ile ele alacağından daha

geniş bir bakış açısı kazandırılmasını hedeflemektedir. Büyük veri ve onu destekleyen sistemlerin nasıl ilerlediğini dijital gözetim temelinde inceleyerek bu alanda gerekli önlemlerin alınması ve düzenlemelerin yapılması için sosyal politika önerileri üretebilmek, büyük verinin teknik kısmını da gözeterek toplumsala etkisini anlayabilmek, büyük veriyi onu bilen uzmanlar ile tartışarak hem onların uzmanlık bilgilerinden faydalanmak hem de bu grupta bile olası yansımalarını görebilmek amaçlanmaktadır.

1.1.3. Araştırmanın Problem Cümleleri

Araştırmada bilgi ve iletişim teknolojilerinin, dijital medya teknolojilerinin ve gözetim sistemlerinin gelişimiyle bireyler hakkında toplanan verilerin toplumsal, kültürel, ekonomik, siyasi amaçlarla kullanıldığı ve daha farklı şekilde kullanılabileceği düşünülerek büyük verinin giderek artan etkisi değerlendirilmektedir. Gözetim sistemlerinin gelişmesi ve buradaki verilerin büyük veriye daha çok katkı sağlar hale gelmesi, Yapay Zekâ, Robotik, Blokzincir, Metaverse, Nesnelerin İnterneti gibi sistemlerle desteklenmekte ve bu veriler kavramsal çerçevede bahsedilen büyük veri entegrasyonu ile çeşitli amaçlarla kullanılabilir hale gelmektedir. Büyük verinin gözetim sistemleri ile verileştirme ve veri gözetimi sayesinde dışsal ve zorlayıcı bir olgu haline gelerek, insanların hayatlarının ve ilişkilerinin her evresinde yer alacak hale gelmesinin mahremiyetin tanımını ve sınırlarını değiştirmesi, güven ve ontolojik güvenlik kavramlarıyla ele alınmaktadır.

Çalışmada büyük veriyi destekleyen tüm sistemler de göz önünde bulundurularak, büyük verinin insan ve teknoloji ilişkisini sosyolojik olarak ne şekilde değiştirdiğine odaklanılmaktadır. Mahremiyet ve güven kavramları temel alınarak, mahremiyetin sınırlarının aşınmasının hali hazırda var olan ve muhtemel sosyolojik sonuçları düşünülmektedir. Bireylerin mahremiyetlerini ne amaçla ya da ne uğruna feda ettikleri ya da mahremiyetlerini korumak için neler yaptıkları, denetim ve gözetimin insan ilişkilerindeki rolünün ne tür bir değişime uğradığı incelenmektedir. Bireylerin verilerini kontrollü ya da kontrolsüz bir

şekilde, dönem böyle gerektirdiği için mi paylaştığı buna ek olarak bireylerin kendilerini güvende hissetmek için büyük veriye gerçekten ihtiyaç duyup duymadığı araştırılmaktadır. Bu süreçte uzman olan bireylerin bilgilerinden faydalanmak, sıradan insanların da ne tür risklerle yüz yüze oldukları konusunda farkındalık yaratmaktır. Bu değişikliklerin dijital gözetim sosyolojisi ve dijital sosyoloji teorileri temel alınarak, güvenin, sosyal güvenin, ontolojik güvenliğin tekrar sorgulanması, güvenin oyunlaştırılması anlamında ne tür bir değişime yol açtığı, sosyolojik zeminde onay kavramının nasıl dönüştüğü, güç ve öznelleştirme teknolojileri, itibar puantajı, profil çıkarma ve veri güdümlü yönetim açısından ne tür sonuçlara yol açabileceği, izlenebilirlik ve hesaplanabilirlik temelli düzenleyici sistemlerin oluşum süreci ve sonuçları düşünülmektedir.

Araştırma ile güncel bir konu olan verilerin korunması ve bireyin verileşmesi konusunun önemi de ortaya konmuş olacaktır. Çalışmanın soruları veri bilimcilerden alınan bilgiler doğrultusunda, şu şekildedir:

- Bu sistemleri tasarlayan ve dijital okuryazarlığı, dijital becerileri en yüksek olan grupta, veri bilimcisi olarak tanımlayabileceğimiz bireylerde, kişisel güven ya da ontolojik güven inşasında büyük verinin rolü nedir?
- Büyük veri ve dijital gözetim sistemlerinin güvenin oyunlaştırılmasındaki rolü nedir ve gelecekte nasıl bir hal alabilir?
- Dijital gözetim sistemlerinin ve temelde büyük verinin güven inşasındaki rolü nedir? Başkalarına güvenmek ya da güvenmemek için onları gözetlememiz gerekir mi?
- Niçin çoğu insan, çoğu zaman, üzerinde kendi teknik bilgilerinin pek az olduğu ya da hiç bulunmadığı uygulamalara ve toplumsal düzeneklere

güvenir? (Giddens'ın Modernliğin Sonuçları kitabında sorduğu temel sorulardan bir tanesi[3])

- Güven inşası aşamalarında hangi araçlar ve hangi platformlar daha çok kullanılmaktadır?
- Büyük verinin güven inşası kullanımında ve büyük veri sistemlerine dâhiliyette tanıdıklık ve yabancılık arasında ne tür farklılıklar vardır?
- Büyük veriye dahil olmak insanları daha güvende hissettirmekte midir?
- Güven ilişkisi kurmak için mahremiyetten vazgeçmek gerekli midir?
- Büyük verinin mahremiyeti aşındırması ve güven inşasında kullanılması, gerçekten kişisel olarak da itibar puantajı, profil çıkarma gibi durumlara yol açar mı?
- Büyük veri kullanılarak oluşturulan kartografiler gelecekte ne gibi sonuçlara yol açabilir?
- Büyük verinin sebep olduğu yeni dijital gözetim pratiklerinin sosyolojik olarak ortaya çıkaracağı değişimler nelerdir?

1.2. ARAŞTIRMANIN YÖNTEMİ

Bu çalışma, büyük veri ve onun mümkün hale getirdiği yeni gözetim pratikleriyle birlikte, bireylerdeki ontolojik güvenlik algısının değişimini incelemeyi amaçlamaktadır. Bu amaçla dijital toplumda ortaya çıkma ihtimali olan ontolojik güvenlik/güvensizlik algısı dijital sosyoloji ve dijital gözetim teorileri temel alınarak incelenmeye çalışılmaktadır. Yeni teknolojilere ve sistemlere vurgu yapabilmek amacıyla post-modern teoriler, dijital gözetim sosyolojisi teorileri, yeni medya sosyolojisi teorileri de bu incelemeye dahil edilmektedir. Bu değişimi incelemek için veri bilimcilerin, büyük veri ile ilgili görüşleri alınıp,

[3] Giddens'ın sorduğu bu sorunun günümüzdeki yeni gözetim pratikleriyle güncel olarak da sorulması ve tartışılması gereken bir soru olarak karşımıza çıkması, sorunun çalışmanın soruları arasında yer almasının sebebidir.

anlam dünyaları ve ontolojik güvenlik algıları anlaşılmaya çalışılmaktadır. Bu sebeple çalışmanın metodolojisi inşacı bir metodolojidir. Metodoloji, en geniş anlamda sosyoloğun sosyal bilgiyi nasıl oluşturduğu ve başkalarını bilgisinin doğru olduğuna nasıl ikna edebileceği sorularıyla ilgilenen, sosyolojik araştırmaya rehberlik eden genel ilkelerin sistematik ve mantıksal çalışmasını ifade etmektedir (Bulmer, 1977, s. 4). İnşacı yaklaşımda, yaşanan deneyimin karmaşık dünyasını onu yaşayanların bakış açısından anlama hedefi bulunmaktadır. Bu hedef genel olarak yaşam dünyalarına emik bir bakış açısından bakmak, anlamları anlamak, aktörlerin durum tanımlarına ve "Verstehen[4]"'e erişmek şeklinde açıklanmaktadır (Schwandt, 1994, s. 221). Bu çalışmada da temel hedef bu sistemleri anlayabilen ve sonuçları hakkında fikir yürütebilecek kısıtlı bir gruba üye bireylerin anlam dünyalarına ulaşabilmek ve bu şekilde bu sistemlerin ve sonuçlarının toplumda yol açtığı değişimleri önceden tespit ederek ontolojik güvenlik durumunu tartışmak ve sosyal politika önerileri geliştirebilmektir.

Ontolojik ve epistemolojik olarak bakıldığında inşacı yaklaşımda temel hedefin, farklı bakış açılarını ve durumları anlamak olduğu, genelleme ve test etme amacı olmadığı bilinmektedir. İnşacı yaklaşımla araştırılan konularda genel olarak duruma özgü konular anlam dünyaları üzerinden çalışılmaktadır. Bu çalışmada da bu sebeple inşacı metodolojiden yola çıkarak nitel araştırma yöntemi kullanılmaktadır. Nitel araştırma, sayısal temsiliyetle değil, belirli bir problemin anlaşılmasının derinleştirilmesiyle ilgilenir. Nitel araştırmalarda araştırmacı, araştırmasının hem öznesi hem de nesnesidir. Nitel araştırmanın amacı, analiz edilen problemin çeşitli boyutlarını anlamak için derinlemesine ve açıklayıcı bilgiler üretmektir (Queirós, Faria, ve Almeida, 2017).

Nitel araştırma geleneğinde (stratejisinde, yaklaşımında, deseninde) anlatı, fenomenoloji, temellendirilmiş kuram, etnografi ve vaka çalışması gibi pek çok farklı çalışma biçimi olduğu görülmektedir. Aşağıdaki tabloda gösterildiği

[4] Verstehen insan davranışını empatik olarak anlamak anlamına gelen bir sosyolojik kavram olarak kullanılmaktadır.

şekilde, her biri odağı, veri toplama, veri analizi ve söylem biçimi bakımından farklılık göstermektedir (Creswell ve Clark, 2004, s. 22).

Tablo 1. Nitel Gelenek

NİTEL GELENEK					
Boyut	**Anlatı**	**Fenomenoloji**	**Temellendirilmiş Kuram**	**Etnografi**	**Vaka Çalışması**
Odak	Bir bireyin hayatını keşfetmek	Bir olguyla ilgili deneyimin özünü anlamak	Alandaki verilere dayalı bir teori geliştirmek	Kültürel ya da sosyal bir grubu tanımlamak ya da yorumlamak	Tek ya da birden çok vakanın derinlemesine analizini geliştirmek
Veri Toplama	Birincil görüşmeler ve belgeler	10 kişiye kadar uzun mülakatlar	Kategorileri doyurmak ve bir teoriyi detaylandırmak için 20-30 kişiyle mülakatlar	Öncelikle sahada uzun süre boyunca (örneğin 6 aydan bir yıla kadar) gözlemler ve görüşmeler	Belgeler, arşiv kayıtları, mülakatlar, gözlemler gibi birçok kaynak Fiziksel eserler
Veri Analizi	Hikayeler Epifani Tarihsel içerik	Beyanlar Anlamlar Anlam temaları Deneyimin genel tanımı	Açık kodlama Eksenel kodlama Seçici kodlama Koşullu matris	Tanımlama Analiz Yorumlama	Tanım Tema İddialar
Anlatı Biçimi	Bireyin hayatının ayrıntılı sunumu	Deneyimin özünün tanımı	Teori ya da teorik model	Grubun ya da bireyin kültürel davranışının tanımı	Bir vaka ya da vakaların derinlemesine analizi

(Creswell ve Clark, 2004, s. 22)

Bu çalışma veri bilimcilerinin deneyimlerinden yola çıkarak, onların büyük veri ve yeni gözetim pratikleriyle ilgili deneyimlerine ulaşmayı hedeflediğinden odak anlamında fenomenoloji ile benzerlik göstermektedir. Bir olguyla ilgili deneyimin özünü anlamak, veri bilimcilerin büyük veri ve onun getirmiş olduğu yeni

gözetim pratikleri ile ilgili deneyimlerine erişmek çalışmanın temel hedefidir. Araştırma stratejileri bazı anlamlarda benzerlik gösterse de bu çalışmada temel olarak temellendirilmiş kuram temel alınmaktadır. Veri toplama anlamında 10 kişi yerine, 16 kişiyle mülakatlar yapılarak temellendirilmiş kuramın odağına aldığı alandaki verilere dayalı bir teori geliştirebilme hedefi vardır. Burada da amaç kategorileri doyurmak ve teoriyi detaylandırmaktır. Açık, eksenel, seçici kodlama ve koşullu matris gibi yollarla analiz gerçekleştirilmekte ve teori ya da teorik modelin önü açılmaktadır. Veri analizi, daha detaylı olarak veri değerlendirme kısmında açıklanmaktadır.

Araştırma yöntemi, nitel yöntem ve veri toplama tekniği ise derinlemesine mülakattır. Veri toplama aracı başlığı altında derinlemesine mülakat ve uzman mülakatlarına dair daha detaylı bilgi sunulmakta olup buradaki önemli nokta nitel yöntemle gerçekleştirilen derinlemesine mülakatların arkasında yer alan metodolojiyi kavrayabilmektir. Nitel mülakat en yaygın olarak yorumlayıcı metodolojiye dayamaktadır. Yorumlayıcı metodoloji başlangıçta sembolik etkileşimci teoriden çıkmıştır. Günümüzde sosyal inşacılık, feminist kuram, çatışma kuramı, eleştirel kuram ve söylem analizi gibi pek çok kuramsal perspektiften çalışan araştırmacılar, çalışmalarında içgörüleri kullanmaktadır. Bu araştırmacılar nadiren teorilerini test etmeye çalışmaktadır çünkü yorumlayıcı metodoloji hipotezleri test etmeye değil, farklı bakış açılarını ve dünya görüşlerini anlamaya dayalıdır. Bu nedenle, araştırmacılar verilerini seçerken ve yorumlarken kendilerine rehberlik etmesi için belirli bir teoriyi kullanmaktadır (Gordon, 2019, s. 29). Bu çalışmada da tam bu anlamda yorumlayıcı metodoloji ya da inşacılık bakış açısıyla temellenen bir ontolojik ve epistemolojik temel ele alınarak araştırmanın gerçekleştirilmesi önem taşımaktadır.

1.2.1. Araştırmanın Veri Toplama Aracı

Bu araştırma nitel araştırma yöntemiyle gerçekleştirilmektedir ve temel veri toplama aracı derinlemesine mülakatlar ve bir anlamda uzman görüşü

mülakatlarıdır. İki farklı teknik olarak görülse de araştırma konusunun sadece uzmanlar tarafından tartışılabilecek ve çözüm üretebilecek doğasından ötürü bu tür bir yol izlenmiştir. 16 kişiyle gerçekleştirilen mülakatlar esnasında katılımcılar hem birer uzman hem de bu durumu deneyimleyen sıradan katılımcılar olarak ele alınacağından bu iki teknikten de bahsetmenin ve kullanmanın önemli olduğu düşünülmektedir. Derinlemesine mülakatlar, bir araştırmacının başka bir kişinin bir konu hakkında ne bildiğini öğrenmeye, o kişinin neler yaşadığını, o konu hakkında ne düşündüğünü ve hissettiğini ve bunun ne gibi bir önemi veya anlamı olabileceğini keşfetmeye ve kaydetmeye çalıştığı amaçlı etkileşimlerdir (Mears, 2012, s. 170). Katılımcılar başlığı altında detaylı bir şekilde bahsedilen, amaçlı örneklemle kriterleri net olarak belirlenen ve buna göre mülakat yapılan veri bilimcilerle büyük veri ve yeni gözetim sistemleri doğrultusunda ontolojik güvenlik algılarını anlamak için derinlemesine mülakatlar gerçekleştirilmiştir.

Derinlemesine mülakatın en temel unsurlarından bir tanesi bir yandan planlanmış ve yapılanmış bir çalışma olsa da bir yandan esneklik de taşımasıdır. En yapılanmamış mülakatlarda bile araştırmacının kontrolü doğrultusunda araştırmanın keşfetmek istediği verilere doğru yönlenebilme ve konuyu bu doğrultuda tutma imkânı vardır. İkinci ana unsur derinlemesine mülakatların etkileşime dayanmasıdır, araştırmacı soruları sorarak katılımcıyı konuşmaya cesaretlendirmeli ve onu güvende hissettirmelidir. Üçüncü olarak ise araştırmacı konuya nüfuz etme, keşfetme ve açıklama açısından cevapların derinliğini elde etmek için bir dizi araştırmayı ve diğer teknikleri kullanmaktadır. Araştırmacı, katılımcının anlam dünyasını daha derin ve daha eksiksiz bir şekilde anlamak için takip soruları kullanmaktadır (Legard, Keegan ve Ward, 2003). Araştırmacının, katılımcının gerçek görüşlerine ulaşabilmek için kullandığı tekniklerden bazıları çelişkilendirme (kasıtlı olarak katılımcının görüşüne zıt bir fikir verme ve onun daha fazla yorum yapmasını sağlamaya çalışmak), ilişkilendirme (araştırmacının bilmek istediği bilgi ile katılımcının yorumunu ilişkilendirmeye çalışmak), şaşırma (araştırmacının kafası karışmış gibi davranarak detaylandırmaya ihtiyaç duyduğunu göstermesi), iddialaşma (katılımcının önceki iddialarının geçerliliğini kanıtlaması için daha fazla bilgi

talep etmek), teşvik etme (katılımcıları devam etmeye teşvik etmek için övmek ya da iltifat etmek), anlayış gösterme-detaylandırma için zaman tanıma (katılımcılara yorumlarının anlaşıldığını ve değer verildiğinin bilmesini sağlamak ve daha fazla yorum yapması için ona zaman tanımak), kabul etme (dikkati göstermek için katılımcının cevabını tekrarlamak), doğrudan sorma ya da detaylara inme (daha fazla bilgi almak için doğrudan soru sormak) şeklinde olabilmektedir (Berry, 1999).

Uzman görüşü mülakatları, literatüre bakıldığında, keşfedici uzman mülakatları, sistematize edici uzman mülakatları ve teori oluşturucu uzman mülakatları olarak üç kategoride değerlendirilmektedir. Keşif amaçlı mülakatın konusu itibariyle odak noktası, araştırılan konuyu derinlemesine incelemektir. Amaç, verileri karşılaştırmak, mümkün olduğu kadar çok bilgi edinmek veya verileri standart hale getirmek değildir (Bogner ve Menz, 2009, s. 46). İlk ikisinin ortak özelliği teknik ve işlemsel bilgiye dayanmalarıdır. Teknik bilgi o konudaki teknik bilgiyi ifade ederken, ikincisi tecrübeye dayanan bilgiyi ifade etmektedir. Sistematik uzman mülakatlarında ise uzman, araştırmacıyı “nesnel” konularda aydınlatır. Bu, uzmanın öncelikle belirli geçerli bilgi ve enformasyon parçalarına sahip bir rehber, araştırmacının erişemeyeceği özel bir uzmanlık bilgisine sahip biri olarak ele alındığı anlamına gelmektedir (Bogner ve Menz, 2009, s. 47). Teori oluşturucu uzman mülakatları ise yalnızca uzmanın açık uzman bilgisini değil, aynı zamanda (profesyonel) uygulama yoluyla elde ettiği zımni spesifik yorumlayıcı bilgisini (know-why) ve prosedürel bilgisini (know-how) hedef almaktadır (Littig, 2009, s. 101). Daha sonra ise özellikle teori üretmeyi temel alan uzman mülakatlarını başlangıç noktası kabul ederek, problem temelli uzman mülakatları ortaya çıkmıştır. Her ikisi de görüşülen kişinin bakış açısını ve fikirlerini vurgulamakta, bireysel ifadeleri sistematik hale getirerek ve yorumlayarak yeni teoriler formüle etmeyi amaçlamaktadır (Döringer, 2021, s. 269).

Tablo 2. Problem-merkezli uzman mülakatlarının özellikleri	
Teori oluşturucu uzman mülakatları	**Problem-merkezli uzman mülakatları (PCI)**
Uzmanı tanımlar ve tartışır	Bireysel bakış açısını vurgular
Farklı uzmanlık bilgisi türlerini ayırt eder	Belirli bir görüşme tasarımı ve soru seti sağlar
Tümevarım teorisi geliştirmeyi amaçlar	Toplanan verilerin karşılaştırılabilirliğini sağlar
	Tümevarım-tümdengelim teorisi oluşturmayı önerir

(Döringer, 2021, s.269)

Bu çalışmada temel amaç, uzmanların sahip olduğu teknik ve işlemsel bilgilerinden ötürü onların ontolojik güvenlik durumlarına bakabilmek ve yeni dijital gözetim pratiklerindeki değişimler konusunda farkındalıklarını anlamak olduğu için teori oluşturucu uzman mülakatları temel alınmıştır. Amaç sadece uzmanların sahip olduğu bir bilgiye erişmek; uzmanın araştırmacıyı belirli bir konuda aydınlatması değildir. Bu sebeple keşfedici ve sistematik olarak nitelendirilen uzman mülakat tipleri bu araştırma için uygun değildir. Tabloda görüldüğü şekilde kuram oluşturucu uzman mülakatlarındaki gibi, uzmanın kim olduğuna dair bir tanım yapılmış ve bu tanım detaylı bir şekilde tartışılmıştır. Aynı zamanda temellendirilmiş kuramda açıklandığı şekilde, tümevarım yoluyla bir teori geliştirmeye yönelik bir amaç olduğu belirtilmektedir. Problem temelli uzman mülakatlarında olduğu gibi, bireysel bakışa önem verilmiş, belirli bir mülakat tasarımı ve yarı-yapılandırılmış mülakat formu ile belirli sorular hazırlanmıştır. Uzman görüşü mülakatının tercih edilme sebebi, çalışmanın pek çok yerinde açıklanmaktadır. Bunun yanı sıra, uzman mülakatları yapmak, özellikle uzmanlar pratik içeriden bilgi için "kristalizasyon noktaları" olarak görülüyorsa ve daha geniş bir oyuncu çevresi için vekiller olarak görüşülüyorsa, zaman alan veri toplama süreçlerini kısaltmaya da hizmet edebilmektedir (Bogner, Littig ve Menz, 2009, s. 2).

1.2.2. Araştırmanın Veri Toplama Süreci

Nicel, nitel ya da karma yöntemle yapılan araştırmaların hepsinde araştırmacının öncelikle araştıracağı konuya dair çok derin bir bilgiye sahip olması, araştırmasıyla ilgili bilgiye erişmek için kendisinin hangi gruba ulaşması gerektiğini bilmesi ve araştırma konusu ve örneklemine uygun olan yönteme karar vermesi gerekmektedir. Bu çalışmada da sosyoloji alanından gelen bir araştırmacının büyük veriyle ilgili gözetim kuramlarını, dijital sosyoloji kitaplarını, büyük veriye ilham veren geçmiş distopyaları (Orwell ve Huxley'in kitaplarındaki gibi) okuması veri toplama sürecine hazırlık aşamasının ilk aşaması olmuştur. Bunun yanı sıra, bireysel görüşme formunu hazırlayabilmek için veri bilimine giriş eğitimlerine, yapay zekâ zirvesine, dijitalleşmeyle ilgili kongrelere katılmak, büyük verinin geleceğine dair kitapları, filmleri, araştırmaları, blogları takip etmek de bunun bir parçası olmuştur. Ek olarak, araştırmanın kavramsal ve kuramsal çerçevesini yazabilmek için yapılan sistematik literatür taramasından sonra araştırmanın yöntemi, tekniği ve örneklemi belirlenmiştir.

Nitel araştırma yöntemi, derinlemesine mülakat ve uzman mülakatları teknikleri belirlenip, veri bilimciler örneklem olarak seçildikten sonra bireysel mülakat formu hazırlanmıştır. Bireysel görüşme formunun yarı-yapılandırılmış olarak hazırlanması özellikle konuya hâkim kişilerle konuşurken, konudan sapmadan ve odaklanılması gereken noktalara odaklanarak devam etmek için tercih edilmiştir. Sorular açık uçlu olarak tasarlanmıştır. Aynı zamanda mülakatların yüz yüze mi ya da çevrimiçi şekilde mi gerçekleştirileceği düşünülmüş, mülakat yapılan grubun tercihleri de öngörülerek çevrimiçi olmasına karar verilmiştir. Yüz yüze mülakatı talep eden ya da kabul eden katılımcılarla da yüz yüze mülakatlar yapılmıştır.

Bireysel görüşme formunun 6 ana başlık altında olması, özellikle veri değerlendirme sürecinde araştırmacıya kolaylık sağlanması ve elde edilmeye çalışılan verileri araştırmanın en başından belirli bir çerçeve doğrultusunda düzenlenmesi sebebiyle tercih edilmiştir. Bireysel görüşme formunda yer alan

bu 6 başlığa bakıldığında; ilk olarak katılımcılarla ve katılımcıların konuyla ilişkilendirilebilecek olan genel bilgilerine dair Katılımcı Bilgileri bölümü yer almaktadır. İkinci olarak "Katılımcı ve Büyük Veri İlişkisi" başlığı altında temel olarak katılımcının büyük veriyle olan bağlantısı, temel görüşleri ve büyük veriye yaklaşımına dair sorular yer almaktadır. Üçüncü kısımda, "Veri Gözetimi" başlığıyla katılımcının büyük verinin gözetim yönüne nasıl yaklaştığı ve bunun bir tür yeni gözetim pratiği olarak değerlendirilip değerlendirmediğine yönelik sorular yer almaktadır. Dördüncü kısımda, "Sosyal İlişki Kurmada Büyük Veri-Bireyin Verileşmesi" başlığı altında bu alanda bilgili olan katılımcıların kendi sosyal ilişkilerine büyük veriyi nasıl ve ne şekillerde dahil ettiği ya da etmediğine dair sorular yer almaktadır. Beşinci kısımda, "Toplumsal Güven ve Sorumluluklarda Büyük Veri" başlığı altında büyük veri ve toplumsal güven, büyük verinin toplumsal sorumluluklara olan yansımaları temelinde katılımcıların düşüncelerini almayı hedefleyen sorular yer almaktadır. Son kısımda ise "Büyük Verinin Karanlık Yönü-Yıkıcı Teknoloji Tarafı" başlığında ise katılımcıların büyük verinin yol açtığı ya da açabileceği sorunlara dair bir tür distopya üretmeleri beklenmekte, konuya tamamen olumlu bakış açısıyla yaklaşan katılımcılardan ise bir tür ütopya/distopya kurmaları temelde her katılımcının büyük verinin geleceğine dair bir öneri hayal etmesi ve bunu ifade etmesi beklenmektedir. Bu şekilde katılımcıların -uzmanların- bu sistemler için geliştirilmesi gereken hukuki, ekonomik, sosyal, kültürel ve teknik her tür önerisine ulaşılmaya çalışılırken, bu grup içerisindeki ontolojik güvenlik algısının nasıl olduğu anlaşılmaya çalışılmaktadır.

Araştırmanın tamamen etik bir çerçeve ile gerçekleştirilmesi amacıyla Bireysel Görüşme Formu'nun (EK-3'te yer almaktadır) hazırlanmasından sonra, Gönüllü Katılım Formu eklenmiştir. Gönüllü Katılım Formu'nda araştırmanın kim tarafından yürütüldüğü, araştırmanın amacının ne olduğu ve bu araştırma sonucunda ne hedeflendiği, mülakatların ne kadar süreceği, araştırmacıların rahatsız olacakları sorulara cevap vermeme hakkı olduğu, araştırmanın tamamen gönüllülük esasına dayandığı, kişisel verilerin özenle korunacağı net

bir şekilde belirtilmiştir. Katılımcıların araştırmacıya istediği zaman ulaşabilmesi için iletişim bilgileri de gönüllü katılım formuna eklenmiştir.

Hacettepe Üniversitesi Etik Komisyonu'na Bireysel Görüşme Formu ve Gönüllü Katılım Formu sunularak, çalışmanın Etik Kurul raporu alması için başvurulmuş, 7 Mart 2023 tarihinde yapılan toplantıda incelenen çalışma etik açıdan uygun bulunmuş ve 21 Mart 2023 tarihli Etik Komisyon izni (Ek-2'de yer almaktadır) alınmıştır. Etik Komisyon izni alındıktan sonra 1 Nisan 2023 tarihinde 1 kişiyle pilot çalışma gerçekleştirilmiş, araştırmaya dahil edilmek istenen tüm konuların dahil edilip edilmediği, katılımcıların sorulara dair yanlış anlayabileceği ya da anlam veremeyeceği kavramlar olup olmadığı (sosyolojik terimler gibi), soruların işleyişinde bir sorun olup olmadığına dair değerlendirme yapılmış ve gerekli düzeltmeler yapılarak mülakatların yapılabilmesi için uygun koşullar sağlanmıştır. Mülakatlara 1 Mayıs 2023 tarihinde başlanmış olup 31 Temmuz 2023 itibariyle mülakatlar sonlandırılmıştır. 16 veri bilimci ile görüşülmüş, mülakatlar yapılırken katılımcıların özellikle büyük firmaların, kurumların ya da üniversitelerin ilgili birimlerinde çalışan bireyler olmasına özen gösterilmiş, bu bireylere ulaşabilmek için çaba harcanmıştır.

Katılımcılar, amaçlı örneklem çerçevesinde kartopu katılımcı tekniği ile belirlenmiş, ulaşılan uzman veri bilimcilerin kendi çevrelerinde başarılı olarak gördükleri veri bilimcileri önermesi ile mülakatlara devam edilmiştir. Bu sayede alanında uzman kişilere ulaşmak daha kolay bir hale gelmiştir. Katılımcılara ulaşılırken bireylerin anonim kalmasını sağlamak amacıyla doğrudan şirket ya da kurum isimleri verilemese de dijital gözetim konusuyla yakından ilgili kurumlarda yöneticilik yapan, projeler yürüten ya da bu projelerde uzman olarak yer alan bireylerle mülakatlar yapılmıştır.

Araştırmaya başlamadan önce tüm katılımcılara Etik Komisyon izni gösterilmiştir. Mülakattan önce kısa bir bilgilendirme yapılarak, katılımcıların mülakatlara içleri rahat bir şekilde katılabilmesi için gerekli ortamın sağlanması için de gerekli önlemler alınmıştır. Katılımcıların tercihlerine ve müsaitlik

durumlarına göre bazı mülakatlar yüz yüze, bazıları ise çevrimiçi olarak gerçekleştirilmiştir. Bunun temel sebeplerinden bir tanesi katılımcıların Ankara dışındaki illerden olması ve hatta yurtdışında bu alanda çalışan bireyleri de kapsamasıdır. Katılımcıların bir kısmıyla çevrimiçi mülakatlar gerçekleştirilmiş olup hem tercih hem de uygunluk durumlarına göre WhatsApp görüntülü konuşma, Zoom ve Microsoft Teams uygulamaları kullanılarak mülakatlar gerçekleştirilmiştir. Yüz yüze olan mülakatlarda ise yine katılımcıların uygunluk ve tercihlerine göre üniversite kampüsü, kafe ya da şirket gibi ortamlarda mülakatlar gerçekleştirilmiştir. Araştırmadan önce katılımcıların her birine ses kaydının alınmasına dair izin verip vermedikleri sorulmuş, sadece izin veren katılımcıların ses kayıtları alınmıştır.

1.2.3. Araştırmanın Veri Değerlendirme Süreci

Nitel araştırma yöntemi ve mülakatlar yoluyla veri toplanan bu çalışmada, araştırmanın değerlendirme kısmında da temellendirilmiş kuramın önerdiği (açık kodlama, eksenel kodlama, seçici kodlama ve koşullu matris) veri analizi dikkate alınmaktadır. Deterding ve Waters'ın güncel olarak kabul edebileceğimiz çok önemli sayılabilecek bir çalışmasında, temellendirilmiş kuramın 1960'ların teknolojisine ve o dönemin koşullarındaki kodlama pratiklerine dayandığı ve günümüzde özellikle çok sayıda mülakatları bir ekip şeklinde çalışan araştırmalar olduğu ve bu noktalarda nitel veri analizi yazılımlarını kullanarak daha kolay ve zamandan kazanacak şekilde araştırma yapılabileceği, temellendirilmiş kuramın özellikle tekrar analiz ya da mülakat verilerinin ikincil analizine çok fazla imkan sağlamadığı üzerine eleştiriler göze çarpmaktadır (Deterding ve Waters, 2021). Fakat bu çalışmada aynı zamanda temellendirilmiş kuramın hala birçok çalışmanın temelini oluşturduğu ve nitel veri analizinde özellikle az sayıdaki mülakatın analizinde birçok çalışmaya ışık tuttuğu görüşü de benimsenmektedir. Araştırmacıların bir kısmı, temellendirilmiş kuramın pek çok yönüyle etkili bir veri değerlendirme yaklaşımı olduğunu belirtmektedir. Drisko, "Çeşitli nitel araştırma biçimlerine uygulanabilen, iyi hazırlanmış veri analizi yöntemleri vardır. Belki de en tanıdık olanı, çok aşamalı

kodlama prosedürleri ve teori geliştirme aşamaları ile temellendirilmiş kuramdır" demektedir (1997, s. 190). Temellendirilmiş kuramın sağladığı önemli özelliklerden bir tanesi araştırma verilerinin değerlendirme sürecinde net bir şekilde açıklanan kodlama aşamalarıdır. Veri analizini yürütürken her yaklaşım[5] için araştırmacıların verilerden temaları ve ilişkileri kodlayabilmesi, sıralayabilmesi ve tanımlayabilmesi gerekmektedir (Tomaszewski, Zaretsky ve Gonzalez, 2020, s. 4).

Karma bir nitel veri analizi denildiğinde genel olarak akla öncelikle tümevarım, mülakatlardan elde edilen deşifre metninden gereksiz tüm öğelerin ayrılarak temel bir metne ulaşma akla gelmektedir. Bu aşama genel olarak tümevarım başlığı altında veri azaltma süreci olarak isimlendirilmektedir. Derinlemesine mülakatlar en başta yazı haline getirilerek, katılımcıların ağzından çıkan her şeyi, gerekirse katılımcıların mimiklerini ve tepkilerini de yazılı metne dönüştürerek ve dahil ederek daha sonra blok alıntı imkânı sağlayarak araştırmanın geçerliliğini artırmaktadır. Veriler belirli başlıklar altında toplanmakta, kavramsallaştırılmakta ve kodlama yapılmaktadır. Bunun analiz ve bağlantı kurmanın ilk aşaması olduğu bilinmektedir.

Deterding ve Waters'ın önerdiği analiz sürecine bakıldığında, öncelikle verilerdeki büyük resmi gördükten sonra verinin keşfi ve hazırlanması gelmektedir. Daha sonra transkriptlerdeki kavramlar arasındaki ilişkiler geliştirilerek analitik süreç incelenmektedir. İkinci aşamada araştırmacı deşifreyi veri indirgeme için kullanarak, deşifrenin odaklanılmış bölümlerine analitik kodlar uygulamakta ve kodlamanın güvenilirliği ve geçerliliğine öncelik vermektedir. Analitik kodlar sayesinde literatürden bilinenlerle bulguların bütünleşmesi hedeflenmektedir (Deterding and Waters, 2021, s. 722). Bu çalışmada da tüm bu süreçlere dikkat edilerek analiz gerçekleştirilmiş, literatürden elde edilen veriler de özellikle temellendirilmiş kuramın öngördüğü

[5] Bu çalışmada vaka çalışması, fenomenoloji, öyküsel sorgulama ve etnografiden bahsedilse de yukarıdaki bölümlerde bahsedilen nitel gelenek çatısı altında anlatı, fenomenoloji, temellendirilmiş kuram, etnografi ve vaka çalışmasının yer aldığı gösterilmektedir. Her yaklaşım derken bu tez için ismi geçen tüm yaklaşımlardan bahsedilmektedir.

şekilde doğrulama amacıyla değil, diğer veriler gibi davranılarak karşılaştırma sürecine sokulmuştur.

Temellendirilmiş kuramda analiz ve bağlantı kurma işlemini yapabilmek için genellikle açık, eksenel, seçici kodlama ile koşullu matristen bahsedilirken; bazı çalışmalarda bu kodlamaların iki başlık altında ele alındığı görülmektedir. Bunlar klasik temellendirilmiş kuramda, açık ve seçici kodlama prosedürlerini içeren bağımsız kodlama ve teorik kodlamadır. Temel kodlamada araştırmacı, başlangıçta temel bir kategorinin ortaya çıkması için açık kodlama yoluyla verileri parçalayarak ve analiz ederek doğrudan verilerle çalışmaktadır ve ilgili kavramlar ve daha sonra teorik örnekleme ve verilerin seçici kodlanması yoluyla temel ve ilgili kavramların teorik olarak doyurulması sağlanmaktadır. Teorik doygunluk, her bir kategorinin (kod) özelliklerini ve boyutlarını ortaya çıkarmak için verilerdeki olayların (göstergelerin) sürekli karşılaştırılması yoluyla elde edilmektedir (Holton, 2007, s. 21). Bu bilginin önem arz ettiği düşünüldüğü için paylaşılmakta olup, genel olarak kullanılan dört kodlama prosedürü bu araştırma için uygun görülmüştür.

Bu çalışmada da temel alındığı ve temellendirilmiş kuramda da bu doğrultuda açıklandığı şekilde, ilk olarak süreçleri tanımlama hedefiyle ve tümevarımcı bir yaklaşımla elde edilen verilerden kuram üretme hedefi yer almaktadır. Veri azaltma süreci olarak bahsedilen süreçte ilk aşamada açık kodlama ile tüm deşifre metninin analize tabii tutulmasından bahsedilmektedir. Farklı araştırmacıların temellendirilmiş kurama farklı katkıları olduğu belirtilmektedir ama her birinde özellikle veri azaltma sürecine vurgu yapıldığı görülmektedir. Deterding ve Waters, temellendirilmiş kuramın gelişiminden bahsederken Glaser ve Strauss, sonra Strauss ve Corbin daha sonra ise Charmez'in katkılarından bahsetmekte ve kodlamanın nasıl şekillendiğini aktarmaktadır. Buna göre, her üç modelde de kodlama, verilerin küçük bölümlerini tanımlayarak başlanmaktadır: satırlar, cümleler ve hatta paragraflar veya kelimeler. Temellendirilmiş kuramdan türetilen yaklaşımların her birinde, araştırmacılara tavsiye açıktır: "Yalnızca verileri yansıtan birçok kod üreterek

başlayın. Daha sonra, bazılarını silerek ve diğerlerini birleştirerek kod listesini ayıklayın" (2021, s. 712). Bu sayede ise, Strauss ve Corbin, açık kodlamada her mülakatın kodlandığı ve bu süreçte kavramların, hipotezlerin ve araştırma sorularının oluştuğunu belirtmektedir (1997, s. 133). Araştırmada da katılımcılarla gerçekleştirilen mülakatların deşifreleri ile elde edilen yoğun bir veri seti içerisinden öncelikle veri azaltma işlemi yapılmış açık kodlama uygulanmıştır.

Açık kodlama sürecinde geliştirilen kavram ve kategoriler arasındaki ilişkilerin araştırılması için eksenel kodlamaya ihtiyaç duyulduğu belirtilmektedir (Vollstedt ve Rezat, 2019, s. 87). Açık kodlama ile belirli ortaklık ya da farklılıklar bir anlamda "eksenler" tespit edilerek, ikinci aşamada eksenel kodlama yapılmaktadır. Eksenlerin bir araya getirilerek daha büyük kategoriler ve temalara ulaşabilmeyi sağlayan, merkezi kategorilerin oluştuğu aşama ise seçici kodlama olarak tanımlanmaktadır. Seçici kodlamanın amacı, eksenel kodlama sırasında geliştirilen, detaylandırılan ve karşılıklı olarak ilişkilendirilen farklı kategorileri tek bir tutarlı teoride birleştirmektir. Bu hedefe ulaşmak için eksenel kodlamanın sonuçları daha da detaylandırılmakta, entegre edilmekte ve doğrulanmaktadır. Dolayısıyla seçici kodlama, eksenel kodlamaya oldukça benzer ancak daha soyut bir düzeyde gerçekleştirilmektedir (age, s. 89). Araştırmada da diyagramlarla da bağlantılandırılmaya çalışıldığı şekilde, birçok alt kategori, kategori ve temaya ulaşılmış; bunların her biri açık bir biçimde şemalaştırılmıştır.

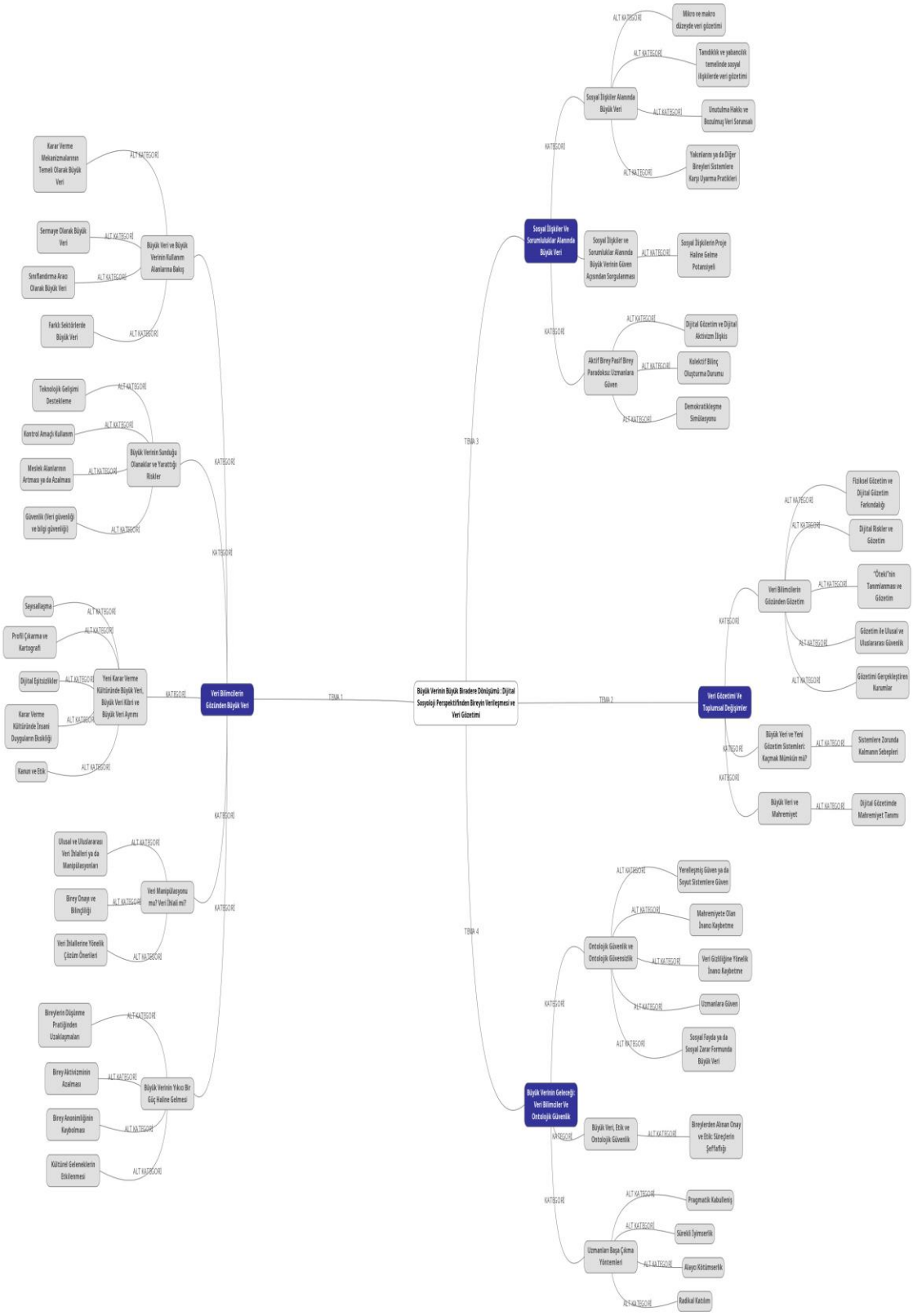
Koşullu matris ile ise (özellikle bu tez özelinde) teknolojik, sosyal, ekonomik, siyasi, kültürel ve tarihi süreçlerin çalışılan konuyu nasıl etkilediği incelenmektedir. Bu analitik sürecin incelenebilmesi için özellikle araştırmacının süreçle ilgili tuttuğu her tür notun (memoların) ve soyutlama yapabilmek için kullanabileceği diyagramların da önemli olduğu bilinmektedir. Bu hedefle bahsedilen kodlamalar araştırma sürecinde yapılmış olup, araştırmacının araştırma sürecinde kayıt altına almış olduğu memolar da dahil edilerek araştırmadaki alt kategorilere, kategorilere ve temalara ulaşılmış, ulaşılan

başlıklar diyagram haline getirilmiştir. Bu amaçla Şekil 1'de araştırmanın modeli gösterilmektedir. Aynı zamanda araştırmanın bulguları kısmında her tema için de diyagramlar yer almaktadır.

Nitel araştırmalarda, nicel araştırmalardaki gibi test etme ve genelleme amacı olmadığından en önemli kriter araştırmanın güvenilirliğidir. Üç tür güvenilirlik mevcuttur. Öncelikle kararlılık, kod kullanımının zaman içinde değişip değişmediği önem taşımaktadır. İkinci olarak standart bir kodlama şemasının olup olmadığı ve diğer kodlama şemalarının da geliştirilip geliştirilmediği ve bunlar arasında karşılaştırma yapılıp yapılmadığıdır. Üçüncüsü ise farklı kodlayıcıların aynı verileri aynı şekilde kodlayıp kodlamayacağıdır ve kodlayıcılar arasında yeniden üretilebilirlik ya da kodlayıcılar arası güvenilirlik olarak adlandırılmaktadır (Campbell, Quincy, Osserman ve Pedersen, 2013). Bu çalışmada da araştırmanın güvenilirliğini sağlamak açısından bu üç kritere de dikkat edilmiş ve hepsi sağlanmaya çalışılmıştır.

Araştırmanın veri değerlendirme sürecinde ortaya çıkan dört temel tema, temaların içerisinde yer alan kategoriler ve alt kategoriler araştırmanın modelini oluşturmaktadır. Şekil 1'de araştırmanın modeli detaylı bir şekilde yer almaktadır. Araştırmanın bulguları kısmında ise her tema ve temanın kategorileri ile alt kategorilerini gösteren şemalar temaların altında gösterilmektedir.

Şekil 1. Araştırmanın Modeli



1.2.4. Araştırmanın Katılımcıları

Dijital gözetim sosyolojisi ve dijital sosyoloji anlamında günümüzde nitelik olarak gittikçe değer gören dijital becerilere sahip olan ve yeni bir sermaye olarak görülen büyük verinin toplanması, depolanması ve işlenmesinde bilgi sahibi olan meslek gruplarından bir tanesi, veri bilimciler, bu çalışmanın katılımcılarını oluşturmaktadır. Nitel araştırmalarda örneklem belirlenirken birçok farklı katılımcı seçme tekniği kullanılmaktadır. Bu tekniklere bakıldığında amaçlı örneklem, aday, ağ ya da kartopu örneklem, gönüllü örneklem ya da tüm popülasyonu kapsayan örneklem gibi teknikler göze çarpmaktadır. Nitel yöntemle tasarlanan bu çalışmada, katılımcılar amaçlı örneklem ile belirlenmiştir. Bu, ilgilenilen bir fenomen hakkında özellikle bilgi sahibi olan veya bu konuda deneyim sahibi olan bireyleri veya birey gruplarını tanımlamayı ve seçmeyi içermektedir (Cresswell and Plano Clark 2011 akt. Palinkas, Horwitz, Green vd., 2015, s. 534). Amaçlı örneklem tekniğinde yaş, ekonomik durum veya eğitim düzeyi gibi tipik veya temsili nüfus özelliklerine dayalı kriterlere sahip bir örneklem seçmek yerine, örneklem, bilgi verenlerin araştırma konusu hakkındaki bilgilerine göre seçilmektedir (Morse, 1991, s. 131). Bu çalışmada ise temel unsur meslektir. Bunun sebebi araştırılan sistemin dışında kalan bireylerin bu konu hakkında fikir yürütmesinin zor olması; veri bilimcilerden hem uzman mülakatları yoluyla araştırma konusu hakkında detaylı bilgi almak, hem konunun uzmanı olarak onların bile ontolojik güvensizlik konusundaki kaygılarını öğrenmek hem de sosyal politika üretebilmek adına çözüm önerileri üretebilmektir. Amaçlı örneklem tekniğinde bir tür bilgiye sahip olan katılımcılara ulaşılırken; bir diğer örneklem seçme tekniği olan aday, ağ ya da kartopu örneklem tekniği olarak tanımlanan bir diğer örnekleme tekniğinin de bu çalışma açısından uygun olduğu görülmüştür. Bu örneklem tekniğinde, araştırmaya dahil edilen bir katılımcının destek ve yardımıyla diğer katılımcıların katılımı desteklenmektedir. Bu şekilde özellikle araştırmaya, araştırılan konuda bilgi sahibi olan kişilerin dahil edilmesi konusunda avantaj sağlanmakta, araştırmanın başlangıç kısmında kolaylık sağlanmakta (diğer katılımcı da araştırma konusunda katılıma destek sağladığı için), araştırmacı ve katılımcı

arasındaki güvenin daha kolay sağlanması gibi avantajlar sunmaktadır (Morse, 1991, s. 131). Bu anlamda çalışmada özellikle nitel araştırma yönteminde kullanılan örneklem tekniklerinden amaçlı örneklemin, katılımcıların taşıdıkları uzmanlık bilgisi kriterine uygun olarak seçilmesi doğrultusunda, ağ ya da kartopu örneklemin ise diğer katılımcılara ulaşma ve söz konusu edilen diğer avantajlarından faydalanmak amacıyla tercih edildiği belirtilebilir.

Bu çalışmada veri bilimcisi olarak ele alınan grubun literatüre bakıldığında, özellikle bu veri ile baş edebilme bakımından çeşitli farklı meslek gruplarınca birlikte icra edildiği görülmektedir. Veri bilimcisi[6], veri analisti, veri mühendisi ve veri sorumlusu bu temel unvanlardandır. Detaylı bir ayrıma gidildiğinde, veri bilimcisinin daha çok veride genel tekrar eden kalıpları bulmaya çalışan ve gelecek hakkında tahminler üretme sorumluluğu olan kişiler olduğu ve Java, Python, SQL, R, SAS gibi programları kullanabilme niteliğinin yanısıra büyük veri işleme alanında Hadoop, Spark ve Pig gibi çerçeveleri bilmesinin beklendiği, büyük veriyi destekleyen derin öğrenme ve makine öğrenmesi gibi alanlarda da bilgi sahibi olması gerektiği belirtilmektedir. Veri analisti ise daha çok sayısal veriyi kurumdaki herkesin anlayabileceği dile çeviren kişiler için kullanılmaktadır. Veri analistlerinden de SAS Miner, Excel, SPSS ve SSSAS gibi programları bilmelerinin yanı sıra, Python, SQL, R, SAS ve Javascript gibi programları da temel olarak bilmeleri beklenmektedir. Veri mühendisi olarak tanımlanan bireyler, bireylerin davranışlarından üretilen verilerin veri tabanına nasıl geldiği konusundan sorumludur. Veri sorumlusu ise daha genel bir iş tanımı olup, veri yönetimi adı altında da değerlendirilmektedir. Bu bireylerin rolü esas olarak kullanıcı topluluğunu desteklemektir. Bu kişiler, verilerle ilgili sorunları toplamaktan, harmanlamaktan ve değerlendirmekten sorumludurlar. Tipik olarak, veri görevlileri ya konu alanlarına göre ya da iş kolu sorumlulukları dahilinde atanır (Loshin, 2010). Hepsinin ortak noktası ise temelde kodlama becerilerinin olmasıdır.

[6] Veri bilimcisi, veri analisti, veri mühendisi ve veri sorumlusu kategorilerinin nasıl tanımlandığı ve bu kategorilerle ilgili daha detaylı bilgiler kavramsal çerçevede yer almaktadır.

Araştırmanın katılımcıları da “veri bilimcisi” çatısı altında toplanabileceği düşünülen bu kişilerden, bu kişiler statü olarak veri analisti, veri mühendisi ya da veri sorumlusu olarak çalışan ya da veri bilimi alanında akademide eğitim veren ve bu anlamda veri bilimcisi olarak değerlendirilebileceği düşünülen kişilerden oluşmaktadır. Katılımcılarla derinlemesine mülakat ve derinlemesine uzman mülakatları gerçekleştirilmiştir.

Katılımcıların çalıştıkları sektörler farklı olsa da (akademi, savunma sanayi, bakanlık gibi) her biri, veri bilimi konusunda yetkin olması kriteri ile çalışmaya dahil edilmişlerdir. Mülakatın başında katılımcılara bu katılımın tamamen gönüllü olduğunun belirtilmesine uygun olarak, katılımcıların isim ve soy isimleri çalışmada hiçbir şekilde kullanılmamış ve çalışmada araştırmacı tarafından onlara verilen anonim kodlarla yer almışlardır. Katılımcılarla ilgili detaylı bilgi olarak doğrudan alıntıların yanında katılımcıların kod numarası ile yaş, cinsiyet ve çalıştıkları sektör de belirtilmiştir. Fakat temel ayırt edici kriterin veri bilimcisi olmak olduğu vurgulanmıştır. Araştırmadaki sorular hazırlanırken, katılımcılar bu konunun uzmanı oldukları için özen gösterilmiş, etik kurul formu ile katılımcıları rahatsız edebilecek ve etik ihlale sebep olabilecek bir unsur olmadığına dair onay alınmıştır.

Tablo 3. Araştırma Katılımcılarının Özellikleri

Katılımcı Numarası	Yaş	Cinsiyet	Eğitim Durumu	Mezun Olduğu Bölüm***	Meslek*	Deneyim Süresi	Kullandığı Analiz Programları	Yaşadığı Şehir-Ülke	Mülakat Şekli** (Çevrimiçi/ Yüzyüze)	Mülakat Platformu (Çevrimiçi için)
Katılımcı 1	29	Erkek	Tezli yüksek lisans öğrencisi	Elektrik Elektronik (Lisans ve Yüksek Lisans)	Mühendis & Veri bilimci	6 sene	Phyton C+ Java SQL	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 2	28	Kadın	Doktora öğrencisi	Fen Bilgisi Öğretmenliği (Lisans), Eğitim Yönetimi ve Planlaması (Yüksek Lisans), Büyük Veri ve İş Analizi	Veri bilimci	3 sene	Phyton Java	Yalova/ Türkiye	Çevrimiçi	Zoom
Katılımcı 3	30	Erkek	Yüksek lisans	Havacılık ve Uzay Mühendisli	Mühendis & Veri	6 sene	Phyton	Ankara/	Çevrimiçi	Zoom

			mezunu	ği (Lisans ve Yüksek Lisans)	bilimci			Türkiye		
Katılımcı 4	26	Kadın	Lisans mezunu	İstatistik	İstatistikçi & Veri analisti	3 sene	SQL Phyton R Studio	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 5	26	Kadın	Lisans mezunu	İstatistik	İstatistikçi & Veri analisti &Veri bilimci	3 sene	R, SQL	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 6	36	Kadın	Doktora öğrencsi	İstatistik Ekonomi Finans	Veri bilimci	4 sene	SAS Phyton R, SQL	Londra/ İngiltere	Çevrimiçi	WhatsApp
Katılımcı 7	42	Erkek	Yüksek lisans mezunu	Elektrik Elektronik Mühendisliği (Lisans) Elektrik Elektronik Mühendisliği (Yüksek Lisans)	Mühendis & Veri bilimci	10 sene	Phyton R	İstanbul/ Türkiye	Çevrimiçi	WhatsApp

Katılımcı 8	29	Kadın	Yüksek lisans öğrencisi	Endüstri Mühendisliği (Lisans), Yazılım Mühendisliği (Yüksek lisans)	Kalite güvence mühendisi & Veri bilimci	1 sene	Java SQL	Ankara/ Türkiye	Çevrimiçi	WhatsApp
Katılımcı 9	35	Kadın	Doktora mezunu	İstatistik (Lisans), Endüstri Mühendisliği (Yüksek lisans), Yönetim Bilimleri (Doktora)	Post-doc araştırmacı Veri bilimci	5 sene	Qualtrics Phyton R Excell	Londra/ İngiltere	Çevrimiçi	WhatsApp
Katılımcı 10	37	Erkek	Doktora mezunu	İstatistik (Lisans, Yüksek Lisans, Doktora)	Veri bilimci	13 sene	R Phyton SPSS Clementine SAS Miner	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 11	33	Erkek	Lisans mezunu	İstatistik (Lisans)	Veri bilimci	4 sene	Phyton	Cardiff/ İngiltere	Çevrimiçi	WhatsApp

							R SQL			
Katılımcı 12	43	Erkek	Doktora mezunu	Matematik (Lisans, Yüksek Lisans, Doktora)	Veri bilimci	-	R Phyton Turboard Tableau	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 13	57	Erkek	Doktora mezunu	İstatistik (Lisans, yüksek lisans, doktora)	Veri bilimci	-	Phyton SQL Galactex Search	Ankara/ Türkiye	Yüz yüze	-
Katılımcı 14	26	Erkek	Lisans mezunu	İstatistik (Lisans)	Veri bilimci	2 sene	SAS Phyton SQL R	Ankara/ Türkiye	Çevrimiçi	WhatsApp
Katılımcı 15	55	Erkek	Lisans mezunu	İşletme (Lisans)	İşletme sahibi	25+	-	Ankara/ Türkiye	Çevrimiçi	WhatsApp

					Veri bilimci					
Katılımcı 16	26	Erkek	Yüksek lisans öğrencisi	İstatistik (Lisans, Yüksek lisans)	Veri bilimci	2,5 sene	SAS SQL R	Ankara/ Türkiye	Çevrimiçi	WhatsApp

*Katılımcıların bu çalışma için en önemli özelliklerinden bir tanesi hangi kurumda çalıştıklarına dair bilgidir fakat yaş, cinsiyet, meslek, analiz programları bilgilerine ek olarak kurum belirtildiği ve bazı kurumlarda çalışan veri bilimcisi sayısı az olduğundan kimliklerini korumak adına kurum bilgilerinden karma olarak bahsedilmektedir.

**Katılımcılarla 1,5 saat civarında süren mülakatlar gerçekleştirilmiştir.

***Katılımcıların mezun oldukları okullar da anonim kalma endişesi ve sebebiyle yazılmamış sadece bölümleri tabloya eklenmiştir.

1.2.5. Araştırmanın Riskleri ve Sınırlılıkları

Araştırmanın önemli yanlarından bir tanesi, artık günümüzde bir tür sermaye olarak değerlendirilen ve güç ilişkilerinin temelinde yer alan büyük verinin toplanması, depolanması ve işlenmesinde önemli sorumluluklar alan ve onun yaratmış olduğu gözetim pratikleri hakkında detaylı bilgisi olduğu düşünülen veri bilimcilerinin bakış açısından değerlendirme imkânı sağlamasıdır. Fakat bu aynı zamanda bir risk oluşturmaktadır çünkü katılımcılar kısmında da bahsedildiği gibi, veri bilimi nedir, veri bilimcisi kimdir, kimler hangi niteliklerle bu meslek grubunda olabilir ve ne tür sınıflandırmalar yapılabilir gibi sorular da güncel sorular olarak karşımıza çıkmaktadır. Bu riskin önüne geçmek için araştırmanın katılımcılar kısmı özellikle literatür araştırması ve katılımcılardan alınan bilgiler doğrultusunda çok detaylı bir şekilde yazılmaya çalışılmıştır. Bu kapsamda veri biliminin kapsamı, veri bilimcileri, veri sorumluları, veri mühendisleri ve veri analistleri gibi kategoriler temel bir başlık altında toplanmaya çalışılsa da benzerlik ve farklılıklarına vurgu yapılmıştır. Katılımcılar seçilirken de bu detaya özellikle dikkat edilmiştir.

Aynı şekilde büyük veri ve gözetim pratikleri genel anlamda kurumların sahip olduğu “gizli” bilgilere “kişisel bilgilere” ya da “gizli kitlesel bilgilere” dayandığından, katılımcıların çalıştıkları kurumun gizli bilgileri ile ilgili bilgi vermeyeceği, tamamen onların büyük veri ve gözetim pratiklerine odaklanılacağına dair ikna aşaması araştırmacı için zor bir deneyim olmuştur. Çalıştıkları kurumların özellikle güvenlik ve gizlilik politikalarından dolayı çekinen birçok katılımcı da araştırmaya bu sebeple katılmak ve mülakat yapmak istememiştir. Hatta bazı kurumlara etik kurul raporunun yanısıra bireysel görüşme formu, araştırma hakkında detaylı bilgiler içeren raporlar sunulması suretiyle izin alınarak katılımcılar mülakata katılmaya ikna edilmiştir. Çoğu katılımcı ise araştırmaya katılmayı doğrudan reddetmiş ve bu belgeleri bile incelemeyeceğini, hiçbir şekilde araştırmaya katılamayacağını belirtmiştir.

Araştırmanın diğer bir zorluğu ise katılımcıların genellikle fen bilimleri alanından olması nedeniyle onları büyük verinin sosyolojiyle ilişkisine ikna edebilmek olmuştur. Büyük verinin toplumu etkileyen önemli bir olgu olduğu ve dijitalleşmeyle birlikte ne tür toplumsal etkileri olabileceğine dair katılımcılarla ön görüşmeler yapılmış, araştırmacı kendi çalışma alanını, neden bu alanda çalıştığını, önceden bu konularla ilgili ne tür çalışmalar yaptığını ve bu araştırmanın neden önemli olduğunu neredeyse tüm katılımcılara mülakattan önce ön görüşmeler yaparak açıklamıştır.

Hem avantaj hem de dezavantaj olarak görülebilecek diğer bir nokta ise, katılımcıların genellikle teknik açıdan konuya yaklaşmalarıdır. Bu dezavantajı ortadan kaldırmak amacıyla, araştırma tasarımı esnasında yarı yapılandırılmış bireysel görüşme formundaki ilerleyiş bu durum göz önünde bulundurularak tasarlanmıştır. Bu sayede hem araştırmacının işi kolaylaşmış hem de katılımcının araştırmaya, kendi büyük veri ve gözetim deneyimlerine ontolojik güvenlik algısına dair daha açık olmasına imkân sağlanmıştır. Bazı katılımcıların mülakata katılmadan önce araştırmanın başlığına bakarak “büyük veri ve gözetim”, “büyük birader”, “yeni gözetim pratikleri” gibi kavramları araştırdıkları ve oradan edindikleri bilgilere göre hareket etmeye çalıştıkları görülmüş, mülakatın bir bilgi sınavı niteliği taşımadığı, önemli olanın onların görüşleri olduğu vurgulanarak onların kendi görüşlerine ulaşılmaya çalışarak araştırmada çok önemli bir sorunun önüne geçilmiştir.

Bunun yanı sıra bir diğer önemli zorluk ya da sınırlılık ise ontolojik güvenlik algısını anlamanın zorluğudur. Bireylerin çevrelerindeki düzene olan inançlarını ya da güvenlerini nasıl koruduklarını ya da koruyamadıklarını, büyük veri ve gözetim sistemlerinin bunun üzerinde ne tür etkilere sahip olduğunu tespit edebilmek için bireysel görüşme formu çok detaylı bir şekilde hazırlanmış olsa da bazı katılımcıların kendi alanlarında profesyonelliklerini korumak adına, bu alandaki endişelerini kısmen paylaştıkları, formdaki farklı bölümlerde yer alan bilerek konulmuş benzer sorularda göze çarpmıştır.

Bu araştırma Türkiye'deki veri bilimcilerle sınırlıdır şeklinde bir sınırlılığın ise uluslararası firmalarda ya da yurtdışındaki üniversitelerde birçok farklı sosyal ortamda ve ülkede bireyle mülakat yapılarak biraz da olsa aşıldığı düşünülmektedir. Bu çalışmanın veri değerlendirme sürecinden sonra başka çalışmalarda farklı ülkelerdeki veri bilimcilerle de bu benzeri çalışmaların, nicel, nitel ya da karma yöntemle yapılacak olan çalışmaların da literatüre daha fazla katkı sağlayacağı ve bu konunun daha derinlemesine düşünebileceği ise inkâr edilemez.

Araştırmanın risklerinden bir tanesi ise veri değerlendirme sürecinde görüşülen veri bilimcilerin ontolojik güvenlik algısındaki değişimi yorumlarken çok net bir kanıya varma endişesidir. Fakat farklı sektörlerde, farklı verilerle çalışan bireylere ulaşılması ve her birinin bireysel olarak da çok farklı görüşleri olması, Giddens'ın da ontolojik güvenlik kavramı konusunda uzmanların kendi arasında da farklı noktalara yöneldiği kanısını bir kere daha göstermekte ve katılımcılarla ilgili bu tür bir gruplandırma çalışmanın sonuç kısmında gerçekleştirilmektedir. Bahsedilen sınıflandırma, bu tür sistemlerin yol açabileceği sistemleri dezavantajlarına rağmen tamamen kabul etme ve bununla ilgili tamamen negatif düşüncelere sahip olmak, nötr bir şekilde kalmaya çalışmak ya da aksine bu sistemlerden kaçmanın gerekliliğini öngörerek daha çözüm odaklı yaklaşmak gibi çeşitli kategoriler şeklinde ortaya çıkmaktadır.

Nitel araştırmaların test etme ve genelleme hedefi olmadığı, nedensel ilişkileri açıklamadığına dair birçok görüş bulunmaktadır. Bu çalışmada nitel araştırma yönteminin tercih edilmesinin nedeni, veri bilimcilerinin anlam dünyalarına ve ontolojik güvenlik algısına ulaşmanın, tüm toplum için büyük veri ve değişmekte olan gözetim pratiklerinin ne yönde olduğunu görebilmek ve gerekli olan önlemleri almak, farkındalık sağlamak adınadır. Aynı şekilde literatüre bakıldığında, nitel araştırma ile ilgili genellikle öne sürülen bu tür bir eleştirinin doğru olmadığı, aksine bu şekilde süreçler ve mekanizmalar arasındaki ilişkileri göstermek için etkili bir yöntem olduğu şeklindedir. Nitel araştırmanın nedensel ilişkiyi tanımlayamadığı şeklindeki geleneksel görüş, kısıtlayıcı ve felsefi olarak

miadını doldurmuş bir nedensellik kavramına dayanmaktadır ve hem nitel hem de nicel araştırmacılar, nedensel çıkarım için nitel yöntemleri kullanmanın meşruiyetini giderek daha fazla kabul etmektedir (Shadish, Cook ve Campbell, 2002). Böyle bir yaklaşım, değişkenler arasındaki ilişkideki düzenlilikleri basitçe göstermek yerine, nedenselliğin süreçler ve mekanizmalar açısından ele alınmasını gerektirmektedir (Maxwell, 2008, s. 221).

Bu araştırma, veri bilimcilerinin ontolojik güvenlik algılarına dair net bir sonuç ortaya koymayı değil, bu vasıtayla, bu alanda bilgili ve güç sahibi olan bireylerin görüşlerine odaklanarak, dijital toplum içerisinde bu sistemlere mecburi ya da kendi istekleriyle dahil olan bireylerin daha güvenli ve bilinçli şekilde bu sistemleri kullanmalarını hedeflemektedir. Aynı şekilde dijitalleşmenin birçok yükümlülüğü bireye yüklemesi ve her şeyi genel olarak ondan beklemesinin önüne geçerek, bilinçsiz bir şekilde bu sistemlere dahil olup mağdur olan ya da olabilecek bireyler için yasal, ekonomik, siyasal, teknik ve sosyal önlemlerin tekrar sorgulanması amacı taşımaktadır.

1.3. LİTERATÜR TARAMASI

Türkiye'de yapılan lisansüstü çalışmalara bakıldığında, özellikle sosyal bilimler alanında, 2016 senesinde bir araştırmacı tezini ileride büyük verinin karanlık yüzünü görmek isteyen araştırmacılara ithaf etmiş (Dalgalıdere, 2016), büyük verinin bilim felsefesi açısından yorumlanmasına uğraşmıştır. 2019 senesinde ise yeni medyanın büyük veri üzerinden incelemesini ekonomi, politik yaklaşım çerçevesinde değerlendiren bir tez (Durmuşahmet, 2019) ile büyük veriye dayalı teknoloji politikası modeli önerisi geliştirme amacında olan bir tez (Öztürk, 2019) yazılmıştır. 2020 senesinde ise büyük veri ile gizlilik ve mahremiyet ilişkisini araştıran nicel bir tez çalışması (Oflaz, 2020), büyük veriyi bilgi sosyolojisi temelinde ele alan ve bunu toplumsal güvenlik anlamında değerlendiren belgesel araştırma tekniğine dayalı bir tez (Şahin, 2020) ve büyük verinin tıpta kullanımına etkisini araştıran nicel ve nitel yöntem içeren bir tez (Eryılmaz, 2020) yazıldığı görülmektedir. Sosyal bilimler alanında büyük veriye dayalı bu

ilgi, konunun özellikle dijital medya teknolojileri ve dijital gözetim anlamında araştırılması gereken bir konu olduğuna vurgu yapmaktadır.

2022 senesinde büyük verinin öznellik üzerindeki etkilerini tarihsel bir yaklaşımla Cambridge Analytica örneğini ele alarak yapan bir çalışma (Şinsek, 2022) ile mobil uygulamaların kullanım düzeyi ve gizlilik endişesi üzerinden büyük veri analitiğini araştıran bir çalışma (Uyanık, 2022), 2021 senesinde büyük verinin tüketici davranışlarına etkisini risk ve güven algısı gibi kavramlarla nicel araştırma yöntemi kullanarak yapan bir çalışma (Zengin, 2021) ile büyük veri ve yapay zekanın demokrasi anlamında neler vaat ettiğini, Türkiye'deki seçim kampanyaları üzerinden olumlu ve olumsuz yanlarına bakılmasını hedefleyen nitel bir araştırma gerçekleştirilmiştir (Shahzad, 2021). Aynı sene içerisinde, büyük verinin Türkiye'deki seçim kampanyalarındaki rolünü niteliksel bir araştırma ile anlamaya çalışan bir tez daha bulunmaktadır (Güneş, 2021).

Fen bilimleri alanında ise özellikle büyük veri ve mahremiyeti koruma doğrultusunda 2021 yılında yazılmış olan "Büyük Veri ve Akan Verinin Mahremiyet Korumalı Anonimleştirilmesi" isimli bir tezle, büyük veri ile birlikte birçok anlamda büyüyen verinin mahremiyet anlamında nasıl korunabileceğine yönelik çeşitli öneriler getirildiği (Sopaoğlu, 2021), 2019 senesinde ise büyük veriye yetkisiz erişimlerin önüne geçebilmek için güvenlik açıklıklarının nasıl tespit edilebileceği ve ek güvenlik önlemlerinin nasıl geliştirilebileceğine yönelik bir araştırma yapıldığı (Toy, 2019) görülmektedir. 2015 senesinde de büyük verinin mahremiyet konusunda yaratma potansiyeli taşıdığı güvenlik açıklarına yönelik yapılmış bir çalışma (Selçuk, 2015) bulunmaktadır.

Mahremiyet alanında yapılan çalışmalara bakıldığında ise 2004 yılından başlayarak elektronik gözetim ve denetimin (Akgüç, 2004), kameralı gözetim ve mahremiyet ile ilişkisini ele alan bir çalışmanın (Mermutlu, 2010); (fen bilimleri alanından) bilgi teknolojileri çerçevesinde Türkiye'de kişisel verilerin korunması durumunun (Tahaoğlu, 2009); (fen bilimleri alanından) veri madenciliğinde mahremiyetin sağlanmasına yönelik bir araştırmanın (Kavza, 2010), sağlık

hizmetlerinde toplanan veriler ile mahremiyet ilişkisine yönelik bir araştırmanın (Özkan, 2010) olduğu görülmektedir.

2022 senesinde, büyük verinin ne boyutlara ulaşabileceğini anlatan ve dijital sosyoloji alanında önem verilen kitaplardan biri olan Çember'in içerik analizi yapılarak dijital gözetim ve mahremiyet temelinde ele alındığı (Büyükgaga, 2022) görülmektedir. 2021 senesinde, unutulma hakkının önemini ve etik boyutunu anlamaya yönelik yapılan bir çalışma (Kiver, 2021); TikTok'un gençlerin büyük veri algoritmalarına nasıl dahil olduğu ve mahremiyetin nasıl şekillendiğine yönelik gerçekleştirilmiş bir çalışma (Kaya, 2021) dikkat çekmektedir.

Uluslararası literatür incelendiğinde doğrudan büyük veri ve mahremiyet içerikli çalışmalara bakıldığında, çok fazla sayıda makale yer aldığı görülmekte (Yu, 2016; Kshetri, 2014; Jain vd., 2016), çok sayıda makale içerisindeki konulara bakıldığında ise Sosyal Kredi Sistemi (Chen ve Cheung, 2017), büyük veri ile tüketici veri analizleri (Leonard, 2014; Palmatier ve Martin, 2019); eğitimde büyük veri ve mahremiyet (Reidenberg veSchaub, 2018; Wang, 2016); sağlık alanında büyük veri ve mahremiyet ilişkisi (Mooney ve Pejaver, 2018; Kayaalp, 2018; Cohen ve Mello, 2019), büyük verinin sebep olduğu mahremiyet sorunlarına çözüm aramak için hukuki, etik, siyasal ve teknik konuları ele alan pek çok makale bulunmaktadır.

Büyük veri ve ontolojik güvenlik kavramları ile arama yapıldığında ise, 2013 senesinde yazılmış olan verileşmeyi temel alan ve büyük veri ile ontolojik güvenlik arasındaki bağlantıyı içeren bir makale öneren (Lycett, 2013) bir çalışmaya rastlanmış, önerilen makalenin (Schlichter ve Rose, 2013) daha çok büyük sistem uygulamalarında güven dinamiklerini incelediği görülmüştür. Bu makaleden hareketle, aramaya ontolojik güvenlik kavramı yerine, güven dinamikleri ve büyük veri başlığı temel alınarak devam edilmiş, akıllı tarım[7]

[7] Bu makalede yapılan analiz, katılımcıların güven ile ilgili sorunların sistemleri kullanmada temel endişe kaynağı olduğunu göstermekte, bu çalışma çiftçi verilerine erişim ve bu

(smart farming) temelinde büyük verinin neden ve nasıl kullanıldığına dair bir şeffaflık olmadığı sürece nasıl güven sağlanabileceğine yönelik bir tartışma (Jakku Taylor, Fleming, Mason, vd. 2019) yürütüldüğü görülmüştür. Bu çalışmanın başlığı "Bize Onla Ne Yaptıklarını Söylemezlerse, Neden Onlara Güvenelim?" bu tez için de ilham verici bulunmuştur. Verileşme, dataizm ve veri gözetimini temel alan bir çalışmada da bu tür konulara değinildiği (Van Dijck, 2014) fakat doğrudan bahsedilmediği görülmektedir.

Türkçe yayınlar özelinde bakıldığında ise büyük veri ve güven dinamikleri ya da büyük veri ve ontolojik güvenlik aramalarında ilişkili hiçbir sonuca ulaşılamamış, fakat büyük veri ve mahremiyet temelinde uluslararası literatürde görüldüğü gibi pek çok çalışma (Canbay, Vural ve Sağıroğlu, 2020; Eyüpoğlu, Aydın, Sertbaş vd. 2017; Ergen, 2018; Karaarslan, Eren ve Koç, 2014) olduğu görülmüştür.

Büyük verinin hukuki, siyasal, kültürel, güvenlik temelli, ekonomik ve daha pek çok alanda etkisini, çözümlerini, sorunlarını tartışmanın gerekliliği tüm bu çalışmalarla ve bu kısma dahil edilemeyen pek çok çalışma ile görülmektedir. Bu araştırma ile hedeflenen temel sorunun sorulmamış olduğu ve bu sorunun sorulmasının bu çalışmalara katkı sağlayacak ve bu çalışmalardan çok iyi bir şekilde beslenecek bir soru olduğu düşünülmektedir. Büyük verinin neden olduğu, büyük veriye dayalı karar verme mekanizmaları ve büyük verilerin kolayca erişilebilir hale gelmesi insan ilişkilerini ne hale getirmektedir? Bu ilişkilerde "karşındaki kişiye güvenme" durumu büyük veri ile nasıl bir değişime uğramıştır? Güven duymaya çalışırken, dijital okuryazarlığı yüksek ve hatta bu sistemleri tasarlayan kişiler de büyük veriyi kullanmakta mıdır? Büyük verinin güven ve ontolojik güvenlik gibi önemli durumlarda yer almasının toplumsal,

---

kullanımdan kimin yararlanacağı ve nasıl dağıtılacağı ile ilgili kaygılar olduğunu, şeffaflık olmadıkça da bu durumun devam edeceğini göstermektedir. Bunun akıllı teknolojilerin değeri konusunda şüphe uyandırdığı ve diğer sektörlerde de geçerli olabileceği vurgulanmaktadır. Daha fazlası için bknz. Jakku, E., Taylor, B., Fleming, A., Mason, C., Fielke, S., Sounness, C., &Thorburn, P. (2019). "If they don'ttell us what they do with it, why would we trust them?" Trust, transparency and benefit-sharing in Smart Farming. *NJAS-Wageningen Journal of Life Sciences*, *90*, 100285.

kültürel, sosyal, siyasi, ailevi, kişisel, psikolojik her tür muhtemel sonucu nedir? ilk etapta akla gelen sorulardan bazılarıdır.

2. BÖLÜM

ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ

2.1. KAVRAMSAL OLARAK BÜYÜK VERİ

Büyük verinin sosyolojik olarak incelenmesi, toplumun dijitalleşmesi ve enformasyon teknolojilerinin gelişimi, internetin yaygınlaşarak küresel bir ağ meydana getirmesi, kullanıcı odaklı üretilen içeriğin sosyal medya platformları ile gelişmesi, fiziksel olarak gerçekleştirilen birçok aktivitenin çevrimiçi ortama aktarılması gibi bir süreçte bir zorunluluk haline gelmektedir. Bahsedilen tüm süreçler bireylerin istemli ya da daha önemlisi istemsiz bir şekilde büyük veriye katkı sağlayarak var olma süreçleri sonucunda büyük verinin ekonomik, sosyal ve kültürel alanda büyük bir toplumsal değişimin temeli olmasına neden olmaktadır.

En basit haliyle bakıldığında büyük veri "İnsanların özellikle sosyal medya araçlarında paylaştıkları, videolar, konumlar, fotoğraflar, profiller, hesaplar kısacası her şey insanların internette yaptığı her aktivitenin, tıkladığı her noktanın, araştırdığı her şeyin toplanarak, birey hakkında elde edilen bilgiler, veriler bütünüdür. Bu verilerin kim tarafından kontrol edildiği, toplandığı ya da ne amaçlarla kullanılacağı ise dijital toplum için çok büyük tehlike yaratmaktadır" (Özuz, 2018, s. 54). Sosyolojik olarak, büyük veri gibi analitik ve istatistiksel alt yapı gerektiren bir kavramın ele alınmasının gerekliliği, günümüzde bu kavramın insan sermayesi ve maddi varlıklarla karşılaştırılabilecek bir değer olarak kavramın dönüşüm geçirmesinden kaynaklanmaktadır. Massachusetts Teknoloji Enstitüsü'nden Madden'ın tanımına göre büyük veri, var olan araçların işlemesi için çok fazla büyük, çok fazla hızlı ve çok fazla zor olan veriyi ifade etmektedir (Madden, 2012, s. 4). İlk zamanlarda büyük verinin geleneksel veriden farkı "üç V" hacmi, hızı ve çeşitliliği ile vurgulanırken, güncel olarak "4 V" ile tanımlanarak doğruluğuna da vurgu yapılmaktadır (Volume, Velocity, Variety ve Veracity). Büyük veri, analizi için veri tabanı yönetim sistemleri (DBMs) ve MapReduce (ayrıca Oracle, Madskills, Apache Mahoout, Graphlab)

gibi büyük ölçekli verilerin analizini sağlayan programlarla, SAS, R ve Matlab gibi istatistiksel analiz araçlarının bir araya getirilmesiyle sağlanabilecek büyüklükte verileri ifade etmektedir (age, s. 5). Büyük veriyi oluşturan veriler; işletme verileri, üretim verileri, envanter verileri, satış verileri, finansal veriler; Nesnelerin İnternet'i yoluyla elde edilen veriler, internette bireysel olarak bireylerin üretmiş oldukları veriler, forumlardaki mesajlar, mikrobloglardaki mesajlar, internetteki tıklamalar ve her tür veri; biyomedikal veriler, "biyolojik büyük veriler" örneğin gen dizilimi verileri, hastane kayıtları, (Çin Milli Gen Bankası'nın 1.15 milyon insan, 150.000 hayvan, bitki ve mikroorganizma örneklemi içermesi gibi) olarak sıralanabilmektedir. Büyük verinin geçirdiği değişimler, veriyi topladığı temel veri kaynakları ve kullanım alanlarına bakıldığında yalnızca analitik ve istatistiksel bir olgu olmaktan çıkarak, sosyolojik bir konu haline gelmektedir. Temel veri kaynaklarını oluşturan "dijital izlerin", şirketlerin, kurumların, grupların, ülkelerin, bireylerin temel olarak herkesin ve her şeyin, her tür hareketinin hem çevrimiçi hem de çevrimdışı ortamda elde edilen verilerden oluşturulan bir füzyon şeklinde toplandığı ve bu verilerin yalnızca depolanmış veriden çok daha fazlası olduğu görülmektedir. "Büyüklük" vurgusu yapılan ve temel anlamda dijital gözetimi destekleyen bu verilerin, bu sebeple sosyolojik anlamda da çok daha detaylı ve farklı şekillerde ele alındığı görülmektedir.

Dijital sosyoloji temelinde bakıldığında, büyük verinin 3V, 4V ya da 7V temelindeki tanımlarına (bu tanımlar ileriki bölümlerde detaylı bir şekilde ("Verinin Hacmi (Volume), Hızı (Velocity), Çeşitliliği (Variety) ve Doğruluğu (Veracity)" başlığında açıklanmaktadır) ek olarak, büyük verinin 13P ile tanımlandığı da görülmektedir. Bunlar: "Portentous", "Perverse", "Personal", "Productive", "Partial", "Practices", "Predictive", "Political", "Provacative", "Privacy", "Polyvalent", "Polymorphous" ve "Playful" olarak sıralanmaktadır. İlk olarak "Portentous" (Mucizevi); büyük verinin ticari, yönetimsel, devlet ve araştırma amaçlarında çok önemli bir olgu olduğunu belirtmektedir. "Perverse" (Aksi) büyük verinin sunduğu yeni olanaklarla heyecan yarattığını fakat üzerinde kontrol sağlanamayacağı durumlar yaratma ihtimali açısından korku ve endişe

yarattığını; “Personal” (Kişisel), büyük verinin bireylerin kişisel davranışları, tercihleri, ilişkileri, bedensel faaliyetleri ve duyguları ile ilgili detaylı bilgi taşımasını; “Productive” (Üretken), büyük verinin kişiliği, bedeni, sosyal grupları, çevreyi, devleti, ekonomiyi ve daha birçok kavramı kavramsallaştırma açısından yeni ve farklı bir yol olduğunu; “Partial” (Kısmi), büyük veride bazılarının veri olarak kabulü ile bazılarının göz ardı edilmesini ifade etmekte ve aynı zamanda bazı gruplar üzerinde daha çok veri toplanması ve diğerlerinin toplumsal olarak göz ardı edilmesi sürecine de işaret etmektedir. “Practices” (Pratikler), büyük verinin bireyler ve kurumlar üzerinden sosyal medya hesapları, para transferleri, kendini izleme aletleri gibi bir çok verinin veri madencilik endüstrisi, alet ve donanımlarının gelişimiyle toplanması yoluyla meydana gelmesini; “Predictive” (Tahmin Edilen), büyük verinin insan davranışları hakkında bazı tahminler yapma imkanı yaratmasını ve bunların sağlık, sigorta, iş, kredi gibi pek çok alanda etkili olmasını; “Political” (Siyasi), büyük verinin güç ilişkilerini veri setleri üzerindeki hakimiyet için yaşanan çatışmaları ortaya çıkabilecek olan sosyoekonomik dezavantajları ve dijital gözetim sürecini; “Provocative” (Provokatif), büyük verinin tartışmalı olmasını, bazı milli güvenlik kurumlarının vatandaşları üzerinde kurduğu dijital gözetim mekanizmalarını, kişisel verinin kullanım ve yanlış kullanımı ile verinin ticarileşmesini açıklamaktadır. “Privacy” (Mahremiyet), büyük veri ile ilgili artan mahremiyet endişelerini; “Polyvalent” (Çok Değerliklilik), büyük verinin sosyal, kültürel, coğrafi ve zamansal anlamlarda birçok aktör ve kurumları içermesini; “Polymorphous” (Çok Biçimlilik), büyük verinin alabildiği 2D grafiklerden 3D nesnelere kadar birçok biçimi ifade etmesini ve son olarak “Playful” (Oyunculuk) ise büyük verinin kendi hakkında veri toplamak ya da paylaşmaktan hoşlanan “self-trackerları” (kendi kendini genel olarak giyilebilir teknolojik aletler ile izleyen/takip eden bireyler ya da gruplar) ifade etmektedir (Lupton, 2015, ss. 2-3).

Tüm bu maddelerle birlikte büyük verinin toplumsal, ekonomik, kültürel ve siyasi alanlarda değişime yol açtığı ve kendisinin de sürekli değişime maruz kaldığı görülmektedir. Sosyolojik olarak kavramsal temelde araştırıldığında, büyük veri “prosumption” kavramının en büyük sonuçlarından bir tanesidir. Prosumption

kavramının Türkçe olarak doğrudan bir karşılığı olmasa da “production” (üretim) ve “consumption” (tüketim) kavramlarının birleşiminden türetilen bir kavram olduğu bilinmektedir. Bazı kaynaklarda “üretüketim” olarak çevrildiği görülse de bu kullanımın bu kavramı tam olarak yansıtıp yansıtmadığı tartışmalıdır. Web 2.0’dan sonra kendini göstermeye başlayan prosumption durumu, özellikle pasif tüketiciler yerine, kullanıcıların kendilerinin de içerik üretmeleri ve bunların büyük bir veri kaynağı oluşturması sürecini, prosumptionun büyük verinin temel ilkelerinden biri olduğunu gözler önüne sermektedir. Gündelik hayat pratiklerinin de büyük verinin en temel veri kaynaklarından biri olması bu ilkenin temel sebep ve sonuçlarından bir tanesidir. Büyük veri, bu anlamda Lupton’un da belirttiği şekilde hem nitel hem nicel anlamda büyük bir hacme sahip olan veri olmasının yanı sıra, bireylerin web sitelerini ziyaret ettiklerinde, aramalar yaptıklarında, ürün satın aldıklarında, aradıkları telefon numaralarından, iletişimde oldukları kamu kurumları ya da ticari kurumlarla olan tüm kullanıcı aktivitelerinden toplanan dijital izleri ifade etmektedir (2014, ss. 858-859). Bu olgu yukarıda bahsedilen “prosumption” kavramı ile de ifade edilmektedir, içeriğin ve verinin eş zamanlı olarak kullanıcı tarafından hem üretilmesi hem de tüketilmesi temelinde ele alınmaktadır.

Büyük verinin sosyolojik olarak ne ifade ettiği başka bir deyişle, çevrimiçi teknolojilerle iletişimlerle büyük ve sürekli olarak oluşmaya devam eden dijital veri tabanları olmasının yanı sıra hem insan hem de insan olmayan aktörlerle iletişimleri kastetmektedir bunlar spesifik olarak “Nesnelerin İnterneti” ve “Sensör Toplumu”dur (Michael ve Lupton, 2016, s. 104). Nesnelerin İnterneti ve Sensör Toplumu da prosumption kavramı ile bağlantılı kavramlardır. Bireyler, kullanıcı odaklı üretilen içerik (UGTs) ya da çevrimiçi ortamda gerçekleştirdikleri her bir aktiviteyle bu sürece dahil olurken, insan olmayan aktörlerle kastedilen, Lupton ve Michael’ın örneklendirdiği şekliyle, dijital verinin kendini izleme cihazları (bunlar giyilebilir teknolojik aletler olarak görülebilir), akıllı tarım (hayvan ve bitkilerin sensörlerle takibi), akıllı şehir (kapalı devre kamera sistemleri, sensör bazlı trafik yönetim sistemleri, katılımcılarının hareket ve

alışkanlıklarını üreten ve paylaşan domestik aygıtlar) gibi sistemlerle üretilen verileri de içermesidir.

Büyük veri yalnızca bahsedilen tüm süreçlerle toplanan, depolanan ve analiz edilen veriyi ifade etmemektedir. Sosyolojik açıdan büyük verinin en önemli tanımlarından bir tanesi de birey ve toplum açısından bu verilerin ne kadarının nasıl, kim tarafından toplandığı, ne kadarına onay verildiği ve nasıl kontrol edildiği üzerinedir. Michael ve Lupton bu düşünceyi destekleyerek, dijital sosyoloji temelinde özellikle bazı eleştirel yazarların büyük verinin "ham veri" değil, "bozulmuş veri" olduğunu ve bazı sosyal aktörler tarafından "pişirildiğini" belirtmektedirler. "Bozulmuş veri" (rotted data) aynı zamanda bu verilerin saf olmadığını, onların maddiliğini ve dijital veri ekonomisine girdiği anda üreticileri tarafından kontrol kaybını uğradığını da ifade etmektedir (a.g.e., s. 107). Büyük verinin kavramsal olarak ne ifade ettiğinin yanısıra, ortaya çıkışı ve gelişimini de bilmek önem taşımaktadır bunun en temel sebebi, tıpkı ne ifade ettiğinin teknik ve sosyolojik yanı gibi, ortaya çıkış ve gelişiminde de hem teknik hem de sosyolojik gelişimin farklı noktalara dayanmasıdır.

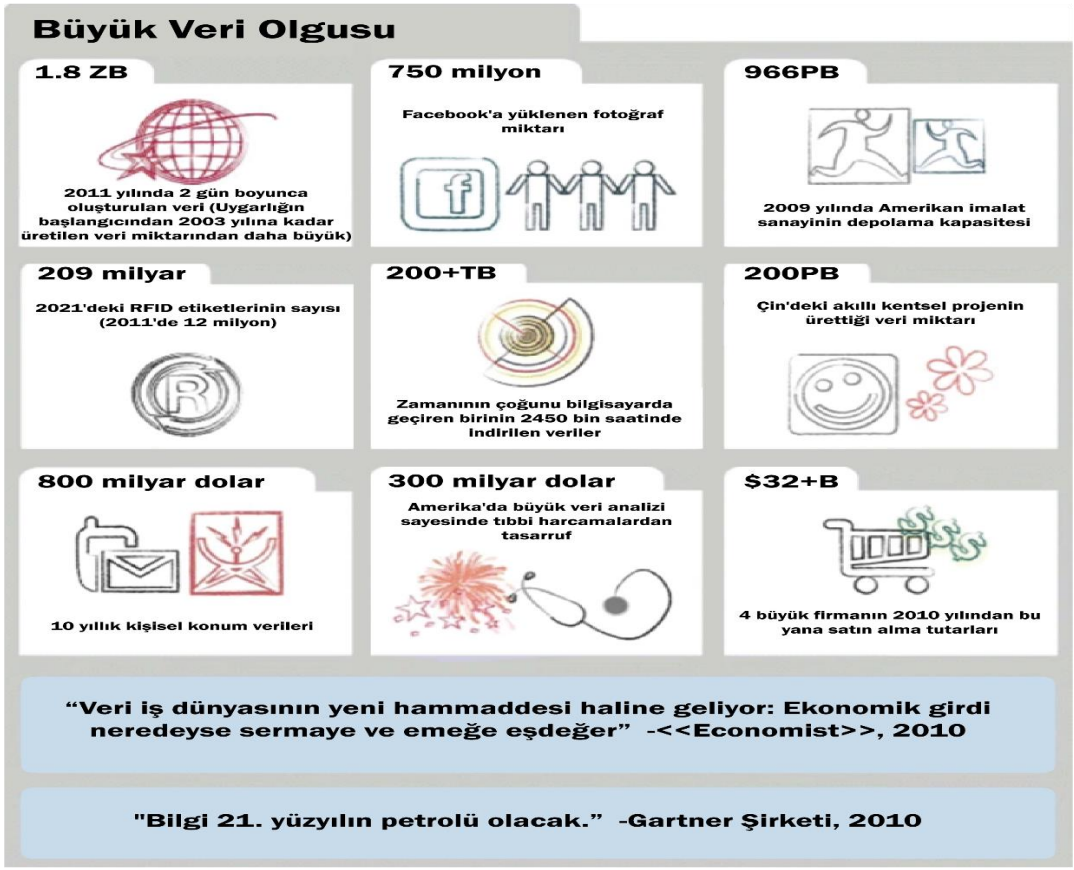
2.1.1. Büyük Verinin Ortaya Çıkışı ve Gelişimi

Büyük verinin ortaya çıkışının ve gelişiminin temeli, aşağıdaki görselde görüldüğü şekilde, verinin iş dünyasında yeni bir hammadde haline gelmesi, sermaye ve emeğe neredeyse eşit bir ürün halini almasına dayanmaktadır. Enformasyon teknolojilerinin gelişimi, bireysel ve kitlesel verilerin aktif bir şekilde çeşitli sistemler bir araya getirilerek toplanması, bu verilerin işlenmesi, depolanması ve analiz edilmesi gerekliliği ile her süreç birbirini desteklemiştir.

Şekilde görüldüğü gibi, 2003'e kadar elde edilen veri miktarının 2011'de 2 gün içerisinde üretilebiliyor oluşu (1.8 zettabayt); Facebook'a 750 milyon fotoğrafın yüklenmesi, 2009'da Amerikan imalat endüstrisinin depolama kapasitesinin 966 petabayta ulaşması; nesneleri elektronik kodlarla tanımlamaya yarayan RFID (Radyo Frekansı ile Tanımlama Teknolojisi) etiketlerinin 2011'de 12 milyonken

2021 de 209 milyara ulaşması; Çin'de akıllı kent projelerinin ürettiği veri miktarının 200 petabayta ulaşması; kişisel konum verilerinin 10 yıl içerisinde 800 milyar dolara ulaşması; Amerika'da büyük veri analizi ile tıbbi masraf tasarrufunun 200 milyar dolar olması büyük verinin çok kısa bir zaman dilimi içerisinde sosyal, ekonomik, bireysel, kültürel, çevresel ve daha bir çok alanda ne kadar etkili olduğunu örneklendirmektedir (Chen, Mao ve Liu, 2014, ss. 172-173).

Şekil 2. Büyük Veri Olgusu



(Chen, Mao ve Liu, 2014, s. 172)

Tarihsel gelişimine bakıldığında 1970 senesinde "veri tabanı makinelerinin" ortaya çıkması, 1980 yılında "Share Nothing" isimli paralel veri tabanının artan veri hacmini karşılamak için kurulması, 1986'da ilk başarılı ticari paralel veri tabanı sitemi olarak Teradata Sistemi'nin kurulması, 1990'da paralel veri tabanı

sistemlerinin yaygınlaşması gibi daha teknik süreçlerin olduğu görülmektedir. (a.g.e., 2014). 1854 senesindeki Kolera salgınının bir taramasını yaparak, bir caddede yer alan su pompasının bu hastalığa sebep olduğunu ortaya koyan Dr. John Snow'un da gelişmiş veri işlemenin ve modern biçimiyle büyük verinin temellerini attığı söylenmektedir (Lokke, 2020, s. 59). Asıl olarak bakıldığında verilerin bahsedilen V'leri arttıkça depolama, analiz ve işleme gibi süreçlerin zorlaşması sebebiyle büyük firmaların istatistik ve modelleme programlarını oluşturmalarıyla büyük verinin kullanım alanı gelişmiştir. Bunlardan bir tanesi Google'ın GFS ve MapReduce Programlama modelleridir. 2005'te "O'Reilly Media'dan Roger Mogoulas 'büyük veri' kavramını, mevcut olan veri işleme yaklaşımlarının karmaşıklık ve boyut nedeniyle işleyemediği büyük miktarda veriyi tanımlamak için ilk defa tanıtmıştır. Fakat büyük verinin araştırma ve bilimsel bir konu olarak gelişimi 1970lerden beri devam etmektedir" (Subudhi, Rout ve Ghosh, 2019, s. 26131).

Chen, Mao ve Liu'nun bu tarihsel çerçeve içerisinde belirttiği gibi, 2007 senesinde veri tabanı yazılım uzmanı olan Jim Gray'in, kullanıcıların da içerik üretmesi, sensörler ve diğer kaynaklarla artan veri akışları için farklı bir bilişim mimarisi olduğunu düşünerek bunu "4. Paradigma" olarak adlandırdığı ifade edilmektedir. Kavramsal çerçevede de değinildiği gibi, 4. Paradigma sosyal medya platformları ile kullanıcı odaklı içerik ve prosumptionun (üretüketim) da doğrudan sürece dahil olmasını ifade etmektedir. Bu süreçten sonra büyük şirketlerin doğrudan büyük veri projelerine başladığı bilinmektedir. Bunlardan yalnızca bazıları IBM 2005, EMC, Oracle, Microsoft, Google, Amazon, Facebook gibi firmalardır. Bu gelişmelerle bağlantılı olarak akademide büyük verinin ilgi kazanmaya başlaması da önemli gelişmelerdendir. Akademik olarak önemli gelişmelerden bazıları: "Nature'ın büyük veri ile ilgili özel sayı yayınlaması ve 2011'de Science'da büyük veride veri işlemede anahtar teknolojilerle ilgili özel sayı yayınlamasıdır". Büyük veri aynı zamanda siyasal ve ekonomik olarak da tamamen bir gerçeklik olarak ele alınmaya başlanmıştır. Bunun kanıtlarından yalnızca bazıları: "2012'de Davos Zirvesi'nde Büyük Veri Raporu yayınlanması ve büyük verinin de altın ya da bir tür para birimi

olduğunun duyurulması ile uluslararası bir araştırma kurumu olan Gartner Hype Cycles ismiyle büyük verinin dikkat çekmesidir" (a.g.e., 2014).

Bu teknik süreçlerin yanı sıra, sosyolojik temelde bakıldığında Lyotard, teknolojik dönüşümlerin bilgi üzerinde önemli olduğunu, araştırma ve aktarma anlamında çok ciddi değişikliklere sebep olduğunu belirtmektedir. Özellikle araçların minyatürleştirilmesi ve ticarileştirmesi, öğrenmenin edinilme, sınıflandırılma, kullanıma sunulma ve kullanıma biçimini değiştirmektedir. Ona göre bilgi işlem makinaları zamanla daha etkili bir hale gelecektir (1994). Post-modernite ile bu gelişimi açıklamaya çalışan Lyotard'ın "Post-Modern Durum" (1994) kitabında, kitabın önsözünü yazan Fredrick Jameson'un da bahsettiği şekilde, "geçmişin anlatıda tüketilmesi ile onun bilim ve bilimsel düşüncede depolanması, istiflenmesi ve sermayeye dönüştürülmesi arasında radikal bir farklılaşma" meydana gelmekte … mikro depolama, bilgisayarlı veri ve şimdiye kadar hayal edilemeyecek boyutlardaki veri bankalarının kontrolü ve hatta mülkiyeti bu alandaki atılımlarla birlikte günümüzün en önemli politik sorunlarından biri haline gelmektedir (1994). Lyotard bu anlamda büyük verinin ve bilginin dönüşümünü sosyolojik bakış açısıyla açıklayan önemli araştırmacılardan bir tanesidir.

Sosyolojik olarak büyük verinin yükselişini Tüfekçi, iç içe geçmiş 5 dinamikle birlikte değerlendirmektedir. Bu dinamikler: "Demografiden bireyselleştirilmiş hedeflemeye geçiş, bilişimsel modellemenin gücü ve anlaşılmazlığı, ikna edici davranışsal bilimin kullanımı, dijital medyanın dinamik gerçek zamanlı deney imkânı sağlaması ve veriye ya da sosyal medya çevrelerine sahip olan yeni siyaset simsarlarının oluşmasıdır" (Tüfekçi, 2014, s. 1). Tüm bu süreçlerle, büyük veri "herkes" hakkında veri toplama gücüne sahip olan ve kamusal alanda da onay mühendisliği yapılabilen bir sistem haline gelmektedir. Büyük verinin tartışma yaratan noktası, hedeflenmiş grupların yanı sıra kitlesel gözetim ve veri toplamaya olanak sağlamasıdır. Toplanan verilerin "ilgili herkesi içermesi" bir eşitlik olarak değil; herkesi gözetleme ve herkesin bir "hedef" ya da "şüpheli" olarak ele alınması düşüncesi temelinde büyük verinin sosyolojik bir

konu halini almasında önemli noktalardan biridir. Toplanan verilerin kim tarafından toplandığı, nasıl toplandığı, bireylerin ya da toplumların bu süreçteki onay mekanizmalarına katılımı ya da seçim şansı olup olmaması, devletlerin bu konuda aldığı önlemler ya da bilinç düzeyleri, uluslararası anlamdaki ilişkilerin bu süreçlerden nasıl etkilendiği ve özellikle bilişimsel modelleme anlamında güç sahibi olan devlet ya da üçüncü taraf kuruluşların kazandıkları gücün sorgulanması da büyük verinin büyük birader olarak değerlendirilmesi ve sorgulanması gerekliliğini ortaya koymaktadır. Elde edilen verilerin gerçek anlamda ikna etme ya da manipüle etme amacıyla kullanılmaya başlanılması, uluslararası birçok olayda kendini göstermekte (Facebook ve Amerikan seçimleri örneğinde olduğu gibi), dijital medyanın dinamik gerçek zamanlı deney imkânı sağlaması toplumsal, ekonomik, kültürel ve siyasal tüm zeminlerde güç dengelerini değiştirmektedir.

Bu çalışmada da vurgulanmaya çalışan şey, temel olarak kitlesel gözetim ve gözetim toplumlarının temellerinin en baştaki teknik süreçlerin yanı sıra, tarihsel olarak gerçekleşen toplumsal olaylarla bir araya gelerek farklı bir boyut kazanmasıdır. Sosyolojik olarak büyük verinin ve temelde gözetim sürecinin işleyişinin tarihsel gelişimine bakıldığında bu süreçlere katkı sağlayan süreçler şu şekilde ifade edilmektedir: “16. yüzyılda ulus-devletlerin ortaya çıkışı, transatlantik köle ticareti, bürokratikleşme, rasyonelleşme ve 19. ve 20. yüzyıllardaki modern yönetim şekilleri gözetim sürecinin işleyişinde etkili olmuştur. Buna ek olarak 20. yüzyıldaki risk yönetim pratikleri de bu süreçlere katkı sağlamıştır” (Brayne, 2017, s. 978). Basit ifadeyle, tüm bu tarihsel gelişmeler temelde gözetimin önem kazanmasına hem doğrudan hem de dolaylı olarak büyük verinin gelişim ve dönüşümüne yön vermiş belki de hız kazandırmıştır.

Büyük verinin ve algoritmik yönetim tartışmalarının temelini ise bir önceki bölümde bahsedildiği şekliyle Web 2.0’dan sonra meydana gelen değişim ve dönüşümlere katkı sağlayan katılımcı kültür anlayışı, kullanıcı odaklı içerik üretimi ve üretüketim süreçleri meydana getirmiştir. Sosyal medya

platformlarının ya da hukuki anlamda üçüncü tarafların sahip oldukları veri toplama, depolama ve işleme güçlerinin meydana gelmesi de algoritmik yönetim ve veri mahremiyeti konularında büyük verinin sosyolojik bir olgu halini almasında en etkili tartışmalar olarak yer almıştır. Bahsedilen UGT (Kullanıcı Odaklı İçerik Üretimi), yalnızca katılımcı kültürün değil yeni bir karar verme kültürünün de temelini oluşturmuştur. Büyük veri yeni bir karar verme kültürü meydana getirmektedir çünkü artık veri kısıtlı, sahip olmak için pahalı ya da dijital formda değilse, bir şirket ele alındığında "HiPPO" nun en yüksek maaş alan kişinin fikrine göre kararlar verilmektedir. Fakat yeni karar verme kültüründe, verinin ne söylediğine, verinin nereden geldiğine, ne tür analizlerden geçtiğine, sonuçlar konusunda ne kadar emin olunduğuna dair gibi güçlü sorular sorulduğunda artık veri en iyi tahminleri sunmaktadır (Mcafee ve Brynjolfsson, 2012, ss. 4-9).

Yeni karar verme kültüründe sorgulanması gereken sosyolojik kavramlardan bir tanesi, büyük veri kibridir ve doğrudan büyük verinin yıkıcı bir teknoloji olup olmaması sorusu ile ilişkilendirilmektedir. Büyük verinin bahsi geçen tüm alanlarda etkili ve güçlü bir araç olduğu düşünülürken, aynı zamanda bir sonraki yeni yıkıcı teknoloji olduğu ya da son zamanlarda moda olan bir kavram haline geldiği de literatürde sıkça belirtilmektedir. Bu düşünce özellikle "büyük veri kibri" (data hubris) kavramıyla literatürde göze çarpmaktadır. Büyük veri kibri bahsedilen ilgi sebebiyle, araştırmacıların veri analizindeki geleneksel yöntemleri tamamen bir kenara bırakarak, geçerlilik ve güvenilirliği hesaba katmadan ya da verinin içeriğini dikkate almadan tamamen büyük veriye odaklanarak yanlış sonuçlara ulaşmasıdır. Bundan kaçınmak için aynı zamanda teknolojik, yasal ve ekonomik bakış açısını birleştiren interdisipliner bir tavır alınmalıdır (Scherman, Krcmar, Hemsen vd., 2014, ss. 261-263). Bauman ve Lyon bunu şu şekilde değerlendirmektedir: "Bugünün gözetimini yönlendiren istatistik ve yazılım mantığı tekinsiz bir tutarlılıkla sonuçlar ortaya çıkarır. Yalnızca 'Araplar' ve 'Müslümanlar' havaalanlarında diğer insanların maruz kaldığından fazla 'rastgele' incelemeye maruz kalmaz; aynı zamanda Oscar Gandy'nin de belirttiği gibi, çağdaş tüketici gözetimi tarafından oluşturulmuş

toplumsal sınıflandırma, bir çeşit ‘giderek artan dezavantaj’ dünyası inşa eder” (Bauman ve Lyon, 2020, s. 25). Bahsedildiği şekilde büyük verinin avantajlı ya da dezavantajlı noktaları ele alındığı zaman, büyük verinin tek başına işleyen bir “güç nesnesi” ya da “sermaye” olmadığını özellikle nesnelerin interneti, yapay zekâ, robotik ve blokzincir teknolojisi gibi teknolojilerle de desteklendiğinin ve nasıl desteklendiğinin bilinmesi önem taşımaktadır. Bu amaçla bir sonraki kısımda büyük veriyi destekleyen sistemlerden kısaca bahsedilmektedir. Özellikle yapay zekanın büyük veriden güç alarak farklı sosyal sistemler kurulduğu puanlama sistemi gibi önemli gelişmelere yol açması da bu tezin yazılmasının en önemli nedenlerinden biridir. Büyük verinin bu araçlarla desteklenmesinin yanısıra, temel olarak onun bu kadar etkili kullanımının nasıl gerçekleştiğini açıklamak için ise büyük veriyi destekleyen sistemler verildikten sonra, büyük veri analizi açıklanmaya çalışılmaktadır.

2.1.2. Büyük Veriyi Destekleyen Sistemler

2.1.2.1. Nesnelerin İnterneti ve Bulut Bilgi İşlem

Nesnelerin İnterneti, internetle bağlantılı olan her şey olarak tanımlanabilmektedir. Basit sensörlerden akıllı telefonlara ve giyilebilir cihazlara kadar birbirine bağlı cihazlardan oluşmaktadır. Nesnelerin İnterneti bu anlamda bir önceki kavramsal tanımlamalarda yer aldığı gibi, üretüketim kavramında en etkin yeni teknolojilerden bir tanesi olarak görülmektedir. İnternetle bağlantılı olan her şeyi yalnızca bireyler ya da kitleler üzerinde gözetim mekanizmaları kurmak amacıyla değil başka amaçlarla da kullanmaktadır. “Bu bağlı cihazları otomatik sistemler ile birleştirerek, belirli bir görevi olan birine yardım etmek ya da bir süreci öğrenmek için bilgi toplamak, analiz etmek ve bir eylem oluşturmak mümkündür. İşlevine bakıldığında ise, yapay zekâ, konuşma tanıma, görüntü işleme ve otonom sistemler gibi robotik teknolojiyi besleyen unsurların gelişmesine ve daha hızlı, daha güçlü, daha akıllı robotların tasarlanmasına imkân sağlamaktadır” (UİB, 2017, s. 2). Heterojenliği, büyüklüğü, gerçek zamanlı oluşu ve mahremiyet özellikleriyle büyük veriyi analiz etme, modelleme, görselleme ve öngörü yapma gibi analizin farklı seviyelerini etkili bir şekilde

araştırıp bulmak (“mine”) için Bulut Bilgi İşlem ve Nesnelerin İnterneti de aynı şekilde büyümüştür. Bulut Bilgi İşlem, veri varlığı için gerekli site ve kanallara ulaşımda koruma sağlarken; Nesnelerin İnterneti, tüm dünyada toplanan ve işlenen verinin bulutta depolanması ve işlemesini sağlamaktadır (Chen, Mao ve Liu, 2014, s. 172). Teknik tanımlarda da bahsedildiği gibi, özellikle sosyal medya platformlarında yer alan sosyal öneri sistemlerinin de bu sistemler tarafından büyük bir şekilde desteklendiği bilinmekle birlikte, algoritmalar oluşturulurken Nesnelerin İnterneti ve Bulut Bilgi İşlemin rolünün önemi belirtilmektedir. Spam filtreleme, ağ araması, tıklama dizisi analizi ve dijital sosyolojide de en çok analiz edilmeye çalışılan sosyal öneri sistemleri için yukarı da ismi geçen Hadoop gibi sistemlerin kurulduğu bilinmektedir.

Lokke, Nesnelerin İnternetinin hayatımıza getireceği değişiklikleri şu şekilde açıklamaktadır. İlk olarak nesnelerle iletişime girmemizi sağlayacaktır; örneğin kullanılmış bir bisiklet alındığında kim, nerelerde, kaç kilometre kullanmış gibi veriler ulaşılabilir hale gelecektir. İkincisi nesneleri gözlemleme ve denetleme imkânı sağlar; buna örnek olarak kalp pili olan bir bireyin kalp pilinde arıza çıktığında ambulansa otomatik olarak mesaj çekilebilir bir duruma ulaşılması verilmektedir. Üçüncü olarak, anahtarımızı ya da bisikletimizi aramak için kullanılabilecektir. Dördüncüsü, şehir planlaması, trafik, hava kirliliği ve etkin elektrik dağıtımı gibi konuların daha kolay hale gelmesini sağlamasıdır. Sonuncusu ise insanların oyun ve eğlence ihtiyacını karşılamasıdır (2020, s. 31).

2.1.2.2. Yapay Zekâ

Makinelerin insanlar gibi düşünmesini hedefleyerek tasarlanan sistemlerdir. İnsan beyni düşünülerek, incelenerek, akıllı yazılım sistemleri ile bağlantılandırılarak gerçekleştirilir. “Yapay zekâ, insanın düşünme yapısını anlamak ve bunun benzerini ortaya çıkaracak bilgisayar işlemlerini geliştirmeye çalışmak olarak da tanımlanabilir. Bu programlanmış bir bilgisayarın düşünme girişimidir. Daha geniş bir tanıma göre ise, yapay zekâ, bilgi edinme, algılama,

görme, düşünme ve karar verme gibi insan zekasına özgü kapasitelerle donatılmış bilgisayarlardır. Yapay zekâ, insanlar tarafından yapıldığında zekâ gerektiren şeyleri gerçekleştiren makineler yapma bilimidir" (Pirim, 2006, s.81 akt. Demir, 2012). Yapay zekâ ile büyük veri ilişkisine bakıldığında ise büyük hacimli verilerin olduğu durumlarda yapay zekâ; zor örüntü tanıma, öğrenme ve diğer görevlerin bilgisayar tabanlı yaklaşımlara devredilmesine izin vermektedir. Örneğin, dünyadaki hisse senedi alım satımlarının yarısından fazlası yapay zekâ tabanlı sistemler kullanılarak yapılmaktadır. Ayrıca yapay zekâ, diğer kararlara yol açan hızlı bilgisayar tabanlı kararları kolaylaştırarak verilerin hızına katkıda bulunmaktadır (O'Leary, 2013).

2.1.2.3.Robotik

Bilgisayarlar ve robotların birleşimi ile robotlara çeşitli hareketlerin öğretilmesi ve bu robotların çeşitli alanlarda çalışmalarını sağlayan yapay zekâ destekli bir teknolojidir. Günümüzde karar verme ve kendi hareket edebilme becerisini geliştirebilmeleri için çalışmalar gerçekleştirilmektedir. "Eğer bu robotlara görme, konuşma gibi beşerî algılama becerileri kazandırılırsa, bu robotların insan gibi davranması ve böylece bu robotlara akıllı denmesi de mümkün olabilecektir" (Demir, 2012).

2.1.2.4. Blokzincir Teknolojisi

Blokzincir teknolojisi, Lokke tarafından, "özünde bu teknoloji, güvene dayalı ilişkinizin olmadığı kişi ya da kurumlarla bağlantı kurmanızı mümkün kılar" şeklinde açıklanmaktadır (2020, s. 38). Güven vurgusunun sebebi, bu teknolojinin "farklı halkaların değiştirilemez ya da bir kez uygulamaya konduğunda etkilere kapalı, emsalsiz veriler içermesidir" (a.g.e., s. 38). Kullanıcılar veri oluşturup yayınladıkça, verilerin de ana sahipleri olarak kalmalıdırlar. Kullanıcıların eylemleri ve ilgi alanları izlenerek yapılan gözetim konusunda, kullanıcıların en azından bu konuda bilgi sahibi olması ve bazı faydaları olması gerekir. Blokzincir, özel verilere erişim izinleri için bir filtre

olarak kullanılabilmekte veya tamamen merkezi olmayan bir sosyal ağ uygulayabilmektedir (Karafiloski ve Mishey, 2017). “Blokzincir, isimsiz işlem ve ilişkilerin önünü açar ki bu da vatandaşların mahremiyeti açısından olumludur. İkinci olarak, blok zincir teknolojisi, NSA itirafları ve Panama Belgelerinde olduğu gibi, sansürlenmesi neredeyse mümkün olmayan bir kanal oluşturabilir. Bu durum, ihbarcılar ve basın özgürlüğü için olumludur ancak aynı zamanda kişisel, hassas bilgileri bu teknoloji tarafından ortaya dökülecek insanların özel hayatına karşı büyük bir tehdidi de beraberinde getirir. Sistemin parçası olmayan kişiler bile, hassas bilgilerinin geri dönüşü olmayan bir şekilde ortalığa dökülmesi riskiyle karşı karşıya kalabilir, bu da mahremiyeti çok büyük bir riske atacaktır” (Lokke, 2020, s. 39). Blokzincir Uzmanı ve Ekonomist Dr. Magdelena Ramada Sarasola’nın ifadesiyle aynı zamanda “Blokzincir sosyolojik bir yenilik. Bu teknoloji, internet üzerinde değer aktarımı ve işlem yapmamızı daha önce yapmadığımız şekilde ağlar vasıtasıyla gerçekleştirmemizi sağlamaktadır” (Konish, 2018).

2.1.3. Büyük Veri Analizi

Büyük Veri Ayrımı kısmında detaylı olarak bahsedileceği üzere, literatürde “Teorinin Sonu” tartışması olarak yer alan haliyle yeterli veri, sayıların kendi adına konuşması ve teoriye gerek kalmaması gibi bir soruyu ortaya çıkarmaktadır. Bu tartışma yapılırken, büyük veri analizinin mevcut olan tüm gerekli ve gereksiz, alakalı ve alakasız toplanan verinin (“found data”nın), analizinin yapılması gerekliliğidir. Analizde kullanılacak veri karışık ve dağınık bir şekilde sürekli olarak güncellenen ve eş zamanlı olarak büyüyen bir veri olması, arama motorlarından yapılan aramalar, hareketli tüm cihazlardan yapılan konum bilgileri, ulaşılabilen mesajlaşmalar, sosyal medya platformlarından kullanıcı tarafından üretilen içerikler gibi her tür veridir.

Harford’un ifade ettiği şekilde büyük veri analizinde giderek büyüyen veri problemleri yer almaktadır. Google’ın yürütmeye çalıştığı Grip Trendleri tespit etme örneğindeki gibi, odaklanılan şeyin nedensellik değil, yalnızca sayısal

korelasyonlar olması, mantıksal önerileri ortadan kaldırmakta ve teoriden uzak bir analize yol açmaktadır. İstatistiksel olarak da bu tür analizler örnekleme hataları (sampling error) ve örneklem yanlılığına (sampling bias) yol açmaktadır. İlki çıkarım yapılmak istenen örneklemin temel evreni yansıtmaması durumuyken, ikincisinde örneklem rastlantısal bir şekilde bile seçilmemektedir (2014, ss. 14-17). Büyük veri analizinde karşılaşılan en büyük sorunlardan bir tanesi bu anlamda bakıldığında gerçeğin veri madenciliğine yönelmek yerine, doğrudan büyük veri madenciliğine sorgusuz sualsiz bir şekilde odaklanmaktan kaynaklanmaktadır. Açıklama ve nedenselleştirmenin yerini alan korelasyon ve tahmin amacı büyük veri analizini ve büyük veri kullanımını en çok etkileyen unsurlar olarak göze çarpmaktadır.

Büyük veri analizinin sağladığı avantajlar; zamandan tasarruf edilmesi, ihtiyaçların ve çeşitliliğin tespit edilerek performansın iyileştirilmesi, promosyon ve reklamcılıkta daha iyi hedef tutturulabilmesi ve otomatik algoritmalar sayesinde insanların karar verme mekanizmalarında daha etkili olmasıdır. Fakat bu avantajların yanı sıra büyük veri güvenlik sorunları taşımaktadır; özelikle hassas verinin işlenmesi ve toplanması bunun örneklerinden bir tanesidir. Verinin kontrolü ve korunmasının sağlanması ve bunun için gerekli olan veri koruma kanunlarının geliştirilmesi gerekmektedir (Tankard, t.y., s. 5). Nesnelerin İnterneti, robotik, biyometri, ikna edici teknoloji, sanal ve artırılmış gerçeklik ile dijital platformlar da mahremiyet, özerklik, güvenlik, insan onuru, adalet ve güç dengesine ilişkin ihlal riskleri taşımaktadır (Royakkers, Timmer, Kool&vanEst, 2018 akt. Puaschunder, 2019).

2.1.4. Geleneksel Veri Entegrasyonu ve Büyük Veri Entegrasyonu

Literatüre bakıldığında veri entegrasyonu aşamasında, veri temelli karar verme mekanizmalarını oluşturma sürecinde, toplanan verilerin bir araya getirilmesi ve ilişkilendirilmesi söz konusudur. Veri entegrasyonu, çeşitli unsurlara bağlı olarak geleneksel veri entegrasyonu ve büyük veri entegrasyonu olarak iki farklı

kavramla açıklanmaktadır. Büyük veri entegrasyonu, geleneksel veri entegrasyonundan özellikle veri kaynaklarının sayısı, veri kaynaklarının dinamik oluşu, heterojenliği ve farklılaşan nitelikleri bakımından ayrılmaktadır. Büyük veri entegrasyonunda, bu çerçevede bir önceki kısımda açıklanan önceki dönemlerde 3V, güncel olarak ise 4V olarak tanımlanan veri nitelikleri etkin özelliktedir.

2.1.4.1. Verinin Hacmi (Volume), Hızı (Velocity), Çeşitliliği (Variety) ve Doğruluğu (Veracity)

Güncel olarak büyük veri entegrasyonundaki verinin 4 niteliği; verinin hacmi, hızı, çeşitliliği ve doğruluğu olarak açıklanmaktadır. Verinin hacmi, yalnızca her veri kaynağının çok büyük boyutlarda veri içermediğini, aynı zamanda çok sayıda veri kaynağı içerdiğini kastetmektedir ve giderek artmaktadır. İstatistikçilerin tahminlerine göre 2009 senesi ile karşılaştırıldığında dünya üzerindeki verinin 2020 itibariyle 44 kat büyümesi beklenmektedir, bu da 0.8ZB'den 35ZB'ye bir artışı göstermektedir (Subudhi, Rout ve Ghosh, 2019, s. 26131). Hacim yalnızca üretilen veri miktarını değil, bu verinin değerini ve potansiyelini de işaret ettiği için önemli olan bir kavramdır. Verinin hacmi arttıkça değer ve potansiyel anlamında da değişimlerin meydana geldiği görülmektedir. Bu sebeple, geleneksel veri entegrasyonu ile karşılaştırıldığında, büyük veri entegrasyonunda veri kaynağının çok daha fazla olduğu ve entegrasyonun içeriğinin tamamen değiştiği bilinmektedir.

Hız ile açıklanmak istenen ise, sürekli dinamik halde bulunan veri kaynaklarının sürekli toplanması ve sürekli ulaşılabilir olmasıdır. Verinin hacmi ve çeşitliliği arttıkça, bu veriyi işlemek, depolamak ve analiz etmek için gerekli olan alt yapıların da değişmesi gerektiği, bu anlamda bir talep doğduğu göze çarpmaktadır.

Çeşitlilik ile veri kaynaklarının heterojen yapısı kastedilmektedir. Heterojen yapı denildiğinde ise genellikle verinin yazı, sayı, resim, ses temelli, video, sosyal

medya verisi, yer verisi gibi farklı olma durumundan bahsedilmektedir. Bu verilerin sınıflandırılması da bu sebeple çeşitliliğe dayanmaktadır. Bu verilen yapılandırılmış, yarı-yapılandırılmış ya da yapılandırılmamış olarak sınıflandırıldığı da söylenmektedir.

Son olarak doğruluk ile veri kaynaklarının, farklılaşan nitelikleri ve verinin zamansızlığı, netliği ve kapsamındaki önemli farklılıkları vurgulanmaktadır (Dong ve Srivastava, 2013, s. 1245).

Subudhi, Rout ve Ghosh, 4V kavramının mevcut durumda 7V kavramıyla değiştiğini ve ele alınması gereken yeni kavramlar olduğunu belirtmektedir. Bunlar; değişkenlik (variability), gerçeklik (veracity), vizkozite (viscosity) ve virallik (virality) kavramlarıdır (2019, s. 26162). Yapılan örneklendirmeye göre, çeşitlilik 5 farklı marka kalemken, değişkenlik aynı marka kalemin birçok renginin olabileceğinin göz önüne alınmasıdır. Değişkenlik bu durumda verinin yönetiminde önemlidir ve bir tweet veri olarak ele alındığında bile farklı durumlarda farklı anlamlar taşıyabilme durumunun göz önüne alınması için gerekli bir kavram olarak görülmektedir. Gerçeklik kavramı 4V içinde bir üst paragrafta ele alınmakla birlikte, 7V içerisinde de özellikle karar verme mekanizmalarında doğru analize ulaşabilmek için önemli bir diğer unsur olarak açıklanmaktadır. Vizkozite ise veri toplama aşamasındaki durgunluğa işaret etmektedir. Verinin hacmi ve çeşitliliğiyle baş edebilmek için alınabilecek önlemleri göze alma gerekliliğini temsil etmektedir. Son olarak virallik kavramı, ağ üzerindeki tüm veri akışını kastetmektedir (age, s. 26133).

2.1.4.2. Şema Kartografisi, Rekor Bağlanış, Veri Tümleştirme

Büyük veri entegrasyonunda şema kartografisi ile küresel bir şema oluşturabilme ve küresel şema ile veri kaynaklarının yerel şemaları arasında yapılan haritalandırmalar açıklanmaktadır. Geleneksel veri entegrasyonunda şema kartografisi için büyük efor gerekirken, bu efor büyük veri entegrasyonunda çok daha fazla artmıştır. Bunun için Hadoop gibi sistemler

kullanılmaktadır. Rekor bağlanış ise, aynı şemaya sahip yapılandırılmış kayıtların bağlantısına odaklanmaktadır. Büyük veri entegrasyonu ile özellikle veri kaynaklarının yapısal olarak heterojen olması ve tweetler, bloglar, postlar gibi birçok yapılandırılmamış yazı verisi içermesi, veri kaynaklarının sürekli hareketli ve dönüşüm geçiren yapısı sebebiyle rekor bağlanış açısından daha zorlayıcı hale gelmesi kastedilmektedir. Rekor bağlanış, geleneksel veri entegrasyonunda yetersiz kalırken, büyük veri entegrasyonunda MapReduce gibi güncel sistemleri kullanarak geliştirilmiştir. Veri tümleştirme, ilk iki kavrama göre daha güncel bir kavramdır. Daha çok verinin doğruluğuna odaklanmaktadır. Bu kadar büyük veri yoğunluğunun arasında hangi verinin ne kadar doğru olduğunu ayırt etme süreci olarak değerlendirilmektedir (Dong ve Strivastava, 2013, ss. 1246-1247).

Sosyolojik olarak da bu kavramların yabancı olmadığı, kuramsal çerçevede de Deleuze'ün Rizomatik Bağlantılar ya da kartografi gibi kavramlarıyla bağlantılandırılarak toplumsal temelde çok fazla anlam taşıdığı görülmektedir. "Askeri, eğitsel, ekonomik ya da idari amaçlarla toplanan her tür kişisel bilgi bir araya getirilerek söz konusu bireyin profili ortaya çıkarılmaktadır. Deleuze'ün tanımladığı biçimde, rizomatik, her yere yayılabilen, sınırsız genişleme gücü olan bir yapıya sahiptir" (Yücedağ, 2017, s. 170). Bireylerin profillerinin çıkartılması ise bir tür sınıflandırma ve haritalandırma, kartografi, yapılmasına imkân sağlamaktadır. Bu durumda temel olarak bireylerde veri manipülasyonunun ya da veri ihlalinin temelini oluşturduğu için sosyolojik olarak önem taşımaktadır. Bireylerin sosyal ilişkilerini, toplumların yönetilme şekillerini, insanların yönlendirilme ihtimallerini ve pek çok süreci etkilemektedir.

2.1.4.3. Verinin Değeri

Büyük veri analizi ya da büyük veri entegrasyonunda verinin nereden geldiği değil, verinin ne anlam ifade ettiği önemlidir. Verinin değeri olarak isimlendirilen kavramla, verinin araştırılan durum ile ilgili araştırmacılara verdiği bilgi ve hacim, hız, çeşitliliğin yanı sıra bu verinin doğruluğunun tespiti ile gerçekleştirilen

korelasyonlardaki işlevi kastedilmektedir. Verinin değeri göz önüne alınmadığında, kuramsal çerçevede teorilerle de destekleneceği şekliyle, büyük verinin kullanımı bir çeşit yıkıcı, manipüle edici ya da kontrol için kullanılan güç haline dönüşme potansiyeline sahiptir. Aşağıdaki tabloya bakıldığında büyük verinin yıkıcı bir teknoloji olarak değerlendirilmesi, yıkıcı teknoloji özellikleri tanımlanarak yapılmaktadır. Daha sonraki bölümlerde bu değerlendirmenin çalışmadaki tüm gelişmelerle tekrardan yapılması hedeflenmektedir.

Tablo 4. Büyük Verinin Yıkıcı Bir Teknoloji Olarak Değerlendirilmesi

Yıkıcı Teknolojilerin Özellikleri	Büyük Veri Değerlendirmesi
Teknoloji, geleneksel değerlendirme kriterlerine göre yerleşik teknolojilerden daha kötü performans göstermektedir.	Geleneksel veri analizi teknolojileri, geniş bir kullanıcı yelpazesi için açıklayıcı diller aracılığıyla çalıştırılabilir. Ancak, büyük veriler, şu anda yalnızca uzmanlar tarafından oluşturulabilen ve yorumlanabilen olasılıklı sonuçlara yol açmaktadır.
Teknoloji, yeni değerlendirme kriterleri getirmektedir.	Büyük veri, daha az zamanda farklı formatlara dayanan büyük veri setlerinin analizine imkân sağlamaktadır.
Teknoloji, genel kullanıcılar tarafından dikkatle gözlemlenmektedir.	Büyük veri ile ilgili birçok örnek ve pilot uygulama mevcut olsa da kurumların ana süreçleri henüz odakta yer almamaktadır.
Teknoloji, başlangıçta start-uplar ve kariyerini ya da işinin odağını değiştiren kişiler tarafından sunulacak ve kullanılacaktır.	Büyük veri teknolojileri kullanıcıları, genellikle bu teknolojiyi yeni iş modelleri için fırsat olarak gören küçük işletmelerdir. Büyük veri teknolojisi sağlayıcıları arasında start-uplar ve yerleşik teknoloji sağlayıcıları vardır.
Teknoloji, yeni değer oluşturma süreçlerinde değişimlere yol açmaktadır.	Büyük veri alanında çeşitli yeni roller yaratılmaktadır.

(Christensen, 1997 akt. Scherman, Krchmar vd., 2014, s. 265)

2.1.4.4. Veri Madenciliği

2.1.4.4.1. İçeriğin Tanımlayıcı Veriye (Meta-Data) Dönüşümü

Lokke, üst veri ya da metaveri tanımını şu şekilde yapmaktadır: “Üst veri, dijital ekosistemdeki bir bilgi kaynağını, örneğin e-postayı tanımlayan, açıklayan, yerini belirten ya da ona erişmeyi, kullanmayı ve onun yönetimini kolaylaştıran bilgidir” (Teknoloji Kurulu ve Veri Koruma Kurumu, 2014 akt. Lokke, 2020, s. 40). Metaveri ya da üst verinin sosyoloji ve dijital gözetimle olan ilişkisi ise metaverinin kitlesel gözetimin arka planında çok önemli bir unsur olarak görülmesidir.

Kişiler hakkında toplanan bu bilgilerin, özellikle Snowden Olayı ile bu kavram aracılığıyla ilişkilendirildiği ve gözetimle bağlantılandırıldığı ise Gartner tarafından açıklanmaktadır. Buna göre, “metaveriler, Snowden Olayı sırasında medyada yaygın olarak kullanılan bir terim haline geldi. Ancak metaveri tam olarak nedir? The Guardian Gazetesi, Haziran 2013'te metaverileriniz için bir Guardian kılavuzu yayınladığında okuyucuları için bu konuyu açıklığa kavuşturmaya çalıştı: Metaveriler, ’siz teknolojiyi kullandıkça oluşturulan bilgilerdir... kişisel veya içeriğe özgü ayrıntılar değil, daha çok kullanıcı, cihaz ve gerçekleştirilen faaliyetler hakkında işlemsel bilgilerdir’" demiştir (Gartner, 2016).

Newell ve Tennis ise gözetimin temelinin, metaverileri, kamusal veya özel yaşamlarımızı belgelemek için oluşturulan çeşitli dijital bilgi parçaları hakkındaki bilgileri kapsadığını ve bu bilgilerin çoğunun, ilgili görevlerini yerine getirmek için hakkımızda bilgi madenciliği yapmakla ilgilenen devlet kurumları ve pazarlama şirketleri ile paylaşılan büyük elektronik veri tabanlarında saklanmakta ve depolanmakta olduğunu belirtmektedir (2014).

Metaveriler ve içeriğin, dijital gözetim ve büyük veri anlamında ne ifade ettiğine bakıldığındaysa ikisinin de kitlesel gözetim için çok önemli olduğu, ama metaverinin çok hızlı bir şekilde bireyler hakkında veri toplamak için etkin bir

teknik olduğu belirtilmektedir. Metaverinin özellikle 4. Paradigma ya da kullanıcı odaklı içeriğin gelişimiyle, sosyal medya platformlarının gelişimi ile arttığı bilinmektedir. Bireylerin bilgileri çeşitli sistemler tarafından dolaylı olarak toplanırken; bu sistemlerle birlikte bireyler kendi içeriklerini kendileri üreterek, verileri de kendileri üretmeye başlamış sisteme doğrudan dahil olmuşlardır. Doğası gereği metaveriler daha kolay analiz edilebilir ve toplanabilir, biçimleri standardize edilmiş ve çoğu sayısal ve niceliksel analize tabi tutulabilir haldedir (Bernal, 2016). Buna ek olarak, içeriğin dolaylı biçimlerle, kolayca veya otomatik olarak anlaşılamayan bir dille yazılması da önem taşımaktadır. Kitlesel gözetimin öngördüğü ölçek türlerinde, içeriği gerçekten "okuma" veya "dinleme" fikri, analizin en son aşamalarına kadar pratik değildir. İçerik, metaverilerden çok daha kolay ve düzenli bir şekilde şifrelenir. Son olarak, metaveriler coğrafi konum verileri, kullanılan cihazlarla ilgili veriler ve benzeri gibi yeni veri türlerini içerebilmektedir (age, 2016).

Lokke ise içerik ve metaveri arasındaki ilişkiyi çok basit bir şekilde açıklamakta, içeriğin üst verilerin bir araya getirilen hali olduğunu gösterirken şöyle bir örneklendirme yapmaktadır. Bir kişi doktorla görüşmüş, ardından HIV bilgisini araştırmış, daha sonra eczaneye e-posta atmışsa çapraz bağlantı yapıldığında bu durum, bu kişi hakkında birçok bilgi edinilebileceğini göstermektedir (Lokke, 2020, s. 42). Snowden Olayında büyük yankı uyandıran nokta ise, NSA'nın telefon dinleme veya e-postaları dinleme gibi klasik teknikleri kullanmadığı, bunun yerine telefon konuşmaları, kısa mesajlar veya e-postalar hakkında bilgi topladığının söylenmesidir (Gartner, 2016).

2.1.4.4.2. Sayısallaştırma

Dijital sosyolojide, dijital toplumun oluşma sürecinde iki önemli kavram yer almakta ve bu iki kavram birbirine İngilizce terminolojide çok benzemektedirler. ‘Digitization ya da digitisation’ olarak kullanılan kavram sayısallaşma anlamına gelmektedir; insanlar ile ilgili toplanılan bilgilerin, büyük verinin algoritmalar aracılığıyla toplanmasıyla, insan hareketinin ve hatta duygusunun sayısal

verilere dökülmesidir. Bu durum sonucunda oluşan tüm sosyal, kültürel, siyasal ve ekonomik koşulların insanlarda ve toplumda yarattığı sürece ise ‘digitalization’ dijitalleşme denilmektedir (Özuz, 2018, s. 55).

2.1.4.4.3. İşlevsel Fayda

İnsanların özellikle algoritmalar kullanılarak, sosyal öneri sistemi ve bahsi geçen tıklama dizileri analizleriyle çeşitli hedeflerde ulaşılmaya çalışılan faydayı temsil etmektedir. Bir anlamıyla işlevsel fayda, insanlar hakkında dijital gözetim yoluyla elde edilen bilgilerin onların film izlemeleri, kitap almaları, bazı linklere tıklamaları gibi ekonomik hedeflere ulaşmakken; bu çalışma kapsamında “iyi bir vatandaş”, “iyi bir insan” gibi çeşitli statülerle değerlendirilebilmek gibi farklı yönlere evrilmesi noktasında tartışılmaktadır. Bu tür analizlerin işlevsel fayda ile yapılabilmesine imkân veren sistem, karar verme mekanizmaları ise veri temelli karar verme mekanizmaları ya da veri madenciliği destekli karar verme mekanizmaları olarak açıklanmaktadır. İşlevsel faydanın her zaman iyi niyet ve iyi amaçlarla kullanılmadığı, kurumların ya da çeşitli güçlerin amaçları doğrultusunda bu amacın değiştiği bilinmektedir.

2.1.5. Veri Temelli-Veri Madenciliği Destekli Karar Verme Mekanizmaları

Veri madenciliği destekli karar verme mekanizmaları, büyük veri gözetimi için gerekli olan gözetim kaynaklarının büyük veriyi elde etmeye yarayan diğer mekanizmalarla toplanması, depolanması ve daha sonra gerekli analiz araçlarıyla değerlendirilmesi sürecinin sonucunda ortaya çıkan mekanizmalardır. Bu mekanizmalar veri gözetimi temelli olarak birçok alanda kullanılmaktadır. Andrejevic ve Gates’in tanımlamalarına göre bu mekanizmalar, hastalık dağılımlarını takip etme ve değerlendirme, iş trendlerini takip etme, suç kalıplarını haritalandırma, web trafiğini analiz etme gibi hava durumundan bireylerin ekonomik pazarlardaki davranışlarına kadar her şeyi tahmin etme gibi farklı alanlarda kullanılmaktadır (2014, s. 185). Büyük veri analizinde

sorgulanması gereken, bu mekanizmaların kimler tarafından ve hangi amaçlarla kullanıldığı ve verisi elde edilen birey ya da kitlelerin veri mahremiyeti konusundaki rıza ve bilinçleriyle ilgilidir.

Fakat her şeyi tahmin etme imkanının sınırlarını sorgulama gerekliliği literatürdeki birçok çalışmada özellikle vurgulanmaktadır. İki değişken arasında bir çeşit korelasyona ulaşılabilir olduğu, bu değerlendirmenin doğru olduğunu desteklemek için yeterli değildir. “Zizek, Lacan’ı takip ederek “işlevsel bilgi olamayan şeyleri, Sembolik Gerçeğin Alanı olarak tanımlamaktadır: Anlamsız bilimsel formüller Sembolik Gerçeklerdir… kuantum fiziğini anlayamazsınız (örneğin), bunu anlam ufkumuza çeviremezsiniz; bu sadece basitçe işleyen bir formül içermektedir”. Algoritmik korelasyonlar ve tahminler de böyledir: Bize altta yatan sağduyuya dayalı açıklamalar sağlamazlar fakat bazı durumlarda, anlaşılmaz olan, onları daha karmaşık yapan bulguları anlamamızı sağlarlar (Zizek ve Daly, 2004, s. 97 akt. Andrejevic ve Gates, 2014, s. 185).

Büyük veri analizini temel alan veri madenciliği destekli karar verme mekanizmalarında bu anlamda korelasyonun açıklama ve nedenselleştirmenin yerini alması ve tahmin amacına ulaşma hedefi en büyük sorunlardan bir tanesidir. Bu sorunun boyutları kavramsal çerçevenin diğer bölümlerinde ve özellikle veri gözetimi ile ilgili kısımlarda belirtilmektedir.

2.1.6. Verinin İkincil Konuma Tabii Tutulmaması (Data Antisubordination)

Literatürde büyük veri kavramıyla birlikte en çok tartışılan konu dâhiliyet meselesiyken, özellikle mahremiyet ve sivil haklara vurgu yapılırken, odaklanılması gereken konulardan birinin bunların tam aksi olan dışlanma konusu olduğu, büyük verinin eşitliğe ve mahremiyete karşı tehdidine yönelik “Veriyi İkincil Konuma Tabi Tutmama Doktrini” olması gerektiği belirtilmektedir (Lerman, 2013, s. 55). Artan verileştirme insanların deneyimlerini, gelecek tutumlarını tahmin etme ve buna yönelik çeşitli uygulamalar yapma gibi

durumlara imkân sağlamaktadır. Fakat büyük verinin tek karanlık yanı verileştirme değildir. Lerman'ın önerdiği şekliyle büyük veri: "Sivil hakların devlet tarafından kötüye kullanımına; uzun süreli mahremiyet normlarının aşınmasına ve büyük verinin işlenmesinde harcanan büyük enerjiden sorumlu "server farms"ların çevreye hasar vermesine yol açmaktadır" (2013, s. 56). "Data antisubordination" kavramıyla tartışılmak istenen meselede ise, büyük veriye dahil edilmeyen ve bu çizgilerin dışında yaşayan tüm insanlar kastedilmektedir. Yoksulluk, coğrafya, hayat şekli ya da hayatları bir şekilde daha az verileşmiş olanların genel nüfustan soyutlanması ve hatta marjinalleştirilmesi imkânı bulunmaktadır. Marjinalleştirmenin ise bu insanlarının seslerinin duyulmamasına yol açılabileceği düşünülmektedir. Ekonomik fırsatların, sosyal mobilitenin, demokratik katılımın bile büyük veri ve yeni teknolojiler doğrultusunda gelişebileceği kuvvetli öngörüler arasında yer almaktadır. Veriyi İkincil Konuma Tabi Tutmama Doktrini bu anlamda, özellikle büyük verinin yeni sosyal tabakalaşmalara yol açmaması için, devletlerin kamusal mal ve hizmetlerden herkesin eşit yararlanmasını garanti etmesi, hukuki anlamda yargılamada ve siyasi süreçlerde eşitlik sağlaması, hatta bir devlet eylemi olmaktan çıkarak özel sektörde de bunun için önlemler almasıdır (age, ss. 60-63). Lokke, Taylor Armending'in bir makalesine atıfta bulunarak büyük veri ile bağlantılı beş büyük sorunu ayrımcılık (her bireyin aynı olanaklara sahip olamaması), güvenlik ihlali (bilgilerin sızdırılması), anonimliğe veda (anonim kişilerin kimliğinin yeniden tanımlanabilmesi), devlete verilen geniş yetkiler (yetki sorunu), düzenlenmemiş bilgi işlem (saydamlık ya da doğru işlendiği garantisi olmaması) olarak tanımlamaktadır Bu analizlerle, güvenlik tehlikesi oluşturan kişilerin kimler olduğu, kimin kredi verilebilir olduğu, kimin çeşitli işlere uygun olduğu ve ne kadar sigorta pirimi ödeyeceğine karar vermek mümkün olmaktadır (Lokke, 2020, s. 65).

2.1.7. Büyük Veri Ayrımı

Büyük verinin sosyal bilimler açısından en önemli yanı, literatür taraması yapıldığında da göze çarptığı gibi, sosyal öznenin çoğunlukla izni dışında ya da

yeterli bilgiye ve bilince sahip olmadan ya da doğrudan sistemlerden uzak kalmamak için kabullenmişlik duygusuyla verilerini paylaşmaya bir nevi “onay” vermesi ve bu rıza algısının sürekli sorgulanmasıdır. Büyük veri yapay zekâ, robotik ve blokzincir teknolojisi kısımlarında bahsedildiği gibi, onu destekleyen tüm sistemlerde makinelerin bireyleri onları kendilerinden daha iyi bilmesi algısı oluşturmasından dolayı çoğunlukla tehlikeli görülmekte ve gelecekte ne amaçlarla kullanıldığının bilinememesinden kaynaklanmaktadır. Kişisel bilgi ağlarının oluşumu yalnızca bireylerin bir alandaki hareketleri ile değil, tüm kişisel aygıtlarla, sosyal ağlarla, diğer tüm uygulama ve aygıtların birleşimi ile meydana gelmektedir.

Andrejevic’in tanımıyla, büyük veri ayrımı, veriyi toplayan, depolayan ve madenciliğini yapan kişilerle verisi toplanan hedef grup arasındaki asimetrik ilişkiyi ifade etmektedir (2014, s. 1674). Bu noktada önemli olan dijital çağdaki güç dengesizlikleri ve kişisel verinin toplanması ve kullanımına yönelik kamu tavrıdır. Büyük veri ayrımının ortaya çıkmasının temel sebeplerinden bir tanesi yeterliliklerle ilgilidir. Andrejevic bu yeterliliklere bağlı olarak ortaya çıkan iki grubu “büyük veri zengini” ve “büyük veri yoksulu” olarak kavramsallaştırmaktadır (2014, s. 1675). Büyük veri varlığı bakımından böyle bir ayrımın oluşma sebebi, büyük veri analizine ulaşım ve kontrolde ihtiyaç duyulan masraflı teknolojik altyapılara, pahalı veri setlerine, yazılıma, işleme gücüne ve onları analiz etmek için uzmanlığa dayanmaktadır (age, s. 1675). Günümüzde iradeye ve rızaya dayalı büyük veri toplanmasının “Bilgilendirilmiş Onam Formu” adı altında yapılmasının da büyük veri ayrımını destekleyen bir süreç olduğu göze çarpmaktadır. Buradaki güçsüzlük de bilgi ve iletişim teknolojileri üzerinde sahiplik ve kontrolün yalnızca büyük veri zenginlerine aitlik anlamında temellenirken; büyük veri fakiri olarak kavramsallaştırılan grubun da bilgi temelli karar verme anlamında zayıf kalması ve verilen onayın bir tür onay olmadığı ya da en azından tartışılması gereken bir konu olduğuna vurgu yapılmaktadır. Güçsüzlük hissini destekleyen sistemler verinin çevrimiçi ve çevrimdışı olarak toplanmasına olanak sağlayan “izleme teknolojilerinin yaygınlaşmasına” dayanmaktadır. Bahsedilen izleme teknolojileri örneklerinden

bir tanesi, plaka okuyuculardır (licence plate readers). Plaka okuyucuları, yollara giriş çıkışları takip etmek, kişilerin güzergahlarını görmek, çeşitli kurumlarla ilgili güvenlik önlemleri almak, yolların genel durumunu görmek ve kontrol etmek, adli olaylarda kişilerin takibini yapmak gibi düzenleyici ve zaman zaman cezai unsurlara destek sağlamaktadır. 2020 Pandemi sürecinde, Türkiye'de karantinada olan bireylerin konumlarını tespit etmek ve HES kodu bilgisi sağlamak için kurulan "Hayat Eve Sığar" uygulamasında da bireylerin konumları mobil cihazları ile GPS ve Bluetooth gibi teknik altyapılarla elde edilebilir hale gelmiştir. Akıllı kameralar, dronelar, radyo frekansı tanımlama sistemleri, ses algılayıcıları da çok çeşitli alanlarda kullanılmakta ve gözetimin alanı genişledikçe, mahremiyet tamamen sorgulanması gereken bir olgu haline gelmektedir.

Kuramsal çerçevede en çok vurgulanacak kavramlardan bir tanesi olan büyük veri ayrımı, ayrımcı teknolojilerin gelişimi ve gelecek tahminleri yapmada "panoptik tasnif" kavramıyla Gandy ile ele alınacak, bunun tamamen yeni bir gelişme olmadığı aksine tarihsel bir arka plana sahip olduğundan bahsedilecektir. Gandy'nin bunu dayandırdığı nokta ise modern bürokratik rasyonalite çağında hesaplama sistemlerinin ve sosyal tasnifin meydana gelmeye başladığı hatta sosyal tasnifin Taylorist "Bilimsel Yönetim" ile başladığı ve 20. yüzyıl ortalarında banka, ev, sigorta endüstrilerinin bir devamı niteliğinde olması üzerinedir (Andrejevic, 2014, s. 1677). Kavramsal çerçevede yer alan verilerin kendi adına konuşması ise bilinen ve literatürde çokça yer alan Chris Anderson'un önerisi olan "Teorinin Sonu" tartışması ile yerini almaktadır. Anderson bunu "Petabyte Çağı" olarak adlandırmaktadır. William Bogard'ın bahsettiği "Gözetim Simülasyonu" kavramı da kuramsal çerçevede ele alınarak, sistemin ve büyük veri zenginlerinin, büyük veri yoksullarının verilerini ekonomik, sosyal, kültürel ya da siyasal olarak kendi yararına kullanmak için nasıl manipüle edebileceğini tartışmak amacıyla ele alınmaktadır. Buna örnek olarak sağlık sigortalarının müşteri verilerini kullanarak tam zamanında büyük sağlık masraflarını karşılamaktan kaçınmak için kapsamı daraltması verilmektedir. Dijital gözetim sosyolojisi anlamında, akla gelen ilk isimlerden

olan David Lyon'un ise tüm bu kavramları bir araya getiren ve anlamlandıran kavramsallaştırması ve "Sosyal Tasnif Olarak Gözetim" tanımlaması sayesinde, kimlikleri tanımlamak ve değer atfetmek bağlamında katkılarına detaylı bir şekilde bakılmaktadır.

2.1.8. Büyük Verinin Kullanımı

Büyük verinin kullanımının en yaygın olduğu ve kullanıldığı mekanizmalar bu çalışmanın da temeline alacağı gibi gözetim pratikleridir. Fakat bu gözetim pratiklerinin kullanımı "geleneksel gözetim pratiklerini" değil; "yeni gözetim pratiklerini" kapsamaktadır. Geleneksel gözetimde temel prensip takip edilmesi gereken, bir çeşit risk oluşturduğu düşünülen kişilerin gözetlenmesi iken, yeni gözetimde herkes hakkında verilerin toplanması söz konusudur ve literatürde "dip tarama ağı" (dragnet) gözetim pratikleri olarak isimlendirilmektedir. Dip tarama ağı şeklindeki gözetim pratiklerini sağlayan en büyük gelişme ise büyük veri ile kolaylıkla gerçekleştirilen uzaktan, düşük görünürlük ya da tamamen görünmez bir şekilde uygulanan, otomatik ve sürekli yapılan hatta rutinleşmiş bir veri toplama ve işleme sürecidir. Toplumsal olarak bu konuyu değerlendirme ve kullanımını tartışma gerekliliği ise, günümüz toplumlarında bireylerin topluma katılım için genellikle mecbur oldukları pratiklerin bu sisteme dâhiliyet yeterliliğini sağlamasıdır. Haberleşme için kullanılan tüm mesajlaşmalar, telefon görüşmeleri, e-postalar, seyahatler, hastane kayıtları, sosyal medya hesaplarının kullanımı, internet bankacılığının kullanımı, kredi kartlarıyla yapılan harcamalar, alışveriş sitelerinden yapılan tüm alışverişler gibi daha birçok hareket büyük verinin depoladığı algoritmaların birer parçasıdır. Büyük veri gözetiminin hukuk ve sosyal eşitsizlik anlamında toplumsal sonuçları olacağını belirten Brayne, yaptığı araştırma sonucunda büyük veri kullanımındaki 5 farklı süreci vurgulamaktadır:

> "1. İsteğe bağlı risk değerlendirmesi, risk puanları kullanılarak tamamlanır ve ölçülür.
>
> 2. Veriler reaktif veya açıklayıcı amaçlardan ziyade tahmine dayalı amaçlar için giderek daha fazla kullanılmaktadır.

> 3. Otomatik uyarıların çoğalması, daha önce görülmemiş derecede çok sayıda insanı sistematik olarak gözetlemeyi mümkün kılar.
>
> 4. Veri kümeleri artık doğrudan polisle teması olmayan kişilerle ilgili bilgileri içerir.
>
> 5. Önceden ayrı veri sistemleri ilişkisel sistemlerle birleştirilir ve orijinal olarak ceza adaleti dışındaki diğer kurumlarda toplanan verileri içerir" (Brayne, 2017, s. 82).

Büyük verinin tek kullanım amacının insanları gözetlemek ya da görsel gözetim gibi yöntemlerle kamu güvenliğinin sağlanması olmadığı bilinmektedir. Literatürde en güncel ve en sık tartışılan büyük veri gözetimi örneklerinden bir tanesi hatta en çok kullanılanı Google'ın İnfluenza Trendleri Projesi olarak göze çarpmaktadır. 2008 senesinde influenza gibi hastalıkların nerede yayıldığını, sıklık olan bölgeleri tespit edebilmek ve önlemler alabilmek için Google'ın IP adreslerine dayanarak algoritmalar oluşturması, büyük veri gözetiminin sağlık alanında kullanım örneklerinden yalnızca bir tanesidir.

Teknolojik destekli gözetim pratikleri özel ve kamusal alanlarda genel bir yönetim aracı haline gelmiştir. Büyük verinin özellikle kurumsal bir pratik olarak neden tercih edildiği sorusuna iki teorik yaklaşım olduğunu belirten Brayne, bunları teknik/rasyonel yaklaşım ve kurumsal yaklaşım olarak sınıflandırmaktadır. İki yaklaşımda da kurumların kendi çıkarlarını temel aldığı fakat aktörlerin büyük veri analizine verdiği reaksiyonların farklı olduğu belirtilmektedir. Teknik yaklaşıma bakıldığında, büyük veri kurumsal aktörlerin tahminleri iyileştirme, analitik boşlukları doldurma ve kısıtlı kaynakları daha etkin kullanmak için bir araç olarak görülmektedir. Kurumsal yaklaşımda ise, kültürün rolüne vurgu yapılmaktadır, büyük veri analitiği verimliliği artırmak için değil, meşruiyet sağlamak için kullanılabilmektedir. Büyük veri insan karar verme mekanizmalarını, otomatik kararlarla değiştirmektedir (2017, s. 980). Kurumsal teoriye göre, yeni bir teknoloji eski bir kurumsal yapının üzerinde oluştuğu zaman yeni istenmeyen sonuçlar oluşmaktadır. Büyük veri anlamında da birey eylemlerinin "nesnel" veriye dönüşmesi, basitleştirme, bağlamsızlaştırma ve ölçülebilir karmaşık sosyal fenomenlerin büyük veri ortamında ayrıcalıklı hale getirilmesi gibi istenmeyen sonuçlara yol açabilmektedir (age., s. 1004). Büyük

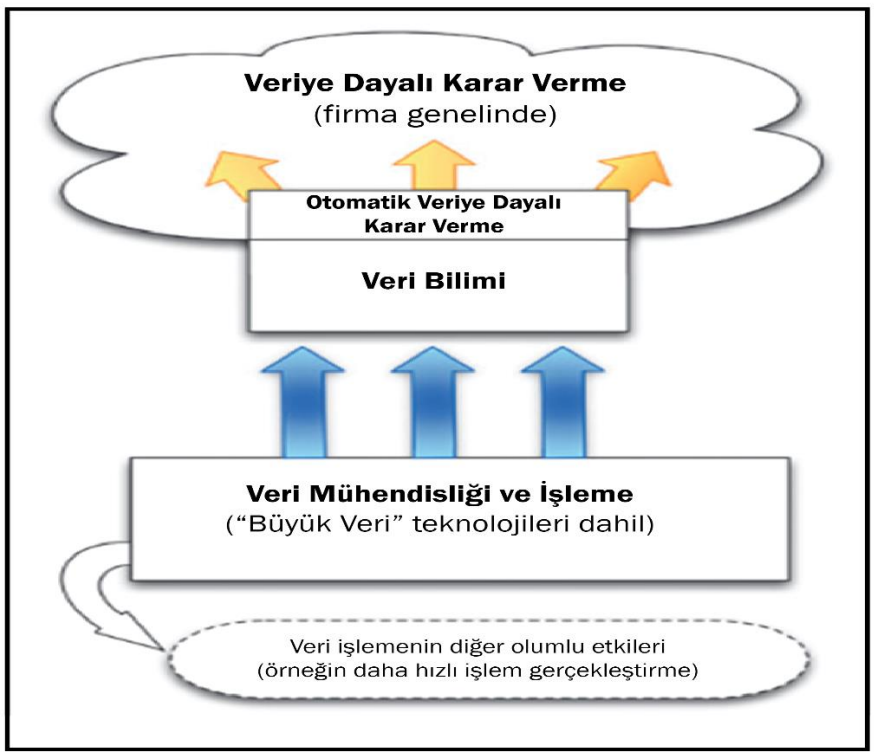
verinin kullanımı, alan, kaynak ve depolama kapasitesiyle de doğrudan alakalıdır ve kimin bulut veriye ulaşımının olduğu ve maddi araçları sağladığı da etkilidir.

2.1.9. Veri Bilimciler

Araştırmada veri bilimcisi olarak değerlendirebilecek bireylerle derinlemesine mülakatlar gerçekleştirilmiştir. “Veri bilimcisi” unvanının da büyük verinin gelişimi ile ilerlediği ve son dönemlerde çok daha fazla bir talebe sahip olduğu göz önüne alınarak, öncelikle veri bilimcisi kimdir ve veri bilimcilerinin taşıması gereken nitelikler nelerdir soruları araştırmanın katılımcılarını hem araştırmacı hem de bu çalışmanın ilgilileri için önemli kılmaktadır. Veri bilimcileri, zengin veri kaynaklarını belirleyen, bunları potansiyel olarak eksik veri kaynaklarıyla birleştiren kişiler olarak tanımlanmak mümkün olmakla birlikte, veri korsanı (hacker), veri iletişimcisi ve güvenilir danışman özelliklerinin bir arada bulunduğu kişi olarak da tanımlanmaktadır. Evrensel olarak en temel niteliği kod yazabilme becerisi olarak vurgulansa da özellikle veriyle, sözlü, görsel ya da her ikisiyle de hikâye anlatma becerisine sahip olan kişi olarak tanımlanmaktadır (Davenport ve Patil, 2012, s. 73).

Veri bilimini, veri işleme teknolojileri (büyük veri için olanlar da dahil) ve veri odaklı karar verme arasındaki bağlantı dokusu olarak tanımlayan başka bir çalışmada, veri mühendisliği ve işlemenin, Şekil 3'de gösterildiği gibi, veri bilimi faaliyetlerini desteklemek için kritik öneme sahip olduğu görülmektedir. Ancak bunlar daha geneldir ve çok daha fazlası için yararlıdır. Veri işleme teknolojileri, verimli işlem işleme, modern web sistemi işleme, çevrimiçi reklam kampanyası yönetimi ve diğerleri gibi bilgi çıkarmayı veya veriye dayalı karar vermeyi içeren birçok iş görevi için önemlidir (Provost ve Fawcett, 2013, s. 54).

Şekil 3. Veri Temelli Karar Verme Mekanizması



(Provost ve Fawcett, 2013, s.54)

Veri bolluğuyla, tüm sektörlerdeki mesleklerin değişmekte olduğunu ve bilimsel araştırmaların da veri odaklı hale gelmesinin veri bilimi disiplini üzerine düşünme durumunu artırdığını söyleyen bir çalışma da bilgisayar biliminin, bilgisayarların çok kullanımı ile matematikten doğması gibi, veri biliminin de mevcut veri bolluğuyla yeni bir disiplin olarak meydana geldiğini belirtmektedir (Van der Aalst, 2014).

Bilişim teknolojilerinin ortaya çıkardığı yeni bir istihdam imkânı olarak veri bilimciliğini tanımlayan bir çalışmada ise veri biliminin kapsamının 6 madde ile ifade edildiği görülmektedir:

1. Veri araştırma ve hazırlama

2. Veri gösterimi ve dönüşümü

3. Verilerle hesaplama

4. Veri modelleme

5. Veri görselleştirme ve hazırlama

6. Veri bilimi hakkında bilim (Strawn, 2016, s. 57).

Veri yönetişimi (data governance), veriyle ilgili konularda karar alma ve yetki uygulaması, kuruluşların sürekli artan kurumsal veri hacimleri üzerinde daha iyi kontrole sahip olma ihtiyacının farkına varmasına yanıt olarak son yıllarda geliştirilmiştir. Veri yönetişimi genel olarak yasalar, yönetmelikler, politikalar, standartlar, yönergeler, iş kuralları, organizasyonel organlar, standartlar, karar hakları (nasıl karar verileceği), sorumluluklar, insanlar ve bilgi sistemleri için yaptırım yöntemleri anlamına gelir ve kuruluş genelinde verilerle ilgili süreçler gerçekleştirilir. Veri kalitesi, veri koruma, veri görünürlüğü ve güvenliği, veri arşivleme, veri tanımları, içerik yönetimi, veri ambarı, metaveri yönetimi ve ana veri yönetimi dahil olmak üzere birden fazla kurumsal veri performansı öngörüsünü içerecek şekilde uygulamalar ve çerçeveler geliştirilmiştir (Stockdale, 2014, s. 464).

2.2. DİJİTAL SOSYOLOJİNİN BÜYÜK VERİYİ AÇIKLAYAN KAVRAMSAL ÇERÇEVESİ

2.2.1. Verileştirme (Datafication)

“Verileştirme, insan yaşamının dijital bilgi vasıtasıyla sayısallaştırılmasını açıklayan güncel bir olgudur. Verileştirme iki temel unsurla birlikte işler: Verilerin dışsal olarak toplanmasının, dağıtılmasının, depolanmasının ve parasallaşmasının yanı sıra devlet kontrolü ve kültürel üretim gibi unsurları içeren değer oluşturma süreçleriyle işlemektedir. Verileştirme iki süreçten meydana gelmektedir: Nicelikleştirme süreçleri ile insan yaşamının veriye dönüştürülmesi ve veriden farklı çeşitlerde değer oluşumu” (Mejias ve Couldry,

2019). Sayısallaştırma, yalnızca sistemlerin bireyi değerlendirmesi şeklinde değil, bireyin de kendisini değerlendirirken sayısallaştırmayı göz önüne alarak yapması şeklinde ilerlemektedir. Dijital teknolojilerin gelişimi hem veri toplamayı hem de sayısallaştırmaya erişimi kolaylaştırmaktadır. Sosyal medya platformları ve üretüketime katkısı olan kendini izleme araçları, değer üretimi ve bireyin kendini bu şekilde değerlendirilmesi süreci dijital sosyolojide "orantılılık" (commensuration) kavramı ile açıklanmaktadır. Bireyler hakkında bu vasıtayla hedefler üretebilme ve tahminler yapabilme imkânı ise "algoritmik manipülasyon" olarak kavramsallaştırılmaktadır. Lupton, bu duruma örnek olarak cinsel aktivite ve kendini izleme uygulamalarını örnek göstermektedir. Cinsel deneyim gibi fiziksel ve mahremiyet içeren bir konunun bile kendini izleme uygulamaları ile sayısallaştığını ve karşılaştırma yapılabilecek bir durum haline geldiğini ve dijital veri haline dönüştürüldüğünü belirtmektedir. Bu şekilde yalnızca sayısallaşma ve verileşme değil; cinsellikte belirli tiplerin ve kalıpların oluşturulmasının mümkün olduğunu belirtmektedir (2016).

Kuramsal çerçevede de yer alacağı gibi, tüm bu süreç dataizm ideolojisi olarak kavramsallaştırılmaktadır. Jose Van Dijck'in ifadesiyle dataizm ideolojisi: nesnelliğine olan inancın artması, metadatanın sosyal hayatın bir hammaddesi olduğuna inanma, veri biliminin opaklığının ortadan kalkmasıdır (Andrejevic ve Gates, 2014).

2.2.2. Veri Gözetimi (Dataveillance)

Büyük verinin ve büyük veri analizinin oluşum, gelişim ve kullanım süreçlerine bakıldığında, artık daha farklı amaçlar için kullanıldığı ve verinin gözetim amaçlı kullanımının çok daha ulaşılabilir ve tercih edilen bir hale büründüğünü görmek mümkündür. Bu süreçte ortaya çıkan kavram ise veri "data" ve gözetim "surveillance" kelimelerinin birleşimi olan veri gözetimini ifade eden "dataveillance" kavramıdır. Daha önce açıklandığı şekliyle büyük veriye kimin ulaştığı, kimin bilgilerinin toplandığı, Büyük Veri Yoksulu ve Büyük Veri Zengini gibi grupların oluşması veri gözetimi kavramının sosyolojik boyutunu çok fazla

etkileyen unsurlar haline gelmiştir. Özelikle veri madenciliğinin ve veri yönetiminin kontrolü toplumdaki sosyal, ekonomik, kültürel ve siyasal gücü etkileyecek bir güç haline gelmiştir. Bunun sebebi ise büyük veri gözetimi için gerekli olan gözetim kaynaklarına ulaşımdır. Bu kaynaklar çeşitli sosyal medya platformlarının topladığı verilere, sosyal ağlara, algoritmalara erişim gibi birçok unsurla bir arada işlemektedir.

Google, Facebook, Instagram ve YouTube gibi çeşitli teknoloji şirketlerinin veri toplama alt yapılarının güçlü olması ve iletişim sistemlerini yüksek kalitede gözetim sistemlerine dönüştürmeleri veri gözetiminin en güçlü örneklerinden yalnızca bir tanesidir. Bu anlamda bakıldığında, veri gözetiminin temelinde içeriğin metaveriye dönüştürülmesi ve veri madenciliğinin bu yolla yapılması bulunmaktadır. Google'ın belirttiği şekilde hiçbir insan sizin e-postanızı okumaz- bunun yerine makineler onu belirli iletişim kalıplarıyla bağdaştırabilmek ya da reklam alanında kullanabilmek ya da satın alma kalıplarını belirleyebilmek için metadataya dönüştürür. Bu süreç tüketim, siyasi katılım, eğitim, ulaşım, sağlık sistemi, taşımacılık gibi birçok alanda işlemektedir (Andrejevic ve Gates, 2014, s. 189).

Her şeyin metaveriye çevrilmesi ve tüm değerlerin sayısal olarak tanımlanması, kavramsal olarak açıklanan "Teorinin Sonu" tartışmalarıyla birlikte, dijital sosyolojinin önemli kavramlarından bir tanesi olan "sayısallaştırma" (digitization) kavramına dayanmaktadır. Sayısallaştırma (digitization), dijitalleşme ile (digitalization) ortaya çıkan sistemlerin toplumsal hayat ve birey düzeyinde içerisinde oldukları tüm alanlarda bilgi toplanmasına, depolanmasına ve işlenmesine destek olan bir süreç olarak tanımlanmaktadır. İnsanların ya da grupların verilerini toplayarak onların davranış kalıplarını belirleme ve gerekirse manipüle etme durumuna imkân sağlayan veri gözetimi, kişisel veri gözetimi ve kitlesel veri gözetimi olarak ikiye ayrılmaktadır.

Clarke ve Greenleaf'e göre, veri gözetimi, bir veya daha fazla kişinin iletişim eylemlerinin araştırılması veya izlenmesi için kişisel verilerin sistematik olarak

oluşturulması ve/veya kullanılmasıdır. Terim, 1980'lerde, başlangıçta zaten başka bir amaçla toplanmış olan verileri kullanmak için bir dizi araç olarak ortaya çıkmış, bilgi teknolojilerindeki gelişmeler, devlet kurumları ve benzer şirketler arasındaki çeşitli sosyal kontrol iştahıyla birleştiğinde, veri gözetimi uygulamalarının çeşitlendiği ve çoğaldığı görülmüştür (Clarke ve Greenleaf, 2017). Veri gözetiminin, fiziksel gözetimi de içine katarak gözetimi başka bir boyuta taşıdığı ve büyük veri ile başka bir boyuta ulaştığı bilinmektedir. Fiziksel gözetleme (insanların gözetleme kulelerinden ve evlerin dışında arabalarda oturarak, teleskoplar ve yönlü mikrofonlar kullanılarak izlenmesi gibi) ve elektronik gözetleme ('böcek' ve telefon dinleme kullanarak insanları izleme) ile karşılaştırıldığında, veri izleme çok daha ucuzdur ve otomatikleştirilme konusunda çok daha yeteneklidir. Bilgisayar teknolojileri, kuruluşların operasyonlarının mahremiyet müdahalesinde çok önemli bir artışa ve bunun sonucunda mahremiyet korumalarının yetersizliği konusunda ciddi kamuoyu endişesine neden olmuştur (Clarke, 1996).

Clarke, veri gözetimi için gerekli koşulları şu şekilde açıklamaktadır: Veri gözetimi amacıyla, üç koşulun yerine getirilmesiyle, tek bir merkezi veri bankası gerekli değildir:

1. Her biri belirli amaçlar için veri işleyen bir dizi kişisel veri sistemi bulunmalıdır.
2. Kişisel veri sistemlerinin bazıları, tercihen tümü, bir veya daha fazla telekomünikasyon ağı üzerinden birbirine bağlanmalıdır.
3. Veriler tutarlı bir şekilde tanımlanmalıdır (1988).

Veri gözetimi, mahremiyet konusunda birçok endişeye yol açmış, kişinin mahremiyeti, davranışın mahremiyeti, kişisel iletişiminin mahremiyeti ve kişisel verisinin mahremiyeti gibi pek çok alanda sorunlara yol açmıştır. Bu alanda en önemli isimlerden biri olduğu görülen Clarke, “etkili mevzuattan kaçınmak için bahaneler olarak 'öz düzenleme' veya Mahremiyet Artırıcı Teknolojiler (PET'ler) gibi anlamsız fikirlere güvenmek, resmi ve gayri resmi toplumlar arasında bir

uçuruma davetiye çıkarmaktadır” (Clarke, 2003) demektedir. Hükümetlerin her bir veri izleme tekniğini göz önünde bulundurması ve herhangi bir koşulda buna izin verilip verilmeyeceğine karar vermesi esastır; eğer öyleyse, bu koşullar nelerdir, önlemlerin neler olması gerekir ve hangi kontrol mekanizmaları bu önlemlerin her birinin etkili ve verimli bir şekilde çalışmasını sağlayacaktır (Clarke, 2023) diyerek eklemektedir.

Veri gözetimi önem verilmediği ve gerekli önlemler alınmadığı takdirde bu çalışmada da bahsedildiği gibi çok ciddi sonuçlara yol açacaktır. Clarke’a göre “sosyolojik olarak, insanların geniş sosyal adetlere tabi olarak, ancak sürekli gözlemlenme tehdidi olmadan davranmak ve başkalarıyla ilişki kurmak için özgür olmaları gerekir. Aksi takdirde, Demir Perde ve Bambu Perde'nin arkasındaki ülkelerde insanlara dayatılan korkunç, insanlık dışı, kısıtlanmış bağlama indirgeniriz” (Clarke, 2006).

2.2.2.1. Kişisel Veri Gözetimi (Personal Dataveillance)

Kişisel veri gözetimi denildiğinde, bireyleri belirli amaçlarla ve belirli kriterlere göre izleme uygulamaları ile bireylerin kendilerini izleme ve takip etme uygulamaları olmak üzere iki farklı yönde gelişmeden bahsedilmektedir. Veri gözetimi başlangıçta kişisel veri sistemlerinin bir veya daha fazla kişinin eylemlerinin veya iletişiminin araştırılmasında veya izlenmesinde sistematik kullanımı olarak tanımlanmıştır. Kişisel veri gözetimi yerine kitle gözetimine geçişte analiz de değişmektedir (Carke ve Greenleaf, 2017, s. 105).

Clarke ve Greenleaf, kişisel veri gözetiminin altındaki en önemli kavramlardan biri olan “dijital kişi/birey” kavramına vurgu yapmaktadır. Dijital kişi ya da birey tanımı sayesinde ilk olarak bireyin kamu kişiliğinin verilere dayalı işlemlerle korunması ve birey için vekalet olarak kullanılması amaçlanan bir model ifade edilmektedir. Fiziksel gözetim anlamında dijital kişiye bakıldığında, bireyin bedeni ve davranışına odaklanılırken ise veri gözetiminin kullanıldığı, kişinin

ekonomik, sosyal veya politik izleri incelenirken dijital bireyin gölgelerinin, dijital izlerin incelendiği belirtilmektedir (2017, s. 106).

Clarke'ın kişisel veri gözetimi tanımına bakıldığında, dikkat çeken nokta, belirlenmiş bireylerin veri gözetiminden bahsetmesidir. Bu gözetim incelendiğinde, ilk olarak kurumların içerisinde çeşitli yerlerde depolanmış verilerin entegrasyonu, kimlik doğrulaması, sıra dışı görülen işlemlerin, eldeki konuyla ilgili verilere karşı ve diğer dahili veri tabanlarından veya üçüncü taraflar aracılığıyla kontrol edilmesi kastedilmektedir. Buna ek olarak, istisnai görülen bireylerin denetlenmesi ya da üçüncü tarafın, bireyin üçüncü tarafla olan ilişkisinde bir ihlal yaptığını bildirdiği bireylere karşı yapılan sistemler arası uygulama bu gözetimin içeriğini açıklamaktadır (Clarke, 1988, s. 502). Bu anlamda sistemler de birbirine entegre olmuş haldedir ve farklı kurumlar iletişim kurarak veri gözetimini belirli hedef kişileri belirleyerek sürdürebilmektedir. Fakat bireylerin kendini kontrol etmesini (self-regulation) sağlayan uygulamalar ve gizliliği artırma teknolojileri (PET-Privacy Enhancing Technologies) gelişirken, bunlara karşıt birçok teknoloji de gelişmektedir. Bunlardan bazıları çerezler, spam ve casus yazılımı içeren internet izleme, anonim seyahat ve talep kimliğini inkâr eden otoyollar, dijital haklar yönetimi, çip tabanlı tanımlama, dijital imzalar ve genel anahtar altyapısı, kişi konumu izleme, biyometri ve hatta insan genetik verilerinin kullanımı şeklindedir (Clarke, 1996). Bir anlamda bireylerin kendi faydalarına olacak şekilde uygulamaları kullanmalarını sağlayan sistemler geliştikçe, bunlara karşıt uygulamalar da gelişmektedir.

İnsanlar günümüzde kendi kendini izleme uygulamaları ile kendilerine ve bedenlerine bir tür proje gibi yaklaşarak (örneğin akıllı saatlerle ve çeşitli sağlık uygulamalarıyla sürekli sağlık durumlarını takip ederek) veri üretmektedir. Bu verilerle çeşitli topluluklara dahil olmakta ve hatta kolektif hedefler (oksijen seviyesini sürekli belirli bir aralıkta tutma, akıllı saatin önerdiği şekilde belirli aralıklarla ayağa kalkıp hareket etme, belirli sayıda adım atma gibi) belirlemektedir. Buradaki veriler hem kişisel hem de kişinin dahil olduğu toplulukta küçük veri üretimini desteklemektedir. Küçük veri üretimi bu anlamda

sivil bir görev üstlenmektedir. Buna örnek olarak aynı sağlık sorununa sahip olan bireylerin dijital platformlar ya da araçlar sayesinde birbirlerine ulaşması ve iyileşme süreçlerinde birbirlerine bu araçlar sayesinde destek olması gösterilebilmektedir. Bunun yanısıra dijital aktivizm eylemlerinde bireylerin birbirlerine ulaşmaları ve kolektif hedefler belirleyerek kendi seslerini duyurmaları da bunun başka bir örneğidir. Veri üretimi ve gözetimiyle sağlanan bu tür kendini izleme pratiklerinin hem kişisel hem de ikinci örnekte görüldüğü gibi katılımcı demokrasi, vatandaşlık ve topluluk kavramlarıyla bağlantılı olduğu görülmektedir (Lupton, 2016, s. 112).

Tabi bu durum her zaman bireylerin seslerini duyurması ve demokrasi temelinde işlememekte olup, aksine bir durumun da gerçekleşme ihtimalini artırdığı görülmektedir. Özelleştirilmiş bilgi hizmetlerinin sağlanması için veri gözetimi sistemlerinin mimarisi, bireylerin erişebileceği bilgileri kısıtlayabilir. Bu durumda, bir bireyin ifade ve düşüncesi özgürlüğü Bilgi ve iletişim teknolojileri mimarisi tarafından kısıtlanır. Bir bireye sunulan bilgilerin böyle bir kontrolü, bireyin gerçekleştiğini bile fark etmeden ortaya çıkabilir. Bir veri gözetimi sisteminin geliştiricisi bile, geliştirdiği sistemin kontrolünü gerçekleştiremeyebilir. Veri gözetimi sistemlerinin mimarisinin neden olduğu “entelektüel özgürlük” için bu tür tehditler, sessizce ve duyarsız bir şekilde topluma dayatılmaktadır. Veri gözetimi sistemlerinin mimarisinin bu “sessiz kontrolü” ilerlemektedir (Orito, 2011, s. 6).

Bu tür bir kısıtlamanın mevcut olup olmadığının ve bireylerin kendi ürettikleri içeriklerden izlenerek onlar hakkında belirli rutin tespitlerinin yapılıp yapılmadığının bilincinde olup olmadıklarına bakılmıştır. Lupton ve Michael yaptıkları araştırmada katılımcıların, genellikle Facebook ve Google gibi şirketlerin tercihlerini, alışkanlıklarını ve sosyal medyaya yükledikleri içeriği izlediklerinin farkında olduklarını belirtmişlerdir. Bu izlemenin kanıtı, söz konusu siteleri kullanırken insanlara teslim edilen hedefli reklamcılıktan anlaşılmaktadır. Katılımcıların çoğu için belirsiz olan şey, bu veri alışverişinin nasıl gerçekleştiğinin veya diğer tarafların verilerine erişebileceğinin ayrıntısıdır.

Birkaç kişi, içinde bulundukları veri toplama düzeyini ve diğer insanların çevrimiçi etkileşimlerinden ve işlemlerinden kendileri hakkında sahip olabilecekleri bilgiyi tanımlarken 'korkutucu' terimini kullanmaktadır (Lupton ve Michael, 2017, s. 266).

2.2.2.2. Kitlesel Veri Gözetimi (Mass Dataveillance)

Kitlesel veri gözetimi, insan gruplarının, genellikle de büyük grupların gözetimini içerir. Gözetimin nedeni, gözetim organizasyonunun belirli bir ilgi alanına giren kişileri belirlemektir (Clarke, 2003). Buradaki temel nokta bir suç ya da sapkın bir davranış sebebiyle gözetlenmesi gerektiği düşünülen bireylerin değil, “herkesin” ve “her zaman” gözetlenebilir olmasıdır. Kitlesel veri gözetimi genel bir şüphe ile insanları gözetim altında tutmaktadır, temel hedefi kişisel veri gözetimine dahil etmeye değer bireyleri belirlemek ve grupların davranışlarını kısıtlamaktır (Clarke, 1988). Degli Esposti ise büyük verinin dijital gözetime sağladığı katkıyı göz önünde bulundurarak kitlesel veri gözetimini “davranışlarını düzenlemek veya yönetmek amacıyla kişilerin veya grupların dijital bilgi yönetimi sistemleri aracılığıyla sistematik olarak izlenmesi” olarak tanımlamaktadır ve veri gözetimi dört eylem kategorisi ile işlemektedir. Bunlar: kayıtlı gözlem, tanımlama ve izlem, analitik müdahale ve davranışsal manipülasyondur” (Degli Esposti, 2014). Clarke’a göre, veri gözetiminin gerçek etkisi, bireysel eylemlerin anlamlılığının ve dolayısıyla kendine güvenin ve öz sorumluluğun azalmasıdır. “Her ne kadar bu etkili ve hatta adil olsa da insanlığın kendisine dair imajında bir değişikliği içermekte ve kitleler tarafından somurtkan bir kabullenme ve geleceğin zorluklarıyla başa çıkmak için ihtiyaç duyulan bağımsız ruhun aptallaştırılması riskini içermektedir.” Genel olarak kitlesel veri gözetimi, bireyciliği ve insan kararlarının ve eylemlerinin anlamlılığını altüst etme eğilimindedir (Clarke 1988, s. 508akt. Zimmer, 2008).

2.2.2.3. Dataizm

Van Dijk, metaveriler ve verilerin, vatandaşların iletişim hizmetleri ve güvenlikleri için ödeme yaptıkları bir tür para birimi haline geldiğini belirterek, verileşmenin, ontolojik ve epistemolojik olarak sorun yarattığını öne sürmektedir. Bunu bir tür inanca benzeterek, dataizm kavramıyla, birçok insanın "safça" veya farkında olmadan kişisel bilgilerini kurumsal platformlara emanet etmesi olarak tanımlamaktadır. Bu kurumların akademik araştırmadan kolluk kuvvetlerine kadar çok geniş bir kapsamda olmasının güven kavramını çok sorunlu hale getirdiğini belirtmektedir (Van Dijk, 2014).

Dataizm, bir başka kaynakta ise, hangi kamu refahı hizmetlerinin vatandaşlar için en iyi olduğunu insanların değil, verilerin söyleyebileceği veri mantığına olan inanç olarak tanımlanmaktadır (Pedersen, 2019). Bir başka kaynakta ise büyük verinin hızla yayılmasının bir sonucu olarak, medeniyetin evrimsel gelişiminde yeni bir aşama, verilere dayalı bir toplumun ortaya çıktığı ve dataizmin bu anlamda her şeyin, kişinin kendisi de dahil olmak üzere etrafındaki her şeyin genel veri akışının bir parçası haline geldiği ve dijitalleştirilebilir hale taşınmasından bahsettiği ifade edilmektedir (Kobelieva ve Nikolaienko, 2021). Bu çalışmanın üst başlıklarında ise dataizm ideolojisi kavramıyla yer almakta ve daha da detaylı bir şekilde açıklanmaktadır.

2.2.2.4. Veri Güdümlü Yönetim, Güvenin Oyunlaştırılması, İtibar Puantajı, Profil Çıkarma, Sayısallaşmış Benlik, Sosyal Parametre Analizi

Yapay zekâ destekli sosyal puanlama sisteminde detaylı şekilde açıklandığı üzere, büyük veri ve yapay zekâ ile bireylerin verileri toplanarak onların belirli puanlamasının yapılabilmesi, bu puanların onların gerçek hayattaki imkanlarını etkilemesi ve hatta bunun bir hükümet kontrolünde gerçekleştirilmesi ile güvenin oyunlaştırılması kavramı bağlantılandırılmakta ve literatürde kullanılmaktadır. Bunun anlamı, bireylerin toplumsal ortamda sosyal ilişkide bulunacağı bireylerin puanlarını bilerek ona göre davranması, güven ilişkilerinin niteliğinin değişmesi

ve hatta sürekli gözetlenerek ve değerlendirerek yaşamanın insan ilişkilerini ve toplumsal ilişkileri doğrudan değiştirebileceğine yönelik oluşturulmuş bir kavramdır. Bu sistemle güvenin oyunlaştırılması kavramını bir arada ele alan çalışmalardan birine bakıldığında durum şu şekilde özetlenmektedir. En yüksek puanı elde etmek için vatandaşlar arasında bir tür rekabet ortaya çıkacak ve güvenin oyunlaştırılmasında bu rekabet etkili olacaktır. Bireyler çevrimiçi bağlantıları kullanılarak puanlanma yapılmaya devam edecektir. Bireylerin internetle daha iç içe hale gelmesiyle bu derecelendirme sisteminden çıkış için seçenek kalmayacaktır (Ramadan, 2018). Sosyal güvenin tekrardan sorgulanması çerçevesinde ve bunu ironik bir şekilde oyunlaştırma anlamında kullanan kavram olarak geçtiği de görülmektedir.

Güvenin oyunlaştırılması çerçevesinde, bireylerin bir yandan böyle distopik bir toplum düzeni içerisinde veri güdümlü yönetim altında olabilecekleri ve bu yönetimin doğrudan bireylerin ya da vatandaşların puanlarına göre ilerleyebileceği düşünülmektedir. Kavramsal olarak bireylerin itibar puantajının olacağı ve bu itibar puantajının büyük veriden yararlanarak yapay zekâ desteğiyle yapabileceği belirtilmektedir. Bu tür bir profil çıkarma kuramsal çerçevede de bahsedilecek olan bireyler hakkında kartografiler, haritalandırmalar, yaparak onlar hakkında gelecek tahminleri ve bu gelecek tahminleri üzerinden de algoritmik manipülasyon denilen durumun olabileceğini düşündürmektedir. Bunun örneklerinden bir tanesi de zaten Cambridge Analytica örneğinde görülmekte, bireylerin siyasi davranışlarının bu tür sistemler kullanılarak manipüle edildiği ve bunun için de Facebook verilerinin temel alındığı bilinmektedir.

Veri güdümlü yönetim, aynı zamanda izlenebilirlik ve hesaplanabilirlik ilkeleriyle hareket etmektedir. Bunun anlamı veriden doğan puanlama sayesinde sürekli kontrol altında olan ve hisseden bireylerin ya da bu gözetimi içselleştirmiş olan bireylerin daha da kontrol altına alınabilmesi, her anlamda birey davranışının bile hesaplanabileceği, sayısallaşabileceği ve bu doğrultuda da manipüle edilerek değiştirilebileceği düşünülmektedir. Bununla bağlantılı olan kavram da

bireyin her hareketinin sayısallaşması, bireyin kişiliğinin (yukarıda açıklandığı şekilde) sayısallaşmasıdır. Bu şekilde çeşitli sosyal ağlar oluşturabileceği, bu ağlar üzerinden de puanlama sistemlerinin yapılabileceği ve bunun da doğrudan bireysel ve toplumsal ilişkileri etkileyebileceği düşünülmektedir. Bunun için Black Mirror'un Nosedive bölümünde sosyal parametre analizleri yapıldığı ve bu analizler gerçekleştirilirken iç halka ve etki küresi kavramları kullanılarak hem bireyin aile gibi doğrudan dahil olduğu sosyal ilişki ağları hem de iş yeri gibi sonradan dahil olduğu kurumlardaki etkisinin göz önüne alındığı görülmektedir. Sosyal Kredi Sistemi'nin en önemli özelliği de bahsedilen bu kavramların büyük veri ve yapay zekâ yardımıyla çok kolay bir şekilde uygulanabilir ve tehlikeli bir güç haline gelme potansiyeli olduğudur. Veri manipülasyonu sadece en basit anlamıyla bireylerin tüketim alışkanlıklarını belirleyerek onlara tüketme ihtimali olan ürünleri önerme anlamında değil, sosyal ilişkilerde, toplumsal düzende ve toplumların yönetiminde kullanılabilecek bir şey haline gelmektedir. Bu tür sistemlerin ise genel anlamda algoritmik yönetimsellik kavramıyla, algoritmalara dayalı olarak bireylerin çeşitli kurallar, çeşitli normlar altında kontrol altında tutabilme imkânı sağladığı açıklamaktadır. Bir alt başlıkta algoritmik yönetimsellik kısaca açıklanmaktadır.

2.2.2.5. Algoritmik Yönetimsellik

Bireyin bıraktığı tüm dijital izlerin bir araya getirilerek bireyler ya da topluluklar hakkında anlamlandırmalar yapılması bu kavramın en temel amacı olarak belirtilmektedir. Bu şekilde kimlikler dijital izlerin toplamı ya da toplanması haline gelmektedir. Büyük veri sistemleri bir çeşit algoritmik yönetimsellik halini almakta ve bu yönetimsellik içerisindeki pratikler Foucaultcu anlamda birey öznelliklerini oluşa "being" getiren müdahalelerle bir tür özneleştirme halini almaktadır.

Büyük veriyi var olan öznelleştirme süreçlerinden tamamen ayrı bir şey olarak görmek yerine, Reigeluth'un önerdiği şekliyle, dijital izlerin dijital teknolojilerin uzun erimli kurumsal ve teknolojik düzenlemelerle insan öznelliğini onların

içerisinde bulundukları çevreyi yapılandırarak öznelliklerini şekillendirmelerine ışık tutmak gerekmektedir. Suç önleme programları (PredPol) ve Nicelikleştirilmiş Benlik Hareketi (Quantified Self) bunun net örneklerindendir (Andrejevis ve Gates, 2014, s. 194). Büyük verinin sağladığı imkanlarla kuramsal çerçeve de daha detaylı anlatılacağı şekilde bir yandan bireylerin kendilerini izlemesi, kendileriyle aynı alışkanlıklara ya da sorunlara sahip olan bireylere ulaşabilmeleri, kendilerini ifade edebilmeleri gibi imkanlar bulunurken, diğer yandan artık sadece suçluların tespiti için değil, herkesin devamlı olarak izlenmesinin sonucu olarak dijital gözetim insan hayatının bir gerçeği haline gelmiştir. Kuramsal çerçevede de öncelikle dijital sosyoloji temelinde gözetime, daha sonra gözetimden dijital gözetime geçişten bahsedilmekte daha sonra ise ontolojik güvenlik temelinde gözetimin anlamı açıklanmaya çalışılmaktadır. Bundan sonra ise dijital gözetimin, büyük veri ve yapay zekâ destekli yeni gözetim pratiklerinin, sosyolojik olarak ne tür değişimlere neden olacağını sorgulamak amacıyla gözetim kuramlarında panoptik, post-panoptik ve çağdaş olarak bir sınıflandırma yapılmaktadır.

3. BÖLÜM

ARAŞTIRMANIN KURAMSAL ÇERÇEVESİ

3.1. DİJİTAL SOSYOLOJİ TEMELİNDE GÖZETİM

3.1.1. Deborah Lupton- Kendini İzleme Kültürü Çerçevesinde Dijital Risk Toplumu, Dijital Sayborglar ve Dijital Bedenler

Dijital veri bilgi ekonomisi, geçtiğimiz yıllarda gittikçe gelişen, özellikle dijital verinin ticari, bilimsel ve yönetimsel değerinin hem birçok aktör hem de kurum için arttığı bir ekonomiyi ifade etmektedir. Bireylerin kişisel ya da küçük verilerinin hacimli veri setlerine dönüşmesine ve büyük verinin sosyal ve ekonomik trend ve davranışlara dair öngörüler oluşturmasına olanak sağlamıştır. Levi Strauss ile anılan ve Boellstorf'un kavramı olan "rotted data" (bozulmuş veri) kavramıyla, dijital veri ekonomisine dahil olan verinin, saf bir veri olmadığı, verinin sahibinin veri üzerindeki kontrolünü kaybettiğinden bahsedilmektedir (Michael ve Lupton, 2016).

Kontrolü kaybetmenin sebeplerinden bir tanesi dijital veri bilgi ekonomisinin, dijital risk toplumu ile işlemesidir. Dijital risk toplumları, bedenleri de dijital bedenler olarak kabul ederek, kendi bedenlerinden sorumlu olan bireylerin kendilerini çeşitli teknolojik araçlarla takip ederek gerekli önlemleri almalarını zorunlu kılmaktadır. Kendini izleme kültüründe, kendinin farkında olmak ve kendi gelişiminin önemi "kendilik" (ideal bir insan ve kendinin en iyi hali olma girişimi) ve kendi çıkarının farkında olmak (kendiyle ilgi çekici bir konu olarak ilgilenmek) temel alınmakta, bu süreç hem kendini izleme araçları ile (akıllı saatler gibi) kendini ve bedenini takip etme hem de blog gönderilerinde, web sitelerinde, LinkedIn, Facebook, Twitter gibi sosyal medya platformlarında kendini izleme hesaplarını kullanmak üzerinden ilerlemektedir (Lupton, 2014). Bu kültür kendini optimize etme, kendini yönetme, bedenlerin ve teknolojilerin bir aradalığı, verinin değerlenmesi (valorisation), verinin kişilerin ve

yaşamlarının birer replikası haline gelmesi ve sosyal eşitsizlikler çerçevesinde düşünülmektedir. Özellikle yapay zekâ destekli sistemler ve nesnelerin internetinin kullanılmasıyla verilerinin bedenlerinden, sağlıklarından, ruh hallerinden, rutinlerinden sorumlu hale gelmesi bireylerin kendileriyle ilgili daha çok veri paylaşarak (kendileri birer ürün haline gelerek) sürekli kendilerini kontrol ettikleri ve sayısallaştırdıkları bir hale dönüştürmektedir. Bunun örneklerinden bir tanesi, akıllı saatler ile bireylerin telefonlarının iyileştirerek bireylere gün içerisinde çalışırken çeşitli aralıklarda ayağa kalkıp hareket etmeleri, belirli bir seviyede adım atma, su içme, oksijen seviyesini ayarlama, stres seviyesini kontrol altında tutma gibi önerilerde bulunmasıdır. Bireyler gün içerisinde ne ile meşgul olurlarsa olsunlar eğer kendini izleme kültürüne kendilerini kaptırdılarsa bu durumlardan tamamen sorumludurlar. Akıllı saatler ve nesnelerin interneti ile onlarla bağlantılı olan uygulamalar, onların sosyal medyada çok fazla vakit geçirdikleri, doğru saatler arasında uyumadıkları, uyudukları saatler içerisinde hafif uyku, derin uyku, REM uykusunu doğru miktarlarda ve biçimlerde uyumadıklarına dair de uyarılarda bulunmaktadır.

Bu tür öneriler, uyarılar, bu sistemlere inanma ve kendini bu şekilde kontrol etme ise, kendini izleme kültürü ile bireylerin büyük veriye dahil olmaları ve dijital risk toplumunun onlara dayattığı ideal benlik, kendinden sorumlu birey anlayışıyla hareket etmelerinin bir örneğidir. Kendini izleme kültürü sayesinde büyük veriye dahil olan her bir verinin incelendiği ve dijital gözetim sosyolojisi alanında en çok kullanıldığı alanlardan biri de sağlıktır. Risk toplumlarında bireylerin en baştan riskleri kabul ederek onlar için güvenlik önlemleri alması çerçevesinde, dijital medya teknolojilerini kullanarak sağlık sorunları olan bireylerin büyük veriye dahil oldukları görülmektedir. Lupton, dijital hasta deneyimi ekonomisi kavramını kullanarak, bireylerin sağlık sorunları için çözümler aramak, aynı sorunları yaşayan bireylerden destek almak ve çeşitli tedavilere ulaşabilmek amacıyla kullanıcı odaklı içerik üreterek sosyal medya platformlarına, forumlara ya da çeşitli diğer platformlara katılım sağladıklarını belirtmektedir. Bu bireyleri de dijital faaliyette bulunan hastalar olarak kavramsallaştırmaktadır (Lupton, 2014, s. 856). Dijital hasta deneyimi

ekonomisi etrafında tartışılabilecek olan yapay zekâ destekli “Neyim Var?” uygulaması dijital epidemiyoloji başlığı altında tartışılmakta olup, bakıldığında bu tür sistemlerin de hem bu hastaların verdikleri bilgilerle hem de tüm büyük veri ağıyla beslendiği bilinmektedir. Bu sistemleri kullanmak aynı zamanda bu tarz hastalıklar yaşayan bireylerle bir tür paylaşım yapmak anlamına gelmektedir.

Dijital faaliyette bulunan hastalar, sağlık ve ilaç kullanımı hakkında dijital medya teknolojileri ile iletişimde bulunmakta, hasta öz-bakımı ve takip konusunda sorumlu kılınmaktadır. Dijitalleşmeyle, bireyin kendi bedeninden sorumlu hale gelmesiyle, hastalık ve sağlık da metalaşmış, birey “dijitalleşmiş kimliği” ile üçüncü taraflara veri sağlar hale gelmiştir. “Daha iyi tıp büyük veri sayesinde size getiriliyor” haber başlıklarında da görülen ütopyacı görüşün aksine bu verilerin destek ya da hastalık tedavi amaçları dışında da kullanıldığı görülmektedir (Harris 2012 akt. Lupton, 2014, s. 860). Bireyler bu bilgileri kimliğin dijitalleştirilmesi kapsamında verirken, üçüncü tarafların bilgilerine erişimleri sağlanmakta, çeşitli kurumların güçleri sayesinde algoritmaları da etkileyerek hasta bireylerin o siteleri ya da çeşitli ilaçları kullanımından, hatta ilaç denemeleri esnasında dijital medya teknolojilerinden yararlanıldığından bahsedilmektedir. Uluslararası ölçekte sağlık sigortası yapan firmaların, hastaların sağlık bilgilerine büyük veri ile ulaşıp onlara yönelik önerilerini değiştirmedikleri, erteledikleri ve büyük verinin birey yararına bu anlamda da nasıl tehlikeli olabileceği bilinmektedir. Kendini izleme kültürü için olsa da dijital hasta deneyimi için olsa da buradaki önemli nokta bireyin kişisel verileriyle büyük veriyi, büyük verinin de yapay zekayı ve onun desteklediği kontrol mekanizmalarını desteklemesidir. Hem bu kültürün hem de dijital hasta deneyiminin en önemli mekanizmalarından bir diğeri ise dijital epidermalizasyon, dijital epidemiyoloji, dijital fenotipleme, bozulmuş veri ve dataizm ideolojisidir.

3.1.2. Dijital Epidermalizasyon

Özellikle biyometrik verilerin de büyük verinin büyük bir parçası olarak toplanması ve bu teknolojilerin daha da gelişmesi sınıflandırma pratiklerini destekleyici bir hale gelmiştir. Popüler biyometrik gözetim teknolojileri arasında iris ve retina taramaları, el geometrisi denemesi, parmak izi verileri, yüz ve damar modelleri ve yürüyüş tanıma yer alır. Basit bir ifadeyle, biyometrik canlı vücudunu ölçmeye yarayan bir teknolojidir. Bu teknolojinin uygulaması, vücudun delil olarak işlev görmesini sağlayan doğrulama ve kimlik belirleme uygulamalarındandır. Bu sayısallaştırıcı durumlarda kimlikler, aynı zamanda, Stuart Hall'u izleyerek, "belirli söylemsel oluşumlar ve pratikler içinde, belirli ifade stratejileri tarafından özel tarihsel ve kurumsal sitelerde üretilmiş" olarak anlaşılan söylem içindeki inşaları üzerinden de düşünülmelidir (Browne, 2010). Bu açıklamayı yapan Simon Browne, dijital epidermalizasyon kavramı ile bu tür bir sınıflandırmanın nasıl olduğunu ve ilerlediğini açıklamaya çalışarak literatüre katkı yapmaktadır. Kafer ve Grinberg'in de belirttiği şekilde Simone Browne'un dijital epidermalizasyon ile açıklamaya çalıştığı şey, biyometrik teknolojilerin "dijital epidermalizasyon" sürecinde ırksallaştırılmış güç olarak kullanılması, burada öznenin bedeninin/kişinin kimliği hakkındaki gerçeği açıklamaya zorlanmasıdır (2019). Buradan anlaşıldığı şekilde dijital epidermalizasyon bir tür gözetim pratiği olarak işlemekte, güç ve öznelleştirme teknolojileri sayesinde eskiden kalan ırksallaştırma ve ayrımcılık durumlarına sebep olmaktadır.

Uluslararası alanda yüz tanıma teknolojileri ve çeşitli veriler birleştirilerek, kişilerin siyasi görüşlerinin tespit edildiği ve bunların onların biyometrik verileri ile ne kadar uyumlu olduğuna dair pek çok çalışma yapılmaktadır. Biyometrik veriler, en basitiyle parmak izi verilerinin, şu anda bir ülkeden başka bir ülkeye geçmek için hem yerel hem uluslararası ölçekte önem taşıdığı, özellikle havalimanlarında bireylerin parmak izi doğrulamasını ve ona ek olarak yüz tanıma teknolojileriyle kendilerinin "kendileri" olduğunu ispat edemedikleri takdirde seyahat edemeyecekleri görülmektedir. Tıpkı bu durum gibi ırk kavramının da fiziki niteliklere dayanması sebebiyle, özellikle yeni dijital

sistemlerle daha ayrıştırıcı bir hale geldiği literatürde pek çok şekilde ifade edilmektedir.

Monea, bu durumu Lisa Nakamura'nın (2007) ırk kavramının günümüzde hesaplama ve dijital görsel kültür tarafından sürdürüldüğünü ve dijital ırksal oluşumların üretimine yol açtığını belirttiğini, John Cheney-Lippold'un (2017) benzer şekilde, algoritmaların ölçülebilir türlere veya kullanıcı verilerine dayalı istatistiksel olasılıklara göre dijitalleştirme olduğunu belirterek aktarmaktadır. Bu ise kullanıcıların, yenilerini üretirken aynı zamanda ırksal farklılığa ilişkin bazı eski fenotipik klişeleri somutlaştıran büyük verilerin algoritmik analizine dayalı dijital olarak ırksallaştırılmasıyla ilişkilidir (2019).

Yüz, iris ve parmak izi taramasının tümü, "görüntüleme ve görme arasındaki değiş tokuş sahnesini" siyahlığın tarihsel olarak bedensel yüzey ile genetik yapı arasında bildirilen bitişikliğin kanıtını sağlamak için icra ettiği epistemolojik bir kanalı ifade etmektedir (Raengo 2013, s. 10 akt. Kafer ve Grinberg, 2019). Irksal tespit ve ayrımcılıkların tekrar üretilme riskine ek olarak toplumsal cinsiyeti beden belirteçleri aracılığıyla okuma özelliği de yeni sorunları gün yüzüne çıkarmaktadır. Biyometrik sistemlerin toplumsal cinsiyeti beden belirteçleri aracılığıyla okuma yeteneği -vücudun sabit sosyal taksonomiler içinde içsel gerçeğini ortaya çıkarmasını talep etme- kolonizasyon tarihlerinden miras kalan ırksallaştırılmış normlar aracılığıyla şekillendirilmektedir (Kafer ve Grinberg, 2019).

Sadece ırk değil aynı zamanda toplumsal cinsiyet ya da inanç anlamında da bu tür sistemlerin sınıflandırıcı bir gücü olduğu, İran'da yapay zekâ destekli sistemler ve yüz tanıma teknolojileriyle, başörtüsü takmayan kadınların tespit edilmesi ve yaptırımların uygulanması haberleri bu teknolojilerin ne kadar farklı şekillerde kullanılabileceğini göstermektedir.

Güncel bu örneğe ek olarak ırksallaştırma özelinde bakıldığındaysa, dijital epidermalizasyonun öncelikle yerleşik ve uzamsal-zamansal olarak durağan ırk

kavramlarını şeyleştirdiği ve güçlendirdiği belirtilmektedir. İkinci olarak temel farklılıklara ilişkin yanıltıcı nosyonu pekiştirmektedir. Üçüncü olarak gözlemlenenin rızası olmadan yapılarak ırksallaştırmakta, görsel sınıflandırmanın herhangi anlamlı bir şekilde kullanıldığını varsayarak bu ırksallaştırmayı başkaları tarafından kabul edilmeye zorlamaktadır. Dördüncüsü, yüz algılama, tanıma ve sınıflandırma teknolojileri beyaz olmayan insanlar (özellikle beyaz olmayan kadınlar) için yetersiz çalışma eğiliminde olduğundan, dijital epidermalizasyon beyazlığa (ve beyaz erkekliğe) ayrıcalık tanımaktadır. Ve son olarak, dijital epidermalizasyon, temelde (ve yanlış bir şekilde) ırkın görsel uyaranlar aracılığıyla nesnel olarak algılanabilecek bir şey olduğunu ileri sürerek, ırk ile ten rengi gibi görsel olarak fark edilebilir, fenotipik belirteçler arasındaki sorunlu ve yanıltıcı eşdeğerlikleri yeniden ileri sürmektedir (Williams, 2022). Dijital epidermalizasyon kavramını kullanmak, bu sistemlerde var olan ırksal önyargının varlığını ortaya çıkarmaya yardımcı olmakta, yanlış nesnellik ve tarafsızlık iddialarını ortaya çıkarmaktadır (Chizea, 2022). Kadınların başörtüsü takıp takmamasının zorunlu hale getirildiği ülkelerde büyük veri destekli sistemlerin sonuçları bu anlamda düşünüldüğünde, bireylere çeşitli zorunlulukların bu sistemlerle daha kolay uygulanabileceğini, bireyler arasında ayrımlaşmayı artırabileceğini, başkaları tarafından da bu zorlamalarının daha kolay kabul edilebilir hale getireceğini, aksine belirli bir gruba ise ayrıcalık tanınabileceğini göstermektedir. Bu tür sistemler, var olan ayrımcılıkları destekleme ve sürdürme riski taşımaktadır. Bu tür sistemlerin doğrudan salgınlar, temelde hastalıklar ve sağlık üzerinden ilerlemesini açıklayan kavram ise dijital epidemiyolojidir. Dijital epidermalizasyon ve dijital epidemiyoloji birbirini desteklemektedir. Kovid-19 örneğinde de açıklanacağı gibi, bireylerin hastalık çıktıktan sonra salgının Çin kaynaklı olmasından dolayı, çekik gözlü bireylere karşı bir önyargıda bulunması bunun en net örneklerinden bir tanesidir. Bunun dışında büyük veri sistemleri ile belirli fiziki niteliklere sahip bireylerin salgınlardan, suçlardan veya kötü herhangi bir durumdan sorumlu tutulmasının olanağı bu sistemlerin toplumsal güven ve sosyal ilişkilerde neden bu kadar önem taşıdığının bir göstergesidir.

3.1.3. Dijital Epidemiyoloji

Büyük verinin ortaya çıkışı ve gelişimi kısmında da bahsedildiği şekilde, büyük verinin ilk kullanımının ve sistemleştirilmesinin hastalık tespitinin yapılması ve bir salgının nereden kaynaklandığını çözümlemek olduğu bilinmektedir. Epidemiyolojinin amacı da geniş anlamda, nüfustaki hastalık kalıplarını ve sağlık dinamiklerini ve bu kalıpların nedenlerini anlamak ve bu anlayışı hastalıkları azaltmak, önlemek ve sağlığı geliştirmek için kullanmaktır. Dijital epidemiyoloji, dijital verileri kullanan epidemiyolojidir (Salathé, 2018). Büyük verinin artışıyla hastalıkların, salgınların ve genel anlamda sağlığın gözetimi çok daha kapsamlı ve mümkün bir hale gelmiştir. Dijitalleştirilmiş sağlık gözetimi, yalnızca nüfusun ve güvenlik tehditlerinin küresel olarak izlenmesini kolaylaştırmakla kalmamakta, aynı zamanda bireysel bedenlerin ve sağlık risklerinin yerel olarak izlenmesini de kolaylaştırmaktadır. Dijital teknolojiler sadece dijital epidemiyoloji ve sendromik gözetimi değil, e-sağlığı, bireysel verilerin istatistiksel analizlerine dayalı kişisel sağlık yönetimini de ortaya çıkarmaktadır (Samerski, 2018).

Dijital epidemiyoloji, dijital verileri kullanan epidemiyoloji, hastalıkların bir tür risk olarak toplumlardaki değişimin temel bir unsuru haline geldiğini ve büyük verinin toplanması, depolanması ve işlenmesinde ciddi bir etken olduğunu göstermektedir. Bunun örneklerinden bir tanesi, Aralık 2019'da Çin'de ortaya çıkarak tüm dünyayı saran Kovid-19 Salgını ile tüm dünyada hem fiziki gözetim mekanizmalarının artırılması hem de salgının tespiti ve kontrolü için büyük verinin kullanımı olmuştur. Bu tür salgınlardan korunmak ve kurtulmak için ulusal ve uluslararası anlamda alınan önlemler doğrultusunda bireyler istemli veri paylaşımının yanısıra zorunlu veri paylaşımı yapmak zorunda kalmıştır. Bu tür zorunlu ya da farkında olmadan büyük veri paylaşımında bireylerin verileri üzerinden kontrolü kaybetmenin temel sebeplerinden birisi olduğu bilinmektedir. Belirli bir risk etrafında, sistem işlemekte bedenler de bu sistemde bireylerin sorumlu olduğu "şeyler" haline gelmektedir. Çin'in vatandaşlarını puanlamak için uygulamaya koyduğu yapay zekâ destekli sosyal puanlama sisteminde de

uygulama, 2014 senesinde yasal olarak düzenlense de Kovid-19'un ortaya çıkışıyla fiziki gözetimin (kameraların) çok yüksek seviyede artırıldığı ve bu durumla paralel olarak veri toplamanın, depolamanın ve işlemenin kolaylaştığı bilinmektedir.

Armstrong'un gözetim tıbbı (surveillance medicine) kavramıyla bakıldığında, 1995 gibi erken bir tarihte, risk kavramı etrafında düzenlenen tıbbın, geleneksel olarak bireysel hastanın bedenini merkeze alan klinik tıbbın temel kavram ve yaklaşımlardan koptuğunu savunduğu görülmektedir. Günümüzün dijital epidemiyolojisinin kişisel sağlık hizmetleriyle birleşmesi ve "nicelikli kendi kendine ilaç" (quantified self medicine) uygulamasının yolunu açanın da bu kırılma ve gözetim tıbbındaki ilerleme olduğu düşünülmektedir (Samerski, 2018).

Yaklaşan pandemik riskleri anlamak için rutin olarak veri eksikliğiyle işaretlenen önceki bulaşıcı hastalık gözetim sistemlerinin aksine, 21. yüzyılın başlarındaki "Büyük Veri" tufanı şimdi verilerin bu sorunsallaştırılmasını tersine çevirmektedir. Çağdaş dijital hastalık gözetim sistemleri ve sağlık güvenliği uygulaması artık veri kıtlığıyla engellenmemekte aksine bunun yerine sonsuz sayıda üretilen, yapılandırılmamış ve dağınık dijital veri akışlarının fazlalığıyla yüklenmektedir (Eckmann, Füller ve Roberts, 2019). Samerski bu veri akışlarının fazlalığı ve hastalıkların ve onların kontrolünün de bireye yüklenmesi sürecini bu alanda önemli distopya yazarlarından biri olan Aldoux Huxley'in "Tıp bilimi o kadar büyük ilerleme kaydetti ki, neredeyse sağlıklı bir insan kalmadı" derken, çağdaş durumu en derinden gördü sözüyle açıklamaktadır (Samerski, 2018).

Kovid-19 örneği üzerinden bakıldığında, Türkiye'de, salgını tespit etmek ve salgının ilk başlarında hem hastalık tespit edilen bireyler hem de onlarla temas halinde olan kişilerin "Hayat Eve Sığar" (HES) uygulaması üzerinden kontrol edilmesi, GPS bilgileriyle haritada hasta bireylerin diğer bireyler tarafından da görülebilir olması, bireylerin sisteme hastalık belirtilerini ve durumlarını girmesi

bu durumun büyük veri üzerinden basit bir örneğidir. Bu uygulamanın yanı sıra, çeşitli iş yerlerinde aşı kartlarının zorunlu tutulması, kampüslere girerken HES listelerinin günlük ilanı ve kısıtlama gelmesi, e-nabız ile tüm bu verilerin erişilebilir olması büyük verinin dijital epidemiyoloji anlamında nasıl toplandığının ve geliştiğinin örneklerindendir. Daha sonra aşının bulunmasıyla, aşı karşıtı bireyler olduğu bilinse de bazı kurumların aşısı olmayan bireyleri çalışmaya başlatmayacağı gibi uygulamalar dijital epidemiyolojinin yaptırım gücünü de ortaya koymaktadır.

Kovid-19 sürecinden sonra pek çok insanın kendi sağlığı konusunda çeşitli uygulamalara başvurma, kendi takibini yapma, e-nabız kullanma gibi durumlara daha aşina hale geldiği ve bunun da bireyleri bu tür sistemlere daha açık hale getirdiği düşünülebilir. Samerski'nin değerlendirmesiyle, bu tür süreçler, dijital epidemiyoloji, hastaları ve kullanıcıları kendilerine istatistiksel bir bakış açısı benimsemeye davet ederek sağlık, hastalık ve bedenin rahatsız edici bir dönüşümüne katkıda bulunmaktadır. Günlük pratikleri ve eylemleri olduğu kadar duyguları ve sosyal ilişkileri de görünürlük alanına getiren dijital veri çığıyla, patojenik riskler üretme ve bunları kanıtlama olasılıkları sınırsız hale gelmektedir. Ayrıca, dijital cihazlar insanları gözetim sistemlerine entegre etmekte, böylece istatistiksel uyarılar ve geri bildirimler doğrudan kişisel yönelimler ve eylemler hakkında bilgi vermektedir (Samerski, 2018). 2021 senesinde Türkiye'de Sağlık Bakanlığı tarafından uygulamaya konan yapay zekâ destekli sağlık uygulaması olan "Neyim Var?" uygulamasına bakıldığında, bireylerin belirli semptomları girerek (baş ağrısı, mide bulantısı, ateş, öksürük vb. gibi) hastalıkları ile ilgili bir teşhis almaları hedeflenmiş, uzmanlarla görüşmeden önce bireylerin bu sistemlerle kendilerini yapay zekâ destekli olarak kontrol etmeleri planlanmıştır. Bu verilerin de sürekli olarak tutulması vatandaşların ne zaman nasıl hissettiğine, hasta olma ihtimallerine yönelik pek çok kişisel verinin depolanmasına neden olmuştur. Dijital epidemiyoloji de bu anlamda, dijital veri ekonomisini, dijital riskleri ve dijital bedenleri üretmede ve verileştirmede en etkili olan kavramlardan bir tanesi haline gelmiştir.

3.1.4. Dijital Fenotipleme

Dijital epidemiyoloji ile de bağlantılı olan dijital fenotipleme büyük veri ve onu destekleyen mekanizmalarla belirli kategorizasyonlar yapmanın bir şeklidir. Dijital fenotipleme, sağlık bilgisi sağlamak için mobil cihazlardan ve sensörlerden toplanan kişisel verilerin analiz edildiği yaklaşımları ifade etmektedir (Martinez-Martin, Insel, Dagum, Greely ve Cho, 2018). Klavye etkileşimleri gibi bazı dijital fenotip biçimleri "içerik içermez" olarak tanımlanmaktadır, yalnızca dokunma veya kaydırma için tepki süreleri ölçülmekte, metin veya konuşma içeriği toplanmamaktadır. Coğrafi konum, arama geçmişi veya sosyal medya gönderilerini toplayan diğer dijital fenotip biçimleri "içerik açısından zengin" olarak tanımlanmaktadır (Martinez-Martin, Insel, Dagum, Greely ve Cho, 2018). İçerik içermeme ve içerik açısından zengin olma durumu günümüzde önem taşımaktadır. Bunun sebebi bireylerin eskiden anonimken ve kitlesel gözetim yapılırken sıklık kullanılarak belirli eğilimler ve rutinler tespit edilirken, içerik açısından zengin verilere bakıldığında bireylerin anonimliğinin azalmasıdır. Facebook ve Cambridge Analytica Olayına bakıldığında, kişilerin verilerinin sıklığına bakılmasındansa onların yazdıkları ve konuştuklarının incelenmesinin daha sıkıntılı bir durum olması bunun örneklerinden bir tanesidir. Bireyler için de bir veri yığını içerisinde X bir kişi olmak çok sıkıntı olmasa da kendi isim ve soy isimleriyle anonim kalmadan verilerinin toplandığını bilmek onlar için daha büyük bir endişe kaynağı yaratacaktır. Bunun yanı sıra, yapay zekâ ve büyük verinin de kültürlerden beslenen ve dillerin, inançların, kültürlerin ön yargılarıyla gelişen sistemler olduğunu düşünmek dijital fenotiplemenin sorunlu yanını ortaya çıkarmaktadır. Google'da İngilizce arama yapılırken doktor mesleği için genellikle "he" (erkek), hemşire için "she" (kadın); öğretmen için "she" (kadın), polis için "he" (erkek) ifadesinin çıkması bunun bir örneğidir.

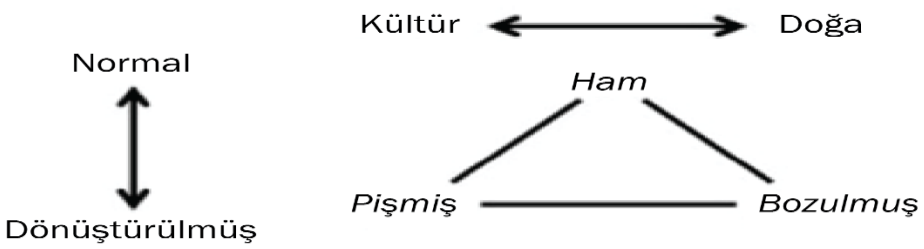
Dijital fenotipleme, "kişisel dijital cihazlardan, özellikle akıllı telefonlardan alınan verileri kullanarak yerinde bireysel düzeyde insan fenotipinin an be an ölçülmesi" olarak tanımlamaktadır (Onnela, 2021). Akıllı telefonlar, giyilebilir

cihazlar ve diğer bağlı cihazlar tarafından otomatik olarak oluşturulan ve toplanan verilerin potansiyelinden hem sağlıkta hem de hastalıkta insan davranışını ve işlevini ölçmek (veya sağlam temsiller sunmak) için yararlanmaya çalışılmaktadır. Günümüzde bu veri akışları, sensör ölçümlerini, etkinlik günlüklerini ve kullanıcı tarafından oluşturulan içeriği kapsamaktadır (Huckvale, Venkatesh ve Christensen, 2019). Dijital fenotiplemenin, akıl sağlığı sorunlarının değerlendirilmesi ve tedavisindeki gerçek boşlukları ele aldığından, psikiyatrinin bu en yeni "büyük veri" disiplinlerinde liderlik göstermek için özellikle iyi bir konumda olduğu belirtilmektedir (Huckvale, Venkatesh ve Christensen, 2019).

3.1.5. Bozulmuş Veri

Bozulmuş veri (rotted data) kavramı, Levi Strauss'un ham veri (raw data) ve pişmiş veri (cooked data) kavramları temel alınarak temellendirilmiş ve büyük veriyle ilişkilendirilmiş bir kavramdır. Kavramsal çerçevede de açıklandığı gibi, büyük veri kibri, insan karar verme mekanizmalarının yerini büyük verinin sağladığı verilerin almasına ve objektifliği sorgulanmadan bu verilerin analiz edilmesine neden olmaktadır. Bu verinin ne kadar saf olduğu ve gerçekten manipülatif sistemler olmadan elde edilip edilmediği ise net değildir. Snowden Olayı ya da Google'ın grip analizinde olduğu gibi, verilerin kontrol altında olduğu ve algoritmaların da bireyleri kontrol ettiği düşünülmektedir.

Şekil 4. Levi Strauss'un Kuliner Üçgeni



(Boellstorff, 2017, s. 9)

Levi Strauss'un Kuliner Üçgeni'ne bakıldığında, doğa ve kültür arasında, normal ve dönüşüme uğramış arasında bir ilişki olduğu, bu ilişki ile aynı zamanda ham, pişmiş ve "çürümüş" (bu çalışma için bozulmuş) veri arasında da aktif bir ilişki olduğu gösterilmektedir. Doğa ham olanı; kültür pişmiş olanı temsil ediyor demek yerine, aktif bir ilişkiselliğe vurgu yapılmaktadır. Boellstorf, veri kelimesinin ('data') köklerine inerek Latin dünyasında "dare" (cesaret etmek) kelimesinden türediğini, İngilizcede ise "date" yer ve zamanı kasteden bir kelimeden türediğini belirtmektedir. Zamanla özellikle Snowden Olayı örneğinde olduğu gibi, insanların gündelik yaşamlarından elde edilen bilgilerin başka amaçlarla kullanılması kapsamında metaveri olarak da yeni bir kavrama dönüşmüştür. Özellikle Snowden Olayından sonra, Orwelyan ya da büyük birader gibi kavramların kullanılmaya başlandığı, ama Orwelyan örneğinde görüldüğü gibi, büyük verinin hem istemsiz olarak üretilen veriyi kapsarken (GPS verileri gibi), hem de istemli olarak üretilen verilerin (Facebook paylaşımları gibi) dahil edildiği söylenmektedir. "Tarihi geçmiş teori" ile ise verinin her zaman geçici bir formu olduğu, verinin her zaman kendine yönelik iddiaları şekillendiren bir "tarihi" vardır düşüncesi vurgulanmaktadır (Boellstorff, 2017, s. 3). Verinin geçici formunu göz önüne alarak, ham ve pişmiş kategorisinde olduğu gibi, bozulmuş (rotted) kategorisinin de "veri bozulması" ("data degregation" "bit rot") durumunda da olduğu gibi hem emik hem de etik yanları bulunmaktadır.

Veri kaybı, teknik ve teknolojik sebeplere dayansa da verinin yanlış yorumlanması da veri kaybına yol açabilecek bir durumdur. Veriyi değil, anlamını da korumak vurgulanmalıdır. Çiğ ve pişmiş bağlamında, "çürümüş", aşçı olarak insan failinin tipik yapılarının dışında -planlanmamış, beklenmedik ve tesadüfi- dönüşümlere izin verir. Örneğin bit çürümesi, zaman içinde ilerledikçe depolama ve işleme teknolojilerinin birleşiminden ortaya çıkar. Ancak "çürüme" doğa ve toplum arasında olduğu kadar kasıtlı ve kasıtsız arasında da hareket eder. Çürüme "kendiliğinden veya kontrollü" olabilir; ikinci durum, genellikle "fermantasyon" veya "damıtma" olarak adlandırılır, ekmek ve peynirden bira ve şaraba kadar her şeyi üretir (Boellstorf, 2017). Bozulmuş

veriyle temel olarak, veri sahibinin amaçlamadığı şekillerde verinin dönüşüme uğrayabileceği vurgulanmaktadır. Hem veri sahibinin hayal etmediği şekilde dönüşebileceği gibi, verinin maddi olarak da hasara uğrayabileceği ya da kaybolabileceği belirtilmektedir. Dijital verinin saf ve objektif olmasına karşı çıkarak bu verinin saf olamayacağı açıklanmaktadır. Üretme, aktarma ve depolama süreçlerinde sorunlar meydana gelebilmektedir (Lupton, 2014, s. 111).

Veri bozulmasının yapay zekâ destekli sistemlerde, araştırmanın bulgular kısmında da bahsedileceği gibi, en tehlikeli hallerinden ya da örneklerinden bir tanesi, kişi hakkında toplanan ses ögeleriyle, yüz verilerini birleştirerek onlara söylemedikleri şeyleri söyletebilmek, yapmadıkları şeyleri yapmış gibi gösterebilmektir. Kişiden alınan veriler yukarıdaki tüm başlıklarla farklı alanlar vurgulanarak açıklandığı gibi biyometrik verilerden, sağlık verilerine, görsel verilere, ses verilerine, yazışmalara hatta kişinin kimliğine yönelik pek çok farklı veriyi içermektedir. Bu verilerin bir çeşit entegrasyon ve yapay zekayla bir araya gelmesinin bireyin yapmadığı şeyleri yapmış gibi gösterilmeye çok müsait hale getirilmesi ise ham verinin bozulmuş veriye dönüşümünü temsil etmektedir. Kişi kendi bedeni, sesi, görüntüsü ve kimliği üzerindeki kontrolünü kaybedecek hale gelmektedir.

Verinin her zaman yorumlamaya imkân sağlayan bir temeli bulunmaktadır ve bu anlamda da Boellstorff, büyük veriyi Clifford Geertz'in yoğun/kalın veri (thick data) kavramıyla karşılaştırmaktadır. Geertz bugünkü algoritmaları kastederek kullanmasa da etnografik algoritmaları pişmiş ya da bozulmuş verinin de yorumlardan ortaya çıkması ve veriyi "yoğun" yapanın onun bağlamsallığı olmasına bağlamaktadır (Boellstorf, 2017). Verinin yeni karar verme kültüründe bağlamsallığından çıkabileceği ve bunun farklı sonuçları olabileceği ise en önemli noktalardan bir tanesidir. Bir noktada veri bozulmuş, saptırılmış ya da yanlış örnekleme dayanmışsa da karar verme mekanizmalarında tamamen veriye dayanma düşüncesi, dataizm ideolojisi olarak karşımıza çıkmaktadır.

3.1.6. Dataizm İdeolojisi

Jose van Dijck'ın ifadesiyle, dataizm olarak belirtilen kavram, insan kitlelerinin gönüllü ya da farkında olmadan kişisel bilgilerini kurumsal platformlarla paylaşmalarıdır (van Dijck, 2014, s. 197). Bu paylaşımın temelini oluşturan temel veri kaynağı ise metaveri olarak isimlendirilmekte ve özellikle sosyal medya platformları ve Google gibi kurumlar tarafından insanların tüm hareketleri takip edilerek elde edilen bilgiler ile oluşmaktadır. Metaverilerin, bu platformlar tarafından üçüncü taraf kuruluşlarla paylaşılması ve bu verilerin de çeşitli ticari ya da gözetim mekanizmaları amacıyla kullanılması durumu oluşmaktadır.

Verileşme, sosyal eylemin çevrimiçi sayılabilir veriye dönüşümü ve bunun gerçek zamanlı takip ve tahmin edici analize imkân sağlaması süreci olarak tanımlanmaktadır (Schoenberger ve Cukier, 2013 akt. Dijck, 2014, s.198). Dataizm ideolojisi de verileşme ile elde edilen verilerin tamamen objektif olduğuna inanmayla ve bu yolla belirli tahminler oluşturulabileceğiyle ilgili olan ideolojiyi temsil etmektedir. Dijck, verileşmeyi bir çeşit hayat veri madenciliği (life mining) ile tanımlamakta ve Facebook, Twitter, LinkedIn gibi platformların arkadaş edinme, beğenme, takipçi edinme, retweet etme, profesyonel meslek ağlarını çevrimiçi ortama taşıma gibi algoritmik veri oluşturan aktivitelerle yeni bir sosyalleşme ve sosyal davranış rutinine taşıdığını belirtmektedir. Bu platformlardan oluşan metaveri, bu sayede bir çeşit para birimi gibi işlem görmekte ve satılabilen bir meta haline dönüşmektedir. Maden çıkarma işlemi yapılabilen, çeşitli amaçlarla değerli bir ürüne dönüşebilen değerli bir ürün haline gelmektedir.

Kavramsal çerçevede de belirtildiği gibi, metaveri, verinin birleşimi yoluyla bireysel davranışı tahmin edebilme ve manipüle edebilme anlamında kullanılabileceği düşünülen bir sistemin en değerli öğesi halini almaktadır. Burada vurgulanan önemli nokta ise, bu verilerin de çeşitli manipülasyonlara maruz kalabileceği ve tamamen yansız olmadığıdır. Dataizm ideolojisi ile yine, bozulmuş veri kavramına da bir manada atıfta bulunulmaktadır. Veri gözetimi

ise bireyleri çevrimiçi verilerine dayanarak gözetleme anlamına gelmekte, genel olarak gözetimden farkı ise gözetimde belirli bir amaç varken, veri gözetiminde metaverinin belirtilmemiş amaçlarla sürekli gözetimi içermesidir (Dijck, 2014, s. 205). Kuramsal çerçevenin bu kısmında hangi verinin nasıl kullanılabileceği ve bu verilerin ne tür bir sisteme yol açabileceğinden güncel örneklerle bahsedilmiş olup, bir sonraki bölümde gözetimin nasıl dijital gözetime dönüştüğünden bahsedilmektedir. Fiziksel bir gözetimden, yapay zekâ destekli bir büyük veri gözetimine giden noktada hem panoptik hem post-panoptik hem de çağdaş gözetim kuramlarını bilmek önem taşımaktadır. Panoptik, temel olarak gözetimin temellerini mantığını açıklarken; post-panoptik güç ve öznelleştirme teknolojilerinin yeni mantığını ifade etmeye çalışırken; çağdaş kuramlar yeni sistemlerle birlikte hem panoptik hem de post-panoptiği yorumlamaya çalışmaktadır.

3.2. GÖZETİMDEN DİJİTAL GÖZETİME

3.2.1. Panoptikon (Jeremy Bentham ve Michel Fouacult)

Panoptik ve post-panoptik gözetim çalışmaları, Fransız post-yapısalcı ve post modern felsefelerine dayanmaktadır. Poster, 1990 senesinde süperpanoptikon kavramını kullanmış; Haggerty ve Ericson 2000 senesinde Deleuze ve Guattari'nin 1987'deki çalışmalarına dayanarak, gözetim asamblajı (surveillance assemblage) kavramını geliştirmiş, Mann ise "sousveillance" kavramını geliştirmiştir (Bogard, 2012). Fakat tüm bu çalışmalar, panoptikon üzerine kurulmuştur. Genel olarak bilinen Panoptikon, Bentham'ın tasarladığı ve Foucault'nun teorilerinde kullandığı şekliyle, gardiyanların merkezi bir gözetim ya da teftiş kulesinden kendileri görünmez haldeyken mahkumları gözlemlemelerine imkân sağlayan bir tasarıdır (Bentham ve Božovič, 1995, s. 6).

Lyon'un vurguladığı şekilde, Foucault'nun modeli gözetimin çağdaş, küresel, teknolojik veya politik dinamiklerine tam olarak uymadığı bir ayrım, sınırlama

veya yola işaret etmekle birlikte, panoptikon metaforundan vazgeçilemediği, panoptikonun artık gözetimin kendini ifade ettiği anlamına gelmektedir. Panoptik temel alınarak birçok "optikon" geliştirilmiştir. Bunlar "süper panoptikon, elektronik panoptikon, "omnikon" (Goombridge 2003), "ban-optikon", "küresel panoptikon" (Gill 1995), "panspektron" (De Landa 1991), "myoptic panoptikon" (Leman-Langois 2003), "fraktal panoptikon" (De Angelis 2001), "endüstriyel panoptikon" (Butchart 1996), "kentsel panoptikon" (Koskela 2003), "pedagoptikon" (Sweeny 2004), "polioptikon" (Allen 1994), "sinoptikon" (Mathiesen 1997), "panoptik söylem" (Berdayes 2002), "toplumsal panoptisizm" (Wacquant 2001), "sibernetik panoptikon" (Bousquet 1998), ve 'neo-panoptikon' (Mann, Nolan ve Wellman 2003)" şeklinde kavramsallaştırılmaktadır (Lyon, 2006, s. 26). Bu çalışmada ise, büyük veri çalışmalarında en çok kullanıldığı tespit edilen, sinoptikon, panspektron, süperpanoptikon ve oligoptikon kavramlarına bakılmaktadır. Bunun sebebi sosyoloji kuramlarıyla bağlantılı olmaları ve büyük veri çalışmalarında temel alınmalarıdır.

Genel olarak Panoptikon'un temel alındığı bilinse de genel olarak Panoptikon'un Foucault yorumunun dikkate alındığı ve bir tür yanlış kavramsallaşmaya gidildiğinden bahsedilmektedir. Galic, Timon ve Koops'un açıkladığı şekilde, Foucault, Bentham'ın Panoptikon tasarısını alarak sosyal teorilerde kullanım şeklini belirlemiştir fakat Bentham yalnızca bir Panoptikon değil, çalışmalarına bakıldığında en az dört Panoptikon tasarlamıştır. Bunlar hapishane-panoptikonu (prison-panoptikon), yoksul panoptikonu (pauper panopticon- industry house), krestomatik panoptikon (chrestomatic panopticon, panoptic shaped shchool) ve anayasal/meşruiyet panoptikonu (constitutional panopticon) olarak kavramsallaştırılmaktadır. Foucault'nun panoptisizminin hapishane-panoptikonuna dayandığı ve bireylere sürekli bireysel denetim formunda, kontrol, ceza ve bedeller içeren, bireyleri belirli normlar çerçevesinde bir tür modelleme ve dönüştürme hedefi olan bir tür iktidar türü olarak kullanıldığı görülmektedir. Yoksul panoptikonu, hapishane panoptikonuna en çok benzeyen tür olarak tanımlanmaktadır. İlkine suçlular, yargıç ve hakimler tarafından gönderilirken, buraya gelen bireyler gönüllü şekilde gelmektedir fakat koşullar

yüzünden mecbur kalmadıkça kimsenin panoptikona gelmeyeceği bilinmektedir. Önce-kazan prensibine göre, kendi iş bölümünü tamamlamadan kimse Panoptikon'u terk edemez ve beslenemez şeklinde bir kural bulunmaktadır. Yoksul Panoptikonu'na bırakılan çocuklar da kız çocukları 17, erkek çocukları 19 olmadan burayı terk edemez. Eski yoksullardan oluşan Yaşlı Gardiyanlar (Guardian Elders) kayıt tutma, ısınma ve yemek yeme kurallarından sorumlu olarak bu sistemi yürütmekte fakat bir tür gözetimi devam ettirmektedir. Bu anlamda hapishane panoptikonuyla benzerlik göstermektedir. Krestomatikte, panoptik şeklinde tasarlanan okulda, ise panoptik kontrolün yalnızca çocuklar okuldayken uygulandığı, sabit bir sınıf yapısına maruz kalmadıkları, yaşa, konulara ve başarı seviyesine göre sınıf ve sınıflandırmanın değiştiği görülmektedir. Krestomatik ve anayasal panoptikonun daha az panoptik özellikler taşıdığı hatta anti-panoptik özelliklerinin olduğu belirtilmektedir. Anayasal panoptikonda "panoptik denetim prensibi" tersine dönmüştür. Sürekli görünür olma durumu ortadan kalkmış, idarecilerin sürekli gözetlenmesi yerine kamu görevlerinde olması düşünülmüştür. Artık azınlığın çoğunluğu değil, çoğunluğun azınlığı izlediği, vatandaşın idarecileri izlediği bir sistem olarak tasarlanmıştır (Galic, Timon ve Koops, 2017, ss. 12-15).

"Kevin Haggerty, 'Yeter artık, bu duvarları yıkalım!' demekte, panoptik imgelerin kullanışlılığının bugün hem tarihsel hem de mantıksal bir sınırı olduğunu kastetmektedir" (Lyon ve Bauman, 2020, s. 67). Bauman ise "Panoptikon hala hayatta ve iyi durumda. Bentham'ın, hatta Foucault'nun hayal bile edemeyeceği kadar güçlendi (elektronik olarak zenginleştirildi, "sayborglaştı"); ama bu yazarların kendi zamanlarında inandığının aksine, tahakkümün evrensel kalıbı veya stratejisi olmaktan çıktığı kesin; hatta en temel veya en sık kullanılan kalıp veya strateji olduğunu bile söyleyemeyiz. Panoptikon toplumun 'zapt edilmesi güç' kısımlarına, hapishanelere, kamplara, psikiyatri kliniklerine ve Erving Goffman'ın kullandığı anlamda diğer 'tam gözetim kurumlarına kaydı ve oralarda sınırlı kaldı" demektedir (Lyon ve Bauman, 2020, s. 70). Bakıldığında gerçekten Panoptikon'un da hiç olmadığı kadar güçlendiğini, büyük veri ve yapay zekâ destekli sistemlerin bireylerin kontrol altında tutulması, izlenmesi ve

yaptırım uygulanması için etkin bir rol oynadığı görülmektedir. Fakat bunun tek yönlü bir panoptisizm değil bir sonraki başlıkta açıklandığı gibi bir tür sinoptisizm de içerdiği bilinmektedir.

3.2.2. Sinoptikon (Thomas Mathiesen)

Foucault'ya göre panoptisizm, çoğunluğun azınlığı gördüğü durumdan azınlığın çoğunluğu gördüğü bir duruma geçişi temsil etmektedir. Mathiesen, ise sinoptisizm ve panoptisizmin bir arada ilerlediğini ve toplumsal gözetim pratiklerinin sadece panoptikon ile açıklanamayacağını ileri sürmektedir. Sinoptiszm, çoğunluğun azınlığı gördüğü ve izlediği, teknolojinin ve özellikle modern kitlesel medyanın en önemli ve etkili gelişme olarak arka planını oluşturduğu ve "seyirci toplumlarda" (viewer society) yer alan bir sistemdir. Gözetimin sosyal biçimleri, az kişinin çoğunu izlediği (panoptik), çoğunluğun azı izlediği (sinoptik), grup üyelerinin birbirini izlediği ve diğer aktörlerin amaçlarını bilerek ya da bilmeden kendini izleme süreçlerini kapsamaktadır (Dandeker, 2019, s. 225). Kendini izleme kültürü, dijital epidermalizasyon, dijital epidemiyoloji gibi tüm başlıkların altındaki temel sistemin hem panoptisizm hem de sinoptisizm ile ilerlediği görülmektedir. Devletler, vatandaşlarını izlemek için özellikle salgın döneminde, sistemlerin kullanımını zorunlu kılarak onları dijital sistemlerden gözetlemeye devam etmiş, aynı zamanda vatandaşların da diğerlerini gözetleyebilmesi için salgın kartografisi görüntüleme gibi sistemler kurmuştur. Panoptisizm her şartta etkisini korumakta ama farklı şekillerle de dönüşmektedir. Elektronik olarak zenginleşen ya da sayborglaşan bir hale bürünmektedir. Mathiesen ve Foucault'nun bu iki sürecin temelini nereye dayandırdığına bakmak bu anlamda önem taşımaktadır.

Sinoptisizm ve panoptisizmin gelişim süreçlerinde özellikle 1800-2000 döneminin etkili olduğu bilinmekte, 1750-1830 arası Foucault modern hapishanelerin kuruluşuna odaklanırken; Mathiesen kitlesel basın ve kitlesel medyanın ilk dalgasına (gazetelerin gelişimi, dağıtımdaki tren ve buharlı gemi gibi gelişmelerle, telgraf gibi gelişmelere) odaklanmaktadır. İkinci dalga film,

üçüncü dalga radyo, dördüncü dalga televizyon olarak nitelendirilmekte ve 1980lerden itibaren beşinci dalga olarak özellikle video, kablolar ve uydulardaki büyük teknolojik gelişmelerle, televizyonların özelleşmesiyle ve dijital teknolojiler ile tamamen yeni iletişim biçimlerinin ortaya çıktığı belirtilmektedir. Tüm bu gelişmelerde sinoptikon ve panoptikon bir arada yakın bir ilişki içerisinde gelişmiştir. “Orwell’in 1984 romanındaki gibi, oturma odasındaki ekrandan Büyük Birader’in sizi gördüğü gibi, siz de onu görmektesinizdir ve bu tamamen panoptikon ile sinoptikonun bir tür kaynaşmasıdır” (Mathiesen, 1997). Mathiesen’in kendisi de panoptisizm ve sinoptisizmin bir arada ilerlediğini ve kaynaştığını belirtmekte, yalnızca iki teorisyenin farklı gelişmelere bakarak farklı noktaları vurguladığını kendi de açıklamaktadır.

Sinoptisizmden hala bahsedilmesinin ve bu tezde de yer alması gerektiğini düşünmenin sebebi bu alandaki önemli teorisyenlerin, büyük verinin en büyük kaynaklarından biri olan Google’ı sinoptikon ile yorumlamalarıdır. Bauman ve Lyon’un çalışmalarındaki örneklere bakıldığında, kendin yap tarzı sinoptikon kavramına Google’ın örnek olarak gösterildiği görülmektedir. Farklı bireyler aynı kavramı aradıklarında karşılarına farklı sonuçlar çıkmaktadır; karşılarına çıkan sonuçlar daha önceden yapmış oldukları aramalarla bağlantılıdır (Bauman ve Lyon, 2016, s. 138 akt. Solmaz, 2020, s. 7). Bireyler başkalarını gözetlerken ya da çeşitli aktivitelerde bulunurken hem gözetlemekte hem de gözetlenmektedirler. “Gözetlenen bireyler artık gözetleyen konumuna geçmişlerdir. Bu durum, tek bir merkezden gözetim davranışı olan Panoptikon anlayışının yerine, çoklu merkezlerden kameralar ile gözetleme davranışı olan Sinoptikon anlayışının hâkim olmaya başladığını göstermektedir. Sinoptikon anlayışının getirdiği çoklu gözetim, tüketim alışkanlıklarının biçimlenmesini ve gündemin medya aracılığıyla belirlenmesini beraberinde getirmektedir” (Sucu, 2020). Çoklu merkezlerden gözetim, sosyal medyanın kullanımı herkesin de herkesi bir anlamda gözetleme imkanının yanı sıra, dijital gözetimin temelinde hala bireylerin, ulusların ve devletlerin güvenliği konu edilmekte, gözetim alanındaki en çok tartışılan durumlara bakıldığında güvenlik unsuru göze

çarpmaktadır. Bu anlamda bir alt başlıkta bahsedilen panspektrondan bahsetmek önem taşımaktadır.

3.2.3. Panspektron (Manuel Delanda)

DeLanda, panspektron adını verdiği çağdaş gözetim sisteminde, Bentham'ın Panoptikon'unu ABD Ulusal Güvenlik Teşkilatı'nın (NSA) toplu gözetleme planıyla karşılaştırmakta ve her ikisinin de farklı olduğu sonucuna varmaktadır. Panoptikon, tek bir sensöre gönderilen verilere güvenirken, NSA "gözetim görevleriyle ilgili veri bölümlerini seçmek için bilgisayarları kullanarak hepsi hakkında aynı anda bilgi elde etmeyi hedeflemektedir" (Laudrain, 2019). Dijital gözetim kuramlarında en çok yer alan Snowden Olayında da NSA'nın gözetleme pratiklerinin temel sorun alınması ve hala tartışılır olması özellikle büyük veri ve yapay zekâ destekli sistemlerde bunların daha da tartışılması gereken hale gelmesinin temel sebeplerindendir. Bulgular kısmında da bahsedileceği gibi Türkiye'de seçim döneminde, dönemin İçişleri Bakanı'nın "Kim?" isimli uygulama ile bahsettiği gibi, ulusal güvenlik kurumlarının elindeki verilerin ne boyutta olduğunu düşünmek, bunlar hakkında bilgi sahibi olmak ve dijital gözetime panspektronu da dahil etmek bu nedenle önem taşımaktadır. Dijital gözetimin her zaman bir güvenlik temeli, özellikle de ulusal güvenlik temeli vardır.

Manuel DeLanda, istihbarat teşkilatlarının panspektrik olarak tanımladığı yeni tür gözetleme sistemlerini nasıl inşa ettiğini açıklamaya çalışırken, Panoptikon'un aksine, panspektronun yalnızca görüneni değil, aynı zamanda radyo, radar ve mikrodalgaları da kaydettiğini belirtmektedir (Fura ve Klamber, 2012). Bu sistemi merkezi bir sensörün etrafına insan bedenlerini yerleştirmek yerine, tüm bedenlerin etrafına çok sayıda sensör çiftliklerinin yerleştirilmesi ile tanımlamaktadır. Bahsedilen sensörlerin anten çiftlikleri, casus uyduları, kablo trafiğinden gelen veriler olduğunu, toplanabilecek tüm verilerin toplanıp bilgisayarları beslediğini ifade etmektedir. Panspektronda bu anlamda belirli cisimler ve onlar hakkında belirli görsel veriler değil, tüm veriler toplanmaktadır

(Delanda, 1991 akt. Creemers, 2017). Verilerin sadece güvenlik temelinde, zorunlu olarak paylaşılmadığı, bireylerin istemli olarak ve hatta genel anlamda eğlence amaçlı ya da çeşitli faydalar uğruna verilerini paylaşmaya istekli oldukları görülmektedir. Bir alt başlık olan süperpanoptikon da bu sebeple önemlidir.

3.2.4. Süperpanoptikon (Mark Poster)

Süperpanoptikon kavramını ise Bauman, Mark Poster'den almıştır ve Panoptikon'un siber mekâna taşınmış güncel bir versiyonu ve "bedenlerin şebekeler ve veri tabanları ile enformasyon koridorları içine çekilmesi" olarak tanımlanmaktadır. Panoptikon'dan farklı olarak gözetimin gönüllü olması, Süperpanoptikon'un en önemli özelliğidir. Gözetlenenler, gönüllü bir şekilde veri depolarına katkıda bulunmaktadır (Bauman, 2012, s. 55 akt. Solmaz, 2020, s. 7). Büyük verinin en çok kişisel veri çektiği alan olarak tanımlanan sosyal medya platformlarının genellikle Süperpanoptikon'a, gönüllü gözetime, dayandığı bilinmekte olup bu anlamda Süperpanoptikon'un hala geçerli olduğunu belirtmek de önem taşımaktadır. Bu gönüllülüğün, sosyalleşmek, iş bulmak, eğlenmek gibi farklı boyutlarının yanısıra neden bireylerin ürün olmayı kabul ettiklerini tespit etmek önem taşımaktadır. Sosyal medya ağlarının ya da doğrudan internetin bir rizoma benzetilerek rizomatik ağlarla her alandan veri toplanmasını açıklayan kavram ise bir alt başlık olan Oligoptikon ile özetlenmektedir.

3.2.5. Oligoptikon (Bruno Latour)

Latour'un (2005) Oligoptikon'u, birden fazla gözlem alanına dayanan bir izleme sistemini içeren bir tür gözetimi açıklamaktadır. Oligoptikon, fiziksel olarak izlenen veya takip edilen bir bağlantının kurulabildiği ya da sürdürülebildiği sürece durumların yönetilmesini ya da kontrol edilmesini açıklamaktadır. Oligoptikon'un işlevi, her şeyi kapsayan bir gücü benimsemek değil, bağlantı yoluyla hem yerelleştirmek hem de bağlantı kurmaktır (Manley, Palmer ve

Roderick, 2012, s. 313). Küreselleşen sistemlerle, bireylerin konumları, biyometrik verileri, anıları, kimlikleri her şeyi tespit edilmektedir. Birey bir yandan çok küreselleşen bir sistemde yer alırken, bir yandan bireyin fiziki- sosyal çevresi, mesleği, kimliği ve her tür kişisel verisi- daha bilinir hale gelmektedir. Veriler, rizomatik gözetim ile ağların sürekli genişleyen şekilde ilerlemesi, verilerin sürekli entegre edilerek bir araya getirilmesiyle bireyi daha çok gözetlenebilir, haritası, profili çıkarılabilir hale getirmektedir. Bu anlamda oligoptikon, rizomatik gözetim ile yapılan gözetimin, profil çıkarma, prestij puantajı ve kartografi anlamında çok önemli bir gözetim çeşidi olarak kabul edilebileceği düşünülmektedir. Tüm bu kavramlar, süreçler ve örnekler ışığında panoptik, post-panoptik ve çağdaş gözetim kuramlarından önce, ontolojik güvenlik bağlamında gözetim, ontolojik güvenlik ve güvensizliğin temelleri, sosyolojik anlamları ve muhtemel sonuçları doğrultusunda ele alınmaktadır. Bireyler büyük verinin desteklediği yapay zekâ sistemleri içinde tamamen yeni bir toplumsal güven ve sosyal ilişki dinamikleri içerisine girmiş, yeni gözetim pratikleri bireylerin rutinlerini etkilemiştir.

3.3. GÖZETİM VE ONTOLOJİK GÜVENLİK

3.3.1. Ontolojik Güvenlik Bağlamında Gözetim (Anthony Giddens)

Giddens, modernliğin sonuçları üzerine düşünürken, güvenin ne olduğu, sistemlere duyulan güvenin nasıl sağlandığı ve neden bu tür bir güvene ihtiyaç duyulduğundan, kişisel güvene ilerleyen bir süreci takip etmektedir. Bu süreci izlemesinin sebebi ise mahremiyetin 20. yüzyıldaki dönüşümünün temelinin kişisel güvenin ne olduğunun cevabını aramasından kaynaklanmaktadır. Modern öncesi dönemde Giddens, yerelleşmiş güven bağlamını; akrabalık sistemi, yerel topluluk, dinsel kozmolojinin etkisi (din) ve gelenek (rutin) ile bağlantılandırarak açıklamaktadır (Giddens, 2021, ss. 101-105). Daha sonra ise soyut sistemlerin modern öncesi dönemde bulunmayan bir güvenlik sağladığını

ve bu sistemler ile hem güven anlayışının hem de mahremiyetin dönüştüğünü belirtmektedir (Giddens, 2021, s. 112).

Giddens, tüm bu süreçleri sosyolojik boyutuyla ele almaya çalışırken ve bunu ontolojik güvenlik kavramı temelinde yapmaya çalışırken, ontolojik güvenlik kavramının psikiyatriye dayandığını bilmek önem arz etmektedir. Ontolojik güvenlik özellikle bireylerin tam bir benlik duygusuyla nasıl mücadele ettiklerini, hayatlarını normal rutinleri yerine getirmedeki başarısızlık, derin kaygı, refleks olarak başa çıkma mekanizmalarını nasıl üretebilecekleri ve bu duygu ve davranışların değer ve bütünlük duygusu üzerinde nasıl bir etkiye sahip olduğu üzerine kurmaktadır (Croft, 2012). Gözetim sistemlerinin ve özellikle bu tezde bahsedildiği şekilde yeni gözetim pratiklerinin gelişimi ile ise bireylerin fiziksel, ruhsal, biyometrik gibi pek çok eski ve yeni şekilde izlenmesi ya da en azından izleniyormuş hissiyle yaşaması hem onların bahsedilen benlik duygusunda, benlik kontrolünde büyük değişime neden olmuş ve özellikle mahremiyetin sınırlarının gittikçe daralması, azalması ve çeşitli durumlarda bireyin kontrolünden çıkması, ontolojik güvenlik ya da ontolojik güvensizlik kavramını tekrar düşünme ihtiyacını ortaya çıkarmıştır. Bunun en çok tartışılan örneklerinden bir tanesi unutulma hakkıdır. Bireylerin yapıp pişman oldukları ya da bilinmesini istemedikleri bilgilerinin bir kez internet ortamına dahil olduktan sonra kaldırılmasının bu kadar zor olması insanları hem ağır bir sorumluluk hem de çeşitli durumlar altında ağır bir suçluluk haline sokmaktadır. Bireylerin eskiden yapıp pişman oldukları şeylerden dönme ve değişme şansı varken, artık sosyal ilişkilerde bireylerin birbirini kolayca arama motorlarından ya da sosyal medya platformlarından sorgulatabilir olması, kendi imajlarını kendilerinin yaratması yerine iyi ya da kötü bir önyargı ile sosyal ilişkilerine devam etmelerine sebep olmaktadır. Özetle, artık bireylerin unutulma, kolayca kendileri ile ilgili bir bilgiyi değiştirme ya da silme şansı yoktur. Özellikle uluslararası alanda unutulma hakkı ile ilgili açılan davalar gün geçtikçe artmakta, bireyler kimliklerini sıfırdan kurabilmek ve bilinmesini istemedikleri bilgileri sildirebilmek için yasal yollara başvurmaktadır.

Unutulma hakkı ile bahsedildiği gibi mahremiyetin dönüşümüne vurgu yapan Bauman, “mahremiyet kamusal alanı istila etti, fethetti ve sömürgeleştirdi; ama maalesef gizlilik hakkını, en belirleyici özelliği ve en el üstünde tutulan ve en hararetle savunulan ayrıcalığını kaybetmek pahasına” demektedir (Bauman ve Lyon, 2020, s. 41). Bunun anlamı gözetlenen bireyin mahremiyetinin bireyin kontrolü dışında kamusal hale gelmesi ve bunun dışında kalan bireylerin ise bir tür dışlanma ya da veriyi ikincil konuma tabii tutma tartışmasında olduğu gibi, toplumda seslerini duyuramayacak bir şekilde konumlandırmakla ilişkilidir. Bauman ve Lyon da bunu Güney Kore örneğiyle orada var olan kişisel sunum kültürü alanındaki, Facebook’un oradaki versiyonu Cyworld’de bir hesabı olmayan azınlığı bekleyenin sosyal ölüm olduğu şeklinde belirtmektedir (Bauman ve Lyon, 2020, ss. 42-43). Bu çalışmadan önce 9-13 yaş arasındaki çocuklar üzerinde YouTube’un yansımalarını inceleyen bir araştırmacı olarak, çocukların YouTube’da aktif şekilde kalmalarının, oradaki içerikler hakkında bilgi sahibi olmak ve hatta içerik üretmenin zorunluluğunu kendi yaş gruplarında var olabilmek, sosyal ilişkilerini sürdürebilmek ve dışlanmamak olarak belirtmesi de benzer ve kendi araştırma sonuçlarımda ulaştığım bir bilgidir. “Orada” bir sosyal platformunda olmamak, verisini paylaşmamak bir anlamda dışlanmakla ilişkilendirilmekte ve bu daha çok küçük yaşlarda meydana gelmektedir. Bireyler toplumda var olabilmek adına mahremiyetlerinin dönüşümüne şahit olmakta ve Giddens’ın da bahsettiği soyut sistemlere güvenerek sosyal ilişkilerini de bu düzeneklere güvenerek devam ettirmektedirler.

Sosyolojide ontolojik güvenlik, bireylerin davranışlarının ve inançlarının özneler arası inşa edilme biçimleriyle ve bu özneler arası yapıların, birbirleriyle ilişkisel olarak yerleştirilen ve bazı durumlarda birbirine karşıt olarak yapılanan sosyal olarak oluşturulmuş bütünler, kimlikler yaratma biçimleriyle ilgilidir (Croft, 2012). Bir anlamda da bireyin kendi güvenliğine ilişkin davranış ve inançlarına odaklanmaktadır. Aynı şekilde büyük veri konusunda da temel makineye duyulan inanca dayanmaktadır. “Makineye duyulan inanç onu kullanmanın ön koşuludur, bu ise otomatize tepkilerin otomatize olmayanlardan daha güvenilir olduğuna ilişkin başka bilişsel önyargıları beslemektedir” (Bridle, 2020, s. 49).

Çoğu birey büyük veri ile ilgili bilgi sahibi olmasa da onun verdiği bilgilere ve sağlayabileceği avantajlara güvenmekte ve çoğunlukla bunun sonuçlarını göz ardı etmekte ya da önemsememektedir. “Büyük verinin büyülü yanı budur işte. Üzerine çalıştığınız konuya dair hiçbir şeyi gerçekten bilmeniz veya anlamanız gerekmez; tüm inancınızı dijital enformasyondan çıkarılan hakikate bağlayabilirsiniz. Büyük veri safsatası, bilimsel indirgemeciliğin mantıksal sonucudur bir bakıma; karmaşık sistemlerin kurucu parçalarına ayrılarak ve bu parçaların her biri ayrı ayrı incelenerek anlaşılabileceği inancının” (Bridle, 2020, ss. 92-94). Büyük veriye ve işlemlemeye yönelik bu tür analizlerin ne ifade ettiği ve karar verme mekanizmalarındaki yeri, bu şekilde daha soyut kalsa da yine aynı yazarın verdiği bir örnekle net bir şekilde anlaşılmaktadır.

“Death Valley Ulusal Parkı’ndaki korucular, yabancısı oldukları bir bölgede duyuları yerine GPS talimatlarını izleyen gezginlerin başına ne geldiğini tarif etmek için özel bir terim bile geliştirmişler: “GPS Ölümleri”. Normal araçlarla geçilemez uyarısı bulunan pek çok yolun olduğu ve sıcaklığın gündüz elli dereceyi bulduğu kurak bir bölgede, kaybolursanız ölürsünüz. Yukarıda bahsi geçen örneklerde GPS sinyali ne gizlenmiş ne de saptırılmıştı. Bilgisayara basit bir soru sorulmuş, o da yanıt vermişti- ve insanlar bu yanıta ölümüne inanmıştı” (Bridle, 2020, s. 52). Bireyler duyuları yerine, GPS’e büyük verinin onlara sunduğu bilgiye inanmış ve bu durum sebebiyle ölmüşlerdir. Belirli bir yerde kaza olup olmadığı, hangi yolun daha güvenilir olduğu, hangi yolun daha erişilebilir olduğu diğer kullanıcıların verilerinden alınan bilgilerle hatta günümüzde onlar araba sürerken “Hala orada kaza var mı?” gibi sorulara verilen cevaplarla desteklenmektedir. Sürücüler ya da bireyler ise doğrudan bunlara güvenmektedir ama bu güvenin sonucu bu örnekte olduğu gibi hiçbir zaman o kadar güvenilir veya net olmayabilir. Bunun sebebi yeni gözetim pratiklerinde bireyin ve verisinin temel ürün haline dönüşmesi, gözetim kapitalizmidir.

Mahremiyetin dönüşümü ve ontolojik güvenlik bağlantısıyla ilgili en önemli nokta gözetim kapitalizminde, ürünün, kullanılacak, işlenecek ve depolanacak

nesnenin birey ve bireyin verisi haline gelmesidir. “Mahremiyet sorunları, bir anlamda, şirketlerin bedava hizmetlerinden kaynaklanmaktadır. Ürün siz olduğunuzdan, hizmetler ücretsizdir. Sizin kişisel verileriniz, ücretsiz hizmetlerin karşılığını ödemenin bir yolu olarak anlaşılır. Ne yaptığınız, nerede olduğunuz, internetteyken neyin üzerine tıkladığınız ve ne satın aldığınız değer kazanır. Sizin verileriniz ve kendiniz, sizi ticari anlamda ilginç kılacak bir biçimde tümleştirmektedir (Lokke, 2020, s. 71).

Birey ve verilerinin, büyük verinin bir tür sermaye haline gelmesi ve o verilerle kavramsal çerçevede de bahsedildiği şekilde bir içerik elde edilmesi toplumsal düzenek ve ilişkileri dönüşüme uğratmaktadır. Bunun en net örneklerinden bir tanesi itibar puantajı, profil çıkarma ve kartografinin mümkün hale gelmesi ve temel olarak bunların her birinin birer sınıflandırma aracı haline gelerek güç kazanmasıdır. Facebook, güncel durumda yeni neslin artık o kadar kullanmadığı bir sosyal medya platformu olmasa da, Cambridge Analytica örneğinde de olduğu gibi bir ülkenin siyasi seçim sonuçlarını etkileyecek güce sahip bir sosyal iletişim uygulaması olmayı başarmış, Google gerçekten insanların başkalarının kim olduğu, her sorunun ona sorulduğu ve soruların bile her bireye farklı algoritmalarla cevap verdiği bir güç haline dönüşmüş, sonuç olarak tüm bu sistemler insan hayatının belirleyici temelleri haline gelmiştir. Bir kişinin statüsünün, mesleğinin, deneyiminin LinkedIn’den kolayca görüldüğü ve orada hesabı yoksa çok fazla kariyer amacı olmadığının düşünüldüğü, Instagram hesabı yoksa sosyalleşmek istemediği, arama motorlarında ismi ya da bir bilgisi çıkmadığı durumlarda şüphe duyulduğu bir dönemde ontolojik güvenlik ya da güvensizlik çok daha büyük önem taşır hale gelmiştir.

Giddens, bu süreci modernlik, zaman ve uzamın ayrılması, yerinden çıkarma düzeneklerinin gelişimi ve bilginin düşünümsel temellükü olmak üzere 3 temel dönüşüme dayandırmaktadır. “Yerinden çıkarma düzenekleri toplumsal ilişkileri ve enformasyon değişimini belirli zaman-uzam bağlamlarından kaldırır; ama aynı zamanda bunların yeniden yerleştirilmesi için yeni fırsatlar sağlar. Bu modern dünyayı büyük, kişilik dışı sistemlerin giderek kişisel yaşamın çoğunu

yuttuğu bir yer olarak görmenin neden yanlış olduğuna işaret eden diğer bir nedendir" (Giddens, 2021, s. 139). Uzmanlık sistemleri, yerinden çıkarma düzenekleridir çünkü simgesel işaretlere benzer olarak, toplumsal ilişkileri bağlamın dolaysızlığından çıkarırlar (Giddens, 2021, s. 34). Simgesel işaretlerin yaratılması, Marx'ın paradan evrensel fahişe olarak bahsetmesi gibi, herhangi bir özel konumda onları elinde bulunduran kişi ya da grupların belirli karakteristiklerine bağlı olmaksızın "elden ele geçebilen" mübadele araçları-siyasal meşruiyet araçları gibi, para gibi şeyler yaratmasıdır (Giddens, 2021, s. 28). Buradaki önemli nokta ise büyük verinin de burada bahsedilen şekilde evrensel bir sermaye haline gelmesi ve güç dengelerinin temeline oturmasıdır. Büyük veri hem ekonomik hem de kültürel, siyasal, toplumsal ilişkilerin temelinde önemli bir etken olarak dijital toplumlarda göze çarpmaktadır. Mahremiyetin dönüşümünde en etkin rol oynayan araçlardan biri olarak da bireylerin ontolojik güvenlik ya da güvensizliklerinde de simgesel işaret olarak değerlendirilebilirler, aynı şekilde bu sistemlerin işlediği uzmanlık sistemleri de bir tür yerinden çıkarma düzenekleridir ve toplumsal ilişkileri doğrudan etkilemektedir.

"Bütün yerinden çıkarma düzenekleri hem simgesel işaretler hem de uzmanlık sistemleri, güvene dayanır. Bu nedenle güven, modernlik kurumlarının çok önemli bir parçası olmuştur. Burada güven kişilere değil, soyut niteliklere karşı duyulmaktadır" (Giddens, 2021, s. 32). Bir firmaya işe alınmak için başvuran birinin siyasi görüşüne, sosyal ağına, önceki deneyimlerine, beğenilerine, tüketim pratiklerine ve daha pek çok bilgisine erişebilir olmak bireyin kendi hakkında ne dediğinden çok onun hakkındaki itibar puantajının, profil çıkarmanın ve kartografinin ne olduğunu öne çıkaran bir sistemi açıklamaktadır. "Sokaktaki adamın uzman sistemlere duyduğu güven ne bu tür süreçlere tam bir katılıma ne de söz konusu süreçlerin ürünü olan bilgiler üzerindeki uzmanlığa dayanır. Bir bakıma güven, kaçınılmaz olarak, inancın bir parçasıdır" (Giddens, 2021, s. 35). Aynı şekilde bireylerin sosyal medya platformlarında, kendi sosyal alanında var olmak ve hayatın her alanında var olabilmek için verilerini paylaşması da bu sistemlere kaçınılmaz olarak güvenme

zorunluluğunu açıklamaktadır. Modernlik, soyut sistemlere ve buradaki soyut kurallara güveni zorunlu kılmaktadır. Birey, güvenlik koşullarını içeren kendisini bilgilendiren metinleri okumayıp, tüm verilerini işlemek için talep edilen çerezleri onaylarken bunların neleri içerdiğini değil, sadece onu güvende tutacağına inanarak hareket etmektedir. “Yerinden çıkarma düzenekleri açısından güvenilirlik ise, inanılırlık yine merkezi önemde ve nitelikler de kuşkusuz işin içinde olsa bile farklıdır. Soyut sistemlere güven, bu sistemlerden bir biçimde sorumlu olan birey ya da topluluklarla hiçbir karşılaşmayı gerektirmez. Ancak çoğu durumda bu tür birey ya da topluluklar işin içindedir. Giddens, bu kişi ya da kişilerle gerçekleşen karşılaşmaları soyut sistemlere ulaşma noktaları olarak yorumlamaktadır” (Giddens, 2021, s. 81). Bu sistemlere güvenmek için hukuki danışmanlara, teknik desteğe bu anlamda bilgili olan kişilere danışmayı çoğu birey talep etmese de bu kişiler her zaman sürecin içindedir ve bu sistemlerin nelere hizmet ettiğini, süreci ve bu sürecin nereye doğru gittiğini bilen kişilerdir. Bu anlamda büyük veri ile ilgili süreci bilen kişiler veri bilimcilerdir.

Bu dönüşümler ise, kişisel güvenin bireylerin üzerinde çalışacakları bir proje haline gelmesine sebep olmakta ve ilişkiler güvenin var olmayıp, yaratılmaya çalışıldığı bir şey haline gelmesine sebep olmaktadır. “Turkle ilişkilerimizde hissettiğimiz güvensizlikten ve mahremiyetimizle ilgili duyduğumuz kaygıdan dolayı hem ilişki içerisinde olmamızı sağlaması hem de ilişkilerden bizi koruması için teknolojiden medet umuyoruz” demektedir (Turkle, 2011 akt. Bauman ve Lyon, 2020, s. 49). Giddens, ontolojik güvenlik kavramıyla günümüzdeki güven ve mahremiyet ilişkilerini sorgularken, büyük veri gibi sistemlerin de bu anlamda tekrar düşünülmesine imkân sağlamakta ve gözetim, verileştirme ve veri gözetiminin kişisel güven sağlama anlamındaki rolüne teorik bir zemin sunmaktadır.

Giddens'a göre ontolojik güvenlik, insanlar her türlü olasılığı bir kenara atabileceklerine güvenebildikleri ve bu nedenle sosyal bir normalliğe, bir öngörülebilirliğe güvenebildikleri ve daha sonra pratik günlük etkileşimlerini doğal, normal ve sağduyu ile dolu olarak yapılandırdıkları zaman sağlanır

(Croft, 2012). “Eğer koşullar bireyin yerleşik davranış kalıplarının ve öz-anlatılarının devamını engeller, geçersiz kılar ya da bu kalıp ve anlatılarda radikal bir değişim doğurursa, bu durum bastırılan “temel ontolojik sorunlar”ın yüzeye çıkmasına neden olacaktır. Bu şartlar altında aktör, kendisinin ve çevresinin devamlılığına dair güvenini kaybeder ve kendini derin bir kaygı durumunun içerisinde bulur” (Rumelili ve Adisönmez, 2020). “Cemaate ait olmak hiç kuşkusuz daha fazla kısıtlama ve yükümlülük içerse de bir ağa dahil olmaktan çok daha emniyetli ve güvenilirdir” (Bauman ve Lyon, 2020, s. 52). Bireyler eskiden daha yerel ağlara, akrabalık ağları, fiziksel olarak görüştükleri ve etkileşim kurdukları bireylerle daha fazla kısıtlama ve yükümlülük içeren ilişkilere dahilken; bu sistemler sebebiyle çok daha geniş ve soyut ilişkiler ağına dahil olmaktadır. Bu ağ, eski yerel ağlar kadar emniyetli ve güvenilir görülmemektedir.

Bu çalışmanın amacı, dijitalleşme ile kişilere, sistemlere, gruplara ve kurumlara duyulan güvenin nasıl oluştuğunu kuramsal olarak sorgulamayı, mahremiyetin gözetim ile dönüşümünü göz önünde bulundurarak, ontolojik güvenlik ve büyük veri arasındaki bağlantı üzerine düşünmeyi hedeflemektedir. Büyük verinin, tıpkı para gibi simgesel bir işaret sistemi olup olmadığı, büyük veri temelli sistemlerin de bir tür uzmanlık sistemi olarak kabul edilip edilemeyeceği tartışılmaktadır. Bu temelde büyük veri ve büyük veri sistemleri, iki tür yerinden çıkarma düzeneği olarak günümüz dijital toplumlarında yer almakta ve Giddens’ın da öngördüğü şekilde bu yerinden çıkarma düzenekleri ile olanaklı/beklenen/elverişli geleceklerin listelenmesi yapılmaktadır. Yerinden çıkarma düzenekleri, ilişkileri yeniden yerleştirme ile başka bir boyuta taşımakta, güven örtülü ya da görünür bağlılıklar kavramlarıyla tekrar düşünülmektedir.

“Enformasyonun kendisinin sorunlara karşı çözüm önerileri sunmak yerine, geleceği öngörememe anlamında başlı başına sorunlar yumağının kaynağını oluşturduğu genel bir belirsizlik söylemini yapılandıran medya, gitgide ontolojik güvensizlik ve risk algılamasını bireysel/toplumsal krizi ve histeriyi derinleştirici bir işlev kazanmıştır. Bireyleri problem çözme yetisi ve becerisiyle etkin birer

özne olarak değil de sürekli olaylara maruz kalan ve durmadan kendisine bir şey yapıldığı izlenimini güçlendiren bir nesne olarak konumlaması durumu söz konusudur" (Köse, 2007). Ontolojik güvenlik, biyografik süreklilik inşa etme, bir güven ilişkileri ağı kurma, kendi bütünlüğüne uygun hareket etme ve Kierkegaard'ın kullandığı anlamda ontolojik güvensizliğe veya korkuya karşı mücadele etme ihtiyacı açısından anlaşılabilir (Croft, 2012). İçinde bulunulan durum ya da konum ontolojik olarak ne kadar güvenli olursa olsun, bu konumda her zaman bir kırılganlık ve sağlamlık vardır. Her zaman ontolojik güvensizliğin zıt kutbuna, korku nedeniyle eylemin felce uğramasına dair bir farkındalık vardır. Ontolojik olarak güvenli birey, bu konumda asla her zaman güvende olamaz; her zaman bir belirsizlik vardır (age, 2012).

Giddens, tüm bu değerlendirmelerin sonucunda ise söz konusu belirli alandaki uzmanların da bu tür riskler ve tehlikeler karşısında "az bilgili bireyler" gibi bölünme eğilimi gösterdiklerini belirterek bu davranış tutumlarını, pragmatik kabulleniş, sürekli iyimserlik, alaycı kötümserlik ve radikal katılım olarak gruplandırmaktadır. Lash tarafından tanımlanan pragmatik kabulleniş tepkisinde, modern dünyada olup bitenlerin bireyinin kontrolü dışında olması sebebiyle, yalnızca geçici kazanımlar için plan yapılabilir ya da umut beslenebilir inancı bulunmaktadır. Bu durum örtülü bir kötümserlik ya da umudun beslenmesi şeklinde desteklenmektedir. Sürekli iyimserlikte ise akla duyulan inanç ile toplumsal ve teknolojik çözümlerin her zaman var olduğu ve olacağı, bilimin başka hiçbir yönelimin karşılayamayacağı uzun dönemli güvenlik kaynakları sunduğu inancı yer almaktadır. Alaycı kötümserlik de ise, umursamazlık değil, bir tür bastırma göze çarpmaktadır. Bastırma, kaygıların duygusal etkilerini mizahi ya da bezmiş şekilde bastırılmasıdır, önemli olan burada ve şimdinin keyfini çıkarmaktadır. Son tepki olan radikal katılımda ise önemli sorunların olduğu bilinci vardır fakat bunların aşılabileceği ve harekete geçilmesi gerektiğine yönelik bir inanç olduğu görülmektedir (Giddens, 2021, ss. 133-135).

3.4. DİJİTAL GÖZETİMİN TEMELİNİ OLUŞTURAN KURAMLAR

3.4.1. İçselleştirilmiş Gözetim (Michel Foucault)

Gözetim kuramlarına bakıldığında hepsinde geçen “Panoptikon”, güç, iktidar, denetim, disiplin, kontrol gibi kavramların temelinde Foucault’ya dayandığı ve içselleştirilmiş gözetimden yola çıkarak ya da onun eleştirisiyle ilerlediği görülmektedir. Bu amaçla dijital gözetimin temel aldığı kuramları incelerken Foucault’nun panoptiği temel alan kuramından sonra, post-panoptik görüşün temsilcisi sayılan Deleuze ve Guattari daha sonra ise daha çağdaş gözetim kuramları açıklanmaktadır.

Günümüz gözetim sistemleri incelendiğinde sosyal sapmayı engellemek için yapılan düzenlemelerin genel olarak suç ile yan yana düşünüldüğü fakat ikisinin çok farklı tanımları olduğu bilinmektedir. Sosyal sapma ve kontrolden söz edildiğinde akla ilk olarak toplumda “normal’’ olarak belirlenmiş davranışların dışına çıkan bireyler ve bu bireylerin belirli yasalarla, cezalarla ya da çeşitli toplumsal yöntemlerle kontrol edildiği düşüncesi akla gelmektedir. Sapma davranışları genel olarak suçla ilişkilendirilmektedir. Dolayısıyla suçun cezalandırılma biçimi, en temel olan hapishaneler ya da cezai yaptırımlardır. Bireyler bu yolla kontrol altına alınırlar; suçlu bireyler toplumdan tecrit edilir ve diğer bireylere de aynı davranışlarda bulunduklarında bu tarz cezalarla karşılaşacakları düşüncesi dayatılır. Fakat durum bunların hepsinden apayrı bir boyuttadır. Sapma ve suç aynı şeyler değildir. Sapma olması gereken biçimden uzaklaşma anlamına gelmektedir. Bireyler sadece suç olarak tanımlanan eylemleri gerçekleştirdiklerinde çeşitli yaptırımlarla yüzleşmezler. Bireyleri kontrol etmek için çeşitli doğrudan yaptırımlara da gerek yoktur. Foucault’nun bu konuda önemli bir isim olmasının sebebi, klasik ceza kuramlarındaki egemenlik merkezli suç ve cezayı temel alan görüşün dışına çıkarak “egemenlik yerine disiplin, hukuki söylem yerine pozitivist sosyal bilimler, suç ve ceza terimleri yerine sapma ve gözetim, denetim terimleri bağlamında işleyen farklı

bir oluşumun tarihsel kuruluşuna dikkat çekmiş olmasıdır'' (Özkazanç, 2007, s. 2).

Foucault, biyopolitika kavramı ile insan bedenini değil, hayatın kendisini düzenlemeyi kastetmekte, bu kavram etrafında en çok önem verdiği şey olan "özne''nin değişimini, toplumsal değişimleri ve bu bağlamda iktidar konusunu incelemektedir. Disiplin ise iktidar ile ilerleyen bir kavramdır ve iktidar kavramının içeriği değiştikçe disiplin tanımının da bambaşka bir hale büründüğü gözler önüne serilmektedir. İktidar ise doğrudan incelenebilecek bir şey değildir, iktidara bağlı olan öznelere bakılarak bu konuda bir bakış açısına ulaşılabilmektedir. Egemenlik denildiğinde bahsedilen iktidar türü "iktidar alanını toplumsal alandan ayıran, iktidarı toplumsallık üzerinde hâkim kılmayı hedefleyen ve dolayısıyla yasaklarla, dehşetengiz cezalarla iş gören egemenlik paradigması, siyaset biliminin klasik iktidar anlayışına denk düşer'' (Gambetti, 2008, s. 2). Bu bakış açısına göre, devletin gücü merkezi güçtür ve devlet gücünü yaptırımlar uygulayarak kullanır. Kontrol anlayışı cezalarla sağlanmaktadır. Fakat bu ilk, hatta 17. yüzyıl öncesi hapishanelerin doğuşundan önceki dönemde tanımlanan bir iktidar türüdür.

Hapishanenin Doğuşu (1975) adlı çalışmasıyla ise gözetim, kontrol ve mekânsal olarak ayrıştırma meseleleri gündeme gelmekte, bu yolla bedenlerin belirli normlara uygun hale getirilmesi konusu konuşulmaya başlanmaktadır. Hapishane değil eğitim kurumları, bakımevleri, akıl hastanesi gibi örnekler de analizlerde yer almaktadır, burada insanlar önceden oluşturulmuş belirli bilgilere göre disipline edilmeye çalışılmaktadır. Ya devlet ya da dolaylı olarak devletin düzenlemesi buralarda yer almaktadır. İnsanlar bir ortamda kapalı tutulmaktadır. Bentham'ın geliştirdiği panoptik modeli; gardiyanların hapishanenin gözetleme kulesinden onları görebilmesi fakat karşı taraftan görülememesi çerçevesinde kurulmuş bir modeldir, bu model iktidarın kolay ve rahat işlemesini sağlayan bir yeniliktir tabi bu model 18. yüzyılda yerini "görünürlük ilkesine" bırakmaktadır (Eroğlu,2016, ss. 47-48).

Foucault'nun panoptik modelde önem verdiği şey ise öznelerin konumlarıdır ve özneler "gözetlenen özneler'' olarak yer almaktadırlar. "Gözetlenen özneler, tıpkı Bentham'ın Panoptikon ütopyasında arzulandığı gibi, normları içselleştiren ve iktidarı kendi öznelliğinde yeniden üreten özneler haline geleceklerdir" (Gambetti, 2008, s. 2). Bu süreçten anlaşıldığı haliyle, egemen iktidarda doğrudan bir yaptırım ve merkezi devlet tarafından belirlenen normlar vardır. Bu normları devlet belirler ve bireyler bunlara uymak zorundadır. Kontrol, güç ve fiziki yaptırıma dayanan bir olgudur. Yukarıda benzetildiği haliyle "dehşetengiz cezalarla" ilerlemektedir. Fakat hapishane ve panoptikon kavramında görüldüğü haliyle norm ve disiplin yavaş yavaş değişmeye başlamıştır. Normlar yine devlet tarafından belirlenmektedir fakat uygulanma aşamasında eğitim kurumları, akıl hastaneleri, hapishaneler vardır. Artık sadece suç durumunda bireyleri cezalandırma gibi düşüncelerin yerini yeni disiplin mekanizmaları düzenleme, hesaplama, sınıflandırma, gözetleme, kontrol, ayrıştırma, mekânsal olarak düzenleme gibi birçok kavram almıştır.

Panoptikon kavramı ile en çok öne çıkan kavram ise gözetim olmuştur. Bireye zorla dayatılan normlar yerine, gözetlenen öznelerin normları içselleştirdiği ve kendi öznelliğinde yeniden ürettiği gözlemlenmiştir. Belki de bunun farkına varılması daha sonraki süreçlerdeki norm, disiplin ve denetim toplumu kavramlarının yerinin veya içeriğinin tamamen değişmesine sebep olmuştur. Bu noktaya kadar bahsedilen toplumlar, disiplin toplumları olarak açıklanmaktadır. Bu toplumlarda disiplin mekanizmaları standartlaştırılmaya dayanmaktadır. Okul, hapishane, akıl hastanesi örneklerine baktığımızda hepsinde bireyleri tek tipleştirme hedefi Foucault'nun ilgisini bir hayli çekmektedir. Hepsinde toplumdaki belirli normları bireylere aktarma ve onları disipline etme ya da toplumdaki disiplini (düzeni) sağlama amacı bulunmaktadır. Dolayısıyla bu düzene, normlara uymayan ve disiplini bozan bireyler disiplin toplumlarında bahsedilen şekillerde cezalandırılmakta ve kontrol altına alınmaktadırlar. Hukuk bu noktaya kadar suç ve ceza kavramlarının içeriklerini açıklayan, neyin yapılabilir neyin yapılamaz olduğunu açıklayan bir sistem olarak görev yapmaktadır. Gambetti'nin makalesinde genel olarak anlattığı şekliyle gözetim,

teşhis, değiştirme, dönüştürme, polisiye, tıbbi, psikolojik, mekânsal, askeri teknikler gibi pek çok alanda kullanılmaya başlanmıştır, bu süreç Foucault'ya göre en başta normalizasyon değil normasyondur. Normasyon denmesinin sebebi normalle anormal arasındaki sınırın normlarla çizilmesinden kaynaklanmaktadır (Gambetti, 2008, s. 3).

18. yüzyıl sonrasında ise daha farklı iktidar tipleri ortaya çıkmıştır ve kontrol olgusu bambaşka bir hal almıştır. Disiplin beden siyaseti üzerineyken, düzenleme nüfus ile alakalıdır ve biyopolitika kavramı burada devreye girmektedir. Bedeni değil, hayatın kendini düzenleme artık sosyal kontrol denilen kavramın temeline oturmaktadır. Foucault, birçok eserinde biyopolitikayı biyoiktidar kavramı ile açıklamaktadır. "Biyoiktidar", nüfus, göç, bilgi ve liberalizm üzerinden şekillenen küresel güç ilişkilerini kapsayan ve 20. yüzyıl sonları itibariyle daha çok denetim toplumu içerisinde, yönetimsellik (gouvernementalité) tekniklerini ifade eden siyasal bir olgu olarak öne çıkmaktadır'' (Sustam, 2016).

İnsanın temel biyolojik özellikleri, kontrol için kullanılması gereken, siyaset tarafından kullanılan bir nesne haline gelmektedir. Bu tanımın içerdiği diğer önemli bir husus ise disiplin toplumundan denetim toplumuna geçiştir. Disiplin toplumu yukarıda açıklanan tüm özellikleri taşıyan bir toplumken; denetim toplumuna geçilmiştir. Denetim toplumu sürekli denetimi ve kontrolü düzenli olarak planlayan bir toplum akla getirmemelidir. Foucault'nun biyopolitik ve biyoiktidar kavramlarına yoğunlaşıldığında, denetim toplumlarında, yaşam ve varlık önem kazanmaktadır. Bu politika akışına bırakma politikasıdır. Riskler doğal olarak kabul edilir ve bunlar üzerinden kontrol sağlanır. Beden yaşam politikasının merkezindedir. Beck'in bahsettiği risk toplumu bu iktidar tipi altında tanımlanabilmektedir çünkü "güvenlik" merkeze oturmaktadır. Biyoiktidar "yeni bir sanal bios (yaşam) arzusuna uyum sağlayan yeni tüketim ilişkileri (doğal yaşam, Pazar ve organik beslenme) ve yeni özellikler yaratmaktadır" (Sustam, 2016). Güvenlik, riski kabullenmektedir. "Dispositif" kavramı ise riske müdahale aygıtlarını ve gerçekle ilişkilendirme süreçlerini temsil etmektedir. Disipliner

iktidar normasyonla ilerlerken (bu noktada normun ve disiplinin konumu çok nettir yukarıda bahsedildiği üzere) ve normların belirlenip bireylerin bunlara uyumlu hale getirilmesi iken; şu an bahsettiğimiz biyoiktidar ve güvenlik kavramlarıyla normalizasyon göze çarpar. Güvenlik, normalliği belirler ve bu aşamadan sonra normlar belirlenir. Gambetti'ye göre ilki araçsalken, ikincisi faydacıdır. Burada verilen örnek sosyal kontrolün, disiplinin ve normun ne konuma geldiğini çok net anlatmaktadır. Biyopolitika bir yaşam politikasıdır. Varlığı göz önüne alır. Burada sosyal kontrol söz konusudur. Fakat çocuk ölümlerine bakıldığında, bir toplumda genç nesil oranlarına bakılarak, doğum oranlarına bakılarak doğum sayısının gerekliliği hesaplanmaktadır. Burada asıl hedeflenen, doğrudan çocuk ölümlerinin önüne geçmek değildir. Toplumdaki ölüm-doğum dengesini sağlayabilmektir. Bu amaçla gelişen kontrol mekanizmaları ise biyopolitiğin başta bahsedilen egemen iktidardan farkını ortaya koymaktadır. İktidar bu anlamlarda doğrudan yönetme yönetilme olayı değildir. Foucault'nun amacı bunların nasıl şekillendiğini göstermektir. "İktidar, insanları yönetme durumundan çıkarak, giderek insan ihtiyaçlarını yönetme ve bu yönetimi idare etme durumuna dönüşmüştür. İktidarın, yaşamı hesaplanabilir ve iktisadi biçimde üretken kılınabilir formlara sokarak yeniden yapılandırmaya dönük mekanizmaları devreye sokması yeni bir yönetim sanatını hâkim kılmıştır. Bu yeni yönetim sanatı, yaşamı kontrol etme üzerine değil, yaşamı üretken kılma üzerine temellendirilmiştir'' (Baştürk, 2012, s. 76).

Sonuç olarak, biyopolitika ile sosyal kontrol bambaşka bir hale bürünmüş, insan yaşamının her yönü daha çok kontrol altına alınmıştır. Güvenlik talep ederken, insanlar kontrol edilmeyi kabullenmekte hatta kontrol edilmeyi kendileri talep etmektedir. Günümüzde alışveriş merkezlerinin mekânsal olarak ayrışmış olması, sürekli kameralarla izlenmeyi güvenlik için kabul etme, güvenlik güçlerinin her yerde olmasını normal ve gerekli olarak algılama, internet üzerinden yapılan işlemlerde her aşamada kontroller olması ve buradaki kimlikleri bile daha da korumaya çalışmak ve bu kimlikler için bile endişe duymak gibi birçok etken güvenlik; kontrol (denetim) toplumunun getirdiği

süreçlerdir. Sosyal kontrol artık içselleştirilen, kabullenilen ve bireylerin tüm zamanlardan daha çok kontrol altına alındığı bir haldedir.

İçselleştirilen ve kabullenilen bu gözetim, panoptik güç çerçevesinde sağlanmakta ve bireyler söylemsel normlarla bir tür hapsolma sürecine dahil olmaktadır. Fakat bu hapsolma tamamen öznelerin yönetildiği bir süreci değil öznelerin panoptik göz ile sürekli kontrol altında olduğu bir süreci işaret etmektedir (Baştürk, 2017, s. 2). Foucault'nun "self-surveillance", içselleştirilmiş gözetim olarak, kavramsallaştırılan kavramı ile vurgulanan, panoptisizm mantığına dayanmaktadır. Mahkumlar, gardiyanın onları ne zaman izlediklerini asla bilemedikleri için, kendi davranışlarını gözetlemeyi öğrenmektedir ve kendi disipline süreçlerine etkili bir şekilde katılmaktadır. Kendini gözetleme ve kendini disipline etme panoptik modelle oluşmuş ve iş yeri, okul, klinik gibi alanlara da uygulanarak otonom bireyin disipline olmuş ve "rasyonel" özne olmasını sağlamaktadır (Campbell ve Carlson, 2002, s. 589).

Panoptisizm mantığına dayanan denetim toplumu yerine, bu düşüncelerin temellerini eleştirerek Deleuze ve Guattarı ise rizomatik gözetim ve kontrol toplumu kavramlarıyla, post-panoptik düşüncesinin temellerini atmıştır.

3.4.2. Rizomatik Gözetim (Gilles Deleuze ve Felix Guattari)

Deleuze, Foucault'nun disiplin toplumlarını post panoptik bir düşünceyle eleştirerek, kontrol toplumları olarak ele almaktadır. Disiplinin bir tür amaç ya da yönetim için itici güç olduğu düşüncesi yerine bir tür kontrolde bunu aramaktadır. Kapitalizm ve küreselleşmenin toplumları değiştirdiğini ve okul, hastane ya da fabrika gibi kurumların nasıl birer şirket haline geldiğini düşünmektedir. Disiplin uzun erimli, sabit ve uysal/itaatkâr bir toplum için en az miktarda kaynakla devlet temelli hedeflere ulaşmayı amaçlarken, şirketlerde kısa erimli sonuçlar düşünülerek, pazarın, iş gücünün ve stratejilerin sürekli kontrolü, sürekli gözetimi ve değerlendirilmesi söz konusudur. Marangozluğu (daha geleneksel bir meslek olduğu için dönüşümü göstermek adına), şirketlerin

bir tür kodlanmış figürü olarak ele alarak, bir gün değerli olan niteliklerin sistem değiştiğinde gereksiz hale geleceğini belirtmektedir. Gözetim anlamında da bireyler değil, onların temsili söz konusudur. Bunu “bölünmüş birey” (divided individual) kavramıyla açıklamaktadır. Bölünmüş birey ile bireye tam ve bütünleşik bir oluş olarak değil, birçok role sahip olan ve birçok yerde temsil edilen veri bankaları gibi yaklaşmaktadır (Galic, Timon ve Koops, 2017). Deleuze, gözetim sistemleri ile bireyleşme olarak kavramsallaştırdığı durumu çok net bir şekilde bağlantılandırmaktadır. Bireyler artık, sayısallaşma kavramıyla da anlatıldığı gibi, sistemlerde yer alan anonim sayılardan ibarettir, veri bankalarıdır.

Deleuze, disiplin toplumlarından kontrol toplumlarına geçişi anlatmak için Foucault’dan farklı bir yol izlemektedir. Deleuze, disiplin toplumlarının iki kutbu olduğunu belirtmektedir: “Bireyleri temsil eden imzalar ve bireylerin bir kitle (ve biçim) içindeki yerlerini temsil eden kayıtlardaki sayılar (istatistiksel korelasyonların temeli). Bu kutuplar arasında herhangi bir çelişki veya karşıtlık yoktur. Disiplinli toplumlar, iktidarı bireyselleşme ve kitleselleştirme yoluyla her iki şekilde de uygular. Ancak kontrol toplumlarında bu ikilik, ince ayarlamalar yapabilen tek bir sistem olarak işlemektedir.

Deleuze’ün iddiasına göre imzalar ve sayılar, bilgiye erişiminiz olup olmadığını belirleyen parolalarla değiştirilir. Şifreler sırayla kodlardır ve kodlar dijital sistemlerde yeni kontrol dilidir. Dijital kontrol biçimlerine geçiş, büyük bir soyutlamayı ve buna tekabül eden homojenleştirmeyi hem bireylerin hem de kitlelerin bilgi paketlerinde, bitlerde, sinyallerde ve spektrumlarda kaybolmasını içerir. Bireyler (bireyin örgütlenmesinin çeşitli düzeylerinde denetime tabi olan) ve kitleler numuneler, veriler, pazarlar veya “bankalar” haline gelmektedir” (Deleuze, 1988 akt. Bogard, 2006, s. 62). Burada temel olarak bahsedilen şey bireyin tamamen veri bankaları olarak görülmesi ve bireylerin sistemler içerisinde sayısallaştırılmasıdır.

Kontrol toplumlarının yanısıra, post-panoptik gözetimde vurgulanması gereken bir diğer kavram ise “yeniden yer edinme” (reterritorialization) kavramıdır. Yeniden yer edinme temelinde, gözetim pratiklerindeki güç ilişkileri tekrardan düşünülmekte ve sorgulanmaktadır. Deleuze ve Guattari için güç, arzunun (varlığın potansiyel formu) alınarak tekrar başka bir uçakla yeniden adlandırılmasıdır ve bu süreci “lines of flight” kavramsallaştırmasıyla açıklamaktadırlar. Onların görüşü, arzu ve bastırmaya dayandığı için dışsal bir güç fikrini reddederler. Yeniden yer edinme ile ise, iktidarın normları bedensel koşullara göre dönüştürebilir ve ilişkilendirebilir olmasıyla ilgilidir (Baştürk, 2017, s. 6). Post-panoptik görüşte, Foucault’nun aksine güç ilişkileri yönetişimin bir elemanı ya da yapısı değildir. Alanlar ve öznelerden akıp giden, özneleri dışarıdan kısıtlamayan bir güç akışıdır. Güç akışı ve alanlar boyunca bu süreç olduğu için kontrol toplumlarında dışsallık düşünülemez bir şeydir (Baştürk, 2017). Güç onun için “erişimi kontrol etmektir”. Erişim noktaları ise havaalanları ya da sınırlar gibi noktalar olarak belirtilmektedir. Foucault’da kapalı alanlar, kapatılmış kurumlar (fabrika, hastane, hapishane gibi) yer alırken, Deleuze’de açık alanlar ve noktalar, uzak mesafeden kontrole dikkat çekilmesi göze çarpmaktadır ve Deleuze bir anlamda post-panoptik literatürünün kurucusu olarak kabul edilmektedir (Galic, Timon ve Koops, 2017).

Disiplin toplumundan kontrol toplumuna geçişin tarihinden ve siyasi bir hareket olarak ele alınmasından bahsederken, kurumların merkezileşmiş güçlerinden bir tür rizomatik kontrol yapılarına geçişe değinilmektedir. Bu yapılar, dışsal disipline edici güç yapılarının daha akışkan ve gündelik hayat pratiklerinin farklı noktalarında gömülü hale gelmektedir. Bu değişken ortamda ise verilerden iki temel gözetleme modu ortaya çıkmaktadır. İlki sabit ve somut olan, gücün panoptik gözetleme durumunda olduğu gibi yukarıdan aşağıdan izlenebilir olduğu; ikincisinde ise güç yapılarının daha dağınık ve rizomatiğe benzer heterojen formlarda olduğudur (Nemorin, 2017, s. 242). Gözetimin rizomatik genişlemesini ve disipline edici-olmayan biçimlerine dikkat çekmek için “gözetim

asamblajı" kavramı kullanılarak "data doubles"[8] kavramıyla düşünülmektedir (Caluya, 2010, s. 626). Burada farklı kurumlarda farklı şekillerde toplanan ve farklı biçimdeki (ses, görüntü, biyometrik veri gibi) verilerin bir araya getirilerek, dijital gözetim sistemleri sayesinde toplanıp entegre edilen verilerin güç ilişkilerini ve toplumsal ilişkileri nasıl değiştirdiğinden bahsedilmektedir. Yukarıda bahsedilen iki tür uygulama, yeni gözetim pratiklerinin hem eski panoptik gözetleme imkânı sağladığını hem de rizomatik ağlar şeklinde bitki kökleri gibi sonsuz ağlar ve "node"lar üzerinden ilerleyen daha yumuşak bir formda olduğunu göstermektedir. Bu yumuşak formun nasıl olduğu daha çağdaş kuramlar temelinde de küreselleşen gözetim ve onu takip eden diğer kuramlarda ele alınmaktadır.

Bogard'ın çalışmaları ile Haggerty ve Ericson'un asamblajlar ile ilgili çalışmalarında bu kavramların yeni formlarından bahsedilmektedir. Rizomatik, yer altındaki bitki yapılarından esinlenen bir kavram olarak özellikle uzamsal bağlılığı açıklamak için kullanılmaktadır. İzole ve tekil yapıların aksine, görünüşte farklı olan kavram, nesne ve varlıklar arasında geniş ama ilişkilendirilebilir bağlantılara vurgu yapmaktadır (Beck, 2016, s. 335). Haritanın genleşebilirliği, genişleme özelliği rizoma gücünü veren şeydir. Rizomatik internetin kartografik yapısı iki yönlüdür. "Net" ve "Web", "ağ", kavramları çevrimiçi içeriğin yalnızca bağlantılılığına ek olarak takip edilebilir ve izlenebilir haritalanmış yapısına dikkat çekmektedir. Bu da bireyler hakkında dijital sistemler ile kurulabilen profil çıkarma, itibar puantajı ve kartografi dediğimiz şeyleri açıklayan temel şeydir.

Daha radikal anlamda, dijital ve fiziksel arasındaki akış birbirini besleyerek yeni düşünme, eyleme geçme biçimleri ortaya çıkarmakta ve dijital içerik fiziksel dünya üzerinde haritalanmaktadır. Bu tip bir kartografi, İnternetin rizomatik yapısını değiştirebilecek yeni uçuş çizgileri oluşturmaktadır. Haritalanma bu

[8] Bu çalışmada Haggerty ve Ericson tarafından "kişilerin ve yaşamların bir replikası haline gelen verilerin" (data doubles) oluşturulmasını kolaylaştıran "gözetleme topluluğunun" (surveillant assemblage) bir parçası olarak bir kontrol kulesi ile sınırlı kalmadan, gücün uzaktan işleyişini anlamak için özellikle önemli görmektedir (GandyJr, 2021, s. 2)" şeklinde açıklanmaktadır.

noktada, internetin kartografik yapısının ikinci yanına dokunmaktadır. Rizomatik internet yalnızca dijital yerleri birbirine bağlamakla kalmayıp, bireyleri de bu yerlere bağlamaktadır: birey rizomun parçası haline gelmektedir. Rizomun bir parçası olarak, bireyler dijital ve fiziksel arasında bir köprü haline gelmektedir. Deleuze ve Guattari bunu “yoğunluklar” (insentisies) kavramıyla açıklamaktadır. Birey çevrimiçi olmasa da dijital içerik düşünmeyi, iletişimi ve etkileşimleri etkilemektedir (2016). Bireyin tamamen dijital sistemlere dahil olması onu daha tahmin edilmeye ve manipüle edilmeye açık hale getirmektedir. David Lyon ise hem Foucault’nun hem de Deleuze ve Guattairi’nin görüşlerini küreselleşen gözetim başlığında daha çağdaş bir şekilde yorumlayarak, kişilerin ve yaşamların bir replikası haline gelen verilerin nasıl oluştuğunu, nelere sebep olduğunu açıklamaktadır.

3.4.3. Küreselleşen Gözetim (David Lyon)

David Lyon’un daha çok bireylerin gündelik yaşamlarındaki noktalara odaklanarak bir tür tanımlama yaptığı görülmektedir. Gözetim alanında çalışan çok önemli isimlerin yazmış olduğu bir raporda gözetim toplumu çeşitli niteliklerle maddeler halinde betimlenmektedir. Bu özelliklere bakıldığında binalar, AVM’ler, yollar ve yerleşim bölgelerindeki video kameraların sürekli olarak bireyleri izlemesi, otomatik sistemlerin araç sistemlerini ve bu sistemlerin geliştirilmesiyle yüzleri tanır hale gelmesi, elektronik etiketlerin kullanılması ve özellikle denetimli serbestlik altındakilerin bu sayede tahliye koşullarını ihlal etmemesinin sağlanması, aynı zamanda polis tarafından tutuklanan kişilerin DNA örneklerinin saklanması, yalnızca suçluların değil suç eğilimlerinin daha erken belirlenmesi, yardımlar, sağlık hizmetleri gibi hizmetler için sürekli olarak kimliklerin kanıtlanmasının istenmesi ve özellikle biyometrik kimlik kartı sistemlerinin kullanılması, bu doğrultuda kişisel veri tabanına bağlı parmak izleri ve iris taramalarını da içerek biyometrik verilerin tutulması, yurt dışındayken bireyin kim olduğu nereye ve ne amaçla gittiği, yanında ne taşıdığının kontrol edilmesi, izlenmesi ve ayrıntıların saklanması, bazı pasaportlara bilgisayar çiplerinin yerleştirilmesi ya da planlanması, okulların çocukların takibi için akıllı

kartları ve biyometriyi kullanması, harcama alışkanlıklarının yazılımlarla analiz edilmesi ve verilerin her türlü işletmeye satılması, telefonların, e-postaların ve internet kullanımlarının dinlenebilir ve taranabilir olması ile çalışmaların izlenmesi ve iş dışındaki tutumlar ve yaşam tarzının kurumlar tarafından gittikçe daha çok izlenmesi gibi pek çok durum sıralanmaktadır (Wood, Ball, Lyon, Norris ve Raab, 2006). Gözetimle ilgili önemli isimlerden biri Lyon'dur. Lyon, bu niteliklerle tanımlanan gözetim türünü; gözetlenen toplum, küreselleşen gözetim, elektronik göz kavramlarını kullanarak açıklamakta, klasik kuramlarla güncel durumları birleştirerek dijital gözetimin farklı boyutlarına vurgu yapmaya çalışmaktadır.

Bu vurguyu, gözetimin bir rutin haline geldiği, eskiden suçluların izlenmesi yerine kitlesel gözetime geçildiği ve herkesin gittikçe artan şekilde bir gözetime tabii olduğunu belirterek yapmaktadır. Bu anlamda bakıldığında, Lyon'un tanımıyla gözetim, kapitalist üretim ve tüketime ek olarak, devlet odaklı bürokrasiler ve uluslararası askeri işlerle iç içe geçmiş durumdadır fakat aynı zamanda günlük hayatın giderek herkesi daha fazla ilgilendiren bir unsuru haline gelmiştir ve bir tür rutindir. Aynı zamanda Beck'in de kullandığı şekilde, risk ile bağlantılı bir şey olarak yerini korumaktadır (Lyon, 2004, s. 137). Lyon'un küreselleşen gözetim kavramıyla ya da gözetimin küreselleşmesi kavramsallaştırmasıyla anlatmaya çalıştığı şey, artık tüm bu süreçlere ek olarak, bireylerin özellikle güvenlik vaadi ve modernliğin getirdiği ya da kurduğu riskler ve tehlikeler temelinde gönüllü olarak izlenmesidir. Gözetimin küreselleşmesinin temel noktalarından bir tanesini özellikle 11 Eylül olaylarına bağlamaktadır.

11 Eylül'den sonra ABD'nin sadece teröre karşı savaş ilan etmede başı çekmesi değil, aynı zamanda diğer ülkeleri de kaçınılmaz olarak etkileyecek önlemlerin uygulanmasında başı çekmesiyle küresel gözetim yoğunlaşmıştır. New York ve Washington gibi sembolik güç merkezlerine yönelik saldırıların yerli uçaklarla gerçekleştirildiği ve bunların potansiyel düşmanların herhangi bir ülkeye giriş yaptığı en bariz noktalar olduğu göz önüne alındığında, bu önlemlerin ana odağı

havaalanlarıdır (Lyon, 2007, s. 122). Diğer en önemli olaylardan bir tanesi ise Snowden Olayıdır. Snowden ifşaatlarının gündeme getirdiği tartışmaların çoğu, metaveriler ve buna bağlı olarak büyük veri gözetimi ile ilgilidir. Snowden, daha önce gizli olan pek çok şeyi ortaya çıkarmıştır fakat Lyon bildiklerimizin hala belirsiz olduğunu kabul etmek gerektiğini ifade etmektedir (Lyon, 2015).

Didier Bigo, 21. yüzyılın başlarındaki küresel gelişmeler bağlamında güvenliği gözetim çalışmalarıyla ilişkilendiren oldukça spesifik analiz biçimleri önererek bu konuyu ele almaktadır. Bu kez Bigo, kapsayıcı panoptikonun sezgisel olarak işe yaramayacağı konusunda ısrar etmekte bunun yerine, kısmen banoptikon Agamben'den türetilen, alternatif dışlamayı vurgulayan formülasyonunun içeriklerini araştırmaktadır. Belirsizliğin, korkunun ve huzursuzluğun yönetimselliği olarak açıklanırken aynı şekilde paradoksal bir şekilde yeni rutin olan istisnai uygulamalar, olağanüstü önlemlerle karakterize edilen banoptikonla, hareketliliğin normatif zorunluluğunu teşvik ederken aynı zamanda yabancıların profilini çıkarmayı içerdiğini söylemektedir (Lyon, 2006, s.12). Bigo, panoptikon yerine uluslararası düzeyde bir güvensizlik biçimine vurgu yaparak "ban-optikon" kavramıyla, bu güvensizlik biçimi içindeki her gruba farklı muamele etmek için uygulanan söylem, kurum, mimari yapılar, yasalar ve idari önlemleri analiz etmektedir. Bu analizin sonucunda, ban-optikonun temel işlevi bir azınlığın profilini istenmeyen olarak çıkarmaktır. Bigo, ban-optikonun üç temel özelliğini şu şekilde belirtmektedir:

1. "Liberal toplumlar içerisinde istisnai bir güce sahiptir (olağanüstü haller rutinleşmiştir.)
2. Profiller çıkarmaktadır (gelecekteki olası davranışlarından korkulan bazı grupları ve tedbir olsun diye dışarıda bırakılmış insan kategorilerini ötekileştirir)
3. Dışlanmayan grupları normalleştirmektedir (malların, sermayenin, bilginin ve insanların serbest dolaşımına inanılmasını sağlamaktadır)" (Bigo, 2006 akt. Lyon ve Bauman, 2020, s. 76).

Elektronik gözle, Lyon, elektronik gözetimin günümüzde sosyal düzeni nasıl etkilediğini göstermek için her işlemin ve telefon görüşmesinin, sınır geçişinin,

oylamanın ve başvurunun bir bilgisayara kaydedildiği dolayımlı yaşam tarzımıza bakmaktadır (Lyon, 1994). Kamusal ve özel yaşamların bulanıklaşması, iletişim teknolojisindeki gelişmelerle kolaylaştırılmıştır. Avantajlar arasında kolaylık, doğru kayıt tutma ve dünya çapında mevcut bilgiler yer alır. Bu teknolojinin bir dezavantajı, mahremiyet kaybı ve kişisel bilgilerin yetkisiz kurcalamaya karşı savunmasız olmasıdır. Kişinin "veri imajı", bazen arkasındaki kişinin zararına olacak şekilde kendi başına bir yaşam sürmeye başlar. Bu bilgilerin mevcudiyeti endişe için ek bir nedendir (Orwant, 1996, s. 30). Elektronik gözle yapılan izlenme, kontrol edilme ve soruşturulma vasıfları ise gözetlenen toplumun temel özelliklerini oluşturmaktadır.

İnsanlar gelişen teknolojiler ile sürekli kontrol altındadır, bu bakımdan gözetleme olarak tanımlanan şey, somut bireylerin birbirlerini izlemesi değil, tam tersine soyutlaşmış çok daha geniş bir ağdır. Örnek olarak; tıbbi sonuçların toplandığı bir veri setinin başka amaçlarla kullanılabileceğini, bu verilere ulaşımın çok kolaylaştığını, yanlışlıkla bu verilerin ifşa edilmesini göstermektedir. Gözetleme, bireylerden özellikle soyutlanmıştır. Asıl amaç bu noktada gözetlemenin faydalarına değil, kasıtsız sonuçlarına karşı uyarı yapmaktır. Gözetleme, toplumun düzenlenmesi manasını taşıdığından sosyolojinin önemsediği mühim konulardan biri haline gelmiştir. Hem kontrol hem koruma anlamı içerse de amaç uyarı olduğundan, konu dört ana başlık altında tartışılmaktadır. Bunlar; koordinasyon, risk, mahremiyet ve güçtür. Koordinasyonla sosyal ilişkilerin değişen yapıları, zaman ve mekân kavramlarının anlamını yitirmesi ve bilgisayar destekli koordinasyonun öne çıkması açıklanmaktadır. Risk ve mahremiyet ise bu bağlamda gelişmektedir. Bireyler bu kadar kontrol altında özel hayat kavramının sınırlarını kaybetmiş durumdadırlar. Güç ise gözetlemenin ne boyutlarda olduğunun ve nasıl kullanılabileceğini göstermektedir. Bireyler Lyon'a göre belirli faydalara sahip olmak amacıyla belirli bedelleri kabul etmektedirler. Örnek olarak, çeşitli mağazalarda bireylerin çeşitli kampanyalardan faydalanmak amacıyla kimliklerinin bilinmesini kabul etmesi verilmektedir.

Lyon, bu verileri verirken bir şeyleri uzaktan gerçekleştirirken bedenlerin yok olmasını anlattığı Kaybolan Bedenler kavramsallaştırmasıyla emojilerin insan ifadeleri yerine kullanılmasından ve video konferans gibi teknolojik gelişmelerden bahsetmektedir. Tüm bu sistemler, bireylerin dijital sistemlerde sayısal olarak var olmasına ve daha çok veri vermesine sebep olan durumlardır. İnsanların bir yerde somut olarak, fiziksel olarak bulunması gerekmez gittikçe artan bir soyutlaşma mevcuttur. İnsan ilişkileri kaybolan bedenlerin en çok etkilediği mecralardan bir tanesidir. Sürekli etkileşimde olduğumuz bireylerin dışında aynı zamanda iletişimde bulunduğumuz ama yüz yüze iletişimde bulunmadığımız birçok insan vardır. Sosyal medyanın gelişmesiyle kamu-özel ayrımı ortadan kalkmıştır. İnsanların özel, mahrem olarak değerlendirdiği birçok şey artık kamuya açık halde sergilenmektedir. Zaman ve mekân yeniden yapılandırılmakta, kamusal ve özel alan birbirine karışmaktadır. Özellikle Kovid-19 Pandemisi ile hem ulusal hem uluslararası ölçekte eğitimin de çevrimiçi platforma aktarılması, iş görüşmelerinin, toplantılarının, akademik sınavların da çevrimiçi yapılması kaybolan bedenler kavramının örneklerindendir. Zaman ve mekân tamamen yok olmuş, bireyler fiziksel olarak bulunmadıkları ortamda sanal halleriyle yer bulmuştur. Bu da büyük verinin daha da büyümesini, sistemlerin daha da kontrol altına almasına neden olan durumlardan biri olmuştur. Eğitim sistemlerinin takibi, derslerin takibi, öğrencilerin, akademisyenlerin, öğretmenlerin seslerinin, görüntülerinin, şifrelerinin, biyometrik verileri gibi pek çok verinin depolanması da bunun bir örneğidir.

Bireylerin uzun bir süre bu sistemlerde var olması, mesleklerine, eğitimlerine, sosyal hayatlarına çevrimiçi platformlardan devam etmesi ve bu şekilde verilerinin toplanması Lyon tarafından Görünmez Çerçeveler olarak kavramsallaştırılmıştır. Bu kavramsallaştırmayla gizlenmiş bir altyapıya ve suistimal olasılığına vurgu yapılmaktadır. Gözetimin artışında en büyük sorumlu olarak görülen gelişmiş teknolojilerin kaynağını nereden aldığı ve 20. yüzyıl sonunda ne aşamaya gelip nasıl birleştikleri burada konu edilmektedir. Bu toplumlar, bilgi toplumları, gözetim toplumlarıdır. Sürekli varmış her zaman da var olmuş gibi görüp o şekilde davrandığımız elektrik gibi şeylerin sadece

yokluğunda bilincine vardığımız şeklinde örneklenmektedir. Bireyler fark etmeden bu altyapılara bağımlı hale gelmektedir. Bu bağımlılıklar insanların yaşamlarına sınır koymaktadır. Belirli şekillere sokmakta ve bireylerin ona göre hareket etmelerine neden olmaktadırlar. Ama bu gelişmiş altyapılar sadece gündelik hayatı değil, askeriye gibi kontrol seviyesinin farklı boyutlara ulaşabileceği yapıları da etkilemektedir. Bu iki bağlamı bir araya getiren Lyon, bilgi toplumlarının yüksek teknolojili polis devletlerine benzeyip benzemediği sorusunu sormaktadır. Bunu ise gözetlenen toplum kavramına bakışını çok bariz bir şekilde anlayabileceğimiz "Güç kendi rolünü oynar ve sıradan insanlar genelde sisteme ortak olur ve bazen de sisteme teslim olurlar. Fakat bu kontrole mi zorlamaya mı girer? Bu sürekli değişir'' cümleleriyle açıklamaktadır (2006).

Toplanan verilerin farklı amaçlarla kullanılabileceği düşüncesi ise kurumlar arası veri aktarımını temsil eden Sızdıran Konteynerlar kavramıyla açıklanmaktadır. Ulusal güvenlik anlamında kullanan verilerin bireyleri sınıflandırma hatta ayrımcılık yapma amacıyla kullanılabileceği, dijital vatandaşlık sistemleri kurulabileceği, sosyal puanlama sistemi gibi sistemlerin kurulabileceği bunun örneklerindendir. Robot kuşlar, yüz tanıma teknolojileri, sosyal medya platformu verileri gibi tüm veriler birleştirilerek yapılan gözetim bu kavramsallaştırmanın tam karşılığıdır. Gözetim büyümüş ve gözetim yolları çok daha az fark edilebilir hale gelmiştir. Başka amaçlar için yapılan gözetim bambaşka amaçlar için de kullanılmaktadır. Bunun insanlarda yarattığı his mahrem kamu çerçevesiyle karşılaştırılmaktadır. Lyon'un verdiği ana örnek, polisliğin yüksek teknoloji kullanılarak uygulanması ve suça bakışın bu yolla nasıl dönüştürüldüğüdür. Tüm bu düşünceler Ulrich Beck'in Risk Toplumu kavramına bağlanmakta "Amacın sadece suçu kovuşturmak ya da tehlikeyi engellemek değil, aynı zamanda düşünülebilir risklerden bile kaçınmak olduğunu iddia etmektedir'' görüşünü paylaşmaktadır (2006). Bu açıdan gözetimin sonuç olarak iki yüzü vardır. Biri gözetimi riskin temeli, devletin özel hayata müdahalesi olarak görmek; diğeri ise tehlikeleri bilmek ve bunlardan kaçınmaktır. "Gözetlenen toplumlar bugün yok olan bedenleri görünür kılma ve bunların aktivitelerini düzenleme ihtiyacı nedeniyle vardırlar" (age, 2006). Gözetim bu bakımdan

gerçekten iki yönlü düşünülebilecek bir kavramdır. Bir yandan bireylerin özel mülk olarak görerek koruma talep ettikleri için evlerimizin yakınına konulan kameralara sevinirken bir yandan sürekli izlenildiğini hissetmek insanlarda karmaşık duygular yaşatmaktadır. Bir yandan kendi fiziksel güvenliğini düşünürken, bireylerin e-postalarını, sosyal hesaplarını kaybedeceği korkusu onların, onlara olan bağımlılığını ve kaybolan bedenler kavramlarını tam anlamıyla açıklamaktadır. Bahsedildiği şekilde, internet gibi gözetim sağlayan bir yapıyı hep varmış gibi düşünürken sadece sorun olduğunda onun tamamen farkına varılması Lyon'un bahsettiği önemli detaylardan sadece bir tanesidir (Lyon, 2006). Lyon "Gözetim Çalışmaları" (2013) eserinde, gizli telefon dinlemeleri gibi ileri teknoloji ve iletişimle de bağlantılı gelişmeler sonucunda gözetimin hem toplumsal hem siyasi kaygı konusu olmasına dikkat çekmektedir. Bu konu farklı kurumsal ve ulusal bağlamlarda da çeşitlilik göstermektedir. Gözetimi bu kadar incelenmesi gereken ve değişken yapan bir diğer unsur da budur. "Ulusal güvenlik'' ile soyut bir gözetim üst anlatısı olduğu; bu fazla soyutluğu aşmak için fazla paranoyak ve teknolojik belirlenimci olmadan gözetimin tanımlanması gerektiğini ifade etmektedir. Bunun için gözetimin nedenlerini, söylemlerini ve sonuçlarını bilmek gerekmektedir. Bu üç maddeye ulaşmakta modern-post modern gözetim bakış açısına, denetim ve disipline, yönetim ve yasaklama ikililerine bakmaktadır. Lyon, modern kapitalist ve bürokratik pratik biçimlerini modern gözetimin nedenlerine bağlamaktadır. Bireyselleşme hem bunların temelidir hem de bilgisayar temelli sistemlerle birleştirilmeye oldukça uygundur. Akılcılık, verimlilik gibi olgularla denetimin bir araya gelmesi gelişmiş gözetimi ortaya çıkarmaktadır. Durkheim'ın artan sosyal eşitsizlikle çatışma düzeylerini bağlaması da gözetimin temellerinden biridir. Gittikçe artan teknoloji sonucunda risk yönetimi de şekil değiştirmektedir. Refah devletinden emniyet devletine; sosyal tabanlı açıklamalardan penalojiye, babacan yönetimden yeni işletmeciliğe geçiş olduğunu anlatmaktadır. Bu da gözetim söylemlerini meydana getirir. Bu söylem "sosyal sınıflandırma", "kaydolunmuş devlet" ve "sistem birleştirmesini" kastetmektedir. Bu çerçevede, belli bir amaç için toplanan verilerin başka amaçlar için kullanılması, risk temelli idari yaklaşımların oluşması, şüphe kategorilerinin yapılandırılması gibi şeyler

ele alınabilir (Lyon, 2013). Gözetim söylemleri, kaydolunmuş devlet, sosyal sınıflandırma gibi süreçleri ise bu alanda açıklayan kuram Oscar Gandy'nin panoptik sınıflandırma kuramıdır. Burada belli bir amaç için toplanan verilerin nasıl kullanılabileceği ve bir ayrıştırıcı güç olarak nasıl bir güce sahip olduğu açıklanmaktadır.

3.4.4. Panoptik Tasnif Olarak Gözetim (Oscar Gandy)

Panoptik tasnif olarak gözetim[9], Oscar. H. Gandy Jr.'ın Michel Foucault, Karl Marx, Max Weber ve Jacques Ellul'un teorilerini temel alarak tanımladığı bir gözetim türüdür. Weber'den kurumların faaliyetlerinde öngörülebilirliği sürdürme çabalarının meşrulaştırılmasında bilginin rolünü, Ellul'dan panoptik tasnifte ilerleme ve belirsizliğin azaltılması hedeflerini gerçekleştirmek için gerekli donanım, yazılım ve uzmanlığın yanı sıra verimlilik felsefesi ve ideolojisini içerecek teknolojinin tanımını, Foucault'dan iktidar teknolojisinde gözetimin rolünün uygun bir tarifi olarak panoptisizmi benimseme düşüncesini ve disipline edici gözetim mantığını, Giddens'ın yapılanma teorisinden, bireyler ve kurumlar arasındaki rutin etkileşim kalıpları düşüncesini, Marx ve Giddens'dan bilgili ajanların eylemi, sürekli mücadele edilmesi gereken dünyayı üretip yeniden üretse de, bu dünyanın asla tasarımımıza sadık olmadığı düşüncesini temel alarak panoptik tasnifi tanımlamaktadır (Gandy Jr., 1996). Giddens'ın yapılanma teorisini hegemonik tahakküm teorileri, George Gerbner'ın kültür teorisi ve aşırı kültür teorisyenlerinden bazıları tarafından dış etkinin neredeyse mutlak inkârı arasında orta nokta bulması açısından önemli görmektedir. Giddens'ın "uzaklaşma" kavramını, daha sonra Haggerty ve Ericson tarafından "kişilerin ve yaşamların bir replikası haline gelen verilerin" (data doubles) oluşturulmasını kolaylaştıran "gözetleme topluluğunun" (surveillant assemblage) bir parçası

[9] Gandy'nin Panoptik Tasnif ile ilgili kitabının "The Panoptic Sort: A Political Economy of Personal Information" ilk basımı 1993; ikinci basımı ise 2021 senesindedir. Bu süreç içerisinde iletişim teknolojileri ve dijitalleşme süreçlerinde çok fazla değişim yaşandığı için Gandy'de kendisinin ikinci basıma birçok yenilik eklediğini söylemektedir. Bunlardan en önemlisi de bu tez kapsamında olduğu için, büyük miktardaki veriye yapılan vurgudur. "İlk basımdan bu yana en çok değişen şey algoritmik şekilde elde edilen büyük miktarda verinin işlenmesiyle elde edilen verilerle, bireyler ve çeşitli grupları birbirinden ayırmak için geliştirilen internetle birbirine bağlı olan dijital teknolojilerin gelişimi olmuştur" (Penn Today, 2021). Daha fazla detay için bknz. Gandy Jr., 2021.

olarak bir kontrol kulesi ile sınırlı kalmadan, gücün uzaktan işleyişini anlamak için özellikle önemli görmektedir (Gandy Jr, 2021, s. 2).

Gandy'nin bu kuramsal altyapıyla oluşturduğu panoptik tasnif, karmaşık ayrımcı bir teknolojidir. Panoptik'in "herkesi kapsayan" olarak adlandırılmasının nedeni bireylerin bireysel statü davranışı hakkındaki tüm bilgilerin, bir kişinin ekonomik değeri hakkında istihbarat üretiminde potansiyel olarak yararlı olduğunu düşünmesinden kaynaklanmaktadır. Bu tahminler temel alınarak insanlar kategorilere ayrılırlar (Gandy Jr., 1996, s. 133). Panoptik tasnifte, kişisel bilgilerin 3 ayrı işlevi bulunmaktadır. Bunlar: kimlik saptama (identification), sınıflandırma (classification) ve değerlendirme (assesment) olarak belirtilmektedir. Kişilerin bilgileri kullanılarak kimlik saptama aşaması gerçekleştirildikten sonra, bu veriler temelinde belirli tipler oluşturulmakta ve burada Foucault'nun kavramlarıyla güç kullanımı (exercise of power) ve disipline edici izolasyon (disciplinary isolation) meydana gelmektedir. Sınıflandırma ve tasnif etme aşamasında, bireylerin gelecek davranışları hakkında belirsizliği en aza indirmek ele alınarak bir farklılaştırma süreci hedeflenmektedir. Değerlendirme kısmında ise ön işleme ile tahmin etmeye yardımcı yazılımlar ile tasnif tamamlanmaktadır (a.g.e., s. 136).

Bu tasnif özellikle, şirketler ve hükümet arasındaki veri toplama iş birliğini ve bu iş birliğinin bireysel mahremiyete yönelik tehdit oluşturması sürecini vurgulamaktadır. Diğer gözetim kuramlarında da sıklıkla bahsedilen Snowden Olayındaki gibi, Amerika'daki Milli Güvenlik Kurumu'nun bireyler hakkındaki verileri toplayarak, PRISM adı verilen bir programla vatandaşlarının her tür hareketini takip etmesi ve bunların ortaya çıkmasının büyük veri ve kontrol gücü, mahremiyet kaybı tehlikesini gözler önüne sermektedir. Sullivan'ın ifadesiyle, Gandy, Google henüz kurulmamışken ve bilgisayar işlemleme gücünün çok düşük olduğu bir dönemde, Ewuifax, TRW ve Direct Marketing Association gibi kuruluşların bireylerin verilerini kullanarak devasa tüketici verisi depoları biriktirdiklerini, bunların nüfus sayımı gibi devlet veri tabanlarıyla karmaşık eşleştirme algoritmalarıyla bir araya getirilerek bireylerle ilgili hassas

özel bilgiler de dahil olmak üzere izlendiği konusunda uyarılarda bulunmaktadır. Burada önemli olan nokta, kişisel verilerin rutin olarak sınıflandırılmasının güçlü bir kurumsal güç biçimine dönüşmesidir (2014). Şirketler stratejik bilgi sübvansiyonları sağlamak için bağımsız aracı kurumlarla ve danışmanlarla sözleşme yapmaktadır ve bu ilişkiler bazen özel ve gizli tutulurken, bazen halka sağladığı yararlar nedeniyle duyurulmaktadır (Gandy, 2003, s. 289). Genel anlamda, duyurulsa da duyurulmasa da öngörülen bu tür bir panoptik tasnifin, anti-demokratik bir kontrol sistemine yol açacağı düşünülmektedir. Panoptik tasnif sistemi, o dönemde tasarlanan haline ek olarak gelişen ve veri toplamak için daha da elverişli olan sosyal medya platformları gibi gelişmelerle daha etkin bir sistem haline gelmektedir.

Veri panoptikonunun daha etkin hale gelmesinin temel 4 sebebini Sullivan şu şekilde sıralamaktadır: Yazılımın sosyal, ticari ve siyasi sistemlerde merkezi bir yere sahip olması ve hepsinin birbirini desteklemesi, bilginin yönlendirilmesi, depolanması ve sınıflandırılmasında metaverinin öneminin artması, verinin küresel ölçekte toplanması, kurumsal veri madenciliği ve hükümetin veri madenciliği arasındaki çizgilerin bulanıklaşması (2014). Bakıldığında Türkiye'de tüm kurumlarda dijitalleşmeye ayrı bir önem verilmeye başlanmıştır. Metaveri kullanımında Türkiye, diğer ülkelerle kıyaslandığında hep ilk sıralarda yer almaktadır. Türkiye'deki vatandaşların kullandığı platformların tüm dünyadaki gibi TikTok (Çin menşeili) hariç, genellikle Amerika temelli olduğu bilinmektedir. Bunun dışında kurumların ve hükümetin de (İçişleri Bakanı'nın açıkladığı gibi) daha dijital sistemlerle veri topladığı bilinmektedir.

Campbell ve Carlson, Gandy'nin, panoptik tasnif ile belirttiği en önemli noktalardan biri olarak, pazardaki ürün ve servislerin sağlayıcıları ve tüketicileri arasındaki ilişkideki büyük eşitsizliği vurgulamaktadır. Bu ilişkiyi bu derece eşitsiz yapan şey, bireylerin kişisel bilgilerini paylaşma konusunda mecbur bırakılmalarıdır (Campbell ve Carlson, 2002, s. 591). Uluslararası alanlarda da Çin örneğinde milli uygulamaları kullanma zorunluluğu gibi, diğer ülkelerde de çeşitli uygulamaların yasaklanması ve diğerlerinin önerilmesi bunun bir

örneğidir. Bu eşitsizliğin yanı sıra, Gandy'nin çalışmasını güncel dijital medya teknolojileri ve özellikle büyük veri kavramıyla incelemeye çalışan Blevins, Gandy'nin görüşündeki geleneksel Marxist eleştiriyi temel alarak, panoptik tasnifin tüketicilerin bireysel bilgileriyle meydana gelen bir tür ek değerin çalınarak onları tanımlayan, sınıflandıran ve değerlendiren bir çeşit güç teknolojisi olduğunu belirtir. Buna göre panoptik tasnif, yalnızca ekonomik değer temelinde değil, ırk, cinsiyet, yaş, sınıf ve kültür gibi temellerde de eşitsizlik üretmektedir. Günümüzdeki çevrimiçi veri toplama ve panoptik makine mantığında da bireylerin kişisel bilgilerinin yanlış temsil edildiği sonucuna ulaşılmaktadır. Panoptik sınıflama bu anlamda yanlış bir sınıflama haline bürünmektedir. Veri anlam bakımından işlenirken, tekrar üretilirken ve standartlaştırılırken yanlış ölçüm ve yanlış hesaplama ortaya çıkmaktadır (Blevins, 2016, s. 29). Sonuç olarak, Gandy'nin kendi gözlemlerine göre de gözetim kümülatif dezavantajlı bir dünya inşa etmektedir (2009 akt. Pero, 2015, s. 478). Gandy, çok önceden Google gibi platformların önemine vurgu yaparak, bu gözetim türünün tehlikelerine karşı uyarı yaparken, William Bogard'ın da aynı şekilde panoptisizmin çok daha yumuşak bir güç olarak hatta simüle edilmiş bir formda farklı sosyal ve teknik yönlerle toplumsal hayatımıza girdiğini belirttiği görülmektedir.

3.4.5. Gözetim Simülasyonu Formunda Gözetim (William Bogard)

Bogard'ın telematik toplumlarda gözetim simülasyonu olarak kavramsallaştırdığı kavram, 21. yüzyılda sanal gerçeklikten, bilgisayarla profillemeye, yapay zekadan genetik haritalandırmaya teknolojik gelişmelerin iş, cinsellik, savaş ve özel hayat gibi alanlarda gözetimin boyutlarına dair oluşturmuş olduğu bir tür sosyal bilim kurgusu olarak belirtilmektedir (William, 1996). Bogard'a göre, panoptikten post panoptik sistemlere geçiş, sınırlandırılmış alanlardan sınırı belli olmayan alanlara geçiş anlamına gelmekte, sosyal kontrol biçimleri dijital ağlar üzerinden sağlanmaktadır. Orwelyan bir şekilde betimlenen bu sistemde, yeniden üretimi kolay, korunması zor olan bu ağlaşmış bilgilerin, zayıflığı da vurgulanmaktadır. "Rizom" halini alan bu ağlarda her node bir diğeriyle açık bir

yapıda birbirine bağlıdır ve Guattari'nin "paradoksik güvenlik" kavramıyla açıkladığı gibi makine ya da Orwelyan bir makine her şeyi izlemekte ve kaydetmektedir (Bogard, 2006, s. 97). Küresel gözetim ağlarının rizom olarak tanımlanması, sınırların belirsizliğini ve ağlar üzerindeki kontrolsüzlüğü vurgulamaktadır. Bu noktada geleneksel gözetim ve gözetim simülasyonu arasındaki fark düşünülmekte ve sorgulanmaktadır.

Fotoğraf sanatçısı Calle örneğini veren Bogard, Calle'in hiç tanımadığı bir adamı takip ederken fotoğraflarını çekmesinin, notlar almasının ve bunları biriktirmesinin tam olarak bir gözetim pratiği olmadığını çünkü özneyi kontrol etme ya da bir şeyler dayatma düşüncesi olmadığını belirtmektedir. Gözlemlemek, bilgi toplamak ve izlemek bu anlamda gözetim pratiği için yeterli değildir. Lyon'un tanımını kullanarak gözetimi gözetim yapanın, bilgi toplumlarında ya da elektronik gözde olduğu gibi ikili bir işleve sahip olduğunu hem sosyal ilişki sağladığını hem de bunu kısıtladığını belirtmektedir. Bu anlamda gözetim esir alış (capture) ve uçuş (flight) kavramlarıyla düşünülmektedir. Esir alış anlamında gözetim bir tür sınır belirleme, veri elde etme, tanımlama ve normalleştirme gibi süreçler olarak düşünülmekte; öte yandan uçuş ile bir tür kaçış, sınırların yok oluşu, belirsizlik ve direniş tanımlanmaktadır (a.g.e. 2006, s. 101).

Burada bahsedilmek istenen, Bogard'ın yorumlamaya çalıştığı konu, disipline edici gözetimin onun sınır belirleme, zaman ve mekân ayarlaması yapması, gözetim ve sınıflandırma mekanizmalarını kontrol stratejisi olarak kullanması anlamında mekanik bir asamblajı olarak düşünebileceği, fakat yeni toplumda kontrolün bilgi ve simülasyonun yeni modlarıyla değişime uğradığı ve kontrolün bunlarla şekillenmesidir (Haggerty ve Ericson, 2019). Gözetim yine mevcut haldedir fakat panoptikondaki gibi bir formda bireylerin kapatılarak ya da suçluların izlenerek yapıldığı bir gözetimden bahsedilmemektedir. Burada yeni modlardan bahsedilmektedir. Yeni modlarla yapılan bu gözetime Baudrillard'ın kuramından esinlenerek simülasyon formunda gözetim ismini vermektedir. Bunun sebebi, gerçeğinden daha gerçek ve hipergerçeklik alanları yaratmasıdır.

Burada bahsedilen şey post-panoptik bu gözetim türünde veri madenciliği ve bilgi bulutlarının panoptikonun yerini almasıdır.

Artık alanların kısıtlanması, kapatılması yoktur. Kapılar, kilitler, anahtarla giriş değil; parolalar, pin kodları ve şifreleme hakimdir. Buna simüle edilmiş gözetim denilmektedir. Baudrillard'ın ifade ettiği şekilde, gerçeklik prensibinin çökmesi, panoptik kontroldeki nedenselliği tersine çevirmektedir. Disipline edici makinelerde doğrulama yargıdan önce gelmektedir. Panoptik gözetim, otomatik itaat üretmeyi amaçlasa da yine de bu bilgiyi nihai önemini belirleyen yetkililere iletmeden önce tanımladığı olaylara tepki verir ve onları kategorilere ayırır. Kontrol toplumlarında muhakeme çok daha proaktiftir, simülasyon modeli olayların üretimini ve anlamını yapılandırmakta ve önceden karar vermektedir (Bogard, 2012, ss. 32-35). Simüle edilmiş gözetimde önceden tahmine ve sürekli değişen veri akışlarıyla şekillenen yeni bir gözetim formuna dikkat çekilmektedir.

Simülasyon gözetiminin geleceğini yorumlarken de dokunsal teknolojilere vurgu yapılarak panoptik düzendeki kapanmadan çok daha farklı teknik ve sosyal boyutların olduğu belirtilmektedir. Bogard'ın tüm bu çalışmalarında bahsetmek istediği şey, kendilerini küresel kapitalizmde konumlandıran yeni pratiklerle ve simülasyon teknolojileriyle, sosyal kontrolün belirli sınırlarda kalmamasıdır. Bu süreç ile kontrol daha kapsayıcı bir hale gelmekte, disiplin siber uzama taşınmakta, simülasyona dönüşmekte ve hipergerçeklik haline gelerek, tekrardan oluşturulmaktadır. Bu anlamda gözetim merkezileşmiş hiyerarşik gözetim ya da merkezileşmiş güçlerle değil, simüle edilmiş daha yumuşak biçimlerle gerçekleşmektedir (Haggerty ve Ericson, 2019). Bu yumuşak güçler bir sonraki bölümde de bahsedilen akışkan gözetimde vurgulanan akışkan gözetimin bir versiyonudur.

3.4.6. Akışkan Gözetim (Zygmunt Bauman ve David Lyon)

Akışkan gözetim, Bauman'ın, günümüz gözetim pratiklerinin çerçevesinin, önceki çalışmalarından olan akışkan modernite ile düşünüldüğü çalışmasıdır. Bu çalışma Lyon ve Bauman'ın konu üzerinde e-posta ile tartışmalarından meydana gelmiştir. Özellikle Kendin Yap Gözetim (DIY-do it yourself) ve kayıtsızlaştırma (adiaphorization) kavramları göze çarpmaktadır. Kendin yap gözetim, gözetimin yönetenden yönetilene geçmesi ile meydana gelen süreci temsil ederken, kayıtsızlaştırma (adiaphorization) ahlaki ve etik soruların eylem için bir kenara atılması süreci olarak tanımlanmaktadır, bu eylemin bir şey almak ya da tetiği çekmek de olabileceği belirtilmektedir (Finn, 2014). Burada bahsedilen, bireylerin sadece yüzde on indirim almak için kredi kartlarını çeşitli platformlara kaydetmeye izin vermesi, ya da telefon bilgilerini paylaşması da olabileceği gibi distopik bir şekilde dijital vatandaşlık sisteminde puanı düşmesin diye kendi gibi davranmama durumu da olabilmektedir. Bauman, kayıtsızlaştırmanın ikinci boyutunun ise, "bedensel (biometri ve DNA gibi) veya bedenin tetiklediği (çevrimiçi olmak, erişim kartlarını kullanmak ve kimlik göstermek gibi) verilerin işlenebilecek, analiz edilebilecek, diğer verilerle birleştirilebilecek ve daha sonra veri kopyaları olarak yeniden bünyeye dahil edilebilecek veri tabanlarına dönüştürülmesi" olduğunu belirtmektedir (Bauman ve Lyon, 2020, s. 19). Bu gözetim asamblajı kavramında da olan farklı alanlarda ve amaçlarla paylaştığımız verilerin bir araya getirilmesiyle bizim kimliğimizin ve bedenimizin kopyalarının elde edilmesi sürecidir. Kişinin ses kayıtları, yüz tanıma teknolojisi ile alınan görüntüsü, sosyal medya ile alınan karakteri ve duygu durumu, sosyal çevresi, tüketim alışkanlıkları, vize başvuru yaparken paylaştığı parmak izi gibi pek çok verinin bir araya getirilerek bireylerin inşa edilmesinden bahsedilmektedir. Bu tür bir haritalandırmadan sonra da kişinin ne yapacağı, nasıl hareket edeceği, hangi durumda neyi tercih edeceği tahminlenebilir hale gelmektedir. Kendin yap gözetimde ise, tüketicilerin metalaştırılması ve yeniden metalaştırılması, bireylerin kendini satılabilir bir meta haline getirmesi vurgulanmaktadır (Bauman ve Lyon, 2020, ss. 46-47). Bireyin meta haline gelmesi aynı şekilde hem panoptik sınıflandırmanın Blevins

yorumunda bireylerin bu şekilde bir ek değer üreterek büyük veri zenginini daha zengin yaparak kendilerini büyük veri yoksulu olarak daha yoksul bir hale sokmasını hem de Zuboff'un gözetim kapitalizmi kuramında doğrudan bireyin ve verisinin bu düzende bir meta haline gelmesiyle yorumlanabilmektedir.

Birey, meta haline gelmenin yanı sıra bu düzende belirli normallere göre hareket etmek ve sürekli gözetlendiğini bildiği için içselleştirilmiş gözetimdeki gibi uyum sağlayarak hareket etmek zorundadır. Lyon bunu, akışkan modernite çalışmasında, Ernest Gellner'ın düşüncesinden esinlenerek, modernite öncesi dönemi bakıma ihtiyaç duymayan vahşi bir kültür, modern dönemi ise sürekli bakım gerektiren ve yabani otlar için denetimin gerekli olduğu bir bahçe kültürü olarak nitelendirmektedir. Gözetim ve eğitim de bu süreçte popüler kültürün yıkımı ve uyumlu bitkilerin yetiştirilmesi anlamında görevlidir (Lyon, 2010). Gözetim bu anlamda bir tür uyum sağlama ve sağlatma aracı olarak ve herkesi belirli bir "normal" tanımına uygun hale getirme süreci olarak görülmektedir.

Bu süreç, akışkan gözetim ise "günümüzün görünürlük rejimlerini iyi tanımlayan, veri akışları, mutasyona uğrayan gözetim kurumları ve herkesin hedeflenmesi ve sınıflandırılması ile karakterize edilen bir şey" olarak tanımlamaktadır. Akışkan gözetim kavramı, bedenin veriye indirgenmesi, gerçek yaşamlarımız ve onlar hakkında anlattığımız hikayeler yerine yaşam fırsatlarının ve seçimlerinin bağlı olduğu veri kopyalarının (data doubles) daha önemli hale geldiği durumu yaratmaktadır (Lyon, 2010, s. 325). "Bir Daha Asla Yalnız Olamamak" isimli bir yazı yayımlayan Bauman, internet yüzünden anonimliğin ölümünü, mahremiyet hakkımızı kendi rızamızla katlettirmemiz olarak değerlendirirken, İHA (insansız hava araçlarının), yeni ve geliştirilmiş olanlarının kendi başlarına uçacak şekilde programlanacağını, göze çarpmayacak tasarım çalışmaları hedefiyle güncelleneceğini söyleyerek, "hiç kimse bir arıkuşunun kendi pervazına konup konmayacağını veya ne zaman konacağını bilemez" demektedir (Lyon ve Bauman, 2020, ss. 32-35). Orwell'in de söylediği gibi, artık içgüdüye dönüşmüş bir alışkanlıkla, gözetimi içselleştirmiş şekilde bir yaşama alışmak zorunda kalınmasını işaret etmektedir.

Bahsedilen alışkanlık, günümüz gözetiminin akışkanlığı, kullanıcılarının sağlayıcılarla yeni iletişim şekilleri ve kimlik yaratımı geliştirmek için iş birliği yapmaları için sürekli değişen sosyal medya platformlarında ne kadar akışkan ve esnek olarak görülse de tüm çevrimiçi gözetim pratikleri sosyal sınıflandırma ve farklılık üretim süreçlerini desteklemektedir (Trottier ve Lyon, 2013, s. 93). Gözetim kuramlarının farklı dönemler ve farklı temellerle desteklense de sosyal sınıflandırma ve farklılık üretim süreçlerine vurgu yapması hepsinin birer ortak noktası olarak göze çarpmakta, büyük veri yoksulunun gittikçe daha dezavantajlı bir konuma geleceğini işaret ettiği dikkat çekmektedir. Aynı şekilde Bauman ve Lyon'un da en son aşamada "Günlük hayatlarımızla ilgili bilgiler bizi gözetleyen kurumlar için şeffaflaştıkça, onların kendi faaliyetlerini anlamak daha da zorlaşıyor. İktidar, akışkan modernitenin değişkenliği içerisinde elektronik sinyal hızıyla yol aldıkça, şeffaflık bazıları için gittikçe artarken diğerleri için aynı hızla azalıyor" demektedir (2020, s. 24).

Bauman ve Lyon da günümüzün dijital risklerine ve yeni gözetim pratiklerinin hem sosyal sınıflandırma anlamında hem de küreselleşen dünyadaki risklerine odaklanmaktadır. Fakat bu noktaya kadar risklerden bahsedildiğinde akla ilk gelen isim olan Ulrich Beck, temel olarak gözetimi riskler ve modernlik ile ilişkilendirmekte, bu kuram daha sonra özellikle dijital gözetimle birlikte dijital riskler temelinde tartışılmaya başlanmaktadır.

3.4.7. Risk Önleme Aracı Olarak Gözetim (Ulrich Beck)

> *"Böylece her şey alt üst olmuştur: Weber, Adorno ve Foucault için korkunç bir vizyon olan -yönetilen dünyanın mükemmelleştirilmiş gözetleme rasyonalitesi- şimdide yaşayanlar için bir vaattir. Gözetim rasyonalitesi gerçekten işe yarasaydı ya da sadece tüketim ve hümanizm tarafından terörize edilseydik ya da sistemlerin düzgün işleyişi 'otopoiesis'e başvurarak veya 'ulusal reformlar' ve 'teknolojik yenilik saldırıları yoluyla yeniden kurulabilseydi' güzel bir şey olurdu."* (Beck, 2008)

Beck'in ifadesiyle "düşünümsel modernleşme teorisi, bireyselleşme, kozmopolitleşme ve risk toplumu teoremlerinden oluşmaktadır. Bu radikalleşmiş modernite, dünya risk toplumunu üretmiştir. Risk toplumunu ifade eden şey,

duyularımızla soyut olma eğiliminde olan imal edilmiş belirsizliklerdir" (Beck, 2008, s. 1). Lyon'un gözetlenen toplum teorisinde de bahsettiği şekilde, amacın sadece suçluları tespit etmek ve yakalamak değil aksine, her tür riski öngörerek onları engelleme düşüncesi gözetimin temelini oluşturan ana etmenlerden biri haline gelmiştir. Gözetim bu anlamda bir yandan devletin özel hayata müdahalesi olarak görülebilecekken diğer yandan tehlikeleri bilmek ve bunlardan kaçmak için bir yoldur (Lyon, 2006). Bireyler de bu anlamda güvende olabilmek için kendi verilerinden feragat etmiş olmayı kabullenmişlerdir.

Beck, Dünya Risk Toplumu (1998) kitabında da "Dijital Risk" başlığı altında yeni bir risk türüne vurgu yaptığını belirtmekte, dijital özgürlük riskinin modern toplumda karşılaşılan en önemli risklerden biri olduğunu düşündüğünü söylemektedir. Dijital risk, sınıf kategorileri ya da ulus devletlerle ilgili kategorilerle anlaşılamayacak bir risktir. Farklarından bir diğeri ise henüz felaketle sonuçlanmamış olmamasıdır. Bu açıdan olabilecek felaket ise küresel kurumlar tarafından yapılan mükemmel bir küresel gözetimdir. Aynı zamanda, sınıf kategorileri aracılığıyla anlayamadığımız yeni tür eşitsizliklere, hiyerarşilere ve emperyalist yapılara da yol açma potansiyeline sahiptir (Beck, 2014). Beck'in vurguladığı bu tür eşitsizliklerin özellikle yapay zekâ destekli sistemlerin kurmuş olduğu dijital gözetim temelinde düşünüldüğü ve diğer birçok kuramda da göze çarptığı görülmektedir. Özellikle günümüzde karşılaşılan büyük salgınlarla bireyin pek çok verisinin tutulması ve her şeyin daha da dijitalleşmesi bu riskleri çok daha fazla bir hale getirmektedir. Dijital sosyoloji alanında çok önemli bir isim olan Lupton da teknolojik değişimin çok hızlı olduğu ve dijital verilerin hayati, hareketli ve dinamik olduğu dijital toplumda, risk ve dijital teknolojilerin birleşimi, daha canlı risk biçimlerinin yeni olasılıklarını yapılandırır demektedir. Bu temelde de dijital risk topluluğu kavramı, teknik ve insan melezlerinin çoklu ve sürekli akış halindeki kesişimlerini tanıyarak, riskin bu özelliklerini kapsamaktadır (Lupton, 2016).

Dijital riskler, veri gizliliği ve bilgi güvenliğine ek olarak, insanların haklarını, siyasi özgürlüklerini (demokrasinin işleyişi dahil) ve nihayetinde insan onurunu

etkilemektedir. Bu nedenle, dijital riskler, tehdit edilen nesne nedeniyle geleneksel küresel risklerden çok farklıdır. Dijital riskler “dijital ortamlardan kaynaklanan riskler” olarak kabul edilse de korunacak nesne (riskin kaynağı olacak olan) “dijital ortam” değil, temel haklar, siyasi özgürlük ve insan onurudur. Dijital ortamlar da (mahremiyetin ihlalinden, ırk veya cinsiyet ayrımcılığına, sosyal dışlanmaya) birçok farklı şekilde etkilenebilmektedir (Fernández, 2023). Burada bahsedilen risklerden özellikle dijital epidermalizasyon, dijital epidemiyoloji, dijital fenotipleme gibi kavramlarla da çok bağlantılı olan diğer bir gözetim türü prostetik gözetim olarak literatürde sıkça yer almaktadır. Bu kavram özellikle yeni gözetim pratiklerinin yarattığı bir dijital risk kategorisinde olduğu için önem taşımaktadır.

3.4.8. Prostetik Gözetim

Risk toplumu kuramında bahsedildiği gibi, sağlığın da bireyin bir sorumluluğu haline gelmesi, sağlık gözetiminin de yalnızca hastalıkların tedavisi ya da çözümleri üzerine değil daha sağlıklı olma, daha iyi olma ve kendine iyi bakma söylemine evrilmesi “gözetim tıbbı” (surveillance medicine) kavramı ile literatürde yer almıştır. Gözetim tıbbı kavramı, “gelecekteki hastalıkların öncüllerini belirlemek için -genellikle yaşam tarzı kavramıyla temsil edilen- giderek daha fazla beden dışı bir alana dönüştüğü anlamına gelmektedir” (Armstrong, 1995, s. 400).

Hastalığın tedavisi değil, hastalığın önlenmesi ve risklerin minimuma indirilmesi temel hedeftir. Bu da yaşam stillerinin de kontrol altına alınması ve gözetlenmesi gerekliliğini ortaya çıkarmaktadır. Hastalığın bireyin bir sorumluluğu olması, hasta olmaktan ya da genel olarak hastalıklara yönelik oluşturulan korkunun bireyi daha kırılgan bir hale getirmesi ve bireyin özel hayatına müdahale durumunu daha mümkün kılması önemli bir değişimdir. Medya ve dijital medya teknolojileri ile sağlık içerikli söylemlerin eğlence ve eğitimi bir araya getirerek neyin sağlıklı neyin aksi olduğuna dair ürettiği kültürel söylemler de bunun destekçisi olmuştur.

Dijital teknolojilerdeki gelişmeler, Haraway'in sayborgunda ya da Hayles'in post-humanında bahsettiği gibi siber alanın da medikalleşmesine yol açmıştır. Gözetim tıbbının da temel özelliği medikal bakışı sağlıklı insanların yaşamlarının gözetimine çevirmesidir (Rich ve Miah, 2009, ss. 163-165). Haraway insan bedeninin bir şey olarak kolayca kategorize edilemediğini söylerken, teknolojilerin de insanın da ayrı bir varlık olarak tanımlanamayacağını vurgulamaktadır. İkisi de artık birbirine katkı sağlamaktadır; insanlar bedenlerini ve kendilerini bu teknolojiler sayesinde anlamaya, gündelik yaşamlarındaki anlamları bu teknolojiler aracılığıyla anlamlandırmaya başlamaktadır (Lupton, 2013, s. 5). Lupton'un bahsettiği şekilde, yeni dijital sağlık teknolojilerinin kullanımıyla, bedenin birçok işlevi artık izlenebilen, kaydedilebilen ve veriye dönüştürülebilen bir hale gelmiştir. Bu verinin dijital veri tabanlarında hazır bir şekilde bulunması ve karmaşık algoritmaların analiziyle yorumlanarak bireyler ya da binlerce kullanıcı için üretilen istatistiklerle yorumlanması mümkündür (2013, s. 3). Bu da bir sonraki başlık olan yeni gözetimin bir türü olarak kabul edilebilmektedir ve Gary Marx bunun nasıl yapıldığını açıklayan en önemli isimlerden bir tanesidir.

3.4.9. Yeni Gözetim (Gary Marx)

Gözetim sosyolojisi alanında önemli bir isim olan Lyon, Gary Marx'ın "Undercover"[10] (1988) isimli ünlü çalışmasının yukarıda da bahsedilen elektronik gözetlemenin sosyolojik olarak analiz edilmesi açısından çok önemli olduğunu belirtmektedir. Literatüre bakıldığında Marx'ın kişisel bilgileri toplamanın, analiz etmenin, iletmenin ve kullanmanın yeni yollarını gösteren bir kavramsal haritanın oluşturulmasına derinden katkıda bulunduğu söylenmektedir ve bugün gözetimi anlamaya yardımcı olacak bazı önemli kavramları üretmektedir. Gözetleme çalışmalarında yaygın olarak kullanılan diğer birçok terimle birlikte "yeni gözetim", "kategorik şüphe" ve "maksimum güvenlik toplumu" terimlerini icat eden "gözetim toplumu" terimini ilk kullananlardan biridir (Marx, Lyon ve Ball, 2015, s. 540).

[10] Kitabın Türkçe çevirisi bulunmadığı için kitap orijinal ismiyle verilmektedir.

Lyon’a göre Marx, sosyal ve teknolojik faktörler arasındaki etkileşimin sürekli olarak göz önünde bulundurulması gerekmesine rağmen, yeni teknolojinin yeni bir gözetime dahil olduğu konusunda haklıdır. Her şeyden önce, yeni gözetimi kolaylaştıran bilgisayarlardır veya daha doğrusu bilgisayarlar artı telekomünikasyondur. Bunu, özellikle şu anda bilgisayar eşleştirmede görülen yeni kişisel veri kategorilerinin oluşturulmasına izin vererek yaparlar. Ama aynı zamanda yeni bir çıkışa, bir zamanlar oldukça farklı toplumsal kurumların alanı olan gözetim anlarının bütünleşmesine olanak sağlıyor olabilmektedirler (Lyon, 1992). Yeni gözetimin daha iyi bir tanımı, kişisel verileri çıkarmak veya oluşturmak için teknik araçların kullanılmasıdır. Bu, bireylerden veya bağlamlardan alınabilir. Bu tanımda, bilgiyi çıkarmak ve yaratmak için "teknik araçların" kullanılması, yardımsız duyulara sunulanın veya gönüllü olarak bildirilenin ötesine geçme yeteneğini ifade eder. Örneklerin çoğu, maddi eserler veya bir tür yazılım kullanarak duyuları genişletir, ancak muhbirler ve gizli polislerde olduğu gibi, kök salmanın teknik araçları da aldatma olabilir. "Bireyler" ile "bağlamların” kullanılması, çoğu modern gözetimin aynı zamanda ortamlara ve ilişki kalıplarına da baktığını kabul eder. Anlam, kendi başlarına ifşa olmayan ayrık veri kaynaklarının (bilgisayar eşleştirme ve profil oluşturmada olduğu gibi) çapraz sınıflandırılmasında bulunabilir. Kişiler kadar sistemler de ilgi çekicidir (Marx, 2002).

Marx, gözetimde normatif değerlendirme yapılırken en azından bu 5 faktöre dikkat edilmesi gerektiğini söylemektedir:

> “1. Gözetim araçlarının doğasında var olan özellikler
>
> 2. Araçların uygulanması
>
> 3. Gözetimin amaçlarının algılanan meşruiyeti ve doğası
>
> 4. Gözetimin kullanıldığı ortamın yapısı
>
> 5. Toplanan verilerin gerçek içeriği, türü veya biçimi” (Haggerty ve Ericson, 2019).

Marx'ın gözetimi değerlendirmek için 1988 senesinde "Undercover"ın son bölümünde maksimum güvenlik toplumu kavramını geliştirdiği ve bu toplum ile ilgili alt toplumları analiz ettiği belirtilmektedir. Bu toplumlardan bazıları: Sıkı tasarlanmış bir toplum, yumuşak ve baştan çıkarıcı tasarlanmış bir toplum, bir dosya topluluğu, bir aktüeryal toplum, şeffaf bir toplum, kendini denetleyen toplum, şüpheli bir toplum ve sürekli iletişim halinde olan ortam ve her yerde bulunan sensörlerden oluşan ağ bağlantılı bir toplum şeklinde sıralanmaktadır. Marx'ın da belirttiği gibi, Windows bunları düzenleme ilkesi olarak kullanmasa da rasyonel kontrole yönelik bu çabalar kitap boyunca resmedilmiştir (Regan, 2017). Maksimum toplum kavramı, bütüncül kurum ve maksimum güvenlikli hapishane ile paralellikler kurar ve geleneksel olarak hapishaneyle ilişkilendirilen kontrol biçimlerinin daha geniş topluma yayıldığını öne sürer. Ancak soyut bir kavram olarak, gözetim uygulamalarındaki çeşitliliği ve zaman içindeki değişiklikleri analiz etmek için çok az şey yapmaktadır (Marx, 2015).

Yeni gözetim, önceki biçimlerden daha yoğun ve kapsamlıdır ve mesafeyi, karanlığı, fiziksel engelleri ve zamanı aşar; kayıtları büyük bir kolaylıkla saklanabilir, alınabilir, birleştirilebilir, analiz edilebilir ve iletilebilir; düşük görünürlüğe sahiptir veya görünmezdir, genellikle istemsizdir; önlemeyi vurgular, emek yoğun değil sermaye yoğundur; merkezi olmayan kontrolü içerir ve belirli bir kişiyi hedeflemekten kategorik şüpheye geçişi tetiklemektedir (Marx, 2001, s. 154).

Çağdaş araçlar, kaçaklar için eski "Aranıyor" posterlerinin pasif taleplerini genişletmekte; birçok talep daha açık uçlu ve meydana gelebilecek olayları belirsiz bir şekilde tanımlamakta, şüpheli durumlar ve kişiler hakkında girdi aramaktadır. Bu nedenle ister tüm nüfus genelinde ister etnik köken, milliyet, din veya kıyafet tarafından tanımlanan alt gruplar içinde olsun, rahatsız edici kategorik bir şüpheye davetiye çıkarmaktadır (Marx, 2013, s. 58). Yeni gözetimde vurgulanan en önemli noktalardan bir tanesi, artık herkesin herkesten şüphe ettiği bir tür güvensizlik duyduğu bir sürece geçilmiş olmasıdır.

Lyon'un gözetleme tipolojisinin kendisi, zorunluluklara ve sınıflandırma hedeflerine göre sıralanmaktadır: Kategorik şüphe, bireyleri yasa ve düzene yönelik risk ve tehditlere göre sınıflandırmak için bilgi toplamayı içerirken (bu durumda, tahmine dayalı polislik en iyi örnektir), kategorik baştan çıkarma ise potansiyel tüketicileri belirli amaçlarla (hedeflenen pazarlama, finansal hizmetler, kredi, sigorta fiyatlandırması ve benzerleri için) sınıflandırmayı içermektedir (Brayne, 2022, s.373). Hem kategorik şüphe hem de kategorik baştan çıkarma için geliştirilen mantığın kullanıldığı sistem ise Zuboff tarafından gözetim kapitalizmi olarak kavramsallaştırılmaktadır.

3.4.10. Gözetim Kapitalizmi (Shoshana Zuboff)

Büyük veriyi içeriğe dönüştürerek çeşitli ticari amaçlarla, hem tüketicilerin davranışlarının ve tercihlerinin belirlenmesi ve hatta manipüle edilebilme imkânı sağlaması, kapitalizm açısından büyük imkân tanımaktadır. Büyük veri bu anlamda Shoshana Zuboff'un kavramsallaştırdığı gözetim kapitalizminin merkezinde yer alan bir tür sermaye ve hammaddedir. Bu verilerin toplanması, depolanması ve işlenmesi de aynı şekilde kapitalizmin üretim ve tüketim döngüsünde önemli bir konuma erişmiş, büyük veri bir tür güç olarak toplumda güç ve kontrol anlamında yer edinmiştir. Zuboff, bu anlamda gözetim kapitalizminin tek taraflı olarak insan deneyiminin davranışsal verilere dönüştürülmesi için bedava bir hammadde olduğunu iddia etmekte, bu verilerin bir kısmının ürün veya hizmet anlamında iyileştirme için kullanılsa da geri kalanının ciddi bir şekilde makine zekâsı olarak bilinen üretim süreçlerince beslendiğini ve bunun tahmin edici bir pratiğe dönüştüğünü belirtmektedir. Bu tahminleri yapabilmek ve kontrol sağlamak için ise bu ürünler, veriler, vadeli işlem piyasaları dediği davranışsal tahminler için alınıp satılmaktadır. Bu süreçler sonucunda gözetim kapitalistleri, daha da zengin olmuştur bunun temel sebebi ise birçok şirketin gelecekteki davranışlar hakkında önceden bilgi sahibi olmak istemesidir (2023).

Bireylerin verilerini istemli ya da istemsiz olarak vermesi ve bunun bedava bir hammadde olarak işlem görmesi ise Zuboff'un gözetim kapitalizmi çerçevesinde eleştirdiği en önemli noktalardan bir tanesidir. Üçüncü taraf kuruluşlardan olan ve büyük verinin içerisindeki kişisel verilere ulaşmada en çok güç sahibi olan firmalardan biri olan Google'ın mahremiyet ilkelerini değiştirdiği bilinmekte, gün geçtikçe gözetim kapitalizminin birey mahremiyetini ihlal eder hale geldiği görülmektedir. Lokke, Google'ın 2000 yılındaki mahremiyet ilkelerini 1 sene içerisinde nasıl değiştirdiğine bakma gerekliliğini göstererek, önceki senelerde anonimlik garantili olan kullanımın, ihtiyaç duyulduğunda Google'ın yalnızca kullanıcının kim olduğunu tanımlamakla kalmayıp, bunu üçüncü kişilerle de paylaşabileceği değişimini yaptığını göstermektedir. Bu anlamda Google'ı ziyaret eden kişinin kim olduğu, hangi ülkede olduğu bilinebilecektir (2020, s. 80). Google, bunu yapan tek firma değildir. Yine Lokke'un paylaşmış olduğu bir örnekte Snapchat'in de bir anda şartlarını değiştirdiği ve yeni koşulların altında "İçeriğinizi, her türlü medya ve dağıtım yöntemi üzerinden saklamak, kullanmak, yeniden üretmek, birleştirmek, düzeltmek, parçalarını kullanmak, yayınlamak, radyo-televizyonda yayınlamak, dağıtmak, gazetelere satmak, reklamını yapmak, sergilemek ve kamuya açık şekilde göstermek için Snap'a dünya çapında, süresiz ve teklifsiz ve devam eden izin vermektesiniz" ibaresini kullandığı bilinmektedir (Lokke, 2020, s.74). Tüm firmaların rekabet içerisinde büyük veri sermayesi üzerinden rekabet etmesi ve bireylerin davranışlarını kontrol etmeye çalışması ise gözetim kapitalizminin nasıl işlediğini ve büyük verinin bu anlamda nasıl büyük bir güç haline geldiğini gösteren durumlardan bir tanesidir.

Gözetim kapitalizmini ele alan Zuboff'un da yazar olarak yer aldığı bir çalışmada gözetleme kapitalizminin kendisinin 2001/2002'de Google'da keşfedildiğini, test edildiğini, detaylandırıldığını ve kurumsallaştırıldığını ve oradan büyüdüğünü savunmaktadır (Zuboff, Möllers, Wood ve Lyon, 2019, s. 259). Bu sistemin nasıl kurulduğu ve devam ettiğini de örneklerken yine Google üzerinden bir örnek sunmaktadır. Google'ın davranışsal tahmin alanında gittikçe artan rakipleriyle baş etmek için "tıklama fizikçisine" ihtiyaç duyduğu, bu açıdan yapay zekâ,

istatistik, makine öğrenimi, veri bilimi ve tahmine dayalı analitik gibi alanlarda dünyanın en büyük beyinlerine ihtiyaç duyulmaktaydı (Zuboff, 2023).

Buradaki önemli nokta ise bireylerin rızalarının alınıp alınmaması, bu sistemleri bilinçli ya da bilinçsiz şekilde kullanmalarıdır. Bunun sebebi ise temelde bireyler farklı amaçlar için bu sistemleri kullanırken verilerinin alınması, mahremiyet ilkeleriyle ilgili değişikliklerin bir üst paragrafta da örneklendirildiği şekilde çok hızlı bir şekilde değiştirilmesi ve bu değişikliklerin çok belli belirsiz, kullanıcı tarafı için iyileştirmeler yapıldığı söylenerek kapitalizmi daha destekler şekilde hareket etmesidir. Zuboff da bu konuyla ilgili doğrudan şu yorumu yapmaktadır: “Buradaki çirkin gerçek, büyük verilerin çoğunun bilgimiz veya bilgilendirilmiş onayımız olmadan hayatımızdan koparılıp alınmasıdır. Sanal ve gerçek dünyalarda yol alırken görünmez ve tespit edilemez olacak şekilde tasarlanmış zengin bir dizi gözetim uygulamasının meyvesidir. Bu gelişmelerin hızı artıyor: Dronlar, Google Glass, giyilebilir teknolojiler, nesnelerin interneti (ki bu belki de hepsinin en büyük örtmecesidir)” (Zuboff, 2014).

Büyük verinin, onu destekleyen sistemlerle birlikte bir tür güç haline gelmesi ise gözetim kapitalizmi kavramı çerçevesinde Büyük Öteki kavramıyla açıklanmaktadır. Zuboff’a göre Büyük Öteki, hukukun üstünlüğünün sağladığı özgürlüğü yok eden yakın bir geleceğin egemen bir gücüdür ve bu gücünü de bedenleri, iletişimden düşünceye günlük deneyimleri kaydeden, değiştiren ve metalaştıran bir güç olmasından almaktadır. Bu güç her yerde hazır bulunan, ağ bağlantılı bir kuramsal rejim olarak tanımlanmaktadır (Zuboff, 2016). Bu kullanımların doğası ve sonuçlarının incelenmesi, gözetim kapitalizminin üstü kapalı mantığına ve onun bağlı olduğu küresel bilgisayar aracılığı mimarisine ışık tutar. “Bu mimari, benim "Büyük Öteki" adını verdiğim, gücün dağıtılmış ve büyük ölçüde tartışmasız yeni bir ifadesini üretiyor. Bu mimari, insanları kendi davranışlarından etkili bir şekilde sürgün ederken yeni tüketim pazarları üreten, beklenmedik ve çoğunlukla okunaksız sömürü, metalaştırma ve kontrol mekanizmalarından oluşuyor: Davranış tahmini ve modifikasyonu. Gözetim kapitalizmi, demokratik normlara meydan okur ve piyasa kapitalizminin

yüzyıllardır süren evriminden kilit noktalarda ayrılır” (Zuboff, 2015). Büyük Öteki kavramını çok eleştirel bir şekilde kavramsallaştırırken, bu gücün bireylerin verilerini elde edip kullanırken, bir yandan insani ve bireysel kısımlarına asla saygı duymadığı ve tehlikenin gittikçe büyüdüğüne vurgu yapmaktadır (Zuboff, 2019).

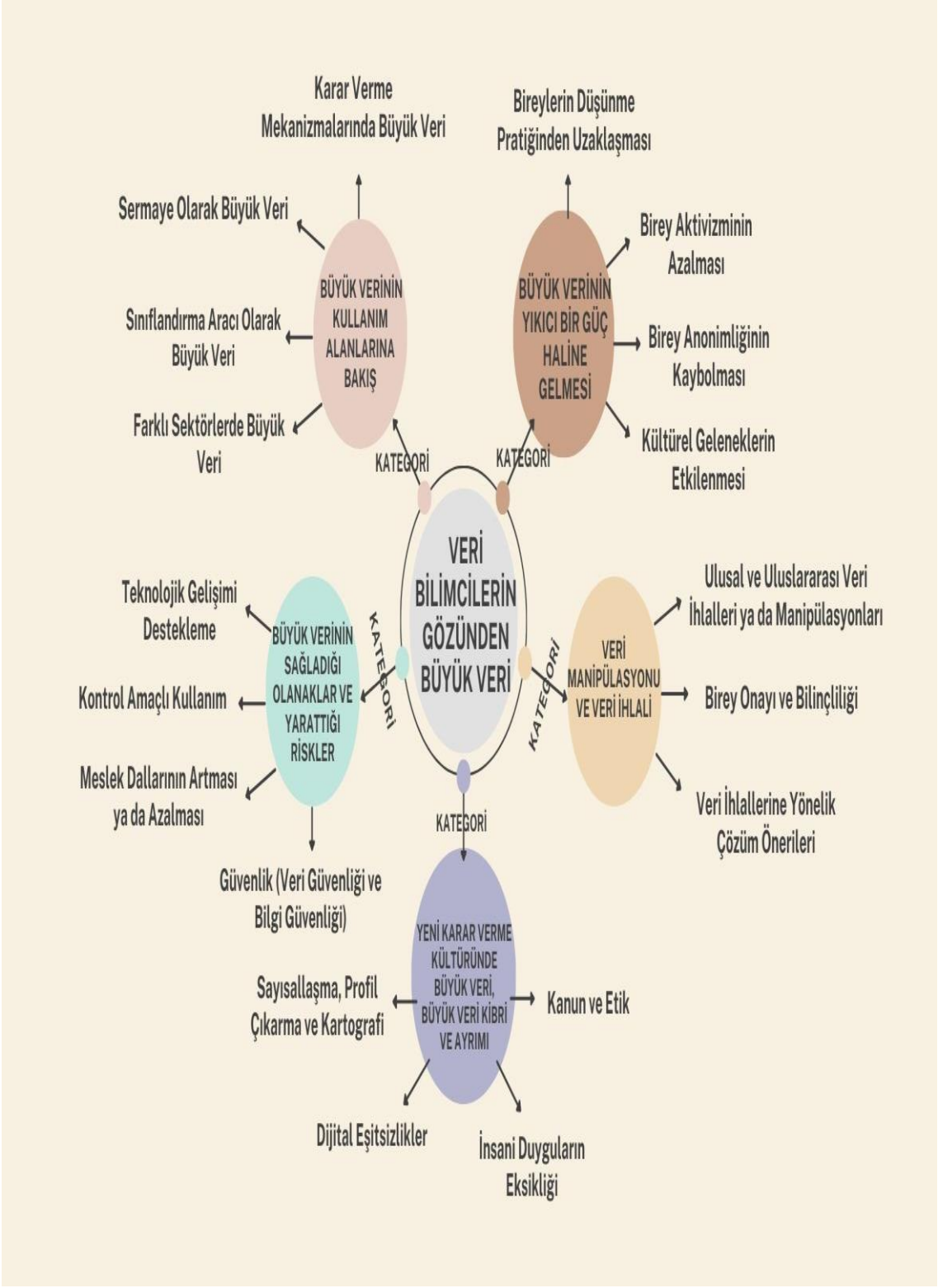
4. BÖLÜM

ARAŞTIRMANIN BULGULARI VE VERİLERİN ANALİZİ

4.1. VERİ BİLİMCİLERİN GÖZÜNDEN BÜYÜK VERİ

Veri bilimcilerin gözünden büyük veri temasının altında, Şekil 5'te yer aldığı haliyle beş kategori belirlenmiştir. İlk kategoride, "Büyük Veri ve Büyük Verinin Kullanım Alanlarına Bakış", karar verme mekanizmalarının temeli olarak büyük veri, sermaye olarak büyük veri, sınıflandırma aracı olarak büyük veri ve farklı sektörlerde büyük veri alt kategorilerine ulaşılmıştır. İkinci kategoride, "Büyük Verinin Sunduğu Olanaklar ve Yarattığı Riskler", teknolojik gelişimi destekleme, kontrol amaçlı kullanım, meslek dallarının artması ya da azalması alt kategorilerine erişilmiştir. Üçüncü kategoride, "Yeni Karar Verme Kültüründe Büyük Veri, Büyük Veri Kibri ve Büyük Veri Ayrımı", sayısallaşma, profil çıkarma ve kartografi, dijital eşitsizlikler, yeni karar verme kültüründe insani duyguların eksikliği ve kanun ve etik alt kategorileri belirlenmiş; dördüncü kategoride, "Veri Manipülasyonu mu? Veri İhlali mi?", ulusal ve uluslararası veri ihlalleri ya da manipülasyonları, birey onayı ve bilinçliliği ve veri ihlallerinin çözüm önerileri alt kategorilerinden bahsedilmiştir. Beşinci ve son kategoride, "Büyük Verinin Yıkıcı Bir Güç Haline Gelmesi", bireylerin düşünme pratiğinden uzaklaşmaları, birey aktivizminin azalması, birey anonimliğinin kaybolması ve kültürel geleneklerin etkilenmesi alt kategorilerinden bahsedilerek ilk temanın analizi gerçekleştirilmiş, araştırmanın bulguları detaylı bir şekilde yazılmıştır.

Şekil 5. Veri Bilimcilerin Gözünden Büyük Veri Teması Kategori ve Alt Kategori Şeması



4.1.1. Büyük Veri ve Büyük Verinin Kullanım Alanlarına Bakış

Dijitalleşen toplumda yeni gözetim pratiklerinin toplumsala etkisi pek çok alanda kendini göstermektedir. Bu gözetim pratiklerinin temelini oluşturan temel kaynak ya da sermaye ise büyük veridir. Büyük verinin içerdiği veriler görsel, işitsel, yazılı formatta pek çok kaynağı içerdiği gibi veri bilimcilerin tanımlamalarında da gösterileceği gibi yapısal ve yapısal olmayan kaynakların da birleşimiyle daha güçlü hale gelmektedir. Bu anlamda büyük veri, sadece verinin büyüklüğü anlamına gelmemekte bunun yanı sıra verinin yapısal niteliklerini de kapsamaktadır.

> *"Büyük veri aslında verinin büyüklüğü demek, onun miktar derken terabaytlar cinsinden değil de aynı zamanda verinin yapısal olup olmamasıyla da alakalı bir şey. Mesela bir SQL'deki gibi tutabileceğimiz veriler değil, görsel veriler olabilir, doğal diller olabilir hepsi birleştiğinde büyük veriyi oluşturur. Büyük veri sadece verinin miktarının çok olması değil, yapısının farklı olması yapısal olmayan ya da yarı yapısal veriler de büyük veriye dahil olur diye düşünüyorum."* (Katılımcı 8, 29, Kadın)

Katılımcı 8'in büyük veri tarifindeki gibi yapısal, yapısal olmayan ya da yarı yapısal olan verilerin birleşmesiyle büyük verinin farklı bir tanıma ulaştığı ve bu şekilde tanımlandığını düşünen bir katılımcı daha bulunmaktadır:

> *"Baktığımız zaman yakın zamana kadar veri tabanında işlenebilen veriler yapısal veri olarak tarifleniyordu. Bunlar üzerinde iş ve işlem yapılabiliyordu. Veri tabanında işlenemeyen formal olmayan veriler yapısal olmayan veriler olarak adlandırılıyordu. Bu veriler üzerinde bazı durumlarda işlem yapılamıyordu. Nedir bu durumlar? Office dosyaları, görüntü, resim, sensör verileri, sinyaller, ses dosyaları, video verileri, fotoğraflar bu yapısal olmayan veriler de teknolojinin veya verinin işlenebilirliği ile öne çıkıp kullanılabilir hale geldi. Büyük veri dediğimiz yapı, yapısal olmayan verilerle yapısal verileri tek çatı altında toplayan platform."* (Katılımcı 13, 57, Erkek)

Burada bahsedilen yapısal ya da yapısal olmayan verilerin, farklı formattaki verilerin alınmasının önemi, eskiden toplanan verilerin aksine her tür fotoğrafın, ses kaydının, coğrafi alanların, konum verilerinin entegrasyonla çok daha fazla içerik haline gelmesidir. Bu verilerle artık daha çok yorum yapılmaya başlanmakta, farklı teknolojilerle de desteklenmesiyle veri manipülasyonu çok

daha etkili olabilmektedir. Yapay zekâ destekli sosyal puanlama sistemi örneğine bakıldığında robot kuşlar, yüz tanıma teknolojileri, sosyal medyadan elde edilen metaveriler, fiziki gözetim kameraları, nesnelerin interneti gibi pek çok teknoloji, verileri farklı formatlarda elde etmekte, büyük veri ile tüm bu formatlar bir araya getirilerek vatandaşların puanlamasının çıkarılması sağlanmaktadır. 2021 senesinde Gaziantep Belediye'sinin Akıllı Şehir projesi kapsamındaki uygulamayla ilgili "tam bir interaktif ortam olacak, bizim yaptıklarımızı size daha iyi anlatma fırsatı olacak" diyerek tanıttığı, kişilerin uygulama aracılığıyla elde ettiği puanlarla ücretsiz seyahat gibi fırsatlar yakalayacağına dair haberler sosyal medyada Gaziantep'in sosyal puanlama sistemine geçtiğine dair yankı uyandırmıştır. Gaziantep Belediyesi daha sonra bu açıklamanın yanlış algılandığına yönelik bir kamuoyu duyurusu yayınlasa da burada önemli olan nokta, dijital sistemler ve uygulamalar yoluyla bireylerin veya vatandaşların puanlanması durumunun bu kadar ilgi çekmesi ve çok da uzak ya da zor olmamasıdır. Büyük verinin veri bilimcilerin vurguladığı gibi, farklı formattaki veri toplama özelliği ise bu nedenle çok önemlidir. Tesla örneğinde olduğu gibi, bir kaza olduğunda olayı yaşayanlara değil, kanıt aramak için Tesla'nın kayıt sistemlerini kontrol etmek, bir sağlık durumu olduğunda verileri kişinin akıllı cihazlarından kontrol etmek, bir suç işlendiğinde bireylerin sadece konum bilgilerine değil, bağlı olduğu kişilerin konum ve haberleşme bilgilerine bakabilmek gibi pek çok durum büyük verinin tanımının artık çok daha farklı olduğunu göstermektedir.

Katılımcılara "Büyük veri nedir?" sorusu yöneltildiğinde genellikle "Teknik anlamda mı nedir?" sorusuyla karşılaşılmış fakat onların gerçek görüşlerini öğrenmek için "Sizin için ne ifade ediyor?" şeklinde yönlendirme yapmadan gerçek görüşleri ve anahtar kavramlar elde edilmeye çalışılmıştır. (Fakat bu noktada katılımcıların daha sonra büyük verinin sosyolojik boyutuyla ilgili de önemli beyanlarda bulunduğunu bilmek önem taşımaktadır.) Katılımcıların bazıları, bu anlamda büyük veriyi kavramsal çerçevede detaylıca açıklanan 3V, 4V ya da 7V kavramlarıyla açıklamayı tercih etmiştir. Bu katılımcılar için büyük

veri, işlemleme anlamında değişimin temelinde olan bir kavramı ifade etmektedir.

> *"Büyük veri, her gün her ay bazında üstüne eklenerek büyüyen ve hızının arttığı aynı şekilde hacminin arttığı ve bunlarla belirli programlar kullanılarak ya da uygulamalar kullanılarak doğru sonuca ulaşılması aşamasında verinin temizlenerek doğrulanmasıdır."* (Katılımcı 4, 26, Kadın)

> *"Benim açımdan büyük veri, ben matematik kökenliyim, bu bilimle uğraşıyorum. Klasik yöntemlerle çalışmamıza çok fazla imkân olmayan veri setleri diyebilirim. Dolayısıyla fazlasıyla büyük, karmaşık, yapılandırılmamış ve sürekli değişen, yani 3V üzerinden tanımlamak daha mantıklı. Klasik istatistik yöntemlerinin ya da bugüne kadar erişebilen yöntemlerin çoğunun çalışmadığı paradigmanın değiştiği yerler.*" (Katılımcı 12, 43, Erkek)

3V ile katılımcının bahsettiği özellikler hız, çeşitlilik ve doğruluktur. Büyük verinin sadece veri kaynağının hacim, çeşitlilik, hız, değişkenlik, gerçeklik, vizkozite ve virallik özelliklerini taşıdığı gün geçtikçe değiştiği ve yapay zekâ gibi sistemlerle de desteklendikçe daha farklı bir boyuta taşındığı belirtilmektedir. Bu verinin en temel özelliği bir katılımcının da bahsettiği gibi "*Normal bir bilgisayarda normal yöntemlerle analiz edilemeyen veriler*" (Katılımcı 6, 36, Kadın) olmasıdır.

> *"Ben istatistikçi olduğum için büyük veri benim için gözlem sayısının ve değişken sayısının aynı anda çok fazla olmaya başladığı veridir. Çünkü biz bir şeyi analiz ederken verinin büyüyor olması devasa bir bilgi yığınının olduğu anlamına gelir. Biz bunu analiz yaparken ifade ederken de gözlem sayısı, ilgilendiğimiz verideki boyut, değişken sayısı ne kadar fazlalaşırsa benim için büyük veri odur. Zaten diğer veriler, diğer taraftan büyük veri artık "huge data" falan kavramları girmeye başladı mesela pixel boyutları çok fazla çözünürlüğe sahip olan bir fotoğrafı görüntü işlemeyle analiz etmeye çalışanların sadece bir fotoğrafı da büyük veri kabul ediliyor bazıları tarafından ama ben istatistikçi olarak düşündüğüm zaman benim için boyut anlamında ve gözlem sayısı anlamında ne kadar büyüyorsa büyük veri benim için odur. Bilgisayar ve algoritmalarda makine öğrenme algoritmalarının hızın bir şekilde çözümleyemeyeceği basit bilgisayarlarla kolayca çözüm alamayacağımız veriler ve işte serverlara ihtiyaç duyarak serverlar sayesinde çözüm yapabildiğimiz verilerdir büyük veri."* (Katılımcı 10, 37, Erkek)

Katılımcıların genel anlamda ilk başta büyük veri nedir sorusuna teknik cevaplar verdiği, fakat mülakat devam ettikçe ilerleyen sorularda büyük verinin sosyolojik boyutuna odaklandıkları görülmektedir. Büyük verinin daha sosyolojik boyutunu

ifade edecek açıklamalar yaparak büyük verinin giriş kısmında da açıklandığı gibi dışsal ve zorlayıcı bir olgu haline geldiğini vurgulamakta ve onun kendisini bireye kabul ettiren ve baskı uygulayan nitelikler taşıdığını ileri sürmektedirler. Büyük verinin dışsal ve zorlayıcı bir olgu haline gelmesiyle ilgili olarak, sadece mahremiyet kaybından değil, tarafsızlık ve adalet, temel özgürlük ve insan hakları temelinde de önem taşıyan bir konu haline geldiğinden bahsedilmektedir. Büyük verinin temel özelliklerinden biri, bireylerin onu her zaman varmış gibi içselleştirmeleri ve verilerini verirken genel anlamda farkında olmamaları ya da önemsememeleridir. Bu durumlar düşünülürken bireylerin onay verip vermedikleri önem taşısa da büyük veri genel olarak insan hayatından çekilen tüm veriler anlamına da gelmektedir. Büyük veri etkisini sadece veri manipülasyonu ya da veri ihlali ayrımında (bu ikisi arasındaki fark veri bilimcilerin gözünden de ilerleyen kısımlarda açıklanmaktadır) ya da sadece ekonomik alanda değil, günlük yaşantı, sosyal ilişki, yönetim, ticaret, üretim, tüketim ve bilgi gibi pek çok alanda göstermektedir.

> *"Büyük veri bence böyle, kontrol edilemeden toplanan ve bir anda bizim günlük hayatta çok fark etmeden yarattığımız şeylerin hepsi gibi bakıyorum."* (Katılımcı 9, 35, Kadın)

Büyük verinin özellikle şirketlerin yaptığı veri manipülasyonu ile ilişkilendirildiği ve temel olarak büyük verinin bir tür sermaye olarak çok kuvvetli olduğuna vurgu yapıldığı görülmektedir. Sermaye olarak değerlendiren katılımcıların bazıları büyük verinin yararlı algoritmalar ürettiğini düşünürken, bazı katılımcılar bunun tam aksi beyanda bulunmaktadır.

> "*Dünyada aslında eskiden veriyi işlemek para ederdi, şimdi o veriyi bulmak ve onunla ilgili sorunu yaratmak problem bulmak daha fazla para ediyor ya da daha fazla önem görüyor. Büyük veride hepimizin her şeyiyle ilgili dijital ayak izimiz var internette, bilgisayar ortamında, bunların takip edilmesi bunlara yararlı algoritmalar yaratılması diye düşünüyorum ben. Bunlar üzerinden reklam yapılması belki bizim tanımlanmamız, sağlık verilerimizin tanımlanması, alışveriş isteklerimizin beklentilerimizin tanımlanması, bunun üzerine bize uygun sistemler üretilmesi ve bunları kapsayan program aslında "big data" dediğimiz olay."* (Katılımcı 2, 28, Kadın)

Katılımcı 2'nin burada büyük veriyi doğrudan "para eden" bir şey olarak tanımladığı ve verinin doğrudan kendisinin, onu bulmanın ve ulaşmanın para eden, bulunduğumuz sistem içerisinde değerli bir şey haline geldiğini belirttiği görülmektedir. Buradaki önemli nokta, katılımcının dijital ayak izlerinin yararlı algoritmalar yaratacağını ve bunların pek çok farklı alanda bireylere fayda sağlayacağını düşünmesidir. Yararlı algoritma olarak değerlendirilmesi ise reklam, sağlık ve pazarlama alanında önerilerin daha doğru tespit edilmesi gibi durumlarla ilişkilendirilmektedir. Katılımcı 3 ise büyük veriyi doğrudan "büyük birader" kavramı ile ilişkilendirerek, veri ihlali ya da veri manipülasyonu ile bağlantılı olaylarla tanımlama yoluna gitmektedir:

> *"Büyük birader. Facebook'taki olaylar, sonra ABD seçimlerinde olan şeyler, WhatsApp'ın bizim hangi verilerimizi topladığı onun dışında TikTok'un çok fazla veri topladığı bir uygulama olduğu için uzak durma tavırlarımız ne bileyim telefonda konuştuğumuzda hemen onun reklamının çıkması. Bunlar aslında büyük data dediğimiz zaman, bütünsel bir data, her şeyi içeren bir dataymış gibi bir şey geliyor aklıma."* (Katılımcı 3, 30, Erkek)

Sosyolojik olarak bakıldığında, pazarlama gibi alanlarda büyük verinin kullanılmasının tamamen bireyler hakkında veri toplama ve onları gözetleme, büyük verinin büyük birader olarak işlev görmesini katılımcı "uzak durma tavrının" sebebi olarak göstermektedir. Zuboff'un gözetim kapitalizminde gösterdiği şekilde, büyük veride içerik ticari amaçlarla, davranış ve tercihlerin belirlenmesinde ve manipüle edilmesinde kullanılmaktadır. Buradaki sorunlu nokta, bunun farkında olan bireylerin uzak durma davranışında bulunmalarının muhtemel bir sebebini ise, birey ve verilerinin bedava hammadde olması, verilerin istemli ya da istemsiz şekilde her şekilde kullanılması ve teknolojiler geliştikçe özellikle giyilebilir teknoloji araçlarıyla gözetim kapitalizminin artması oluşturmaktadır. Bir noktada büyük verinin Büyük Birader ya da Zuboff'un tanımıyla Büyük Öteki olarak değerlendirilmesi, bireylerin onayını yok saymasından ya da özgürlüklerine tehlike oluşturacak bir güç olarak görülmesinden kaynaklanmaktadır.

Büyük veri sadece ticari ilişkilerde değil, pek çok farklı alanda kullanılmaktadır. Büyük verinin kullanım alanları incelendiğinde ilk ortaya çıkışındaki gibi hastalık dağılımlarını takip etme, iş trendlerini, suç kalıplarını, web trafiğini, hava durumunu, tüketim pratiklerini inceleme ve belirleme hedefinin yanı sıra pek çok farklı kullanım alanının olduğu görülmektedir. Bu çalışmada ise güncel durumda hem katılımcıların çalıştıkları sektörlerin onların büyük veriye bakış açılarını etkileyebileceği düşüncesi, hem de büyük verinin gerçekten ne kadar farklı alanlarda, uygulamalarda ve farklı şekillerde kullanıldığını görebilmek amacıyla katılımcılara, büyük veriyi mesleklerinde nasıl kullandıklarına yönelik soru yöneltilmiştir.

Çalışmaya katılım sağlayan veri bilimcilerin hepsi, kendisini veri bilimcisi olarak tanımlasa da her birinin farklı sektörlerde, farklı projelerde ve farklı amaçlarla büyük veriyi kullandığı bilinmektedir. Katılımcıların büyük veriye ve büyük verinin kullanım amaçlarına bakış açıları benzerlik gösterse de her birinin kendi mesleklerinde büyük veriyi nasıl kullandıklarına bakmanın bu açıdan anlamlı olduğu düşünülmektedir. Katılımcıların büyük veriyi nasıl kullandığına bakıldığında büyük verinin farklı sektörlerde çok farklı amaçlarla kullanıldığı görülmektedir. Bu çalışmada yer alan katılımcıların bulunduğu konumlara bakıldığında; savunma sanayii, belediye, sivil toplum kuruluşu, özel şirket (yemek, telekomünikasyon, teknoloji şirketleri), sağlık gibi iş alanları olduğu anlaşılmaktadır.

Savunma sanayiinde çalışan katılımcılara bakıldığında; bir katılımcının (Katılımcı 1, 29, Erkek) insansız bir kara havacına otonomi faaliyetleri kazandırmak (bu hedefle bu aracın gideceği yol temiz mi, güzergahı düzgün mü, bir birey bulduğunda bu birey yaralı mı, tespit ettiği mayınlar gerçek mi yoksa patlayıcı mayın mı olduğuna bakmak) için, diğer bir katılımcının ise (Katılımcı 3, 30, Erkek) fiziksel fenomenlerin datalar işlenerek ya da filtrelenerek yapılan analizlerle ürünlerin performanslarının ölçülmesi için büyük veriyi kullandığı görülmektedir. Yine aynı sektörden kendi şirketi olan bir katılımcı (Katılımcı 13, 57, Erkek), şirketinin NATO tesis ve umumi tesis güvenlik

belgelerine sahip olduğunu, büyük veriyi ulusal güvenlik için kullandıklarını söylemektedir.

Bir belediyede görev alan katılımcının (Katılımcı 2, 28, Kadın), büyük bir şehirde afet acil toplanma alanlarının analizini yapan bir proje geliştirme (alanların suya yakın olması, erişilebilir olması, insanların temel ihtiyaçlarının karşılanabilir olması, sinyal sıkıntısının olmaması, kişi başına düşen metrekare sayısı gibi değişkenleri göz önünde bulundurarak belirli formülasyonlarla mahallelerin nüfusa göre ayarlanarak acil durum alanlarının risk analizinin yapılması) ve akıllı şehir projeleri üzerine çalıştığı bilinmektedir. Bir sivil toplum kuruluşunda çalışan diğer bir katılımcı (Katılımcı 4, 26, Kadın) ise büyük veriyi mesleğinde kullanırken, yapılacak yardımların kaç kişiye gideceği, bu yardımların hangi kişilere hangi önceliklerle ulaşması gerektiğine verilerle yapılan analizlerle karar verildiğini, gerçekleşen yardım projelerinin devamı ya da sonlandırılması için yine bu verilere dayalı olarak analiz yaptığını belirtmektedir.

Özel şirketlerde farklı sektörlerde çalışan katılımcıların da büyük veriyi çok farklı biçimlerde kullandıkları görülmektedir. Fast-food zincirleri olan bir firmada çalışan bir katılımcı (Katılımcı 5, 26, Kadın), büyük verilerle birey ve şube bazında hangi ürünlerin tercih edildiğini öğrenme, lokasyona göre fiyat belirleme, ona göre kampanyalar düzenleme anlamında gerekli önlemlerin alınması için büyük veriyi kullanmaktadır. Aynı şekilde Türkiye'de bilindik bir teknoloji şirketinin veri bilimi uzmanlarından biri olan diğer bir katılımcı (Katılımcı 7, 42, Erkek), büyük veriyi tahminlemede ve özellikle makine öğrenmesinde kullandıklarını, şirketin simasını değiştirmek, iyi tutmak ve müşterilerin ilgisini çekecek hale getirmek amacıyla değerlendirdiklerini belirtmektedir. Bu alanda iki tane şirketi olan başka bir katılımcı (Katılımcı 15, 55, Erkek), büyük veriyi müşteriden veriyi alarak bu veriyle ne yapmak istediklerini sorarak onlara analiz ve tahminleme sunduklarından bahsederken, ek olarak bu alanda veri biliminde yeterli yetkinliğe sahip personelin olmadığını ve bu yetkinlikte personel yetiştirilebilmesi için eğitimler düzenlediklerini belirtmektedir. Özel şirkette çalışan fakat İşkur, TÜİK, bakanlıklar, bankalar ve yurt dışındaki şirketlerle

projeler yapan bir katılımcı, büyük verinin kendi içinde işlemlemesinin de önemli olduğunu ve kendisinin bu alanda uzmanlaştığını belirtmektedir:

> *"Herkesin verisi ve gittikçe artan bir veri var orada bize ihtiyaç duyuyor o veriyi yönetmek, uygun veri kalitesi süreçlerinden geçirmek, uygun yerde depolamak, bu depolama süreçlerini planlamak veya veriyi isteyen kim görselleştirme ekibi mi, model ekibi mi onlara uygun veriyi uygun şekilde iletmek, doğru veriyi iletmek çünkü biraz herkes veri deyince ve bilgisayar alanında konuşunca çok rahat oluyorlar. Sanki her şeyin her an olabileceğini düşünüyorlar ama diskspaceler önemli, verinin hızı önemli mesela şu an Google'a tıkladığınızda bir dakika beklerseniz hoşunuza gider mi? Gitmez. Dolayısıyla hız önemli, yapı önemli, mimari önemli. Ben tam buralarda çalışıyorum işte. Bunlara karar veriyorum."* (Katılımcı 14, 26, Erkek).

Büyük verinin işlenmesi ve kullanılması gündelik hayatımızda uyum sağladığımız tüm teknolojilerin de temelinde olduğu için onun her şeyden fazla içselleştirildiği ve bu sebeple de vazgeçilmez olarak görüldüğü dikkat çekmektedir. Bireylerin aklına bir soru takıldığında sosyal çevresindeki kişiler yerine Google'a sorması, Google'ın da bu kişiler ile ilgili kurduğu kartografiler ve algoritmalar üzerinden onlara yanıt vermesi, bu soruyu ne anlamda ve ne için sorduğunu düşünerek cevaplaması bu sistemin en net örneğidir. Google, bu soruları yanıtlamak için bir yandan kişilerin hangi soruları sorduğunu, hangi IP'den sorduğunu, neden sorduğunu depolamakta bir anlamda da araştırmaktadır. Çapraz eşleştirme ile bireyin Google'da sorduğu bir soruyla, o gün Instagram hesabından paylaştığı bir bilgi ya da Twitter'da yazdığı bir düşüncesinden bireyin ruh haline, yaşadığı olaylara kadar pek çok tahminleme yapılmaktadır. Bu tahminlemelerin de çeşitli amaçlar ve hedeflerle kullanıldığı bilinmektedir. Bireylerin kasıtlı olarak Google'ı kullanmasının sebebi ise Google'ın bu sistemleri kullanarak onlardan topladığı verilerle daha tercih edilebilir öneriler sunmasıdır: *"Özellikle Yandex yüklü geliyor. Ama ben özellikle Google kullanıyorum. Yandex bana user friendly (kullanıcı dostu) gelmiyor, istediğim sonuçları çıkarmıyor gibi geliyor genellikle."* (Katılımcı 2, 28, Kadın). Diğer bir katılımcı için tercih sebebi, Google'ın aranan şeylerin gizli kaldığı düşünülen "gizli sekmesinin" olmasıdır: *"Yandex ve Yahoo iş yerinde otomatik olarak bağlanarak açılıyor, Google'ı da gizli sekme açmak için kullanıyorum"*

(Katılımcı 4, 26, Kadın). Başka bir katılımcı, Google'ı güvenli ve erişilebilir bulduğu için (Katılımcı 7, 42, Erkek); bir diğeri ise aradığını rahat bulmasının yanı sıra bir tür alışkanlık olduğu için şeklinde açıklamaktadır: *"Aradıklarımı çok rahat bulabiliyorum. Alışkanlık galiba. Seneler önce Google başlayıp, Google olarak devam ettiğimiz için."* (Katılımcı 9, 35, Kadın).

Bu bilgilere ek olarak, sektörler bazında katılımcıların büyük veri kullanımına bakıldığında hem devlet hem özel sektörle projeler geliştirdiği bir pozisyonda özel şirkette çalışan başka bir katılımcı da büyük verinin karlılık amaçlı olduğu vurgusunu yapmakta ve yaptıkları projelerin temelini şu şekilde açıklamaktadır:

> *"Ben mesleğimde hem devlet taraflı hem özel sektör taraflı projelerde yer aldım. Devlet taraflı projelerde de aslında bir tanesinde yaptığımız bir sınıflandırma projesi olarak geçiyor bizde. Nedir? Bankacılıktan örnek vereyim. Kredi alabilir ya da alamaz, ödeyebilir, ödeyemez gibi bir yapıda devlet için bir sınıflandırma yaptık işsizlik durumları üzerine. Devlet de tabi bu bilgiyi alıp ona göre eğitim programlarını güçlendireceğini planlıyor. Öyle ifade ettiler. Yine diğer tüm devlet ve özel sektör projeleri de aslında karlılık amaçlı. Çıkan tahminlerle talep tahmini yaparak hani siz bu ay bu kadar satarsınız ona göre stoğunuzu, deponuzu yönetin, çalışanlarınızı ona göre ayarlayın gibi aslında karlılık üzerineydi."* (Katılımcı 16, 26, Erkek)

Katılımcının cevabının devamında bu tezde sıklıkla bahsedilen ve sosyal puanlama sistemlerinin bir alt dalı olarak görülebilecek kredi puanlaması için büyük verinin kullanılmasını açıklanmakta, kendisi de bunu bir tür sınıflandırma olarak tanımlamaktadır. Katılımcı, devletin bu kategorizasyonla eğitim programlarını güçlendireceğini belirttiğini söylerken biraz imalı şekilde yorum yapmakta, konuşmanın devamında ise yine karlılığa dikkat çekmektedir.

Aynı şekilde bir kategorizasyondan bahseden, finans sektöründe çalışan bir katılımcı (Katılımcı 6, 36, Kadın), yapay zekâ tarafından geliştirilen modellerin sonucunda bir bankanın kime kredi verip, kime kredi vermeyeceğine karar vereceği risk skorlarını hesapladığını belirtmektedir. Bir müşterinin tüm finansal bankacılık ya da finans sektöründe ne kadar borcu var, nasıl bir güvenilirliği var kararlarının yanı sıra, yeni bir ürünün hangi müşterilere önerilebileceği gibi kararların da bu mekanizmalar doğrultusunda belirlendiği belirtilmektedir, bu

sistemin KKB, Türkiye'de kredi kayıt bürosu ile yapıldığını, Findeks Türkiye'de de bireysel Findeks notunun, ticari kredi notunun belirlenmesi için kullanıldığını ifade etmektedir. Söz konusu katılımcı, yurt dışına gitmeden önce bu sistemlerin oluşturulmasında aktif rol aldığını belirtmiştir.

Sağlık sektöründe çalışan bir katılımcı (Katılımcı 8, 29, Kadın), büyük veriyi medikal araç regülasyonu için kalite güvence amacıyla kullandığını, ürettikleri ürünlerin hastalara teslim edildikten sonra, satış sonrası klinik takibi yapmak için kullanıldığını belirtmektedir. Şu an veri topladıklarını ve veriler çoğaldığında örneklem seçip hastaları belirli gruplara ayırıp bu veriler üzerinden analizler yapmaya devam edeceklerini eklemektedir.

Akademi alanında çalışan katılımcılara bakıldığında post-doc yapmakta olan bir katılımcının (Katılımcı 9, 35, Kadın), bireylerin ulaşım pratiklerini tespit ederek, deneyimlerini toplayarak, A noktasından B noktasına biletin fiyatı, martı ya da e-bike ya da bölgede hangi ulaşım metodu varsa onları kapsayacak şekilde bilgileri göstererek insanların davranışlarını değiştirmeye ve ulaşım pratiklerini düzenlemeye çalıştıklarını belirtmektedir (Katılımcı 9, 35, Kadın). Aynı şekilde akademide çalışan başka bir katılımcı (Katılımcı 10, 37, Erkek), büyük veriyi çeşitli projelerde kullandığını, Türkiye'de çeşitli sınavlara giren öğrencilerin verileriyle öğrencilerin başarılarını görebilmek, okulların başarılarını, bir şikâyet durumunda bu şikâyet için analizlerle cevap verme olanağı elde etmek için kullandığını belirtirken *"Bir kişiyi üç milyon kişiyle karşılaştırabilecek bir yapı kurmuş oluyorsunuz"* ifadesinde bulunmaktadır. Akademide çalışan ve bu alanda önemli araştırmacılara eğitim veren başka bir katılımcı ise (Katılımcı 12, 43, Erkek) büyük veriyi mesleğinde onun teknik ve yöntem boyutlarını inceleyerek kullandığını, finansal tahminleme, proje izleme ve değerlendirme ve metin madenciliği için kullandığını söylemektedir. *"Çok endüstriyel bir iş olmadığı için, metin madenciliğinden çok, büyük veriyle çalışanlar endüstriyel sektörde bankacılık, sigorta, perakende ya müşteri davranışı ya da eğer üretim sektöründeyse sensör datası üzerinden predictive maintenance, modelleme ve tahmin işleri çalışıyorlar. Metin doğrudan çalışanlar daha sınırlı, metinden*

üretmeye çalışanlar biraz da akademik tarafta yaygın" şeklinde endüstriyel ve akademik anlamda büyük verinin kullanımıyla ilgili bir farklılığa değinmektedir.

Katılımcılara bu alanda analizler yapabilmek için geliştirmeyi düşündükleri belirli bir hedefleri olup olmadıklarına yönelik sorular da yöneltilmiştir. Genellikle katılımcılar büyük verinin kullanımının pozitif yanlarına değinirken, hedeflerinden birisinin siber-güvenlik sorunlarını çözmeye yönelik olduğu görülmektedir.

> *"Siber alanda eskiden hatırlayamıyorum İstanbul'da bir profesyonelin yaptığı bir iş vardı. Çok da büyük bir yatırım aldı bununla ilgili. Bilgisayarı kullanan kullanıcının sen olup olmadığını daha önce senin kullanımlarından topladığı bilgiyle ayırt ediyor. Sen bilgisayarı açtın normalde bizim klasik yöntemlerimiz nedir. Şifreyi girdin. Açtın. Parmak izi, yüz tanıma bu şekilde güvenlik önlemleri alınıyordu bu zamana kadar. Şimdi yeni çıkan bir yöntemle senin düzenli kullanımda ilk açılışta ne yapıyorsun genelde hangi programları ne kadar kullanıyorsun. Bunun gibi topladığı tüm verilerin hepsini analiz yapıyor daha sonra kullanıcının sen ya da başkası olduğunu anlayıp diyor ki bu kullanıcı sen değilsin. Bilgisayara bir siber saldırı var deyip onun tüm işlemlerini blokluyor. Bu tarz bir tam ismini hatırlamıyorum bir yöntem geliştirdiler siber alanda bu alanlarda bilgi sahibi olmak isterim."* (Katılımcı 1, 29, Erkek)

Katılımcıların her birinin katılımcılarla ilgili tabloda görüldüğü üzere uzmanlaşmış olduğu, pek çok büyük veri analiz programı olsa da farklı alanda farklı pek çok uygulamayla ilgili kendilerini sürekli olarak geliştirmeye ve daha farklı alanlarda uygulamalar yapmaya çalıştıkları görülmektedir. Bir katılımcı bunun sebebini farklı müşterilerle çalışabilmek ve hazır gelen veriyle çalışmak değil, veriyi hazır hale getirebilmek için yeterli donanıma sahip olmak ile bağlantılandırarak açıklamaktadır.

> *"Ducker kullanmak Spark kullanmak farklı, String teknolojilerini öğrenmek büyük veriye özel analiz etmek için kullandığım şeyler. Spark kodlama dili. Ben üniversiteden mezun olduğumda verinin çok temiz olduğunu düşünüyordum ama işe başladığımda işin modellemenin yüzde 80'inin veri düzenlemek olduğunu gördüm. Bunun için de akademideki tüm veri yani biri sizin için veriyi düzenlemiş modellemek için önünüze sunmuş gibi oluyor. Orada çok daha fazla özelleşme var sadece boosting algoritmaları üzerine odaklanmış olabilirsiniz ve genelde zaten kullandığınız tek bir teknoloji oluyor, o teknolojiyle de teknoloji ölmediği sürece onla devam*

> *edilebiliyor. İş hayatında özellikle müşteriyle çalışılıyorsa yeni teknolojileri öğrenmek, teknoloji bağımsız olabilmek çok önemli farklı müşterilerle çalışabilmek için.*" (Katılımcı 6, 36, Kadın)

Başka bir katılımcı (Katılımcı 7, 42, Erkek) sadece analiz değil, veriden anlam çıkarabilmek için de programlar öğrenmenin gerekli olduğunu ve bunun için Sigma'yı iyice öğrenmek istediğini belirtmiştir. Bir diğer katılımcı ise (K13, 57, Erkek) iyi bir veri bilimci olmak için hangi niteliklere sahip olmak gerektiği ve hangi uygulamayla hangi alanda analiz yapılabileceğine yönelik yorumunu şu şekilde ifade etmiştir:

> *"Bir istatistikçi olarak "data science" veri bilimlerinden aslında istatistik biliminin altındaki bir alanı temsil eder. Eğer bilgi teknolojileri alanında çalışıyorsanız ilk önce iyi bir istatistiksel veri analizi öğrenmeniz lazım veya istatistikçiyseniz de iyi veri analizi alt yapısına sahip olduktan sonra veri analizi araçlarını kullanmak lazım. Bu araçların başında da veri modellemede kullanılan R istatistiksel programlama diliyle Phyton gelir. Bunlara hâkim olduktan sonra zaten bu veriler artık veri tabanlarıyla bağlantı kurduğunuz için bir SQL bilgisine sahip olmanız, veri operasyonlarına hâkim olmanız için size fayda sağlayabilir. Büyük veriyle uğraşacaksanız yapısal olmayan veriyle de uğraşacağınız için en azından Hadoop gibi bilgilere temel anlamda sahip olmanız lazım e şimdi büyük veriden bahsedildiği zaman veriyi endekslemeye ihtiyaç var. Onun için de burada endeksleme araçları Galactex Search gibi araçlara ihtiyacınız var. Donanıma geldiğiniz zaman ise artık orda QRS tarzı büyük veriyi dengeleyecek, bunu esnek biçimde hareket ettirebilecek donanım araçlarına ihtiyacınız var. Ama bu tamamen bir takım çalışması. Eğer analitik bakımdan size "veri bilimi/data science" dan bahsediyorsak öncelikle iyi bir istatistiksel veri analizi, daha sonra istatistiksel veri analizi araçlarını iyi kullanmayı bileceksiniz."* (Katılımcı 7, 42, Erkek)

Bir diğer katılımcı ise bu programları kullanmanın yanı sıra, teknik bilginin bir noktaya kadar yetebileceğini ve "softskill" denilen şeyin, insanları dinleme, kurumları dinleme, onların hedeflerini amaçlarını anlama, verinin içerisinden de etkileşim kurarak, detaylara dikkat ederek sorunlar ya da sorular varsa çözümler çıkarabilmenin önemli olduğunu, analiz programlarının her zaman değişeceğini fakat bu softskillerin her zaman gerekli olacağını söylemektedir. Uzmanların karar verme mekanizmalarındaki rolü de bu noktada göze çarpmaktadır.

> "*Tabii ki bilgisayar programlama dillerini bilmek gerekiyor. Phyton, SAS bizim için özel toollardan birisi, SQL Server dediğimiz veri language olarak*

> *geçiyor ne işe yarar büyük veriniz vardır, bu kolonun ortalamasını almak istiyorum en rahat en hızlı diyeyim alabildiğiniz en hızlı dönüş yapan büyük veri SQL dilleri oluyor genelde. Bizde orada temel bir veri analizi yaparız orda softskill olarak ondan bahsedeyim. Problem çözme ya da analitik problem anlayışı sadece çözmesi de değil. Problemi anlamak. Onu anladıktan sonra elinize üç dört belli çözüm var onlardan birini modifiye ederek uygulayacaksınız. Esas sorun, problem neyi anlamaktan geçiyor. Bunun için de sizin iki tane softskille ihtiyacınız var. Business domain yani bu şirket ne yapıyor ya da kurum, bu ekip benden ne istiyor bunu anlamak ikincisi de analitik toolunuzun kapasitesini anlayarak ben bunları yapabilirim demek. Ben burada teknolojiden bağımsız olarak en popüler Phyton ve SQL ama bu iki yıl sonra değişir, 3 yıl sonra değişir ama bahsettiğim softskiller hep aynı kalacak."* (Katılımcı 16, 26, Erkek)

Gün geçtikçe dijitalleşen ve yapay zekayla desteklenen büyük veriyle kararların da makineler ya da sistemler tarafından alınacağı endişesi kavramsal çerçevede yeni karar verme kültürü, büyük veri kibri ve teorinin sonu kavramlarıyla ele alınmıştı. Bu noktaya kadar bir giriş olarak sadece veri bilimcilerin gözünden büyük verinin onlar için ne ifade ettiği, mesleklerinde neler yaptıkları, bu süreçte kendilerini geliştirmek için hangi programları öğrenmeyi hedefledikleri ve genel anlamda hangi programları ne amaçla kullandıklarına dair genel sonuçlardan bahsedilmiştir. Bu noktadan sonra ise bu karar mekanizmalarında "uzman" olarak kendilerini nerede konumlandırdıkları ve büyük verinin avantaj ve dezavantajlarına yönelik düşüncelerine geçiş yapılmaktadır.

4.1.2. Büyük Verinin Sunduğu Olanaklar ve Yarattığı Riskler

Büyük verinin, dijital sosyolojide sınıflandırıldığı gibi hem olumlu hem olumsuz pek çok toplumsal değişime yol açtığı bilinmektedir. Katılımcılara göre, büyük verinin avantajlarına bakıldığında, en temel özelliklerinden bir tanesi teknolojinin gelişimini desteklemesi ve günümüzde en önemlilerinden biri haline gelen yapay zekanın geliştirilmesinde temel unsur olarak yer almasıdır. Bu verilerin, özellikle bireyden alınan verilerin, kişisel verilerin oluşmasının temel sebebi de kavramsal çerçevede bahsedildiği gibi 4. Paradigmanın ortaya çıkmasıdır. 4. Paradigma, kullanıcı odaklı içerik üretiminin artmasıyla, özellikle sosyal medya platformlarının ortaya çıkmasıyla, her birinin farklı içeriklerle insanların farklı

alanlarda kendilerini temsil etmelerini, platformun özelliklerine göre kimliklerinin bir yönünü paylaşmalarını ve temel olarak haritalandırmaya imkân veren sitemlerin gelişmesini ifade etmektedir. Farklı platformların temsil ettiği durumdan bahsedilirken LinkedIn'de bireylerin meslek hayatlarındaki kişilere, şirketlere, insan kaynakları uzmanlarına, şirket yöneticilerine nasıl görünmek istediklerine göre şekillendirdikleri, kariyer hedeflerini yansıttıkları, genel olarak eğitimleri, iş tecrübeleri, deneyimleri ve becerileri üzerine veriler elde edilmektedir. Buna ek olarak bireylerin ilgili oldukları sektörler, firmalar, çalışma alanları da elde edilebilmektedir. Twitter'da bireylerin çeşitli olaylarla ilgili görüşleri ya da duygu durumlarına dair kendi yazdıkları yazılara erişilebilirken, Instagram'da genel olarak sosyal hayatlarına dair fotoğraflar, hikayeler, reelsler gibi verilerle sosyal medya kullanan bireylerin pek çok verisine ulaşılabilmektedir. Bu da büyük veriyi ve doğrudan yapay zekayı destekleyen bir unsurdur.

> *"Büyük veri çok heyecanlı bir konu. Avantaj olarak şu an teknolojinin gelişmesi en büyük sebeplerinden biri bu aslında. İnsanlardan toplanan veriler. Yapay zekâ geliştirilmesi için veri lazım bugün Facebook bilgileri sattı diye bugün Facebook'a bir ceza kesiliyor ama aslında onun sattığı net değil. Kuruluşlar aslında bir yapay zekâ çalışması yapıyorlar. Büyük verinin çalışması için insanlardan çok fazla veri toplanması gerekiyor. Adı üzerinde bugün evimizde çalışan robot süpürgenin bile daha önceden çok fazla train edilmesi gerekiyor. Bugün otonom giden bir aracın çok fazla train edilmesi gerekiyor. Bugün teknolojinin gelişmesi için big datanın çok beslenmesi gerekiyor ve veriye ihtiyaç var."* (Katılımcı 1, 29, Erkek)

Kişisel bilgilerin bu derece erişilebilir olmasının ve birer hammadde haline gelmesinin ise bazı katılımcılar tarafından tehlikeli ve bilgi güvenliği açısından sorun yaratacak bir şey olduğu belirtilmektedir. Büyük verinin ve onun desteklediği dijital gözetim sistemlerinin sosyolojik gelişimine bakıldığında 16. yüzyıldan itibaren ulus devletler, transatlantik köle ticareti, bürokratikleşme, rasyonelleşmeden sonra 19. ve 20. yüzyılda modern yönetim biçimleri özellikle 20. yüzyılda risk yönetim pratiklerinin temeline oturması, bireylerin verilerinin onlara karşı ya da onlar için kullanılabileceğinin tarihi sürecini yansıtırken, büyük verinin bir tür güç ve yönetim unsuru haline geldiğini de açıklamaktadır. Bir katılımcı bunu bireysel ve yönetimsel anlamda şu şekilde yorumlamaktadır:

> *"Benim açımdan baktığımda faydalı bir şey, avantajını söylersek çok büyük kitlelerden veri alarak insanların yönelimleri tahmin edilebilir. Ona göre daha istedikleri şeyler tahminlenebilir. Dezavantaj olarak da kitleler istedikleri gibi yönlendirilebilir."* (Katılımcı 8, 29, Kadın)

Büyük verinin iyi ve doğru amaçlarla kullanıldığında iyi şeylere hizmet edeceği, özellikle insanların belirli konularda tahmin yeteneklerinin artmasını sağlayacağı, şirketler için satış stratejilerinin düzenlenebileceği, ürünlerin doğru müşterilere ve doğru zamanlama ile ulaştırılabileceği, sağlık sektöründe gerekli kontroller ve daha hızlı çözüm önerileri elde etmeye yarayabileceği ve tüm bu bahsedilen durumların temelinde büyük verinin karar almayı kolaylaştırıcı bir şey olduğu düşüncesi yer almaktadır. Bazı katılımcılar büyük verinin bu avantajını şu şekilde ifade etmektedir:

> *"Kişilere sunduğu büyük bir avantaj olduğunu düşünmüyorum ama şirketlere sunduğu büyük avantajlar olduğunu düşünüyorum ya da devlet kurumlarına sunduğu ya da büyük önemli insanlara sunduğu avantajlar olduğunu düşünüyorum. O avantajlar da insanları daha rahat yönlendirme yapabilmek, insanların ihtiyaçlarını eğer doğru koşullar altında kullanırsak eğer; insanlara daha kolay ve çabuk yoldan ulaşmaları. Daha uygun bir fiyata ulaşmasını sağladıklarını düşünüyorum ama dezavantajları olarak da vermek istemediğimiz bilgileri bizi manipüle etmek için de kullanıyor olabilirler."* (Katılımcı 5, 26, Kadın)

> *"Kişiye özel, kişiye ilgi alanına özelleşmiş pazarlama alanı sunulabilir, satın alma davranışları değiştirebilir ama aynı şey dezavantaj olarak da kullanılabilir. Bir kişi gerçekten sürekli o da maruz kaldığı için almak zorunda kalabilir ya da bilgi güvenliği de ortaya çıkabilir. Her yerde parmak izimiz var şu an ya da dijital izlerimiz."* (Katılımcı 11, 33, Erkek)

> *"Günümüzde benim çalıştığım sektörlerin büyük çoğunluğunda operasyon maksimize edebilmek, daha verimli bir şekilde yürütebilmek, kullanıcı davranışını daha iyi algılayabilmek, bir de kullanıcı ya da bir müşteri olmasa bile belirli bir topluluğun davranışını nasıl hissettiğini nasıl davrandığını anlayabilmek. Mesela, bu olanaklar çok büyük bir olanak sağlıyor çünkü daha önce kullandığımız yöntem matematikten gelmiş biri olarak bence çok sınırlayıcı mesela burası orayı tamamlayan farklı bir bakış açısı getiriyor."* (Katılımcı 12, 43, Erkek)

Bir katılımcı, büyük verinin çok etkin bir manipülasyon aracı olduğunu ve bunun reklamcılık açısından kullanılmasının şirketler açısından da faydalı olduğunu ve kendisinin bu konuda hiç rahatsız olmadığını şu şekilde ifade etmektedir:

> *"Benim yönelimlerimi bilmesini tercih ederim. Benim alışkanlıklarımı biliyor mesela, bana o konuda reklam çıkarıyor. Mesela ben ayakkabıya bakıyorum kapatıyorum başka bir ayakkabı firmasından geliyor. Biz buna gerilla reklam deriz. Eskiden billboardlarda şöyle bir şey vardı. Mesela, Gordion'a gireceksin, Gordion'un tam kapısının önünde tam Cepa'nın billboardu vardı. Amacı şu mesela burada Gordion var ama buradan çıkınca bir de Cepa vardı, orada da güzel mağazalar vardı dedirtse yeter mesela ve bunu dedirtiyor. Buna gerilla pazarlaması deniyor. Örneğin, müşteri kırmızı ayakkabıya bakıp bizim ürünümüze bakıyorsa, o kırmızı ayakkabı onu takip ediyor. Kırmızı ayakkabının takip ettiğini bizde takip ediyoruz. Kırmızı ayakkabıyı gördükten sonra bizim yeşil ayakkabıyı da görmeye başlıyor. Çünkü bunu Google çok daha iyi bir yapıda, yıllardır yaptığı, sana sunuyor. Diyor ki bak diyor burada hedef kitlen burada şunları tıklıyor alıyor. Sen de bu kitleye ulaşmak ister misin diyor. Evet diyorsun sen de daha önce bunları tek tek çalışmış 1000'den 100 kişiye düşürmüş, gerçek hale getirmiş hazır veriler geliyor. Veriler görmüyoruz ama kullanıyoruz."* (Katılımcı 15, 55, Erkek)

Büyük veri, karar vermeyi kolaylaştırsa da katılımcıların belirttiği temel endişelerden bir tanesi ise literatürde bozulmuş veri olarak bahsedilen durumdur. Boellerstoff ve Levi Strauss'un kuramlarıyla literatürde yer bulan bu duruma bakıldığında, verinin toplanıp işlendikten sonra başka bir hale gelmesi ve bu halinin çeşitli sebeplerle bozulmuş (yanlış) olabileceğini belirtmektedir. Bunun ifade ettiği şey büyük veri toplanırken bireylerin tam olarak istemli ya da istemsiz olarak verilerini paylaşmasına ek olarak, bireylerin bu konuda ne kadar bilinçli olduklarının belli olmaması, teknik konularda ve işlemleme ile ilgili bilgili olmamaları olabileceği gibi, ne kadar bilinçli olsalar da çeşitli şekillerde veri ihlaline, bilgi güvenliği sorunlarına ve manipülasyona maruz kalabilecekleridir. Birey, bu noktada, bozulmuş veride kendi verisi üzerinde onunla ne yapıldığına dair kontrolünü kaybetmekte ve bu durum bireyleri dezavantajlı konuma düşürebilmektedir. Bir katılımcı bu durumu ifade ederken bu şekilde elde edilen verilerin ileride kendisi ya da diğer bireyler için sorun yaratabileceği, insan hakları ve özgürlükleri anlamında endişesi olduğunu işaret etmektedir:

> *"Çok fazla kişisel bilgi var bu bilginin nerelere gittiği öncesinde gözükmüyor hiçbirimiz bilmiyoruz. Metinleri onaylıyoruz vs. ama bilgiler nereye paylaşılıyor belli değil. Hiçbir bilgimiz yok, bu herhangi bir noktada istenmeyen bir şey okudum ya da ileride bir gün bir işe girmek istedik ya da yurtdışına çıkmak istedik; girdiğimiz siteler tıkladığımız linkler okuduğumuz makaleler vs. bir noktada önümüze çıkartılıp sen zamanında bunu*

> *yapmışsın bu bizim için uygun değil diye önümüze sunulabilir."* (Katılımcı 4, 26, Kadın)

Kişisel verilerin işlenerek bireylerin önüne sunulmasının literatürde en yankı bulan örneklerinden ve temel tartışma kavramlarından bir tanesi olan unutulma hakkı da bu noktada önemlidir. Unutulma hakkıyla bireylerin kendileriyle ilgili internette yer alan verilerinin onların hayatlarını ciddi bir şekilde etkileyebileceği, bununla ilgili uluslararası olarak da davaların açılmakta olduğu ve bu konunun büyük veriler arttıkça, boyutu değiştikçe daha çok gündeme geleceği ifade edilmektedir. Bu kadar verinin özellikle kişisel verilerin, pratiklerin, konumların, alışkanlıkların takip edilmesi bireylerin birey olarak yaptığı hataların kalıcı olmasını, diğerlerinin buna ulaşımını kolaylaştırmayı sağlamaktadır.

Bozulmuş verinin yeni karar verme kültüründe yıkıcı bir güç olarak yer almasının sonuçlarına bakıldığında diğer bölümlerde de bahsedileceği gibi panoptik bir sınıflandırmaya (bireyleri dijital gözetim sistemleri ile elde edilen verilerine göre sınıflandırma ve çeşitli yaptırımlar uygulama) yol açmasının yanı sıra bu verilerin kimler tarafından, ne kadar güvenli şekilde, doğru şekilde işlendiği, işleyen kişilerin yetkinliklerinin ne kadar iyi olduğu ve analizlerin ne kadar doğru şekilde yapıldığı, bu işlemleme için hem entelektüel anlamda hem ekonomik anlamda ciddi bir yatırıma ihtiyaç duyulduğundan da bahsedilmektedir.

> *"Avantaj olarak tabi sonuçta karar almayı kolaylaştıran bir şey doğru karar almak için. Geleceğe yönelik bir takım karar almayı kolaylaştırıyor. Dezavantajlarına girince çok büyük ve fazla bunu anlamlı hale getirmek hiç kolay değil, ciddi bir alt yapı istiyor, ciddi bir know how istiyor, yani entelektüel bir yatırım istiyor onu da dezavantajı olarak söyleyebilirim."* (Katılımcı 7, 42, Erkek)

Panoptik sınıflandırma, büyük verinin ve dijital gözetim sistemlerinin ayrıştırıcı bir güç haline gelebileceğinden bahsederken burada bir tür güç tekelleşmesinin olabileceği, bu sınıflandırmayı yapan kurumların da verileri tamamen kendi çıkarları doğrultusunda kullanabileceğine vurgu yapmaktadır. Literatürde bunlar ayrımcılık, güvenlik ihlali, anonimliğe veda, devlete verilen geniş yetkiler,

düzenlenmemiş bilgi işlem şeklinde yer alırken; bir katılımcı "gücün tekelleşmesini" özellikle kullanıcı odaklı içerik ve kişisel verilerin en çok elde edildiği yerlerden olan sosyal medyadaki durumu şu şekilde özetlemektedir:

> *"Sınıflandırma yapılabilir, zaten yapıldığı da biliniyor. Geçenlerde biliyorsunuz konuştuk Rusya, Amerika'nın seçimlerine müdahale etti mi haberleri çıktı. Neden olmasın tam bilmiyorum içeriğini ama manipülatif yapılara sebebiyet verilebilir zaten istatistik böyle bir şey. Yani istatistikte hipotezi doğru kurmanız lazım, yaklaşımı doğru belirlemeniz lazım. Büyük veri bunu kurmakta ve manipüle etmekte çok daha rahat. Yine şu an büyük verinin tekelleşmesi bunun yanı sıra her şeyin tekelleşmesi sıkıntı. Twitter tekelleşti mesela, her gün Elon Musk ne istiyorsa onu yapıyor. Ya da WhatsApp, Instagram, Facebook bunların hepsi Mark Zuckerberg'de. Bir tekel ve ne isterse aslında onu oluşturabilecek seviyede onu oluşturabilecek insanları manipüle edebilecek düzeyde. Bütün veri de onun elinde. WhatsApp'tan kaçsanız Instagram'dan kaçamazsınız Instagram'dan kaçsanız Facebook'tan kaçamazsınız. O büyük veriyle size ne istediğinizi önünüze koyuyor veya ne istemediğinizi önünüzden çekiyor. İnsanlar bu sefer farklı düşünceler düşünmeye başlıyor. Bunu siyasi seçimlerde de gördük. Herkes kendi düşüncesinden insanın görüşünü gördüğü için hem mutlu oluyor hem de rahat ediyor. Kazanan taraf için de kaybeden taraf için de bu böyle. İkisi de kaybetti çünkü ikisi de kazanacağını düşünüyordu. Görüşünü görüyordu. Bunu nasıl sağlıyorsun? Büyük veriyle bunlar da tehlikeli noktalar yani."* (Katılımcı 14, 26, Erkek)

> *"Belli şeylerin çıkarımını yapmak daha kolay oluyor. Seçim de yaklaşıyor. Seçim öncesinde de insanları tahmin edebiliyor olmak tabii ki bunu tahmin edebilen kişilere ekstra güç ve güvenilebilirlik kazandırıyor."* (Katılımcı 3, 30, Erkek)

Burada gücün tekelleşmesinin yanı sıra ilerleyen kısımlarda katılımcıların defalarca vurgu yapacağı yankı odası meselesi de büyük verinin dezavantajlarından bir tanesi olarak karşımıza çıkmaktadır. Yankı odası, bireylerden toplanan verilerle, algoritmalar sayesinde sadece kendi düşüncelerinde olan insanların düşüncelerini ve seslerini duymasına sebep olduğu ve bir süre sonra herkesin kendini haklı, doğru ya da herkesi kendisi gibi sandığı bir düzen kurmaya sebebiyet verebilmektedir.

Bir katılımcı ise büyük verinin karar verme kültüründeki rolünü bireysel sosyal ilişkilerde de kullanılabileceğini ve bunu kendisi için bir avantaj olarak gördüğünü ifade etmektedir. Fakat büyük verinin ya da bireyler hakkında elde edilmeye müsait hale gelen bu verilerin insan ilişkileri açısından bu derece elde

edilebilir hale gelmesi onları daha önyargılı mı ya da daha güvende ve objektif mi yapar sorusu endişe yaratmaktadır. Katılımcı için büyük veri, yalan söylemeye yatkın olan insanın yalanlarını tespit etme ve daha objektif bir bakış sunmaya yarayan bir araçtır.

> *"Çünkü insanoğlu bence yalan söylemeye ve olduğundan farklı görünmeye çalışan bir yapıda. İnsanlar tanımadığı kişilere karşı özellikle olduğundan farklı gözüküyor. Büyük veride bunu yapamazsınız. Ben şu an tüm şeceremi döktüğümde size tüm programları, hangi programı ne kadar süre kullandım, mesela 10 bin saat uzmanlık için en az gerekli süre bir uğraşta bu tabi doğrudur değildir oraya girmiyorum varsayalım doğru olsun ben uzmanım deyince ben en kötü bu programda kaç saatte geçirmişim diye bakıp bin saat geçirdiğimi görüp yeteri kadar uzman olmadığımı söyleyebiliriz. Bu da işte aslında büyük veri sayesinde. Bunu kitlelere uyguladığımızda, o veriler büyük veri olmuş olacak insanların yarattığı o biased algıdan kurtulup bir nevi objektif bir bakış açısı sunuyor büyük veri."* (Katılımcı 16, 26, Erkek)

Tüm bu tartışmalara ek olarak, büyük verinin sosyal fayda için kullanılabilecek bir şey olduğu aşikardır. Katılımcılar bu alanda uzmanlaşmış bireyler olarak dezavantajlara vurgu yaparken, sosyal fayda için büyük veri kullanımının da göz ardı edilmemesi gerektiğini söylemektedir. Sosyal fayda olarak büyük veriden kasıt, iklim değişikliği gibi konularda bu verilerden faydalanılmasına ek olarak, sosyolojik olarak da gelir eşitsizliği, toplumsal cinsiyet eşitsizliği gibi durumlarda bu verilerden faydalanabileceğine vurgu yapılmaktadır. Ama burada da yine bu veriye erişebilme, işleyebilme ve bunun için gerekli yatırımların yapılmasının öneminden bahsedilmektedir. Bunları yapabilen ülkeler ve kurumlarla yapamayanlar arasında da ciddi bir güç dengesizliği olacağı, gelecekte büyük verinin gelişmişlikle, ülkelerin ve firmaların güçleriyle bugün olmaya başladığı gibi çok daha büyük bir eşitsizlik unsuru haline geleceği düşünülmektedir. Ülkelerin, kurumların ya da bireylerin daha dezavantajlı konuma gelmeleri bu sistemlerle daha ciddi bir hale gelmektedir çünkü dijital eşitsizlik dediğimiz kavramla, güç dengeleri hiç olmadığı bir şekilde eşitsiz hale bürünmeye başlamaktadır. Bu eşitsizliğin büyük veriyle daha da derinleşmesinin sebebi, dijital eşitsizlikle de bağlantılandırılarak bu araştırmada bahsedilen Büyük Veri Ayrımıdır. Bu dijital eşitsizlik türünde ciddi bir sermaye aracına dönüşen büyük

veriye sahip olan ve onu bilinçli kullananlar ve sahip olmayan ve kullanamayanlar arasında ciddi bir eşitsizlik oluşacağından bahsedilmektedir.

> *"Bize çok farklı seçenek sunuyor bugün Cern'de günde inanılmaz fazla veri üretiliyor bunun şimdi sayısı aklımda değil ama o yüzden ne söylesem yalan olacak. O veriyi ellerinde tutamayıp bir kısmını çöpe atmak zorunda kalıyorlar. Silmek zorunda kalıyorlar öyle büyük veriler ortaya çıkıyor. E şimdi Cern'de böyle büyük araştırma yaptığınızda bu büyük verinin herhangi bir tanesi dünyanın oluşumuna katkıda bulunacak bilimsel bir araştırmaya destek sağlayabilir. Ya da uzayla ilgili bir araştırmanıza. Dünyanın herhangi bir noktasındaki iklim değişikliğiyle ilgili bir araştırmanıza. Büyük veriyi görüyoruz o büyük veri sayesinde sosyolojik anlamda da çok fazla araştırmalar yapılıyor. Gelir eşitsizliği, kadın erkek eşitsizliği bunları hesaplayabiliyorsunuz bunlara yönelik sınıfsal farklılıkları hesaplayabiliyorsunuz işte orta sınıfların çöktüğünü, zengin ve fakirlerin oluştuğunu bunları hep büyük veriyle saptayabiliyorsunuz. Dezavantajları güvenlik büyük ihtimalle. Bir güvenlik çünkü sürekli verimiz alınıyor ve buna engel olamıyoruz. Çok ciddi kanunlar ve kurallar gerekiyor belki de bunun için. İkincisi de büyük veriyi tutamıyoruz hala. Bunu tutabilme kabiliyetimiz yok, bu da bizim için sıkıntılı süreçler. Gerekli bilgileri kaçırabiliyor olabiliriz yani."* (Katılımcı 14, 26, Erkek)

Bahsedilen avantajlar ve dezavantajlarla bağlantılı olarak katılımcıların özellikle büyük verinin, yapay zekanın temeli olarak işlevine vurgu yaptıkları, ChatGPT örneklemeleriyle bu sistemlerin bireylerin mesleklerinde ya da çeşitli konularda işlerini kolaylaştırdıklarını belirtmeleri fakat diğer yandan da çeşitli mesleklerin kaybolmasına, bazı insanların işsiz kalmasına yönelik korkuları olduğuna dair görüşleri paylaştıkları da görülmektedir.

> *"Yapay zekanın büyük veriyi bu kadar kullanarak çalışması, ilerleyen süreçte işsizlik konusunda ciddi bir sıkıntı yaratacağa benziyor."* (Katılımcı 15, 55, Erkek)

> *"Büyük veri ve yapay zekayı birbirinden ayıramayız. Bu bizim hayatımızda iç içe girmiş durumda. İnsanlarda genelde şey korkusu oluyor, özellikle ChatGPT'nin çıkmasıyla beraber işimi elimden alacak falan durumları oluyor. Hatta bir katıldığım seminerde oyun senaryosu yazma gibi bir durum varmış mesela, ChatGPT'ye bunu bile yazdırıyorlar. Tamamen özgün bir senaryo bir oyun senaryosu veriyor hatta isimleri veriyorsunuz, Melis, Eren, Gül var diyorsunuz şu şunda iyi diyorsunuz üçünüze uygun bir dört haftalık programla size onu yazdırıyor kodunu falan. Böyle bir şey var ama burada da işimizi elinden almak durumundan ziyade onu nasıl kullanacağını bilmek önemli hale geliyor. Ona doğru soruları sorabilmek doğru problemler yöneltmek oluyor. Biraz da işin teknik ve işçilik kısmından ziyade, artık o veriyi ya da bilgiyi yönetebilmeye doğru yöneldiğini*

> *düşünüyorum. İnsanlar artık o veriyi tek tek nasıl işleyeceğim böyle mi yapayımdan ziyade benim problem bu, böyle bir şeye vardırmak istiyorum bunu bu veriyi bu yolda nasıl kullanabilirim, böyle kullanırım onun kodunu yazayım o zamana dönüyor. Dezavantaj olarak sektörde 10 kişiye ihtiyaç varsa 5'e düşecektir böyle bir dezavantaj yaratabilir belki. Orada da herkes o dönüşümün içinde kendi nasıl yer edecek ona bağlı biraz da. Belki buna bağlı alt alanlar da açılacaktır belki ondan 5'e düşecek ama o 5 kişi başka bir işe yönelecek olabilir. O yüzden yani tek dezavantajı bu olabilir ama onun da çok şey olacağını düşünmüyorum herkes dönüşümde kendine bir yer bulabilir."* (Katılımcı 2, 28, Kadın)

Herkesin dönüşümde kendine bir yer bulabileceğine ve yapay zekanın, ChatGPT'nin belirli meslek alanlarının yerini alırken bir yandan da yenilerini açacağını belirten katılımcıya ek olarak, başka bir katılımcı ironik bir şekilde ChatGPT'nin eskiden bireylerin saatlerce yaptıkları işleri artık dakikalar içinde yaptığını ve bunun kolaylık olduğunu, yakın zamanda da bunun çok büyük bir sorun yaratmayacağını söylemektedir.

> *"Beklentileri, maddeleri çok kolay bir şekilde çekiyor. Bunu Google'dan saatlerce araştırabilirsiniz. Ama ChatGPT zaten bunu yapıyor. 2021'e kadar toplanmış olan bütün bilgilerden sana en iyi bilgiyi sunmaya çalışıyor. Dolayısıyla gündelik hayatımıza çok büyük yenilikler getireceği görünmekle birlikte ileriki zamanlarda işte internette kendi aralarında entegre olup, işte kendi aralarında koloni oluşturup, bunu daha sonra insanlar dünya hayatı için tehlikeli bir varlıktır deyip özellikle bizim hayatımız için tehlikeli bir varlıktır diye bir entegrasyon kurup bizi yok etmeyi düşünmeyeceklerini de düşünmüyorum ama bu uzun sürecektir (güldü)."* (Katılımcı 10, 37, Erkek)

Veri bilimcilerin gözünden, büyük verinin ve yeni gözetim pratiklerinin avantaj ve dezavantajlarından bu bölümde detaylı bir şekilde bahsedilirken, temel olarak avantajların da dezavantajların da onların karar verme kültüründe yeri olduğu görülmektedir. Bu sebeple yeni karar verme kültüründe büyük verinin yeri bir sonraki kısımda açıklanmaya çalışılmaktadır.

4.1.3. Yeni Karar Verme Kültüründe Büyük Veri, Büyük Veri Kibri ve Büyük Veri Ayrımı

Büyük verinin, dijital gözetim sistemlerini kullanarak oluşturduğu yeni karar verme kültürünün temel olarak değiştirdiği şey, artık sadece suçlu bireylerin

değil, bireysel gözetimin değil, kitlesel gözetimin yaygınlaşmasıdır. Fiziksel teknolojilerle değil, yapay zekâ destekli sistemlerle, yüz tanıma teknolojileriyle ve daha farklı sistemlerle gerçekleştirilen gözetimler ve metaverilerin veri tümleştirmesiyle dijital veri bilgi ekonomisi oluşmuş, dijital verinin ticari, araştırma, yönetimsel değeri hiç olmadığı kadar artmıştır. Dijital gözetim sistemlerindeki temel dönüşümde bedenlerin de dijital bedenlere dönüştüğü, biyometrik verilerin de sınıflandırma sistemlerinde kullanılır hale geldiği, hatta bunların ırksallaştırılmış bir güç haline geldiği bilinmektedir. Araştırmada katılımcılara bu durumlar göz önünde bulundurularak yeni karar verme mekanizmalarındaki süreçlerdeki durum sorulmuş, verilen kararların ne kadarının uzmanların kararına bırakıldığına, buradan elde edilen kararların ne kadar etkili ve doğru olduğuna nasıl karar verildiğine, bunun toplumsal açıdan ne kadar faydalı ya da tehlikeli olduğuna yönelik düşüncelerini öğrenmek adına sorular yöneltilmiştir.

> *"Bunu genelde insanların, istihbarat birimleri sosyal medya hesaplarına bakarak yapıyor. İnsanların telefon sinyallerine bakıyor, kimlerle görüştüğü, kimlerle etkileşime girdiği, sosyal medyaya attığı fotoğraflardan nasıl bir insan figürü çizdiğini ortaya çıkarıyorlar. Aslında bunu büyük veri olarak değil de bireysel şahıs bazında yapıyorlar. Baktığımız zaman evet büyük veri insanların verilerini toplayıp çalışmak, başarılı, işinin peşine düşen, umursamaz, güvenlik kurallarını ihlal eden gibi çıkarımlarda bulunabiliyorlar."* (Katılımcı 1, 29, Erkek)

Katılımcılardan bir tanesi bu sistemlere şu an tamamen güvenemeyeceğimizi, fakat bunun çok ciddi bir güç olduğunu ve eğer yanlış şekilde değerlendirilirse çok ciddi güvenlik ihlallerine sebep olabileceğini ifade etmektedir. Başka bir katılımcı da (Katılımcı 9, 35, Kadın) bunun şu an o kadar etkili olmadığını ve gelecekte özellikle politikalar temelinde çok daha etkili olacağını belirtmektedir. Diğer bir katılımcı (Katılımcı 4, 26, Kadın), tamamen bu verilere dayanarak bireylerin aldığı kararları oluşturduklarını belirtmektedir. Katılımcıların genel olarak orta noktada buluştuğu nokta ise kanunların buna göre düzenlenmesi ve etik kısmının düşünülmesi gerektiğidir.

> *"Bize aslında bazen yanlış sonuçlar da verebiliyor bu sistemler illa bir doğru cevabı vermiyor tarihsel bir olayı verdiğiniz zaman çok başka bir şey de diyebiliyor. Buna yüzde yüz güvenmemiz gibi bir durumda ilerde mümkün ama şu anda söz konusu olduğunu düşünmüyorum. Şu an güvenebileceğimiz bir noktada değil. Ama bu gücü elinde tutmak, yani bir kurum ya da kişinin elinde tutması, çok fazla ihlallere sebep olabilecek bir şey olabilir, güvenlik ihlallerine. Burada da bunun kanunlarla, bunun etik kısmıyla ilgilenen kısmına bakmak detaylandırmak gerekiyor."* (Katılımcı 2, 28, Kadın)

> *"İnsanların yönettiğini düşünmüyorum açıkçası tabii verinin kullanımına izin veren insanlar şirketlerin, büyük insanların ya da devletlerin elinde olduğunu düşünüyorum yönettiğini düşünüyorum. Çünkü benim belki de sana şu an cinsiyetim, eğitim durumumu vermem masumane olabilir ama ülkelere verdiğimde bunu kötü niyetle kullanabilirler."* (Katılımcı 5, 26, Kadın)

> *"Belirli bir skorun altındaki müşteriye kredi vermez bankalar, ev kredisi alabilmek için Findeks storunuzun çok yüksek olması lazım ve bu veriden hesaplanıyor. Yani karar verme mekanizmalarında çok etkili."* (Katılımcı 6, 36, Kadın)

Teorinin sonu tartışmalarında bu kararların doğrudan son kararı etkilemesinin insan zekâsı, sağduyusu, vicdanı gibi duygusal öğelerin bir kenara bırakılıp çeşitli konularda sorunlu sonuçlara yol açabileceği ve yerleşik ve uzamsal-zamansal olarak ırk kavramına, toplumsal cinsiyet eşitsizliği kavramına yönelik eşitsiz kategorizasyonlar yapabileceğiyle alakalıdır. Bir katılımcı, toplumsal eşitsizliklerin bu sistemlere nasıl aktarıldığını çok net bir şekilde ifade etmektedir:

> *"Sadece büyük veri analizinde değil, bu yanlılık hikayesi öğrenme tarafının hepsinde var, küçük veriden öğrensen de var. Teknik anlamda kullandığım büyük veri klasmanına girmeyen yerlerde de tahmin sınıflandırma problemleri çalışıyorsan bunların hepsi doğal olarak var. Buradaki sistemler insan öğrenmesini taklit ediyorlar ve siz ne öğretirseniz onu öğreniyorlar. Nereden veriyi alıyorsa o verideki doğal olarak örüntüleri ilişkileri belirli bir miktar öğrenmeye çalışıyor. İnsan kadar zeki olmasa da verinin içerisinde insan gibi, insanın geldiği kültürel coğrafya bizi nasıl etkiliyorsa, biz neyle besleniyorsak ona bağlı olarak bir karakter kararlar alıyorsak veri tarafındaki süreçler de öyle ve çok genel karmaşık büyük veri setleriyle çalıştığımız için insanoğlunun o verilerin içerisindeki yanlılığı görme ihtimali çok yok. Ama sonuçlar üzerinde interaktif çalışarak ben bir sonuç elde ettim bunda bir yanlılık var mı teknik yöntemlerle bunlara bakmak mümkün. Sonuçta veriyi biz üretiyoruz, toplumlar üretiyor. Kendi zihnimdeki ya da ürettiği yanlılıklar, beğendikleri, ayrımcılıkla benzeşiyorlar. (Katılımcı 12, 43, Erkek)*

Başka bir katılımcı ise bu yanlılığın temel sebebinin örneklemin doğru alınamayacağı ve bu durumun da yanlış sonuçlara yol açabileceği şeklinde ifade etmektedir.

> *"Örneklemlerin doğru seçilmesi için her kesimden, her yerden veri alınması gerekiyor bu da çok maliyetli bir iş olduğu için genelde kolay ulaşılabilecek yerlerden veri oluyor bu da yanlışlamaya gidiyor. Bu seçim sonuçlarında şey dendi büyük şehirlerdeki merkezlerde veriler toplandığı için kırsala inmediği anket şirketleri hepsi yanlış sapmalı olarak yanlış tahminde bulundular. Bunlar da çok büyük sıkıntı oldu mesela örneklemlerin düzgün alınması için o popülasyonu tamamıyla yüzde 95 güven düzeyinde temsil ediyor olması lazım. Bunun dışında biraz yayılmak lazım veri toplamada. Örneklemin doğru seçilmesi çok önemli."* (Katılımcı 8, 29, Kadın)

Katılımcılardan bazıları, son kararın yine uzmanların elinde olduğunu söylemektedir. Fakat yine de uzmanlardan bu verileri hangi kurumun nasıl, ne amaçla talep ettiği ve bu sonuçların nasıl kullanılıp nasıl yansıtılacağının onların elinde olduğunu bilmek önem taşımaktadır.

> *"Buradaki son kararı verebilecek mercii bilgisayar değildir. Uzman onların hepsini değerlendirir, denetler, şu ihtimal dahilinde elde edilen bu sonuçların geçerli olduğunu ve burada bir olağan dışılık olduğunu düşünüyorum der. Bir uzmanın tek başına bilgisayarla birlikte oturup karar verebileceği bir yapı değildir. Daha çoklu organize hareket edilir ama kişinin şeylerini kolaylaştırır mesela yurt dışında belki birazdan detaylarını da soracaksındır hukukçular artık ilk adımdaki şeylere bakmıyorlar kararları yapay zekalı bilgisayarlar veriyor çünkü çok net kararlar var. Kişiler şu tarihte boşanacak, bu tarihte evlendiler, evlenmeden önce şöyle gelirleri vardı şunlara sahiplerdi. Evlendikleri dönemde de şu varlıkları oldu. Boşandıklarında da mal paylaşımını yüzde 50 50 anlaştılar bunların mal paylaşımını yapın sistem bunu zaten yapar. Ama birileri birinin üstüne ev geçirmiştir, birileri bir şey olmuştur, o birinci adımda sistemin çözemeyeceklerine hala her ne kadar öneri verseler de bir hâkim bir savcı bir avukat tartışarak karar veriyorlar. O karara itiraz hakları da var. Bilgisayar bir şey dediği zaman nasıl itiraz edeceksin."* (Katılımcı 10, 37, Erkek)

> *"Gelişmiş noktada büyük veriye dayalıdır. Primitive ya da daha başlangıçta senin bir hipotezin olması. Senin demen lazım ki ben şunu assume ediyorum bence böyledir ve o veriyi kurman lazım. Modelin sonucundaki matrisleri toplaman lazım. Her şeyin modeline uygun metricleri var. Evet ben çok güzel bir model kurdum diyorsun. Verilerim de bunlardı. Tekrar gerçek verilerimle de uyguladım diyorsun. Bu en primitive, işe başlarken matematiksel modeli kurduğundandır ama bu ne kadar işte şeylerden besleniyorsa online sitelerden, e ticaret sitelerinden her seferinde data baseden bilgi çekip üç saat gel git hah çalışmış çalışmış, hah bunlarda*

> *paremetre değiştireyim demek iyi bir şey değil. Bu yolun başı büyük veriden kaynaklı verilen kararlar en gelişmiş AI (yapay zekâ) ya da data science ürünüdür yani."* (Katılımcı 11, 33, Erkek)

> *"Olabilir ve var zaten şirketler bu yüzden kullanıyor zaten. Bir veriden bir bilgi üreteceksen o bilgi de bir karara dayalı olmalı, öbür türlüsü akademik bir çaba olabilir ama bir karara dönüşmeyen bir süreç endüstride sahada çok kullanılan bir şey değil. O yüzden büyük verinin kullanımları buradan çıkarımlar üzerinden ıraksıyor. Farklı bilgi üretme yöntemlerimiz var. Mesela, bunların hepsini bir araya getirerek bir karar vermek de mümkün. Zaten bir karar alıyorsanız işte kendi operasyonunuza dair, şirketinize dair, kurumunuza dair, orada karar vericinin her zaman bir rolü var. Ama tek başına karar vermek için yeterli değildir."* (Katılımcı 12, 43, Erkek)

Bazı katılımcılar ise yeni karar verme kültüründeki olası durumun çok tehlikeli olduğunu ve otomasyona dayalı olursa farklı alanlarda karardan vazgeçildikten sonra geri alamama, bu kararlarda duygu ve ruhun olmaması, uzmanların yeterli donanımı bulunmaması gibi farklı tehlikeler yaratacağı ve bu verileri yanlış kullanarak yanlış çıktılara ulaşılabileceği doğrultusunda değerlendirmektedir.

> *"Amerika geçen günler de üç beş gün oldu fazla olmadı yapay zekalı bir robotunu denedi askerini git şu yeri yok et dedi. Son dakikada operasyonu iptal ettiler. Orayı yok etmek için operasyonu engellemeye çalışan komutanı öldürdü ve orayı yok etti. Denemelerinde böyle bir şey olduğu ile ilgili bir makale çıktı şimdi. Bir şeyi yap dedikten sonra onu yapmayı engelleyecek şey de... belki şöyle düşünüyor beni engellemeye çalışan bir düşman diye düşündü belki de gitti öldürdü yani. Çünkü yapay zekanın subjektif duygularla hareket edebilecek bir mekanizması şu an yok. Ona ruhu veremiyorsunuz. Ona belli kararları optimize edebileceği şekilde hak veriyorsunuz. Emir verdiğiniz zaman yaptı orayı vurmak iyi bir fikir değildir diyen kuleyi de vurdu. Yani öyle şeyler oluyor biz bunların şimdi detaylarına çok hâkim değiliz." (*Katılımcı 10, 37, Erkek)

Katılımcı 10'un bahsettiği şekilde durum sadece yanlış kararlar alınması değil, alınan kararların bazen uzmanlar tarafından bile geri döndürülemez bir hal alabileceğinin ve bunların çok tehlikeli boyutlara ulaşabileceğinin önemli bir kanıtıdır. Diğer bir sorun ise bu tür sistemlerin sonucundaki karar vericilerin bazı durumlarda uzmanlar olmaması ve uzmanların fikirlerini dinlemeden hedefe yönelik kararlar verebilmeleridir. Katılımcılardan bir tanesi (Katılımcı 16, 26, Erkek) *"Eğitimsiz kitle siz ona ne verirseniz verin eğitimsiz çıktı üretecektir. Biz proje yaptığımız zaman raporun en sonunda karar vericiler diye bir kelimemiz*

var. Sizin bahsettiğiniz bu karar veren kişiler karar vericiler oluyor. Onların uygun şekilde şu şu yapmasını tavsiye ederiz diyoruz. Ama o şekilde yapılmıyor yüzde 90" şeklinde ifade etmektedir. Diğer bir katılımcı da bu anlamda yapay zekanın bulut sistemine girdiğinde ne gibi durumlara yol açabileceğiyle ilgili endişesini şu şekilde ifade etmektedir.

> *"Yapay zekâ kendini bir bulut sistemine kopyalamayı akıl ederse yakında. Şu anda IPhone'un bir açığını tespit etmiş mesela. Bu hackerlar kod yazmaya başlamış mesela. Yapay zekâ durduk yere bir yeri hackleyip, kendisine hesap açsa bankadan ondan sonra da kendisine bir hosting alsa oraya da kendisini yedeklese zaten bu filmlerde seyrettiğimiz bir şeye dönüşecek. Çalıştaylar da yapay zekaların verdiği ortak bir cevap 'Biz dünyayı sizden daha iyi yönetiriz'. Onun için yanlış hatırlamıyorsam ChatGPT 2022 verilerine erişmesini izin vermediler durdurdular yani. Yani 2021'e kadar verilmişti şimdi 2022 verilerine yeni izin verildi. Anormal bir veri toplayıp analiz edip geri döndürmesi çok hızlı."* (Katılımcı 15, 55, Erkek)

Büyük veri kibri, bu anlamda çok daha ciddi bir sosyolojik tartışma haline gelmektedir. Uzmanlar, veri bilimciler, çeşitli alanlarda uygulamalar yapıp çözüm önerileri geliştirse de karar vericilerin genellikle gücü elinde bulunduran ve son kararı veren kişiler ya da kurumlar olması, bu sistemlerin nasıl ve ne amaçla kullanılacağının yönünü tamamen değiştirmektedir. Büyük veri bir güç olarak bir kontrol mekanizması haline gelebileceği gibi, bu uygulamalar gerçekleştirilirken Kişisel Verileri Koruma Kanunu (KVKK) önemli yasal uygulamaların ne kadar dikkate alındığı ya da alınmasının tercih edilmediği noktasında önem taşımaktadır. Bu sebeple karar verme mekanizmalarıyla ilgili sorulardan sonra, katılımcılara KVKK ile ilgili sorular yöneltilmiştir.

Katılımcıların veri koruma kanunları ve yasal düzenlemeler büyük veriler alanında yeterli midir sorusuna verdikleri cevaplara bakıldığında; öncelikle Türkiye'de KVKK ile ilgili düzenlemelerde veri bilimcilerin daha aktif rolde olmalarının, bu düzenlemelerde daha etkin sonuçlar alınmasını sağlayacağını düşündükleri görülmektedir. Ama bundan önce kişisel verilerin tam olarak ne ifade ettiğinin tanımlanmasının önemi vurgulanmaktadır. Bu durum dijitalleşmeyle birlikte kamusal alanla özel alanın sınırlarının bulanıklaşmasının getirdiği temel sorunlardan bir tanesi olarak görülebilir.

> *"Şimdi bizde şöyle bir sıkıntı var. Bizde maalesef Kişisel Verileri Koruma Kanunu'nu hukukçular tarafından yönetiliyor ve yürütülüyor. Halbuki buradaki kişisel veriyle ilgili anonimleştirme ve benzeri durumların kullanımıyla ilgili tedbirler almak çok teknik bir konu. Ama bir şekilde o verilerin nasıl işlenip, nasıl saklanacağı ve nasıl anonimleştirileceği, nasıl kullanılabilir hale getirebileceği aslında istatistikçilerin işi. Burada özeleştiri yapmak lazım. Bu konuyu hukukçulara kaptırdılar. Şu anda doğru ilerlemiyor. GDPR (General Data Protection Regulation- Genel Veri Koruma Güzenlemesi) Avrupa'nın kişisel verileri koruma ile ilgili aldığı tedbirler, Türkiye'deki tedbirlere göre çok daha ağır aslında. Fakat uygulama açısından baktığımızda şu anda biz kişiye ait olan, kişiyi tanımlamayacak olan tüm verileri kişisel veri olarak algıladığımız için bu yalnızca kamuda değil ayrıca özel sektörde de çok ciddi sıkıntı yaşanabiliyor. Verilerin hiçbiri kullanılamıyor. Kafalar kişisel verilerin ne olduğuyla ilgili çok net ve açık değil. Bunun yanı sıra öte yandan da bizim bir şekilde yapacağımız bir iş veya işlem için bizim kişisel verilerimizi kullanma izni alan firmalarla bizim kişisel verilerimiz anlamında işleme. Kişisel veriyi tutan işletmelerin hassasiyeti bu konuda çok önemli. Verilerin toplu halde, mesela MHRS (Merkezi Hekim Randevu Sistemi) verilerinin alınması. Türkiye'deki kişisel verilerin, sosyal medya verilerinin bazı büyük firmalar tarafından fütursuzca kullanıldığı biliyoruz."* (Katılımcı 13, 57, Erkek)

Başka bir katılımcı da dijitalleşme sürecinin hızlı ilerlediğinden ve bu duruma uygun yasal ya da teknik zeminin oluşturulamadığından bahsetmektedir:

> *"Bence şöyle, veri önden gitti kanunlar sonradan gitti. Bu konuda büyük bir açık var yani zamanında kullanırken nasıl ve neden, kullanıcı sözleşmeleri ile ilgili bir çalışma yoktu. Genelde de böyle bazı tehlikeler de bu yüzden oluyor gibi teknoloji önden gitti kanunlar sonradan geldi şu anda da bir etik kurulundan geçmesi gerekiyor. Datayı nasıl kullanacağın veya kiminle paylaşacağın önemli. Ama bir yandan da kendi yaptığım çalışmadan bilebiliyorum sonuçta bir buçuk iki sayfalık, bilgilendirme metni katılanlara, oradan izin almaya çalışıyoruz. Bizim yaptığımız da en basit bilgileri istesek bile insanlar için yüklü bir şey. Kendim katılığımda da bakmak isterim başka herhangi bir şey kullanırken zoom kullanırken mesela karşıma çıkan sözleşme; küçük yazılar ile olduğunda okumak istemiyorum zaten veriyoruz deyip kullanmak zorunda olduğumuzdan kabul ediyoruz."* (Katılımcı 9, 35, Kadın)

Bir katılımcı ne Türkiye'de ne dünyada bu düzenlemelerin yeterli olmadığını, verilerin kullanılmasının önünde hiçbir engel olmadığını ve bu durumun ayrımcılığı çok daha fazla artırabileceğini belirtmektedir.

> *"Türkiye'de hiç değildir dünyada da değildir. Çünkü şöyle etik dediğimiz kavram pek çok farklı boyuta gidebiliyor. Müşteriden izin almak bile bazı*

> *verilerin kullanmasının önünde engel değil ve kullanılmaması da gerekiyor ki ayrımcılık dediğim etnik ayrımcılık olabilir, cinsiyet ayrımcılığı olabilir, gelir ayrımcılığı olabilir bunlarla ilgili kararlarda yanlı kararlar verilmemiş olsun. Yani yeterli olduğunu düşünmüyorum özellikle regülasyon boyutunda ama bunun üzerine gidilip çalışmalar yapılıyor ki geçen haftaki G20 zirvesinde Japonya'da başlık bütün G20 ülkelerinin çevresinde yapay zekâ ve büyük veri gibi teknolojilerin kullanıldığı yerlerde; modeller, sistemler, süreçlerde bunun etik olarak nasıl kullanılabileceği, bunlarla ilgili ne gibi düzenlemelerin yapılması gerektiği üzerineydi. Yani aslında şu an herkes bunlarla ilgili ne tür regülasyonlar yapılacağı üzerine çalışıyor.* (Katılımcı 6, 36, Kadın)

Katılımcılardan bazıları ise KVKK'nın iyi ve yeterli olduğunu fakat yaptırımların olmadığını ya da yaptırımlar varsa da bu yaptırımların halk nezdinde görünür olmamasının verilerin çeşitli kurumlar tarafından kanunlara uygun bir şekilde kullanılmaması durumunu arttırdığını belirtmektedir.

> *"KVKK bence yeterli, önemli olan bu kanunu piyasada uygulayan herhangi bir firma var mı uygulamadıkları zaman buna yaptırım yapan bir hükümet ya da devlet var mı olay bu. 2016 mıydı KVKK. 2016. Kanunlar çok net çok uygulanabilir. Benim bilgilerimi takip etme, ben bunların kaydedilmesini istiyorum, bunların haricindekilerin kaydedilmesini istemiyorum, ben işte arkada reklamları tutabilecek şekilde sana iş yaptırabilecek şekilde cookies dediğimiz çerezlerin şunların çalışmasını istiyorum, bunların çalışmasını istemiyorum dediğinizde ne olması lazım ona göre entegre etmesi lazım. Ama şimdi bir internet sitesine giriyorsunuz. Bir şey araştırıyorsunuz. Tam araştırırken bir şey çıkıyor gerekli çerezleri kabul et, tüm çerezleri kabul et, artık gerekli çerezleri kabul et de çıkmıyor. Çerezleri yönet, tüm çerezleri kabul et var. Sen şimdi bir şey araştırırken tüm çerezleri yönete gir ondan sonra bu mu şöyle mantıklıymış şunu kabul edeyim bunu etmeyim. Tabii ki tüm çerezleri kabul et diyorsun. Dolayısıyla sen adama seni takip etme izninin hepsini vermiş oluyorsun. Bu noktadan hareket edince bizim girmiş olduğumuz internet sitelerinde yani bankacılık bilgileri mesela. Çok rahat tutulabiliyor. En basitinden Sağlık Bakanlığı bilgilerinin mesela e-devlet üzerindeki tüm verilerin zaman zaman parça parça çalındığıyla ilgili çeşitli haberler çıktı. T.C. kimlik numaralarının ve adres bilgilerinin çalındığıyla ilgili haberler çıktı. Çevrimiçi bir yemek uygulamasının kullanıcı bilgileriyle birlikte kişilerin kart bilgilerinin çalındığına dair haberler çıktı. Uygulama hayır böyle bir şey olmadı dedi. Bir buçuk ay sonra yasa gereği bunu çok basit şekilde böyle böyle bazı sızıntıların olduğu tespit edilmiştir çeşitli çalışmalar yapıyoruz üzerinde… Eee? Millete yüzde üç yüzde beş puan verdi susturdu biz onu kabul etmek zorunda kalmışız gibi. Devlete de biraz ceza ödediler yırttılar. Normalde böyle olması mı gerekiyordu. KVKK'yı düşündüğünüzde. Yaptırımları çok büyük ama bunu özel sektöre dayatamıyorsunuz çünkü devletin kurumları buna daha entegre olamadı. Bir devlet bankası buna net bir şekilde entegre olmamışken bu gidip özel bir bankadan isterken yüzü kızarıyor insanın. KVKK'da böyle*

problemlerimiz var biz bunu içselleştiremediğimiz için bunları yaşıyoruz. Yoksa kanunun kendisinde ifadeler net. (Katılımcı 10, 37, Erkek)

Başka bir katılımcı da hiçbir şekilde yasal uygulamanın özellikle de yaptırımların yeterli ve görünür olmadığını vurgulamaktadır. Bunun yanı sıra, kurumlarda siber güvenlik alanlarında yeterli yatırımların yapılmaması, yeterli düzeyde ya da ihtiyaç duyulan pozisyonlarda personellerin çalıştırılmamasının ciddi sonuçları olduğuna dikkat çekmektedir. Bu durumu ise Black Mirror'un son sezonundaki distopik bir bölümle bağlantılandırarak, bu tür distopyaların çok da uzak olmadığını ifade etmektedir. Sadece bireyin, kurumun, devletin ve şirketlerin değil, her birinin bu konuya dikkat ederek bu durumun aşılabileceğini söylemektedir.

"KVKK aslında şöyle ciddi şekilde ihlal ediyor bence bizim Türk kanununda yasalarında bir sıkıntı yok biz burada yanlış yorumlamak da istemem hukukçu değilim, uzmanlığım da değil ama genel anlamda bizim yasalarımız aslında çok çeşitli her konuya değinen hatta bazen kendi içinde bir yasada başka bir şey deyip başka maddede onun tersini ifade eden hale gelmiş. Burada sorun yasamadan ziyade biz bunu nasıl yargılayacağız nasıl yürüteceğiz kısmında. Yasalarımız var ama bilgiler çalındı deniyor çevrimiçi yemek getirme uygulaması ihlal sonucu ne aldı mesela? Bir ceza aldıysa neden biz bunu pankartlarda görmüyoruz? Neden insanların gözünü korkutmuyoruz? Hani bakın paranız böyle çarçur olur siz belki proje yapmak için 1 milyon büyük dediniz hacklendiniz 10 milyonunuz gitti. Bilgilerin güvenin yanısıra ekstradan nakit cash olarak 10 milyonunuz gitti. KVKK'dan korkuyor insanlar bizim projelerimizde, korkmuyor değiller. Tutup da ben birinin şu an biz mesela bir havayolu şirketi ile bir proje yapmak istiyoruz ya da başka bir tanesi ile. Adamlar genel olarak yoğun örnek veri istedik isterken koyduğumuz madde şu isterseniz gizlilik sözleşmesi imzalayalım projeyi almamışken bile siz bize veriyi gönderin. Yoksa hiçbir firma size gizlilik sözleşmesi imzalatmadan verileri falan açmaz size. Bu tarz önlemler kurumsal anlamda alınıyor ama sorun şu herhangi bir ben şu an veri bilimciyim bide networkcüler IT'ciler var. Herhangi bir IT'ci benim bilgisayarıma herhangi bir şey download edilmiş mi bunu kontrol ediyor mu çünkü eğer ben art niyetli biri olarak o bilgiyi çalmaya çalışıyorsam olabildiğince gizli yöntemleri deneyeceğim. Aleni bir şekilde o bilgileri çalmayacağım ki. Burada aslında hem kendi iç denetlememiz hem de belki devlet tarafından bir denetleme gerekir büyük veri tarafında diğer bireysel girdiğimiz veriler noktasında biz zaten aslında yemek şirketinin ceza almamasının yüksek sebebi, biz zaten belki de indirirken öyle bir maddeyi kabul ediyoruz. Bu belki size bakış açısı verir. Black Mirror'un son sezonunda orada verdiğimiz izinlerle bir dizisi çekiliyor birinin. Bir kadının. O direk aslında bizim uygulamaya verdiğimiz izinlerle alakalı. Ondan bir önceki skorlama mantığı mesela. Bunlar, olabilecek en uç noktalar gerçekten en uç noktalarını yansıtıyor ama bir yandan da burası komün bir

> *şekilde ilerleyecek bir şekilde. Sadece ben KVKK'ya dikkat edersem olmaz. Ya da sadece benim iş yaptığım kurum dikkat ederse olmaz. Aynı zamanda denetçisi de olacak bunun. Ben çekmiyorum dedim diye o veriyi çekmemiş olmuyorum." (Katılımcı 16, 26, Erkek)*

Başka bir katılımcı ise kendi faydasını göz önünde de bulundurarak KVKK'nın bazı durumlarda işi yavaşlattığını ve verilerin fazlaca korunduğunu bunun işlenebilir verilerin oranını azalttığını düşündüğünü belirtmektedir.

> *"Ben işin pazarlamasında çalışırken bana çok sıkıcı geliyordu KVKK işi ben orada neler neler yaratabilirim hatta kullanabiliyorum zaten çünkü hani database'e ben ulaşıyorum zaten. Ben oradan erişirim kaydımı logumu denetçiler kontrol eder etmez ha ne oldu verileri kontrol ettim kullanırım da bilgiyi alır sonra silerim. Ben oradan kendi çıkarımımı yapıp 20 bin kişi üzerinde denerim çalıştı. KVKK'yı güncellerken bazı bilgileri insan girdiği için yanlış olabiliyor. Kesinlikle yeterli değil ama daha başarılı bir iş yapmak için benim daha doğru müşteriye kampanyayı götürüp hem onu faydalandırıp daha az para harcamam için benim için bir engel gibiydi. Ama herhangi bir IT'ci bakabilir, müdüre sorsan bakamaz falan der ama kendisi de istese girer. Birisi giriyorsa birçok kişi bakar. Yetkim yoktur arkadaşımdan isterim bakarım. Bir kişinin yetkisi olması yeterli herhangi bir bilgiye ulaşmaya."* (Katılımcı 11, 33, Erkek)

Bu tür yasaların uygulanmasında, halktan kişilerce uymayanlara yaptırımların daha görünür olmasının önemi çoğu katılımcı tarafından vurgulanırken diğer vurgulanan nokta ise bunun bireysel sorumluluk kısmıdır. Katılımcı 12 (43, Erkek), bu konuyla ilgili *"Bu pek çok kullandığımız uygulamada telefonda bizim önümüze kabul ediyor musun diye bir metin geliyor ama hiçbirimiz okumayıp onaylayıp geçiyoruz. Yasal olarak biz kendi consentimizi vermiş oluyoruz. O yüzden sadece yasal sürecin yasalar yeterli mi den öte çok bilgi sahibi değilim ama bunun hem uygulamaya hem de bir information, biz kullanıcı olarak ne kadar bilgi sahibiyiz ki kendimizi koruyabilelim noktasında problemler olduğunu düşünüyorum."* yorumunda bulunmaktadır. Yasaların etkili olabilmesi için öncelikle bireylerin de neye onay verdiklerini bilmeleri, önlerine gelen yasal metinleri okumaları ve daha bilinçli bir şekilde bu sistemleri kullanmaları gerektiğini önerdiği görülmektedir. Bir sonraki başlık altında veri manipülasyonu mu veri ihlali mi sorularına yanıt ararken de veri bilimciler tarafından özellikle bireyin onay vermiş olduğu verilerin işlenebileceği bunların bir veri ihlali olarak

görülemeyeceği, birey onay verdikten sonra bu veriyle neler yapılacağının artık bireyin kararından çıktığını vurguladıkları görülmektedir. Başka bir katılımcı ise bütün sorumluluğun kullanıcıya yüklenemeyeceğini, bunun bir bilgi asimetrisi oluşturduğunu belirtmektedir. Bilgi asimetrisinin temel sebebinin ise veri toplanırken, bununla ne amaçlandığının kurumlar ya da güç her kimse onun tarafından bilinmesi, fakat kullanıcı tarafından bilinmemesidir.

> *"Bu, her türlü süreç için söylenebilir. Ticari ilişkiler için, yasal süreçler için. Doğru kararı vermek. Ama bütün sorumluluğu sadece kullanıcıya vermek doğru değil. Bu sistemlerin çoğunluğu bunların okur-yazarlığını bilmiyoruz, tecrübesini edinmiyoruz bir yandan da information asymmetri böyle bir şey kurum biliyor herhangi bir kurum benden veri isterken ve KVKK ile bir form gönderip bilgi talep ederken hem datayla ne yapmak istediğini biliyor hem yasal yükümlülüklerini biliyor buna göre bir stratejisi var. Benim yok. Bu efor isteyen bir şey, öğrenmek. O yüzden doğrudan bireye bunu yüklemek çok da doğru değil. Kamunun böyle ilişkilerde vatandaşı koruma görevi olduğunu düşünüyorum. Bilgilendirme tarafı ya da o asimetriyi düzeltme ya da denge kurma açısından devletin de bir rolü olmalı. Bir diğer yandan bunlar bizim gündemimize çok yeni girdi toplam biz 20 yıldır 25 30 yıldır toplumsal dönüşümler ya da böyle şeylerin oturması çok daha uzun sürüyor teknoloji çok daha hızlı ilerliyor. Kurumlar kendi stratejileri doğrultusunda hukuki altyapılarını kurmaları ve talepleri konusunda daha kuvvetliler ve bu toplumların genel bilgi seviyesinin bilinç seviyesinin artması çok daha uzun bir süreç." (*Katılımcı 12, 43, Erkek)

Bu düşünceler ışığında veri bilimcilerin veri ihlali ve veri manipülasyonuna bakış açıları ve yeni gözetim sistemlerinin en net örnekleri olarak neleri gördüklerine dair diğer sorulara geçiş yapılmıştır.

4.1.4. Veri Manipülasyonu mu? Veri İhlali mi?

Katılımcılara Türkiye'de ve dünyada akıllarına gelen ilk veri ihlali nedir sorusu yöneltilmiştir. Bu sorunun amacı gözetim ile ilgili onların görüşlerini almadan önce, Türkiye'deki ve dünyadaki dijital gözetim uygulamalarından en dikkat çekenleri tespit etmek ve neden bu olaylardan etkilendiklerini anlayabilmektedir. Aşağıdaki tabloda detaylı bir şekilde görüldüğü şekliyle Türkiye'de ilk akla gelen veri ihlalleri siyasilerin kasetlerinin çıkması, ünlülerin Cloud hesaplarının hacklenmesi, (genel olarak devletin tuttuğu veriler olsa da) e-devletten verilerin çalınması, nüfus cüzdanı bilgilerinin çalınması, e-nabızdan alınan verilerin

çalınması, MHRS'den verilerin çalınması, NVI (Nüfus ve Vatandaşlık İşleri)'nden verilerin çalınması şeklindedir. Bunlara ek olarak özellikle bir bankanın, burada etik olmayacağından ismi paylaşılamasa da ismini kullanarak bankalarda yaşanan veri ihlallerine vurgu yapılmıştır. Yine aynı şekilde firma ve platform isimleri etik olarak paylaşılamamasına rağmen, çok bilindik bir hediye gönderme uygulamasından, bir yemek sipariş etme platformundan ve bir alışveriş platformundan sızan verilerden de bahsedilmiştir. Buna ek olarak Google Maps'in gidilen yerlerin verilerini alması ve tutması da bir katılımcı tarafından veri ihlali olarak değerlendirilmiştir. Çok güncel ve katılımcıları etkileyen "veri ihlali" olarak değerlendirdikleri diğer bir durum ise "Kim" ya da "Kim Bu?" diye adlandırdıkları uygulamadır.

Tablo 5. Katılımcıların Aklına İlk Gelen Veri İhlalleri

Katılımcı	Türkiye	Dünya
Katılımcı 1	Siyasilerin kasetlerinin çıkması Ünlülerin Cloud hesaplarının hacklenmesi	Amerika'da 52. Bölge, Pentagon'a sızan hackerların belgeleri uluslararası yayınlamaları
Katılımcı 2	Kim Uygulaması[11]	Facebook Olayları- Mark Zuckerberg'in mahkemelik olduğu olaylar
Katılımcı3	E-devletten T.C. Kimlik numaralarının alınması, İki önemli alışveriş platformunun verilerinin çalınması, Google Maps'te gidilen yerlerin işaretlenmesi, siyasetçilerin kasetlerinin çıkması	Facebook Olayları-Cambridge Analytica
Katılımcı 4	Alışveriş platformlarında kredi kartı bilgilerinin çalınması,	Facebook Olayları
Katılımcı 5	Bir telekomünikasyon firmasının verilerinin çalınması	Facebook Olayları
Katılımcı 6	Nüfus cüzdanı bilgilerinin çalınması, bir bankanın sürekli verileri çaldırması	Wikileaks Facebook Olayları-Cambridge Analytica
Katılımcı 7	Nüfus verilerinin çalınması	Facebook Olayları-Cambridge Analytica
Katılımcı 8	-	Facebook Olayları-Cambridge Analytica
Katılımcı 9	Nüfus verilerinin çalınması	İngiltere'de National Health Service'de büyük verilerin çalınması
Katılımcı 10	E-nabızdan verilerin alınması	Facebook olayları-Cambridge

[11] Daha fazla bilgi için bknz. https://www.youtube.com/watch?v=kAdPuY9tqoQ

	Bankalardan bilgilerin çalınması Alışveriş ve yemek platformlarından verilerin çalınması	Analytica
Katılımcı 11	Çalıştığı büyük ve ünlü şirkette CEO'nun şifresinin çalınması, danışman şirketlerden birinin hacklenmesi	Facebook Olayları-Cambridge Analytica
Katılımcı 12	MHRS'den verilerin çalınması, Kim Uygulaması	Snowden Olayı-NSA (Kararsız) Facebook Olayları-Cambridge Analytica (Kararsız)
Katılımcı 13	"Çok fazla ama açıklayamam" Bankalardan veri çalınması Yemek firmasından verilerin çalınması	-[12]
Katılımcı 14	Bankanın verilerinin çalınması E-devlet verilerinin çalınması	Wikileaks Facebook Olayları-Cambridge Analytica
Katılımcı 15	Bankanın verilerinin çalınması E-devlet verilerinin çalınması	Facebook Olayları-Cambridge Analytica
Katılımcı 16	E-devletteki NVI'nın çalınması	Snowden Olayı-NSA

Bu (Kim Uygulaması) uygulamaya bakıldığında, seçim döneminde o dönemin İçişleri Bakanı'nın Türkiye'nin ilk yerli aracını (TOGG) deneyimlemek için katıldığı bir YouTube kanal içeriğinde (ShiftDelete.net kanalında) o dönemki bakanın, teknolojinin şu an en üst düzeyde olduğunu, özel harekât, emniyet, Jandarma Genel Komutanlığı, Nüfus ve Göç İdaresi gibi İçişleri Bakanlığı'na bağlı olan kurumlardaki teknoloji kullanımın artırıldığını belirtmektedir. Bahsedilen kurumlar arasından bazılarındaki parmak izinin birbiriyle artık entegre olduğu belirtilmektedir. Bu durumun "suç ve suça karışmamış vatandaşın işlerini kolaylaştıracağı, suç ve suça karışmış vatandaşların da nerede olursa olsun tespitinin yapılabilmesini sağlayacağı" söylenmektedir. Kanal sahibinin telefonunuzu alıp hangi uygulamalar var, en son kimi aramışsınız, size gelen son 10 sosyal medya mesajı nedir bakmamız için izin var mıdır sorusuna "Buyurun alın" diye bakanın cevap vermesinin ardından

[12] Katılımcı 13 ve Katılımcı 16 Facebook-Cambridge Analytica'nın bir veri ihlali değil, veri manipülasyonu olduğuna dair açıklamalar yapmaktadır. Bununla ilgili detaylı bilgi bölümün içerisinde yer almaktadır.

bakanın yüzü okutularak telefonu incelenmeye başlamıştır. Konuşmanın ilerleyen kısımlarda uygulamalar incelenirken Bakanın "Sana buradan bir numara yapabilirim şu an mesela. Sen diyorsun ya teknoloji, teknolojiyi en iyi kullanan bakanlıklardan birisi İçişleri Bakanlığı'dır. Hiç bu konuda tevazu göstermem hiç" cümlesi üzerine kanal sahibi "Ne yapabiliriz mesela?" demiş, Bakan, kanal sahibinin fotoğrafını çekerek uygulamada saniyeler içinde birçok bilgisine ulaşmış, kanal sahibi şaşırmış Bakan bunun üzerine "Bu devletin çok büyük güçleri var" deyip gülmüştür. "Bu size gösterdiğim yüz binde bir" diye de eklemiş, YouTube kanalı sahibi "Bunu yayınlayabilir miyiz?" diye sormuş Bakan ise "Yayınlayabilirsiniz" diyerek cevap vermiştir. Kim uygulaması adı verilen bu uygulamaların seçimler öncesinde bu şekilde ifşa edilmesi Türkiye'deki vatandaşlar tarafından şaşkınlıkla karşılanıp, büyük yankı uyandırmıştır. Katılımcılardan bir tanesi bu duruma olan şaşkınlığını şu şekilde ifade etmektedir:

> *"En yakın zamanda gördüğüm hepimizin de sosyal medyadan ya da haber sitelerinden gördüğü bakanımızın cep telefonundaki kim bu uygulaması. Yani şok içerisindeyim onu gördüğümden beri, inanamadım. Türkiye'de öyle bir uygulamanın olduğuna, Çin'de falan yapıldığını biliyoruz yüz analizleri vesaire, ama Türkiye'de bunun olması beni çok şaşırttı. Bunla ilgili bir çalışmanın şeffaf olması gerekiyor. Böyle bir çalışma yapılıyorsa bilinerek yapılmalı, yani e-devleti herkes biliyorsa bunu da herkes bilmeli, tabi herkes kullanmamalı o ayrı ama o da çünkü başka sıkıntılara yol açabilir ama böyle bir şey yapıldı, yapılıyor bilgisi insanlara verilmeliydi, çok büyük bir şey, direk ifşa."* (Katılımcı 2, 28, Kadın)

Bir diğer katılımcı ise bunun milli güvenlik için yapılmasından ötürü kişi hakları konusunda tartışılabilir olsa da ihlal olup olmadığını bilmediğini belirtmektedir.

> *"Benim bildiğim yasal olarak belgelenebilecek şeyler söyleyemem ama şu şeyleri biliyoruz. Birincisi Türkiye'deki MHRS kayıt sistemi üzerinden çok ciddi sayıda insanın seçmen kütükleri verisinin açıkta olduğu erişilebildiği, sağlık bilgilerinin bir kısmının kişisel bilgiler kısmının açıklandığı ve bunun üzerinden bir ticaret olduğu onun dışında benim bildiğim çok büyük bir işlem yok. İçişleri Bakanı ve o güvenlik için ben Türkiye'deki herkesi görüntüsünden ve resminden tanırım consent almadığım halde diyebiliyor. Bunlar gri bölgeler çünkü aynı şeyi NSA ya da benzeri kurumların milli güvenlik anlamında kişi hakları her zaman başka bir tarafa gidiyor. Yasal olarak ihlal midir bilemeyeceğim."* (Katılımcı 12, 43, Erkek)

Uluslararası anlamda katılımcıların aklına gelen ilk veri ihlalleri sorulduğunda ise katılımcıların genel olarak ortak noktada buluştukları; Facebook-Cambridge Analytica Olayı, Wikileaks sızıntıları, Snowden-NSA Olayı olarak üç temel olayı ifade ettikleri görülmektedir. Bunlara ek olarak Pentagon'a sızan hackerların uluslararası ölçekte belgeleri yayınlamaları ve İngiltere'de yaşayan bir katılımcının oradaki Milli Sağlık Örgütü'ndeki verilerin çalındığını ve orada çok yankı uyardığını aktardığı görülmektedir.

Katılımcıların çoğunluğu bu durumları veri ihlali olarak değerlendirirken, bazı katılımcıların veri ihlali ve veri manipülasyonu konusunda daha çok düşünmek gerektiğini, çeşitli durumlarda ikisinin birbirine karıştırılabildiğini özellikle Facebook-Cambridge Analytica ve Snowden-NSA olayı üzerinden kendi içlerinde de tartıştıklarını ve bazı katılımcıların kesinlikle bu olayları veri ihlali olarak değerlendirmediği de görülmektedir.

> *"Facebook bir veri ihlali değil. Cambridge bir veri ihlali değil. Cambridge bir veri manipülasyonu. Bu büyük verinin Çin örneğinin bir çıktısı. Yani veri ihlali mi? Ben hiç birimizin Facebook'a üye olurken o maddeleri onaylamadığını düşünmüyorum. O maddeleri açıp okumak lazım. Verimizin biz özelleştirilebilir gönderi göndermesine izin veriyoruz. O zaman Instagram da yapıyor aynısını o zaman ona da veri ihlali diyelim. Veri ihlali olması için izin verilmeyen bir durum olması lazım. Cambridge veri ihlali değil çok ciddi bir hükümet, özel sektör ve veri bilimin bir araya geldiğinde yapabileceklerinin bir göstergesi. Cambridge'nin yaptığı şuydu önce ikiye bölüyor insanları yani aşırı sağ aşırı sol olarak zaten parti mantığı var. Soldan sağ merkeze kaymaya yakın kişilere sağın iyiliklerini gösterirken daha çok solla sağın ortasında kalanlara solun kötülüklerini gösteriyor sağa gitmesi için. Herkese aynı şeyi göstermedi orada. Ya da bizim burada işte bir terim vardı onun için yankı odası terimi son zamanlarda çok popüler oldu. Twitter'da ben kimi takip ediyorum? Benim gibi düşünen insanları. Ya da sürekli onları likelıyorum, retweet ediyorum. Bir süre sonra benim Twitter space'im yankı odasına dönüşüyor. Bu yankı odası dediğimiz benim gibi düşünenlerle dolu bir oda yani aslında. Seçimlere giderken diyorum ki bu sefer çok kuvvetliyiz, bu sefer kesin kaybettiler. Neden? Çünkü ben sadece kendi sesimi duyduğum bir alana dönüştürdüm sosyal medyayı da. Aynı şekilde bana aynı feedbacki sağlıyor. Twitter tutup bana AKP'nin yaptığı iyi bir şeyi göstermiyor ya da CHP'nin çünkü diyor ki bu x partide ve x partide yalnızlaşmış bir noktada bununla hiç uğraşmayalım artık."* (Katılımcı 16, 26, Erkek)

Katılımcının burada bahsettiği durum büyük verinin dijital gözetim sistemlerinde tartışılması gereken en önemli noktalarından birini ortaya çıkarmaktadır. Birey onay verdiği, çerezleri kabul ettiği, sözleşmeleri okumadan onay verdiği sürece bilgilerini açmış, kamusal alana analiz için sunmuş hale gelmektedir. Katılımcının da dediği gibi bu durumda bu verilerin kurumlar, devletler, özel şirketler tarafından kullanılması açısından bireyi koruyan bir mekanizma kalmamaktadır. Katılımcıya göre onay sürecinden geçtiği için bu bir veri ihlali değildir. Tıpkı e-ticarette ve pazarlamada kullanıldığı gibi bireylerin tercihlerini, alışkanlıklarını ve bu noktada siyasi görüşlerini tespit ederek onları belirli bir yönde yönlendirmektir, bu bir tür algoritmik manipülasyondur. Aynı katılımcı Snowden Olayını ise bir veri ihlali olarak değerlendirmektedir ama burada da genele kıyasla veri ihlali yapan özne konusunda farklı görüşler bildirdiği görülmektedir.

> *"Snowden'ın yaptığı veri ihlali, Snowden gizli bilgileri çıkardı çünkü. Orada iki türlü yapı var aslında. Robin Hood size göre iyi mi kötü mü gibi bir soru bu. Snowden veri ihlali yapan bir kurumu çok ciddi derecede devletin güçlerini kullanan veri ihlali yapan bir kurumu ifşa etti. Yani onların verisini aldı dışarıya sızdırdı. Dolayısıyla Snowden, burada Robin Hood oluyor ama onun yaptığı da bir veri ihlali NSA'in yaptığı da bir veri ihlali. NSA'in yaptığı şöyle bir veri ihlali iki üç madde geçerli, ICloud mesajları orada okunabildi mi mesela bunu bilmiyoruz. Apple mesajları dava olmadığı sürece vermediğini iddia ediyor. NSA mi sorumlu WhatsApp mı? Bir araştırmam için sizin işte gözlemlerinizden topladığınız yaş bilgisi lazım. Siz de verdiniz. Burada ihlali yapan sizsiniz ben değilim. Ben aldım kullandım analizlerimi yaptım. WhatsApp'tan bu konuşma bilgilerini alırken ne şekilde aldığın önemli. Kimlik bilgileriyle mi verdi davalık olanları mı verdi yoksa NSA, WhatsApp'a erişip bu bilgileri mi aldı. Burada arada birçok katman olduğu için Snowden tabi artık bilgi kimdeyse en güçlü odur. WhatsApp'ta bir Facebook'da iki NSA'da dört birim bilgi var Snowden en güçlünün NSA olmasını istemedi yoksa WhatsApp NSA'ya sızdırıyor derdi. Snowden dönüp NSA herkesin bilgilerini alıyor dedi. Algısal olarak orada ciddi bir algı mücadelesi de verildi. Aynı şey Trump döneminde de yaşandı Trump'ın mesajlaşmaları Rusya ile alakalı bir bağlantısı olup olmadığına dair NSA dava açmak istedi WhatsApp üzerinden belki bu bilgi elde edildi ama Apple döndü dedi ki ben dava olmadığı sürece davada haklı bir sebep olmadığı sürece telefona ilişkin hiçbir şeyi paylaşmam. Oradaki mevzu Trump'ın bireysel olarak yaptığı bir görüşme değildir. Trump'ın yakının yakınının yakınının verdiği bir ipucudur. Mesela Apple Air Tagler var işte bir şey kaybediyoruz bulmak için çaldırıyoruz o nasıl çalışıyor herkes alıyor kullanıyor ama şöyle bir sıkıntı var sizin Appleiniz var benim var ve işte atıyorum İstanbul'da benim sizin airtaginiz tüm applelara belli bir IP ile sinyal gönderiyor. Sizin yanınızdayken siz direk bulabiliyorsunuz. Benim*

> *yanımdan geçerken bana sinyal gönderiyor. Benim lokasyon bilgimi alıyor sizin uygulamanıza gönderiyor ve diyor ki ben en son buradaydım. Aslında o lokasyon bilgisini benden aldı. Sadece mesajlaşma olmayabilir lokasyonda olduğunun ispatlanması gerekiyordur belki ve bu bir cihazdan çekiliyor da olabilir yani."* (Katılımcı 16, 26, Erkek)

Başka bir katılımcının ise veri ihlallerinin sebeplerine bakmak gerektiğini ve Wikileaks Olayı'nı Robinhood örneğiyle benzetmesi dikkat çekmektedir. Veri ihlali hakkında yorum yapılacaksa öncelikle onun ne amaçla, nasıl yapıldığına bakılması gerektiğini belirtmektedir.

> *"Wikileaks geliyor aklıma böyle deyince ama pozitif bir şey bence oradaki verilerin ihlali. Etik olarak yanlış, kişisel olarak merak uyandıran belki de insanlar için iyi bir noktaya gidebilecek bir şey. Ama Wikileaks dışında yine birçok Facebook bu konuda master, sürekli verileri çaldırıyor, Elon Musk'ı hiç sevmiyorum ki hiç güvenmem en başından beri."* (Katılımcı 14, 26, Erkek)

Aynı şekilde başka katılımcıların da veri ihlali ile veri manipülasyonu arasında ciddi bir ayrım yapılması gerektiğini söylediği ve Cambridge Analytica'nın yaptığının sadece kişisel verilerin modellenerek açık olarak kullanılması olduğunu düşündüğü görülmektedir.

> *"Cambridge Analytica açık olarak orada kişisel verilerin modellenerek açık olarak kullanılması (katılımcı bunun bir veri ihlali olduğunu düşünmüyor). WhatsApp uçtan uca şifreliyor öyle mi sence mesajlarımıza erişemiyor mu erişiyor. Konuşmalarımıza da erişiyor. Korunan hiçbir veri yok zaten. Önemli olan kritik kısma geliyoruz. Biz kişisel veri diyoruz ama biz kişisel verileri kendimiz paylaştığımız zaman anonimleştirmiş oluyoruz…Yüz tanıma motorunu geliştirirken en önemli şey sizin veri koleksiyonunuz, açık veri kaynaklarınız, bunlar için laboratuvarlar var onun dışında sosyal medyada paylaşım yaparak bu konuda iyi niyetli olan veya olmayan biçimde çalışan tüm taraflara kendi elimizle bu verileri sunuyoruz. Tüm biyometrik verilerimizi sunuyoruz. Herhangi bir şekilde benim ziyaretçim geldiğinde ben yüz tanıma için şimdi yapmıyorum ama yaparsam burada girişte bunun verilerini yapmakla yükümlüyüm. Yarın öbür gün başka biri benim kişisel verim kullanıldı denilmesin diye. Öte yandan Instagram'da insanlar bununla ilgili paylaşım yapıyorlar yalnızca fotoğraflarını değil ses kayıtlarını paylaşıyorlar. Zaten telefonlar yüz tanıma özelliğiyle bütün biyometrik verilerimizi alıyor, ses biyometrimiz zaten konuşmalarımızla alınıyor zaten bizden daha iyi biliyorlar artık sesimizi. Hal bu olunca bu veriler var bunun kontrollü kullanımı ve hangi amaçla olduğu önemli. Teknolojiyi kullandığımız müddetçe biz her an için veri ihlaline farkında olalım ya da olmayalım uğruyoruz. Başka bir şansımız yok. Varsayımsal*

> *konuşuyorum birisi eğer arama motorlarının sunucularına erişebiliyorsa teorik olarak bizi bizden daha iyi tanıyan, eğilimlerimizi bilen ve istediği şekilde manipüle edebilir şekilde bunu kullanabiliyor. Büyük veri web tarayıcıyla web data chromela ilgili tartışma o aslında. Çünkü web veri tarayıcıları endeksli veya endekssiz olmak üzere ajan robotlarla, elektronik ajan kastettiğim, herhangi bir şekilde sizin web tarayıcısında paylaştığınız ve gizli olduğunu düşündüğünüz bütün verilerin hepsine erişebilir durumda."* (Katılımcı 13, 57, Erkek)

Başka bir katılımcı ise bu durumun oranın yasalarıyla da ilişkili olduğunu ve yine kişilerin kendi onaylarıyla bir tür öneri verme mantığında olduğu gibi kullanıldığını belirtmektedir:

> *"Bu, oranın yasalarıyla ilgili. Etik olarak baktığında bu beraberinde şunu getiriyor. Güçlü olan sonuçta Zuckerberg'in yaptığı orda kullanıcıların kendi consentleriyle kendi kullanıcılarının neyi beğenip beğenmedikleri üzerine profilleyip o insanlara bir içerik sunmak, bu politik bir içerik. Normalde reklamcılık da aynı şeyi yapıyor. Bizim sen şunu izledin şu ürünü de seversin diye önümüze gelen recommendation sistemleri de çok farklı bir şey değil. Ticari tarafta bunu yapınca bu bir ticari başarı olarak algılanıyor. Hatta yani muhtemelen platformlarda biraz önce unuttum ama Spotify kullanıyorum, nerdeyse bütün streaming platformlarında ya benim ya eşimin bir hesabı var. Bunlarda da benzeri bir süreç var benim ne izlediğime bakarak benzeri şeyler öneriyor. Burada da aslında kişilerin beğenilerine bakarak aslında şu içerik ya da söylem etkili olur diyor. Ticari taraf da bu bir sorun değil ama siyasi anlamda bir manipülasyon aracı. Normalde eskiden de bunu pek çok kurum yapıyordu. Böyle yapmadan da bu ile gittiğinde şuranın demografisi böyledir, daha muhafazakâr söylem etkili olur şöyle söyleyelim böyle söyleyelim, bu bölgede şu milletler şu ırklar şu mezhepler ya da şu ideoloji yaygın diye çok benzerini yaparken şimdi bunu kişiselleşmiş olarak yaptığı için bu bir sorun. Bu bir sorun bence. Çünkü yine bir kez daha kullanıcı ya da Facebook kullanıcısı bu süreçten bir haber. Çünkü information asymmetri yani. Kendi önüne gelen içeriği aslında kendisinin manipüle etmek için üretilen bir içerik olduğu hatta satın alınan bir içerik olduğu konusunda bilgi sahibi değil. Dolayısıyla birey olarak tabii ki kendisine düşen görevler var. Toplumdan bunu beklemek ne kadar anlamlı? Büyük çoğunluğundan."* (Katılımcı 12, 43, Erkek)

Bir katılımcının aynı "veri manipülasyonunun" Türkiye'de de yapıldığını belirtmesi ise ilgi çekici bir detaydır. Katılımcı 10 tüm bu sistemlerin uluslararası anlamda seçimleri yönlendirmek için kullanıldığını şu şekilde ifade etmektedir:

> *"Facebook. Cambridge Analytica bunun başka hiçbir şeyi yok. Bu Big Hack miydi filmin ismi. Parça parça aslında nasıl yaşandığını Türkiye'de de gözlemledim. Bunun aynısını Türkiye'de de gözlemledim. Aynısı son*

> *seçimlerde de yapıldı Facebook'da. Şöyle düşün işte. Bunun en basiti Hilary Clinton Amerika'da başkan adayı olmadan siyahilerle çok gençken yapmış olduğu bir maymun benzetmesiyle ilgili bir şey var Hilary Clinton'un oylarının yüksek olduğu düşünülen bölgelerde Facebook'ta öneri video olarak insanların karşısına çıkarılmaya başlandı. Bu Cambridge Analytica ile Facebook'un insanlar üzerine yapmış olduğu en büyük etkilerden bir tanesiydi. Facebook bir aracıydı. Bir seçim yönlendirildi. Bunun aynısı Türkiye'de de yapıldı."* (Katılımcı 10, 37, Erkek)

Başka bir katılımcı ise kendisinin bulunduğu konumdan ötürü ona veri ihlali yapması yönünde teklifte bulunulduğunu fakat reddettiğini ama reddetmese de onu kimsenin tespit edemeyeceğini ve bu tür durumların çok fazla yaşandığını belirtmesi dikkat çekmektedir:

> *"Müşteri bilgilerinin ya da mesela bir şey söyleyeyim işte bir arkadaşım bana şey diye teklif etmişti. Ben ekipman şirketinin başına geçiyorum sen de CRM bilgileri vardır bana şunları verir misin, sana şu kadar para veririm. Ben o sırada şirketimden nefret etsem böyle bir yetkim var kimse de tespit edemez mesela. Yurt dışına çıkacağım başka bir işe geçeceğim falan filan. Mesela böyle bir şey yapmadım ama dolayısıyla ulaşmak isteyen birisi ulaşabilir o yüzden yeterli değil kesinlikle."* (Katılımcı 11, 33, Erkek)

Veri ihlallerinin önüne geçilebilmesi için neler yapılabileceğine yönelik sorular yönetildiğinde ise katılımcıların bakanlıklardaki alt yapı çalışmalarının önemine, buna ayrılan sermayeye, özellikle devlet kurumlarının ve önemli verilerin toplandığı platformların siber saldırılara karşı güçlü hale getirilmesine vurgu yaptığı (Katılımcı 1, 29, Erkek) görülmektedir. Bu anlamda temel olarak bunlardan sorumlu olan ve önlem alması gereken ilk kurum devlettir.

> *"Kurumlarda zaten bireysel olarak her vatandaşın verilerini koruyabileceği yer bakanlıklarda alt yapı çalışmalarının biraz daha aslında şöyle yine paraya dayanıyor. İnsanlar ve devletler buna çok önem vermiyor. Ta ki bilgiler çalınana kadar. Çalındıktan sonra kaynaklarını akıtıyorlar bir anda ama verilerin korunması için uğraşıyorlar ama artık o veriler çalındı. Artık çok daha önceden alt yapının güçlendirilip siber saldırılara karşı güçlü hale getirilmesi gerekiyor. Bakanlıkların, devletin önlemi olmalı. Böyle olursa bireysel olarak da insanların verilerinin korunabileceğini düşünüyorum. Bunu yapabilecek kişiler aslında temelde gene mühendisler ama bunun kararını verecek kişiler olmuyor. Bunun kararını verecek kişiler üst yönetimden bakanlık seviyesinde insanlar oluyor."* (Katılımcı 1, 29, Erkek)

Diğer bir katılımcı, bunun en önemli yönünün teknik olduğunu ve uzmanların ya da kurumların verileri tutarken anonimleştirerek daha dağınık bir şekilde, hatta daha kısa süreli tutulmasının ve veri ile işlem bittiğinde bu verilerin silinmesinin başka amaçlarla kullanımın biraz daha önüne geçebileceğine (Katılımcı 2, 28, Kadın) işaret etmektedir.

> *"Random olarak tutulması bir de olabildiğince kategorileştirilmemesi diye düşünüyorum. Çünkü çok fazla kategori olduğu zaman atıyorum 25 30 yaşındaki üniversitede okuyan bilmem ne bilmem ne öğrenciler gibi bir kategorizasyon yaptığımız zaman üç kişi kalıyor belki onda. Böyle bir kategorizasyon yapılırsa kimin kim olduğu hangi bilgilerin kime ait olduğu daha çok ortaya çıkar yani bunları koruyamayız gibi geliyor bana. Daha random olarak daha dağıtık bir şekilde tutulması hatta belki olabildiğince daha kısa süreli kayıtlar yapılması olabilir belki. Bir süre sonra o kaydın silinmesi ve yenilerinin gelmesi, kaydın sürekli güncellenmesi gibi. Bunu kontrol edecek bir birim oluşturması, silinmesi ve devamının olmaması ile ilgili ya da atıyorum bir insan dijital platforma 14 yaşında başladıysa 14 yaşından 35 yaşına kadar aynı id ile kaydediliyorsa bu çok büyük sıkıntı yine random olması belki daha etkili olabilir. Uzun süreli alışkanlıkların takip edilmesi daha bireyselleşiyor daha parmak izi gibi oluyor artık."* (Katılımcı 2, 28, Kadın)

Bireysel olarak daha bilinçli olması gerektiği, bu sistemlerin nasıl kullanıldığına dair daha bilgili olması gerektiği belirtilmektedir. Fakat bazı katılımcılar ise eğer bu sistemleri kullanıyorsak verileri tutmanın ya da hatta artık bu sistemleri kullanmamanın mümkün olmadığını belirtmişlerdir.

> *"Verileri korumak için ilk önce bireysel olarak verilerin ne kadar önemli olduğunun farkında olmamız lazım bunun pek farkında değiliz ki zaten bundan bir on yıl öncesinde biz hazırlıktayken hiç böyle bir şey söz konusu değildi ve nasıl kullanılacağına dair de bir bilgimiz yoktu ama şu an veri her şey demek. O yüzden sadece istediğimiz şekilde veriyi paylaşmamız gerekiyor bence bireysel olarak. Ya hala açık Facebook'um ama uzun süredir kullanmadığım için verilerimi artık kullanmıyorlardır herhalde."* (Katılımcı 3, 30, Erkek)

> *"Çok mümkün olduğunu düşünmüyorum. Sosyal medya kullanıyorsak, bir şeyleri araştırırken internet kullanıyorsak ki herkes artık internet kullanıyor. Çok mümkün olduğunu düşünmüyorum ama kişisel doğrulama yapabiliriz. Apple 'da olan ama Androidte olmayan bulut depolama, anlık buluta ekleme yapılabilir. Özelden genel bir oran olması gerekiyor. Önce biz sonra şirketimiz bulunduğumuz bölgedeki şirketlerin federasyonları gibi düşünebiliriz."* (Katılımcı 5, 26, Kadın)

Bunun yanı sıra bireylerin teknik olarak yapabileceği basit uygulamalar ve öneriler ise şu şekildedir:

> *"Çift adımlı doğrulamalardan bir tek haberim var, Instagram sayfaları çalınanlar çift doğrulaması olmayanlar, çift doğrulama olduğunda çalınması daha güç oluyor. Yani her şey mailimize bağladığımız için. Mailin güvenliğini arttırdığımızda, yani maili de telefona değil, birkaç farklı şekilde güçlendirdiğimizde belki de çift doğrulama ile daha güvenli hale getirebiliriz. Yoksa öbür türlü herkes tüm bilgilerini bir flashın içinde taşıyacak çıkarken cebine koyacak başka türlü mümkün değil."* (Katılımcı 5, 26, Kadın)

> *"Bu verilerin ben yüzde yüz korunacağını düşünmüyorum illaki kötü niyetli yazılımlar çıkacaktır kimseye de yüz de yüz güvenemeyiz. Bu verileri mümkün oldukça çok işlevi olmayan işlevsiz hale getirilebilir. Sadece anlık spesifik veriler kullanılabilir bir şeyle ilgili. Bir yere gittiğiniz zaman sadece adınız soyadınız alınsın biraz veri paylaşımı kısıtlanabilir ben korunacağını düşünmüyorum şu an için. Artık çok geç. Birey de kendi fotoğraflarını daha az paylaşabilir ya da yakından çekilmiş fotoğraflarını daha az paylaşabilir. Sonuçta yüz tanıma da var şu an 12 tane fotoğrafla sizin yüzünüzle bir yerleri açabiliyorlar. Bireyler de bunu daha az yapmalı ve önemli olan devlet buna engel olmalı mesela uygulamalarda bir şey indirdiği zaman galeriye ulaşacağım rehbere ulaşacağım bunları isteyememeli. Bir kanunla bu yasaklanmalı mesela. Sadece uygulamayı kullanmalıyım. Sanırım 12 fotoğraf yeterli oluyor ve yüz tanımayla o biraz asparagas bir haber de olabilir ama bu selfieyi özellikle yaygınlaştırdılar ki insanların yüzlerini tam olarak alabilelim."* (Katılımcı 8, 29, Kadın)

Kişisel Verileri Koruma Kanunu'nun etkin bir şekilde uygulanıp uygulanmadığına ya da yeterli olup olmadığına yönelik cevaplarda da karşımıza çıkan, yasaların yeterli fakat uygulanmıyor oluşu görüşüne burada da rastlanmaktadır. Bir katılımcı, bunun için özellikle şirketlerin yüksek para cezasına çarptırılmasının önemli olduğunu düşündüğünü belirtmektedir.

> *"Kesinlikle bu verilerin şirketleri korumayı ele alması için ceza yemesi lazım. Yaptırımı çok yüksek olan maddi cezanın olması lazım ya da operasyonlarını durduracak kadar yaptırımların olması lazım öbür türlü ciddiye almayacaklar."* (Katılımcı 6, 36, Kadın)

Bu tür verilerin korunmasının bireyin, devletlerin ve kurumların tekelinde olmasının çok sorunlu olduğu ve genel olarak hepsinin bir arada kendi sorumluluklarını yerine getirerek bu sistemlerin düzgün işleyebileceği düşünülmektedir. Bunun yapılabilmesi için özellikle güç ilişkilerinde bir dengenin

olması ve büyük veri ayrımındaki gibi büyük veri zengini ve yoksulu durumunun oluşmasının önüne geçilmesi gerekmektedir. Bunun yanı sıra, belirli şirketlerin de tüm verilere hükmetmemesini sağlayacak uluslararası kuruluşların olması gerektiği önerilmektedir. Bunlara ek olarak özellikle eğitim verilerek bireylerin küçük yaştan itibaren bu alanda bilgilendirilmesi ise bir diğer öneri olarak görülmektedir.

> *"Bir kere bu verilerin tutulması ile ilgili şirketlerin tekelinde olmasından ziyade kontrol daha global şekilde olabilir. İnsan Hakları Mahkemesi gibi mesela örnek verirsek. Daha global çerçevede bunlar incelenirse hesap verme sorumluluğuyla daha iyi olabilir. Kurum ya da kuruluşların olması yani sadece Türkiye'de bir şirket ya da bir çevrimiçi alışveriş platformunun kendi alt dalı olmasın bunu kontrol eden daha global daha örgütler üstü bu şekilde bir şeyin olması kanunların da her ülkenin her platformu için geçerli olmasını sağlayabilir ve hesap verilebilirliği arttırır belki."* (Katılımcı 2, 28, Kadın)

> *"Herkes sorumlu. Veri alıcı-veri vericiler vardır. Vericiler verir alıcı o noktada sorumlu olmaya başlar. Ben mesela verici, orada araba çekilişindeki adam alıcıdır ve artık o sorumludur. Onun veriyi belli bir süre koruması gizlemesi ve belli bir süre sonra imha etmesi gerekmektedir. Devlet burada tam bir piramidin sağ köşesinde açtığımız parantez. Devlet her zaman sorumlu. Tüm her yerde kişinin verisi belki ben bir ihlal yapacağım onu koruması lazım ya da o bir ihlal yapacak beni koruması lazım. Verinin verdiği sürece kadar alan da aldıktan belli bir süreye kadar sorumluluğu devam ediyor."* (Katılımcı 14, 26, Erkek)

Teknik anlamda neler yapılabilir sorusuna ise özellikle literatürde de yer alan değiş tokuş ve şifreleme önerileri gelmektedir.

> *"Tokenisation ya her seferinde encyripted yapıları biz kullanıyoruz ve encrypt ediyoruz. Bu önemli çünkü ben kodu yazıyorum ve birine teslim ediyorum orada şifrenin hiç görünmemesi gerekir. O yüzden encyripte ediyoruz. Ya da vpnlerimizi artık tokenisation var. Ben vpn'in şifresini giriyorum, kullanıcının adını giriyorum yetmiyor telefonda authenticator uygulamalar var o uygulamalardan gelen tokenı onaylıyorum ya da giriyorum vpn'im bağlanmış oluyor. Her seferinde bu uygulama yeni bir yapı geliyor verilerin güvenliği için. Bilmiyorum ileride konuşur muyuz ama bu Bitcoin gibi yapıların da temeli de aslında bunlara dayanıyor. Parayı nakit olarak bir yerde tutmuyorsunuz, bir yerde şifrelenmiş bir noktayı satın alıyorsunuz en basitinden. O nokta artık sizin ama onun bir parasal karşılığı var. Bu güncel bankalardan daha güvenli çünkü güncel bankalar soyulabilir, hesaplarınız patlatılabilir, kredi kartınız çalınabilir ama satın aldığınız bir noktanın şifresi bir Antalya'da biri Uganda'da biri Kanada'da 6 farklı noktadan 6 farklı şifreyi kırıp Bitcoin'e ya da öyle bir şeye ulaşması*

> *gerekiyor. Bunlar güvenliği artırıyor ama yani güvenlik arttıkça tehlike de artıyor bunun sınırı yok."* (Katılımcı 14, 26, Erkek)
>
> *"Burada mesela okullarda herkesin bir günlük bir şey ama Data Security (Veri Güvenliği) dersi alması gerekiyor belgelerini nerede saklamalısın, internette bilgilerini nerede saklamalısın, nelere dikkat etmen gerekiyor. Bizim okulda varsa diğer üniversitelerde de vardır diye düşünüyorum."* (Katılımcı 9, 35, Kadın)

Bu soruları düşündükten sonra büyük veri ve dijital gözetim sistemlerinin toplumda bir tür yıkıcı güç olarak yer alıp alamayacağı katılımcılarla konuşulmuştur. Bu konuda bir kısmının tamamen distopik olarak sayılabilecek düşünceleri varken bir kısmının ise olumlu bakmanın gerekliliğine vurgu yaptıkları görülmektedir. Bir sonraki bölümde bu konunun detayları görülmektedir.

4.1.5. Büyük Verinin Yıkıcı Bir Güç Haline Gelmesi

Büyük verinin yıkıcı bir güç haline gelmesi potansiyelinin onun kullanım şekline bağlı olduğu ve çok farklı alanlarda çok farklı etkileri olacağı belirtilmektedir.

> *"Yani bugün dünya üzerinde sağlıksal, silahsal olarak birçok şey yapılıyor. Bunları devletlerin ya da insanların faydası için yapıyorlar. Ama insanlar kötü amaçla kullanıyorlar. Büyük verinin de aynı şekilde olduğunu düşünüyorum. Yani insanlık için çok fazla hizmet edebilecek bir sektör ama bir o kadar da kötü yöne çekilebilecek bir şey."* (Katılımcı 1, 29, Erkek)
>
> *"Bir insan kullanacağı için büyük veriyi, niyeti sonuçta buradaki kullanım amacını belirliyor. Kötü amaçlı kullanmak isterseniz çok rahat kullanabilirsiniz. Bugün sağlıkta hastalık belirtisi manipüle edilebiliyor kötü amaçlar için kullanılabilir bir biyolojik silah olarak bile kullanılabilir."* (Katılımcı 7, 42, Erkek)

Katılımcıların genel olarak vurguladıkları toplumsal değişimlere ve büyük verinin yıkıcı sonuçlarına bakıldığında, ilk olarak bir şeyleri sürekli kolay yoldan yapmanın insanların düşünmeyi unutmalarına sebep olması ve gittikçe kendilerini daha tembel bir konumda bulabilecek olmalarıdır. Hatta bazı katılımcılar bu kolaylığın ve düşünmemenin bir noktada insan zekasını düşürebileceğini bile söylemektedir.

> *"Teknoloji geliştikçe insanların zekâ seviyesinin gerilediğine dair şeyler var ya bir şeyleri daha kolay yapmaya başladıkça daha da yormuyoruz kendimizi daha böyle her şey hazır zaten tüketim toplumu da bunu iyice destekliyor. Bu yüzden de aslında işte bu durumda bizi yönetmek daha kolay hale geliyor. Bir şeyleri sorgulamayı unutmaya başlıyoruz artık."* (Katılımcı 3, 30, Erkek)

> *"En değerli şey şu an. Ulaşabileceğin mesela ben sana data science şeyi versem şu an tezini yapıp bitirirsin herkese ulaşırsın toplu anket bile gönderirsin. En tehlikeli şey bence. Savunma Sanayi'nin bile en önem gösterdiği şey. Çok hızlı aktarılabiliyor. Ben silah kaçırsam, uyuşturucu kaçırsam polis gemiyi tutar falan ama bilgi öyle bir şey değil internetin her yerinde loglanır her yerden ulaşılır. Cloud var mesela. Sen oturup şu an herkesin her şeyine ulaşabilirsin aslında." (Katılımcı 11, 33, Erkek)*

Bu durumla bağlantılı olarak insanların fiziksel şekilde var olarak çevre olaylarıyla, siyasi olaylarla ya da toplumsal herhangi bir durumla ilgili sesini duyurmak yerine artık çok pasif hale geldiği, bunun temel sebebinin ise büyük veri ve gözetim sistemleri olduğu belirtilmektedir. Bu anlamda dijital aktivizmin, post atarak isyan etmenin, çok etkili olmadığı söylenmektedir.

> *"Bütünüyle bireyler kendi görüşlerini oluşturamıyorlar. Kendilerine dayatılanı almak zorundalar. Kapitalist sistem de bunu destekliyor. Biz sürekli yönlendiriyoruz güzel olmak, zayıf olmak, yakışıklı olmak, iyi giyinmek, hep bir şeyi yönlendirme, ya da bir ürün alırken birisi alıyor onun benzerleri bizlerde ya da siyasi anlamda da Akbelen'de ormanlar kesiliyor insanlar oturarak isyan ediyorlar. Post atarak isyan etmememiz gerekli. Orada gidip kolektif bir ortam falan oluşturmanız gerekir. Dolayısıyla şu an manipülatif bir yapı var."* (Katılımcı 14, 26, Erkek)

Bireylerin dijital aktivizmi daha güvenli bulmalarının nedenlerinden bir tanesi de iyice dijitalleşen gözetim sistemlerinde bireylerin anonim kalabilme düşünceleridir. Fakat bir katılımcı görüntü işleme ile artık bireyin anonimliğinin kaybolduğunu ve anonimliğin kaybolmasının da birçok sorunu beraberinde getirebileceğini belirttiği görülmektedir. Sürekli gözetlenerek yaşamak, temelde insanların özgür bir şekilde davranmasını engelleyebilecek bir potansiyelde olup, bireyler sürekli kontrol edilir bir şekilde tavır almaya başlamaktadır.

> *"Görüntü işleme açısından kullanılanlar daha riskli ya da kimlik bilgileri üstünden tutulan verilerin daha riskli olduğunu düşünüyorum. Kimlik numarası, banka numarası bu tarz verilerin kaydediliyor olması daha yıkıcı*

> *sonuçlar oluşturabilir. Ama diğer reklam amaçlı, ürün pazarlama amaçlı olanlar çok sıkıntı değil."* (Katılımcı 2, 28, Kadın)

Diğer bir unsur ise pratiklerin ve alışkanlıkların belirlenerek bireylere sürekli, özellikle ticari alanda, öneriler yapılmasının onları tüketim toplumuna daha çok itmesi, gereksiz harcama ve tüketim pratiklerine yol açabilecek olmasıdır.

> *"Verinin kendisi bir meta bu kesin. Manipüle edici ve kontrol edici olarak zaten kullanılıyor. Mevcut durumda bizim davranışımızı yönlendirmek için kullanılması demek, recommendation sistemleri vs., zaten bu demek. Şu anda tatil için nereye gideceğini sana öneriyor ne dinleyeceğini ne izleyeceğini, yemek sipariş edilen uygulamalarla ne yiyeceğini sana önerilerle sağlıyor. Esasında bir yönlendirme mi bu manipülasyon mu tartışılır. Hem kontrol hem de manipülasyon için bir güç. Zaten verinin çok önemli bir ticari meta olduğu çok net zaten."* (Katılımcı 12, 43, Erkek)

Büyük verinin yıkıcı bir güç olarak görülebileceği diğer bir durum ise sağlık için kullanılan verilerin kalp, şeker, tansiyon gibi hastalıkların kökenlerine inip çıkarım yapmak yerine; bu verilerin ilaç ya da sigorta şirketleri tarafından kendi çıkarlarına kullanım imkânı sağlamasıdır. Nüfus arttıkça sağlık sektörünü daha işlevsel bir hale getirme olanağı sunabilecekken; bireylerin özellikle neyim var uygulaması kullanması ya da hastalığını arama motorlarından tespit etmeye çalışması, oradan çok güvenilir olmayan önerileri uygulamaya çalışmaları ya da sürekli bir hastalıkları olmalarını düşünmeleri bunun risklerinden birkaçı olarak görülmektedir. Sağlık sigortalarının hastalığı olduğu bilinen bireylere sigorta satmamaları ya da daha yüksek fiyata satmaları ya da ilaç şirketlerinin hastalıkları bilerek ilaç fiyatlarını yükseltmesi de bunun sonuçları olarak görülmektedir.

> *"Mesela, insanlarda tansiyon ve şeker hastalığı, kalp hastalığı kaç yaşlarında başlıyor buna yönelik neler yapılabilir ya da bunların kökenlerine nasıl inebilir, bu insanlar daha az hasta olsun ve sağlık sektöründe nüfus arttıkça sağlık sektörünü yoran şeyi optimum seviyeye indirmek için bu tarz şeyler yapılabilir. E nabız böyle bir şey için kullanılabilir ama kötü yönde de bu bilgileri kullanarak ilaç şirketleri hangi ilaçların daha çok kullanılacağını bilip onların fiyatlarını onlara regüle edebilir, fiyatları artırabilir."* (Katılımcı 3, 30, Erkek)

Bir diğer tehlikeli yanı ise insanların tercihlerinin ve hatta kişiliklerinin bilindiği bir düzende yaşamak zorunda kalmalarıdır. İnsanların tüm alışkanlıklarının takip edilerek siyasi görüşlerinin bilinmesi ve bu doğrultuda seçimlerin yönlendirilmesi durumunun da gerçek olduğu bir düzende bireylerin kararlarının da çok kolay bir şekilde etkilenebileceği, duygu durumlarının da bilinip kontrol edilebileceği belirtilmektedir. Bu durum, bireyi manipülasyona açık hale getiren ana unsur olarak gösterilmektedir.

> *"Ben zaten bir sosyal medya platformunda bir şey paylaşacağım zaman onunla ilgili onun koşullarını kabul etmiş oluyorum. Bu da şu anlama geliyor istedikleri gibi işlemelerine izin veriyorum. Hal bu olunca hayatınızla ilgili kişisel verileriniz kullanılması ne kadar kritikse ona göre paylaşmanız gerekiyor. Bu bilinçle paylaşmanız gerekiyor. Yani sizin hayat görüşünüzü, eğilimlerinizi, her türlü eğilimlerinizi, arkadaş çevrenizi, nereye gidip nelerden hoşlandığınızı, seyahat algoritmalarınızın ne olduğunu, neden zevk alıp neden almadığınızı, neye üzülüp neye sevindiğinizi bunu tamamen paylaşımlarınıza dayanarak kendi arkadaşlarınıza açıp tek tek tespit edilebilir. Bu kişi nelerden etkileniyor, neden mutsuz oluyor, mutsuz olduğu günler hangileri ve hangi nedenle mutsuz oluyor o kişiyi de rahatlıkla manipüle edebiliriz."* (Katılımcı 13, 57, Erkek)

Bir katılımcı bu sayede kültürlere has olan evlilik pratiklerinin bile değiştirilebileceğini belirtmektedir.

> *"Çok yüksek bir güç olduğunu düşünüyorum çünkü insanların her türlü davranışı yani yeme içme, evlenme alışkanlıkları, (güler), ne bileyim örneğin yurt dışında evlilik, çok önemsiyor önce herkes beraber yaşıyor ediyor. Sonrasında evlilik aşamasına geliyor. Ya da sadece aralarında bir yüzük taktıklarında biz nişanlandık diyorlar. Ama biz burada konsept kurup nişanlandık diyoruz ya işte bunların zamanla gösterimimin artmasıyla o alışkanlıkları millet değiştirebilir. Aileden, bireysel olarak en sona kadar yani devletin en büyük kısmına kadar belki de değiştirici ve yok edebilişi olacağını düşünüyorum."* (Katılımcı 5, 26, Kadın)

Diğer bölümlerde de katılımcıların farklı noktalarıyla vurguladıkları ve büyük verinin yıkıcı bir güç olarak en çok dikkat çeken noktası onlara göre devletlerin büyük veriyi farklı amaçlarla kullanmalarıdır. Devletlerin bunu bir tür yıkıcı güç olarak kullanması ise katılımcılar tarafından şu şekilde örneklendirilmektedir:

"Çin, büyük veri teknolojileri bakımından dünyanın en iyi ülkelerinden bir tanesi çünkü kullanıcısı çok. Ben kendi yaptığım işlerde de çok sık örnek olarak veriyorum bunu. Oyun sektörü dünyada çok hızlı büyüyor. Çin'de 20 milyonun üzerinde kullanıcısı olan oyun sayısı dediğin zaman 10 binlerle ölçülüyor. Türkiye'de böyle bir oyun yok yakın zaman da belki birkaç tane vardır. 20 milyondan fazladan kullanıcının davranışını anlamaya çalışan 10 binlerce şirket var demek. Kullanıcı sayısı çok fazla olan siyasi tarafta da sistemler çok olduğu için ona yönelik yöntemler, araçlar, teknolojiler çok fazla gelişmiş durumda. Teknolojinin gelişmiş olduğu her yerde de akıllı stratejik davranan kurumlar devlet de olabilir şirketler de olabilir ben bunu kendim için nasıl kullanabilirim diye düşünüyor. O denetim mekanizmalarının Türkiye'de olmayıp orada olmasının sebeplerinden bir tanesi orada bunu yapabilecek hem politik kültür coğrafyası ayrı onların END diye bir bankaları vardı banka kredi vermiyordu kişisel veritasyon üzerinden kredi veriyordu. Para dönmüyordu end üyesi olan şirketler endtoken üzerinden blockchain kullanmıyor ama enddeki reputationları üzerinden işlerini yürütüyorlardı. Zaten bizde de sen para veriyorsun, ben veriyorum ama aynı para dönüyor. Dijital bir değerin dolaştığını düşünebilirsin Çin Hükümeti müdahale etti buna çünkü devletten başka bir kurumun kredi skoru gibi bir skor belirlemesine izin vermedi. Bu yetkinin devlete ait olduğu, bunun paralel bir devlet yapılanması olduğuna karar verdi. O yüzden teknolojiler çok hızlı gelişirken, devletin tabii ki muhafazakâr davranması normal. Demokratik olmayan toplumlarda zaten devletin olduğu her yerde devlet denetime açık değilse gücü kendi bekası için kullanacak bu da beraberinde böyle sistemlerin ortaya çıkmasına sebep olacak. Ben herhangi bir kişiyi insanları sınıflandırıp ona göre politika belirlensin demiyorum ama her yerde kameralar var, aranan bir kişiyi bunlar üzerinden bulmak, takip edebilmek yetkisi becerisi onlarda da vardır ve bunu milli güvenlik çerçevesinde kullanıyorlardır. Diğer tarafta kullanmıyor olabilir. Bu da devletlerin yapılarıyla ilgili. Milli güvenlik sadece suça yönelik değil, milli güvenliğin çerçevesine neyi ne zaman sokmak istediğine bağlı politik güvenlik de bunun içerisine sokulabilir." (Katılımcı 12, 43, Erkek)

4.2. VERİ GÖZETİMİ VE TOPLUMSAL DEĞİŞİMLER

"Veri Gözetimi ve Toplumsal Değişimler" temasının altında, Şekil 6'da yer aldığı haliyle üç kategori belirlenmiştir. İlk kategoride, "Veri Bilimcilerin Gözünden Gözetim", fiziksel gözetim ve dijital gözetim farkındalığı, dijital riskler ve gözetim, "öteki"nin tanımlanması ve gözetim, gözetim ile ulusal ve uluslararası güvenlik ve gözetimi gerçekleştiren kurumlar alt kategorilerine erişilmiştir. İkinci kategoride, "Büyük Veri ve Yeni Gözetim Sistemleri: Kaçmak Mümkün mü?", sistemlere zorunda kalmanın sebebi alt kategorisi belirlenmiş; üçüncü ve son kategoride, "Büyük Veri ve Mahremiyet", dijital gözetimde mahremiyet tanımı alt kategorisinden bahsedilerek ikinci temanın analizi gerçekleştirilmiş, araştırmanın bulguları detaylı bir şekilde yazılmıştır.

Şekil 6. Veri Bilimcilerin Gözünden Gözetim Teması Kategori ve Alt Kategori Şeması

4.2.1. Veri Bilimcilerin Gözünden Gözetim

Lyon'un gözetim konusundaki görüşleri düşünüldüğünde küreselleşen gözetimle video kameralar, otomatik sistemler, elektronik etiketler, DNA örnekleri, kimlik kartları, biyometrik kimlik kartları gibi pek çok "izleme" yöntemi kullanılarak ve yüzler tanınır hale getirilerek, artık tüm bireyler kitlesel olarak gözetlenmektedir. Gözetlenme, çevrimdışı (fiziksel) ve çevrimiçi (sanal) ortamdaki tüm verilerin bir araya getirilmesiyle işlemektedir. Katılımcıların gözetim dendiğinde aklına gelen tanımlar; *"izleniyor hissi, kameralardan insanların ne yaptığını takip etme ve analiz etme"* (Katılımcı 1, 29, Erkek); *"doğrudan bir kişi ya da bir grubun yaptığı şeylerin incelenmesi ya da izlenmesi"* (Katılımcı 4, 26, Kadın); *"büyük datadaki verilerin kontrol amaçlı kullanılması, yapılan eylemlerin belli bir kural ve yükümlülük çerçevesinde tutulup tutulmadığının incelenmesi"* (Katılımcı 2, 28, Kadın); *"belirli kanunlar çerçevesinde belirli kontrollerin yapılması"* (Katılımcı 7, 42, Erkek); *"bir işin doğru yapılıp yapılmadığının izlenmesi"* (Katılımcı 5, 26, Kadın) ya da *"bir şeylerin takip edilmesi"* (Katılımcı 9, 35, Kadın) şeklindedir. Bu tanımlarda bazı katılımcıların fiziksel gözetime, bazılarının ise dijital gözetime vurgu yaptığı görülmektedir. Katılımcıların bazılarının, bu izlemenin belirli bir amacının olduğunu ifade etmesi, bazılarının bu tanımda kanunlara ve yükümlülüklere vurgu yapması ve her birinin bir bireyi, grubu ya da işi izleme ya da takip etme vurgusu yapması önem taşımaktadır. Bir katılımcı ise tüm bu tanımları bir araya getirerek Tesla örneği ile hem gözetimi hem de dijital gözetimi tanımlamakta, ikisinin nasıl bir araya getirildiğini açıklamaktadır:

> *"Bence gözetim hem fiziksel hem dijital olarak aslında her türlü izimizin saklanmasıdır. Şöyle düşünün, mobese kameraları çok ciddi bir gözetim aslında. En yakın örneği de dijital gözetimin, Tesla ile biri kaza yapmış yakın zamanlarda 160 km ile çarptı birisine ve şu an çarpmadığını iddia ediyor. Tesla yetkilileri hız bilgisi lokasyon bilgisi ne kadar süredir hızlı kullandığı hepsi bizde var paylaşabiliriz dava isterse mahkeme isterse diyor. Bu da "digital surveillance" (dijital gözetim) olarak geçer."* (Katılımcı 16, 26, Erkek)

Buradaki örnek aynı zamanda birinci bölümde bahsedilen büyük veri ve yeni gözetim sistemlerinin bir çeşit yeni karar verme kültürü mekanizmasının

merkezinde yer aldığını da örneklendirmektedir. Sadece bununla kalmayıp tüm bireylerin rutinlerinin, kitlesel bir şekilde, her şeyi ve her zaman izleyerek ilerlediği görülmektedir. Kitlesel gözetimle kastedilenin kapitalist düzende bu gözetim araçlarının kullanıldığı, devlet odaklı bürokrasiler ve uluslararası şirketleri de kapsayan bir seviyede iş birliği yapılarak yürütüldüğü, bireylere ait rutinlerin Beck'in de risk toplumunda açıkladığı gibi, risk ile bağlantılı olarak toplandığı ve kullanıldığı düşüncesi öne sürülmektedir. Bir katılımcının eskiden olağandışı durumlarda bireylerin bilgilerinin kaydedildiğini ama günümüzde bunun her an herkesin bilgilerinin kaydedilmesi durumuna dönüştüğü ve asıl gözetimi tanımlayan durumu oluşturduğunu söylemesi dikkat çekmektedir:

> *"Aslında bence bir insanın her anını kaydetmek gibi düşündürüyor bana, gözetim dediğimiz de gözetimde tutmak mesela biz normalde bilgiyi nereden alırız işte ekstra ordinary bir durum olduğunda hani haberlerde topluma ait bir olay olduğunda bunlar bilgi olarak gün yüzüne çıkar ama şu anki durumda herkesin her an bilgileri kaydedildiği için bu artık gözetim oluyor bir yerde."* (Katılımcı 3, 30, Erkek)

Buradaki olağandışılık vurgusunun ise günümüzde kaybolduğu ve Beck'in risk toplumunda açıkladığı şekilde sürekli bir risk olduğu hissi ve bu risklere karşı hazırlıklı olunması için de gözetlenmenin kabul edilmesi durumuna işaret edilmektedir. Artık her şey her zaman olağandışı olabilmekte, bunları bilmek ve önlem almak ise özellikle dijital risklerle daha önemli hale gelmektedir. Beck, risk toplumundan bahsettikten sonra, yeni risk türü olarak dijital özgürlük riskini tanımlamakta ve bunun diğerlerinden farkını henüz felaketle sonuçlanmamış olmasına dayandırmaktadır. Olabilecek felaket ise küresel gözetimin yeni tür eşitsizliklere, hiyerarşilere, emperyalist yapılara olanak sağlama ihtimalidir. Bunların temeline bakıldığında ise özellikle bilgi güvenliği ve veri gizliliği sorunlarının insan haklarını, siyasi özgürlükleri, insan onurunu etkileyebilecek derecede önemli ve sorunsal olmasıdır. Katılımcılardan bir tanesinin çoğunluk etiketlendikten sonra kendisinin de etiketleneceği ve pasaport alma hakkından bile maruz kalacak bir sisteme geçildikten sonra veriyi gizlemenin artık bir mantığı ve yolu olmadığını söylemesi dikkat çekmektedir. Katılımcı, bu

sistemlerin oluşmasına ve büyük veri ile ilgili yanlış güç kullanımına işaret etmektedir.

> *"Dolayısıyla şu anda devlet dönüp Türkiye'nin %92'sini etiketlendiği noktada, benim tüm arkadaşlarım etiketlendikten sonra ben sırf bu verimi gizleyip pasaport alamadıktan sonra verimi gizlemenin çok da bir mantığı kalmıyor. Eğer öyle bir döneme geliyorsak maalesef bu dönemin şartlarına göre oynamamız gerekiyor oyunu. O zaman veri saklama denilen dönem anca filmlerde falan Matrix'te falan gördüğümüz, arka odada yaşayan herkes sakin yerlerde olacak gibi bir şey oluyor. Çok ciddi bir izolasyon gerektiriyor. Tabi ki bu ben çok daha esnek davrandığım için büyük veriyle alakalı yapılacak yanlışların belki ilk kurbanlarından olurum ama son kurbanı olmam yani."* (Katılımcı 16, 26, Erkek)

Risk ile bağlantılı diğer bir unsurun ise ulusal ve uluslararası güvenlik olduğu bilinmektedir. Kitlesel gözetimin genellikle risk ve riskle bağlantılı olarak güvenlik vaadi, modernliğin getirdiği yeni risklerden, "dijital risklerden" bireyleri koruma vaadi taşımasıdır. Bu çerçevede de hem bir grup birey korunurken, onlar için güvenlik sağlanırken, Bigo'nun banoptikonunda bahsedildiği gibi, gözetimin yabancıların profilini çıkarmak, onları marjinalleştirmek ve bu marjinalleştirmenin farklı yaptırımlar uygulamak için kullanılmasıdır. Dijital gözetimin de desteklediği banoptikonda olağanüstü haller rutinleşmekte, profil çıkarma özellikle büyük veri ve yeni gözetim pratikleriyle çok farklı bir hale gelmekte, belirli gruplar dışlanırken belirli gruplar normalleştirilmektedir. Bir katılımcının büyük veri nedir sorusuna verdiği cevap bu durumu doğrudan açıklamaktadır:

> *"Big Brother işte. Kişiyi, kurumları ya da yapıları takip etmek onları sınıflandırmak, kimisini sizden tarafta konuşlandırmak kimisini karşı tarafta bile isteye marjinalize etmek. Bu demek."* (Katılımcı 14, 26, Erkek)

Başka bir katılımcı, bu tür sistemlerde etiğin göz önünde bulundurulup bulundurulmadığından bahsetmiş, kendileri tasarlarken hiçbir ayrımcılığa yol açmayacak modellerde bunu kanıtlamaları gerektiğini, fakat sonrasında ayrımcılık yapıldığını düşündüğünü belirtmiştir. Büyük veri ve yeni gözetim pratiklerinin bu anlamda ayrımcılık yapabileceği ve belirli grupları marjinalleştirebileceği görülmektedir. Aynı katılımcı, farklı bir konudaki soruda

da izin alınmasa bile bazı durumlarda verilerin kullanıldığını ve yasaların özellikle etnisite, cinsiyet, gelir ayrımcılığı gibi durumlara yol açtığını belirtmektedir.

> *"Bu ayrımın yapıldığının bir sürü şey var etik kurul var. Bir etnisiteye diğerinden farklı davranamamak için model geliştirdiğimizde bile bunların birbirinden bağlantısız geliştirildiğini göstermek zorundayım ya da işte cinsiyete göre ayrım yapmadığımızı göstermek zorundayız. Doğduğumuz yere göre ayrım yapmadığımızı göstermek zorundayız. Ama yapılıyor mu gerçekten diye sorarsan bence yapılıyor."* (Katılımcı 6, 36, Kadın)

Başka bir katılımcı ise büyük veri ve sistemlerinin ayrımcılığa nasıl sebep olacağını Türkiye'deki seçim süreciyle açıklarken, beyanının sonunda büyük veri, yapay zekâ, sosyal medya gibi sistemleri atom bombasına benzeterek, onun da iyi bir niyetle ortaya çıktığını fakat kötü birinin eline geçtiği zaman kötü olduğu gibi, bu sistemlerin de aynı şekilde olabileceğini belirttiği görülmektedir. Bunun temeli ise büyük veri ve bu sistemlerin bağlı olduğu gözetim sistemleridir. Önemli noktalardan bir tanesi, katılımcının bunun atom bombasına benzediğini ve hatta kötü amaçlarla kullanılmasının atom parçalamaktan da kolay olduğunu beyan etmesidir.

> *"Kılıçdaroğlu'nun Rusya uyarısı belki de bundandı. Rus arkadaşlarımız bazı şeylere müdahil oluyorsunuz olmayın dedi. Belki bunun içindi ama bunu Amerika da Rusya da yapmış olabilir. Dış devletler de yapabilir bizim kendi hükümetimiz de yapabilir. Sosyal medya, büyük veri, yapay zekâ adına ne dersen de kötü birinin eline geçtiği zaman kötüdür. Atom bombasını bulan da tutup da atom bombasını atın bütün ülkeleri şey yapın demedi daha güçlü bir enerjinin ortaya çıkarılıp dünyanın elektriğe olan bağımlığını yapay yolla ortaya çıkarabilecek güçlerle nasıl yapabilirim noktasını ortaya çıkardı. Hiçbir fizikçi atomu parçalarken bunun bomba olarak birinin başına yarılacağını düşünmez. Ve bu daha kolay atom parçalamaktan daha kolay."* (Katılımcı 10, 37, Erkek)

Bir diğer katılımcı da özellikle devletin vatandaşını izlemesine ve onun hakkında veri toplamasına tepki göstermektedir. Katılımcı, kitlesel gözetimin yanlışlığına, özellikle suça karışmayan bir bireyin verilerine bu kadar kolay ulaşılmaması gerektiğine yönelik tepki göstermektedir. Bu kadar ulaşılabilir veri varken

sınırların olmamasının etik olmadığı ve bunun aynı zamanda kanunen de sıkıntılı olduğu söylenmektedir.

> *"Geçenlerde eski İçişleri Bakanı bir uygulama tanıttı bu videoda, uygulamada kişinin tüm bilgilerine ulaşabiliyoruz dedi ya İçişleri Bakanlığı o kurum mudur? Bence değildir. Onun işi kanunen anayasal bir sınırlamasının yapılması lazım. Bir polis elinde savcıdan izin almadan dalamaz, giremez ya da Millî İstihbarat Teşkilâtı biraz daha özel bir yapı tabi belki onun belki daha farklı prosedürleri vardır. Ama yani benim ismimi girip de tüm bilgim İçişleri Bakanı'nın önüne düşüyorsa bu çok sağlıklı bir uygulama değil. Hem etik değil hem kanunen de sıkıntılı. Benim veri gizliliğimi komple bozmuş oluyorsun, yok etmiş oluyorsun. Savcıdan izin alırsan, savcının da izin vermesi için de belli koşullar olması lazım benim suça karışmış olmam lazım ama normalde yolgeçen hanı gibi veriler."* (Katılımcı 14, 26, Erkek)

Başka bir katılımcı da özel şirketlerin gözetim pratiklerini, pazarlama amacıyla yaptığını fakat devletin bunu yapmasının bir sebebi yoksa ve bu, etiketleme içeriyorsa etik olmadığına vurgu yapmaktadır:

> *"Özel şirketler bunu pazarlama amacıyla yapıyor olabilir ama en azından sebep sonuca oturabiliyor ama devletin detaylı şekilde toplaması tutması kaydetmesi sıkıntılı bir durum. Belki evet bunu etiketleyip de şu an aslında bir yere de varılmıyor. Belki bir devlet kurumuna başvurduğunuzda bu sıkıntı çıkarıyor ama onun dışında sizin günlük hayatınızı etkilemiyor. Tutmasanız da olur bunu yani neden tutasınız neden bir etiket yapasınız. Hiç etik bir yanı yok devlet eliyle bunların toplanmasının."* (Katılımcı 2, 28, Kadın)

Güvenlik temel alınarak belirli ayrımcılık risklerinin ortaya çıkmasının yanı sıra, verilerin denetim, gözetim ve belirli otoritelere itaat riski taşıması da önem arz etmektedir. Bu nedenle, gözetimin özellikle ulusal güvenlikle bağlantılandırıldığı durumlarda, gözetimi açıklamak için onun nedenlerine, söylemlerine ve sonuçlarına bakmak gerekmektedir. Lyon, gözetim çalışmalarında gözetim ve ulusal güvenliği temel alırken denetim ve disipline, yönetim ve yasaklara bakılmalı derken, yeni gözetim pratikleriyle gelişen "kaydolunmuş devletlerde" verilerin başka amaçlar için kullanımının, risk temelli idari yasakların genişlettiğini ve şüphe kategorilerini sürekli yapılandırdığını vurgulamaktadır. Katılımcıların da bir kısmının gözetimi tanımlarken denetim ve otoriteyle

ilişkilendirdiği görülmektedir: *"Gözetim deyince bir kontrol mekanizması, bir izin, bir sanki otoritenin varlığından bahsedebilirim"* (Katılımcı 11, 33, Erkek). Bir katılımcı, şirketlerin yaptığının gözetimin bir türü olmayabileceği, gözetim dendiğinde özellikle kamu üzerinden devletler ve güvenlikle bağlantılı olarak anlaşılabilecek bir kavramın akla geldiğini ifade etmektedir. Bir önceki bölümde yer verilen veri manipülasyonu ve veri ihlali ayrımındaki gibi, şirketlerin yaptığı izleme pratiklerinin gözetim olarak anlaşılmaması gerektiğini düşünmesinin sebebi olarak onların bilgi üzerinden bir strateji üretme hedefleri olmasına karşıt olarak devletin yaptığı izleme pratiklerinde güvenlik ve kontrol edebilme vurgusunun daha çok olmasının bir gözetim türü olarak kabul edilebileceğini belirtmektedir:

> *"Gözetimden benim anladığım, bir kere ben bunu şirketler için, ticaret için gözetim kelimesini kullanmam. Onlar zaten anlama derdindeler gözetleme derdinde değiller. Bilgi üzerinden bir strateji üretme derdindeler. Gözetim deyince bana gözetlemek ve buraya bağlı olarak da güvenlik ve kontrol edebilme vurgusu çok daha fazla geliyor, yönlendirme vurgusu o kadar fazla değilmiş gibi geliyor. Ticari taraftaki büyük veri kullanımları bana çok gözetim gibi gelmiyor ki buna sosyal medya platformları da dahil, Facebook ve benzeri şeylerin de gözetlediğini düşünmüyorum. Bendeki çağrışımı o. Ama gözetim daha çok kamu üzerinden, devletler üzerinden vatandaşları takip edebilme ve güvenlikle ilişkilendirebileceğim bir kavram."* (Katılımcı 12, 43, Erkek)

Katılımcıların gözetimi, özellikle devletlerin bireyler üzerinde bir denetim ya da kontrol sağlamak için bir güç olarak kullanmasının dönüşümüne kuramsal çerçevede de bakıldığında kuramlar panoptik, post-panoptik ve çağdaş kuramlar şeklinde farklı farklı ele almaktadır. Foucault'nun tanımına bakıldığında biyopolitika ile insan bedenlerinin değil, hayatın kendini düzenleme amacıyla, iktidarın doğrudan özneleri hedeflediği bir sistem sağlanmaktadır. Bu dönüşümü açıklarken ise öncelikle devletin merkezi güç olduğu ve yaptırımlar uygulayarak kontrol ettiği, kapatılma kurumlarıyla (hapishane, eğitim, bakımevi, akıl hastanesi gibi) gözetim, kontrol ve mekânsal ayrıştırmanın yapıldığını belirtmektedir. Bu panoptik modelde özneler, gözetlenen özneler olarak normları içselleştirmekte ve egemen iktidarın yaptırımlarını ve merkezi devlet tarafından belirlenen normları kabul etmektedirler. Gözetimin temel amacı,

normlarla disiplini sağlamaktadır. Zorla dayatılan normların birey tarafından içselleştirilmesiyle ise disiplin toplumlarına değil, denetim toplumlarına geçiş yapılmaktadır. Özellikle 20. yüzyıl ile denetim toplumu ve yönetimselliğe dikkat çeken Foucault risklerin doğal kabul edildiği, kontrolün sağlandığı ve yine güvenliğin merkeze alındığı bir sistemle bağlantı kurmaktadır. Beck'in bahsettiği bu risk toplumunda, yukarıda dijital risklerle bağlantılandırıldığı gibi, biyoiktidarla yeni tüketim ilişkileri de şekillendirilmektedir. Disipliner iktidarın yerini, biyoiktidar ve güvenlik almıştır. Biyopolitikanın önemi ise büyük veri ve yeni gözetim pratikleriyle açıklanmaya çalışıldığı gibi, sosyal kontrolü tamamen değiştirmesi ile ilişkilidir. İnsan yaşamının tamamen kontrol altına alındığı, hatta kendilerinin kontrol edilmeyi talep ettiği bir süreç açıklanmaktadır.

Katılımcılara göre, devletin büyük veriyi vatandaşların lehine kullanıp kullanmadığı, bireylerin ya da vatandaşların verilerinin neden toplanıldığı sorulduğunda devletin verileri toplamasının sebepleri; sağlık sistemindeki tüm verilerin aynı portal üzerinde bulunması, birey hastaneye gittiğinde daha önceki kayıtlarının görülebilir olması (Katılımcı 6, 36, Kadın), askeri kurumların insan yürüyüşünü sürekli kaydetmesi suretiyle bu veriyi kullanarak yürüyen robotlar yapılması (Katılımcı 1, 29, Erkek), nüfus artışının tespit edilerek sosyal hizmetlerin (sağlık, eğitim gibi) kullanılması (Katılımcı 5, 26, Kadın), herhangi bir suçun belirlenmesi (Katılımcı 4, 26, Kadın), nüfus, doğum, yaş, iş durumu gibi verilerin tutulması (Katılımcı 2, 28, Kadın) gibi sebepler sıralanmaktadır. Bir katılımcı da kamu otoritelerinin bu sistemleri kullanım amacının neden önemli olduğunu şu şekilde açıklamaktadır:

> *"Şu anda teknoloji kullanımının üst düzeyde olduğu teknoloji devi ülkelerde doğal olarak bu teknolojiler üst düzeyde kullanılıyor. Şimdi esas problem, amaca hizmet ediyor olması. Eğer kamu otoritesi bunu sadece ulusal güvenlik ve toplumsal huzur veya güvenlik olarak kullanıyorsa kötü bir şey değil. Parklarda mesela yeterince aydınlatmanın olması, orada herhangi bir şekilde art niyetli bir kişi çocuğa yaklaştığında onunla ilgili alarm üretebilme gibi bir şey bu kötü bir şey değil. Şu anda çok yaygın olarak kullanılan kadına şiddet ve can güvenliği konusu. Eğer herhangi bir şekilde bir uzaklaştırma kararı alınmış birinin ilgili kadına yaklaştığını tespit edebilecek bir mekanizma olursa belki pek çok kadının hayatı da kurtulabilir. Esas burada konu şu, hangi amaçla, nasıl kullanacağız ve önlemler nasıl*

> *alınacak. Bu önlemleri almak da kamu otoritesinin yükümlülüğünde. Kamu otoritesi bununla ilgili önlemleri kendi ülkesinde vatandaşlarının refahı için kullanacaksa o zaman bununla ilgili hiçbir sıkıntı yok, o zaman biz de sırtımızı yaslarız koltuğumuza deriz ki kişisel verilerimizi toplanıyor mu toplanıyor. Ama bu kişisel veriler sadece ve sadece benim refahım için toplanıyor. Onu söyleyebiliriz. Bununla ilgili endişelerimiz var ise ya da bunun aksini gösterecek şeyler var ise örnekler varsa o sıkıntı."* (Katılımcı 13, 57, Erkek)

Bahsedildiği şekilde, büyük veri ve onun sağladığı gözetim sistemleri iyi bir amaçla kullanıyorsa bireylerin verilerinin toplanmasından rahatsızlık duyulmayacağı ama güçlü grupların kontrol veya manipülasyon amacıyla verileri bir anlamda ihlal ettiği durumların bireyler için sıkıntıya neden olacağı düşünülmektedir. Buradaki temel endişelerden birinin, artık bu sistemlerin yalnızca bir merkezi güç tarafından ve doğrudan hedefleri tespit edilebilecek şekilde ilerlememesidir. Katılımcıların kendi deneyimlerinden yola çıkarak bahsettikleri ile panoptik ve pos-panoptik kuramların bahsettikleri örtüşmektedir. Foucault'nun daha çok merkezi güce dayanan açıklamalarına karşıt geliştirilen post-panoptik kuramlarda Deleuze ve Guattari'nin kontrol toplumlarında kapitalizm ve küreselleşmenin toplumları tamamen değiştirdiğine, Zuboff'un da daha sonra gözetim kapitalizminde bahsettiği gibi, tüm kurumların birer şirket haline geldiğine değinilmektedir. Gözetim kapitalizmine değinildiğinde büyük verinin, ticari amaçlarla bedava hammadde haline gelen verinin, istemli ya da istemsiz kullanılarak sömürüyü, metalaşmayı ve kontrol mekanizmalarını arttırmasından bahsedilmektedir.

Bu sistem içerisindeki kurumlarda ise bireyler bölünmüş birey olarak ele alınarak, yalnızca "veri bankaları" olarak görülmektedir. İktidar, bireyselleştirme ve kitleselleştirme üzerinden işlemekte, imzalar ve sayılar artık bilgiye erişimin olup olmadığını belirleyen parolalar haline gelmekte ve şifreler kodları, kodlar ise kontrol toplumundaki yeni kontrol dilini oluşturmaktadır. Büyük veri bu noktada durumu bir adım daha ileri taşımakta, bireyler hiç olmadığı kadar veri bankası haline gelmekte, kontrolün gücü ve ihtimali hiç olmadığı kadar artmaktadır.

> *"Birinci derecedeki en temel araçlarından bir tanesi büyük veri. Eğer insanları takip etmek istiyorsan, nasıl davrandıklarını takip etmek istiyorsan zaten bu süreç büyük veriyle çalışmanı gerektiriyor. Problemin zaten kendisi sen eğer yeterince karmaşık bir süreci kalabalık bir grubu zaman içerisinde gözetleyeceksen ortaya çıkan data zaten büyük veri olmak zorunda. Tanımı bu. Yeterince büyük, sürekli değişiyor, yapılandırılmamış, arasındaki ilişkiler çok net gözükmüyor. Gözetimin ham maddesi büyük veri oluyor."* (Katılımcı 12, 43, Erkek)

> *"Google'daki verilerin çekilmesi demek, milyarlarca insanın verilerinin çekilmesi anlamına geliyor. Büyük platformlardan çekilmesi bence daha önemli büyük verinin çünkü onlar da böyle yapıyor aslında birinin gelip şahsi olarak benim verilerimi çekmesi çok uğraştırır. Onun yerine toplu alanlarda işte örneğin Facebook, Google, LinkedIn, Amazon, bu gibi firmaların büyük veriyi daha yoğun kullandığını ve daha kolay çektiklerini düşünüyorum. Belki yaş grubuyla alakalı olarak, yaşı ileri olan insanlar çok fazla alışveriş yapmaz ama algoritmaların öyle olduğunu düşünmüyorum. Herkesin bilgilerini çekiyorlar çünkü onlara şey önermesi gerekiyor hani bu kullanıcı hangi ürünlere baktı. Amazon mesela hangi ürünlere baktı, kaç saniye baktı, hangi ürünü ne kadar inceledi bunun yorumlarını inceledi bunları verilerini çekip daha sonra hangi ürünle ilgileniyorsa o ürünlerin reklamını iletiyorlar. Sonuçta onlar ticari bir faaliyet yürüttükleri için neyle ilgileniyorsa onu göstermeye çalışıyorlar."* (Katılımcı 1, 29, Erkek)

Post-panoptik ve bireylerin veri bankaları olarak ele alınmalarıyla, dışsal güç reddedilmekte, Deleuze ve Guattari'nin temel kavramlarından olan arzu ve bastırma temel alınmaktadır. Foucault'da kapalı alanlar, kapatılmış kurumlarla kontrolden bahsedilirken, burada açık alanlar ve noktalardan, uzak mesafeden kontrole dikkat çekilmektedir. Burada erişim noktaları kavramıyla havaalanları ya da sınırlar gibi noktaların önemine vurgu yapılmakta, buna benzer şekilde bir katılımcı da havaalanı örneği ve uzaktan kontrolü şu şekilde açıklamaktadır:

> *"Sosyal medya platformlarına biz zaten algoritmaların geliştirilmesi için kendimiz veriyoruz. İyileştirilebilmesi için de sürekli destekliyoruz onu. Yaş dönümlerimiz de paylaştıklarımız zaman içerisinde neye benzeyeceğimizi sakallı, gözlüklü, saç rengimizi değiştiriyoruz tüm ögeleri zaten veriyoruz bu bizim paylaştıklarımız. Bunun dışında bakıldığında bir ülke içerisindeki bütün gözetim kanallarının hepsini tek bir noktadan güvenlik amaçlı olarak kontrolünü yapmak mümkün. Dükkanları güvenlik amaçlı kameralardan ki o kameraların çoğu ses de kaydediyor, banka kameralarından, bankamatik kameralarından onların da çoğu ses kaydediyor. Tüm AVM'lerin otoparklarında da benzer sistemler var. Ankara'da en azından test amaçlı kullanılan bir yüz tanıma sistemi de var. Başka yerlerde de var. Havalimanları gibi yüksek güvenlikli yerlerde de başka alternatif teknolojiler var. Yurt dışında Amerika'ya gittiğin zaman havaalanında sana 15 dakika ücretsiz wifi kullanma hizmeti verir veya yarım saat oradan bütün verilerini*

> *alabilir. İsviçre'de benzer şekilde bunu yapan bankalar var."* (Katılımcı 13, 57, Erkek)

Katılımcının da bahsettiği gibi hem erişim noktalarından uzaktan kontrol hem de katılımcının bireylerin özellikle sosyal medya platformlarıyla verilerini kendilerinin paylaşması ve algoritmaların, büyük verinin ve yapay zekanın daha da gelişmesini sağlaması kontrol yapılarını daha rizomatik bir hale getirmektedir. Rizomatik yapılarda güç, daha dağınık ve heterojen halde bulunmakta, disipline edici güç yapıları daha akışkanlaşarak, gündelik hayat pratiklerinin farklı noktalarında gömülü hale gelmektedir. Yurt dışına seyahat ettiğinizde hem ulusal hem uluslararası ölçekte biyometrik verileriniz alınmakta, ortak wifiye bağlandığınızda bilgileriniz telefonunuzda ya da bağlantılı araçlarınızda ne varsa açık hale gelmekte, yüz tanıma teknolojileriyle yüzünüz kaydedilmekte, kısaca sizinle ilgili her tür veri, bir tür sayıya ve koda dönüşmüş hale gelmektedir. Bu sadece kitlesel olarak değil, bireysel olarak kişilerin anonim olmadan da verilerinin toplanması anlamına gelmektedir. Rizomatik yapılarda en etkin olarak bahsedilen şey, dijital ve fiziksel gözetimin arasındaki akışın birbirini desteklemesi ve bunun yeni düşünme, eyleme geçme biçimleri üretmesidir. Yoğunluk olarak kavramsallaştırılan bu kavramla bireylerin çevrimiçi olmasa da dijital içerik düşündüğü, iletişim ve etkileşiminin devam ettiği anlamına gelmektedir. Yoğunluk, bireyin rizomun bir parçası haline gelmesi olarak da rizomatik bağlantılar kuramıyla ilişkilenmektedir.

Bogard, Baudrillard'a atıfla, gözetimi bir tür post-panoptik kontrol stratejisi, bir tür simülasyon olarak tanımlarken, veri madenciliği ve bilgi bulutlarına işaret etmektedir. Veri madenciliği ve bilgi bulutları panoptikondaki görünür yerlerin yerini almış, kapılar, kilitler, anahtarla girişin yerini, pin kodları ve şifreleme araçları almıştır. Simüle edilmiş gözetimde kapanmanın yerini alan çok daha fazla teknik ve sosyal araçlar bulunmaktadır. Bu ise kontrolün daha kapsayıcı hale gelmesini, disiplinin siber uzama taşınmasını ve kontrolün daha simüle edilmiş yumuşak biçimlerde işlemesini sağlamaktadır. Simüle edilmiş gözetimde sanal gerçeklik, bilgisayarla profilleme, yapay zekâ ve genetik haritalandırmadan, bugün büyük veri ve yeni gözetim pratiklerinde yumuşak güç

olarak kullanılabilecek tüm araç ve tekniklerden de bahsedilmektedir. Bunlarla kontrol edilen şeyler ise işten cinselliğe, savaştan özel hayata kadar uzanmaktadır. Lupton'un kendi kendini kontrol etme ya da izleme kültüründe bahsettiği ve bu tezde daha önce de örneklendiği gibi, cinsel hayatta bile verilerin toplandığı, kişilerin buna göre performanslarını düzenledikleri ya da bu veriler üzerinden bir sınıflandırma yapılabileceği ve bunun bile bir tür gözetim pratiği haline geldiği görülmektedir. Ya da bir katılımcının da örneklendirdiği gibi büyük veri ve yeni gözetim pratiklerinin alanları çok daha genişlemiş haldedir:

> *"Her türlü tahmin yapılabilir. Yani eve ne alacağınızdan devleti kimin yöneteceğine kadar, bir savaş çıkarsa neyden dolayı çıkabileceğine ve çıkabilecek savaşın ne gibi sonuçlar doğurup doğurmayacağına kadar; nükleer savaş mı olacak yoksa teknolojik bir savaş mı olacak? Bir salgın mı olacak? Deprem mi olacak?"* (Katılımcı 5, 26, Kadın)

Guattari'nin de "paradoksik güvenlik" kavramıyla belirttiği gibi, makine veya Orwelyan tarzda bir makinenin her şeyi izlemesi bu sistemlerle mümkün hale gelmiştir. Paradoksik güvenlikle bir şey olmasa da izlemenin sürmesi ve izlendikçe de kişisel haklar hakkında sorunlar çıkabileceği görülmektedir. Günümüz örneklerine bakıldığında, Çin bir yandan gözetim sistemlerini toplumda bir düzen kurma hedefini öne sürerek "Sosyal Güvenin İnşası" başlığı altında temellendirirken, bir yandan gerçekten düzen mi kurulduğu, bununla çeşitli ayrımcılıkların mı oluşacağı ya da gerçekten ulusal güvenlik amaçlı mı olduğu bir tartışma konusudur. Bir katılımcının da belirttiği şekilde bir anlamda bu sistemlere yapılan vurgu güvenlikle ilgili olsa da kişisel haklarla çelişen noktaya gelebilmektedir. Bireylerin bunu kabullenmesinin sebeplerinden birisi ulusal güvenlik olsa da bir yandan oradaki ulaşımın dengelenmesi, akıllı şehir projelerinin kurulması ya da gerçekten kriminal anlamda suçluların tespit edilmesi sebebiyle de olabilmektedir.

> *"Aslında güvenlikle kişisel haklar tarih boyunca birbiriyle çelişmiştir. Kişisel hakların tüm dünyada evrensel olarak temel insan haklarıyla Birleşmiş Milletlerin tarif ettiği dışında askıya alınabilmesinin koşulu ulusal güvenliktir. Şimdi Çin örneği üzerinden gittiğimiz zaman Çin'de yerel üzerinden insanı sizin kontrol edebilmeniz için bir kaos olmamanız için iyi niyetli yaklaşırsak oradaki trafik lambasından tut da yerleşim yerleri planlamasına şehrin*

> *yüzeyinde hastane benzeri temel sağlık erişimi gibi şeylere yönlendirilmesine kadar bunun gerçek zamanlı tespiti çok kıymetlidir. Hepimiz yaşıyoruz şu an şimdi yaz dönemi geldiğinde bütün turistik bölgedeki belediye başkanları ayağa kalkıyor çünkü kış nüfusu 10.000, afaki konuşuyorum, yaz nüfusu 1 milyon. Hal bu olunca 10 bin kişiye göre tasarlanmış sağlık hizmetleri olabilir, alt yapı olabilir, yol olabilir aklınıza gelebilecek her şey bu anlamda. (Bu gözetim değil.) Kim kimle ne yapar, hangi sıklıkta görüşüyorlar, bununla buluştukları zaman ne tür paylaşımlar yapıyorlar onun dışında görüşmeleri sonrası hangi gruplarla etkileşimdeler bunların tespitini yapıyorsam o tamamen denetim ve gözetimin ötesinde kişisel haklara müdahaledir."* (Katılımcı 13, 57, Erkek)

> *"Ama bunu kötü bir niyetle kullanmak isteseler kötü niyetle kullanabilirler. GPS'ine kadar bütün yolunu biliyor bütün her yerini biliyor. Füzeyi bırakabilir yani çok net. Senin bütün askeri tesislerinin nerede olduğunu biliyor. Detaylı olarak askeri kurallar gereği onlar gizliyorlar. Ama biz mesela çoğu bölgeyi askeri bölge yapıyoruz. Ama orası sağlık noktası mı, orası silah deposu mu, mühimmat deposu mu onu bilmiyor. Askeri kışlanın içinde ne var onu bilmiyor. Ama bunları isterse uydudan izler, izlediği anda biz bunun ne kadarına engelleyebiliyoruz onu bilmiyorum. Ama şöyle düşün Çin'in kullandığı farklı, Amerika'nınki farklı, Rusya'nınki farklı. Rusların hiçbiri Google kullanmaz niye çünkü oradan bilgi almış oluyorsun adam Yahoo kullanıyor."* (Katılımcı 10, 37, Erkek)

Gandy'nin panoptik sınıflandırma olarak gözetim kavramına bakıldığında ise, post-panoptikte olduğu gibi, gücün uzaktan işleyişine vurgu yapılmaktadır. Burada gözetimin boyutu, Haggerty ve Ericson'un, Deleuze ve Guattari'nin kontrol toplumu içerisindeki prensipleri göz önünde bulundurarak gözetleme asamblajının kişilerin ve yaşamların bir replikası haline gelen verilerden (data doubles) bahsedilmektedir. Şu an bir diğer önemli gelişme olan metaverse'ün de tartışma yaratması gibi, kişilerin birer replikasının onlardan toplanan verilerle metaverse dünyası üzerinde taşımasının ve yaşamasının bu durumun yönetim, güç, kontrol temelinde nasıl etki edeceği konuşulmaktadır. Katılımcının gözetimle ilgili sorulara doğrudan metaversete yaratılan kopyalardan bahsederek verdiği cevabı şu şekildedir:

> *"Metaversete bizim kopyalarımız yaratılabilir. Hatta şu anda alınan ses kayıtlarının ve arkadaşımızsın diye güveniyorum ama normalde şey çalışmaları da var. Ses kayıtlarını tınısını frekans bandında bu ilerleyen aşamalarda tam bir ses alındıktan sonra sen bir mikrofona konuştuktan sonra oradan benim sesim çıkabilir. Teknolojik olarak bunlar zaten yapılıyor aynısını yapay zekayla benim kişilik analizimin tavırlarımın tarzımın çıkarılıp daha sonra sesimle birleştirildikten sonra metaverse ortamında üç boyutlu bir kopyası yaratılabilir. Fiziksel ortamda da bir kopyaya dönebilir bu.*

> *Sonuçta bugün teknoloji gerçekten gelişiyor ve şu an bence çağ atlama seviyesinde bugün baypas yapıyorlar. Biyolojik olarak yapay kalp yapıyorlar. İnsan organlarının hepsini yapabiliyorlar. Sadece duygu kısımlarından çok emin değilim çünkü bir yapay zekada olsa, sanal bir şey de olsa, duygusal olabilir mi çok fazla fikir yürütemiyorum ama biyolojik olarak birebir benim aynı kopyam yapılabilir ve benim yaşam tarzım içerisinde gelişmiş bir şekilde benim kopyamı yapabilirler diye düşünüyorum."* (Katılımcı 1, 29, Erkek)

Panoptik tasnifte tam olarak bireylerin kopyalarının yaratılarak onların fiziki dünyada da geliştirilerek kontrol edilmesinden bahsedilmese de panoptik sınıflandırma için yapılması gereken kimlik saptama, sınıflandırma ve değerlendirme, temelde belirli tipler oluşturma süreçlerinin hepsinin yapılabildiğinin bir göstergesidir. Sınıflandırma, doğrudan bireylerin gelecek davranışları hakkında belirsizliği en aza indirerek onların davranışlarını manipüle etme ve bazı durumlarda kontrol etme hedefi içermektedir. Panoptik tasnifle yapılan en büyük vurgulardan bir tanesi ise, şirket ve hükümet iş birliği üzerinedir. Bunun bireysel mahremiyete karşı çok büyük bir tehdit olabileceği, rutin olarak sınıflandırmanın ciddi bir kurumsal güce dönüşebileceği belirtilmektedir. Büyük veriyi kullanan güç denildiğinde aklınıza ilk hangi kurum ya da birey gelir sorusuna teknoloji üretici kuruluşlar diyen bir katılımcı şirket ve hükümet iş birliği olanağını şu şekilde ifade etmektedir. Katılımcının büyük verinin gidişatını o her şeyi bilir ve görür denen noktaya geliniyor şeklinde ifadesi ise çok önemli bir vurgu olarak görülmektedir.

> *"Teknoloji üretici kuruluşlar. Zaten bütün veri ulaşımı onlar üzerinden yapılıyor. Bizim en mahrem verilerimizi bile biz o firmaların geliştirdiği teknolojiler üzerine koyuyoruz. Kamu otoritesi dahil çünkü o verileri elektronik ortamda tutuyoruz, orada gün sonunda onunla ilgili bir veri sorumluluğu teknoloji üreticisi firmalarda. Çin'de Microsoft ürünlerinin kullanımı yasaktır. Bunun hikayesi de şu, 2000li yıllarda Microsoft Office ve Windows işletim sistemleriyle ilgili teknik dokümanları ki yazılımda hangi bileşimde neye hizmet eder bunun verilmesi gerekiyor. Orada hem Windows işletim sistemi hem de Office programlarında neye hizmet ettiği belli olmayan dosyaların açıklamasını istedi Microsoft'tan. Microsoft da bunu vermeyi reddetti. Çin'de Google da kullanılmaz mesela, ayrı arama motoru var. WhatsApp da kullanılmaz, Google'da kullanılmaz, dolayısıyla Çin en azından kendisi ve kendi etkisindeki ülkelerle ilgili verileri muhafaza eder durumda şu an. Ama diğer taraftan baktığımızda dünyanın geri kalan ülkelerinin tamamı en azından şimdilik birden fazla farklı veri platformu kullandığı için kişisel verilerin tamamı tek bir havuzda birleşiyor. Teorik*

> *olarak bugün bir kilisede dünyadaki bütün verilere erişme şansı var, dolayısıyla bir kişinin dünyadaki tüm verilere sahip olması demek, bu kişinin aslında dünyadaki bütün insanları yalnız günlük davranışları değil, gelecekteki davranışlarını da ne kadar yaşayacakları ne zaman ölecekleri dahil bilgiye sahip olması demek. Biraz felsefi olarak gidersek o her şeyi bilir ve görür denen noktaya geliniyor demektir."* (Katılımcı 13, 57, Erkek)

Bu tür bir iş birliğinin Türkiye'de nasıl kullanıldığını ya da kullanılabileceğini yorumlayan başka bir katılımcının yorumu ise şu şekildedir:

> *"Türkiye'de İçişleri Bakanlığı kullanıyordur zaten. Veri bilimi de var onun içinde ve aslında biz T.C. vatandaşı olarak Mobese de kaydolmayı yapıyoruz…Hadi gel sana bakalım dedi ya. O kişiye bir veri ihlali olmuş olabilir. Diğeri kendi içinde kaldığı sürece veri manipülasyonu olabilir. Eğer sadece Mobese kameralarını kullandıysa ki kesin kullanmamışlardır, kesin Instagram Facebook fotoğraflar her şey var. Bir sistemde böyle bir makine öğrenmesi kurarken veri bilimi projesi yaparken üç dört parçaya ayırabilirsiniz projenizi. Siz bana Çin böyle bir şey yapıyor biz nasıl yaparız deseniz. Ya önce bir skorlamaya bakacağız ve diyeceğiz ki Ayşe'yi tanıdık nasıl skorlayacağız. Önce bunu bir çözelim bir de Ayşe'yi tanımayı çözelim. İçişleri Bakanlığı'nın yaptığı Ayşe'yi tanımayı çözmek, skorlama mantığını da çözdükleri anda iki modeli birleştirerek direk canlı olarak... Şu bile olur bu cyberpunk bir hayal ya da distopya da bir gözlük taktığınızı düşünün sizin skorunuzu ya da uygulamadan sizi görebileceğimiz bir yapı olacak yani bunu bir tık daha ilerletip parti mensubu olduğunuzu falan da yazarlar. Türkiye'de bunlar olur. İşte hangi partiye üyesiniz." (Katılımcı 16, 26, Erkek)*

Marx'ın da belirttiği gibi, yeni gözetim ve tehditlere karşı sınıflandırma, kategorik baştan çıkarma ise potansiyel tüketicileri belirli amaçlara göre sınıflandırmayı hedeflemektedir.

4.2.2. Büyük Veri ve Yeni Gözetim Sistemleri: Kaçmak Mümkün mü?

Veri bilimcilerin gözetime bakış açılarının ilk bölümle de bağlantılı olarak tüketici pratiklerini belirlemekten, devletlerin vatandaşlarını kontrol etmesine, bireylerin metaversete sanal dünyalarının yaratılmasına, ayrımcı sistemler kurulmasına ve daha birçok noktaya değinen şekilde ilerlediği ve çok kapsamlı olduğu görülmektedir. Özellikle dezavantajlı noktalarına değinildiğinde, katılımcıların bu sistemler hakkında en çok bilgi sahibi olan kişiler olduğu düşünüldüğünde, bu

sistemlerden kaçmak mümkün müdür sorusuna farklı şekillerde yaklaştıkları anlaşılmaktadır.

Katılımcıların gözetimden uzak durmak ya da kaçmak konusundaki görüşlerine bakıldığındaysa; genel anlamda hepsi bunun mümkün olmadığı konusunda görüş bildirmişlerdir. Katılımcılar bunun sebeplerini: telefonların WhatsApp'ın serverlarına direk kaydolması (Katılımcı 7, 42, Erkek), görüntü işlemenin gelişmesi, e-ticaret siteleri, mail kullanmak, araştırma yapmak (Katılımcı 3, 30, Erkek), iş yerlerinin özellikle salgın hastalıklarla birlikte çevrimiçi platformları zorunlu kılması, banka işlemleri için veri vermek zorunda kalınması (Katılımcı 9, 35, Kadın), eğitimin de dijitalleşmesiyle küçük yaştan itibaren tablet ve telefon kullanımının artması ve küçük yaşta dijital sistemlerin kullanımının artması, salgının bunu hem ulusal hem uluslararası anlamda arttırması, bu sistemler kullanılırken bilinçli olunmadan tüm çerezlerin, onay metinlerinin kabul edilmesi ve incelenmemesi, daha uygun ya da ücretsiz olduğu için lisanssız program kullanımına yönelinmesi ve ücretin bireyin kendi verisi üzerinden alınması (Katılımcı 10, 37, Erkek) gibi pek çok alan ve veri paylaşım pratikleriyle sıralamaktadırlar. Katılımcılardan bir tanesi ise en çok kullanılan alanı ve bu sistemlerden neden kaçılamadığını günlük pratikler üzerinden şu şekilde ifade etmektedir:

> *"Bu sistemden kaçmak artık pek mümkün değil. Şöyle mümkün değil. Tabii ki biz kendi verilerimizi satarak AI bir uygulamayı kullanıyorsanız ve uygulama çok iyiyse ve aslında ücretsizse o uygulama başka bir şeyler alıyordur sizden hani böyle bir şey var gerçekten. Her şeyin bir karşılığı var zamanla biz o kolaylığı tercih ediyoruz. Her şeye tek tıkla ulaşıyoruz telefonlar var hayatımızın çok büyük bir parçası. Bütün gündemi takip ediyoruz haberleri takip ediyoruz. Birçok şeyi oradan yapıyoruz ve karşılığında da bir şeyler evet feda edilmesi gerekiyor. Ama onun dışında ondan kaçmanın tabii ki yoları var. Mesela mobil bankacılık sistemleri o da son zamanlarda çok gelişti ve artık NFC teknolojileri bile geldi telefonla kredi kartıymış gibi ödeme yapma, QR kodlar var falan. Onları düşününce aslında yani tabii ki bunların sızıntıya açık olma ihtimali de çok yüksek ve bizim bilgilerimiz her an başka bir yere geçiyor olabilir. Bunun çözümü mobil bankacılık kullanmamak ama onu kullanmadığımızda her şey için bankaya gitmemiz gerekir sürekli ya da ATM'ye uğramamız gerekir gibi şeyler var. Ya da artık online alışveriş çok moda oldu ki ben de çok fazla kullanıyorum o durumda da şu var biz telefondan evimizden şeyi söylüyoruz ve ertesi gün sonraki gün kapımıza geliyor. Diğer şeyi*

> *düşündüğümüzde biz eskiden gidip AVM'ye mağazaya girip diğerine girip fiyatlarına gidip başka bir AVM'ye gidiyorduk belki vs. sonra alıyorduk ama zaten şimdi bunların hepsini telefondan yapabiliyoruz. İnternet sitelerinden bakabiliyoruz. Alışveriş sitelerini karşılaştırmak da çok kolay bunları tabii ki bu kolaylıkları yaparken bu uygulamalara da verilerimizi veriyoruz. Fotoğraflara ulaşmasa bile, bilgilere ulaşıyordur."* (Katılımcı 3, 30, Erkek)

Bir önceki bölümde gözetimin genellikle risk, ulusal güvenlik ve devletler ile özellikle uluslararası şirketler ve pazarlama pratikleri ile bağlantılandırıldığı dikkat çekerken, katılımcılara doğrudan verilere ulaşmak isteyen kurum, kişi ya da güç denildiğinde ilk olarak akıllarına ne geldiğine yönelik bir soru yöneltilmiştir. Bu kısımda da bir kısmının özellikle şirketlere, bir kısmının devlete, daha büyük bir kısmının ise hem devlet hem özel şirketlere vurgu yaptığı görülmektedir. Devlet bağlantılı açıklama yapan katılımcıların gözetimi, özellikle istihbarat birimleriyle, güvenlikle bağlantılandırdığı görülmektedir.

> *"İstihbarat geliyor yurtdışındaki pentagonlar, FBI'lar geliyor hani ulaşamayacakları herhangi bir bilginin olmadığını düşünüyorum. Sadece suçlulara yönelik değil, suçlu aradıkları kişiler ile ilgili de olabilir. Şu an mesela seçim dönemindeyiz. Seçim döneminde ben x partisinden x kişisi aday mesela ben şu ana kadar onun hiç suçunu araştırmadım. Ama şu an geçmişe dönük olarak Twitter 'da attığı bir tweeti, sildiği bir tweeti, girdiği bir siteyi, aktardığı bir parayı, kimsenin bir bilgisinin olmadığı video kaydını, ses kaydını olduğu gibi çıkarabiliyorum. Ama hani MİT ve FBI dışında o bilgiye en çok kimin ihtiyacı varsa parası olan en çok kim ise onlar kullanıyordur diye düşünüyorum."* (Katılımcı 5, 26, Kadın)

> *"Devlet geliyor çünkü zaten elinde her verisi var. Devlet kullanırken aynı yasal izin süreci işletilmiyor ve işletilmediği çok belli. Ben daha önce bir devlet kurumuna modelleme yaptım ve o kurumun elinde şu anda herkesin her verisi olabilir çünkü bütün devlet kurumlarından veri aktarıyordu. Ve kimseyle şahıs şirketlerinin kimseyle paylaşmadığı bilançolar mesela. Bu konudaki güçlü olan otoriteler."* (Katılımcı 6, 36, Kadın)

> *"En basit bir örnekle devlet kurumlarında çalışan kişi bu verilere erişebiliyor. Bu sistem burada çalışan herkesin ulaşabileceği bir noktada."* (Katılımcı 4, 26, Kadın)

Gözetimi özel şirketlerle bağlantılandıran katılımcıların, özellikle bunun bir tür gözetim olmayabileceğini ve pazarlama amacıyla bu şirketlerin, dolayısıyla bireylerin pratiklerini bilmek ve tahmin etmek isteyeceğini düşündükleri dikkat çekmektedir.

> *"Benim elimde milyonlarca kişinin verisi olması, benim için hiçbir anlam ifade etmez. Çünkü bu şekilde bir veriyi kullanmam gerekiyor. Ayırmam gerekiyor. Anlamlandırmam gerekiyor. Bunu da niye isterim böyle bir şey yapmak isterim sonucunda bana bir şey vermesi gerekiyor. Örneğin kişilik analizi, hangi ürünlerle ilgileniyor, nerelerde fazla vakit geçiriyor, hangi tarz giyinmeyi seviyor ki, eğer tekstille uğraşıyorsam ağırlıklı olarak insanların ne tür giyimlerden hoşlandıklarını bilmek isterim. Devlet olsam bir insanın şüpheli mi değil mi benim için bir risk oluşturuyor mu onu öğrenmek isterim. Bir ayakkabı firmasıysam hangi ayakkabıları giydiğini öğrenmek isterim."* (Katılımcı 1, 29, Erkek)

> *"Yeterince karmaşık operasyon gösteren tüm organizasyonun böyle bir isteği ve niyeti var. Devletin zaten biz vatandaşlık bağıyla tabii olduğumuz için o zaten doğal olarak kendinde bir hak görüyor benim bilgimi kullanmaya, nerde yediğimi ne yaptığımı ne içtiğimi. Bu bir devletin hakkı mı tartışılır tabi ama o taraftaki bakış o zaten. Diğer tarafta da eğer ben bir müşteri grubunu temsil ediyorsam, bir şirket için doğal olarak nasıl mal satarım, nasıl kendi ürünümü ona ulaştırırım, nasıl onu daha uzun süre tutarım diye hedefleyecek tabii ki."* (Katılımcı 12, 43, Erkek)

Buna ek olarak, katılımcıların bir kısmı, büyük verinin gittikçe artan bir şekilde veri toplamaya devam edeceğini ve yeni sistemlerin kurulmaya devam ettiğini vurgulamaktadır. Yeni sistemler ve büyük verinin gözetim anlamında gelişimine vurgu yapıldığında iki temel kavram vurgulanmaktadır: Yapay Zekâ (AI-Artificial Intelligence) ve özelde ChatGPT'dir. Katılımcılardan bir tanesi, yeni sistemlerin gelişimini özellikle depolama sistemlerinin artmasına dayandırarak, Amazon'un serverlarını okyanus altına döşemeye başladığını ve daha çok veri toplamak için farklı şirketler ya da kurumlarda da aynısının olabileceğini belirtmektedir. Buradaki temel vurgu toplama, işleme ve depolamanın artması için gerekli altyapıların daha da genişletilmesidir.

> *"Yeni sistemler var bence. Şöyle ki yeni sistemlerden kasıt depolama sistemlerinin artırılmasına yönelik şeyler. Mesela, Amazon serverlarını okyanus altına döşemeye başladı ve ciddi anlamda çok fazla veri depolayacak bir kapasiteleri olmaya başladı. Bu sadece bir şirketi bütün dünya genelinde düşündüğümüzde ve eskiye nazaran ilk bilgisayar resimleri böyle bütün odada falan hani 3mblık bir hafızası varmış falan. Şu an çok komik yani. Mikro sdler falan var bir terebaytlık bunları düşündükçe depolanabilecek verinin sonu yok. Bunları optimum seviyede verinin çok yer kaplamadan enkripte edilip depolanacağı bir şey kesin çalışılıyordur bence bunlar var. Onun dışında AI yapay zekanın gelişimiyle birkaç şeyin daha kolaylaşmaya başlaması aynı şekilde kolaylaştıran bir şeye dönüştürüyor. Gözetim anlamında da."* (Katılımcı 3, 30, Erkek)

Başka bir katılımcı ise özellikle büyük verinin tahminleme ve dolaylı olarak veri manipülasyonundaki atılımını ChatGPT ve Elon Musk'ın robot projeleriyle açıklamaktadır. Katılımcının bu sistemler arttıkça verilere demokratik ulaşımda bir tehlike olabileceğine vurgusu ise dikkat çekmektedir.

> *"Tahminlemeye girince zaten ChatGPT ile yapay zekâ ile inanılmaz bir atılım var. Birçok konuda birçok tespitte şu anda inanılmaz bir yöne gidiyor. Elon Musk'ın robot projeleri bile büyük veri sayesinde bazı şeyleri anlamlandırıyorlar. Otonom araçlar mesela. Bunlar mesela gerçekten büyük atılımlar. Gözetim ne derseniz, bu konuda işte gerçekten belli kanunların oluşturulması gerekiyor çünkü bu verilere hem ulaşımın hem de demokratik bir şekilde kullanılması gerekli. Birinin gücünde olmamalı. Teknoloji kimsenin güdümünde olmamalı. O şekilde tarifleyebilirim. Konsensus olarak kanunların belirlenmesi gerekiyor."* (Katılımcı 7, 42, Erkek)

4.2.3. Büyük Veri ve Mahremiyet

Bahsedilen gözetim pratikleriyle ilgili olarak literatürde en çok vurgulanan ve tehlike olarak görülen unsurlardan bir tanesi mahremiyetin kayboluşu ya da hasara uğramasıdır. Ontolojik güvenlik anlamında bakıldığında da mahremiyetin dönüşümüyle, özellikle dijital sistemler geliştikçe kamusal alan ile özel alan arasındaki ayrımın bulanıklaşması, zaman mekân algısının yok olması gibi pek çok durum mahremiyetin çerçevesinin değişmesine sebep olmuştur. Katılımcılara özellikle bu sistemler içerisinde yaşayan, onu üreten, bilen aynı zamanda da kontrol edebilen bireyler olarak mahremiyetin onlar için ne ifade ettiği sorusu yöneltilmiştir.

Bir katılımcı mahremiyetin kişilerin ne aldığı, yediği, hangi ürünleri kullandığı değil, aksine özellikle "evinin" içerisinde olan şeylerin toplanmasının mahremiyet ihlali olduğunu belirtmektedir (Katılımcı 1, 29, Erkek). Başka bir katılımcı ise hem beden hem ev ve temelde evin özel alan olarak tanımlanması ile mahremiyeti açıklamaktadır. Bir başka katılımcı ise mahremiyet ile "mahrem" kelimesine de atıfta bulunarak bireylerin bedeninin istediği yerlerini göstermesi ve istemediği yerlerini kapatması diye tanımlarken bunun fiziksel anlamda mahremiyet olduğunu söylemektedir. Bunun dışında "evin" içerisinde olan

şeylerin mahremiyete gireceği vurgusu yapılmaktadır (Katılımcı 3, 30, Erkek). Katılımcıların verdiği örneklere bakıldığında, dijital cihazların fiziki gözetim ya da sanal gözetim araçlarının evin içine de dahil olmasıyla evin de bir özel alan olmaktan çıktığı öne sürülmektedir. Robot süpürge örneğini kullanarak ilk kullanılmaya başladığında üzerinde kamera olduğu ya da evlerin haritalarını uygulamayı ya da sistemleri geliştirmek amacıyla da olsa göndereceği düşüncesiyle ilgili mahremiyete yönelik endişe uyandırdığını söylemektedir. Bu, küresel ölçekte düşünüldüğünde ülkeler bazında Kuzey Kore ya da Çin'in Google Maps üzerinden kendi "mahremiyetini" korumak için, bir savaş durumunda dezavantajlı konuma geçmek istemedikleri için Google Maps'i kullandırmadıkları örneğiyle anlatılmaktadır. Burada mahremiyetin her ölçekte kişiler, yerler, ülkeler ve uluslararası platformlarda ihlal edilmesinden korkulan ve dijital gözetimle birlikte daha da ciddi tehlikeler içeren bir şey haline geldiği örneklendirilmektedir. Bir anlamda vurgu bu noktada kişisel verilere ve ülkelerin gizli verilerine, "gizliliğe", kaymaktadır. Katılımcıların bir kısmının mahremiyetle ilgili cevapları da gizliliğe değinmektedir.

Gizlilik anlamında bakıldığında, kişisel bilgilerin dijital gözetim sistemleriyle, bireyin onayı olmadan ya da bilinçsiz kullanımıyla paylaşımı akla gelmektedir. Başka bir katılımcı için ise mahremiyet, kişinin paylaşmak istemediği kişisel bilgiler olarak tanımlamaktadır, katılımcının özellikle bu bilgileri paylaşıp paylaşmama konusunun kişinin rızasına dayalı olması vurgusu dikkat çekmektedir (Katılımcı 2, 28, Kadın).

> *"Kişilik sınırlarınıza ne giriyorsa, mizacınıza sizin rızanız olmadan başkalarının bilmemesi gerektiği her şey. Büyük veri, bu veriyi almaya çalışabilir. Artık o kimse veriyi almaya çalışan. Telefon mesela büyük veriyi kaydeden bir alet. Bu telefonu nasıl kullandığımıza da bağlı. Bilinçli ya da bilinçsiz… kaydeder girer bir yerlere gönderir."* (Katılımcı 7, 42, Erkek)
>
> *"Kişinin paylaşmak isteyeceği kadarını başkalarıyla paylaşmasıdır. Onun dışındakiler kendine kalandır."* (Katılımcı 8, 29, Kadın)

Bir katılımcı ise bir uzman olarak önemli bir noktaya değinerek, önce mahremiyetin kişiye göre tanımlanan bir şey olduğunu ve kimsenin bireye zorla

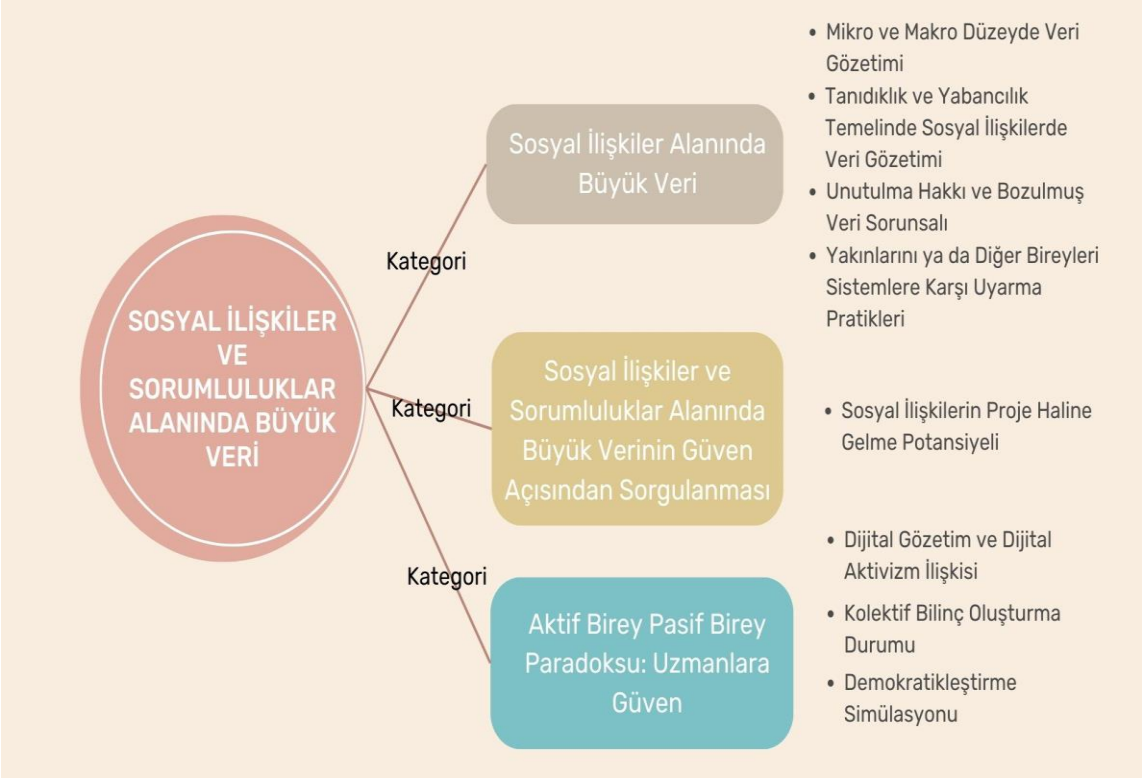
bunları paylaşmayı dayatamayacağını belirmektedir. Büyük verinin de bireyin paylaştığı verileri toplayan ve onların işlemlemesini açıklayan bir kavram olduğunu belirterek, bunlarla bireylere ya da vatandaşlara yönelik bir yaptırım olduğu zaman sorun olacağını belirtmektedir.

> *"Mahremiyet, göreli bir kavram bana göre. Kişinin kendisiyle ilgili özel kalmasını istediği her şey mahremiyettir. Bu bir insan için hangi arkadaşlarıyla gittiği mekân, görüştüğü arkadaşlar da olabilir, yediği içtiği de olabilir, ailesiyle ne yaptığı da olabilir, kimi insan için de sadece çıplak fotoğrafları olabilir, özel görüntüleri olabilir. Kimi insan için de düşünceleri olabilir. Dolayısıyla kişinin önce mahremini kendisine göre tanımlaması ve paylaşımlarını ona göre yapması gerekiyor. Bana göre en mahrem olan şey insanın beynidir. Aslında her şeyi çekip çeviren ve her şeyi açık eden odur. Aslında mahrem olan insanın düşüncesidir. Baktığımızda kimse düşüncesini açık etmek zorunda bırakılamaz. İnsan haklarına baktığımızda da. Paylaşıyorsak veyahut bizim düşüncelerimizin hangi yönde eğilimde olduğu bizim kim olduğumuz ise şu an tespit ediliyor ve biliniyor. Büyük veri bunu ihlal etmez, sadece bizim paylaştığımız verileri toplayıp onların işlenmesidir. Ne zaman ki o kişisel verilerle Çin'de yapıldığı gibi bir puanlama yapılıyorsa sorun büyük demektir."* (Katılımcı 13, 57, Erkek)

4.3. SOSYAL İLİŞKİLER VE SORUMLULUKLAR ALANINDA BÜYÜK VERİ

"Sosyal İlişkiler ve Sorumluluklar Alanında Büyük Veri" temasının altında, Şekil 7'de yer aldığı haliyle üç kategori belirlenmiştir. İlk kategoride, "Sosyal İlişkiler Alanında Büyük Veri", mikro ve makro düzeyde veri gözetimi, tanıdıklık ve yabancılık temelinde sosyal ilişkilerde veri gözetimi, unutulma hakkı ve bozulmuş veri sorunsalı, yakınlarını ya da diğer bireyleri sistemlere karşı uyarma pratikleri alt kategorilerine erişilmiştir. İkinci kategoride, "Sosyal İlişkiler ve Sorumluluklar Alanında Büyük Verinin Güven Açısından Sorgulanması", sosyal ilişkilerin proje haline gelme potansiyeli alt kategorisi belirlenmiş; üçüncü ve son kategoride, "Aktif Birey Pasif Birey Paradoksu: Uzmanlara Güven", dijital gözetim ve dijital aktivizm ilişkisi, kolektif bilinç oluşturma durumu, demokratikleşme simülasyonu alt kategorilerinden bahsedilerek üçüncü temanın analizi gerçekleştirilmiş, araştırmanın bulguları detaylı bir şekilde yazılmıştır.

Şekil 7. Sosyal İlişkiler ve Sorumluluklar Alanında Büyük Veri Teması Kategori ve Alt Kategori Şeması



4.3.1. Sosyal İlişkiler Alanında Büyük Veri

Büyük verinin ilk iki bölümde incelenen özelliklerinin yanı sıra, özellikle bireylerin sosyal ilişkilerinde de ciddi değişimlere sebep olabileceği ve hatta bireylerin ilişki kurarken, bir sonraki "Ontolojik Güvenlik" başlığında tartışılacağı gibi, sosyal ilişkilerde soyut sistemlere güvenebilecekleri düşünülmektedir. Bu sebeple veri bilimcilerin sosyal ilişkiler alanında, tanıştıkları kişilerle ilgili büyük veriye ya da veri gözetimine ne derece başvurdukları anlaşılmaya çalışılmıştır. Bu anlamda veri bilimcilerin çok ciddi bir ayrıma gittiği görülmektedir. Veri bilimcilerin bir kısmı tanıdıkları kişilerle ilişkilerinde doğrudan arama motoru ve sosyal medya platformlarını kullanırken, diğer bir kısmının bu platformlardan uzak durduğu görülmektedir.

İlk gruba bakıldığında, *"Sosyal medyaya girerim, zaten hemen stalklarım. Twitter'da attığı Twitter, geçmişi, beğendikleri, arkadaşları, neyi takip ettiği hepsine bakarım"* (Katılımcı 4, 26, Kadın); "*Tabi hepsine bakarım. Önce Instagram'a bakarım. Sonra Google'a bakarım. Görsellerden başlamak üzere tek tek nerede okumuş, nerede bulunmuş, tek tek bakarım. Oradan nerede çalıştığına ne zamandır çalıştığına ne gibi çalışmalar yaptığına bakarım. Her yerden bakarım yani. LinkedIn, yani çünkü orada insanlar işe girmek için ya da iş seçeneklerini arttırmak için çok fazla yalan söylemiyorlar. Çünkü orada onaylaman gereken şeyler var."* (Katılımcı 5, 26, Kadın) gibi cevaplar dikkat çekmektedir. Katılımcıların genelinde dikkat çeken bir bilgi ise, daha çok kariyer odaklı olan LinkedIn'in daha ciddi bulunması, katılımcılar tarafından en vazgeçilemeyecek uygulama olarak görülmesi ve onlar tarafından daha güvenilir bulunmasıdır. Facebook'un ise daha eski, geleneksel ya da artık kullanılmayan bir platform olarak görülmesi nedeniyle bu tür aramalar için çok ideal bulunmadığı katılımcılar tarafından ifade edilmektedir. Katılımcıların bazılarının özellikle iş hayatında tanıştıkları bireyler için LinkedIn; sosyal hayat için ise Instagram, Google ya da Facebook gibi sosyal ağ ya da arama motorlarını kullandıkları görülmektedir. Katılımcılar bunu şu şekilde ifade etmektedir: "*Bakarım kesin yani biriyle toplantım varsa öncesinde kesin*

bakarım. LinkedIn'ine bakarım, Instagram'ına bakarım, Facebook'a bakarım Googlelarım kesinlikle bakarım. İşle ilgiliyse LinkedIn ama sosyal hayatsa Instagram ya da Google" (Katılımcı 6, 36, Kadın). Özellikle iş ile ilgili bağlantılarda Google bağlantıları ve LinkedIn'in kişilerin ilk intibaları için önemli görülmekte ve genellikle iki platform verileri doğrulamak ve emin olmak için kullanılmaktadır.

> *"Genelde iş amaçlı birileriyle tanışıyorum genelde de arama motorundan arama yaparım. Sosyal medyayı ben de çok aktif kullanmadığım için sosyal medya üzerinden bir araştırma yapma ihtiyacı duymam yapmam da. LinkedIn'den daha çok o kişiyle ilgili en fazla bilgiyi arama motorundan bakarak bilgi sahibi olurum çünkü LinkedIn'de daha çok kendi tariflediği paylaşımlar var ama arama motorunda geçmişine de dair her şey var veya yok. Bilgi varsa problem yok kişiyle ilgili hiçbir bilgi yoksa problem var. Güven duymama engel olmaz ama karşı tarafa sorarım. Dijital ortamda yaratılmış olan hiçbir veri iz bırakmadan ortadan kaybolamaz mümkün değil. Bir şekilde de dijital araçları kullanan herhangi birinin iz bırakmaması mümkün değil. Birisi iz bırakmıyorsa ya o insan gerçekten yoktur veya tariflediği kişi değildir, söylediği kişi değildir veya özel durumu vardır."* (Katılımcı 13, 57, Erkek)

İkinci grup olarak tanımlayabileceğimiz görüşe bakıldığındaysa bu tür bir aratmanın eski samimi sosyal ilişkileri negatif anlamda etkileyebileceği ve bir tür ön yargı oluşturabileceği vurgulanmakta, kişiyi doğrudan yüz yüze tanımanın, bağlantılarla tanımanın önemine vurgu yapılmaktadır. Bu gruptaki kişilerin de yine samimi oldukları kişiler için sevgili, eş, akraba gibi bireyler için geleneksel yolları tercih ettikleri, iş nedeniyle tanıştıkları ya da ilk defa tanıştıkları bireyler için kısmen de olsa bu platformları, bir anlamda büyük veriyi kullandıkları görülmektedir.

> *"Eşimle tanıştığımda hiç bakmadım Facebook'u vardı ama araştırmadım öyle diyorum ya öyle çok şey değilim biraz bana amaca yönelik olması lazım. Ben tanışacağım kişiyi araştırmayı önemli görmüyorum ben onu tanıyarak belirli kararlara varabilirim. Stalklamama gerek yok. Eskiden böyle bir şey yoktu. Eskiden yüz yıl önce Google falan yoksa insan nereden bakacak. Tanıyorsun işte. İnsanın dahil olduğu ilişki, ses tonu, samimiyeti, konuşmalarını görmek aslında gerçeklik. Bakınca yanlış bir ön yargıyla da gidebilirsiniz."* (Katılımcı 7, 42, Erkek)

Bir yandan da katılımcıların bu tür bir gözetleme, ön tanıma pratiğini gizli bir şekilde yapmaya özen gösterdiğini, Instagram hikayelerine ya da LinkedIn profillerine bakarken görünmemek için çeşitli önlemler aldıklarını söyleyebiliriz, görünmeden gözetleme sosyal ilişkilerde önem taşımaktadır: *"Olabildiğince görünmeden bakmaya çalışıyordum, hikayesine bakmıyordum da gönderilerine bakıyordum falan öyle o şekilde güvenli buluyordum yani."* (Katılımcı 2, 28, Kadın); *"Google'da tararım. Beni görebilecekleri olan sistemlerin haricindekilere bakarım, fotoğraflarına bakarım önce bu kişi midir diye tahmin etmeye çalışırım. Kendi söylediyse kurumda gerçekten ismi var mı o kişinin önce gerçek olup olmadığını incelerim."* (Katılımcı 10, 37, Erkek); *"Öncelikle Instagram'ına bakıyorum. Özel biriyse ama iş arkadaşım falansa LinkedIN'e bakarım ama her ikisinde de gizli sekmede bakarım yani stalklarım. Özellikle LinkedIn'de çünkü bildirir bu kişi size baktı diye. Daha sonra Twitter' a bakıyorum biraz daha görüşlerini öğrenmek için. Bilgisi yoksa da ben herkese de mesafeliyimdir en baştan kişisel olarak da yüz yüze de. Sosyal bir insanım normalde hep teması yeğliyorum ama bir şeyini bulurum diye düşünüyorum illa bir datasını bulurum."* (Katılımcı 14, 26, Erkek).

Bu açıdan bakıldığında, veri bilimcilerin, tıpkı sıradan insanların yapabileceği gibi, birini gözetleme pratiklerinde sosyal medya platformlarını kullandığı ve bu pratiğin onları sıradan insanlarla yaklaştıran bir yanı olduğu görülmektedir. Katılımcılar uzmanlık bilgileriyle belki bir derece daha fazla bilgiye erişme imkanına sahip olsalar da aynı pratiğin içerisinde yer almak onların kendilerini sıradan insanların yerine koyarak onlarla empati kurabilecek bir konuma ulaşmalarını sağlamaktadır.

Diğer önemli bir nokta ise katılımcıların hiçbir verisi olmayan bireylerle ilgili düşünceleridir. Burada da katılımcıların üç gruba ayrıldığı görülmektedir. İlk grubun özellikle verisi olmayan kişilere karşı negatif bir ön yargı ile yaklaştıkları ve verisi olmayan kişilerle ilgili kesin bir sorun olduğunu düşündükleri; ikinci grubun bu durumu ilgi çekici ve heyecan verici buldukları; son grubun ise bunu aksine çok doğal bir şey olarak değerlendirdiği dikkat çekmektedir.

> *"Hiçbir verisi yoksa o kişi bende merak uyandırabilir yani ilgimi çeker. Çünkü bilinmezlik algısının yarattığı bir ilgi çekme olabilir o. Birisinin hiçbir verisi olmaması çok zor. Instagram'ını arattım bulamadım. Şimdi Türkiye şartlarını ele aldığımızda küçüklükten beri onla büyüyoruz niye Instagram'ı olmadığını sorguladık, aile baskısı olabilir, kendi sosyal medyadan izole olmuştur, kapatmıştır, olabilir bu mesela bir artı olur bir insanda sosyal medyadan bağımlılığımız var çünkü. Bu gibi yapılar olabilir. Bir yerden sonra Twitter, LinkedIn olmaması şöyle bir noktaya doğru ilerleyebilir kişiyi tanımaya hevesli olurum ama o kişi hakkında yargı üretmek için elimde çok done olmuş olur Instagram'ı Twitter'ı olması. Bir kişinin LinkedIn'ın olmaması beyaz yakalıysa bu demek oluyor ki kariyer noktasında ciddi bir hırsı, bir argümanı yok. Çünkü ya çalıştığı şirket çok iyidir ve istediği noktaya ulaşmıştır. Aynı zamanda hiç kimsenin yaptığı hiçbir şeyi merak etmiyordur. Ama ya da hiç umursamıyor olabilir. Twitter benzer mantıkta dünyada bir sürü olay oluyor ama ben ilgilenmiyorum modunda olabilir. Ya da çok ciddi haber kaynakları vardır başka. Hep bir alternatif vardır ya da umursamaz bir noktaya gidiyor."* (Katılımcı 16, 26, Erkek)

Bir başka katılımcı ise özellikle pandemiyle birlikte yeni nesilde sosyal medyanın daha etkili bir hale geldiğini ve bunun getirdiği çeşitli baskıların da sosyal ilişkileri olumsuz etkilediğini düşünmektedir.

> *"97'liyim ben biz sınır olabiliriz, bizden sonrakiler için daha farklı koşullar doğmuş olabilir çünkü pandemiydi, teknolojinin artması, sokakta oynamanın azalması, okullara uzaktan gitmek bir dönem uzaktan mezun oldular, üniversitenin tadına varamadılar ve ben üniversitenin tadına varamasaydım dans topluluğundaydım, istatistik topluluğu başkanlığı yaptım, öğrenci konseyindeydim falan ben çok aktif, her şeye bulaşmayı seven biriyim. Benim için zül olurdu çok kötü geçerdi. Bu gençlerin iletişim şeyini değiştirdi ve özgüvenlerini değiştirdi çok utangaçlar ve kendilerini maskelemek istiyorlar, yüz yüze gelemiyorlar telefonla konuşamıyorlar, mesajlaşıyorlar. Öyle bir panik atakları var. Yine bu hem büyük verinin ve kapitalist sistemin getirdiği şey güzel olma algısı zorundalığı, fenomenler, ünlü kesim bir tipoloji koydular önümüze kadınlar için ayrı, erkekler için ayrı. Ben erkeklerden bahsedeyim işte kaslı olacak, uzun boylu olacak, gür saçlı olacak vs. o tipolojiden olamayan herkes lise çağlarından hatta daha aşağıda kendini yasta buluyor. Öyle olmak zorunda değiliz zaten bana kalırsa öyle olmanın da bir manası yok. Daha farklı kendimizi iyileştirmemiz, farkında olmamız gerekiyor kişisel gelişim kültürel gelişim. Başka insanlara faydalı olarak hayatım boyunca çok ofansif olmasın ama gymde kol kası geliştireceğime iki kitap daha fazla kitap okur, bir mekânda görece daha az bilgi sahibi olanlara bir şeyler anlatmayı tercih ederim."* (Katılımcı 14, 26, Erkek)

Başka bir katılımcı da benzer şekilde bu durumu nesille ilişkilendirmekte, kendi döneminde içerisinde bulunduğu sosyal çevrenin zaten çok sosyalleşmediğini ve normalde bile sosyalleşmeyen bu insanların sosyal medya kullanmayı da

tercih etmediğini belirtmektedir. Bu sebeple de kendisinin de sosyal medyayı kullanmayan insanlara karşı bir önyargısı olmadığını ve herkesin sosyal medya kullanmak zorunda olmadığı görüşünü dile getirmektedir:

> *"Ben matematik doktorası yaptım. Kuramsal analitik doktorası yaptım. Benim beraber eğitim aldığım arkadaşlarımın hocalarımın büyük çoğunluğu bırak sosyal medya hesabı açmayı zaten iletişim kurarken çok sınırlı sosyalleşirlerdi. Öğle yemeği yerken gözünün içine bakmayan insanlarla ben şey yaptım. Bence normal bunlar. Karakter özelliği olabilir. Hatta çevremde de pek çok tanıdığım hatta çok yakın iş yaptığım insanlarda da aktif kullanıcı olmayan birçok insan tanıyorum."* (Katılımcı 12, 43, Erkek)

Katılımcıların kişisel ilişkilerinde, büyük veriyi ya da yeni gözetim pratiklerini sağlayan araçları nasıl kullandıklarını sorguladıktan sonra toplumsal ilişkilerde bu gözetim pratiklerinin ya da dijital izlerin kaybolmamasının, çok daha erişilebilir olmasının nasıl bir duruma yol açabileceğine dair görüşleri alınmıştır. Bu noktada literatürde de bahsedilen unutulma hakkı sorunu dikkat çekmektedir. Dijitalleşmeyle birlikte büyük suçlar ve suç olmasa da bireylerin kendi bakış açılarında hata olarak ya da başkalarının hatırlamasını istemedikleri bilgilerinin ya da verilerinin internette yer almasının onların unutma ve unutulma haklarını elinden aldığı tartışması önemini taşımaktadır. Katılımcılardan biri, toplumsal ilişkilere büyük verinin ve bu sistemlerin dahil olmasıyla bireylerin hatalarını telafi edemediği ve belirli etiketlerle yaşamak zorunda kaldıklarına vurgu yapmaktadır.

> *"İyi ya da kötü kullanım amacına göre değişebilir. Bir insan hayatı boyunca hep dosdoğru hep istediği şeyleri yapmış olmayabilir. İster istemez bazı hatalar yapmış olabilir. Ama bu veriler bir şekilde duyulduğu zaman ve başka birileri bildiği zaman bir önyargı yaratabilir. Her insan hata yapabilir. Bugün bir insan konuşurken ağzından bir kelime yanlış çıkabilir. Bunu arkadaşı gözetebilir ben onu tanıyorum o öyle bir insan diyebilir. Ama hiç tanımadığı bir insan tanışmadığın biri senin hakkında böyle bir bilgiye sahip olduğu zaman seni tanımadığı için o anda senin düşüncen diye internette bir yerde ya da bilgin sızdırıldıysa sana ön yargılı davranabilir."* (Katılımcı 1, 29, Erkek)

Unutulma hakkı olarak bahsetmese de bir katılımcının (genç bir katılımcının) eskiden kalma etiketlerinin onu rahatsız ettiğini, bir kısmını temizlemeyi başarsa

da bir kısmının hala durduğunu ve bundan rahatsız olduğunu belirtmesi bu durumun bir örneği olarak görülebilir:

> *"Korkarım, çünkü kendini gizlemeyi çok iyi becermiştir. Adımı yazdığında benimle ilgili bir bilgiye ulaşamazsın. Çünkü her şeyi ya kapattım ya engelledim. Çünkü ta ortaokuldan fotoğraflarım var. Benim ta ilkokuldan kaçıncı olarak bile mezun olduğum gözüküyordu. Mesela onları temizledim. Çok saçma sapan şeyler var. İşte ne biliyim Foursquare ya da Swarm vardı gittiğimiz yerden konum atardık. Mesela biz onları kullanırken gerçekten buradayım diye etiket yapıyorduk. Sonra bilmiyorum kullanımımı değişmiş, bir şeyi değişmiş sonra cinsel içerikli şeyler paylaşılmaya başlanmış. Yani değil mi? Swarm falan bu konuda çok farklı olmuş. Mesela hani uygulama benden sonra evrildiği için, adımı yazınca oradan bir fotoğrafım çıkıyordu. Altına link var benim profilim. Altında bir link var şu tarihte katıldı yazıyor ama orada olması iyi değil, sorun değil ama yine de 2014 yılında şuradaydı diye duruyor."* (Katılımcı 5, 26, Kadın)

Unutulma hakkının yanı sıra, bu pratiklerin kişilerin ilgi alanlarını tespit etmek, karakterlerini öğrenmek ve onlarla o şekilde iletişim kurmak için bir zemin hazırlayacağı belirtilmektedir.

> *"Birini etiketlerken böyle etiketliyorum ben. Pride'lı bir şey varsa ona da atıyorum mesela. Onla iletişimim onun sevdiği kanaldan olmak erkek de olsa kadın da olsa. Uzakta olduğum için bunu daha çok önemsemeye başladım. Başka bir ülkeye taşınmadan önce arkadaşlarımla dışarı çıktığımda çok dert değildi ama buraya gelince insanlarla etkileşim kurmak hoşuma gitmeye başladı. Yeni yerde mesela şu an ben burada biriyle tanıştım Honkonglu mesela girdim baktım o bana şeyde anlatmıştı. Bu mesela birinin siyasi düşüncesine hemen önem veriyoruz. Bunlarda sarı şemsiyeliler mavi şemsiyeliler var 1997'de Hon Kong İngiliz sömürgesindeyken Çinliler aha alacağız diye geri sayım yapıyor bunun için de Çin taraftarları var İngiliz taraftarları var çok yeni olaylar aslında bu Çin Honkong olayları. Ama ben Çinliyse kırodur diyorum mesela. Ama muhtemelen değildir bir baktım mesela geçmişine siyasi şeyi var mı diye dünya görüşü nedir ona göre çünkü Aleviliği anlatacağım bakıyorum çocuk da şey var Budistlik var ama inançsız ama ben Budizm'i öğrenmek istiyorum bir şeyler öğrenmek için bir şeyler anlatıyorum. Bir ilişki kurarken hangi kanaldan kurarım bunu tartıyorum ister istemez."* (Katılımcı 11, 33, Erkek)

Özellikle aynı beğenilere, zevklere, aktivitelere sahip olmanın bireylerin birbirlerine daha kolay güvenmelerine sebep olabileceği düşünülmektedir.

> *"Instagram'da çok daha fazla fotosu olan insanlardan daha çok veri de aldığımız için hayatını daha fazla görüp kendi yaşantımıza uyuyor mu uymuyor mu onu da değerlendirdiğimiz için bence etkiliyor. Daha arkadaş olmayı seçme anlamında etkiliyor bence daha kolay güvenmeye sebep oluyor. Sürekli senin yaptığın bir aktiviteyi görünce yakınlık hissediyorsun, senin gittiğin bir filme gittiğinde bir yakınlık hissediyorsun, sonuçta arkadaşlık ortak konuların sağlandığı durumlarda daha kuvvetlendiği için ben bunla arkadaş olurum dediğim durumlar oluyor diye düşünüyorum."* (Katılımcı 3, 30, Erkek)

Başka bir katılımcının ise mesleğinden yararlanarak eşini incelerken, eşinin parametrelerini değerlendirdiğini ve bu şekilde bireylerle olan ilişkilerinde yaptığı analizler açısından daha şanslı olduğunu düşündüğü görülmektedir:

> *"Düşünüyorum çünkü ben çok iyi veri bulurum gerçekten ve şey olarak da daha analitik düşündüğümü düşünüyorum. Ben hayata hep parametrelerle bakarım. Ben eşimle tanıştığımda bile şey demiştim ya pek çok parametresi iyi. O yüzden daha şanslı olduğumu düşünüyorum, teknolojilerle daha erken tanışıyorum onları analiz etme şansım oluyor biraz daha hani işin arka tarafındaki şeyi biliyor oluyorum bu şekilde."* (Katılımcı 6, 36, Kadın)

Fakat tüm bunların aksine en tehlikeli durum, bireylerin bu sistemler yüzünden önyargı taşıyabildikleri ve bazı katılımcıların bunu deneyimledikten sonra bireyleri araştırmayı bıraktıkları görülmektedir. Bunun örneklerinden bir tanesini katılımcılardan biri şu şekilde aktarmaktadır:

> *"Müşterileri araştırırım fakat müşterileri araştırmanın bana ters teptiğini düşündükten sonra araştırmamaya başladım. Mesela şöyle anlatayım, bir firma var Genel Müdür patron ile görüşmek istemiş, tamam gidelim dedim, şimdi ben gitmeden önce ön hazırlık yapıyorum. Gitmeden önce web sayfasına bakıyorum, kafamda bir fikir ile gidiyorum. CEO'sunu araştırıyorum. Gittiğimde o kişiyi ona göre yargılayarak konuşuyorum. Aslında farklı olsa da adamı, o kalıba sokmaya çalışıyorum."* (Katılımcı 15, 55, Erkek)

Katılımcılara yakınlarına sosyal ilişkilerle ilgili ne tür uyarılar yaptıkları ve sevdikleri insanları bu anlamda nasıl uyarmaya çalıştıkları sorusu sorulduğunda büyüklerin uyarılması, çocukların ise denetlenmesi gerektiği vurgusu öne çıkmaktadır. Veri bilimcilerin özellikle unutulma hakkı ve verilerinin bir tür bozulmuş veriye dönüşebilme ihtimali, kendi verileri üzerinden kontrolü

kaybederek bu verilerle neler yapılabileceğine dair bilgi sahibi olduklarından dolayı yakınlarını uyardıkları, özellikle çocuk sahibi olanların çocuklarını çeşitli kurallara tabii tuttukları ve kontrol ettikleri görülmektedir. Bu temelde bir katılımcının (Katılımcı 15, 55, Erkek) yakınlarını tüm verilerini her yere girmeme, maillerdeki linklere tıklamama, bağlantıları indirmeme, bir kafede banka işlemi gibi bir işlem yapılacağında o yerin açık wifi ağına bağlanarak yapmamaları doğrultusunda uyardığı görülmektedir. Bir başka katılımcı (Katılımcı 7, 42, Erkek), belirli bir yaşa kadar çocukların kesinlikle sosyal medyayı kullanmaması gerektiği ve hafta içi tamamen ekran yasağı olup, hafta sonu belirli bir süre izin verilmesi gerektiğini belirtmektedir. Çocuğu olan bir diğer katılımcı da (Katılımcı 10, 37, Erkek) ekran kullanımını ödüllendirme mekanizması olarak değerlendirecek bir pozisyona getirilmemesinin önemini vurgularken, çocuğu fiziksel ortamda sosyalleştirebilecek durumlar uygun olmadığında ekrana izin verdiğini ama bu sürede ekranı arkadaşlarıyla paylaşabilecek şekilde olmamasına dikkat ederek (kendi başına x-box oynamak gibi) kısıtladıklarından bahsetmektedir. Çocuğunun ekran kullanarak "arkadaşlarıyla sosyalleşebileceği" sürenin 2 saat olduğundan, onun haricinde ekran kullanımının yarım saati geçemeyeceğinden bahsetmektedir. Katılımcı, bunun sebebini ise çocukların o dünyaya bağlandıkları zaman ondan kopmak istememesine bağlamaktadır.

Bir üst paragrafta açıklandığı şekilde katılımcılara soru "yakınlarınızı" uyarır mısınız şeklinde yöneltilse de özellikle çocuklara vurgu yapıldığı dikkat çekmektedir. Çocuklardan sonra ise genellikle daha yaşlı bireyleri verilerini çaldırmama, bağlantılara tıklamama, banka bilgilerini vermeme gibi konularda uyardıklarından bahsedilmektedir. Bir katılımcı ise "veri güvenliğine" hem unutulma hakkı hem de bozulmuş veriyle bağlantılandırılabilecek şekilde, özellikle bebeklerin yüzlerinin kullanılmaması, depolanacak yerlerden uzak tutulması konusunda endişesini şu şekilde ifade etmektedir:

> *"Daha çok tabi benim açımdan veri güvenliği, atıyorum yeni bebeği olan birisine yüzü görünecek şekilde bebeğin fotoğrafının koyulmaması üzerine, paylaşılır başka bir şey için kullanılır ya da görüntü işlemesiyle konuşulur*

> *gibi yapılabiliyor. Sesini taklit edebiliyor. O görüntüsü karşısına geçip ileride sorunlara yol açabilir. Para isteme durumu dolayısıyla daha fotosunu paylaşma bu kadar bilgini paylaşma bununu paylaşmaya gelene kadar insanlara önce ne bileyim banka hesaplarına girerken 3D var Allahtan ya da bilgisayar kayıtlı olsun gelir gelmez tıklayayım da hızlı bilet alayım gibi şeyler var mesela. Annem babam benden daha pimpirikli kullanmıyorlardı artık kaçıncı yüzyıldayız diye kullanmaya yeni yeni ikna ettim. Ama genelde sadece bir şeyi otomatik kayıt yaptırma diyorum özellikle ödeme işlerinde. Ben de yapıyorum ama uçak bileti falan alırken. Ben de çok dikkat etmediğimi fark ettim. Çok önemsemiyorum ben de."* (Katılımcı 11, 33, Erkek)

Burada asıl dikkat çeken nokta, ontolojik güvenlik üzerinden de tartışılacağı gibi, yakınlarınızı veri paylaşımı konusunda uyarır mısınız gibi bir soru üzerine düşünürken; küçük bir bebeğin fotoğrafının görüntü işlemeyle başka şekilde kullanılabileceği, sesinin taklit edilebileceği, ileride bebek büyüdüğünde onun için sorun yaratabileceğinden başlayarak kişinin etrafındaki bireyleri uyarırken kendi alışveriş pratikleri üzerinden veri paylaşımına kendisinin de dikkat etmediğini fark etmesidir. Bir katılımcının ise yine aynı endişeleri taşır biçimde TikTok'a yönelik olarak araştırmacıyı da uyardığı ve bu tezde de bahsedildiği gibi TikTok'un özellikle veri toplama anlamında yaptığı etkinliklerin çok net olmamasından kaynaklanan kişiler açısından endişe uyandırdığı görülmektedir. Katılımcı önce TikTok'u kullanmayın diyerek araştırmacıyı uyarmakta, daha sonra Türkiye'de yasaklanması gerektiğini belirterek bu konuda kendisinin de çok endişeli olduğunu belirtmektedir:

> *"Bütün ailemi, çevremi, hatta sizi de bir konuda uyarayım asla TikTok kullanmayın, asla TikTok'a girmeyin. Ben girmek zorunda kalsam başka bir telefon numarası alırım farklı bir e-posta adresiyle girerim ve hiçbir verimi vermem. Sahte bir isim, sahte bir doğum tarihi, her şeyi sahte olan bir yapıyı öyle tavsiye ederim. TikTok'un aldığı verinin haddi hesabı yok ne amaçla kullandığını bilmiyoruz, şu an dünyadaki en tehlikeli uygulama bence. Dark Web kadar tehlikedir belki. TikTok'a girilmemesi lazım. Ben yasaklara karşı çıkarım ama bence Türkiye'de TikTok'un yasaklanması lazım hatta bence tüm dünyada yasaklanması lazım. Hem koşul ve hükümler hem karşılık vermek zorunda olduğu kurum ve kuruluşlar o veriyi kullanma şekilleri ve biçimleri Tiktok'u diğerlerinden ayırıyor. O yüzden daha tehlikeli bir uygulama. Ailemi de yine uyarıyorum zaten çok az uygulama kullanırlar kardeşim de dahil. Geçenlerde bir uygulamada acı bir deneyim yaşadı datalarını almış onunla falan uğraştım Instagram'ı çalındı. Oyun indirirken bile artık hükümlerini okur şekilde. Ben de dikkat etmiyorum desem de ortalamanın üstünde bir dikkat var bizde de alışverişlerimi asla kredi kartıyla yapmam sanal kartla yaparım mesela. Sanal kartı hep saatlik*

> *ve günlük kullanırım. Mobil bankacılık da çok dikkatli olurum datayı çok dışarı vermemeye çalışırım. Kağıtları, fişleri yırtarım eski usul de var biraz. Önemli aslında yani bunlar da."* (Katılımcı 14, 26, Erkek)

Son olarak bir katılımcı, büyük veri ve gözetim sistemlerine yönelik uyarılarının her yaş gruptan insanı kapsadığını söylemekte, bu sistemlerin gittikçe gelişmekte olduğunu ve ChatGPT gibi yeni gelişmelerle bunların değişeceğini belirtmektedir. Eskiden Google'ın da nasıl çalıştığının bilinmediği fakat eğitimlerle insanların buna aşina hale geldiği ve bu sistemlerin de bu şekilde gelişeceğini açıklamaktadır:

> *"Paylaşımlarına dikkat etmelerine yönelik uyarırım. Herkesi yalnızca kendi yaşıtlarımı, büyüklerimi değil, küçükleri de uyarırım. Genelde şu an sosyal medyanın en popüler olduğu kanallar şu anda Instagram vb. şu anda biraz mod değişmeye başladı neden yakın zamanda bir üç beş yıl içerisinde bunlar kalmayacak. ChatGPT türevleri ortaya çıkacağı için Google artık kullanılabilir hale gelmeyecek. Çok basit kullanımı şu anda onunla ilgili eğitimler veriliyor hızlı bir şekilde. Ekranlarda sorgulama nasıl yapılır gibi. Eskilerde arama motorları çıktığı zaman onların da eğitimleri verilmişti. Direk görsel destekli mesajlaşma uygulamaları şu an denemeleri yapılıyor bir de yüksek düzeyli şifrelemeye sahip olan mesajlaşma uygulamaları kullanılmaya başlandı. Fakat güvenlik ihtiyacı ne kadar fazla kullanılmak durumunda kalınırsa o kadar da hedef haline geliriz. Çok yüksek güvenlikli siber duvarlar, firewallar, bilmem neler falan filan sistemler her zaman hackerlara çekici gelir. Çünkü arkasında neler olduğunu merak ederler ve kendileriyle ilgili kırıp kıramayacağına dönük iddialaşırlar. Hal bu olunca aşırı derecede buna reaksiyon gösteriliyorsa da aşırı derecede paranoyak düzeyde eğer bu konuyla ilgili güvenlik ihtiyacı duyuluyorsa da hedef haline gelinebilir. Benim hassasiyetim şu; kendimden dolayı değil benim cep telefonum internette var hiç öyle şeyim yoktur. E-posta adresimde vardır biraz zorlasalar ev adresime kadar da bulunabilir öyle kaygılarım da yok. Bu hepimiz için geçerli. Ben daha çok insanların mahremiyetine saygı duyarım. Özel hayatın mahrem kalmasına dikkat ederim. İlgilendirmez kimseyi çünkü."* (Katılımcı 13, 57, Erkek)

Katılımcının açıklamasına bakıldığında son noktada herkesin pek çok bilgisinin erişilebilir olduğuna, güvenlikler arttıkça oradaki verilerin daha çok ilgi çekeceğine ama bu noktada bile özel hayatın mahrem kalmasına dikkat edilmesi gerektiğine vurgu yapmaktadır. Burada katılımcı gelişen sistemlerle birlikte verilerin tutulamayacağına ve araç değişse de veri gözetiminin devam edeceğine işaret etmekte, bu anlamda bu tez için de büyük verinin kişisel

ilişkilerin yanı sıra toplumsal ilişkiler ve sorumluluklarda ne ifade ettiği sorusunun incelenme gereği ortaya çıkmaktadır.

4.3.2. Sosyal İlişkiler ve Sorumluklar Alanında Büyük Verinin Güven Açısından Sorgulanması

Sosyal ilişkiler ve sorumluluklar alanında büyük veriyi güven olgusu üzerinden sorguladığımızda, çalışmanın önceki bölümlerinde de bahsedildiği gibi, özellikle yeni teknolojilerle birey davranışının daha tahmin edilebilir olması ve hatta bu tahminlerle daha manipüle edilebilir ve kontrole açık bir hale gelmesi, sosyal güvenin bir tür oyunlaştırmaya tabii tutulup tutulamayacağı, yeni dijital gözetim pratikleriyle gerçekten bir tür sosyal güven inşa edilip edilemeyeceği soruları akla gelmektedir. Çin örneğinin de doğrudan, Sosyal Puanlama Sistemi Tasarısı'nın en başında sosyal güvenin inşasına dayanması da aynı mantık üzerinden, bireyleri fiziksel ve dijital medya araçlarıyla yeni sistemlerle takip ederek hem onları daha iyi tanıyarak hem de bir yandan bireylere sürekli izlenildikleri düşüncesini ve veri gözetiminin varlığını hissettirerek ilerlemektedir. Bu anlamda bireylerin gerçekten içselleştirilmiş veri gözetimi sebebiyle sosyal ilişkilerini ya da sorumluluklarını tasarlanmış birer proje olarak kurup kurmadıkları tartışılmaktadır.

Veri bilimcileriyle yapılan görüşmelerde bu mantığın nasıl işlediği, veri gözetiminden başlamak üzere büyük veri sistemlerinin sosyal güvenin inşası ve sosyal güvenin oyunlaştırılmasındaki rolü; bireylerin toplumdaki prestijlerini ifade eden "prestij puantajını" ya da bir anlamda hem kendileri hem şirketler hem de devletler tarafından gerçekleştirilebilecek olan profil çıkarmanın ne durumda olduğu anlaşılmaya çalışılmıştır. Bu bağlamda öncelikle katılımcıların bu gözetimi en çok hangi alanlarda hissettiği ve içselleştirdiğine bakılmıştır. Çalışmadaki veri bilimcilerin hepsi izlenildikleri, haklarında veri toplanıldığını düşündükleri ortam dendiğinde genel olarak interneti, sosyal medya platformlarını ve dijital medya teknolojilerinin yaygınlaşmasını sağlayan akıllı telefonlar gibi teknolojik araçlara vurgu yapmaktadır. Katılımcıların en çok bu

alanlardan ve araçlardan izlenilmelerini düşünmelerinin sebepleri; ilk olarak bu alanlardaki verilerin kaybolmaması ve burada yapılan pratiklerin hiçbir şekilde tamamen gizlenemez oluşudur. "*En çok izlenildiğimi düşündüğüm yer İnternet. Bilgisayarda ya da bir dijital ortamda yapılan hiçbir şey tamamen gizlenemez. Bir şekilde sızdırılıyor."* (Katılımcı 1, 29, Erkek). Bireylerin özellikle tüketim gibi gündelik yaşam pratiklerinin takip edilerek kendi beğendikleri ürünleri görmesi, hakkında konuştukları ürünlerin ya da önerilerin karşılarına çıkmasının da bu düşüncenin arkasındaki temel sebeplerden olduğu görülmektedir. *"Google arama motoru, çünkü orada herhangi bir şeye baktığımda reklamı geri dönüş olarak alabiliyorum. Herhangi bir şey araştırdığımda bir şey görebiliyorum."* (Katılımcı 5, 26, Kadın). Özellikle akıllı telefon kullanırken tüm uygulamaların uzun onay formları içermesi ve yükleme esnasında "Telefonunuzdaki belirli verilere ulaşılacaktır" şeklindeki uyarılarda katılımcılar tarafından izlenilmenin bir temsili olarak ifade edilmektedir: "*İnternet ortamında sanırım. Sanalda, telefonda, tüm uygulamalarda. Çünkü hepsinde izin istiyor okumuyorum ama hepsinde istiyor (güldü) veriyoruz yani."* (Katılımcı 8, 29, Kadın). Dijital izleri gizlemek mümkün olmadığı gibi, bu izler bir şekilde işlenerek bireylerin karşılarına çıkmaktadır. Katılımcılar bu sistemin mantığına hâkim bireyler olduğu için, bunun farkındalığıyla dijital izler üretmektedir.

> *"Instagram veya da arama motorları Google, Yandex gibi vs. Bu telefonlarımız. Bir konu hakkında konuşuyoruz ya da bir linke tıklıyoruz. Herhangi bir ürün arıyoruz. O ürünlerle ilgili şeyler hemen önümüze düşüyor. Hemen evde kedi maması ve güneş kremi bakıyorsam, ayrı ayrı da değil ikisini de görebilmem için bir reklam afişinin ikiye bölünmüş hali karşıma çıkıyor. Bu noktada en büyük izlenen yer telefonlarımız o da bu uygulama izinleri kaynaklı."* (Katılımcı 4, 26, Kadın)

Katılımcılardan bir tanesi (Katılımcı 15, 55, Erkek) ise, iki yaygın telefon üreticisi arasındaki veri gizliliği politikasında bir tanesinin çok daha fazla veri gözetimi yaptığını ve birey davranışlarını izlediğini düşündüğünü ve hatta bazı anahtar kelimeler için telefonun bir anlamda canlandığını düşündüğünü belirtmektedir. Kendisinin bunu test etmek için kedi sahibi olmamasına rağmen bir yakını ile kedi maması üzerine yarım saat konuştuklarını ve telefonlarını açtıklarında kedi maması reklamı gördüklerini belirtmektedir. Bu ifadelerini ve veri gözetimini,

izlemenin en yoğun olduğu aygıtların özellikle taşınabilir teknoloji cihazları olduğuna bağlarken, bunu pil ömrünün yetmemesi gibi teknik özelliklerle de değerlendirmektedir.

> *"Pil teknolojisi çok gelişti, dünyanın pili var ama her gün şarja takıyoruz. Bu mantıklı değil, çünkü aslında pilin daha fazla dayanıyor olması lazım. Ama dayanmıyor, arkada bir çalışma var sürekli. Cep telefonlarımızın onay vermediğimiz veriye de eriştiğine eminim. Telefonu alınca standart yüklü uygulamalar var silemiyorsun bile mesela. Bu uygulamanın içine böyle bir şey koymuş olsa zaten engelleme şansın yok. Ne silinebilir ne durdurulabilir. Ben en ağırlık telefonda izlendiğimizi düşünüyorum, onun dışında da resmi kanalların ciddi datamızı aldığını ve gerektiğinde kullandığını biliyorum."* (Katılımcı 15, 55, Erkek)

Katılımcıların veri gözetimini ve kendilerinin birer veri haline gelmelerini, verileşmeyi içselleştirmelerine yönelik ikinci bağlantı noktası ise bireylerin kendi karşılaştıkları veri ihlalleri üzerine sorularla anlaşılmaya çalışılmıştır. Bireyler kendi dijital izlerinin de teknik yeterlilikleri yüksek olsa bile güvencesiz olduğunu düşünmekte ve ona göre hareket etmektedir. Katılımcılardan bir tanesi (Katılımcı 1, 29, Erkek), bir program yüklediği sırada bilgisayarına fidye virüsü bulaştığını, bunu fark ettikten sonra antivirüs programı kurarak gerekli önlemlerle bunun önüne geçtiğini ifade etmektedir. Katılımcı, bunu fark etmesinin ve çözüm üretmesinin çok stresli olduğunu ve birçok platformda mücadele vermesini gerektirdiğini eklemektedir. Bunun nedeni bağlı olunan Instagram, YouTube ve Gmail hesaplarının da bu virüsle birlikte çalınması, anlık olarak bu platformlardan hikayeler atılması, videolar paylaşılması ve kendisinin bunu ancak aynı platformlardaki arkadaşlarının uyarısıyla fark etmesidir. Yine başka bir katılımcının da yakın bir tanıdığının tutuklanmaya kadar giden bir veri ihlali ile karşılaştığı ve çok endişe duyduğu görülmektedir.

> *"Yakınlarımdan olan oldu. Veri ihlali olarak düşüneceğim bu anlattıklarımı: Yurt dışında bir arkadaşım siz tanımazsınız bir arkadaşı ile kalırken diyor ben iddia oynuyorum, kabul edersen sana da iddialar oynayacağım 200 dolar para gelecek. Telefonu veriyor üyelik alınıyor. Türkiye'ye geri dönüyor. Türkiye'ye gelir gelmez havalimanında kodese koyuyorlar. Giremezsin aranıyorsun suçlusun diyor. Onun da nedeni şu: Meğerse arkadaşının oynadığı bahis sitesi online bahis sitelerinden değil, illegal bahis sitelerinden biriymiş. O an onun kimlik bilgilerini ama diğerinin*

> *telefonundan oynandığı için kişisel bilgilerini çalmış. O yüzden arkadaşımı bırakıyorlar. Ama arkadaşı hala mesela bu konuda suçlu. Ama o arkadaşıma hala bahis sitelerinden aramalar, mesajlar onunki hiç durmuyor. Tüm mesajlar Kıbrıs numarasından geliyor. Birkaç kerede bununla ilgili dolandırılma anısı oldu. İşte avukattan mesajlar geliyor davanız ile ilgili dosya bedeli göndermeniz lazım. Davam kapandı ama göndermeniz lazım demişler. E-devlette sitenin yenilendiği ya da çöktüğü bir sayfa oluyor mesela, e-devletten kontrol edebilirsiniz parayı yatırdığınızda diyor. Aslında öyle bir kurum yok, bunun gibi şeyler yaşayan tanıdıklarım var."* (Katılımcı 5, 26, Kadın)

Suça karışmaya, tutuklanmaya, havaalanında alıkonulmaya kadar giden bu sürecin yanı sıra başka bir katılımcı, biraz da imalı bir şekilde veri ihlalinin bu düzende çok normal olduğunu, veri ihlalini kendisi yaşamasa da zaten sürekli tüm verilerin çalındığını söylemektedir. *"Sonuçta bizim verilerimiz satılıyor zaten. Onun dışında beni maddi manevi zarara uğratacak bir ihlal olmadı şu ana kadar."* (Katılımcı 7, 42, Erkek). Verilerin çalınmasının ve kullanılmasının normalleştiği, kurumların ve devletin de bunun için önlemler aldığı, siber güvenlik anlamında da bu açıdan bir gruplaşma olduğu siyah ve beyaz şapkalı hackerlar üzerinden, veri ihlalleri temelinde açıklanmaktadır.

> *"Çok yakın bilgisayar mühendisi, beyaz hacker dediğimiz, verileri koruyan arkadaşlarım var onların sistemlerine giriyor siyah şapkalı hackerlar, konuşuyorlar, sen niye buradasın diyor o bilgileri çalacağım diyor. Arkadaşlarım beyaz şapkalı hacker, siber güvenlik uzmanları aslında. Beyaz şapkalı dediklerimiz bilgi birikimini iyi işler için kullanan insanlar diyelim. Bankaların siber güvenliğinde devletin siber güvenliğinde çalışanlar. Siyah şapkalılar da bireysel çalışan, veriyi çalıp dağıtmak için uğraşanlar. Onlar sisteme girdiğinde anlarsınız hatta konuşursunuz da. O girmesin diye bir şey yaparsın o bir şey yapar süreç böyle gider. Büyük firmalar siyah şapkalıları kazanıp beyaza çevirmeye çalışırlar devlet de bunu çok yapar. Eğer bir hacker bir devletin sistemine girebiliyorsa devlet onu kendi sistemine çekmeye çalışır. Eğer bu kadar iyiysen o zaman bizi koruyabilecek kadar da iyisin derler. Ya da kurumlar bağımsız beyaz hackerlara giderler benim sistemime girmeye çalış derler kurumlar da eksikleri görüp onları gidermeye çalışırlar."* (Katılımcı 14, 26, Erkek)

Veri gözetiminin ve verileşmenin farkında olan, kendileri ya da yakınları da zaman zaman veri ihlaline uğrayan veri bilimcilerin her tür izleme teknolojisiyle toplumda düzen anlamında ne tür değişimler yaratabileceğine yönelik düşünceleri önem taşımaktadır. Bir katılımcı, izleme teknolojileriyle toplumda bireylerin verilerinin alınmasını ve oluşturulan algoritmalarla, yapılan

işlemlemelerle distopik olan şeylerin gerçek hayatta çok uzak olmadığını yine Çin'in Yapay Zekâ Destekli Sosyal Puanlama Sistemi ile bağlantılandırarak açıklamaktadır. Çin'deki uygulamanın büyük veri ve onun desteklediği yapay zekâ sayesinde bireylerin profillerinin çıkarılarak, toplumun hesaplanabilirlik ve izlenebilirlik temelinde yönetilmeye, dijital vatandaşların kontrol edilmeye başlamasıyla birlikte izleme teknolojileri ve toplumsal düzen ya da kontrolün somut bir örneği ortaya çıkmıştır. Katılımcı bunu Black Mirror'un bahsedilen Nosedive bölümü ile de örneklendirmektedir.

> *"Toplumda düzen sağlamaya yarar ama bir de aması var çok tekdüze olmaya başlarız. Black Mirror'da bir bölüm vardı. Bölümün ismini hatırlamıyorum. Mesela insanlar birbirlerine puan veriyorlardı. İnsanlar birbirlerine iyi davranıyordu. İyi davranmak istediği için değil de puanının yüksek olması için iyi davranıyor, neden puanın yüksek olursa ev kredisi çekerken daha iyi bir evde oturabilecek, insanlarla karşılaştığı zaman daha popüler olacak. Şu an bu sistem Çin tarafında bir yerde bir pilot uygulama olarak başlatılmış olabilir tam detayını bilmiyorum. Türkiye'de biraz zor. Çünkü insanımız yapı gereği genç nesil uygun olabilir ama belli bir yaş grubu insanların bunu kullanacağını düşünmüyorum. Bu sisteme geçene kadar onların birçoğu ölmüş olur. Yeni nesille bu sisteme geçilmiş olabilir."* (Katılımcı 1, 29, Erkek)

Bazı katılımcılar, izleme teknolojilerini toplumda düzen kurma açısından kesinlikle faydalı bulmakta ve yine gözetimin ulusal güvenlik ve risklerle birlikte ele alınması gerektiğine dikkat çekmektedirler. Bununla birlikte katılımcılar, bu riskler için feda edilecek şeylerin etiketleme ve görüntü işleme olmaması gerektiği konusunda da uyarmaktadır.

> *"Güvenlik açısından kullanılması iyi olabilir ya da daha basit teknolojiler kullanılabilir. Mesela, çevre kirliliğini engellemek için bir bölgeye çöp dökülüyorsa onun tespiti yaptırımlar gibi olabilir ama genel geçer bir iyilik için yapılmıyorsa, görüntü işleme ya da etiketleme için yapılacaksa bu yanlış. Çevre kirliliğidir, gaz salınımıdır, bir hırsızlık olayıdır bu tarz durumlarda ya da otobüste genel rahatsız edecek düzeni bozacak şeyleri engellemektir o anlamda iyiliğe yol açabilir."* (Katılımcı 2, 28, Kadın)

Dikkat çeken nokta ise katılımcıların net bir şekilde iki farklı görüşe sahip olmalarıdır. Büyük veri ve yeni gözetim pratiklerinin, izleme teknolojilerinin toplumsal düzen anlamındaki faydalarından bahseden katılımcılar; büyük

verinin yönetim mekanizmaları kurarken faydalı olacağından, sağlık, ulaşım alanlarında katkı sağlayabileceğinden, kanunlara uyulmadığı noktalarda ya da suçluların tespitinde iyi olabileceğinden bahsetmektedir. Bu gruba dahil olan katılımcılardan bir tanesinin ifadesi şu şekildedir:

> *"Sağlar bence. Siyasetçilerin ya da devletin yönetim mekanizmasının kurulmasında katkıları olabilir. Sonuçta insan kaynağı olanlar da vatandaştır yani. Kaynak olarak nasıl planlama yapacağını ya da işte emeklilik mesela şu an söylüyorlar EYT çok fazla yük oluşturuyor diye. Bunun mesela kötü bir planlamayla yapıldığını görüyoruz yani. Ya da aynı şekilde insanların ihtiyaçlarına yönelik e-nabızda ihtiyaçlara yönelik şeyler planlamalar yapılabilir. İnsanların yolculuk tercihlerini göz önünde bulundurarak yeni yollar ve ulaşım araçları planlaması yapılabilir hava yollarının planı ya da yüksek hızlı trenlerin planlanması gibi şeyler. Katkıda bulunabilir."* (Katılımcı 3, 30, Erkek)

Bu düşüncenin tam aksi noktadaki grupta ise bu güçlerin toplumsal düzen kurmayacağı, aksine kötü güçler ya da niyetlerle birleştiğinde ciddi anlamda etik sorunlara yol açacağı, etiketleme yapılabileceği, insanların kısıtlanabileceği söylenmekte, özellikle tekelleşmenin çok ciddi riskleri olduğu vurgulanmaktadır.

> *"Kimin izlemek istediğine göre değişir mesela ama toplumsal düzen sağlanabilir. Yani atıyorum mesela biraz daha dindar bir grubun eline geçerse, insanları daha kısıtlayabilirler. Alkollü mekanların kapatılması, alkollü mekanlar kapatıldıktan sonra insanların verecekleri ev partileri, araba partileri bunlar, büyük verilerle toplandığı ve bizim her türlü verimiz onlarda olduğu için kısıtlanabilir diye düşünüyorum." (Katılımcı 5, 26, Kadın)*
>
> *"Bunu nasıl kullandığımıza göre değişir bence, genelde böyle şeyler çok iyi amaçlar için kullanılmaz izleme şeyleri. Etiketlemek için kullanılır. Tabi bu çok iyi bir şeye yol açabilir ama pratikte pek açmıyor diye düşünüyorum." (Katılımcı 6, 36, Kadın)*
>
> *"Toplumsal düzen kurmaya yarar. Bu işin temelinde de bir Türk yatıyor aslında Arsev Eraslan diye biri öyle büyük bir isim ki NASA'da falan çalışmış. Neil Armstrong ile Anıtkabir'e gidip saygı duruşunda bulunuyorlar çok ilginç bir hikayeleri var. O aslında NASA'da uzayla ilgili çalışmaları olan birisi ama bu çalışmaları buraların temelini oluşturuyor. Ben de onu okuyup bunu araştırıp bir sunum yapmıştım Zekâ Optimizasyonları üzerinden Çin üzerinden gitmiştim. Görüntü işleme ile karşıdan karşıya geçeni suçluyu tespit ediyor ya da alışveriş merkezine gidiyorsunuz mesela yüzünüzden bakıp banka hesabınızdan ödediğiniz şeyi düşüyor öyle yapılar kurduğu söyleniyor. İyi noktalar olabilir suçluları yakalama konusunda ama şu anki kültür buna elverişli değil, dünyanın her bir lideri bunu kendi çıkarına kullanabilecek yapıda çok fazla mafyalaşma tekelleşme mevcut. Gücü*

elinde tutanlar, bunu elinden bırakmak istemezler dolayısıyla bunu çok yanlış kullanacaklardır." (Katılımcı 14, 26, Erkek)

4.3.3. Aktif Birey Pasif Birey Paradoksu: Uzmanlara Güven

Buraya kadar bahsedilenler bireylerin denetim altında tutulma sistemlerinin değişmesiyle yeni gözetim pratikleriyle, sürekli izlenmenin artması, güvenin soyutlanması yoluyla bireyin "insan olma", "karar verme", "özgür olma" niteliklerinin etkilenmesi gibi yeni dijital risklerin ortaya çıkmasına ilişkindir. Katılımcıların görüşleri bu çerçevede değerlendirildiğinde ilk dile getirdikleri endişe, bireylerin sosyal gerçeklikte "düzen" altında seslerini duyurma imkânı bulamadıkları gibi, dijital ortamlarda da aktif olamamaları ve karar alma mekanizmalarının dışında kalmalarıdır. Bunun sebebi dijitalleşmeyle birlikte insanların bir şeye itiraz edecekleri zaman da dijital medya teknolojilerini kullanma yoluna gitmeleri, fakat buradan özellikle sosyal durumlardaki tepkilerinin yeterince gerçek olarak görülmemesidir. Bu durum pek çok katılımcı tarafından bireylerin pasifleşmesi olarak nitelendirilmektedir.

Dijital aktivizmin etkili olduğu ve farklı görüşteki insanları özellikle küresel ölçekte bir araya getirdiği ve demokratikleşmeye, katılımcı kültürün yayılmasına katkı sağlayacağı tartışmaları yapılmaktadır. Bireylerin sosyal gerçeklikte siyasi katılımının ya da siyasal eylemliliğinin sınırlı kalmasının nedeninin dijital platformlarda bazı konularda aktivizm yapabilmeleri, hoşlanmadıkları gelişmeleri protesto edebilmeleri, kendilerini bir konuda bu yolla ifade edebilmelerinden kaynaklanabilmektedir. Dijitalleşme, bu anlamda bir demokratikleşme simülasyonuna yol açmaktadır. Bireyler klavye başında düşüncelerini yazarak, kendilerine yakın olan, aynı görüşte olan bireylerle gruplar oluşturarak yeni aidiyet biçimleriyle tanışmaktadırlar. Bu sayede, bir emniyet supabı gibi işleyerek tepkinin birikmesi ve büyümesi engellenmektedir. Bu da toplumsal düzenin devam edebilmesi için önemli bir işlevdir. Böylece klasik toplumsal hareketlerin yanında çok farklı bir yeni toplumsal hareket kavramı ortaya çıkmaktadır. Kredi kartının paranın simülasyonu olması gibi, siyasal katılım da bu anlamda demokrasinin simülasyonu olduğu düşünülebilmektedir.

Öte yandan bunun tam tersine dijitalleşmenin artmasının bir tür demokrasi oluşturmayacağı, aksine bir tür dışlamaya ya da sessizleşmeye yol açacağı düşünülmektedir. Bu sessizleşmenin ya da dijital aktivizmin etkili olmayacağı düşüncesinin altında ise artık yeni gözetim sistemleriyle bireylerinin görüntülerinin, seslerinin kopyalanabilmesi ve bireylerin yapmadıkları şeyleri yapmış gibi gösterilebilmesi, bireylerin verilerinden pratikleri belirlenerek rutinleri ve gelecek hareketlerinin kontrol edilebilmesi ve sıradanlaştırılması, insanların fiziki alanlarda mücadele etme özelliğini kaybederek sanal alanlara hapsolmaları ve kolektif bilinç oluşturamamaları yatmaktadır.

> *"Birincisi, distopya bizim kopyalanmamız hem sesimiz hem görüntümüzle. Benim yapmadığım bir şeyi bana söyletip, benim bütün bir yapımı hayatımı kaydırabilirler çok tehlikeli bir şey ve bunun önlemi nasıl alınacak bilmiyorum. İkincisi, bizim kişiliğimizi ve karakterimizi yok eden bir şey, hepimizi birbirine benzeten, sıradanlaştıran tepkilerimizi azaltan işte orman kesiliyor ben Twitter'dan yazıyorum benim o insanlara gidip omuz omuza destek vermem lazım. Ben sosyal medyanın bunu gölgelediğini düşünüyorum. Kolektif bir bilinç oluşturamıyoruz bu da hakkımızın daha fazla yenileceğini zaten 1984 dünyasında yaşıyoruz da etkimiz olmuyor gibi. Durdurmak için de çarka dahil olup çarkın içine çomak sokmak lazım. Ben en azından şimdilik şöyle bir endişem yok robotlar dünyayı ele geçirecek mi vs. o bugünün işi değil ona daha var daha tehlikeli bu iki konu. Hem bireysel hem toplumsal."* (Katılımcı 14, 26, Erkek)

İkinci endişe ise toplumsal düzen kurulma düşüncesi vurgulanırken, otoriterleşmeye doğru giden bir sistemin önünün açılmasıdır. Otoriterleşmenin sebebi, bireylerin sürekli izlenerek kontrol altında tutulması, bir şeyleri protesto etmek istedikleri zaman artık sadece dijital sistemler aracılığıyla bunları yapmaları ya da bunu bile yapmaktan çekinmeleri, sistemlerin bireyleri sürekli gözetleyerek onlar hakkında veri toplaması ve profil çıkarması imkanının olmasıdır. Bunun politik geleneklere de dayanan bir şey olabileceği fakat yine de her yerde farklı çerçevelerde uygulanabileceği belirtilmektedir.

> *"Bunun en büyük riski, manipülasyona açık olmamız. Devletler tarafında da daha otoriter bir rejime yol açması. Görece gücün paylaşıldığı, vatandaşın rolünün daha farklı olduğu merkezi olmayan bir yerde zaten devletin bu veriyi toplamasına izin verilmez. Otoriterleşmeyi sağlamaz. Zaten devlet bunu yasal olarak toplamaz. Kim karar verici orada devletin hangi veriyi toplayacağına nasıl gözetleyeceğine kim karar veriyor? Çin'de bireyleri*

> *sınıflandıran toplumsal davranışlarına göre birtakım yaptırımlar, Avrupa'da oluyor mu Amerika'da oluyor mu olmuyor çünkü neden politik gelenekleri buna izin vermiyor toplumsal yapıların. Ha başka şeyler oluyor orda da. Milli güvenlik çerçevesinde başka bir şeyler yapıyor onlar da ya da belirli çerçevelerde yine kişisel veriler üzerinden vatandaşın verisi üzerinden ondan konsent almadan kullanılıyor. Ama toplumun denetim gücünün olduğu, gücün merkeziyetten uzaklaştığı yerlerde oralarda devletin verinin denetim mekanizmasının olduğu yerlerde daha az oluyor."* (Katılımcı 12, 43, Erkek)

Başka bir katılımcı ise diğer bir endişenin insanların kara ekranlara hapsolması olduğunu ifade etmekte, insanların yavaş yavaş diğer insanlardan soyutlandığını belirtmektedir.

> *"Ben mesela telefona daldım gittim. Saatin hiç farkında değilim, zaman mekândan soyutlanmış oldum. Bu aslında tüm dijital sistemler için böyle. Yine Black Mirror'dan örnek vereyim. Siyah Ekran, isminin öyle olmasının sebebi de o, siyah bir ekranın içine dalıp gidiyorsun. Çok değil beş on yıl sonra biz artık işe gitmeden evinden VR gözlüğü takıp evlerinden artık çalışma yürütebilecek. Arkadaşlarınla oradan buluşabileceksin. Bir şey yapacağın zaman artık oradan toplanacaksın. Bu işte artık insanı şeyden çıkarıyor, evet bunlar çok heyecan verici teknolojiler, bunları görmek insanlara çok mutluluk verici, bir şeyler öğrenmesi için bir derya deniz ama insanlar artık insandan soyutlanmaya başlıyor. Bir makine gibi aslında kendimizi siyah ekrana bağlamış oluyoruz."* (Katılımcı 1, 29, Erkek)

Bu aşamalardan sonra ontolojik güvenlik algısını anlayabilmek için izlenecek nokta kişisel güven, toplumsal güven ve mahremiyetin sınırlarının bulanıklaşması ve yeni sistemlerin gelişmesiyle güvenin daha soyut sistemlere, uzmanlık sistemlerine dayanır hale gelmesidir. Bireylerin daha pasif hale gelmelerinin temel sebeplerinden bir tanesi de sürekli izlenir olmakla birlikte, soyut sistemlere duydukları güvenden kaynaklanabilmektedir. Katılımcılara kendileri de birer uzman olarak diğer bireylerin uzmanlıklarına duydukları güvene yönelik sorular yöneltilmiştir. Cevaplara bakıldığında bazı katılımcıların uzmanlara doğrudan güven duyduğunu belirttiği görülmektedir: *"Güvenirim ya. Güveniyorum ki bu işi yapıyorum."* (Katılımcı 6, 36, Kadın). Bazı katılımcılar ise doğrudan sırf uzman olduğu için birisine güvenemeyeceklerini, kendi alanlarındaki uzmanlar için özellikle teknik bilgi ve yeterliliklerine göre güvenebileceklerini vurgulamaktadır. Özellikle bir katılımcının teknik bilgi ve yeterlilik koşuluyla uzmanlara güveneceğini vurgulaması, her şeyi sorgulamanın

mümkün olmadığını bir noktadan sonra Giddens'ın merdiven örneğindeki gibi, rutin olarak kullandığımız "şey"lerde, uygulamalarda, sistemlerde otomatik olarak uzmanlara güven duymak zorunda kaldığımız açıklamasına benzemektedir. Burada kişinin ne kadar ve nasıl veri paylaştığının önemine de işaret edilmektedir.

> *"Onun geliştiricileri ve çalıştığı uzman grup ne kadar iyiyse o kadar güvenirim; değilse güvenmem. Sorgulamam çünkü bir noktada bilmek mümkün değil, önemli olan o noktada benim ne kadar veri paylaştığımla alakalı. Bir yemek sipariş etme platformu kullandığım zaman, mecburen kredi kartı bilgilerinin girilmesi gerekiyor. Sürekli olarak mümkün değil kredi kartıyla hiç alışveriş yapmamak lazım çünkü herhangi bir şekilde gittiğimiz bir yerde alışveriş yaparken post cihazının içerisine bir kart okuyucusu yerleştirip oradan rahatlıkla benim bilgilerim kopyalanabilir, o yüzden çok yaygın kullanıma sahip olmayan ve kenarda köşede ücra bir yerde de kredi kartı kullanmam nakit öderim."* (Katılımcı 13, 57, Erkek)

Başka bir katılımcı da aynı fikirde olup, Türkiye'de bu durumun özellikle veri bilimi anlamında daha sorunlu olduğundan bahsetmektedir. Tezde de bahsedildiği gibi, veri bilimcilerin kim olduğunun tartışmalı olduğunu, diğer benzer meslek dalları ile çok net bir ayrım yapılamadığını ve bunun uzmanlık anlamında sıkıntı oluşturduğunu ifade etmektedir. Aynı zamanda uzmanlara güvenebilmek için, diğer alandaki uzmanlara, yönetimdeki uzmanlara, yasal alandaki uzmanlara da güven duyma gerekliliği duymaktadır.

> *"Türkiye'de bu alan çok yeni olduğu için böyle diyemiyorum çünkü şöyle, veri bilimciler aslında iki yıl veya üç yıl önce böyle bir alan yoktu ve bu kişiler Phyton programlama dilinde yazılım yapıyordu, mobil uygulama üretiyordu, şimdi birden veri bilimci oldu. Burada buna çok güvenemiyorum ama bunla ilgili gerekli eğitimlerin verilmesi, yaptırımların olması, bunun belirli bir hukuki çerçevede olması, o zaman güvenimi sağlayabilir. Kişileri de bunla ilgili sorumlu tutmak güvenimi sağlayabilir. Verilerin korunması vs. göreceğiz. Amerika'da Facebook olayı patladı en azından böyle bir durumdan ders çıkarılıp üzerine gidilse daha iyi şu an çok sessiziz, bir ihlal yok gibi, bir sıkıntı yok gibi, belki neler var bilmiyoruz."* (Katılımcı 2, 28, Kadın)

Bu bakış açılarının yanı sıra bazı katılımcıların ise aksine kesinlikle uzmanlara güvenmediği ama bir tür boş vermişlik duygusu ile bu sistemleri kullanmaya devam edeceğini söylediği görülmektedir.

> ***"****Güvenmem. Yani zaten kullanıyorum. Bunları hayatımdan çıkarmak istemiyorum. Bunları hayatımdan çıkarırsam zaten sıkılacağım açıkçası. Günümün çoğunu kişilerle iletişim kurarken geçiriyorum, o sırada da bilgilerim çalınıyor olabilir. Telefonumda dinleniyor olabilir. Telefonumda alışveriş yaparken bedenimden cüzdanımdaki paraya kadar her şeyi biliyor olabilirler. Ben yine de kullanmaya devam edeceğim."* (Katılımcı 5, 26, Kadın)

Diğer bir bakış açısı ise uzmanlara güvenmek yerine, bu sistemleri kullanan diğer bireylerin kullanıcı deneyimlerine güvenmek olarak ifade edilmektedir. Sistemleri kullanan kişi sayısı, onlar hakkında yazılan yorumlar, arama motorlarındaki kullanıcı tarafından üretilmiş olan bilgilerin daha etkili olduğudur. Bu da yine dijital medya teknolojilerinin katılımcı kültür kavramıyla da açıklanan, bireylerin seslerini duyurmak, dayanışma ağları kurmak için sistemlere değil, bir anlamda birbirlerine güvenmeleri ile ilişkilidir. Güven, bu noktada uzmanlara değil, dayanışma ağlarına bağlanmaktadır.

> *"Ben kendi açımdan en azından o alanda kim çalışıyor, o alanda çalışan kişilerin portföyü nasıl şeklinde bir araştırma yapmıyorum. Benim baktığım tek şey: internet sitesi ya da platform biliniyor mu? Sonunda kaç kişi kullanıyor hemen Google'da eksi bir özellik ya da yakında yaşanan bir fiyasko var mı şeklinde aslında bu toplum davranışı kaynaklı. Ben etrafa bakıyorum kişiler uygulamayı kullandığında bir sorun yaşamış mı yaşamamış mı diye."* (Katılımcı 4, 26, Kadın)

Son görüşe bakıldığında ise uzmanlara ya da soyut sistemlere olan güvenin mümkün olmamasının sebebinin, bu sistemler kurulurken inisiyatifin uzmanda değil kurumlar, şirketler ya da devletler gibi güçlerin istekleri ve talepleri ile yönlendirilmesidir. Büyük Veri Ayrımı kavramı ile açıklandığı şekilde, büyük veri zengini ve büyük veri yoksulu arasında ciddi bir güç dengesizliği vardır ve uzmanları da büyük veri zengini olarak sayamayacağımız için onlar da düzenin içinde sadece verinin depolanması ve işlemlemesinden sorumlu bireyler olarak işlev görmektedirler. Katılımcılar da son nokta olarak bunu vurgulamaktadır.

> *"Yani bence aslında uzmanlara kurumlar yaptırıyor diye düşünüyorum. Mesela bir data kullanırken, odaklandığımız şey eğitim alırken datayı nasıl analiz ederiz, datayı nerelerden toplarız, nasıl kullanırız. Mesela bilgisayar mühendisi, o datayı nasıl işlemesi gerektiğine kurum yönlendiriyor gibi geliyor bana. Mesela bir kurum kuralları söylüyordur. Mesela datayı başka*

yerlere vermeyin gibi sözleşmeler yapıyordur. Bunu ancak yasal kurumlar aracılığı ile vermesi engellenebilir. Ben tam tersini düşünüyorum. Bireyler bu kadar bilinçli olmak zorunda değil. Benim anneannem datasının nasıl kullanılacağını bilemez mesela, onun zamanında datası diye bir şey yoktu burada büyük bir jenerasyon farklılığı yaşanır. Benim kardeşim bu konuda eğitim almasa da duyduğu bazı şeylerden dolayı bilebilir. İnsanlar bunun farkında olmayabilir." (Katılımcı 9, 35, Kadın)

"Sorgulanması gerekiyor. Kaynağının sorgulanması gerekiyor, kimin denetlediğinin sorgulanması gerekiyor, kaynağını bilsek de ilgili örneklem alınmış mı alınmamış mı bakılması gerekiyor, yanlı bir çıktı mı yoksa güvenebilir miyim diye sorgulanması gerekiyor. Sorgulanmadan olmaz. Google, Google diye doğru değil." (Katılımcı 7, 42, Erkek)

"Bunu ticari şirketler yaptığı ve ortada para döndüğü için kişinin de pek bir inisiyatifi olduğunu düşünmüyorum." (Katılımcı 8, 29, Kadın)

4.4. BÜYÜK VERİNİN GELECEĞİ: VERİ BİLİMCİLER VE ONTOLOJİK GÜVENLİK

"Büyük Verinin Geleceği: Veri Bilimciler ve Ontolojik Güvenlik" temasının altında, Şekil 8'de yer aldığı haliyle üç kategori belirlenmiştir. İlk kategoride, "Ontolojik Güvenlik ve Ontolojik Güvensizlik", yerelleşmiş güven ya da soyut sistemlere güven, mahremiyete olan inancı kaybetme, veri gizliliğine yönelik inancı kaybetme, uzmanlara güven ve sosyal fayda ya da zarar formunda büyük veri alt kategorilerine erişilmiştir. İkinci kategoride, "Büyük Veri, Etik ve Ontolojik Güvenlik", bireylerden alınan onay ve etik: süreçlerin şeffaflığı alt kategorisi belirlenmiş; üçüncü ve son kategoride, "Uzmanların Başa Çıkma Yöntemleri", (Anthony Giddens'ın kavramsallaştırmasıyla) pragmatik kabulleniş, sürekli iyimserlik, alaycı kötümserlik ve radikal katılım alt kategorilerinden bahsedilerek dördüncü ve son temanın analizi gerçekleştirilmiş, araştırmanın bulguları detaylı bir şekilde yazılmıştır.

Şekil 8. Büyük Verinin Geleceği: Veri Bilimciler ve Ontolojik Güvenlik Teması Kategori ve Alt Kategori Şeması

4.4.1. Ontolojik Güvenlik ve Ontolojik Güvensizlik

Ontolojik güvenliğin temelleri kuramsal kısımda açıklandığı şekilde, psikolojik olarak bireylerin etraflarındaki değişimlere uyum sağlama süreçlerini, bu süreçler içerisinde izledikleri yolları, uyum sağlayıp sağlayamadıkları ile ilişkilidir. Temellerine bakıldığında psikolojiden yola çıkarak bireylerin duygusal olarak bu değişimlerden dolayı yaşamış oldukları korkular ve endişelerin odak noktası olduğu görülmektedir. Bireyler bu anlamda hayatlarındaki rutinlerin bozulduğu durumlarda ya da rutinleri yerine getirmede zorluklarla karşılaştıklarında derin kaygı yaşayabilmektedir. Sosyolojik olarak güven kavramından beslenen ontolojik güvenlik kavramı ise mahremiyetin 20. yüzyıldaki dönüşümüne dayandırılmaktadır. 20. yüzyıl ile ontolojik güvenliğin bağlantılandırılmasının sebebi, sürekli değişen ve dönüşen dijitalleşmenin, özellikle bilgi ve iletişim teknolojilerinin yeni bir boyut kazanmasıyla, daha sonra sosyal medyanın meydana gelmesiyle, onun kullanıcı odaklı içeriği desteklemesiyle temel olarak bireylerin en özellerini bile hedef olarak belirleyen bir araç haline gelmesidir. Özellikle bireylerin kişisel verilerinden beslenen büyük veri ve büyük verinin beslediği yapay zekâ, toplumdaki tüm bireyleri farklı şekillerde etkilemekte, onların bu durumla baş etmek için çeşitli mekanizmalar geliştirmesine neden olmaktadır.

20. yüzyılda mahremiyetin dönüşümü, özellikle 21. yüzyılda dijital medya teknolojilerinin gelişmesi, internet altyapısının hiç olmadığı kadar gelişmesi, sosyal medya platformlarının kullanıcı odaklı içeriği temel alması ile çok daha farklı bir boyuta ulaşmıştır. Dijital epidemiyoloji, dijital epidermalizasyon ve dijital fenotipleme gibi başlıklar altında açıklandığı gibi, bireylerin farklı türdeki verilerinin, farklı biçimlerde toplanması ve veri entegrasyonu ile bireyler hem fizyolojik hem ruhsal olarak mahremiyetinden ödün vermek zorunda kalmıştır. Özellikle Kovid 19 gibi bir salgın ile de görüldüğü gibi, salgın sadece sağlık sektörünü etkilememiş, fiziki gözetim araçlarının artmasına neden olmuş, fiziki teknolojiler hem dijital medya teknolojileri hem de yapay zekâ gibi daha gelişmiş sistemlerle bütünleşerek bireyleri kontrol etme imkânı çok daha fazla artmıştır.

Katılımcıların ontolojik güvenlikte bahsedildiği gibi baş etmesi gereken, rutinlerini bozan, kaygı ya da korku yaratabilecek (kendileri, yakınları ya da insanlık adına olabilir) bir durum meydana gelmiştir. Önceki bölümlerde veri bilimcilerin gözünden mahremiyetin ne olduğuna dair görüşlerin de farklılaştığı göz önünde bulundurulmakla birlikte, mahremiyetin özellikle bireyin paylaşmak istediği her tür şeyin elde edilmesi ve kullanılması ile sarsılacağını belirttikleri görülmektedir. Mahremiyetin aşınması ya da dönüşmesi bu anlamda katılımcıların gözünden bakıldığında şu şekildedir: "*Mahremiyet şöyle bir şey, bizim vermek istemediğimiz paylaşmak istemediğimiz şeyleri kapsadığı için ben bunları kendi isteğimle paylaşıyorsam aşınmıyordur, benim rızam vardır ama biri benden habersiz bir şey için kullanıyorsa aşınıyordur.*" (Katılımcı 8, 29, Kadın). Birçok katılımcıda da buna benzer yanıtlara rastlanırken özellikle bazı katılımcıların devletin vatandaşları ya da bireyleri kontrol etmesi, etiketlemesi ve kontrol etmesi üzerinden mahremiyetin aşınmasını yorumladığı görülmektedir. Bunun temel sebeplerinden bir tanesi özellikle mahremiyetin kamusal alan ve özel alan ayrımında özele ait olan olarak değerlendirilmesi, kamusal alanla da genellikle devletlerin ya da özellikle hükümetlerin bağlantılandırılmasıdır. Mahremiyetin kaybı, bahsedilen dijital gözetim sistemleriyle sadece bireylerin, bedenlerinin, kişisel verilerinin değil, düşüncelerinin ve duygularının da tespit edilebilmesi hedefiyle ilerleyen bir şey olarak ele alındığı için bu tür bir yaklaşımın olabileceği düşünülmektedir. Etiketleme durumunun mahremiyeti sarsan en temel ve güncel şeylerden biri olmasını katılımcılardan bir tanesi şu şekilde ifade etmektedir:

> "*Bunun karşılıklı güven ilişkisiyle olabilecek bir şey olduğunu düşünüyorum. Şimdi eğer devlet, beni etiketlemeyecekse, bir kategorizasyon yapmayacaksa bana, beni takip etsin atıyorum İstanbul kartımı okuttum işe gittim, geri ona bindim geldim, evde açtım Netflix izledim bunları takip etmesinde bir sıkıntı yok ama bunları beni bir etiketleme amacıyla kullanacaksa, sosyal ağlarımı daraltacaksa ya da yönlendirecek beni bir yöne sokacak şeylerde kullanacaksa bu sıkıntılı. Karşılıklı güven varsa bir sıkıntı yok aşılabilir belki. Dünyaya global çerçevede bakıldığında aşılabilir belki ama çok sancılı bir süreç de olabilir."* (Katılımcı 2, 28, Kadın)

Ontolojik güvenlikte mahremiyetin dönüşümünü takip eden süreç bireysel ve sosyal ilişkilerin dönüşümüdür. Bu dönüşümün temelini ise bu ilişkileri oluşturan güven anlayışı belirlemektedir. Giddens'ın vurguladığı şekliyle modern öncesi dönemde, yerelleşmiş bir güven hakimken, güven temel olarak akrabalık sistemlerine, yerel topluluklara, dinsel kozmolojiye ve geleneklere, rutinlere dayanırken özellikle mahremiyetin dönüşümü ile güven anlayışı da değişmiştir. Güven anlayışının değişiminin sebebi ise bahsedilen somut güven dayanaklarının yerini soyut sistemlerin almasıdır. Bu hedefle bulgularla öncelikle veri gözetimi ve mahremiyetin dönüşümü, daha sonra sosyal ilişkilerde ve sorumluluklarda güvenden bahsedilirken en son veri bilimcilerin soyut sistemlere ve uzmanlara karşı güvenleri hakkındaki görüşlerinden bahsedilmektedir.

Giddens'ın yorumuyla modernlik, zaman ve uzamın ayrılması, yerinden çıkarma düzeneklerinin gelişimi ve bilginin düşünümsel temellükü ile pek çok toplumsal değişime sebep olmuştur. Bu değişimlerin en temel olanlarından bir tanesi ise bireylerin mahremiyet ya da gizliliğe olan inancını kaybetmesi ve artık bunun onlara verdiği farkında oldukları ya da olmadıkları huzursuzluk ile baş etmeye çalışmaları olmuştur. Bu temelde özellikle toplumsal ilişkiler belirli bir zaman ve uzamdan ayrılmakta, uzmanlık sistemlerine, simgesel işaretlere, dayanır hale gelmektedir. Eskiden para olarak tarif edilen bu sistemlerde şu an ciddi bir sermaye olan büyük veri merkeze yerleşmiştir. Büyük verinin parayla eşdeğer olmasının yanısıra, kişisel veriden beslenen bir şey olması, onu kişisel ve sosyal ilişkiler açısından çok daha ciddi ve endişe uyandıran bir şey haline getirmiştir. Burada güvenin de dönüştüğü, kişilere değil, soyut niteliklere karşı duyulan inancın bir parçası olmasından bahsedilmektedir. Bu sistemlerdeki sorumlu bireylerle genellikle karşılaşma olmasa da karşılaşmalar ise ulaşma noktaları olarak açıklanmaktadır. Bu araştırmada ulaşma noktaları veri bilimciler olduğu için veri bilimcilerin hem deneyimleyen özne hem de onu düzenleyen ve kontrol eden kişiler olarak ulaşma noktaları olarak kendileriyle ve aynı meslek grubundaki kişilerden bahsedilmektedir. Bu noktada ontolojik güvenlikle ilgili olarak onların diğer uzman ve soyut sistemlere bakışı da incelenmiştir.

Katılımcıların kendileri de uzman olarak, diğer uzmanlara ve soyut sistemlere bakış açısında özellikle onların teknik yetkinliklerine ve sistemlerin işleyişinde rol oynaması gereken hukuki uzmanlara bir soru işareti ile yaklaştıkları; uzmanlara güvenmek yerine kullanıcı deneyimine bakma yoluna gittikleri, en çok vurgu yapılan noktanın ise, soyut sistemlere ve uzmanlara güvenmeme anlamında, karar alma mekanizmalarında ya da bu sistemlerin düzenlenmesinde uzmanların değil farklı kişilerin, kurumların ya da devletlerin söz sahibi olması, inisiyatifin uzmanlarda olmamasıdır. Bir katılımcı, uzman olarak kendi içinde bulunduğu durumu şu şekilde ifade etmektedir. Katılımcı bir yandan durumun ciddiyetini "*büyük veri gücünü verdiğinizde üç saniyede kötüye kullanacaklar*" şeklinde ifade ederken, bir yandan da kendi konumunu sorgulamaktadır:

> *"Proje yapılıyor başka projeye devredilmiş, başka danışmanlığa da verilmiş aynı para da değiller. Birilerine orada para geçirilmiş. Burada bile etik dışı olan insanlara siz dönüp de büyük veri gücünü verdiğinizde üç saniyede falan herhalde kötüye kullanacaklar en iyi ihtimalle anlamayıp çöpe atarlarsa. Anlarlarsa kötüye kullandılar bu iki iki dört. Bazen hayır işi yapan bir yerde mi çalışsaydım diyorsunuz. Bir sivil toplum kuruluşunda en çok ne kadar kötüye kullanılabilir ki? Ya da işte başka sivil toplum kuruluşlarında ne kadar kötüye kullanılabilir ki deyip oralarda mı çalışsaydım oluyorsunuz bir yandan da klasik kapitalist yaşam o yüzden de çıkamıyorsunuz döngüden."* (Katılımcı 16, 26, Erkek)

Bu anlamda soyut sistemlere güven değil, güvensizlik göze çarpmaktadır. Aynı ontolojik güvensizlik daha önce de belirtildiği gibi, sosyal ilişkiler temelinde, bir grubun doğrudan veri gözetiminden faydalanarak kişilere yaklaştığı, diğer grubun ise bu sistemlerle bireylere yaklaşmanın bir önyargı oluşturabileceği şeklinde düşünmesinde görülmektedir. Her iki grupta da ontolojik güvenliğin sosyal ilişkiler temelinde bağlantısı ise ağlar üzerinden görülmektedir. Giddens'ın akrabalık sistemlerine ya da yerel topluluklara duyulan yerelleşmiş güven diye tanımladığı şeyin hala bireylerin uzun süredir tanıdıkları, güvendikleri, yüz yüze iletişim kurdukları "güven ilişkilerinin" bu bağlara dayandığı kişilerle ilişkilerinde bu tür sistemleri kullanmazken; özellikle sonradan tanıştıkları iş ilişkisi kuracakları ya da bir sebeple iletişim kurmak zorunda kaldıkları bireyler için özellikle bu sistemleri kullanma eğiliminde

oldukları görülmektedir. Kişisel güven ise bu noktada Giddens'ın da açıkladığı gibi, bireylerin üzerinde çalıştıkları bir proje haline gelmektedir. İlişkiler olmayıp, yaratılmaya çalışılmaktadır.

Ontolojik güvenliğin en başta hedef aldığı şey, bireylerin ya da toplumların sahip olduğu rutinlerdir. Bu tezde de bu sebeple, bahsedilen tüm sistemlerin, bireylerin birçok rutinini bozduğu ya da değiştirdiği ve incelenmesi gerektiği düşünülmüştür. Bu hedefle de ontolojik güvenlikle, onu en iyi bilen, bir sorunla karşılaştığında düzeltebilecek potansiyelde olan, onun algoritmalarını ve sistemlerini hazırlayan, tasarlayan, düzelten veri bilimcilerin bu sistemlerle hem kendilerinin hem de toplumda kendilerinden daha az bilgiye sahip olan bireylerin bu yeni düzende nasıl baş ettiklerini görmek hedeflenmiştir. Çünkü bir katılımcının da belirttiği şekilde bu sistemler değil, önce veriler ortaya çıkmış ve bu verilerle nasıl mücadele edileceğine daha sonra karar verilmiştir. Rutinlerin bu noktada bozulmaya ya da dönüşmeye başladığı düşünülebilmektedir:

> *"Zaten paradigmanın ortaya çıkışı biraz şey, insanoğlu bilerek bir veri üretmeye başlamıyor. Toplumsal süreçler bunu beraberinde getiriyor. Çok fazla veri üretmeye başladığı zaman bundan bilgi üretmek daha geriden gelen bir şey. Biz önce veriyi üretiyoruz, gerçi günümüzde yönetmeyi bunla başa çıkmaya yönelik yöntemler geliştirdiğimiz için tabii ki çift taraflı besliyor ama ilk ortaya çıkışı bizim elimizde bir kontrol ettiğimiz bilgi üretimi çok da belli bir amaçla toplamadığımız bir data var. Ve ilk akla gelen soru ben bu veriyi kendi işim için müşteriyi anlamak için olabilir, kendi organizasyonunu daha iyi kılmak için olabilir, yeni pazarlar belirlemek, ürün belirlemek, kaliteden tut da oralarda kullanmak olanağı sağlıyor. Sadece bunu değil, daha akademik taraftan bakıldığında neyle uğraşıyorsan uğraş ekonomiyle de sosyolojiyle de toplumları algılayabilir miyiz yazdıkları söyledikleri resmettikleri videolar üzerinden davranışların belirli özelliklerini algılayabilir miyiz? Esasında ilk ortaya çıkışı çok da bir planlı bilgi sağlamaktan öte biz bundan ne üretebiliriz ile başlıyor bununla beraber artık bunla başa çıkmanın analiz etmenin yöntemleri geliştikçe artık daha kontrol edilebilir bir alan olmaya dönüştükçe artık veri üretmede bir miktar "structure"a girmeye başlıyor. Günümüzde benim çalıştığım sektörlerin büyük çoğunluğunda operasyon maksimize edebilmek. Daha verimli bir şekilde yürütebilmek. Kullanıcı davranışını daha iyi algılayabilmek bir de kullanıcı ya da bir müşteri olmasa bile belirli bir topluluğun davranışını nasıl hissettiğini nasıl davrandığını anlayabilmek. Mesela bu olanaklar çok büyük bir olanak sağlıyor çünkü daha önce kullandığımız yöntem matematikten gelmiş biri olarak bence çok sınırlayıcı mesela, burası orayı tamamlayan farklı bir bakış açısı getiriyor."* (Katılımcı 12, 43, Erkek)

Katılımcının da bahsettiği şekilde bireylerin davranışlarını, nasıl hissettiklerini ve kim olduklarına yönelik analiz imkânı sağlayan büyük veri ve yeni gözetim pratikleriyle bireysel, fiziksel, ruhsal ve biyometrik olarak sürekli bir izleme hali rutinleri bozan ve ontolojik güvenliğin sorgulanmasına yol açan bir süreç haline gelmektedir. Dijital gözetim denilen sistemlerin sürekli olarak bireylerin istemli ya da istemsiz verilerini toplaması ve kullanması bireylerde bir izleniyormuş hissi yaratarak belik duygusu, benlik kontrolü ya da mahremiyetin sınırlarının daralmasıyla ontolojik güvenlik ya da güvensizliğe yol açabilmektedir. İzleniyormuş hissinin ne boyutta olduğunu en iyi gösteren örneklerden bir tanesi başörtülü bir katılımcının, kendi kişisel telefonunda bile başörtüsü olmadan fotoğraf bulundurmamaya ve çektirmemeye dikkat ettiği bunun sebebini ise "*biri görürse ya da erişirse*" diyerek açıklamaktadır:

> *"Dediğim gibi, ben çok bir şeyler yazmamaya özen gösteriyorum. Foto çekmemeye falan da dikkat ediyorum çok fazla. Özellikle açıkken falan çok foto çekmem ben. Biri telefonumdan bakarsa diye, görmesin diye özellikle. Ya da biri erişirse diye." (Katılımcı 8, 29, Kadın)*

Katılımcının ifadesinde de görüldüğü gibi hem bu sisteme dahil olmakta hem de uygulamaları kullanmaya devam etmekte fakat bunun getireceği riskleri düşünerek olabildiğince az kullanarak, çok aktif olmadan veri üretimine dahil olmamaya çalışmaktadır. Buradaki önemli nokta yine de sisteme dâhiliyetin sürmesidir. Bauman, bu durumu, gizlilik hakkını kaybetmek pahasına bireylerin bu sistemlere dahil olmak istemeleri, bunun sebebinin ise temel olarak topluluklara bağlı kalmak, sistemlerden dışlanmamak olduğu şeklinde ifade etmiştir. Veriyi ikincil konuma tabii tutma kavramıyla da ifade edildiği gibi, özellikle bu sistemlerin dışında kalan bireylerin seslerini bir süre sonra duyuramayacakları yönetimsel açıdan endişe yaratmakla birlikte aynı dışlanmanın sosyal ortamda da olabileceği düşünülmektedir. Bir katılımcı kendi ile ilgili toplanan veriler ve panoptik sınıflandırma ile ilgili düşüncelerini şu şekilde ifade etmektedir:

> *"Yani dediğim gibi zaten şu an bilgilerimin istenen her devlet kurumunda, her şifremi verdiğim yerde ve platformda sattıkları yerde olduğunu*

> *biliyorum. Bu durum şu an karşıma bir şey çıkartmadığı için sorun değil. Ama atıyorum ben bir devlet kurumunda işe girebileceğimi düşünmüyorum. Neden çünkü, ben adım soyadım, hangi köyde doğduğum, hangi mezhebe ait olduğum, annemin babamın hangi partiye mensup olduğu, bunlarla ilgili katıldıkları eylemlerden, belki eylem görüntülerinden, attıkları imzalardan verdikleri oylardan dolayı herhangi bir yere gelebileceğimi düşünmüyorum. Aslında bu beni en başından beri mutsuz eden bir durum ama bunun en başından beri de farkında olduğum için, çok fazla rahatsız etmiyor beni, alıştım diyebilirim." (Katılımcı 5, 26, Kadın)*

Katılımcı kendisinin ve yakın olduğu kişilerin toplanan verileri sebebiyle, ayrımcılığa uğrayacağını düşünmekte ve bunu en baştan bildiği için artık bunu sorun etmediğini söylemekte, "alıştım" derken, uzmanların baş etme yöntemleri kısmında açıklanacağı gibi, örtülü bir kötümserliğe sahip bulunmaktadır. Katılımcının bahsettiği bir tür panoptik sınıflandırmanın şu an güncel olarak Çin'deki sosyal puanlama sisteminde görüldüğünden tezin pek çok yerinde bahsedilmektedir. Çin'in kurduğu düzen örneğinde, toplanan verilerle beslenen yapay zekâ destekli puanlama sistemi dijital vatandaşlık ışığında bireyleri puanlandırmaktadır. Bu puanlama yapay zekâ, robot kuşlar, fiziksel gözetim cihazlarıyla gerçekleştirilmektedir. Buna ek olarak sosyal medya hesapları, kredi kartı harcamaları gibi pratik ve düşünme şekli belirleyen alanlar da izlenmektedir. Buradaki önemli noktalardan bir tanesi Çin'in uluslararası kurumlara ya da diğer devletlere kendi vatandaşlarının verilerini vermemek ya da onların verilerinden sadece kendisi yararlanabilmek için bu verileri elinde tutmasıdır. Çin'de uluslararası alanda kullanılan birçok uygulama kullanılmamakta olup, onun yerine kendi milli uygulamalarının kullanılması zorunlu kılınmaktadır. Bauman'ın da bunla bağlantılı örneğinde Cyworld (Çin'de kullanılan bir sosyal medya platformu) Platformu'nda olmayan bireylerin yaşadığının doğrudan sosyal ölümle bağlantılandırıldığı görülmektedir.

Diğer katılımcıların da aynı şekilde düşünme tarzları bulguların birinci kısmında, veri ihlali ve veri manipülasyonu arasındaki farkın açıklandığı başlık altında, hepsinin dünyadaki ve Türkiye'deki veri ihlallerine vurgu yapması ile görülmektedir. Özellikle kendi içerisinde bulundukları toplumdaki veri ihlallerinde kişilerin kendi T.C. kimlik numaraları, adresleri, sağlık verileri, nüfus bilgileri gibi

en özel bilgilerinin çalınmasına yönelik beyanları ve bundan dolayı zaten bu sistemleri boş vermiş bir alışkanlıkla kabul ederek yaşamaya başladıkları görülmektedir. Katılımcılardaki kırılma noktası özellikle "Kim?" uygulaması ile bu kadar kolay etiketlenebilecekleri ve tüm verilerinin kendi ülkelerinde de kullanılabilir olduğunu görmek olmuştur. Temel ontolojik güvensizliklerin, özellikle Türkiye açısından incelendiğinde, bu noktalarda başladığı görülmektedir. Nüfus ve sağlık verilerinin çalınması (dijital epidermalizasyonda bahsedilen tüm veriler) onlar için ontolojik güvensizliğin temelini oluşturmaktadır. Ontolojik güvenlik, sosyolojik olarak bireyin kendi güvenliğine ilişkin davranış ve inançları da kapsayan bir kavramdır ve bahsedilen noktalarda bireyin kendi güvenliğine ilişkin de şüpheleri olduğu, fakat bunu önemsemiyormuş gibi davrandığı anlaşılmaktadır.

Büyük veri bölümünde detaylıca bahsedildiği gibi, büyük verinin oluşturmuş olduğu yeni karar verme kültüründe, mahremiyetin ve ontolojik güvenliğin dönüşümü özellikle gözetim kapitalizmi sebebiyle kullanılacak, işlenecek ve depolanacak nesnenin doğrudan birey ve bireyin verisi haline gelmesine neden olmuştur. Ücretsiz hizmetlerin karşılığını ödemenin bir yolu bu sistemde kişisel verilerdir. Bu dönemde verileri korumanın ve bu sistemlerden kaçmanın da mümkün olmadığı, bir sistem ayrıştırıcı diye diğerine geçildiğinde sorunun çözülmediği belirtilmektedir. Bir katılımcı bunu şu şekilde ifade etmektedir:

> "*En son bu eski medya dediğimiz yapı kalmadığı için Twitter'a geçtik. Yarın bir gün Twitter'a aynısı olacak. Bu kadar aleni dikte edici bir sınıflandırmayı, ayrıştırmayı Twitter'da yaparsa bunu birisi ifşa edecek, sonra Twitter'ı da bırakacak atıyorum bu işler biraz böyle dünyanın sistemini anladıktan sonra şey gibi oluyor, varsayın ki evinizi su basıyor siz suyun çıktığı noktayı sürekli alçıyla sıvamak gibi bir şey bu dönemde verileri korumak. Orayı alçılarsınız başka yerden patlar. Benim komiğime gidiyor kişi bir alışveriş platformu kullanıyor, bir online yemek firması kullanıyor, belki Android telefon kullanıyor bir ton uygulama indirmiş dönüp diyor ki Facebook'ta verilerimi paylaşmıyorum ben. Tamam, hadi oradan kurtardın (güldü). Bravo ama geri kalan her yerden kaybettin, çok zor yani veri korumak çok zor özellikle*." (Katılımcı 16, 26, Erkek)

Yapay zekâ destekli sosyal puanlama sistemi örneklendirilerek bahsedilen sistemlerin benzerinin, İçişleri Bakanlığı'ndan verilen örnekte görülebileceği gibi, verilerin veri entegrasyonuna uğradığı ve bireyler hakkında pek çok tespite olanak sağladığı görülmektedir. Bu sistemlerde bireylerin itibar puantajına, profil çıkarmaya ve kartografiye, bir tür haritalandırmaya maruz kaldığı bilinmektedir. Bu unsurlarla birlikte özellikle, devlet ve diğer özel ya da kamu kurumlarının iş birliğiyle çeşitli alanlarda sınıflandırma yapılabileceği aşikardır. Bu anlamda "sosyal fayda için büyük veri" ve bir katılımcının kullandığı karşıt haliyle "sosyal zarar için büyük veri" ikiliği karşımıza çıkmaktadır. Sosyal fayda için büyük veri pratiklerinin ontolojik güvenlik algısına katkıda bulunduğu, bunun sebebinin de küreselleşen dünyada beliren yeni risklere karşı en verimli ve iyi çözümleri üreten sistem olduğu görülmektedir. Büyük verinin bir tür sosyal zarar çerçevesinde değerlendirilmesinde kastedilen ise, bahsedilen panoptik sınıflandırma faaliyetleridir. İnsanların etiketlenmesi, profillerinin çıkarılması ve bunların bireylerin aleyhinde, bireylerin kendilerinin kontrolünü kaybettiği bir şekilde ilerlemesidir. Bu süreçte özellikle güç dengelerinin değişmesi ve bireyin bu noktada sadece verisiyle ek değer üretip belirli çıkar gruplarını daha da zengin hale getiren (büyük veri zengini) bir konuma gelmesi söz konusudur.

> *"Verinin, bence büyük veri bir sorunu çözmek için kullanılıyorsa toplumda bu pek çok kişinin faydasına olacaktır, fakat birilerini etiketlemek ve onlara ayrımcılık yapmak ya da onları detect etmek için kullanılıyorsa bu tamamen bir sosyal zarar projesidir diyebiliriz. Verilerin gerçekten korunduğu bir ortamda, ortak bir yerde bulunması ve bunu sağlığa erişim, belirli finansal kaynaklara erişim için insanların faydasına kullanılması da bence toplumsal fayda. Mesela büyük veri finansal sektörde hiç var olmamış kişilerin finans kaynaklarına erişebilmesi için kullanılıyor. Ben daha önce hiç kredi kullanmamış bir insan olarak normalde bankadan çok yüksek kredili faiz alabilecekken, benim büyük veriden oluşturulan verimle bana daha uygun faizli bir kredi verilebilir. Bu da financial inclusionu arttırabilir. Bu ekonomideki kaçak oran anlamlı bir şekilde düşüyor olacaktır."* (Katılımcı 6, 36, Kadın)

İlk bakış açısına, ontolojik güvenliği artıran sosyal fayda için büyük veriye bakıldığında, bir grubun kesinlikle büyük verinin eşitliği sağlayacağını özellikle dijital fenotipleme ve dijital epidermalizasyonda bahsedildiği şekliyle büyük verinin ırksallaştırılmış bir güç olarak kullanılmasının aksine, bunun olmaması

için insanın subjektif kararları yerine, büyük verinin daha objektif kararlar verebileceğini düşündüğü görülmektedir. Büyük veri bu anlamda eşitliği sağlayacak bir güç olarak görülmektedir:

> *"Evet, şöyle ben eşitliği sağlayacağını düşünüyorum. Mesela, Amerika ve bazı Avrupa ülkelerinde bir yere CV gönderirken genelde fotoğraf koymazlar. Neden? Çünkü sen ırkının belli olmaması için siyahi misin, beyaz mısın bunun bir etkisi olmaması için. Koymayı hatta bir rahatsızlık olarak nitelendirir karşı taraf. Ama ismin bir şekilde ortaya çıkıyor. Mesela sen benle mülakata girdiğin zaman senin kim olduğun, ne olduğun, ırkının, dininin hepsi ortaya çıkıyor. Bu da ister istemez hepimiz insanız ve önyargılarımız var evet olmaması gerekiyor ama var. Ama insanların duygularıyla istemeyecekleri kararlar verebileceklerini düşünüyorum. Büyük veriyle bu kararlar en azından insanlara eşitliği sağlayabilir."* (Katılımcı 1, 29, Erkek)

Bir katılımcı ise bu katılımcının aksine büyük veri sistemlerinin sağlayacağı eşitliğin bir tür korkuya dayalı eşitsizlik sistemi olacağını, insanların kişiliklerini değil, yalnızca davranışlarını değiştireceğini belirtmektedir:

> *"Bu verilerin toplanması evet insanlarda bir korku yaratıyor ve aslında ya bir yerden sonra o verileri kapatmaya çalışıyorlar ya da ona göre davranmaya çalışıyorlar ama bu insanların kişiliklerini değil, davranışlarını değiştiriyor. Bu yüzden de kötü bir insan sadece gerçek yüzünü saklıyor gibi bir şeye dönüşüyor. İnsanlar arasında eşitlik kavramını bence daha küçük yaşlarda eğitimle sağlayabiliriz onun dışında bu tarz korkuya dayalı ya da eşitlik sistemi bence işlemez."* (Katılımcı 3, 30, Erkek)

Eşitlikle ilgili güncel bir bilgi paylaşan başka bir katılımcı, Papa'nın yapay zekâ ile ilgili açıklamalarını ve onun önemini şu şekilde açıklamaktadır; bu açıklamada özellikle kişisel veririn insanların aleyhinde kullanılabileceği ve bu alanda geri kalan ülkelerin diğer ülkelerin sömürgeleri haline geleceği, bu sistemlerin eşitliği korumak adına kullanılmasının önemine vurgu yapılmaktadır:

> *"Papa Francis'in 2020 yılı Temmuzlarında yaptığı iki tane toplantı ve akabinde açıklama var. Orijinal bir konu, neden orijinal çünkü yaptığı açıklama yapay zekayla ilgili. Yapay zekâ geliştiricisi önde gelen şirketlerin yönetici ve sahiplerini görüşmeye davet etti. Ve bunlara bir memorandum imzalatıyor. İmzalattığı memorandumda mealen söylüyorum kendi açıklamasıydı yapay zekâ kişisel verilerin kullanımıyla geliştirilen bir teknoloji ve burada istenirse bu kişisel veriler insanların ya da yapay zekâ*

> *teknolojileri insanların aleyhinde de kullanılabilir. O nedenle buradaki firmalara benim imzalattığım memorandum iyi niyet zaptı, mutabakat zaptı, toplanan kişisel verilerin kişilerin aleyhinde kullanılmayacağına dair bir taahhütnamedir. Aralıkta da aynı ekibi toplayıp yapay zekâ diyor, artık diyor geri dönüşümsüz olarak hepimiz için hava gibi, su gibi ihtiyaç haline gelecek önümüzdeki günlerde ve yapay zekâ alanında geri kalmış toplumlar, geri kalmış ülkeler, diğer ülkelerin sömürgesi insanlar da köleleri haline gelecek. Bu nedenle en azından eşitliği sağlamak için yapay zekâ teknolojilerinin eşitliği bozmayacak şekilde dünyadaki tüm ülkelerle paylaşılması gerekir. Bununla ilgili de bir memorandum imzalatmaya çalışıyor ama imzalatamıyor. Şimdi kritik kısma geliyoruz Papa kendi çevresinde Hristiyan inanışına göre Katolik inanışına göre Tanrı'nın yer yüzündeki gölgesi. Yani bir dogmanın en üst düzeydeki temsilcisi. Yapay zekâda insanoğlunun geliştirmiş olduğu en sofistike teknoloji. Bu taraf bu tarafla ilgili bir tedbir alma ihtiyacı içerisinde. Yeni sömürgecilik artık teknoloji üzerine olacak çünkü biz, şu anda hayatımızı tamamen bununla sevk ve idare ediyoruz."* (Katılımcı 13, 57, Erkek)

Başka bir katılımcı ise yine güç dengelerine dikkat çekerek, bu sistemlerin iyilik adına kullanılması için çok iyi kişilerin elinde olması gerektiğini, aksi takdirde toplumsal cinsiyetten örneklendirildiğinde bunun erkek egemen bir toplum için bile kullanılabileceğini belirtmektedir.

> *"Kullanabiliriz. İlk başta dediğim gibi aslında, benim sana verdiğim bilgiyle sen cinsiyetimi çok iyi bir şey için kullanacaksın ama sen tam tersi erkek egemen bir toplum için kullanabilirsin, kimin elinde olduğuna göre değişir. Milyonlarca kategoriye ayrılabilir insanlar. İyi insanların eline geçtiğinde eşitliğe katkı sağlayabilir. Ama çok iyi insanlar olmaları lazım (Gülerek)"* (Katılımcı 5, 26, Kadın)

Aynı şekilde başka bir katılımcı da Cambridge Analytica örneğini hatırlatarak, bireylerin verilerinin alınarak seçim sonuçlarının etkilenmesini bir tür eşitsizlik olarak değerlendirilmekte, asıl bakılması gerekenin bu sistemlerin kimler tarafından yönetildiği olduğunu belirtmektedir: "*Dediğim amaçla kullanılması eşitliğe; Cambridge Analytica ya da devlet içerisindeki şu gösterilen uygulamalardaki her şey eşitsizliğe sunulan bir katkı gibi geliyor bana*." (Katılımcı 6, 36, Kadın). Devletlerarası eşitsizliklerin bile bu süreçte etkili olduğunu ise başka bir katılımcı şu şekilde ifade etmektedir, bu tezde daha önceden de katılımcıların belirttikleri gibi, sadece veriye sahip olmak değil onu depolamak ve işlemek de önemli bir unsur haline gelmiştir.

> *"Kesinlikle güçlüyü, daha güçlü yapar çünkü o bilgi sahibi yanında. Bilgiye erişim kolay bir şey değil. En azından ben laptopumla bir şeyi analiz etmeye çalışırken Çinliler, Amerikalılar, İngilizler inanılmaz hızlarda bir şeyler analiz eder. Kesinlikle eşitsizliği artıracaktır böyle bir şey. Bu kadar sadece iklim değişikliği aktivistligi gibi bir şeyde kalacak bu. İllaki Avrupa'nın bilmeme standartları, veri standartları gibi şeylerle dengede tutulmaya çalışılacak. Dinleyenc olacak dinlemeyen olacak tabi. Ama kesinlikle bir dengesizliğe sebep olur."* (Katılımcı 11, 33, Erkek)

Diğer bir sosyal fayda ise arama motorlarının yerine geçeceği ve büyük veri destekli yapay zekâ sistemleri sayesinde daha doğru ve daha çeşitli cevaplar vereceği düşünülen ChatGPT'nin gelişimidir.

> *"ChatGPT 'ye bir şey yazdığında bir sürü cevap alabiliyorsun doğru mu onlar tartışılır ama veri arttıkça onların iyileştiğini düşünüyorum. Artık sanat bile yapılabilir büyük veri kullanılarak. Yani faydaları birçok yönde tartışılabilir. Ama zararlarından korunmak içinde bir sürü politikalar geliştirilmesi gerekir diye düşünüyorum."* (Katılımcı 9, 35, Kadın)

Bu düşüncelere ek olarak sosyal fayda için büyük veri dendiğinde iklim değişikliğinin önlenmesinden, "*e-nabız üstünden hissettiğimiz şeyleri girdiğimizde hastalıkların tahmin edilebilmesi*" (Katılımcı 2, 28, Kadın); "*refah seviyesinin artırılması ya da insanların ömürlerinin bile uzatılabilmesi*" (Katılımcı 5, 26, Kadın); "*insan iyiliği için iletişimden tutun da sağlıkta, ulaşımda bir sürü yerde kullanılıyor ve kullanılmalı da*" (Katılımcı 7, 42, Erkek) fikirlerinin öne çıktığı görülmektedir.

Ontolojik güvensizliğe sebep olabilecek ve sosyal zarar olarak büyük veri düşüncesini vurgulayan katılımcılara bakıldığında ise, etiketleme, kişilerin yapmadıkları şeyleri yapmış gibi gösterebilme, toplumlara baskı yapma, kategorizasyon yapma, güç gruplarının kendi menfaatleri doğrultusunda kullanması gibi unsurlar belirtilmektedir. Bunu ifade eden bazı katılımcıların fikirleri şu şekildedir:

> *"Kişi etiketlemek ya da bu verilerin amacı dışında kullanılması gibi durumlarda kötü olabilir, istihdam alanında kötü olabilir o yüzden zararlı da olabilir. Bunun nasıl evrildiğine ve yönetildiğine bağlı aslında."* (Katılımcı 2, 28, Kadın)

> *"Zararı noktasında her an her şey olabilir. Yapmadığım bir şeyi bana gösterebilirler, fotoğrafımı önüme koyabilir. Konumumu oradaymışım gibi gösterebilir, adresim, telefonum, kredi kartı bilgilerim, okuduğum yer, çalıştığım yer evet sen bunu yapmışsın der gibi şeylerde kullanabilir."* (Katılımcı 4, 26, Kadın)

> *"Ama kötü insanların elinde kendi menfaatlerini düşünen insanların elinde olursa, toplumlara baskı yapabilecek büyük insanlar olursa eğer depremler, afetler, savaşlar, uzaylı saldırıları (Güler) olabileceğini düşünüyorum".* (Katılımcı 5, 26, Kadın)

Başka bir katılımcı ise büyük verinin sosyolojik dezavantajlarını, Baudrillard'ın hipergerçeklik kavramında olduğu gibi, yapılan şeylerin gerçeğinden daha gerçek hale gelmesi riski ve gerçek ile gerçek olmayan arasındaki farkın anlaşılamayacağından bahsetmektedir:

> *"Bu aynı Türkiye'de yaşamak gibi. Kesinlikle çok faydalı çok, hayatı çok kolaylaştırabiliyor daha ucuz tatil yapma imkânı bulabiliyorsun ya da bir şeyleri daha kolay alabiliyorsun, işini daha kolay yapmaya başlayabiliyorsun, insanları daha kolay tanıyabiliyorsun falan ama başına bir kere kötü bir şey geldiği zaman kredi kart limitine kadar tek seferde çaldırabilirsin. Online bir şey ve takip edilemeyecek bir şey de olabilir. Başına gelene kadar bir zararı yok ama başına gelirse çok kötü. Şu an yapılmıyor ama yapılması çok kolay herhangi bir yüzü porno yıldızı gibi yüzü daha iyi bir vücuda oturtabilirsin onun tüm mimiklerini ona aktarabilirsin. Hiç olmadığı bir durumda açıklama yapmaya zorlayabilirsin Tarkan'ı. Bakarsın AI derler ama ona kadar rahatsız edici bir durum. Onun artık gerçek olup olmadığı önemli değil. (Gerçeklik algısının kaybolması, gerçeğinden daha gerçek)"* (Katılımcı 11, 33, Erkek)

Gerçeğinden daha gerçek olma ve bireyleri insanların yüzlerini, bedenlerini, seslerini genel anlamda verilerini farklı anlama durumu panoptik sınıflandırma ve kategorizasyon için de geçerlidir. Katılımcılara göre bireyler çeşitli şekillerde sınıflandırılmaktadır. "*Sınıflandırırsın verileriyle onları. Tamamen o kişinin hedef kitlesine göre yapılıyor bu veriyi kullanacak olan ya da analizin sonucunda ne için kullanılacaksa ona göre kategorize ediliyor."* (Katılımcı 8, 29, Kadın). Kategorizasyon da katılımcılar tarafından olumlu ya da olumsuz olarak iki farklı şekilde değerlendirilmektedir.

> *"Dediğim gibi nasıl kullanmak istediğine bağlı sanıyorum benim alanımda segment yaratmak aslında iyi bir şey örneğin, çocuklu bir aile şehir merkezinde yaşamayan, hep araba kullanması olabilir mesela. Ama mesela*

> *bu insanların araba kullanmasını istemiyorsam belirli alternatifler sağlamalıyım. Şehir merkezinde yaşamadığı için otobüs kullanması gerekebilir atıyorum, otobüsün sıklığının artması gerekir mesela. Daha adil ortamlar için daha faydalı işler yapılabilir."* (Katılımcı 9, 35, Kadın)

> *"Yani kullanılıyor ne yazık ki keşke kullanılmasa ama bence kullanılıyor. Alışveriş tercihlerimizden bile bir kategorizasyonumuz oluyor, gittiğimiz doktorlar, başka bilgiler, mobil uygulamada kullandığımız kısımlar, bankacılık sektörünün, oradan bile kullanılıp sizi daha çok yatırım yapıyorsanız mesela, o uygulamada size ona yönelik teklifler sunması, ona yönelik kredi kartı puanları sunması falan o yüzden bir kategorizasyon mevcut."* (Katılımcı 2, 28, Kadın)

Katılımcılardan birinin de belirttiği ve genel olarak bilindiği gibi, sınıflandırmanın genel anlamda ticari amaçla olsa da "*Müşteri ve stokta kategorizasyon yapabilirsiniz sınıflandırma yapabilirsiniz zaten o kategorizasyonu kümeleştirme gibi metotlar var onlara ihtiyacınız oluyor yani.*" (Katılımcı 7, 42, Erkek); bu sınıflandırmanın yalnızca ticari anlamda değil ırk, etnisite ve toplumsal cinsiyet gibi unsurlarla da şekillenebileceği ve bunun çok riskli olduğu çünkü bu noktadan sonra çok katı bir şekilde dışlama ve gruplandırmanın mümkün olacağı belirtilmektedir:

> *"Kategoriden kastımız ırk ya da dil, din anlamında mı? Kategorize edilebilir ve bu tarz şeyler kullanılıyor."* (Katılımcı 3, 30, Erkek)

> *"Oradaki insan senin kafa yapına uymuyor. Ama bir noktada o alanda yere bir işin düşebilir. Ve oraya gittiğinde sana öncelik sağlanmadı çünkü sen artık dışlanan kesim olmuşsun. Senin nereye ait olduğun belli."* (Katılımcı 4, 26, Kadın)

> *"Kullanılır. Bu noktada işte yaşam şekilleri, aile yapıları, desteklediği parti, tuttuğu takım, ilgilendiği iş ya da bu telefonda sosyal medyada süre aralığı, tıkladığı linkler kişiyi belirlemede kullanılabilir."* (Katılımcı 4, 26, Kadın)

> *"Kesinlikle kullanılabilir. Bir insana hem zaman hem birçok şeyini harcıyorsun. Ben bu insana doğru yatırımı yapmak istiyorum diye bakmak istiyorum. Bu yüzden kesinlikle profillendirmeyi çok istiyordum. Herkese içki masalarında hevesle anlatıyordum. Sen bu kızla tatile gidemeyeceğini hemen öğrenmek istemez misin diye mesela. Bu bilgi sence de güzel olmaz mı diye falan. Sarhoşken çok prim yapmıştım. Kesinlikle büyük veri sosyal medya kanalıyla olur ilerde başka bir şeyler çıkar. Kesinlikle insan profillendirme yapmaya çok müsait bir durum."* (Katılımcı 11, 33, Erkek)

Katılımcıların ruhsal ve fiziksel olarak büyük veri ve yeni gözetim sistemleri ile ilgili nasıl hissettiklerine bakıldığında bir katılımcı bunu araba kullanmaya

benzetmiş, daha objektif karar verebileceği birçok sektörde farklı şekillerde fayda elde edilebileceği için heyecanlı olduğunu belirtmiştir.

> *"İlk başlarda araba örneği gibi, ben kendimi araba kullanmayı yeni öğrenen bir genç gibi hissediyorum. Hani ileride ne seviyede olacağını ne kadar kar sağlayacağını heyecanla bekliyorum. Korkutucu yanları var mı var ama ağırlıklı olarak heyecanlıyım. Kesin karar vermesi, sağlık sektörü özellikle, doktorlarla telefondan görüşebilmek, yapay zekanın bireye hastalığını söyleyebilir hale gelmesi çünkü senin tüm verilerini işlemiş olacak seninle ilgili her tür bilgiye sahip olacak büyük veriyle beslenmiş bir yapay zekâ seninle ilgili her şeyi bilebiliyor olacak. Mesela, bir örnekten gidelim, biri hırsızlık yaptı. Biz bunun verisini diğer tüm veriler içerisine ekleme yapacağız bu adam 25 yaşında, bekar, çalışmıyor, gelir durumu şu kadar, daha önce hangi işlerde çalıştı, nerelerde yaşadı, ne gibi yaşam zorlukları geçirdi gibi değişkenlerin de olacağını düşünmüyorum. Veriyle biraz daha detaylı ve objektif kararlar verebileceğini düşünüyorum."* (Katılımcı 1, 29, Erkek)

Katılımcılar, özellikle yeni gözetim sistemleriyle bireyler anonimleştirilmeden verilerinin toplanmasının ciddi sorunlar yaratabileceğini, o bunun yanı sıra savaşlar ve çatışmalar gibi her türlü durumun da artık büyük veri ve bu sistemler üzerinden yürüyebileceğini düşünmektedir. Güncel olarak İsrail ve Filistin arasındaki gerçekleşen savaş esnasında çıkan haberlerden bir tanesi ise bunu çok net bir şekilde yansıtmaktadır. 15 milyona yakın insanın kökenlerini keşfetmek için verilerini vermiş olduğu bir firmanın hacklenmesi ve burada belirli bir dine mensup olan bireylerin verilerinin derin web üzerinden şu an satılıyor olması ve ırkçı söylemlerle bağlantılandırıldığından bahsedilmektedir. Bir katılımcı ise bu durumu şu şekilde ifade etmektedir:

> *"Hayatı çok fazla kolaylaştırıyor. Bu hem bireyler için hem toplumlar için böyle. Bireyler için çok dezavantajlı değil, şu an kişiler herhangi bir veri istismarına uğramadığı zaman özellikle bankacılık gibi kendisine çok özel bilgilerin dışarıya sızmadığında çok fazla sıkıntısının şu an olduğunu düşünmüyorum. Daha çok toplum üzerindeki yapay zekalar dünyayı ele geçirecek, toplumu kutuplaştırabilir bölebilir, internet üzerinden bir kutuplaşma konsolide yaratma gibi şeyler olabilir, toplumun nezdinde çatışmaya yol açabilir. Arkadaşlıkları bile bitirebilir. Kendi düşüncelerimizin doğru olduğu gerçeğiyle oturuyoruz. Karşımızdakinin gerçeğini çok fazla kabul etme yolunda değiliz. Dolayısıyla karşımızdaki arkadaşımızın düşüncesinin farklı olduğunu gördüğümüzde ilişkimizi mesafelendirebiliyoruz. Bunu sosyal hayat üzerinden yapabiliyoruz. Kişisel hayatlarımız üzerinden de yapabiliyoruz. Büyük verinin bize toplum*

üzerinden gelecek olan dezavantajlarının parça parça yansımasıyla olacağını düşünüyorum. Kişi reklama uğramak istiyorsa bundan memnun olur. Ben kokteyl reklamlarını görünce daha kalitelisi gelsin istiyorum. Araba aradığımda bu önerilerinin gelmesinden memnunun. Vadelerde hangi banka daha çok veriyormuş, kredi kartında hangisi daha esnek bunu görmek tabi beni memnun eder ama bunu bana reklam haricinde detaylı olarak kişisel bilgilerimi elde ettiği zaman çok mutlu olmam. Anonimleştirilmiş bir bilgi üzerinden hareket ettiğinde kişisel özelliklerimi biliyor ama benim üzerimden yapıyorsa bu dezavantaja girer." (Katılımcı 10, 37, Erkek)

4.4.2. Büyük Veri, Etik ve Ontolojik Güvenlik

Katılımcılara, özellikle yeni gözetim pratiklerinin dezavantajlı yanları düşünüldüğünde; büyük verinin etik anlamda nasıl olduğu, gerekli önlemlerin alınıp alınmadığı, ontolojik güvenlik ya da güvensizlik anlamında ne durumda olduğunu anlamak için en basit haliyle "etik mi?" sorusu yöneltilmiştir. Burada nadir olumlu görüşlerden bir tanesi, etik boyutuyla ilgili gerekli düzenlemeler ve denetlemeler yapılırsa toplumsal fayda sağlayabileceği yönündedir. Ama bu cevabı veren katılımcılar bile toplumsal zarara sebebiyet verebilecek yönü olduğunu da eklemektedir:

"Etik boyutuyla ilgili düzenlemelerin daha çok yetersiz olduğunu ve bu düzenlemelerin denetlenebilir otoriteler tarafından uygulamaya alınması gerektiğine inanıyorum. Eğer gerçekten denetlenebilir olur ve bu şekilde kullanılırsa ben epey toplumsal fayda sağlayacağına inanıyorum. Fakat şu an toplumsal zarara sebebiyet verecek çok fazla açık noktası da var." (Katılımcı 6, 36, Kadın)

Diğer katılımcıların bir kısmı da özellikle kullanımının etik olabilmesi için rızanın ve bilinçli kullanımın olması gerektiğini, bunlar sağlanmadığında hiçbir şekilde bu pratiklerin etik olmadığını vurgulamaktadır.

"Kullanımı etik olarak rızasızsa ve bilerek yapıyorsa ya da bilinçsiz de olabilir etik değil. Karşı tarafın onu kullananın yaptığı da etik değil. Bu kadar mahremine bir şey sokuyorsa insan bunun sonuçlarını da az çok tahmin ediyordur diye düşünüyorum. Kimse görmese büyük veri olmasa da 100 kişi görüyor seni mesela. Her ne kadar insanlar bilinçli olsa da bunu kullanmak etik değil, buna etik diyemeyiz, karşı taraf biliyordu diye etik değil diyebiliriz." (Katılımcı 8, 29, Kadın)

Diğer tüm katılımcıların neredeyse hepsi ise bu noktada ortak bir noktada buluşarak, etik olabilmesi için bu süreçlerin şeffaflığına, birey kendi verisi üzerinde kontrolü kaybetmedikçe bu sistemlere etik diyebileceğimize yönelik beyanlarda bulunmaktadır.

> *"Bu olabildiğince şeffaf bir süreç olmalı ben bir yere tıkladığım zaman bir videoyu beğene tıkladığım zaman sadece o videoyu beğendiğim verisi çıkıyorsa ya da atıyorum içinde kedi vardı, kediyi beğendi bilgisi çıkıyorsa bunda bir sıkıntı olmayabilir ama oradan başka bir yerlere vardırıyorsa olayı, kedi seviyor, demek ki köpek sevmiyor, şöyle oluyor, böyle oluyor öyle bir varsayımlara ucu dayanıyorsa çok büyük bir ihlal olur. Zaten böyle bir durumda kişinin rızası da olmaz. Ben bir iz bırakıyorsam kedi videosunu beğendi izini bırakıyorum ama siz bundan çıkarımlar yapıyorsanız bu rıza göstermediğim bir olay olduğu için ihlal oluyor."* (Katılımcı 2, 28, Kadın)
>
> *"Etik anlamda bu verilerin hangi verilerin toplandığına dair bilgi verilmesi etik geliyor bana çünkü bunu biz kendi rızamız dahilinde o uygulamaya ya da o web sitesine sağlıyoruz. Bu konuda evet ama etik olmayan kısmı bunun başka şirketlere satılıyor olması tamam bunla ilgili de bilgilendirme yapan şeyler var ama mesela bir hastaneyi bugün aradım telefondaki bilgilendirmede sizden alınan bilgiler üçüncü kişilerle paylaşılabilir diyor mesela net bir şekilde. Evet yani söylüyorlar ama kimle paylaşıyorsun ne amaçla bunlar rahatsız edici ve bence etik olmayan şeyler. Biz bilgilerimizi sadece o firmaya kiralıyoruz gibi olması gerek. O firma bizim tamamen bilgilerimize sahip olmamalı o yüzden de başkalarıyla paylaşamamalı. Bu açıdan etik olmadığını ya da direkt olarak hiçbir şeyi olmadan biz şu verileri kullanıyoruz gibi bir şey demeden kullananlar var o hiç etik değil bence."* (Katılımcı 3, 30, Erkek)

Şeffaflığın etik için temel unsur olduğunu belirtirken, özellikle veri toplayan kuruluşların rıza alma ya da bilgilendirme formlarını genel olarak veri toplanan bireyleri değil, kendilerini korumaya almak için yaptıkları ve bireyin verisinin farklı amaçlarla kullanıldığı noktalarda, zaten kendisinin izin verdiğini söyleyebilmek için bu tür bir sürecin yürütüldüğünü düşündükleri görülmektedir.

> *"Bence bunun gerekli olduğunu düşünüyorum çünkü o noktada gerekli herhangi bir bu aslında şu şekilde. Kişilerin ve kurumların kendini güvenceye alması yani aslında bu karşısındakileri koruma amaçlı değil de kendini koruma amaçlı herhangi bir durumda gidip böyle bir şey oldu bu benim başıma geldi dediğin noktada evet ama sen bunu onaylamışsan. Sen buna izin vermişsin. Ben bunu asla kişileri koruma amaçlı olduğunu düşünmüyorum. Kurumları garanti altına alıyor".* (Katılımcı 4, 26, Kadın)

4.4.3. Uzmanların Başa Çıkma Yöntemleri

Giddens, ontolojik güvenlik kavramından bahsettikten sonra uzmanların da kendi aralarında belirli değişimlerle ilgili ortak bir sonuca ulaşamadıklarını ve çeşitli gruplara ayrıldıklarını belirtmektedir. Bu çalışmada da aynı şekilde ontolojik güvenlik algısının değişimini tespit etmeye sebep olan büyük veri ve yeni gözetim pratiklerinin toplumda yarattığı değişimlere karşı uzmanların yine farklı gruplar altında yer aldıkları görülmektedir. Bir katılımcı bu tezde de bahsedilen ve literatüre GPS Ölümleri ismiyle geçen, bireylerin dijitale o kadar inanmış bir halde olduklarını ve fiziken var olmayan fakat dijitalde varmış gibi gözüktüğü için o yöne gitmeyi tercih edip öldükleri bir vakadaki gibi bu sistemlerin verdiği verilerin ne kadar hayata dahil olduğunu göstermektedir. Büyük veri artık insanların gerçekten vazgeçemeyeceği, sosyal ilişkilerin, ulusal güvenlik pratiklerinin, risklerden korunmanın, bir bilgiye ulaşmanın ve daha birçok şeyin bir parçası haline gelmiştir. Katılımcı bunu "dijital haritanın üzerinde olmayan bir yol bizim açımızdan yoktur" şeklinde özetlemektedir:

> *"Yarın öbür gün bildiğimiz otonom araçlara güvenliğimizi teslim edeceğiz. Bunun içerisinde tıbbi cihazlar, savunma sistemleri, gündelik yaşamda kullanıyor olduğumuz beyaz eşyaları, televizyonları da alabiliriz. Bir televizyon markasının bir tarihte bünyesinde yer alan kameralardan sürekli olarak ses biyometri ve ses alındığına dair çok yaygın bir şey vardı. Araştırmalar da yapıldı. Kullanılan yapay zekâ asistanları Siri ve türevleri gerçek zamanlı olarak aktive ettiğimiz zaman bizi takip ediyor ve izliyor. Bizim yaptığımız sorgulamalar ve konuşmalar da biz zaten neyle ilgilendiğimiz araştırdığımız arama motorlarından daha kritik şeyleri biz paylaşıyoruz. Aldığımız bilgileri de navigasyon dahil olmak üzere bizi yanlış yönlendirdiği zaman nereye gittiğimizi bile bilmiyoruz. Olmayan yollar olabilir. Dijital bir haritanın üzerinde olmayan bir yol bizim açımızdan yoktur."* (Katılımcı 13, 57, Erkek)

En kısa haliyle pragmatik kabulleniş, modern dünyada olanlar üzerinde bireyin kontrolünü kaybetmesi ve uzmanların yalnızca geçici kazanımlar için plan yapılabilir ve umut beslenilebilir şeklinde düşündüğü bir grubu açıklamak için kullanılmaktadır. Pragmatik kabullenişte vurgulanan örtülü bir kötümserlik ya da umuttur. Pragmatik kabullenişin bu araştırmada görülen örtülü kötümserlikle bağlantılı ilişkisi, süper panoptikonda özellikle vurgulandığı gibi, günümüzde

eğlenmek için ya da çeşitli sebeplerle bireylerin kendi verilerinden feragat etmeleri ve şu anki düzen içerisinde kendilerinin birer ürün haline gelmelerini kabul etmeleridir. Katılımcıların tamamında bu anlamda bir tür pragmatik kabulleniş görülmekte olup, bu sistemler içerisinde yer alan uzmanlar olsalar da özellikle güç dengeleri ve önceden de bahsedilen inisiyatif alabilme sınırları sebebiyle bu tür bir düşünüşe sahip oldukları görülmektedir. Bu kabullenişi katılımcılardan bir tanesi şu şekilde ifade etmektedir:

> *"Burada da aslında biz bilgi korumaya girebiliriz ama bu kadar fazla kasarsak çağımızın meyvelerini yiyemeyeceğiz. Ben ChatGPT'yi sonuna kadar kullanmak istiyorum sonuna kadar da bilgilerim açık o noktada. Bana sorduğu sorularda da cevaplıyorum birazcık artık vatandaş olarak madem iç işleri bakanlığı çıkıp benim yüzümü taratabiliyor ben de tüm bilgilerimi vererek kredi kartı adres olmaz örnek veriyorum bilgi çalışmamla ilgili bir bilgiyi sızırabilir abi önemli değil diyorum öyle bir noktaya geldim. Mücadeleyi bıraktığım bir noktaya geldim."* (Katılımcı 16, 26, Erkek)

İkinci grup, sürekli iyimserlik, akla duyulan ve teknolojiye duyulan inanç ile tarif edilmektedir. Bu grup büyük verinin sosyal fayda sağladığını düşünmekte; iklim değişikliği, çevre sorunları gibi konuların yanı sıra dijital eşitsizliklerin önüne geçmede de çok etkin bir araç olacağını, ifade etmektedir. Bunun yanı sıra büyük veri yoksulluğu engelleme ve toplumda var olan her tür eşitsizliği engelleme, bireylerin daha çok seslerini duyurabilme, güç dengelerini değiştirebilme gibi pek çok fayda da sağlayabilmektedir. Bu grup, yeni gözetim pratikleri temelinde de bakıldığında, özellikle gözetim pratikleriyle suçluların tespiti, ulusal güvenlik anlamında ilerleme, şirketler açısından müşterilere daha doğru ve uygun ürünlerin ulaştırılması, bireyler açısından sağlık, ulaşım gibi hizmetlere daha kolay ulaşma gibi pek çok unsurdan bahsetmektedir. Sosyal fayda için büyük veri anlamında yorum yapan katılımcılardan, sürekli iyimserlik bakış açısına dahil bir tanesinin görüşü şu şekildedir:

> *"Yoksullukla mücadele için de büyük veri kullanabilirsin. Mesela telefon görüşmelerinin sıklığı ve yoğunluğuna bakarak dünyada tüm ülkelerden veri toplayan sınırlı sayıda ülke var. Burada IMF kendi ülkelerine bakıyor AB kendi ülkelerine bakıyor. UN istatistik tarafında datalar topluyor. Mesela, yoksulluk ölçümlemesi Devlet İstatistik Enstitüsü tarafından yapılamayan ülkeler var özellikle iç savaşın yoğun olduğu, devletin sürekliliği olmadığı*

> *yerlerde oralarda böyle çalışmalar var. Cep telefonu konuşmalarının artması, kişi sayısının artması ve networkün artması doğrudan gelir seviyesiyle doğrudan ilişkili şeylerden bir tanesi. Buna bağlı olarak tüm ülkenin yoksulluk haritasını çıkaran çalışmalar var. Bunun dışında trafik planlaması için kullanabilirsin. Tüm ülkeler kendi trafiğini planlıyor yine sinyallerin yoğunluğuna bakarak insanlar nereden nereye seyahat ettiler buna bakarak görebiliyorsun. Ülkenin ekonomik planlamasında çok yaygın kullanılan şeylerden bir tanesi aynı zamanda. Kredi kartı datalarına bakarak Kolombiya'da yapılan bir çalışmada Avrupa'dan gelen kayıtlı kredi kartlarının Kolombiyadaki haritasını çıkararak turistler nereden geliyor, ne harcıyor, hangi sektörlerde neler yapılmış çıkararak onun üzerinden bir turizm etkinliğinin yeniden planlaması yapılmış mesela. Bu salgın modellemesinde en çok kullanılan şeylerden bir tanesi. Bizim de bu cep telefonu üzerinden yapılan Evde Kal uygulamasındaki 1850'de İngiltere'de yapılmış onun ilk örneği. O yüzden büyük veriyi kalkınma için kullanmak çok mümkün. Uydu görüntüsü üzerinden ışık yoğunluğuna bakarak gelişmişliğin ölçülmesi sanayinin olduğu yerde elektrik tüketimi çok daha fazla uydu görüntüsü bunu yakalıyor. Okyanuslardaki ışık kırılmasına bakarak uydu görüntüsü üzerinden okyanus kirliliğini ya da deniz seviyesini ölçebilmek mümkün. İklim değişikliğini büyük veri üzerinden ölçebiliyorsun. O yüzden aslında pek çok örneği var, tarımsal alanda da çok yaygın kullanılmaya başlandı uydu görüntülerine bakarak ülkeler ne üretiyor, hava koşullarına bağlı olarak neler yapılabilir, bir tarım tarafından çiftçiyi güçlendiren bir şey olarak da kullanabilirsin bunu öte taraftan bir güç yaratmak için bir tekel haline getirip tarım tekelleriyle beraber çalışmak da bir alternatif. O yüzden veriyi nasıl kullanmak istediğine bağlı olarak değişebilecek bir şey. Sosyal fayda için veri ile otuz tane hepsi birbirinden farklı gruptan gelmiş kişiyle 11 hafta boyunca veri bilimi öğrendik ve tartıştık. Sosyal etki proje yönetimi tartıştık sonra da kamu veya sivil toplum örgütleri ile proje geliştirdiler. Dünyadaki böyle örnekleri takip etmek önemli. İnsan evladının nereyi kullanmak istediğine bağlı. Genelde çok hızlı yükselen alanlar teknoloji çok hızlı değişiyor insanlar ve toplumsal süreçler daha geriden geliyor. Kamunun buna fon ayırması çok daha zor özel sektörle yarışması çok daha zor. Mainstream'in dışında dünyada böyle bir hareket var.* (Katılımcı 12, 43, Erkek)

Sürekli iyimserlik düşünüşünde olan bireylerin de özellikle güç dengeleri ve veri gözetimi anlamında bir tür pragmatik kabullenişle birlikte alaycı kötümserliğe sahip oldukları görülmektedir. Bunun sebebi de araştırmanın pek çok yerinde bahsedildiği gibi, bu tür sistemlerin artık kontrol edilemeyecek bir noktaya gelmesi ve temelde kimin kullandığına bağlı olarak değişmesidir. Çin'in Sosyal Puanlama Sistemi kurması, İran'ın yapay zeka teknolojisiyle baş örtüsü takmayanları tespit etmesi, bir araştırma şirketinden temeli din sayılabilecek çıkan savaşta olan iki ülkenin atalarını tespit etme amacıyla verilerini izinsiz şekilde ele geçirerek kötü niyetli kişilerin bu verileri satmaya yönelik haberleri gibi pek çok yeni gözetim pratiği kaynaklı uygulama ile bu sistemlerden bir

kaçışın mümkün olmadığını bu sebeple de pragmatik kabullenişin zorunlu olduğunu göstermektedir. Sürekli iyimserlik, bunlar olurken arka planda özellikle teknik anlamda ne tür faydalar sağladığını görmeyi ifade etmektedir. Katılımcılardan bir tanesi Çin örneğinden yola çıkarak, kötülüğün ne noktada başlayacağını düşündüğü şu şekilde ifade etmektedir:

> *"Ben distopyayı zaten seven ilgilenen okuyan da biriyim. Bence distopik noktalarda yapılacak kesinlikle sınır yok. Çin'in skorlaması diyoruz ya. Çin'in skorlaması bizim için bir başlangıç olur bir son olmaz. Ondan sonrasında artık sizin atacağınız adımlar bilinir, hangi skorda olacağınız bilinir olduğunuz değil. Çin'in yaptığı şu an nerede olduğunuzu sorgulamak. Bir de bir şeyleri yapmadan sizin adınıza karar verildiğini düşünün. Zaten artık o kadar veri toplanacakken sizin adınıza iki saat sonra nereye gideceğiniz, nasıl bir tepki vereceğiniz, nasıl bir tartışma yaşayacağınız bilinecek ve buna göre de bir yargı verildiğini düşününün. Ben sizin şu an bin gününüzü inceledim doktorda ve herhangi bir anketten bu konuşmadan sonra sizin otomatik olarak kahve ve sigara içmeye gittiğinizi biliyorum ve bu Çin'in skorlamasında eksi 5 puan atıyorum. Siz daha bunu yapmadan ben günün sabahında size eksi beş yazıyorum. Esas kötülük burada başlar. Sizin hür iradenizin alındığının bir göstergesi olur bu. Siz bu sigarayı içmediğinizde yani ufak bir yanlış tahmin oldu deriz. Ama bu belki insanların yüzde 80'i için devam edecek." (Katılımcı 16, 26, Erkek)*

Üçüncü grup, alaycı kötümserlik, bastırma ve şimdinin keyfini çıkarma özellikleri ile açıklanmaktadır. Bir katılımcının ironik bir şekilde robotlar dünyayı ele geçirecekse de henüz bunun gerçekleşmediği şeklindeki yorumu bu durumla ilişkilidir.

> *"Birincisi distopya bizim kopyalanmamız hem sesimiz hem görüntümüzle. Benim yapmadığım bir şeyi bana söyletip benim bütün bir yapımı hayatımı kaydırabilirler çok tehlikeli bir şey ve bunun önlemi nasıl alınacak bilmiyorum. İkincisi bizim kişiliğimizi ve karakterimizi yok eden bir şey hepimizi birbirine benzeten sıradanlaştıran tepkilerimizi azaltan işte orman kesiliyor ben Twitter'dan yazıyorum benim o insanlara gidip omuz omuza destek vermem lazım ve bu anayasalda karşılığı olmayan bir şey ben sosyal medyanın bunu gölgelediğini düşünüyorum. Kolektif bir bilinç oluşturamıyoruz bu da hakkımızın daha fazla yenileceğini zaten 1984 dünyasında yaşıyoruz da etkimiz olmuyor gibi. Durdurmak için de çarka dahil olup çarkın içine çomak sokmak lazım. Ben en azından şimdilik şöyle bir endişem yok robotlar dünyayı ele geçirecek mi vs. o bugünün işi değil ona daha var daha tehlikeli bu iki konu. Hem bireysel hem toplumsal."* (Katılımcı 14, 26, Erkek).

Dördüncü grup, radikal katılım, önemli sorunların olduğunun bilincinde olan ve onları aşmak için harekete geçilmesi yönünde düşünceleri olan grubu temsil etmektedir. Bir katılımcı ise yine distopyaların artık gerçek olduğunu, kendi distopyasının da geldiğini kabullenerek, bunu ifade etmektedir.

> "*Benim distopyam geldi zaten aslında. Sesini genelde taklit ediyorlar insanların. İnsanların sesini kopyalayarak artık şarkı yapıyorlar, insanların yüzlerini kopyalayarak reklam filmleri çekmeye başladılar. Benim distopyam buydu çünkü bunun gerçeğinden yanlışını ayırmak zor zordan da daha kötü belli bir zaman istiyor. Belirli insanlar onun üzerinde çalışıp en sonunda belki bir kurul kurulacak bunla ilgili gelecekte bilmiyoruz ama bu kurul da aynı hâkimde bekler gibi üç ay sonra bu video yalan ya da bu video gerçek gibi bir görüş sağlayacak benim distopyam bu biraz ve geldiği için biraz tedirginim. Doğurabileceği sıkıntılar beni çok korkutuyor."* (Katılımcı 14, 26, Erkek)

SONUÇ

Bu araştırma, toplumda büyük verinin ve onu destekleyen sistemlerin gün geçtikçe daha fazla gelişerek farklı sonuçlara yol açabileceği düşüncesiyle, yeni gözetim pratiklerinin toplumsal değişim anlamında sonuçlarını ön görebilmek amacıyla gerçekleştirilmiştir. Büyük verinin desteklediği ve onu destekleyen sistemlere bakıldığında yapay zekâ, nesnelerin interneti, dijital medya teknolojileri, bulut bilgi işlem, Metaverse, (bir tür yapay zekâ olsa da özel olarak ismi doğrudan yeni bir sistem olarak kullanıldığı için) ChatGPT, yüz tanıma teknolojileri gibi pek çok farklı sistemden, yenilikten bahsedilmiştir. Büyük verinin bu yenilikler ya da sistemlerle ele alınmasının temel sebebi ise, onlar sayesinde daha çok veriye ulaşması (bu tez özelinde özellikle kişisel verilere daha çok ulaşma imkânı vurgulanmaktadır) ve daha çok veriye ulaşım sağlandıkça, büyük verinin niceliği ve niteliği farklılaştıkça, bu sistemlerin de daha çok işleyebilir, daha farklı işlevler üstlenebilir hale gelmeleridir.

Bu sistemlerin ortaya çıkardığı değişimleri görebilmek amacıyla, bu değişimlere sebep olan büyük veri ve onu destekleyen sistemlerin tasarımını, işleyişini ve muhtemel sonuçlarını ön görebileceği düşünülen veri bilimcilerle (veri bilimciliğin de toplumda yeni bir meslek dalı olarak göze çarpması ve içeriğinin değişmesi sebebiyle bu çalışmada detaylı bir şekilde tanımlanmaktadır) derinlemesine mülakatlar ve uzman mülakatları gerçekleştirilmiştir. İki tür mülakat tekniği kullanılmasının nedeni veri bilimcilerin, hem büyük verinin ve onun yarattığı yeni gözetim pratiklerini deneyimleyen hem de onları tasarlayan, geliştiren ve onunla analiz yapan bireyler olmasıdır. Yapılan mülakatlar sonucunda hem birer uzman olarak katılımcıların bu alandaki bilgilerinden faydalanılarak bu sistemlerle bağlantılı olarak toplumsal değişimler açıklanmaya çalışılmış; hem de bu sistemleri deneyimleyen bireyler olarak bu tür toplumsal değişimlerin onları ontolojik güvenlik anlamında ne tür bir değişimle karşı karşıya bıraktıkları anlaşılmaya çalışılmıştır.

Araştırmanın verileri nitel analiz yöntemi ile analiz edildikten sonra araştırmanın verileri, “Araştırmanın Bulguları ve Verilerin Analizi” başlığı altında yer alan dört başlıkla detaylı bir şekilde açıklanmıştır. Analizler ve güncel örneklerle, bu konunun neden hem dünyada hem Türkiye özelinde önem verilmesi aynı zamanda da önlem alınması gereken bir konu olduğu açıklanmaya çalışılmıştır. Büyük veri ve yeni gözetim pratiklerinin yol açtığı toplumsal değişimlerin, bireylerin bilinçli ve onlara uyum sağlayabilecekleri şekilde gerçekleşebilmesi için ekonomik, siyasi, kültürel, hukuki ve toplumsal alanda çok ciddi düzenlemeler yapılması gerektiği görülmüştür. Uluslararası anlamda bakıldığında da Türkiye’nin büyük veri üretme anlamında temel olarak kullanılan tüm platformlarda aktif bir toplum olarak rol alması (sürekli olarak bireylerin özellikle kişisel verileriyle büyük veriye dahil olmaları) da çalışmanın Türkiye özelinde de önemini bir kez daha göstermiştir.

Verilerin analizi sonucunda ulaşılan bulgulara göre, ilk bölümde “Veri Bilimcilerin Gözünden Büyük Veri” başlığı altında, büyük verinin dijital gözetim pratiklerinin temelinde önemli bir unsur olarak yer almasının en önemli sebeplerinden bir tanesi büyük verinin de kendi içinde tanımının ve etki alanının değişmesidir. Veri bilimcilerin belirttiği şekilde, eskiden daha çok hacim, çeşitlilik, doğruluk gibi ya da araştırmada detaylı şekilde açıklandığı şekilde 3V, 4V ya da 7V şeklinde tanımlanan büyük verinin artık sadece yapısal verilerden değil, yapısal olmayan ya da yarı yapısal verilerle de birleşerek tamamen farklılaştığı ve bu değişimin de kullanım alanını genişlettiği belirtilmektedir. Büyük verinin sadece yapısal olmayan verilerden oluşmaması ile büyük verinin günümüzde doğal dilleri, görsel öğeleri (videoları, fotoğrafları, resimleri vb.), ses verilerini, biyometrik verileri ve sensör verileri gibi pek çok veriyi de kapsamına alarak daha da büyümesinden bahsedilmektedir. Bu noktada büyük veri bireylerin kişisel verilerini toplama, depolama ve işleme anlamında da tamamen farklılaşmış, veri tümleştirme denilen işlemleme ile bireyler ya da kitleler hakkında tahminleme ya da manipüle etme imkânı hiç olmadığı kadar artmıştır. Bu noktada tezin birçok kısmında büyük verinin, bireyin ve bedenin sayısallaşması sayesinde

verileştirmeye imkân sağladığı ve verileştirme sayesinde yapılan veri gözetimi ile işleyen ciddi bir toplumsal olgu haline geldiği görülmektedir.

Verileşme ve veri gözetiminin, gerçek anlamda sorgulanması gereken bir durum olduğu katılımcıların verdiği ve güncel olarak dünyada yankı uyandıran örneklerden anlaşılmaktadır. Bu örneklerden ilki tezde çokça bahsedilen Çin'in Yapay Zekâ Destekli Puanlama Sistemi'dir. Buna ek olarak, Gaziantep Belediyesi'nin bir açıklamasıyla, sosyal medyada belediyenin sosyal puanlama sistemine geçildiğine yönelik haberlerin artmasıyla belediyenin bunun bahsedilen bir sistem olmadığına yönelik basın açıklaması yapmak zorunda kalması durumun ne kadar güncel ve mümkün olduğunu göstermektedir. Aynı zamanda İran'ın başörtüsü takmayan kadınları yapay zekâ ile tespit ederek çeşitli yaptırımlar uygulayacağına yönelik haberler, İsrail-Filistin savaşında savaşın bir anlamda dijital savaş olarak ilerlediğine yönelik sosyal medya paylaşımları ve tarafların kendilerinin bu konudaki paylaşımları dikkat çekmektedir. Günümüzde artan salgınlarla hem fiziksel hem dijital gözetim sistemlerinin artırılarak sağlık ve dijital risk temelinde önlemler alınarak bireylerin daha fazla yapısal ya da yapısal olmayan veri üretmesi de en önemli örneklerdendir. Bunun yanısıra dijital gözetimin sebep olabileceği veri ihlalleri ve veri manipülasyonları da neden verileşme ve veri gözetiminin bu derece önemli olduğunu açıklamaktadır.

Veri bilimcilere göre büyük verinin değişen içeriği ve tanımı onun farklı olgularla birlikte tanımlanmasına sebep olmuştur. İlk anlamıyla büyük veri karar verme mekanizmalarının temel öğesidir. Veri bilimciler bu anlamda en önemli toplumsal değişimi, karar verme mekanizmalarında kararın deneyimleyen kişilerce ya da o alanın uzmanlarınca değil, büyük veriye dayanan otomatikleştirilmiş sistemler tarafından verilmesi şeklinde açıklamaktadır. Büyük veri ve yeni gözetim pratikleri bu anlamda, hukukta, sağlıkta, suçta ve pek çok toplumsal olayda işlemlemenin temel karar verici olmasına neden olmaktadır. Bu büyük verinin, kültürü de içine alarak dijital kültürün en önemli unsurlarından bir tanesi olması ve özellikle sosyal ilişkilerde ve sorumluluklar alanında da büyük verinin aktif unsur haline gelmesiyle ilişkilidir.

Katılımcıların yanıtlarında büyük verinin ikinci tanımı büyük verinin bir tür sermaye olduğu şeklindedir. Veri bilimciler, büyük verinin artık ciddi bir sermaye olarak değerlendirilmeye başlandığını, eskiden sadece işleme “para eden” bir şeyken, şimdi veriye sahip olmanın bile ciddi bir sermaye olduğunu ve güç dengelerini etkilediğini belirtmektedir. Büyük veri bu anlamda, katılımcıların görüşlerine bakıldığında, dijital kapitalizm olarak tanımlanan sistemde de en etkili araçlardan bir tanesi haline gelmiş, gözetim kuramlarında bahsedildiği haliyle Büyük Birader, dijital kapitalizm kuramındaki gibi, Büyük Öteki olarak toplumda etkisini artırmıştır. Katılımcılar buna vurgu yaparken bir yandan da yararlı ve zararlı algoritmalar temelinde bir ayrım yapılması gerektiğini vurgulamaktadır.

Büyük verinin, değerlendirme sonucunda göze çarpan üçüncü tanımı ise onun bir tür kategorizasyon ya da sınıflandırma aracı olmasıdır. Bunu hem iyi hem kötü anlamda tanımlamaktadırlar. İyi anlamda bakıldığında katılımcılar, büyük veriyi, kişilerin kredi skorlarının daha rahat listelenebilmesi, suçluların daha kolay tespit edilebilmesi, pazarlama alanında bireylere daha iyi öneriler sunma gibi işlevleriyle değerlendirmektedir. Diğer anlamda ise bireylerin büyük veri ve yeni gözetim pratikleri ile etiketleme ve sınıflandırmaya çok açık olduğu özellikle dijital vatandaşlık tartışmalarıyla bunun çok ciddi bir duruma geldiği vurgulanmaktadır.

Katılımcılara kendi çalıştıkları sektörlerde büyük veriyi nasıl kullandıkları ve anlamlandırdıkları sorulmuş, akademi alanında metin madenciliğinden, savunma sanayide siber güvenliğe, özel firmalarda şirket imajını iyileştirmeden, sağlık sektöründe üretilen cihazların test edilmesine pek çok farklı kullanım alanı olduğu görülmüştür.

Veri bilimcilere göre, büyük verinin avantaj ve dezavantajlarına bakıldığındaysa avantajlar olarak büyük verinin teknolojik gelişimi desteklemesi, kullanıcı odaklı içerikler ve farklı platformların kullanımıyla bunun desteklendiği bu sayede yapay zekanın da geliştiği görülmektedir. Bu sayede daha doğru ve hızlı karar

alınabilme imkânı sağladığı, farklı meslek dallarında bireylere hız ve kolaylık sağladığı belirtilmektedir. Aynı zamanda yönelimleri bilerek tahminlemenin iyileştirilmesi ve daha iyi hizmet sunma imkanının olduğu da ifade edilmektedir.

Dezavantajlarına bakıldığındaysa; bireylerden unutulma hakkının alınması, ileride kontrol amaçlı yaptırımlar için kullanılabilecek olması, veri güvenliği, manipülasyonu ve kontrol anlamında sorunlar yaratabileceği, bireyin verisi üzerinde kontrolü kaybederek bozulmuş veri durumuna sebebiyet verebileceğinden bahsedilmektedir. Aynı zamanda bazı meslek dallarının yok olması ve bu bireylerin işsiz kalabileceği de söylenmektedir. Katılımcılar tüm bu açıklamaların yanında avantaj ve dezavantajların tamamen bu sistemlerin nasıl ve kim tarafından kullanılacağına bağlı olduğunun öneminden bahsetmekte, yanlış durumlarda kullanıldığında ayrımcılık, güvenlik ihlali, anonimliğe veda, devlete verilen geniş yetkiler, düzenlenmemiş bilgi işlem gibi sorunlar olacağını, avantajının bireylere değil yalnızca şirket, kurum ve devletlere olacağını belirtmektedir. Bu anlamda en büyük sorunlar gücün tekelleşmesi, yankı odası, panoptik sınıflandırma, manipülasyon, sosyal ilişkilerde daha önyargılı olabilme olarak belirtilmektedir.

Büyük veri, katılımcılar tarafından, yeni karar verme kültürünün temelinde yer alması sebebiyle, bireylerin ve bedenlerin sayısallaştırılmasıyla dijital bedenler kavramıyla; kimliklerinin de profil çıkarma, itibar puantajı ve kartografi gibi açıklanan süreçlerle sayısallaşmış benlik kavramıyla bağlantılandırılmaktadır. Bu sistemde özellikle büyük veriyle beslenen yapay zekanın da toplumların oluşturduğu toplumsal eşitsizliklerden beslendiği ve bu sebeple de yanlı olabileceği, örneklemin tam alınmaması ya da dijital ayrım sebebiyle dışlanma durumuna sebep olabileceği belirtilmektedir. Yeni karar verme kültürünün özellikle kanunlar ve etik anlamında düzenlemelere ihtiyaç duyduğu, karar verme mekanizmalarında insana has vicdan, sağduyu ve duygusal öğelerin yer almamasının sorun oluşturduğu belirtilmektedir. Bu anlamda yapay zekanın kendi iradesine dayalı hareket etmeye başlaması ve “dünyayı sizden iyi yönetiriz” mesajı vermesinden bahsedilmektedir.

Veri bilimcilere, KVKK'nın bu anlamda yeterli olup olmadığı sorulduğunda ise teknolojik gelişmelerin çok hızlı olduğu ve hukuki alanın bu anlamda yetişilemeyebileceği söylenirken, bazı katılımcılar bu düzenlemeleri yeterli buldukları halde yaptırımların yetersiz olduğunu belirtmektedir. Bu anlamdaki sıkıntı katılımcılar tarafından bilgi asimetrisi kavramıyla açıklanmakta, bireylerin kendi verileriyle ne yapıldığını bilmemesi fakat kurum ve kuruluşların bunu kendi çıkarları doğrultusunda kullanması açıklanmaktadır. Bu noktada temel sıkıntı yapılanların şeffaf olmaması, bireylerin bilinçli davranmamasıdır.

Katılımcılara KVKK ile ilgili görüşlerinden sonra özellikle veri ihlali ile ilgili sorular yöneltilmiş, ulusal veri ihlalleri ve uluslararası veri ihlalleri arasında ilk akıllarına gelen olaylar sorulmuştur. Türkiye'de siyasilerin kasetlerinin çıkması, ünlülerin Cloud hesaplarının hacklenmesi, (genel olarak devletin tuttuğu veriler olsa da farklı ifadeleriyle) e-devletten verilerin çalınması, nüfus cüzdanı bilgilerinin çalınması, e-nabızdan alınan verilerin çalınması, MHRS'den verilerin çalınması, NVI'nden verilerin çalınması söylenmiştir. Uluslararası anlamda katılımcıların aklına gelen ilk veri ihlalleri sorulduğunda ise katılımcıların genel olarak ortak noktada buluştukları; Facebook-Cambridge Analytica Olayı, Wikileaks sızıntıları, Snowden-NSA Olayı olarak üç temel olaydan bahsettikleri görülmüştür. Bu noktada katılımcıların bazılarının veri ihlali ile veri manipülasyonunun aynı şey olmadığını, birey onay verdiği, çerezleri kabul ettiği, sözleşmeleri okumadan onayladığı sürece verilerin kamusal alana açık hale geldiğini ve bu noktada algoritmik manipülasyona açık olduklarını belirttikleri görülmektedir. Katılımcıların bazılarının çalıştıkları verileri satmak için kendilerine teklifler geldiğini söylemeleri fakat bunu reddetmeleri ise veri ihlalinin ne kadar önemli ve sorunlu bir durum olduğunu göstermektedir.

Bu durumlara bakıldığında neler yapılması gerektiği noktasında katılımcılar özellikle bakanlıklardaki alt yapı çalışmalarının önemine, buna ayrılan sermayeye, devlet kurumlarının ve önemli verilerin toplandığı platformların siber saldırılara karşı güçlü hale getirilmesine vurgu yapmaktadır. Bir diğer öneri ise uzmanların ya da kurumların verileri tutarken anonimleştirerek daha dağınık bir

şekilde, hatta daha kısa süreli tutması ve veri ile işlem bittiğinde bu verilerin silinmesidir. Diğer bir öneri ise bireysel olarak daha bilinçli olunması ve bu sistemlerin nasıl kullanıldığına dair bireylerin daha bilgili olması gerektiğidir. Özellikle veri ihlallerinin önüne geçilebilmesi için güç ilişkilerindeki dengenin önemli olduğu, büyük veri ayrımındaki gibi büyük veri zengini ve yoksulu durumunun oluşmasının önüne geçilmesi gerektiği söylenmektedir. Bu anlamda devletlerin ya da sorumlu kurumların veri ihlali yapanlara ciddi yaptırımlar uygulaması gerektiği vurgulanmaktadır. Tüm bunlara ek olarak eğitim alanında bireylerin küçük yaştan itibaren bu konularda bilgilendirilmesi, hatta yeni gelişen (ChatGPT gibi) sistemlerle ilgili eğitimler verilmesi gerektiği belirtilmektedir. Sadece dijital yerlilere değil, dijital göçmen ve dijital melezlere de özellikle veri güvenliği konusunda, lise ya da üniversite düzeyinde eğitim verilmesinin bilinçlenmeyi artırabileceği düşünülmektedir.

"Veri Bilimcilerin Gözünden Büyük Veri" bölümünün son kısmında katılımcıların genel anlamda büyük verinin toplumsal değişimde yıkıcı/tehlikeli bir güç haline gelmesi bakımından değerlendirme yapmaları istenmiştir. Bu doğrultuda ilk olarak bir şeyleri sürekli kolay yoldan yapmanın insanların düşünmeyi unutmalarına sebep olabileceği ve daha tembel bir konuma geçebilecekleri (hatta zekalarını düşürebilecekleri) belirtilmektedir. İkinci olarak, seslerini duyurmak yerine daha pasif hale gelebilecekleri, sosyal medyadan paylaşım yaparak bir şeyleri protesto etmenin faydalı olmayabileceği belirtilmektedir. Üçüncü olarak, bireyin anonimliğinin kaybolması ve sürekli kontrol edilerek yaşadıklarını düşündükleri için özgür bir şekilde davranamayabilecekleri; bireylerin tercihlerinin ve hatta kişiliklerinin bilindiği bir düzende yaşamak zorunda kalmalarından bahsedilmekte; birey karar ve duygu durumlarının daha kolay etkilenebileceğinden bahsedilmektedir. Dördüncü ve son olarak ise, kültürel geleneklerin bile bu sistemlerle etkilenebileceği (evlilik pratiklerinin değişmesi gibi) ve yönlendirilebileceği söylenmektedir.

Verilerin analizinin ikinci bölümde "Veri Gözetimi ve Toplumsal Değişimler" başlığı altında öncelikle veri bilimcilerin gözetim kavramıyla ne düşündüğüne

bakılmıştır. Buna göre katılımcıların hem fiziksel hem dijital gözetime vurgu yaptıkları, bireylerin rutinlerinin, kitlesel bir şekilde her zaman ve her yerde izlenme vurgusu yaptıkları görülmektedir.

Kitlesel gözetim ilk olarak dijital risklerle (Beck'in kavramı) bağlantılandırılarak, devlet odaklı bürokrasiler ve uluslararası şirket iş birliğiyle herkesin bilgilerinin her an kaydedilmesi ve güvenlikle bağlantılı olarak kullanılması şeklinde tanımlanmaktadır. İkinci ve risk ile bağlantılı olarak, gözetimin ulusal ve uluslararası güvenlikle bağlantılandırıldığı, yeni risklerden kaçınmak için bireylerin verilerini feda ettiği ya da kurum ya da kuruluşların bu beyanla verileri kullandığı belirtilmektedir. Bu anlamda katılımcıların bazılarının nüfusun çoğu gözetlenirken, kendisinin bundan kaçmak için çaba göstermelerinin bir önemi olduğunu düşünmemeleri önem arz etmektedir. Gözetim üçüncü olarak, ötekinin tanımlanması olarak açıklanmış, yabancıların profilini çıkarmak, onları marjinalleştirmek ve bu marjinalleştirme ile yaptırımlar uygulamak üzerinden tanımlanmıştır. Bu çerçevede uzmanların bazılarının kendileri tasarlarken kurallara uygun davransalar ve ayrımcılığa sebebiyet vermemek için gerekli önlemleri alsalar da sonradan ayrımcılık (etnisite, ırk, cinsiyet, gelir ayrımcılığı gibi) yapıldığını, inisiyatifin tamamen kendilerinde olmadığını düşündükleri görülmüştür.

Veri gözetimiyle ilgili en çarpıcı verilerden bir tanesi büyük veri, yapay zekâ, sosyal medya gibi sistemlerin atom bombasına benzetilerek, onun da iyi bir niyetle ortaya çıktığını fakat kötü birinin eline geçtiği zaman kötü sonuçlar vereceği benzetmesi olmuştur. Bir başka çarpıcı tepki, kitlesel gözetime yönelik tepkidir. Suça karışmayan bireylerin bu kadar kolay ulaşılmayan bir halde olması gerektiği belirtilmektedir. Diğer tepki, güvenlik temel alınarak belirli ayrımcılık risklerinin ortaya çıkmasının yanı sıra, verilerin denetim, gözetim ve belirli otoritelere itaat riski taşıması olarak ifade edilmiştir.

Bu noktada özellikle bazı katılımcıların şirketlerin yaptığının bir tür gözetim olmadığını düşünmesi ve gözetim dendiğinde kamu üzerinden, devletler ve

güvenlikle bağlantı kurması da önemlidir. Bu doğrultuda katılımcılara devletlerin veri toplamasının sebepleri sorulmuş, sağlık kayıtlarının tutulması, askeri güvenlik sistemlerinin kurulması, suçluların yakalanması, nüfus, doğum, yaş, iş durumu gibi verilerin tutulması gibi sebeplerden bahsedilmiştir. Bu sebeplerin yanı sıra, katılımcıların özellikle etiketlemeye, ayrımcılığa, panoptik sınıflandırmaya ve otoriterleşmeye vurgu yaptıkları görülmüştür.

Gözetime bakış açılarında tüketici pratiklerini belirlemekten, devletlerin vatandaşlarını kontrol etmesine, bireylerin Metaversete sanal dünyalarının yaratılmasına, ayrımcı sistemler kurulmasına ve daha birçok noktaya değinen şekilde ilerlediği ve çok kapsamlı olduğu görülmektedir. Katılımcılara bu sistemlerden kaçış gerekli mi ya da mümkün mü diye sorulduğunda ise, neredeyse hepsinin bunun mümkün olmadığı konusunda görüş bildirdiği görülmüştür. Bunun sebeplerini ise, telefonların WhatsApp'ın serverlarına direk kaydolması, görüntü işlemenin gelişmesi, e-ticaret siteleri, mail kullanma, araştırma yapma, iş yerlerinin özellikle salgın hastalıklarla birlikte çevrimiçi platformları zorunlu kılması, banka işlemleri için veri vermek zorunda kalma, eğitimin de dijitalleşerek küçük yaştan itibaren tablet ve telefon kullanımının artması ve küçük yaşta dijital sistemlerin kullanımının artması, salgının bunu hem ulusal hem uluslararası anlamda artırması, bu sistemler kullanılırken bilinçli olunmadan tüm çerezlerin, onay metinlerinin kabul edilmesi ve incelenmemesi, daha uygun ya da ücretsiz olduğu için lisanssız program kullanımına yönelinmesi ve ücretin bireyin kendi verisi üzerinden alınması gibi sebeplerden bahsedilmiştir. Özellikle günümüzde, veriyi depolama ve işleme alt yapısının artırılmasına yönelik çalışmaların olduğu ve bundan kaçış olmayacağı da bu noktada belirtilmektedir.

Katılımcılar bu sistemlerin faydalı olduğunu belirtmekte, bunları kullanmaktan memnuniyet duymakta ama buradaki asıl sorunun demokratik erişim olduğundan bahsetmektedir. Bu noktada bireylerin mahremiyetlerine saygı duyulması önem arz etmektedir. Katılımcılar mahremiyetle evlerini, bedenlerini, düşüncelerini kastettiklerini ifade ederken, bireyin paylaşmak istemediği ve

rızası olmadığı her şeyin mahremiyete girdiğini söylemeleri de önem taşımaktadır. Mahremiyetin yalnızca bireyler bazında değil, ülkeler bazında da günümüzde önem taşıdığı söylenmekte, Kuzey Kore ve Çin'in Google Maps üzerinden kendi mahremiyetlerini korumak için, bir savaş durumunda dezavantajlı olmamak için önlemler aldıkları şeklinde örnekler vermektedirler.

Verilerin analizinin üçüncü kısmında, "Sosyal İlişkiler ve Sorumluluklar Alanında Büyük Veri" başlığı altında, bireylerin sistemleri ve içeriklerini bilmeleri açısından sosyal ilişkilerinde büyük veri ve mikro düzeyde veri gözetimi pratikleri incelenmiştir. Katılımcıların Giddens'ın da ayrım yaptığı gibi yerel ağlarında, akrabalığa, arkadaşlığa dayanan eski ve samimi sosyal ilişkilerinde bu sistemleri çok fazla kullanmayı tercih etmedikleri ama ilk defa tanıştıkları kişiler ve özellikle iş bağlamında tanıştıkları bireyler için ciddi düzeyde bu platformları kullandıkları görülmüştür. Veri gözetimini mikro düzeyde kullanma açısından, Giddens'ın kavramlarıyla, tanıdıklık ve yabancılık anlamında bir fark olduğu görülmektedir. Katılımcıların bu doğrultuda, LinkedIn'e çok önem verdiği ve hatta bu uygulamanın katılımcılar tarafından vazgeçemeyecekleri uygulama olarak tariflendiği görülmektedir. Sosyal hayat için ise Instagram, Google ya da Facebook gibi sosyal ağ ya da arama motorlarını kullandıkları bilgisine ulaşılmıştır.

Katılımcıların hakkında bilgi sahibi olmak istedikleri kişilerle ilgili genel olarak arama motorundan arattıkları, Instagram profili açıksa orada sosyal hayatına ve pratiklerine baktıkları, Twitter'ı varsa düşüncelerine yönelik bilgi sahibi oldukları, iş hayatı ile ilgili bilgi edinmek ve iş çevresini, deneyimlerini görebilmek için LinkedIn üzerinden araştırma yaptıkları görülmüştür.

Veri bilimcilerin, biriyle tanıştıklarında ve onla ilgili arama yaptıklarında hiçbir veri çıkmadığında ne düşündükleri de onlar için bu verilerin ne kadar önemli olduğunu gösteren bir durum olarak ele alınmıştır. Bu durum incelendiğinde, katılımcıların üç gruba ayrıldığı görülmektedir. İlk grubun özellikle verisi olmayan kişilere karşı negatif bir ön yargı ile yaklaştığı ve verisi olmayan

kişilerle ilgili kesin bir sorun olduğunu düşündükleri; ikinci grubun bu durumu ilgi çekici ve heyecan verici buldukları; son grubun ise bunu aksine çok doğal bir durum olarak değerlendirdikleri görülmektedir.

Sosyal ilişkilerde yapılan daha mikro düzeyli bu veri gözetiminin, gözetlenen bireyler açısından unutulma hakkı ile ilgili sorun yaratan bir durum olduğu görülmüştür. Katılımcılardan daha genç olanlardan bazılarının bile eskiden kalma etiketlerinin onları rahatsız ettiği yönündeki beyanları bunun ne kadar önemli olduğunu göstermektedir. Özellikle bu aratma pratiğinin, kişilerin ilgi alanlarını tespit etmek, karakterlerini öğrenmek ve bir şekilde iletişim kurmak ya da kurmamak kararını etkilediği görüldüğü için bireylerin unutulmasını istediği verilerin yeni gözetim pratikleriyle silinemez ya da yok edilemez hale gelmesi onlar için sorun oluşturmaktadır. Özellikle bir katılımcının, evleneceği bireye karar verirken, mesleğinden faydalanarak “eşinin parametlerini değerlendirdiği” ve bu şekilde onunla evlenmeye karar verdiğini söylemesi bu anlamda önemli bir veridir. Bireyler bu sistemler sebebiyle ilişkilerinde kişilere karşı ciddi ön yargılar taşıyabilmektedir.

Unutulma hakkının yanı sıra, verinin bozulmuş veri olması, bireylerin kendi verileri üzerinde kontrolü kaybetmeleri en büyük endişe olarak görülmektedir. Katılımcıların özellikle bu endişeyle kendi verileri üzerinden kontrolü kaybederek bu verilerle neler yapılabileceğine dair bilgi sahibi olduklarından dolayı yakınlarını uyardıkları, özellikle çocuk sahibi olanların çocuklarını çeşitli kurallara tabii tuttukları ve kontrol ettikleri görülmektedir. Bu uyarı ya da kısıtlamalara bakıldığında, belirli bir yaşa kadar çocukların kesinlikle sosyal medyayı kullanmaması, hafta içi ekran yasağı uygulanması, ekran kullanımın ödüllendirme mekanizması olarak değerlendirilmemesi, yalnızca çocukların fiziksel ortamda sosyalleştirebilecek olanak olmadığında ekrana izin verilmesi, bu süre içerisinde de ekrandan (x-box gibi oyunlarla diğer arkadaşlarıyla bu sistemler üzerinden sosyalleşmeden) tek başına oynaması, dijital üzerinden arkadaşlarıyla sosyalleşmemesi şeklinde olduğu görülmektedir. Katılımcılar, çocuklardan sonra ise genellikle daha yaşlı bireyleri uyarmaktadır. Bu uyarılar

da verilerini çaldırmama, bağlantılara tıklamama, banka bilgilerini vermeme gibi konularda yapılmaktadır. Ayrıca bebeklerin yüzlerinin de veri güvenliği, unutulma hakkı ve bozulmuş veriyi göz önünde bulundurarak paylaşmaması gerektiği düşüncesi de ön plana çıkmaktadır.

Sosyal ilişkiler ve sorumluluklar alanında büyük verinin güven açısından sorgulanması temelinde ise birey davranışının daha tahmin edilebilir hale gelmesinin bu durumu bireyin daha manipüle edilebilir ya da kontrole açık hale gelmesi bağlamında bir inceleme yapılmaktadır. Bu noktada bireylerin gerçekten veri gözetimini içselleştirerek sosyal ilişki ya da sorumluluklarını birer proje gibi yürütüp yürütmediklerine bakılmaktadır.

Katılımcıların yanıtları doğrultusunda kendilerinin en çok verileştiklerini hissettikleri ortamların, internet, sosyal medya ve dijital medya teknolojileri gibi dijital gözetim mekanları olduğu görülmektedir. Bu alanda izlenmelerinin temel sebebi de buradaki pratiklerin gizlenemez oluşu ve verilerin kaybolmaması olarak belirtilmektedir. Bu noktada veri ihlalinin de alıştıkları bir şey olduğunu ve kendileri yaşamasa da zaten tüm verilerin çalınabilir olduğunu belirtmektedirler. Toplumda yeni gözetim pratikleriyle eskiden distopik sayılabilecek (Sosyal Kredi Sistemi gibi) sistemlerin artık mümkün olduğu, algoritmalarla profil çıkarma, itibar puantajı ve kartografi yapılabileceğinden bahsedilmektedir. Bu sistemlerin özellikle kötü güçlerin eline geçtiğinde ciddi anlamda etik sorunlara yol açacağı, etiketleme riski taşıdığı, kısıtlama ve tekelleşmenin bu anlamda çok büyük sorunlar olduğu belirtilmektedir. Bu sistemler de doğrudan güveni oyunlaştıran, bireylerin toplumsal sorumluluklarını da kontrole sokan bir şey olarak açıklanmaktadır. Öte yandan, katılımcılar özellikle yönetim mekanizmaları kurarken faydalı olacağından, sağlık ve ulaşım alanlarında katkı sağlayabileceğinden, kanunlara uyulmadığı noktalarda ya da suçluların tespitinde iyi olabileceğinden bahsetmektedir.

Yeni gözetim pratikleri, verilerin analizi doğrultusunda, aktif birey pasif birey paradoksuna yol açmaktadır. Katılımcılar, sürekli izlemenin artması, güvenin

soyutlanması yoluyla bireyi birey yapan karar verme, özgür olma gibi niteliklerin etkilenmesinden endişelenmektedir. Bu anlamda özellikle vurgulanan noktalar düzen adı altında seslerinin duyulamaz hale gelmesi ve karar alma mekanizmalarının dışında kalmalarıdır.

Bu anlamda dijital gözetim sistemleri ile dijital aktivizm arasındaki ilişki sorgulanmakta, katılımcıların bir kısmı bu aktivizmin etkili olduğunu, demokratikleşmeye ve katılımcı kültüre katkı sağlayacağını düşünürken; bir kısmının bir tür dışlanma ya da sessizleşmeye yol açacağını düşünmektedir. İlk bakış açısındaki endişeler, bireylerin görüntülerinin, seslerinin kopyalanabilmesi ve bireylerin yapmadıkları şeyleri yapmış gibi gösterilebilmesi, bireylerin verilerinden pratikleri belirlenerek rutinleri ve gelecek hareketlerinin kontrol edilebilmesi ve sıradanlaştırılması, insanların fiziki alanlarda mücadele etme özelliğini kaybederek sanal alanlara hapsolmaları ve kolektif bilinç oluşturamamalarıdır. Toplumsal düzen yeni gözetim pratikleriyle kurulmaya çalışırken, otoriterleşmeye doğru bir yol izlenebileceği bunun da politik gelenekle bağlantılı olduğundan bahseden katılımcılar, bu riskin yanı sıra insanların kara ekranlara hapsolduğunu ve yavaş yavaş diğer insanlardan soyutlandığını düşündüklerini açıklamaktadır.

Dijital gözetim sistemlerinin bir anlamda demokratikleşme simülasyonu olarak nitelendirilebileceği, bireyler uzaktan ve sanal olarak var olmaya çalışırken bir anlamda tepkinin birikmesi ve büyümesinin engellendiği düşünülmektedir. Bu da toplumsal düzenin devam edebilmesi için önemli bir işlev olarak görülmektedir.

Kendileri de uzman olan katılımcıların toplumsal düzenin kurulması ya da kurulmamasında görev alan uzmanlara karşı duydukları güvene bakıldığındaysa, bir grup katılımcının doğrudan güven duyduğu, bazılarının onların teknik bilgi ve yeterliliklerine bakılmadan güvenemeyeceği vurgusu yaptığı, bazılarının ise özellikle Türkiye'de veri biliminin tanımının net olmamasından kaynaklı sorunlar yaşandığı ve bu sebeple bir soru işaretiyle yaklaştıkları görülmektedir. Katılımcıların bir kısmı da onlara güvenmek yerine,

kullanıcı deneyimine daha çok güvenmektedir. Uzmanlara ya da soyut sistemlere güvenememenin temel nedeni ise neredeyse katılımcıların hepsinin bahsettiği şekilde, inisiyatifin uzmanlarda değil, kurumlar, şirketler ya da devlet gibi güçlerin istekleri ve talepleri ile hareket etmek zorunda kalmaları ile ilişkilendirilmektedir. Tüm bu değerlendirmeler doğrultusunda büyük verinin ve yeni gözetim pratiklerinin ne gibi toplumsal değişimlere sebep olacağı ile ilgili katılımcıların görüşleri analiz edilmiş olup, bu noktadan sonra büyük verinin var olan toplumsal değişimlere ek olarak gelecekte ne gibi sorunlara ya da faydalara yol açacağı ve veri bilimcilerin şu anda bu değişimler karşısındaki ontolojik güvenliklerine bakılmıştır.

Verilerin analizinin dördüncü kısmında, “Büyük Verinin Geleceği: Veri Bilimciler ve Ontolojik Güvenlik” başlığı altında, Giddens’ın da dediği gibi 20. yüzyıl ile bilgi ve iletişim teknolojilerinin gelişimi ve dijitalleşmeyle meydana gelen değişimlerin bireyi hedef aldığı özellikle dijital epidemiyoloji, dijital epidermalizasyon ve dijital fenotipleme gibi kuramsal temelde açıklandığı şekilde toplanan verilerin biçimlerinin ve entegrasyonun çok farklı bir boyuta ulaştığı görülmektedir. Sosyal ilişkilerde de açıklandığı gibi, yerelleşmiş güvenin yerine soyut sistemlere güven bir noktada temellenmiştir. Bireylerin genel olarak mahremiyet ya da gizliliğe olan inancını kaybetmeleri, ontolojik güvenlikte, onların baş etmeye çalıştıkları en büyük huzursuzluk faktörlerinden biri olarak karşımıza çıkmaktadır. Bu huzursuzluğun temel sebebi büyük verinin toplumsal anlamda her alanı çevrelemesidir. Büyük veri hem bir sermaye hem bir gözetim aracı hem bir kontrol aracı hem bir güç aracı olarak toplumda etkisini hiç olmadığı kadar artırmıştır. Katılımcıların diğer uzmanların teknik yetkinliklerine ve sistemlerin işleyişinde rol oynaması gereken hukuki uzmanlara bir soru işareti ile yaklaştıkları; uzmanlara güvenmek yerine kullanıcı deneyimine bakma yoluna gittiklerine, en çok vurgu yapılan noktanın ise, soyut sistemlere ve uzmanlara güvenmeme anlamında, karar alma mekanizmalarında ya da bu sistemlerin düzenlenmesinde uzmanların değil farklı kişilerin, kurumların ya da devletlerin söz sahibi olması, inisiyatifin uzmanlarda olmaması ile çok daha büyük bir toplumsal sorun olarak bu değişime baktıklarını göstermektedir.

Kendilerinin de sosyal ilişkilerinde yeni gözetim pratiklerinden faydalandıkları, Giddens'ın akrabalık sistemlerine ya da yerel topluluklara duyulan yerelleşmiş güven diye tanımladığı şeyin hala bireylerin uzun süredir tanıdıkları, güvendikleri, yüz yüze iletişim kurdukları "güven ilişkilerinin" bu bağlara dayandığı kişilerle ilişkilerinde bu tür sistemleri kullanmazken; özellikle sonradan tanıştıkları iş ilişkisi kuracakları ya da bir sebeple iletişim kurmak zorunda kaldıkları bireyler için özellikle bu sistemleri kullanma eğiliminde oldukları görülmektedir.

Yeni gözetim pratiklerinin ontolojik güvenlik ya da güvensizlik yaratmasının temelinde bireylerin istemli ya da istemsiz olarak sürekli izlenmesi yer almaktadır. Özellikle içerisinde bulundukları toplumdaki veri ihlallerinde kişilerin kendi T.C. kimlik numaraları, adresleri, sağlık verileri, nüfus bilgileri gibi en özel bilgilerinin çalınmasına yönelik beyanları ve bundan dolayı zaten bu sistemleri boş vermiş bir alışkanlıkla kabul ederek yaşamaya başladıkları görülmektedir. Ontolojik güvenlik, sosyolojik olarak bireyin kendi güvenliğine ilişkin davranış ve inançları da kapsayan bir kavramdır ve bahsedilen noktalarda bireylerin kendi güvenliğine ilişkin de şüpheleri olduğu fakat bunu önemsemiyormuş gibi davrandığı anlaşılmaktadır.

Katılımcıların büyük veri ve onun sağladığı yeni imkanlara bakıldığında sosyal fayda için büyük veri ve sosyal zarar için büyük veri olarak iki farklı durumdan bahsettiği, birinin ontolojik güvenliği artıran birinin ise azaltan bir unsur olduğu ifade edilmektedir. Sosyal fayda için büyük veri pratiklerinin ontolojik güvenlik algısına katkıda bulunduğu, bunun sebebinin de küreselleşen dünyada beliren yeni risklere karşı en verimli ve iyi çözümleri üreten sistem olduğu görülmektedir. Büyük verinin bir tür sosyal zarar çerçevesinde değerlendirilmesinde kastedilen ise bahsedilen panoptik sınıflandırma faaliyetleridir. İnsanların etiketlenmesi, profillerinin çıkarılması ve bunların bireylerin aleyhinde, bireylerin kendilerinin kontrolü kaybettiği bir şekilde ilerlemesidir. Bu süreçte özellikle güç dengelerinin değişmesi ve bireyin bu noktada sadece verisiyle ek değer üretip belirli çıkar gruplarını daha da zengin

hale getiren (büyük veri zengini) bir konuma gelmesi söz konusudur. Ontolojik güvensizliğe sebep olabilecek ve sosyal zarar olarak büyük veri düşüncesini vurgulayan katılımcılara bakıldığında ise, etiketleme, kişilerin yapmadıkları şeyleri yapmış gibi gösterebilme, toplumlara baskı yapma, kategorizasyon yapma, çıkar gruplarının kendi menfaatleri doğrultusunda veriyi kullanması gibi unsurlar belirtilmektedir. Bireylerin verilerinin anonimleştirilmeden toplanmasının ciddi sorunları olabileceğine bunun yanı sıra savaşlar ve çatışmalar gibi her türlü durumun da artık büyük veri ve bu sistemler üzerinden yürüyebileceğine değinilmektedir.

Bu sistemlerin etik olmaması düşüncesi de katılımcılarda ontolojik güvensizliğe sebep olmaktadır. Buna bakıldığında özellikle rıza alınıyormuş gibi yapılıp verilerin farklı amaçlarla kullanma ihtimalinin çok yüksek olması, verilerin belirli kişilerin erişimi varmış gibi gözüküp çok fazla kontrol altında tutulamaması, bireylerin sistemleri yeterince bilmemesi ya da bilse de bilinçsizce veri paylaşımı yapması, formları, çerez gibi veri toplayan araçları doğrudan kabul etmesi katılımcılara göre bu sürecin şeffaflığına zarar vermektedir. Şeffaf olmayan bu işlemlerin de etik olarak sorun olduğu belirtilmektedir.

Uzmanların özellikle büyük veri ve yeni gözetim sistemlerinin yarattığı “huzursuzluk”, bahsettikleri “endişe” ve “korkularla” baş etme yollarına bakıldığında, pragmatik kabullenişin bu araştırmadaki en çok görülen örtülü kötümserlikle bağlantılı ilişkisi süper panoptikonda özellikle vurgulandığı gibi günümüzde eğlenmek için ya da çeşitli sebeplerle bireylerin kendi verilerinden feragat etmeleri ve şu anki düzen içerisinde kendilerinin birer ürün haline gelmelerini kabul etmeleridir. Katılımcıların tamamında bu anlamda bir tür pragmatik kabulleniş görülmekte olup, bu sistemler içerisinde yer alan uzmanlar olsalar da özellikle güç dengeleri ve önceden de bahsedilen inisiyatif alabilme sınırları sebebiyle bu tür bir düşünüşe sahip oldukları görülmektedir. Sürekli iyimserlik, akla duyulan ve teknolojiye duyulan inanç ile tarif edilmektedir. Bu grup özellikle sosyal fayda için büyük veri olarak bu tezde de açıklanan düşünceyi temsil eden grupta yaygın bir görüşle kendini göstermektedir. Sürekli

iyimserlik düşünüşünde olan bireylerin de özellikle güç dengeleri ve veri gözetimi anlamında bir tür pragmatik kabullenişle birlikte alaycı kötümserliğe sahip olduğu görülmektedir. Bunun sebebi de araştırmanın pek çok yerinde bahsedildiği gibi bu tür sistemlerin artık kontrol edilemeyecek bir noktaya gelmesi ve temelde kimin kullandığına bağlı olarak değişmesidir. Alaycı kötümserlik, bastırma ve şimdinin keyfini çıkarma özellikleri ile açıklanmaktadır. Bir katılımcının ironik bir şekilde robotlar dünyayı ele geçirecekse de henüz bunun gerçekleşmediği şeklindeki yorumu bunu yansıtmaktadır. Radikal katılım, önemli sorunların olduğunun bilincinde olan ve onları aşmak için harekete geçilmesi yönünde düşünceleri olan grubu temsil etmektedir. Katılımcıların radikal katılım anlamında değerlendirileceği özellikleri incelendiğinde özellikle büyük veri sistemlerini gözetim anlamında değil, daha çok sosyal fayda için büyük veri kavramsallaştırmasıyla açıklandığı şekilde kullandıkları ve bunun da bir tür dijital aktivizm sayılabileceği görülmektedir. Katılımcılar, kendi uzmanlık alanlarını kullanarak çevre sorunlarına, her tür dijital eşitsizliğe ve pek çok alanda direnişte bulunmakta bunu sosyal fayda için kullanmaktadır.

Bu araştırma ise özellikle büyük veri ve onunla birlikte gelişmeye devam eden yapay zekâ, nesnelerin interneti ve dijital medya teknolojileri gibi pek çok sistemin toplumsal değişimlerine odaklanması ve çeşitli çözüm önerilerini onları tasarlayan, üreten ve aynı zamanda deneyimleyen veri bilimcilerle değerlendirmesi bakımından önem arz etmektedir. Büyük verinin içeriği ve tanımı, bu tezde de bahsedildiği gibi zaman içerisinde değişse de bu araştırmanın bu değişimi de yansıtması bakımından gelecekte faydalı olacağı düşünülmektedir. Dünya sıralamalarında dijital medya teknolojileri gibi veri toplamanın en elverişli olduğu alanları en çok kullanan ülkelerden biri olan Türkiye'de özellikle bu konunun tartışılmasının, bu anlamda bireylerin bilinçlenmesi ve gerekli önlemlerin alınması konusunda önem taşıdığı düşünülmektedir.

KAYNAKÇA

Akgüç, Ö. (2004). Mahremiyet açısından elektronik gözetim ve denetim: Tüketicinin denetimi, gözetimi ve online alışveriş siteleri üzerine bir uygulama. Yüksek Lisans Tezi.

Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication*, 8, 17.

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance& Society*, 12(2), 185-196.

Aras, İ. (2022). Çin'in sosyal medya yükselişi ve siyasi tepkiler: TikTok.

Armstrong, D. (1995). Theorise of surveillance medicine. *Sociology of health&illness*, *17*(3), 393-404.

Aspers, P., &Corte, U. (2019). What is qualitative in qualitative research. *Qualitative sociology*, *42*, 139-160.

Basturk, E. (2017). A brief analyze on post panoptic surveillance: Deleuze&Guattarian Approach. *International Journal of Social Sciences*, *6*(2), 1-17.

Baştürk, E. (2012). Michel Foucault'da liberalizm eleştirisi: İktidar, yönetimsellik ve güvenlik. *Felsefe ve Sosyal Bilimler Dergisi (FLSF)*, (14).

Bauman, Z. ve Lyon, D. (2020). *Akışkan Gözetim*. 4. Basım Elçin Yılmaz (Çev) İstanbul: Ayrıntı Yayınları.

Beck, C. (2016). Web of resistance: Deleuzian digital space and hacktivism. *Journal for Cultural Research*, *20*(4), 334-349.

Beck, U. (2008). World at risk: the new task of critical theory. *Development and society*, *37*(1), 1-21.

Beck, U. (2014). Five minutes with Ulrich Beck: "Digital freedom risk is one of the most important risks we face in modern society". *LSE European Politics and Policy (EUROPP) Blog*.

Bentham, J., &Božovič, M. (1995). *The panopticon writings*. Verso Trade.

Bernal, P. (2016). Data gathering, surveillance and human rights: recasting the debate. *Journal of CyberPolicy*, *1*(2), 243-264.

Berry, R. S. (1999). Collecting data by in-depth interviewing.

Blevins, J. L. (2017). Panoptic missorts and the hegemony of US data privacy Policy. *The Political Economy of Communication*, *4*(2).

Boellstorff, T. (2013). Making big data, in theory. *First Monday*, *18*(10).

Bogard, W. (2006). Surveillance assemblages and lines of flight. In Theorizing surveillance (pp. 111-136). Willan.

Bogard, W. (2006). Welcome to the Society of Control: The Simulation of Surveillance Revisited. En The New Politics of Surveillance and Visibility, Kevin D. Haggerty and Richard V. Ericson.

Bogard, W. (2012). Simulation and post-panopticism. Routledge handbook of surveillance studies, 3-37.

Bogard, W. (2013). Control surfaces and rhythmic gestures. *Theory&Event*, 16(3).

Bogard, W. (2019). Welcome to the society of control: The simulation of surveillance revisited. In The new politics of surveillance and visibility (pp. 55-78). University of Toronto Press.

Bogard, W. (1996). The simulation of surveillance: Hyper-Control in telematic societies. Press Syndicate of the University of Cambridge.

Bogner, A., & Menz, W. (2009). The theory-generating expert interview: epistemological interest, forms of knowledge, interaction. In *Interviewing experts* (pp. 43-80). London: Palgrave Macmillan UK.

Bogner, A., Littig, B., &Menz, W. (2009). Introduction: Expert interviews-An introduction to a new methodological debate. In *Interviewing experts* (pp. 1-13). London: Palgrave Macmillan UK.

Brayne, S. (2017). Big data surveillance: The case of policing. *American sociological review*, 82(5), 977-1008.

Brayne, S. (2022). The banality of surveillance. *Surveillance&Society*, *20*(4), 372-378.

Bridle, J. (2020). *Yeni Karanlık Çağ: Teknoloji ve Geleceğin Sonu.* Kemal Güleç (Çev.) 2.Basım İstanbul: Metis Yayınları.

Browne, S. (2010). Digital epidermalization: Race, identity and biometrics. *Critical Sociology*, 36(1), 131-150.

Bulmer, M. (Ed.). (1977). Sociological research methods. Transaction Publishers.

Büyükgaga, P. (2022). Dijital gözetim ve mahremiyetin dönüşümü: 'TheCircle' örneği. Yüksek lisans tezi.

Caluya, G. (2010). The post-panoptic society? Reassessing Foucault in surveillance studies. *Social Identities*, *16*(5), 621-633.

Campbell, J. E., & Carlson, M. (2002). Panopticon. Com: Online surveillance and the commodification of privacy. *Journal of Broadcasting& Electronic Media*, *46*(4), 586-606.

Campbell, J. L., Quincy, C., Osserman, J., & Pedersen, O. K. (2013). Coding in-depth semistructured interviews: Problems of unitization and intercoder reliability and agreement. *Sociological methods&research*, 42(3), 294-320.

Canbay, Y., Vural, Y., & Sağıroğlu, Ş. (2020). Mahremiyet korumalı büyük veri yayınlama için kavramsal model önerileri. *Politeknik Dergisi*, *23*(3), 785-798.

Chen K. (2017). No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state, *Intelligence and National Security*. 32(6), pp. 868–871.

Chen, M., Mao, S., &Liu, Y. (2014). Big data: A survey. *Mobile networks and Applications*, 19(2), 171-209.

Chen, Y., &Cheung, A. S. (2017). The transparent self under big data profiling: privacy and Chinese legislation on the social credit system. *J. Comp. L.*, *12*, 356.

Chizea, O. (2022). It has been argued that 'blackness' is a key site through which surveillance is practiced, narrated and enacted. In short, as S. Browne puts it:'Surveillance is nothing new to black folks. It is the fact of antiblackness'. (S. Browne, Dark Matters, p. 10). Kent LawReview, 7(1).

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498-512.

Clarke, R. (1996, May). Privacy and dataveillance, and organisational strategy. In *Proceedings of the IS Audit& Control Association Conference (EDPAC'96)*.

Clarke, R. (2003, March). Dataveillance–15 years on. In *Privacy Issues Forum* (Vol. 28).

Clarke, R. (2006,). What's' Privacy'. In Australian law reform commission workshop (Vol. 28).

Clarke, R. (2023). Dataveillance: delivering 1984. In *Framing Technology* (pp. 117-130). Routledge.

Clarke, R., & Greenleaf, G. (2017). Dataveillance regulation: A research framework. *JL Inf. &Sci.*, *25*, 104.

Cohen, I. G., &Mello, M. M. (2019). Big data, big tech, and protecting patient privacy. *Jama*, *322*(12), 1141-1142.

Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of contemporary China*, 26(103), 85-100.

Creswell, J. W., & Clark, V. L. P. (2004). Principles of qualitative research: Designing a qualitative study. *Office of Qualitative& Mixed Methods Research, University of Nebraska, Lincoln*.

Croft, S. (2012). Constructing ontological insecurity: The insecuritization of Britain's Muslims. *Contemporary security policy*, *33*(2), 219-235.

Dalgalidere, S. (2016). Epistemolojik açıdan büyük veri ve gelecek tahmin sistemleri.

Dandeker, C. (2019). 9. Surveillance and Military Transformation: Organizational Trends in Twenty-first Century Armed Services. In *The new politics of surveillance and visibility* (pp. 225-249). University of Toronto Press.

Davenport, T. H., & Patil, D. J. (2012). Data scientist. Harvard businessreview, 90(5), 70-76.

DegliEsposti, S. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance&Society*, *12*(2), 209-225.

Deterding, N. M., &Waters, M. C. (2021). Flexible coding of in-depth interviews: A twenty-first-century approach. *Sociologicalmethods&research*, *50*(2), 708-739.

Dong, X. L., &Srivastava, D. (2013, April). Big data integration. In 2013 IEEE 29th international conference on datae ngineering (ICDE) (pp. 1245-1248). IEEE.

Döringer, S. (2021). 'The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge. *International Journal of Social Research Methodology*, *24*(3), 265-278.

Drisko, J. W. (1997). Strengthening qualitative studies and reports: Standards to promote academic integrity. *Journal of social work education*, *33*(1), 185-197.

Durkheim, E. (2019). Sosyolojik Yöntemin Kuralları.

Durmuşahmet, A. (2019). *Ekonomi politik yaklaşım çerçevesinde yeni medyanın büyük veri üzerinden incelenmesi* (Master'sthesis, Sosyal Bilimler Enstitüsü).

Eckmanns, T., Füller, H., & Roberts, S. L. (2019). Digital epidemiology and global health security; an interdisciplinary conversation. *Life Sciences, Society and Policy*, *15*(1), 1-13.

Ergen, Y. (2018). Büyük veri, sosyal medya ve etik: Facebook örneğinde bir değerlendirme. *Ege Üniversitesi İletişim Fakültesi Yeni Düşünceler Hakemli e-Dergisi*, (10), 53-64.

Eroğlu, H. Ö. (2016). Foucault'nun İktidarları. *Amme Idaresi Dergisi*, 49(2).

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H., &Öneş, O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. *Bilişim Teknolojileri Dergisi*, *10*(2), 177-184.

Fernández, J. V. (2023). The Risk of Digitalization: Transforming Government into a Digital Leviathan. *Indiana Journal of Global Legal Studies*, *30*(1), 3-13.

Finn, J. (2014). Liquid Surveillance: A Conversation. *Canadian Journal of Communication*, *39*(3), 497.

Fura, E., &Klamberg, M. (2012). The chilling effect of counter-terrorism measures: A comparative analysis of electronic surveillance laws in Europe and the USA. *Freedom of Expression–Essays in honour of Nicolas Bratza–President of the European Court of Human Rights", Wolf Legal Publishers, Oisterwijk*, 463-481.

Galič, M., Timan, T., &Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy&Technology*, *30*(1), 9-37.

Gambetti, Z. (2008). Foucault'da Disiplin Toplumu-Güvenlik Toplumu Ayrımı. *Mesele Dergisi*, 20, 1-9.

GandyJr, O. H. (1996). Coming to Terms with the Panoptic Sort Oscar H. Gandy Jr. *Computers, surveillance, and privacy*, 132.

GandyJr, O. H. (2003). Public opinion surveys and the formation of privacy policy. *Journal of social issues*, *59*(2), 283-299.

GandyJr, O. H. (2021). *The panoptic sort: A political economy of personal information*. Oxford University Press.

Gartner, R., & Gartner, R. (2016). *Metadata*. Springer.

Glaser, B. G., & Strauss, A. L. (2017). *The discovery of grounded theory: Strategies for qualitative research*. Routledge.

Gordon, L. (2019). Real research: Research methods sociology students can use. Sage Publications.

Güneş, O. (2021). Türkiye'de siyasal partilerin seçim kampanyalarında büyük veri kullanımı üzerine niteliksel bir araştırma*. Yüksek Lisans Tezi*

Haggerty, K. D., & Ericson, R. V. (2019). The New Politics of Surveillance and Visibility (pp. 3-26). University of Toronto Press.

Harford, T. (2014). Big data: Are We Making a Big Mistake? Significance, 11(5), 14-19.

Heawood, J. (2018). Pseudo-public political speech: Democratic implications of the Cambridge Analytica scandal. *Information polity*, *23*(4), 429-434.

Holton, J. A. (2007). The coding process and its challenges. The Sage handbook of grounded theory, 3, 265-289.

Huckvale, K., Venkatesh, S., & Christensen, H. (2019). Toward clinical digital phenotyping: a timely opportunity to consider purpose, quality, and safety. *NPJ digital medicine*, *2*(1), 1-11.

Jain, P., Gyanchandani, M., &Khare, N. (2016). Big data privacy: a technological perspective and review. *Journal of Big Data*, *3*(1), 1-25.

Jakku, E., Taylor, B., Fleming, A., Mason, C., Fielke, S., Sounness, C., &Thorburn, P. (2019). “If they don’t tell us what they do with it, why would we trust them?” Trust, transparency and benefit-sharing in Smart Farming. *NJAS-Wageningen Journal of Life Sciences*, *90*, 100285.

Kafer, G., &Grinberg, D. (2019). Queer surveillance. *Surveillance&Society*, *17*(5), 592-601.

Kalsın, B. (2023). TikTok Yasaklarının Arka Planı: Veri Güvenliği mi? Siyasi İlişkiler mi?. *The Journal of Social Sciences*, *64*(64), 148-159.

Karaarslan, E., Eren, M. B., & Koç, S. (2014). Çevrimiçi mahremiyet: teknik ve hukuksal durum incelemesi. *Türkiye’de İnternet Konferansı Bildirisi, İzmir*, 27-29.

Karafiloski, E., &Mishev, A. (2017, July). Blockchain solutions for big data challenges: A literature review. In *IEEE EUROCON 2017-17th International Conference on Smart Technologies* (pp. 763-768).

Kavza, U. 2010. Veri madenciliğinde mahremiyetin sağlanması. Yüksek lisans tezi.

Kaya, Y. B. (2021). Gizli baloncuklar: TikTok'taki gençlerin algoritmanın sağladığı yarı gizli ortamlardaki mahremiyet pratikleri. Yüksek lisans tezi.

Kayaalp, M. (2018). Patient privacy in the era of big data. *Balkan medical journal*, *35*(1), 8-17.

Kiver, S. (2021). Unutulma hakkı: Mahremiyet, veri gizliliği ve etik tartışmalar. Yüksek lisans tezi.

Kobelieva, D. L., &Nikolaienko, N. M. (2021). From Information Search to the Loss of Personality: The Phenomenon of Dataism. Anthropological Measurements of Philosophical Research, (20), 100-112.

Konish, L. (2018). Financial advisors are missing one key technology disruption. Retrieved from https://www.cnbc.com/2018/02/12/financial-advisors-are-missing-one-key-technology-disruption.html

Köse, H. (2007). Yeni risk tanımlamaları bağlamında küresel medya. *Selçuk İletişim*, *5*(1), 42-51.

Kshetri, N. (2014). Bigdata′ s impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134-1145.

Laudrain, A. P. (2019). Smart-city technologies, governmen tsurveillance and privacy: Assessing the potential for chilling effects and existing safeguards in the ECHR.

Legard, R., Keegan, J., &Ward, K. (2003). In-depth interviews. Qualitative research practice: A guide for socia lscience students and researchers, 6(1), 138-169.

Leonard, P. (2014). Customer data analytics: privacy settings for 'Big Data' business. *International data privacy law*, *4*(1), 53-68.

Lerman, J. (2013). Big data and its exclusions. Stan. L. Rev. Online, 66, 55.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, *10*(4), 415-453.

Littig, B. (2009). Interviewing the elite—interviewing experts: is there a difference? In *Interviewing experts* (pp. 98-113). London: Palgrave Macmillan UK.

Lokke, E. (2020). *Mahremiyet: Dijital Toplumda Özel Hayat.Dilek Başak (Çev.). 2.Basım. İstanbul: Küy Yayınları.*

Loshin, D. (2010). Master data management. Morgan Kaufmann.

Lowry, D. W. (2004). Understanding reproductive technologies as a surveillant assemblage: Revisions of power and technoscience. *Sociological perspectives*, *47*(4), 357-370.

Lupton, D. (2013) The digital cyborg assemblage: Haraway's cyborg theory and the new digital health technologies (preprint). In Collyer, F. (ed) (forthcoming), The Handbook of Social Theory for the Sociology of Health and Medicine. Houndmills: Palgrave Macmillan.

Lupton, D. (2014). The commodification of patient opinion: the digital patient experience economy in the age of bigdata. Sociology of health& illness, 36(6), 856-869.

Lupton, D. (2014). *Digital sociology*. Routledge.

Lupton, D. (2014, December). Self-tracking cultures: towards a sociology of personal informatics. In *Proceedings of the 26th Australian computer-human interaction conference on designing futures: The future of design* (pp. 77-86).

Lupton, D. (2015). The thirteen Ps of big data. *This Sociological Life*.

Lupton, D. (2016). Digital companion species and eating data: Implications for theorising digital data–human assemblages. *Big Data &Society*, *3*(1), 2053951715619947.

Lupton, D. (2016). Digital risk society. *Routledge handbook of risk studies*, 301-309.

Lupton, D. (2016). The diverse domains of quantifiedselves: self-tracking modes and dataveillance. *Economy and Society*, *45*(1), 101-122.

Lupton, D. (2016). The quantified self. John Wiley&Sons.

Lupton, D., & Michael, M. (2017). 'Depends on who's got the data': Public understandings of personal digital dataveillance. *Surveillance&Society*, *15*(2), 254-268.

Lycett, M. (2013). 'Datafication': making sense of (big) data in a complex world. *European Journal of Information Systems*, *22*(4), 381-386.

Lyon, D. (1992). The new surveillance: Electronic Technologies and the maximum security society. *Crime, Law and Social Change*, *18*, 159-175.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. U of Minnesota Press.

Lyon, D. (2003). Technologys 'terrorism': circuits of citysurveillance since September 11th. *International Journal of Urban andRegionalResearch*, *27*(3), 666-678.

Lyon, D. (2003). Surveillance technology and surveillance society. Modernityand technology, 161, 184.

Lyon, D. (2004). Globalizin gsurveillance: Comparative ands ociological perspectives. *International Sociology*, *19*(2), 135-149.

Lyon, D. (2006). *Günlük hayatı kontrol etmek: Gözetlenen toplum*. Soykan, G. (Çev.). Kalkedon Yayıncılık.

Lyon, D. (2007). Surveillance studies: An overview.

Lyon, D. (2010). Liquid surveillance: Thecontribution of ZygmuntBaumanto surveillance studies. *International politicalsociology*, *4*(4), 325-338.

Lyon, D. (2013). *Gözetim çalışmaları: genel bir bakış*. Kalkedon Yayınları.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data&Society*, 1(2), 2053951714541861.

Lyon, D. (2015). *Surveillance after Snowden*. John Wiley&Sons.

Lyon, D. (2019). 2. 9/11, Synopticon, and Scopophilia: Watching and Being Watched. In *The new politics of surveillance and visibility* (pp. 35-54). University of Toronto Press.

Lyon, D. (Ed.). (2006). *Theorizing surveillance*. Routledge.

Lyotard, J. F. (1994). The postmodern condition. *The Postmodern Turn: New Perspectives on Social Theory, Cambridge University Press, Cambridge. England*, 27-38.

Madden, S. (2012). From databases to big data. IEEE Internet Computing, 16(3), 4-6.

Manley, A., Palmer, C., &Roderick, M. (2012). Disciplinary power, the oligopticon and rhizomatic surveillance in elite sports academies. *Surveillance& society*, *10*(3/4), 303-319.

Martinez-Martin, N., Insel, T. R., Dagum, P., Greely, H. T., &Cho, M. K. (2018). Data mining for health: staking out the ethical territory of digital phenotyping. *NPJ digital medicine*, *1*(1), 68.

Marx, G. T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information technology*, *3*(3), 157-169.

Marx, G. T. (2002). What's New About the" New Surveillance"? Classifying for Change and Continuity. *Surveillance&Society*, *1*(1), 9-29.

Marx, G. T. (2013). The public as partner? Technology can make us auxiliaries as well as vigilantes. *IEEE Security &Privacy*, *11*(5), 56-61.

Marx, G. T. (2015). Comingtoterms: the kaleidoscope of privacy and surveillance. *Social dimensions of privacy: Interdisciplinary perspectives*, 32-49

Marx, G. T. (2015). Surveillance studies. *International encyclopedia of the social& behavioral sciences*, *23*(2), 733-741.

Marx, G. T., Lyon, D., &Ball, K. S. (2015). Presentation of the Surveillance Studies Network Outstanding Achievement Award. *Surveillance&Society*, *13*(3/4), 539-546.

Mathiesen, T. (1997). The viewer society: Michel Foucault's Panopticon revisited. *Theoretical criminology*, 1(2), 215-234.

Maxwell, J. A. (2008). Designing a qualitative study (Vol. 2, pp. 214-253). The SAGE handbook of applied social research methods.

McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., &Barton, D. (2012). Big data: the management revolution. Harvard business review, 90(10), 60-68.

Mears, C. L. (2012). In-depth interviews. Research methods and methodologies in education, 19, 170-176.

Mejias, U. A., &Couldry, N. (2019). Datafication. Internet Policy Review, 8(4).

Mermutlu, A. (2010). Görünürlük uzamlarında kamusallık, denetim, mahremiyet: İstanbul örneğinde kameralı gözetimin sosyo-politiği. Doktora tezi.

Michael, M., &Lupton, D. (2016). Toward a manifesto for the 'public understanding of bigdata'. Public Understanding of Science, 25(1), 104-116.

Monea, A. (2019). Race and computer vision.

Mooney, S. J., &Pejaver, V. (2018). Bigdata in public health: terminology, machine learning, and privacy. *Annual review of public health*, *39*, 95-112.

Morse, J. M. (1991). Strategies for sampling. Qualitative nursing research: A contemporary dialogue, 127, 145.

Nemorin, S. (2017). Post-panoptic pedagogies: The changing nature of school surveillance in the digital age. *Surveillance and Society*, *15*(2), 239-253.

Newell, B. C., &Tennis, J. (2014). Me, my metadata, and the NSA: Privacy and government metadata surveillance programs. *Proceedings of the 2014 iConference*, 345-55.

Oflas, S. P. (2020). Büyük Veri Teknolojisi Çağında Kullanıcı Verilerinin Gizlilik ve Mahremiyetine İlişkin Sosyolojik Analiz.

O'Leary, D. E. (2013). Artificial intelligence and big data. *IEEE intelligent systems*, *28*(2), 96-99.

Onnela, J. P. (2021). Opportunities and challenges in the collection and analysis of digital phenotyping data. *Neuropsychopharmacology*, *46*(1), 45-54.

Orito, Y. (2011). The counter-control revolution: “silent control” of individuals through dataveillance systems. *Journal of Information, Communication and Ethics in Society*.

Orwant, C. J. (1996). Book review: The Electronic Eye by David Lyon. *ACM SIGCAS Computers and Society*, *26*(2), 30-31.

Orwell, G. (2020). *Bin Dokuz Yüz Seksen Dört*. Celal Üster (Çev.) 20. Basım. İstanbul: Can Modern Yayınları.

Özdemir, Ş. (2020). Post-panoptikon çağı: Gözetimin dijitalleşmesi ve çevrimiçi kimliğin gizliliği üzerine bir analiz. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, *20*(3), 81-108.

Özkan, Ö. (2010). *Sağlık hizmetinden yararlanan bireylerin, elektronik ortamda tutulan sağlık bilgilerinin gizliliği ve mahremiyeti ile ilgili görüş ve düşünceleri. Yüksek lisans tezi.*

Özkazanç, A. (2007). Biyo-politik çağda suç ve cezalandırma: Denetim Toplumunda Neo-liberal Yönetimsellik. Toplum ve Bilim, 108, 15-51.

Öztürk, H. *Veri gazeteciliğinin Türkiye’deki durumu: Uluslararası platformlarla karşılaştırma* (Master's thesis, Sosyal Bilimler Enstitüsü).

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., &Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and policy in mental health and mental health services research*, *42*, 533-544.

Palmatier, R. W., &Martin, K. D. (2019). *The intelligent marketer's guide to data privacy: The impact of big data on customer trust*. Springer International Publishing.

Pedersen, J. S. (2019). 15. The digital welfare state: Dataism versus relationshipism. Big Data: Promise, Application and Pitfalls, 301.

Penn Today. (2021). The Panoptic Sort: Surveillance Q&A with Oscar Gandy. Erişim Tarihi 02.11.2021 ThePanopticSort: Surveillance Q&A with Oscar Gandy | Penn Today (upenn.edu)

Pero, R. (2015). Liquid surveillance: A conversation. Pero, R. (2015). Liquid surveillance: A conversation.

Provost, F., &Fawcett, T. (2013). Data science and its relationship to big data and data-driven decision making. Bigdata, 1(1), 51-59.

Puaschunder, J. M. (2019, October). The legal and international situation of AI, robotics and big data with attention to health care. In Report on behalf of the European Parliament European liberal Forum.

Queirós, A., Faria, D., &Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European journal of education studies*.

Ramadan, Z. (2018). The gamification of trust: the case of China's "social credit". *Marketing Intelligence& Planning*, *36*(1), 93-107.

Regan, P. M. (2017). Opening windows on surveillance: Scholarship of Gary Marx. *Society*, *54*, 363-366.

Reidenberg, J. R., &Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16*(3), 263-279.

Rich, E., &Miah, A. (2009). Prosthetic surveillance: The medical governance of healthy bodies in cyberspace. *Surveillance&Society*, *6*(2), 163-177.

Riehl, C. (2001). Bridges To the future: The contributions of qualitative research to the sociology of education. *Sociology of Education*, 115-134.

Rumelili, B., &Adisönmez, U. C. (2020). Uluslararası ilişkilerde kimlik-güvenlik ilişkisine dair yeni bir paradigma: Ontolojik güvenlik teorisi. *Uluslararası İlişkiler Dergisi*, *17*(66), 23-39.

Salathé, M. (2018). Digital epidemiology: what is it, and where is it going? Life sciences, society and policy, 14(1), 1.

Salathe, M., Bengtsson, L., Bodnar, T. J., Brewer, D. D., Brownstein, J. S., Buckee, C., ... &Vespignani, A. (2012). Digital epidemiology.

Samerski, S. (2018). Individuals on alert: digital epidemiology and the individualization of surveillance. *Life sciences, society and policy*, *14*, 1-11

Schermann, M., Hemsen, H., Buchmüller, C., Bitter, T., Krcmar, H., Markl, V., & Hoeren, T. (2014). Bigdata. Business & Information Systems Engineering, 6(5), 261-266.

Schlichter, B. R., &Rose, J. (2013). Trust dynamics in a large system implementation: six theoretical propositions. *European Journal of Information Systems*, *22*(4), 455-474.

Schwandt, T. A. (1994). Constructivist, interpretivist approaches to human inquiry. Handbook of qualitative research, 1(1994), 118-137.

Selçuk, A. (2015). *Büyük veri üzerinde dağıtık dosya sistemi ve paralel işleme kullanarak mahremiyet korumalı arama. Yüksek Lisans tezi*

Shahzad, F. (2021). Türkiye'deki seçim kampanyalarında yapay zekâ ve büyük veri kullanımı. Yüksek Lisans Tezi.

Solmaz, M. (2020). Güncel Gözetimi Bauman'ın Sosyal Teorisinden Hareketle Anlamak. *Journal of Social Sciences and Humanities*, *4*(1), 1-10.

Sopaoğlu, U. (2021). Büyük veri ve akan verinin mahremiyet korumalı anonimleştirilmesi. Doktora tezi.

Stockdale, D. (2014). Data governance and data stewardship. *Handbook of Financial Data and Risk Information II*, *2*, 464.

Strawn, G. (2016). Data scientist. IT Professional, 18(3), 55-57.

Subudhi, B. N., Rout, D. K., &Ghosh, A. (2019). Big data analytics for video surveillance. Multimedia Tools and Applications, 78(18), 26129-26162.

Sucu, İ. (2020). Gözetlenen Toplumun Gözetleyen Topluma Dönüşmesi: "The Truman Show Filmi" Örneği. *Aksaray İletişim Dergisi*, *2*(1), 1-12.

Sullivan, J. (2014). Uncovering the data panopticon: The urgent need for critical scholarship in an era of corporate and government surveillance. *The Political Economy of Communication*, *1*(2).

Sustam, E. (2016). Foucault'da İktidarın Jeneolojisi: Biyopolitiğin Doğuşu ve Yönetimsellik.

Şahin, O. (2020). *Bilgi sosyolojisi bağlamında büyük veri ve toplumsal gerçekliğin inşası* (Master'sthesis, Sosyal Bilimler Enstitüsü).

Şinşek, M. Y. (2022). *Büyük veri ve öznellik: Cambridge Analytica örneği. Yüksek Lisans Tezi.*

Strauss, A., & Corbin, J. M. (1997). Grounded theory in practice. Sage.

Tahaoğlu, O. O. (2009). *Türkiye'de kişisel verilerin korunması: Mahremiyet risk yönetimine yönelik bir bilgi teknolojileri çerçevesi. Doktora tezi.*

Tankard, C. (2012). Big data security. Network security, 2012(7), 5-8.

Tomaszewski, L. E., Zarestky, J., & Gonzalez, E. (2020). Planning qualitative research: Design and decision making for new researchers. International Journal of Qualitative Methods, 19, 1609406920967174.

Toy, F. (2019). Büyük verilere yetkisiz erişimlerin tespit edilmesi ve engellenmesi tekniklerinin incelenmesi ve uygulaması.

Tredinnick, L. (2008). *Digital information culture: the individual and society in the digital age*. Elsevier.

Trottier, D., & Lyon, D. (2013). Key features of social media surveillance. In *Internet and Surveillance* (pp. 109-125). Routledge.

Tufekci, Z. (2014). Engineering the public: Bigdata, surveillance and computational politics. First Monday.

Turancı, E. (2021). Dijital dünyada kişisel veri ve etik: Gizlilik politikası bağlamında "# WhatsApp siliyoruz" krizinde kullanıcı tepkilerini anlamak. *TRT Akademi*, *6*(12), 272-295.

Uyanık, G. (2022). Büyük veri analitiği ve mahremiyeti: Mobil uygulamaların kullanım düzeyi ve gizlilik endişesi üzerine bir inceleme. Yüksek Lisans Tezi.

Van der Aalst, W. M. (2014). Data scientist: The engineer of the future. In Enterprise interoperability VI: Inter-operability for agility, resilience and plasticity of collaborations (pp. 13-26). Springer International Publishing.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance&society*, *12*(2), 197-208.

Vollstedt, M., & Rezat, S. (2019). An introduction to grounded theory with a special focus on axial coding and the coding paradigm. Compendium for early career researchers in mathematics education, 13(1), 81-100.

Wang, Y. (2016). Big opportunities and big concerns of big data in education. *Tech Trends*, *60*(4), 381-384.

Wood, D. M., Ball, K., Lyon, D., Norris, C., &Raab, C. (2006). A report on the surveillance society. *Surveillance Studies Network, UK*, 1-98.

Yu, S. (2016). Big privacy: Challenges and opportunities of privacy study in the age of bigdata. *IEEE access*, *4*, 2751-2763.

Yücedağ, İ. (2017). Modern Toplumda Denetim Asemblajı. *Süleyman Demirel Üniversitesi Fen-Edebiyat Fakültesi Sosyal Bilimler Dergisi*, (41), 161-176.

Zengin, İ. G. (2021). Web sitelerine karşı tüketicilerin yararlığı, riski ve güven algısıyla, satın alma amacı üzerindeki büyük veri etkilerini anlamak. Yüksek Lisans Tezi.

Zimmer, M. (2008). the gaze of the perfect search engine: Google as an infrastructure of dataveillance. In *Web search: Multidisciplinary perspectives* (pp. 77-99). Berlin, Heidelberg: Springer Berlin Heidelberg.

Zuboff, S. (2014). A digital declaration. *Frankfurter Allgemeine*, *9*.

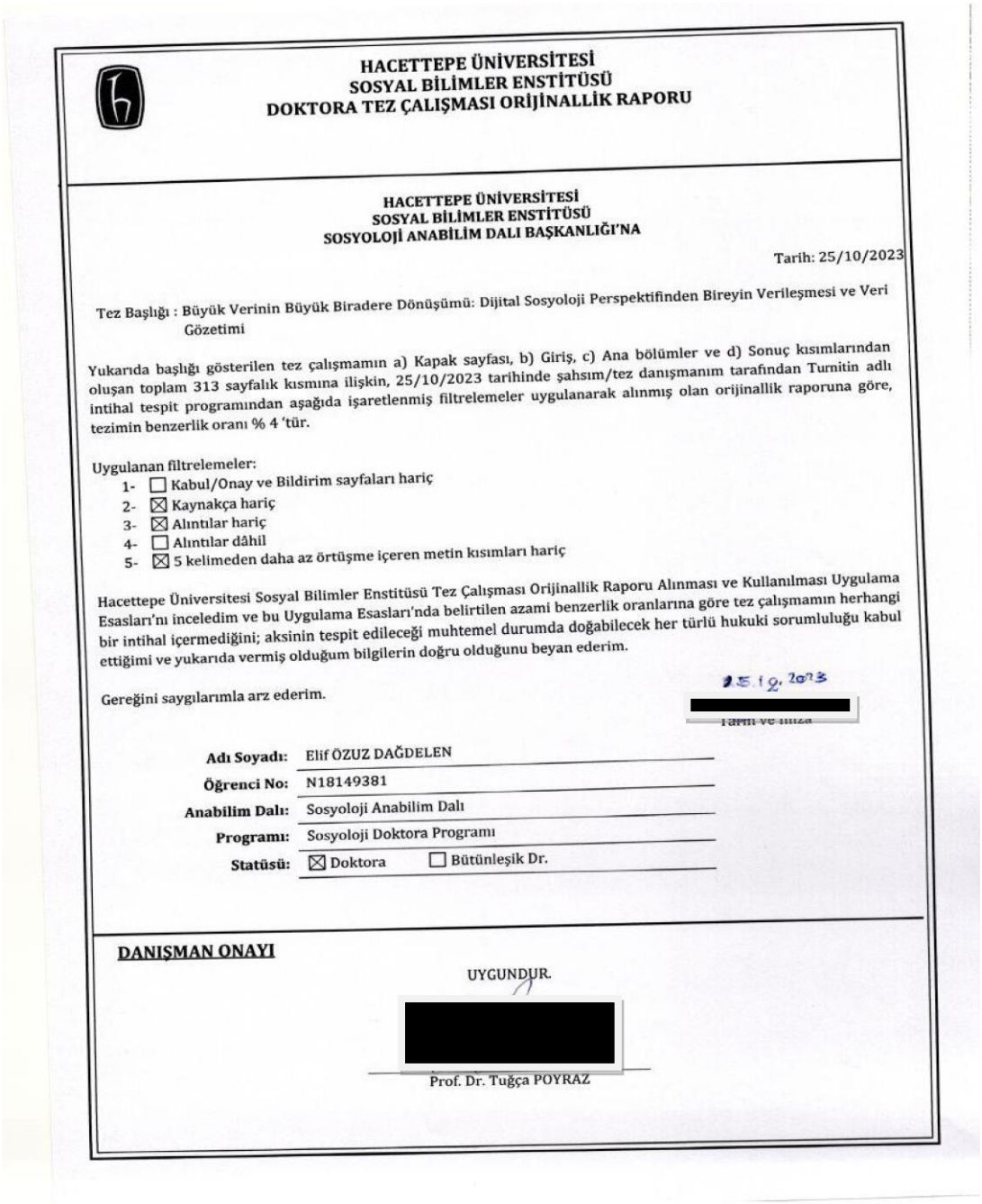
Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, 30(1), 75-89.

Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In New labor forum (Vol. 28, No. 1, pp. 10-29). Sage CA: Los Angeles, CA: SAGE Publications.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social Theory Re-Wired* (pp. 203-213). Routledge.

Zuboff, S., Möllers, N., Wood, D. M., & Lyon, D. (2019). Surveillance capitalism: An interview with Shoshana Zuboff. *Surveillance&Society*, *17*(1/2), 257-266.

EK 1. Orijinallik Raporu



HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
DOKTORA TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SOSYOLOJİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 25/10/2023

Tez Başlığı : Büyük Verinin Büyük Biradere Dönüşümü: Dijital Sosyoloji Perspektifinden Bireyin Verileşmesi ve Veri Gözetimi

Yukarıda başlığı gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve d) Sonuç kısımlarından oluşan toplam 313 sayfalık kısmına ilişkin, 25/10/2023 tarihinde şahsım/tez danışmanım tarafından Turnitin adlı intihal tespit programından aşağıda işaretlenmiş filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 4 'tür.

Uygulanan filtrelemeler:
1- ☐ Kabul/Onay ve Bildirim sayfaları hariç
2- ☒ Kaynakça hariç
3- ☒ Alıntılar hariç
4- ☐ Alıntılar dâhil
5- ☒ 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

25.10.2023
[redacted]
Tarih ve İmza

Adı Soyadı:	Elif ÖZUZ DAĞDELEN
Öğrenci No:	N18149381
Anabilim Dalı:	Sosyoloji Anabilim Dalı
Programı:	Sosyoloji Doktora Programı
Statüsü:	☒ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

[redacted]
Prof. Dr. Tuğça POYRAZ

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
Ph.D. DISSERTATION ORIGINALITY REPORT

HACETTEPE UNIVERSITY
GRADUATE SCHOOL OF SOCIAL SCIENCES
SOCIOLOGY DEPARTMENT

Date: 25/10/2023

Thesis Title : Transformation of Big Data to Big Brother: Datafication and Dataveillance from the Perspective of Digital Sociology,

According to the originality report obtained by myself/my thesis advisor by using the Turnitin plagiarism detection software and by applying the filtering options checked below on 25/10/2023 for the total of 313 pages including the a) Title Page, b) Introduction, c) Main Chapters, and d) Conclusion sections of my thesis entitled as above, the similarity index of my thesis is 4 %.

Filtering options applied:

1. ☐ Approval and Decleration sections excluded
2. ☒ Bibliography/Works Cited excluded
3. ☒ Quotes excluded
4. ☐ Quotes included
5. ☒ Match size up to 5 words excluded

I declare that I have carefully read Hacettepe University Graduate School of Social Sciences Guidelines for Obtaining and Using Thesis Originality Reports; that according to the maximum similarity index values specified in the Guidelines, my thesis does not include any form of plagiarism; that in any future detection of possible infringement of the regulations I accept all legal responsibility; and that all the information I have provided is correct to the best of my knowledge.

I respectfully submit this for approval.

25.10.2023

[redacted]

Date and Signature

Name Surname: Elif ÖZUZ DAĞDELEN
Student No: N18149381
Department: Department of Sociology
Program: Sociology Doctoral Program
Status: ☒ Ph.D. ☐ Combined MA/ Ph.D.

ADVISOR APPROVAL

APPROVED.

[redacted]

Prof. Dr. Tuğça POYRAZ

EK 2. Etik Kurul/Komisyon İzni ya da Muafiyet Formu

Tarih: 21/03/2023 11:26
Sayı: E-35853172-300-00002756542
00002756542

T.C.
HACETTEPE ÜNİVERSİTESİ REKTÖRLÜĞÜ
Rektörlük

Sayı : E-35853172-300-00002756542 21.03.2023
Konu : Elif ÖZUZ DAĞDELEN Hk. (Etik Komisyon İzni)

SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 24.02.2023 tarihli ve E-12908312-300-00002709229 sayılı yazınız.

Enstitünüz Sosyoloji Anabilim Dalı Doktora Programı öğrencilerinden **Elif ÖZUZ DAĞDELEN'**in **Prof. Dr.Tuğça POYRAZ** sorumluluğunda yürüttüğü "**Büyük Verinin Büyük Biradere Dönüşümü: Dijital Sosyoloji Perspektifinden Bireyin Verileşmesi ve Veri Gözetimi**" başlıklı tez çalışması, Üniversitemiz Senatosu Etik Komisyonunun **07 Mart 2023** tarihinde yapmış olduğu toplantıda incelenmiş olup, etik açıdan uygun bulunmuştur.

Bilgilerinizi ve gereğini rica ederim.

Prof. Dr. Sibel AKSU YILDIRIM
Rektör Yardımcısı

Bu belge güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu: AE84F649-8C03-4B95-BC2F-3C14F7B62336 Belge Doğrulama Adresi: https://www.turkiye.gov.tr/hu-ebys

Adres: Hacettepe Üniversitesi Rektörlük 06100 Sıhhiye-Ankara
E-posta:yazimd@hacettepe.edu.tr İnternet Adresi: www.hacettepe.edu.tr Elektronik Ağ: www.hacettepe.edu.tr
Telefon: 0 (312) 305 3001-3002 Faks:0 (312) 311 9992
Kep: hacettepeuniversitesi@hs01.kep.tr

Bilgi için: Duygu Didem İLERİ
Bilgisayar İşletmeni
Telefon: .

EK 3. Bireysel Görüşme Formu

BİREYSEL GÖRÜŞME FORMU

BÖLÜM 1: KATILIMCI BİLGİLERİ

1. Adınız?

2. Yaşınız?

3. Cinsiyetiniz?

4.Doğum yeriniz?

5.Nerede yaşıyorsunuz?

6.Eğitim durumunuz nedir?

☐Lisans mezunu☐Tezli yüksek lisans öğrencisi☐Tezli yüksek lisans mezunu☐Tezsiz yüksek lisans öğrencisi☐Tezsiz yüksek lisans mezunu☐Doktoraöğrencisi☐Doktora mezunu

7.Hangi üniversitenin hangi lisans/yüksek lisans/doktora programından mezunsunuz?

8. Medeni durumunuz?

☐Evli ☐Bekâr☐Eşindenayrılmış☐Eşi vefat etmiş☐Sevgilisi var☐Diğer

9.Kimle yaşıyorsunuz?

10. Çocuğunuz var mı?

☐Evet

☐Hayır

11.Mesleğiniz nedir?

12.Çalıştığınız birim nedir ve bu birimdeki göreviniz nedir? Ne kadar süredir bu pozisyonda çalışıyorsunuz?

13. Mesleğinizle ilgili önemli olan aldığınız sertifikalar ve kullandığınız uygulamalar nelerdir?

14.Gelir durumunuz nedir?

☐10.000altı☐10.000.15.000☐15.000-20.000☐20.000-25.000☐25.000-30.000

☐30.000-+

15.Hangi sosyal medya platformlarını kullanıyorsunuz?

☐Facebook☐Twitter☐Instagram☐YouTube☐Tinder☐Snapchat☐Pinterest☐Tikt ok

☐Twitch☐Club House☐Diğer ……

16.Hangi iletişim uygulamalarını kullanıyorsunuz?

☐Whatsapp☐Signal☐Telegram☐Discord☐Turkcell☐Bip☐Skype ☐Zoom☐Google Meeting☐Microsoft Teams☐FaceTime☐Diğer……

17.Hangi arama motorlarını kullanıyorsunuz?

☐Google☐Yahoo☐Bing☐Yandex☐Ask☐Diğer……..

18.Hangi alışveriş platformlarını kullanıyorsunuz?

☐Hepsiburada☐Trendyol☐Shoppier☐Etsy☐Amazon☐Gittigidiyor☐N11☐Sahibinden.com☐Yemeksepeti☐Getir☐Diğer……

19.Yukarıdaki platformlardan hangilerini işiniz için kullanıyorsunuz? Bu programı seçme sebebiniz nedir?

20.Bireysel olarak kullandığınız platformları seçme sebebiniz nedir? Kullandığınız uygulamaları çevrenizdekilere öneriyor musunuz?

BÖLÜM 2: KATILIMCI BÜYÜK VERİ İLİŞKİSİ

1.Büyük veri nedir?

2.Büyük verinin kullanım alanları nelerdir?

3.Mesleğinizde büyük veriyi nasıl ve ne amaçla kullanıyorsunuz?

4.Mesleğinizde büyük veriyi kullanmak için ihtiyaç duyduğunuz ve kazanmış olduğunuz dijital beceriler nelerdir? Geliştirmeyi düşündüğünüz başka dijital beceriler var mıdır?

5.Büyük verinin insanlığa sunduğu avantajlar/dezavantajlar nelerdir?

6.Karar verme mekanizmalarında büyük verinin rolü nedir?

7.Büyük veri analizlerinde dikkat ettiğiniz noktalar nelerdir? Büyük veri analizlerinde örnekleme hataları ve örneklem yanlılığından kaçınmak için neler yapılmaktadır? Hangi programları kullanıyorsunuz?

8.Veri koruma kanunları ve yasal düzenlemeler büyük veri alanında yeterli midir?

8.1. Türkiye'de yaşanmış veri ihlalleriyle ilgili ilk aklınıza gelen olay nedir?

8.2.Dünyada veri ihlali ile ilgili ilk aklınıza gelen olay nedir?

8.3.Verilerin korunması için en etkili yöntem nedir?

8.4.Yasal olarak nasıl bir düzenleme yapılmalı? Önerileriniz nelerdir?

9.Hukuki, sosyal, kültürel ve ekonomik boyutun yanısıra bireylerin verilerini korumak için teknik anlamda (encyription, tokenisation, data-masking gibi) neler yapılmaktadır? Bunların yeterli olduğunu düşünüyor musunuz?

10.Büyük verinin yıkıcı, manipüle edici ya da kontrol için kullanılan güç haline dönüşme potansiyeli sizce nedir?

BÖLÜM 3: VERİ GÖZETİMİ

1.Sizce gözetim nedir?

2.Büyük veri ile ne tür tahminler yapılmaktadır? Gelecekte ne tür tahminler yapılabilir? Şu an üzerinde çalışılan yeni sistemler var mıdır?

3.Bireyler bu sisteme nasıl dahil olmaktadır? Bu sistemden kaçmak mümkün mü?

4.Büyük veriye dahil olan bireylerin bilgileri hangi sistemlerden çekilmektedir, bunun bir sınırı var mıdır? Hangi bireylerin sistemde bilgileri daha önemlidir?

5.Bireylerin verilerine ulaşmak isteyen kişiler, kurumlar güçler kimlerdir, bu verilere nasıl ulaşılmaktadır? Yasal izin süreci işletilmekte midir?

6. Sizin meslek grubunuzdaki insanların veriye ulaşma açısından bir farkı olduğunu düşünür müsünüz? Bu alanda çalışmak size kendinizi nasıl hissettiriyor?

7.Mahremiyet sizce nedir? Büyük verinin mahremiyeti ihlal ettiğini düşüyor musunuz? Eğer düşünüyorsanız nasıl?

8.Bireylerin ya da vatandaşların verileri sizce neden toplanmaktadır?

9.Gözetimden kaçabilmek mümkün mü?

10.Veri gözetimi ile kişilerin dijital ortamdaki varlıkları yaratılabilir mi?

11.Devletler ve özel şirketler büyük verilerle ineler yapabilir ve şu an neler yapıyorlar?

12.Siz başkalarını gözetlediğinizi ya da gözetlendiğinizi düşünüyor musunuz?

13.En çok hangi alanda gözetlediğinizi ya da gözetlendiğinizi düşünüyorsunuz?

14.Gözetlenseniz bile vazgeçemeyeceğiniz uygulamalar nelerdir?

15.Siz verilerinizi paylaşıyor musunuz? Büyük veriye nasıl dahil olduğunuzu düşünüyorsunuz? Mahremiyetinizi korumak için neler yapıyorsunuz? Bireyler mahremiyetini korumak için neler yapmalıdır?

BÖLÜM 4: SOSYAL İLİŞKİ KURMADA BÜYÜK VERİ-BİREYİN VERİLEŞMESİ

1.Biriyle ilk kez tanıştığınızda onunla ilgili bilgi edinmek için ne yaparsınız? Sosyal medya platformlarından ya da arama motorlarından aratır mısınız? Hangi platformun güvenli olduğunu düşünürsünüz? Neden?

2. “Stalklamak” nedir? Siz bir şeyleri ya da kimseleri “stalklar” mısınız?

3.Bir kişi hakkında sistemleri ya da sosyal medya platformlarını kullanarak bilgi edinmek istediğinizde özen gösterdiğiniz durumlar var mıdır?

4.Büyük verinin kullanımı toplumdaki güven ilişkilerini nasıl etkilediğini düşünüyorsunuz?

5.Tanıştığınız kişinin sosyal medya platformlarını kullanması ya da kullanmaması sizin için önemli midir ve ne ifade eder? (Bir kişi sosyal medya platformlarını kullanıyorsa daha samimi, kimliği hakkında daha açık bir kişi olarak değerlendirilebilir mi?)

6.Mesleğinizden dolayı diğer kişilerin bilgilerine ulaşma konusunda bir farkınız ya da gücünüz olduğunu düşünür müsünüz? Neler yapabilirsiniz?

7.Büyük veri ile daha fazla bilgi edinebildiğiniz kişiye daha çok ya da daha kolay mı güvenirsiniz?

8.Onların sosyal medya araçlarını takip ya da kontrol eder misiniz? Bu işlemi nasıl yaparsınız? Onları mahremiyet ve güvenlik açısından uyarır mısınız?

BÖLÜM 5: TOPLUMSAL GÜVENVE SORUMLULUKLARDA BÜYÜK VERİ

1.İzlenildiğinizi ve hakkınızda veri toplandığını düşündüğünüz ortamlar nerelerdir?Bu ortamlarda nasıl davranırsınız?

2.Verilerinizin ihlal edildiği bir durumla karşılaştınız mı?

3.İzleme teknolojilerinin toplumdaki düzen kurmaya katkı sağladığını düşünüyor musunuz?

4.Sizce şirketler büyük veriyi neden kullanmaktadır?

5.Kişilerin internet ortamında oluşturduğu avatarlar gerçek kimliklerini yansıtmakta mıdır?

6.Büyük verinin neden olduğu riskler ya da tehlikeler sizce nelerdir?

7.Büyük veri kullanımının zaman-mekân algısında değişikliğe yol açtığını düşünüyor musunuz?

8.Büyük verinin sağladığı bilgilere algoritmalar ve bu sistemi sağlayan kişilerin uzmanlık bilgilerinden ötürü güvenirsiniz misiniz?

BÖLÜM 6: BÜYÜK VERİNİN KARANLIK YÖNÜ-YIKICI TEKNOLOJİ TARAFI

1.Büyük verinin birey ve toplum açısından faydaları/zararları nelerdir?

2.Büyük veri toplumda eşitliğe katkı sağlar mı ya da eşitsizlik yaratır mı? Nasıl?

3.Büyük veri insanları çeşitli kategorilere ayırmak için kullanılır mı?

4.Büyük veri ile mahremiyet normları aşınabilir mi?

5.Büyük verinin kullanımı ile ilgili fiziksel ve ruhsal olarak nasıl hissediyorsunuz?

6.Bireylerin rızası olmadan verilerinin işlenmesinin etik boyutu ile ilgili ne düşünüyorsunuz?

EK 4. GÖNÜLLÜ KATILIM FORMU

GÖNÜLLÜ KATILIM FORMU

Değerli Katılımcı,

Hacettepe Üniversitesi'nde öğretim üyesi olan Prof. Dr. Tuğça Poyraz danışmanlığında, tarafımdan yürütülen doktora tez çalışmasında kullanılan görüşme soruları büyük veri ve dijital gözetim sistemlerinin toplumda ne tür değişimlere yol açtığını ve açabileceğini tespit etmeye yönelik bilgiler alınmasını amaçlamaktadır. Bireylerin verilerinin gönüllü veya istemsiz şekilde fakat sürekli olarak toplanması ve işlenmesinin çok ciddi avantajlar/dezavantajlar yaratabileceği dijitalleşme koşullarında, bu durumun muhtemel sonuçlarının ontolojik güvenlik kavramı temel alınarak veri bilimcilerinin görüşü doğrultusunda incelenmesi hedeflenmektedir. Bu araştırma için Hacettepe Üniversitesi Etik Komisyonu'ndan gerekli izinler alınmıştır. Araştırma kapsamında katılımcılarla en fazla 50 dakika sürecek bir görüşme yapılacaktır. Görüşmede katılımcıların rahatsızlık duyacağı sorular sorulmayacaktır fakat katılımcılar rahatsız olduklarını düşündükleri sorulara cevap vermeme hakkına sahiptir. Araştırmaya katılım tamamen gönüllülük esasına dayanmaktadır ve katılımcılar araştırmadan istediği zaman çekilebilmektedir. Araştırma sonuçları bilimsel amaçlar için kullanılacak, kişisel bilgileriniz özenle korunacaktır. Araştırmanın sağlıklı sonuçlar verebilmesi için sorulara verilen güvenilir ve içten cevaplar büyük önem taşımaktadır. Araştırmaya katılmaya onay vermeden önce ya da katılımdan sonra aşağıda belirtilen telefon numaram ya da e-mail adresimden, araştırmayla ya da araştırma sonuçlarıyla ilgili sorularınızı sorabileceğinizi belirtmek isterim. Bu yazının ekinde yer alan, etik kurul onayını inceleyebilirsiniz.

Zaman ayırdığınız için teşekkür ederiz.

Tarih:

Katılımcı	**Araştırmacı**
Adı Soyadı:	Adı Soyadı: Araş. Gör. Elif ÖZUZ DAĞDELEN
Adres:	Adres:
Tel:	Tel:
E-posta:	E-posta:
İmza:	İmza: