

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GAZETECİLİK ANABİLİM DALI
BİLİŞİM YÜKSEK LİSANS PROGRAMI

**GÖZETİM KAPİTALİZMİ BAĞLAMINDA NESNELERİN İNTERNETİ: GİZLİLİK
ÇÖZÜMLERİ ÜZERİNE BİR İNCELEME**

Yüksek Lisans Tezi

RUKİYE SENA TÜLÜ

İstanbul, 2025

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
GAZETECİLİK ANABİLİM DALI
BİLİŞİM YÜKSEK LİSANS PROGRAMI

**GÖZETİM KAPİTALİZMİ BAĞLAMINDA NESNELERİN İNTERNETİ: GİZLİLİK
ÇÖZÜMLERİ ÜZERİNE BİR İNCELEME**

Yüksek Lisans Tezi

RUKİYE SENA TÜLÜ

Tez Savunma Jürisi

- Tez Danışmanı: Doç. Dr. Cemile Tokgöz Şahoğlu
- Üye: Prof. Dr. Çiğdem Aytekin
- Üye: Dr. Öğr. Üyesi Alper Değerli

İstanbul, 2025

ÖZET

Gözetim kapitalizmi, insan deneyimlerini bir hammadde olarak kullanan ve bu deneyimlerden davranışsal veri üreterek sermaye birikimi sağlayan bir modeldir. Nesnelerin İnterneti teknolojisi ise insan ile nesne arasındaki ilişkileri bağlantılı hâle getiren bir bütünlüğü temsil etmektedir. Bu çalışmada, gözetim kapitalizmi yaklaşımı nesnelerin interneti ekosistemi üzerinden incelenmiştir. Eleştirel ekonomi politik çerçevede yapılan bu araştırma, nesnelerin interneti teknolojilerinin kapitalist sermaye birikim modelinin her yere yayılmasını kolaylaştırdığı üzerine temellenmektedir. Nesnelerin İnterneti teknolojileri ve artan cihaz kullanımı gözetimi daha da derinleştirmektedir. Bu durum beraberinde veri mahremiyeti sorununu da getirmektedir. Nitekim gözetim operasyonları şirketler tarafından her yere yayılmakta ve kişilerin en mahrem sayılabilecek ortamlarına nüfuz etmektedir. Dolayısıyla yaşanan mahremiyet ihlallerine karşı geliştirilen mevcut gizlilik çözümlerini ve geliştirilebilecek gizlilik çözümlerini incelemek bir gereklilik olarak görülmüştür. Bu çalışmada gizlilik çözümlerinin sorgulanması ve yöntemlerin uygulanmasındaki sınırlılıkların ekonomi politik bağlamda değerlendirilmesi amaçlanmaktadır. Araştırma, nitel araştırma yönteminin uzman görüşleri veri toplama tekniğine dayanmaktadır. Uzman görüşlerinden elde edilen bulgular gizliliğin sağlanması için teknik, yasal ve kullanıcı farkındalığının artırılmasına yönelik çözümler olmuştur.

Anahtar Kelimeler: Gözetim Kapitalizmi, Nesnelerin İnterneti, Mahremiyet, Gizlilik Çözümleri

ABSTRACT

Surveillance capitalism is a model that uses human experiences as raw material and generates behavioral data from these experiences to enable capital accumulation. The Internet of Things (IoT) technology, on the other hand, represents a networked structure that connects relationships between humans and objects. In this study, the approach of surveillance capitalism is examined through the lens of the Internet of Things ecosystem. Conducted within a critical political economy framework, this research is based on the premise that IoT technologies facilitate the pervasive spread of the capitalist model of capital accumulation. IoT technologies and the increasing use of connected devices further deepen surveillance. This, in turn, brings about significant data privacy issues. Indeed, surveillance operations are expanding ubiquitously through corporate actors, penetrating even the most intimate spaces of individuals. Therefore, it has become necessary to examine both existing and potential privacy solutions in response to the ongoing violations of privacy. This study aims to critically assess privacy solutions and evaluate the limitations of their implementation from a political economy perspective. The research is based on a qualitative method using expert interviews as the data collection technique. Findings obtained from expert opinions point to solutions for ensuring privacy, including technical measures, legal frameworks, and the enhancement of user awareness.

Keywords: Surveillance Capitalism, Internet of Things (IoT), Privacy, Privacy Solutions

ÖNSÖZ

Bu çalışmanın ortaya çıkışı, teknoloji ve veri kavramlarına dair yürüttüğüm bireysel sorgulamalar ve akademik okumalarla şekillendi. Başlangıçta rastlantısal şekilde karşılaştığım bazı kaynaklar, zamanla düşünsel yönelimimi belirleyen temel referanslara dönüştü. Dijital teknolojilerin giderek daha derin ve karmaşık bir yapı kazanması, bu alana olan ilgimi pekiştirdi ve çalışmamın odak noktasını oluşturdu. Özellikle büyük veri kavramı etrafında şekillenen tartışmalar, verinin yalnızca teknik bir unsur değil, aynı zamanda ekonomik ve toplumsal ilişkiler içinde anlam kazanan bir yapı olduğunu fark etmemi sağladı. Veriye ekonomi-politik bir perspektifle yaklaşan literatür, beni verinin kim tarafından toplandığı, nasıl kullanıldığı ve bu süreçlerin toplumsal etkileri üzerine düşünmeye yöneltti. Bu bağlamda, verinin birey ve toplum üzerindeki etkilerini sorgulamak ve bu etkilerin dönüştürücü gücünü anlamaya çalışmak bu tezin temel motivasyonunu oluşturdu. Amacım, dijital veri üretimi, kullanımı ve dolaşımı etrafında şekillenen yapıları görünür kılmak ve bu alanlardaki güç ilişkilerine eleştirel bir bakış geliştirmektir. Bu tez, yalnızca bir bitirme çalışması değil, aynı zamanda veri, birey ve toplum arasındaki karmaşık ilişkileri anlamaya yönelik uzun soluklu akademik yolculuğumun ilk adımıdır.

Tez çalışmamın ilk safhasından sonuna kadar yoluma ışık tutan, cesaretlendiren ve engin akademik bilgi birikimiyle daima şevklendiren kıymetli danışman hocam Doç. Dr. Cemile Tokgöz Şahoğlu'na sonsuz teşekkürlerimi sunarım. Tez savunma jürimde yer alan kıymetli hocam Prof. Dr. Çiğdem Aytekin ve Dr. Öğr. üyesi Alper Değerli'ye yorum ve eleştirileri için teşekkür ederim. Tezimde görüşlerine başvurduğum uzmanlara değerli vakitlerini ayırdıkları için, kaynaklarını paylaştıkları için ve bana uluslararası network kurma olanağı sağladıkları için ayrıca teşekkür ederim.

Çocukluğumdan bu yana eğitim süreçlerimi daima destekleyen ve bana olan inançlarını hep yansıtan değerli annem, babam ve abime teşekkür ederim. Son olarak daima elimden tutan, çalışmaya olan azmimi arttıran, aynı zamanda akademik bilgi birikimiyle araştırma sürecimi daima destekleyen kıymetli eşim Mehmet Emin Tülü'ye müteşekkirim.

İÇİNDEKİLER

1. GİRİŞ.....	1
2. GÖZETİM, BÜYÜK VERİ ve KAPİTALİZM KESİŞİMİ	4
2.1. Gözetim Olgusu	4
2.1.1. Gözetime Kuramsal Yaklaşımlar.....	4
2.1.2. Dijital Gözetim.....	5
2.2. Büyük Veri	6
2.2.1. Büyük veri ve Gözetim.....	8
2.2.2. Veri Güvenliği ve Gizlilik Mefhumu.....	11
2.2.3. Veri Odaklı Kapitalizm.....	13
2.3. Ekonomi Politik Çerçeve ve Dijital Gözetim	13
2.3.1. Christian Fuchs, Sosyal Medyanın Ekonomi Politikası ve Sosyalist Gizlilik Önerisi 14	
2.3.2. Nick Couldry ve Ulises Mejias'ın Veri Sömürgecilik Yaklaşımı.....	19
2.3.3. Shoshana Zuboff'un Gözetim Kapitalizmi Yaklaşımı ve Eylem Ekonomileri	24
3. NESNELERİN İNTERNETİ ve GİZLİLİK ÇÖZÜMLERİ.....	29
3.1. Nesnelerin İnterneti: Tarihsel ve Kavramsal Çerçeve	29
3.1.1. Nesnelerin İnternetinin Özellikleri	30
3.1.2. Nesnelerin İnterneti Mimarisi	31
3.1.3. Nesnelerin İnternetinde Kullanılan Teknolojiler	33
3.1.3.1. Radyo Frekanslı Tanımlama (RFID).....	33
3.1.3.2. Kablosuz Sensör Ağları (WSN)	34
3.1.3.3. Ara Katman Yazılımı (Middleware)	34
3.1.3.4. Bulut Bilişim.....	34
3.1.4. Nesnelerin İnterneti Uygulama Alanları	34
3.1.4.1. Akıllı Şehir Uygulamaları.....	35
3.1.4.2. Akıllı Ev Uygulamaları	35
3.1.4.3. Akıllı Sağlık Hizmetleri.....	35
3.1.4.4. Giyilebilir Cihazlar.....	36
3.1.4.5. Endüstriyel Nesnelerin İnterneti Uygulamaları	36
3.2. Nesnelerin İnterneti ve Büyük Veri Gözetimi.....	37
3.2.1. Akıllı Şehirlerde Veri Gözetimi.....	38
3.2.2. Akıllı Ev Ürünlerinde Veri Gözetimi.....	40
3.2.3. Giyilebilir Teknolojilerde ve Konum Tabanlı Teknolojilerde Veri Gözetimi.....	43
3.3. Hesaplanabilir Gizlilik Çözümleri	47
3.3.1. Anonimleştirme	48
3.3.2. Diferansiyel Gizlilik.....	49

3.3.3. Blok zinciri	49
3.3.4. Kişisel Bilgi Yönetim Sistemleri	51
3.3.5. Tasarım Yoluyla Gizlilik Yaklaşımı (Privacy by Design-PBD).....	52
3.3.6. Veri Minimizasyonu	53
4. GİZLİLİK ÇÖZÜMLERİ ÜZERİNE BİR ARAŞTIRMA	58
4.1. Araştırmanın Amacı ve Kapsamı.....	58
4.1. Metodoloji	58
4.2. Araştırmanın Örnekleme ve Veri Toplama Tekniği.....	59
4.3. Temalar ve Bulgular.....	62
4.3.1. Ekonomi Politik Bağlamda Nesnelerin İnterneti.....	62
4.3.2. Nesnelerin İnterneti ile Gözetimin Yaygınlaşması ve Derinleşmesi.....	65
4.3.3. Nesnelerin İnterneti ve Mahremiyet Sorunsalı.....	66
4.3.4. Çözüm Önerileri Bağlamında Teknik ve Yapısal Görüşler	69
4.3.5. Devlet Politikaları Bağlamında Yapılabilecek Uygulamalar.....	72
4.4. Araştırmanın Sonucu	77
5. SONUÇ.....	80
KAYNAKLAR.....	86

Tablolar Listesi

Tablo 1. Gizlilik Stratejileri	53
Tablo 2. Uzmanların Araştırma Alanları	61
Tablo 3. Araştırma Soruları	62



Şekiller Listesi

Şekil 1. Yaygın IoT Mimarileri.....	32
Şekil 2. Hesaplanabilir Gizlilik Çözümleri	47
Şekil 3. Kapitalist Termostat Modeli	55
Şekil 4. Minimize Edilmiş Termostat Modeli.....	56
Şekil 5. Uzman Haritası	60



1. GİRİŞ

Gözetim olgusu, geçmişten günümüze varlığını daima sürdürmüştür. Modern öncesi dönemlerde daha ilkel yöntemlerle uygulanan gözetim, modern zamanlarda özellikle teknolojinin gelişimiyle birlikte farklı bir anlam kazanmıştır. Bir kontrol ve tahakküm aracı olarak da kullanılan gözetim, internetin yaygınlaşmasıyla birlikte şirketlerin çıkarları doğrultusunda kullanılan bir araca dönüşmüştür.

Google'ın çevrimiçi arama motorunu geliştirmesiyle birlikte, insanların web ortamına katılımı önemli ölçüde hız kazanmıştır. Arama motoru kullanıcıları, gerçekleştirdikleri her aramayla dijital ayak izleri bırakmış ve bu süreçte “ikincil veri” olarak adlandırılan veri atıkları ortaya çıkmıştır. Başlangıçta bu veriler, kullanıcı deneyimini iyileştirmek ve daha iyi hizmetler sunmak amacıyla analiz edilmiştir. Ancak zamanla, atık veri olarak değerlendirilen bu ikincil verilerin aslında ekonomik değere sahip olduğu fark edilmiş ve özellikle kullanıcı profillemeye, hedefli reklamcılık gibi uygulamalarda kullanılmaya başlanmıştır. Bu durumu Shoshana Zuboff *gözetim kapitalizmi* kavramı ile ifade etmektedir.

Gözetim kapitalizmi, şirketlerin kullanıcı davranışlarını bir hammaddeye dönüştürerek bunlardan elde edilen veriler aracılığıyla kâr maksimizasyonu sağladığı bir sermaye birikim modelidir. Bu modelde kullanıcıların çevrimiçi etkileşimleri ve davranışları, veriye dönüştürülerek metalaştırılmakta ve ticari amaçlarla işlenmektedir. Elde edilen bu davranışsal veriler yalnızca geçmişini analiz etmek için değil, aynı zamanda gelecekteki davranışları öngörmek ve yönlendirmek amacıyla da kullanılmaktadır. Bu noktada, *eylem ekonomileri* kavramı devreye girmektedir. Şirketler, kullanıcıların gelecekteki tercih ve tepkilerini tahmin ederek bu davranışları yönlendirecek dijital mimariler ve algoritmalar tasarlamakta, böylece veriye dayalı karar süreçlerini ekonomik kazanca dönüştürmektedir. Dolayısıyla gözetim kapitalizmi, yalnızca veriyi metalaştırmakla kalmamakta, aynı zamanda bireylerin eylemlerini öngörme ve şekillendirme gücüne de sahip bir ekonomik yapı haline gelmektedir.

Kullanıcı davranışları, gözetim kapitalizmi içerisinde önemli bir yer tutmaktadır. Bu bağlamda, yalnızca çevrimiçi ortamda sergilenen davranışların değil, gündelik hayattaki pratiklerin de gözetlenmesinin daha kârlı sonuçlar doğurabileceği anlaşılmıştır. Kapitalizmin el değmemiş ormanları artık insan yaşamlarının sermayeleştirilmesine karşılık gelmektedir. Dolayısıyla, çevrimiçi ortamda başlayan gözetim pratikleri bilgisayar başındaki kullanıcıyı yerinden kaldırmış ve fiziksel mekânın her noktasına sirayet eden teknolojiler aracılığıyla gözetimi daha da derinleştirmiştir. Bu derinleşen gözetimin en büyük destekçisi ise nesnelerin interneti (IoT) teknolojileri olmuştur. Fiziksel mekânın her

yerine yayılan sensörler ve akıllı cihaz teknolojileri, anlık olarak ortam ve kullanıcı verisi toplamakta; böylece sürekli bir veri akışı meydana gelmektedir.

Nesnelerin İnterneti teknolojileri, yalnızca nesneler arasındaki iletişimi sağlamakla kalmayıp, aynı zamanda insan ve nesne arasındaki etkileşimi de çeşitli altyapısal teknolojiler aracılığıyla mümkün kılmaktadır. Bu teknolojiler aracılığıyla üretilen sürekli veri akışı, büyük veri gözetiminin temelini oluşturarak kullanıcıların davranışlarının daha kapsamlı bir şekilde izlenmesine olanak tanımaktadır. Akıllı şehir uygulamalarıyla kamusal alanlara yayılan gözetim pratikleri, daha sonra akıllı ev sistemleri aracılığıyla özel yaşam alanlarımıza ve nihayetinde giyilebilir teknolojiler, biyometrik sensörler ve konum izleme sistemleri yoluyla doğrudan bedenlerimize kadar sirayet etmiştir. Bu yayılma, gözetimin yalnızca dijital alanla sınırlı kalmadığını; fiziksel mekânı, günlük yaşam rutinlerini ve bireyin mahremiyetini kuşatan çok katmanlı bir yapıya dönüştüğünü göstermektedir. Nesnelerin İnterneti ile bütünleşen büyük veri gözetimi, böylece hem görünmez hem de sürekli bir denetim mekanizması oluşturarak gözetim kapitalizminin etkisini bireyin en mahrem alanına kadar genişletmektedir.

Nesnelerin İnterneti teknolojilerinin yaşamın her alanına nüfuz etmesiyle birlikte gözetim, yalnızca çevrimiçi etkileşimlerle sınırlı kalmayıp, bireyin fiziksel varlığına ve gündelik rutinlerine kadar genişlemiştir. Bu durum, gözetimin mahiyetini niteliksel olarak dönüştürmüş; sürekli, görünmez ve otomatik hale getirmiştir. Artık bireyler yalnızca dijital ortamlarda değil, evlerinde, sokaklarda ve bedenlerinde de izlenmektedir. Dolayısıyla temel sorunsal, nesnelerin internetinin sunduğu sürekli veri akışı ve nesne-insan etkileşimi üzerinden gözetimi nasıl daha derin, daha kapsamlı ve daha nüfuz edici hale getirdiğidir.

Nesnelerin İnterneti ile derinleşen gözetim, kullanıcı mahremiyetini büyük ölçüde ihlal etmektedir. Şehirlere, evlere ve bedenlere sirayet eden akıllı teknolojiler, kapsamlı bir veri gözetimini mümkün kılmaktadır. Tüm bu teknolojilerin fiziksel mekânı kuşatması, kullanıcı gizliliğinin korunması adına ciddi girişimleri zorunlu kılmaktadır. Gizliliğin sağlanması ise hem çeşitli teknik önlemlerle hem de devlet düzeyinde geliştirilecek ve uygulanacak politikalarla mümkün olabilir.

Bu çalışmanın teorik çerçevesi iki bölümden oluşmaktadır. İlk bölümde, gözetim olgusundan başlanarak büyük veri gözetimine ve ardından gözetim kapitalizmi yaklaşımına geçilmiş; ekonomi politik yaklaşımlar değerlendirilmiştir. İkinci bölüm ise daha özelleşmiş bir içeriğe sahip olup, gözetimin fiziksel mekâna yayılması temel alınarak nesnelerin interneti teknolojileri, uygulama alanları ve bu teknolojilerle ilişkili gözetim örnekleri incelenmiştir. Bu bağlamda, mevcut hesaplamalı gizlilik çözümleri incelenmiş ve nesnelerin interneti özelinde ortaya çıkan kapitalist gözetim pratikleri ile mahremiyet ihlallerine karşı taşıdıkları önlem potansiyelleri değerlendirilmiştir.

Tezin son bölümü, araştırma kısmını içermektedir. Uzman görüşlerine dayanan bu araştırma, gizlilik çözümleri üzerine odaklanmakla birlikte nesnelerin internetinin ekonomi politiğinin incelenmesine olanak sağlamıştır. Araştırmada, mevcut gizlilik çözümlerinin etkinliği hem teknik hem de yasal düzlemde tartışılmıştır. Son olarak, uzmanlar tarafından önerilen gizlilik çözümleri, teknik yaklaşımlar ve politikalar bağlamında kategorize edilmiştir.



2. GÖZETİM, BÜYÜK VERİ ve KAPİTALİZM KESİŞİMİ

Bu bölümde gözetim, büyük veri ve kapitalizm arasındaki çok katmanlı ilişki ele alınmıştır. İlk olarak gözetim olgusunun tarihsel gelişimi ve dijital teknolojilerle birlikte nasıl dönüşüme uğradığı incelenmiş, ardından büyük veri kavramı tanımlanarak veri toplama, analiz etme ve kullanma biçimleri tartışılmıştır. Büyük veri gözetimi bağlamında bireylerin dijital izleri üzerinden sürekli denetlenmeleri, mahremiyetin nasıl aşıldığı ve bu süreçte teknolojik altyapının rolü açıklanmıştır. Bölümün ilerleyen kısımlarında, gözetim ve verinin sermaye birikimi süreçlerinde nasıl araçsallaştırıldığı ortaya konmuş; özellikle dijital platformlar, algoritmalar ve veri temelli iş modelleri üzerinden yeni kapitalist dinamikler analiz edilmiştir. Ekonomi politik yaklaşımlar çerçevesinde, bu dönüşümün güç ilişkilerini nasıl yeniden yapılandığı ve bireyleri ekonomik değer üretiminin bir aracı haline getirdiği tartışılmıştır. Böylece gözetim, büyük veri ve kapitalizm kesişiminde ortaya çıkan yapılar ekonomi politik boyutlarıyla değerlendirilmiştir.

2.1. Gözetim Olgusu

Gözetim olgusu geçmişten günümüze daima varlığını sürdürmüş ve çeşitli nedenlerle gerçekleştirilmiştir. Geçmiş çok eskilere dayanan gözetim, daha çok modern zamanlarda yaygınlık kazanmış ve özellikle ulus devletlerin ortaya çıkmasıyla beraber etki alanı genişlemiştir (Bozkurt, 2001). Gözetim olgusunun amaç ve işlevselliği bakımından toplumsal denetim ve iktidar ilişkileriyle ele alınmasının bir zorunluluk olduğunu vurgulayan Dolgun (2008), gözetim tarihinin insanlık tarihi kadar eskilere dayandığını ifade etmektedir. İktidarların toplumsal düzeni sağlamak ve toplum üzerinde kontrol sağlama amaçları doğrultusunda bu ilişkileri düzenleyebilmek adına belirli norm ve kurallar bir zorunluluk olarak ortaya çıkmıştır. Kontrol mekanizmalarının baş aktörü ise şüphesiz gözetim olmuştur (Dolgun, 2008, s. 21).

Modern öncesi dönemlerde kabileler ve imparatorluklar için gözetim bir egemenlik mekanizması oluştururken modern dönemde ulus devletlerin ortaya çıkışı, kapitalizm ve sanayi devrimiyle beraber gözetim pratikleri kurumsal bir hal almıştır. Kapitalist süreçlerin daha iyi işleyebilmesi için fabrikalarda işçilerin her anının gözetlenerek maksimum verimin alınması hedeflenmiştir. Enformasyon teknolojilerinin gelişmesiyle beraber de gözetim artık sınır tanımayan bir hale bürünmüştür (Dolgun, 2008, s. 22).

2.1.1. Gözetime Kuramsal Yaklaşımlar

Gözetimin tarihsel sürecine bakıldığında “kapatılma” olgusunun dikkat çekici bir yer tuttuğu görülmektedir. İlk olarak, salgın hastalıklarına yakalanan bireylerin hastalıkları yaymalarını engellemek

amacıyla uygulanan kapatılma, zamanla toplumsal denetim amacı güden bir uygulamaya dönüşmüştür (Foucault, 1995, s. 83).

Gözetim çalışmalarında önemli bir model olan ve bir metafor haline gelmiş olan kavram panoptikondur. Panoptikon, ilk olarak Jeremy Bentham tarafından tasarlanmış bir mimari tasarımıdır. Gözetleme üzerine tasarlanan bu mimari tasarım esasında bir hapishane modelidir. Halka biçimli olan ve hücrelere bölünmüş bu hapishane modelinin ortasında bir kule bulunmaktadır. Kuleden yansıtılan ışık bütün hücrelere yansıtılmaktadır ve böylelikle hücrede kalanlar daima gözetlendiklerinin farkındadırlar ancak kendilerini gözetleyeni asla görememektedirler. Panoptikon, aslında hiç inşa edilmemiş bir modeldir ancak gözetim literatüründe önemli bir anlam taşımaktadır. Gözetlemenin disipline edici bir yöntem olduğunu vurgulamakta ve birçok çalışmaya entegre edilmektedir.

Panoptikon, Foucault ile daha geniş bir anlam kazanmıştır. Foucault (1995), panoptikonun yalnızca bir hapishane tasarımı olmadığını, modern toplumlarda iktidarın bir sembolü olduğunu savunmaktadır. Ona göre, toplumun pek çok kurumunda yer alan denetleyici bir göz sayesinde iktidar, belirli bir mekâna bağlı kalmaksızın her yerde varlığını hissettirmektedir. Bu durum, toplum üzerindeki kontrol mekanizmasını daha sistematik ve etkili bir yapıya dönüştürmektedir.

On dokuzuncu yüzyıla gelindiğinde gözetim, modern dönemin temel bir güç mekanizması haline gelmiştir. Bu dönemde sanayi kentlerinin büyümesi, ulus devletlerin yükselişi, kapitalist üretim süreçlerinin genişlemesi ve fabrikaların ortaya çıkışı gibi etkenler, gözetim pratiklerini dönüştürmüştür. Bu dönüşümle birlikte sosyo-ekonomik yaklaşımlar da şekillenerek yeni dinamikler ortaya çıkarmıştır (Tokgöz, 2011, s. 19). Sosyo-ekonomik yaklaşımlardan bir tanesi de Karl Marx'ın kapitalist üretim süreçlerinde emek, sermaye ve gözetim arasındaki ilişkiyi açıklayan yaklaşımıdır. Marx, gözetimi emek ve sermaye arasında bir mücadele unsuru olarak tanımlamıştır. Fabrika işçilerinin üretim yaparken maksimum verime ulaşmaları için kapitalist yöneticiler tarafından sürekli olarak denetlenmesi ve disiplin altına alınması günümüzdeki yönetim anlayışının gelişmesine zemin hazırlamıştır (Bozkurt, 2001).

2.1.2. Dijital Gözetim

Enformasyon teknolojilerinin yaygın kullanılmasıyla beraber toplumsal birçok olgu değişim ve dönüşüme uğradığı gibi gözetim olgusu da dönüşüme uğramıştır. Dijital gözetimin geleneksel gözetimden farklı olmasının odağında teknoloji bulunmaktadır (Tokgöz, 2011). Teknolojik aygıtların insan hayatına ve topluma giderek nüfuz etmesi gözetimin sınırlarını genişletmektedir. Dijital gözetim, geleneksel gözetimde var olan belirli bir merkezde belirli bir noktadan kişilerin izlenmesinden farklı olarak her zaman her yerde ve sessiz bir şekilde gözetimin gerçekleşmesine yol açar. Dijital devlet

uygulamaları, GPS cihazlar, sosyal medya uygulamaları, nesnelerin interneti (IoT) uygulamaları vb. teknolojik uygulamalar kullanım amaçlarının yanı sıra gözetimin de daha derin bir şekilde gerçekleşmesine yol açan sistemlerdir.

Gözetimin yeni bir soluk aldığı dijital gözetim çağında bireyler adeta bir elektronik göz tarafından merceğe alınmakta ve günlük hayatta gittikçe yaygınlaşan teknolojik aygıtların kullanımı buna zemin hazırlamaktadır. Bilgisayarlar ve enformasyon teknolojileri sayesinde gözetim gittikçe görünür olmaktan uzaklaşmakta ve enformasyonel gözetim tıpkı panoptikon gibi hayatın içerisine nüfuz etmektedir (Dolgun, 2008, s. 150). Dolayısıyla modern dönem öncesi gözetim pratikleri, günümüz dijital çağında enformasyon teknolojilerinin etkisiyle farklı bir boyuta evrilmiştir. Gözetim, artık daha görünmez ve derin bir şekilde toplumsal yapıya nüfuz etmiştir. Gelişen bilgi işlem teknolojileri, günlük hayatın dokusuna öylesine entegre olmuştur ki, varlıkları çoğu zaman fark edilmez hale gelmiştir. Bu teknolojiler, fiziksel mekanlara yayılan gözetimi sessiz ve etkili bir şekilde işler kılarak kontrol mekanizmalarının görünmez bir yapı içinde çalışmasına olanak tanımıştır. Gözetimin bu yeni biçimi, modern yaşamın sıradan bir parçası gibi algılanmakta ve bireylerin farkında olmadan gözetim altında kalmalarını sağlamaktadır (Weiser, 1999).

Günümüzde dijital gözetimin en önemli dayanaklarından biri şüphesiz internettir. World Wide Web'in geliştirilmesinden bu yana internet, kullanım açısından sürekli bir büyüme göstermektedir. Web ortamındaki aramalar, çevrimiçi alışverişler, sosyal medya içerikleri, elektronik postalar, internet bağlantılı nesneler ve daha birçok sayısız çevrimiçi işlem internete bağlı bir şekilde gerçekleştirilmektedir. Bu işlemler ve paylaşımların giderek artması internet tabanlı gözetimin de genişlemesine zemin hazırlamaktadır. İnternet gözetimi her zaman her yerde ağa bağlı cihazların kesintisiz bir şekilde devam eden veri akışından faydalanmaktadır. Bu veriler web ortamındaki insan etkinlikleri ve kullanım verilerini içermektedir. Verilerin toplanması, analiz edilmesi, işlenmesi, ilişkilendirilmesi ve istenilen zamanda kopya edilmesi gibi faaliyetler internet gözetiminin birer parçasıdır. Bu çabalarla kullanıcıların ürettikleri emek sonucunda birer dijital kimlik ortaya çıkmaktadır (Uluk, 2022, s. 58). İnternet tabanlı gözetimin birçok farklı amacı bulunmaktadır. Bu amaçların başında daha iyi hizmet gelişimi ve ticari faaliyetler (Gözetimin ticari kâr amacıyla yapılması ekonomi politik yaklaşımların bulunduğu bölümde detaylı bir şekilde incelenmektedir) gibi önemli maddeler yer almaktadır.

2.2. Büyük Veri

Günlük yaşamda bilgi ve iletişim teknolojilerinin yaygınlaşmasıyla birlikte büyük veri kavramı giderek daha önemli hale gelmiştir. Sosyal medya uygulamaları, nesnelerin interneti, giyilebilir teknolojiler ve web ortamındaki kişisel eylemler gibi birçok teknolojik aygıt, sürekli olarak veri

üretimine yol açmaktadır. Veri miktarının ve türlerinin artması, farklı veri kümelerinin oluşmasını ve devasa veri yığınlarıyla karşılaşılmasını beraberinde getirmektedir. Bu verilerin düzenlenmesi ise kapsamlı bir veri işleme sürecini gerektirmektedir. Verinin değerli bir kaynak olduğunu fark eden sektörler, bu verileri doğru şekilde işleyerek ve kullanarak olumlu sonuçlar elde etmektedir. Sağlık, spor, pazarlama, politika, medya ve eğitim gibi pek çok alanı etkileyen veri, aslında hayatın her alanında yer alan ve disiplinler arası bir öneme sahip olan güçlü bir araçtır.

Büyük veri kavramı farklı şekillerde tanımlanmaktadır. Örneğin büyük veri kavramının birçok açıdan yanıltıcı bir kavram olduğu ve bu kavramın yalnızca devasa büyüklükte veri yığınlarını ifade etmediğini aynı zamanda veri setleri üzerinde anlamlı sonuçlar elde edebilme yeteneğine karşılık geldiği ifade edilmektedir (Boyd & Crawford, 2012). Diğer taraftan büyük verinin yalnızca hacimle ifade edilmediğini ancak büyük miktarda verinin toplanması ve analiz edilmesine olanak sağlayan dijital sistemleri ifade ettiği öne sürülmektedir (Kitchin, 2014). Türk literatüründe ise Sütçü ve Aytekin (2018), büyük veriyi karmaşık ve büyük boyutlu özelliğinden ötürü mevcut yöntemler aracılığıyla veya veri madenciliği yazılım araçlarıyla yönetilemeyen veri kümelerinin çatısı olarak kullanılan yeni bir terim olarak tanımlamaktadır (s.157).

Boyd ve Crawford (2012), büyük veriyi üç temel unsurun etkileşimine dayandırarak şu şekilde bir bağlantı kurmaktadır:

- (1) Teknoloji: Büyük veri setlerini toplamak, analiz etmek, bağlamak ve karşılaştırmak için hesaplama gücünü ve algoritmik doğruluğu en üst düzeye çıkarma. (2) Analiz: Büyük veri setlerinden yararlanarak ekonomik, sosyal, teknik ve yasal iddialarda bulunmak amacıyla kalıpları belirleme. (3) Mitoloji: Büyük veri setlerinin, önceden imkânsız olan iç görüler üretebileceği ve doğruluk, nesnellik ve kesinlik havasıyla daha yüksek bir zekâ ve bilgi formu sunduğuna dair yaygın inanç.

2018 yılında hazırlanan bir raporda, küresel veri hacminin 33 zetabayt olduğu belirtilmiştir. Aynı rapora göre, 2025 yılına kadar bu hacmin 175 zetabayta ulaşacağı öngörülmektedir. Bu artış, verilerin katlanarak büyüdüğünü göstermekte ve 2025 yılının “veri çağı” olarak adlandırılmasına zemin hazırlamaktadır. Bu raporda veri alanının genişlemesine yardımcı olan birtakım unsurlar açıklanmaktadır. Bunlardan bazıları gömülü sistemler ve nesnelerin interneti, mobil ve gerçek zamanlı veriler ve bilişsel/yapay zekâ sistemleri olarak karşımıza çıkmaktadır. Nesnelerin interneti tabanlı bağlantılı cihazların artan kullanımıyla beraber 2025'e gelindiğinde ortalama bir kişinin bu cihazlarla günde 4.800 kez etkileşim kuracağı öngörülmektedir (Sütçü & Aytekin, 2018, s. 155).

Büyük veri kavramından bahsederken bu kavramı hayatımıza dahil eden arka plandaki aktörlere değinmek yerinde olacaktır. Bu bağlamda algoritmalar, makine öğrenmesi ve yapay zekâ gibi

uygulamaların varlığı büyük ölçüde önemlidir. Birbiriyle iç içe geçmiş olan yapay zekâ, makine öğrenmesi ve algoritma kavramlarının aslında çok da yeni olduğu söylenemez. Algoritmalar, geçmişten günümüze hayatın içerisinde daima var olan ve karar verme süreçlerini içeren adımlardır. Yapay zekâ ve makine öğrenmesi yöntemleri ise son otuz yıl içinde giderek gelişmiş ve birçok alanda yaygın şekilde kullanılmaya başlanmıştır. Bu kavramlar büyük veri özelinde incelendiğinde aralarında sıkı bir ilişki olduğu sonucuna varılmaktadır. Çünkü makine zekasının çalışabilmesi için sürekli olarak veriyle beslenmesi gerekmektedir. Dolayısıyla veri analizleri gerçekleştirilirken makine zekâsı, beslendiği veriler aracılığıyla bir tahmin modeli oluşturur. Yapay zekâ ise benzer şekilde makine öğrenmesi ve algoritmaları kullanarak bir insanın karar verme davranışına en yakın şekilde karar verebilen sistemlere karşılık gelmektedir. Yapay zekâ için de veri, önemli bir besin kaynağıdır.

Makine zekâsı, otomasyon ve yapay zekâ uygulamaları günden güne daha fazla gelişmekte ve giderek daha yaygın şekilde kullanılmaktadır. Gün geçtikçe fiziksel alanı daha fazla kuşatan bu teknolojiler, yalnızca bilimsel çalışmaların yapıldığı laboratuvar ortamlarında değil, gündelik yaşamın her alanında kendini göstermektedir. Dolayısıyla yaşamın içine sirayet eden bu teknolojiler, bireylerin yaygın teknolojileri kolaylıkla kullanmasına olanak tanımakta ve insan-bilgisayar etkileşimi giderek daha yaygın hâle gelmektedir. Sonuç olarak dijital teknolojiler ile bireyler sıkı bir iletişim hâlinde bulunmaktadır.

2.2.1 Büyük veri ve Gözetim

Yukarıda değinilen Boyd ve Crawford'un (2012), yaklaşımı gözetim çerçevesinde değerlendirildiğinde, veri analizi süreçlerinde kullanılan kalıplar, teknolojinin hangi toplumsal amaçlarla kullanıldığını ortaya koymaktadır. Örneğin, bir platformun amacı hedefli reklamcılık üzerinden sermaye birikimini artırmaksa, algoritmalarını da buna uygun şekilde tasarlayacaktır. Dolayısıyla büyük veri yalnızca teknik bir mesele değil, aynı zamanda diğer toplumsal olgularla da ilişkilidir. Sonuç olarak, bir şirketin ideolojisine göre analiz süreci şekillenmekte ve bu noktada gözetimi temel bir araç olarak kullanmak, özellikle kapitalist üretim süreçlerinde şirketlerin sermaye birikimini artırmasında önemli bir rol oynamaktadır.

İkinci olarak, teknolojiye duyduğumuz sonsuz güven algoritmik gözetimin doğallaştırılmasında büyük bir rol oynar. Ian Bogost (2015), bu durumu sayısal mutlakiyet ve algoritmalara tanrısal güç atfedilmesi kavramsallaştırması üzerinden eleştirmektedir. Nitekim bu yaklaşım, algoritmaların tarafsız, objektif ve insan yanlılığından arınmış araçlar olduğu inancını pekiştirerek, bireylerin sürekli izlenmesini ve verilerinin işlenmesini meşrulaştırır. Algoritmaların aldığı kararlar sorgulanmaz hâle gelirken, bu kararların arkasındaki ekonomik ve ideolojik çıkarlar görünmez olmaya başlar. Böylece

algoritmik gözetim yalnızca teknik bir süreç olarak değil, aynı zamanda toplumsal yapıları şekillendiren bir iktidar biçimi olarak işler.

Yapay zekâ, algoritmalar ve makine öğrenmesi süreçleri, gözetimin derinleşmesine zemin hazırlamıştır. Veri ve gözetim arasındaki ilişki son derece güçlü ve iç içedir. Önceki bölümde de vurgulandığı gibi, veri üretimi her geçen gün artmakta, veri üretim araçları ise giderek daha yaygın hale gelmektedir. Öyle ki, bu süreç gündelik hayatın tüm evrelerine öylesine nüfuz etmiştir ki, fark edilmesi dahi zorlaşmıştır. Sonuç olarak veri, gözetim için adeta keşfedilmiş bir altın madeni gibi büyük bir değer taşımaktadır.

Bu bölümde, yakın geçmişte yaşanan iki önemli skandal olan Edward Snowden'ın ifşaları ve Cambridge Analytica olayı ele alınacaktır. Bu bağlamda, veri gözetiminin hem siyasal etkileri incelenecek hem de kapitalist şirketlerin ekonomi politik düzende oynadığı roller vurgulanacaktır.

2013 yılında Edward Snowden'ın NSA hakkında yaptığı ifşalar, uluslararası çapta büyük yankı uyandırmıştır. Snowden'ın The Guardian gazetesine sunduğu belgelerde, NSA'nın Verizon şirketi aracılığıyla ABD vatandaşlarının telekomünikasyon verilerini izlediğine dair kanıtlar yer almaktadır (Greenwald, 2013). Ayrıca, Snowden'ın ifşaları, NSA'nın PRISM programı aracılığıyla Apple, Google, Microsoft, YouTube ve Facebook gibi büyük teknoloji şirketlerinden doğrudan kullanıcı verilerine erişim sağladığını ortaya koymuştur (Gellman & Poitras, 2013). Bu belgelerin yayınlanması kamuoyunda geniş çapta tepki uyandırmış ve halkın çeşitli protestolar düzenlemesine yol açmıştır. Lyon (2014), bu tepkilerin olağan olduğunu, çünkü gözetim mekanizmalarının ilk kez bu kadar açık bir şekilde gözler önüne serildiğini belirtmektedir. Ancak, benzer bir durum Google için de geçerliken konu NSA olunca kamuoyunun bu denli sert tepki vermesi dikkat çekicidir. Nitekim Google da çevrimiçi ortamda üretilen büyük miktardaki veriyi kendi veri merkezlerinde saklamakta ve milyonlarca kullanıcının çevrimiçi faaliyetlerini izlemektedir. Ancak şirketler tarafından yürütülen gözetim perdelendiği için bu durum kullanıcılar tarafından pek de fark edilmemektedir.

Snowden'ın ifşaları, büyük verinin gözetimi hem hız hem de etki alanı açısından önemli ölçüde genişlettiğini göstermektedir. Aynı zamanda kontrol mekanizmalarını güçlendirerek tahmin yeteneğini daha etkili hale getirmiştir. Bu durum, yalnızca geçmiş verilerin analiz edilmesini değil, aynı zamanda gelecekteki davranışların öngörülmesini de mümkün kılmaktadır (Lyon, 2014). Snowden ifşaları sonrasında, büyük veri alanının artık yalnızca teknik gelişmelerle ilgili olmadığı, aynı zamanda toplumsal ve politik bir boyuta da sahip olduğunun anlaşılması gerektiği görülmüştür. Nitekim, hükümetlerin özellikle güvenlik politikaları geliştirme noktasında büyük veriyi gittikçe daha fazla kullanması ve algoritmaların, tahmine dayalı analizlerin ve veri madenciliğinin güvenlik oluşturma

sürecinde giderek merkezî bir yer edinmesi eleştirilmektedir. Burada eleştirilen en önemli husus, büyük verinin güvenlik amaçlı kullanımının sistematik gözetimi meşrulaştırma çabasına dönüşmesi ve kitlesel gözetimin giderek yaygınlaşmasıdır (Aradau & Blanke, 2015).

Snowden ifşaları, büyük teknoloji şirketlerinin ekonomi politik düzendeki gücünü gözler önüne sermiştir. Devlet kurumlarının kitlesel gözetimi gerçekleştirirken söz konusu teknoloji şirketleri aracılığıyla veri toplaması, bu şirketlerin gözetim pratiklerinde önemli aktörler olduğunu ortaya koymaktadır. Kullanıcı verileri aracılığıyla kâr maksimizasyonu gerçekleştiren teknoloji şirketleri, Snowden ifşalarıyla birlikte artık yalnızca kapitalist işletmeler olarak değil devletle kurdukları iş birliği neticesinde siyasal mekanizmanın da bir parçası olmuştur.

Skandallar silsilesinin bir diğer ayağını Cambridge Analytica-Facebook skandalı oluşturmaktadır. 2013 yılında bir veri şirketi olarak kurulan Cambridge Analytica, 50 milyon Facebook kullanıcısının mikro hedefleme yoluyla detaylı analizlerinin çıkarıldığına dair haberlerle 2018 yılında kamuoyuna duyurulmuştur. ABD'deki Clinton ve Trump arasındaki rekabette, siyasi kampanyalar aracılığıyla Facebook kullanıcılarının verilerine erişilmiş ve siyasi olarak etkilenebilecek kullanıcılara daha hedefli siyasi reklamlar gösterilmiştir (Harbath & Fernekes, 2023). Kullanıcı verilerinin toplanması aşamasında, Cambridge Üniversitesi kıdemli öğretim görevlisi Aleksandr Kogan'ın büyük bir rolü olduğu iddia edilmektedir. Hem veri bilimi hem de psikoloji alanında çalışan Kogan, kullanıcı verilerini toplama amacının bir kişilik profili uygulaması tasarlamak olduğunu belirtmiştir (University of Cambridge, 2018).

Facebook kullanıcılarının verilerine erişilmesi ve manipüle edilmelerinin ortaya çıkmasından iki yıl önce, Cambridge Analytica'nın eski CEO'sunun bir röportajında, her birey hakkında yaklaşık dört ila beş bin arasında veri noktası bulunduğunu dile getirmesi, durumun çok daha ciddi olduğunu göstermektedir. Bu da, ABD'deki yaklaşık 230 milyon insanın kişiliğinin modellenmekte olduğu anlamına gelmektedir (Cheshire, 2016). Ayrıca, eski CEO Alexander Nix, İngiliz Parlamentosu önünde verdiği ifadede, Cambridge Analytica'nın Acxiom, Experian ve Infogroup gibi veri araçlarından ticari veriler temin ettiğini açıklamıştır. Cambridge Analytica şirketinin 50 milyon kullanıcı hakkında veri edinmesi her ne kadar yalnızca Kogan ile ilişkilendiriliyor olsa bile adı geçen veri araçları kaynağın yalnızca Kogan olmadığını göstermektedir (Lomas, 2018).

Cambridge Analytica skandalının yaşanmasının hemen ardından, Federal Ticaret Komisyonu'nun bu konuyla ilgili bir soruşturma başlatması kaçınılmaz olmuştur. Ancak, ne yazık ki başlatılan bu soruşturma, ciddi endişelerin ele alınması noktasında yetersiz kalmıştır. Soruşturmanın

sonucu ise Facebook'a beş milyar dolarlık para cezası verilmesi ve yeni gizlilik standartlarının oluşturulması olmuştur (Hu, 2020).

2.2.2. Veri Güvenliği ve Gizlilik Mefhumu

Günümüzde birçok iş süreçlerinin dijitalleşmesi veri güvenliği ve mahremiyet ihlalleri gibi etik sorunların açığa çıkmasına yol açmıştır. Özellikle dijital gözetim eylemleriyle kişilerin gündelik pratiklerinin kayıt altına alınması ve çoğu eylemlerinin verileştirilmesi kişi mahremiyeti ve güvenliği açısından sorun oluşturup oluşturmadığına dair araştırmaların ortaya çıkmasına zemin hazırlamıştır.

Verilerin gizliliği ve güvenliği, başlı başına çok geniş kapsamlı ele alınması gereken önemli bir konudur. Nitekim bu konu, birçok farklı disiplin tarafından incelenen uçsuz bucaksız bir alanı kapsamaktadır. Güvenlik ve gizlilik, verilerin kötü niyetli yazılımlardan korunması amacıyla çeşitli teknik ve stratejik çerçeveler altında değerlendirildiği gibi yasal düzenlemeler bağlamında da ele alınabilir. Örneğin, Avrupa'daki Genel Veri Koruma Yönetmeliği (GDPR) ve ülkemizdeki Kişisel Verileri Koruma Kanunu (KVKK) bu konuda verilen yasal örnekler arasında yer almaktadır.

Kişisel verilerin mahremiyet ihlalleri dikkate alındığında, akla ilk gelen genellikle kötü niyetli hackerlar tarafından sızdırılan casus yazılımlardır. Mühlhoff (2023), mahremiyet ihlallerine yönelik saldırıları tarihsel süreç içinde üç ayrı kategoriye ayırmaktadır: Bunların ilki, 1960'lı yıllarda ortaya çıkan ve günümüzde hâlâ devam eden bilgisayar korsanlığı ve veri sızıntılarıdır. İkincisi, 1990'lı yıllarda ortaya çıkan ve yeniden tanımlama olarak ifade edilen bir saldırı türüdür. Bu saldırıda anonimlik ortadan kaldırılarak istatistiksel yöntemlerle kimlik tespiti yapılmaktadır. Son olarak, üçüncü saldırı türü 2010 yılından itibaren gelişen tahmine dayalı saldırılardır. Bu yöntemde, desen eşleştirme (pattern matching) yoluyla bilinmeyen bilgiler tahmin edilmektedir (Mühlhoff, 2023). Özellikle üçüncü saldırı türü, bu araştırmanın özel kapsamı içerisine girmektedir. Nitekim şirketler, milyonlarca kullanıcının bilinmeyen bilgilerini tahmin etmek için çeşitli yöntemler kullanmakta ve bu durum, birçok araştırmayla desteklenmektedir. Burada dikkat edilmesi gereken en önemli nokta, tahmine dayalı analizlerin gerçekleştirilmesi için bireylere tahmin modelleri uygulamanın bir gizlilik ihlali olduğu vurgusudur.

Veri güvenliği ve gizliliğin sağlanmasına yönelik teknik çözümler, araştırmanın ikinci bölümünde daha detaylı bir şekilde incelenmektedir. Ancak özetle, anonimleştirme, diferansiyel gizlilik, homomorfik şifreleme ve blokzincir vb. teknikler ile güvenliğin sağlanması gibi kavramlardan bahsedilebilir. Hukuki açıdan bakıldığında ise, Avrupa Birliği Genel Veri Koruma Yönetmeliği (GDPR) değerlendirildiğinde, veri koruma ve demokratik hakların korunması açısından önemli bir araç olduğu açıktır. Ancak, ne yazık ki bu düzenleme yeterli değildir. Örneğin, GDPR'ın tutarsız bir ikili yapıya

sahip olduğunu, yani bir yandan veri sahipliğini teşvik ederken diğer yandan kişisel verilerin metalaştırılma sürecini kolaylaştırdığı da iddia edilmektedir (Manokha, 2023).

Ülkemizde ise, 2016 yılından itibaren hayata geçen Kişisel Verileri Koruma Kurumu (KVKK) ile kişisel verilerin korunması konusunda yeni bir aşamaya geçilmiştir. KVKK, kişisel verilerin işlenmesinin kanunlara uygunluğunu denetlemekte ve aksi bir durumla karşılaşıldığında çeşitli yaptırımlar uygulama yetkisine sahiptir (Çubukcu, 2024).

Veri güvenliği başlığı ele alınırken, gizlilik mefhumunun da değerlendirilmesi ve bu iki kavramın birbirini tamamladığının gösterilmesi isabetli olacaktır. Çünkü gizlilik olmadan güvenliğin olması da pek muhtemel değildir. Gizlilik konusu, birçok disiplin açısından incelenebilecek bir olgudur. Bu bağlamda gizlilik; matematiksel, hukuki ve felsefi açılardan ele alınabildiği gibi, eleştirel ekonomi politik düzlemde de incelenebilecek bir kavramdır.

Gizlilik kavramı farklı şekillerde tanımlanabilmektedir. Tavani (2008), enformasyonel gizliliği “kısıtlı erişim kuramı” çerçevesinde ele almakta ve başkaları tarafından kişisel enformasyona erişimin sınırlandırılması olarak tanımlamaktadır. Diğer taraftan gizlilik, “rahat bırakılma hakkı” olarak da ifade edilmektedir (Warren & Brandeis, 1890). Gizlilik kavramı aynı zamanda, kişilerin kendileri hakkında var olan bilgileri, bir başka tarafla istedikleri zaman ve istedikleri ölçüde paylaşma yetkisini ellerinde bulundurma hakkı olarak tanımlanmaktadır (Westin, 1967). Enformasyonel gizliliğin bu üç tanımı da, kişisel enformasyona nasıl ve kimler tarafından erişileceği ile bu erişimin nasıl düzenleneceği gibi ahlaki sorulara yanıt arama noktasında ortak bir zeminde buluşmaktadır (Fuchs, 2020).

Gizlilik kavramına yönelik eleştirel görüşler de mevcuttur. Örneğin, gizliliğin güçlendirilmesinin değerli ve olumlu bir düşünce olduğuna dair yaygın kanaatin, Amerikan liberal inancına dayandığını savunan yaklaşımlar bulunmaktadır. Ayrıca, gizliliğin kamu yararını olumsuz yönde etkileyebileceğine dair görüşler de öne sürülmektedir (Fuchs, 2020). Gizliliğe yönelik yasa ve söylemlerin gerçek anlamda vatandaşların mahremiyetini sağlamaya yönelik mi yoksa iktidarların ekonomik ve politik çıkarları göz önüne alınarak mı geliştirildiği bazı kitleler tarafından tartışılmaktadır.

Gizlilik, kapitalist sosyal medyada da bir çelişki içinde kendine yer bulmaktadır. Nitekim Facebook ve Google gibi oldukça yaygın kullanılan platformların mottosu, gizliliğin bir çelişki içinde bulunduğunu anlamamıza yardımcı olmaktadır. Facebook, hep daha açık bir ağ olma yolunda ilerlemeye çalışmakta ve kullanıcılarını sürekli daha fazla paylaşım yapmaya teşvik etmektedir. Oysa kullanıcıların gizliliği, eğer şirketlerin ticari mantıklarını zedeliyorsa, gizlilik kavramı onlar tarafından pek de iyi karşılanmamaktadır. Çünkü söz konusu bu şirketler, ticari kaygıları sebebiyle kullanıcıları hep daha açık olmaya ve verilerini paylaşmaya iterek gizliliğin son bulmasını savunmakta; ancak kendi çıkarları söz

konusu olduğunda ise finansal gizliliğin değerli olduğunu savunmaktadırlar. Sonuç olarak kapitalist düzen, gizliliğin çelişkili bir yapısını ortaya koymaktadır (Fuchs, 2020, s. 274).

Gizlilik hakkının sağlanması ve veri koruma hakkının temel haklardan biri olduğunu destekleyen birtakım değerler bulunmaktadır. 2009 yılında Lizbon Antlaşması'nın yürürlüğe girmesiyle birlikte, Avrupa Birliği Temel Haklar Şartı da yürürlüğe girmiştir. Şart'ın 8. maddesine göre, veri koruma hakkı ilk kez tek başına bir temel hak olarak ilan edilmiştir. Veri korumaya yönelik atılan bu adım her ne kadar önemli olsa da gerekçelendirilmesinin ve içeriğinin muğlak olması nedeniyle McDermott (2017), veri korumayı destekleyen değerleri “mahremiyet, özerklik, şeffaflık ve ayrımcılık yapılmaması” olmak üzere dört temel kavram altında sınıflandırmıştır.

2.2.3. Veri Odaklı Kapitalizm

Günümüzde verinin ekonomik süreçlere önemli ölçüde değer sağladığı bilinmektedir. Şirketlerin verinin değerini keşfetmesiyle beraber veriyi ekonomik çıkarları doğrultusunda kullanması ve bunun üzerinden gelir elde etmesi mümkün hale gelmiştir. Veri ve kapitalizm arasındaki ekonomik ilişki birçok farklı etiket ile anılmaktadır. Örneğin gözetim kapitalizmi, enformasyonel kapitalizm, iletişimsel kapitalizm ve ikapitalizm kavramları ve yaklaşımları bu etiketlerden bazılarıdır (Sadowski, 2019). Veri ile kapitalizm arasındaki en temel ilişki, verinin bir hammadde unsuru olarak kullanılmasına dayanmaktadır. Tarihsel olarak, geleneksel kapitalist yöntemler her zaman bir “şeyin” metalaştırılmasını gerektirmiştir. Günümüz kapitalizminde ise veri, kritik bir rol üstlenerek yeni bir meta türü haline gelmiştir.

Bir sonraki başlıkta, dijital gözetim olgusu ekonomi politik perspektiften ele alınacaktır. Bu çerçevede, verinin kapitalist sistem içindeki belirleyici rolünü eleştirel bir bakış açısıyla inceleyen üç önemli yaklaşıma yer verilecektir.

2.3. Ekonomi Politik Çerçeve Dijital Gözetim

Gözetim eylemi, önceki bölümlerde de belirtildiği gibi çeşitli amaçlar doğrultusunda gerçekleştirilmektedir. Bir kontrol mekanizması olarak işlev gören gözetim, ekonomi politik perspektiften değerlendirildiğinde ise çok daha farklı bir anlam kazanmaktadır. Bu bağlamda, gözetim artık yalnızca denetim ve güvenlik aracı olmanın ötesine geçerek ekonomik değer üretme sürecine dönüşmüş ve sermaye birikiminin temel unsurlarından biri haline gelmiştir. Öyle ki, şirketler bireylerin davranışlarını izleyerek gözetim mekanizmalarını devreye sokmakta ve bu sayede kârlarını en üst düzeye çıkarmaktadır. Geçmişten günümüze, şirketlerin bu tür faaliyetlerini eleştirel bir perspektifle inceleyen birçok düşünür ortaya çıkmış ve geliştirdikleri kavramlarla kapitalist düzenin daha iyi anlaşılmasına katkı sağlamışlardır. Örneğin Shoshana Zuboff (2021), şirketlerin gözetim teknolojileri

aracılığıyla topladıkları verilerden kâr elde etmesine dayanan *gözetim kapitalizmi* kavramını ortaya koymuştur. Christian Fuchs (2020), ise kullanıcıların çevrimiçi ortamda veri üretirken dijital emek harcadıklarını ve bilginin bir meta olarak konumlandığı *enformasyonel kapitalizm* kavramını geliştirmiştir. Buna ek olarak, Nick Couldry ve Ulises Mejias, *veri sömürgeciliği* yaklaşımıyla, büyük veri çağında kapitalist üretim süreçlerinin sömürü mekanizmalarına nasıl evrildiğini ele almaktadırlar.

2.3.1. Christian Fuchs, Sosyal Medyanın Ekonomi Politikası ve Sosyalist Gizlilik Önerisi

Christian Fuchs (2021), Karl Marx'ın kendi dönemi içerisindeki teknolojinin bakış açısını bugüne taşıyarak ve günümüz teknoloji toplumu bağlamında inceleyerek önemli çalışmalara imza atmıştır. Bununla birlikte, dijital emek ve dijital emeğin sömürsü üzerine yaptığı çalışmalar ile sosyal medyanın eleştirel analizini ve kapitalist ekonomideki rolünü ele almaktadır (Fuchs, 2020). Bilişsel kapitalizm ile enformasyon toplumu arasında güçlü bir ilişki kurarak, hem tarihsel kapitalizm ile günümüz kapitalizmi arasındaki bağlantıyı ortaya koymuş hem de bu kavramların sınıfsal açıdan bağlayıcı rolüne değinmiştir (Fuchs, 2014).

Günümüz kapitalizmini değerlendirirken Karl Marx'ın argümanlarına başvuran Fuchs (2021), iletişimsel ve enformasyonel kapitalizmin anlaşılmasında Marx'ın kavramlarının kullanılmasının ve günümüz kapitalizmi ekseninde değerlendirilmesinin önemine vurgu yapmaktadır. Nitekim kapitalizm, doğası gereği eleştirel bir şekilde incelenmesi gerekmektedir ve varlığını sürdürdüğü sürece Marx'ı yeniden okumak kaçınılmaz hale gelmektedir. Ayrıca, günümüz kapitalizmine karşı durabilmek için Marx'ın düşüncelerine tekrar başvurulması gerektiği savunulmaktadır.

Fuchs (2021), kapitalizmi yalnızca ekonomik bir oluşum olarak ele almanın eksik olduğunu düşünmektedir. Dolayısıyla, kapitalizm ekonomik bir sistem olmanın yanı sıra toplumu ve insan yaşamını da derinden etkileyen bir olgu olarak değerlendirilmelidir. Bu bağlamda, Marx'ın sömürü, artı-değer, emek, sınıf mücadelesi ve ideoloji gibi kavramlarını günümüz kapitalizmi özelinde incelemek önemlidir. Marx'ın kapitalizmdeki sermaye birikim sürecinde sömürülen artı-değer analizini, sosyal medya platformları ve bağlantılı ağ ekosistemleri bağlamında yeniden okumak mümkündür. Sosyal medyanın sermaye birikim modeli, büyük ölçüde hedefli reklamcılık ve kullanıcı gözetimi üzerine kuruludur. Google, Facebook ve benzeri şirketleşmiş medya platformları, kullanıcı verilerini bir meta haline getirerek reklamcılara satmaktadır. Bu bağlamda, kapitalizmdeki sömürü kavramı dijital kapitalizm perspektifinden ele alındığında, kullanıcıların dijital emeğinin sistematik olarak sömürüldüğü ve karşılığı ödenmeyen bir sermaye birikim modelinin ortaya çıktığı görülmektedir. Dijital emek kavramı derinlemesine incelendiğinde, 1970'li yıllarda Dallas Smythe'in "izleyici metası" olarak geliştirdiği kavrama dayandığı görülmektedir. Sosyal medya platformlarında kullanıcıların

gerçekleştirdiği birçok eylem (görüntü yükleme, ileti gönderme, profil inceleme, arkadaş ekleme vb.) sayesinde bir izleyici metası oluşturulmakta ve bu meta reklamcılara satılmaktadır. Dolayısıyla dijital emek kavramı, günümüz kapitalizminin sömürü anlayışını anlamak için kritik bir çerçeve sunmaktadır (Fuchs, 2020, s. 195).

Sosyal medyanın ekonomi politliğini incelerken Google özelinde detaylı bir inceleme yapan Fuchs (2020), Google'ın her yerde olduğunu, kapitalist üretim süreçlerinde rol oynayan baş karakterlerden biri haline geldiğini ve bir medya şirketinden ziyade hedefli reklamcılık makinesi olarak işlediğini eleştirel bir bakış açısıyla ortaya koymaktadır. Google'ın ekonomik gücü, 1998 yılında kurulmasından bu yana sürekli olarak kâr artışı şeklinde ilerlemiştir. Bir reklam ajansı olarak görülen Google, kâr maksimizasyonunu sürdürme başarısını çevrimiçi reklamcılık, kullanıcı gözetimi ve kişiselleştirme yoluyla elde ettiği muazzam kaynaklara borçludur. Yaklaşık 10 yıl önce yapılan bir araştırmada, çevrimiçi reklamcılıktan elde edilen toplam gelirlerin %54,5 gibi önemli bir oranında Google'ın başrol oynadığı belirtilmektedir. (Fuchs, 2020, ss. 230-231).

Google aynı zamanda “Bir Gözetim Makinesi ve Denetim Aygıtı” olarak nitelendirilmektedir. Bu bağlamda, büyük veri ve gözetim başlığı altında incelenen Snowden ifşaları, Google ve Facebook gibi şirketlerin gerçekleştirdiği kullanıcı gözetimi eylemlerinin yalnızca ekonomik değil, aynı zamanda siyasal gözetimin de bir parçası olduğunu göstermektedir (Fuchs, 2020, s. 236).

Sosyal medya platformlarından biri olan Facebook'a bakıldığında ise durum pek farklı değildir. Facebook, finansal değerini büyük oranda kullanıcı gözetimiyle korur ancak bununla sınırlı değildir. Facebook'un satın alma yoluyla ortaya koyduğu stratejiler de incelenmeye değerdir. Fuchs (2020), Facebook'un satın alma stratejisi sayesinde kendine rakip olabilecek şirketleri bünyesine katarak (Whatsapp, Instagram) medya ekosistemi içinde bir genişleme sağladığını düşünmektedir. Tüm bu çabalar ise şüphesiz kullanıcı gözetiminden bağımsız değildir.

Fuchs'un (2020), sosyal medya eleştirisini yaparken dikkate aldığı hususlardan biri de sosyal medyanın kamusal alan olup olmadığına dair düşünceleridir. Kamusal alan mefhumunu özellikle X uygulaması çerçevesinde değerlendirmekte ve Habermas'ın kamusal alan argümanından etkilenerek eleştirisini gerçekleştirmektedir. Bu bağlamda, kamusal alanın hem siyasal açıdan tartışmaların gerçekleşebileceği bir düzlem olması hem de bu alana katılım sağlayacak kişilerin erişiminin eşit olması gerekmektedir. Ancak Fuchs (2020), X uygulamasında çevrimiçi zorbalık, taciz, şiddet vb. unsurların varlığı nedeniyle kamusal alan tanımıyla bir çelişki oluştuğunu belirtmekte ve bu durumu eleştirmektedir.

Sosyal medya eleştirisine devam ederken, sosyal medyanın katılımcı kültür olarak değerlendirilmesi noktasındaki temellere bakmak da faydalıdır. Kitleli medyanın karşıtı olarak görülen sosyal medyada, kullanıcıların nispeten daha etkin bir şekilde var olması, birçok düşünür tarafından toplumu daha demokratik hale getirdiği ortak görüşüyle ele alınmakta diğer bir deyişle teknoloji-belirlemler yaklaşımı hakimdir. Katılımcı kültür argümanını ele alırken Henry Jenkins'in düşüncelerine atıfta bulunan ve onun göz ardı ettiği noktaları vurgulayan Fuchs (2020), sosyal medyanın katılımcı kültür doğasına eleştirel bir perspektifle yaklaşmaktadır.

Henry Jenkins'in (2006), sosyal medyanın katılımcı kültürüne dair iyimser bir bakış açısına sahip olduğu ve hatta şirketleşmiş sosyal medya ile kullanıcılar arasındaki güç asimetrisinin farkında olsa da bunu göz ardı ettiği görülmektedir. Buna rağmen günümüz medyasının kullanıcıları daha fazla güçlendirdiğine dair çeşitli argümanlar öne sürer. Ayrıca, katılımcı kültürün kültürel çeşitliliği artırdığına yönelik düşünceleri de bulunmaktadır. Bu düşünceleri eleştirel bir bakış açısıyla iki şekilde değerlendirmek mümkündür. Birincisi kültürel çeşitlilikten söz edebilmek için güçlü seslerin var olması gerekir ancak üretilen her ses aynı güçte değildir. İkincisi üretilen içeriklerin bir kenara itilmesi, daha uygun bir ifadeyle, görünürlüğün medya şirketleri gibi güçlü aktörler tarafından yönetildiği gerçeğinin göz ardı edilmesidir (Fuchs, 2020).

Fuchs (2020), sosyal medyanın şirketleşmiş yapısına daima vurgu yaparak onu kapitalist bir ekosistemin parçası olarak görmektedir. Bu bakış açısının arka planında, Web 2.0'in sömürü düzeninin temeli olduğuna dair argümanı yer almaktadır. Bu bağlamda, sosyal medya sayesinde kullanıcıların yaratıcılıklarının abartılı bir şekilde ifade edilmesi eleştirilmektedir. Nitekim, "Yaratıcılık, internet kullanıcılarının daha fazla metalaşmasını, dikkatlerinin, faaliyetlerinin ve ürettikleri verilerin metalaştırılmasını ve sömürülmesini sağlayan bir güçtür." Dolayısıyla, Jenkins ve benzer düşüncedeki düşünürlerin göz ardı ettiği önemli sorular şunlardır: Şirketleşen sosyal medyanın sahibi kimdir? Şirketleşen sosyal medyayı kim kontrol eder? Bu sistemden maddi olarak kimler fayda sağlar? (Fuchs, 2020, ss. 115-116).

Sosyal medyanın ekonomi politikasını incelerken, "üretketici" mefhumundan bahsetmek kaçınılmazdır. Üretketici (prosumer), üretici ile tüketici arasındaki sınırın belirsizleşmesi olarak tanımlanmaktadır (Toffler, 1980, s. 267). Ekonomi ve siyasi demokrasinin yeni bir tezahürü olarak değerlendirilen üretketici mefhumu, Fuchs'a göre "ücret almadan çalışan tüketiciler" ekseninde değerlendirilmemesi nedeniyle göz ardı edilmektedir. Dolayısıyla, Toffler'in eleştirel olmayan üretketici mefhumu, derin değişimleri tanımladığı için eleştirel çalışmalara uygulanabilir (Fuchs, 2020, s. 193).

Web 2.0'ın üretketici kapitalizmini kolaylaştırdığı veya hızlandırdığı yönünde görüşler bulunmaktadır. Sosyal medya platformlarında kullanıcılar sürekli olarak içerik üretir ancak bunun karşılığında herhangi bir ücret almazlar. Üretilen içeriklerin parasal değeri, yine içeriğin üretildiği şirkete dönmektedir. Bu durum, üretketici mefhumunun kapitalist sömürünün yeni bir biçimi olarak değerlendirilmesine ve kullanıcı emeğinin gizli bir şekilde sömürüldüğüne işaret etmektedir. Dolayısıyla üretketicilerin dijital emekleriyle oluşturulan tüm içeriklerin devasa bir veri metası oluşturduğunu ifade etmek yanlış olmaz (Fuchs, 2020).

Christian Fuchs'un sosyal medya eleştirisine dair buraya kadar ortaya konan düşünceleri özetlemek gerekirse, sosyal medyanın ekonomi politiğini kapitalist üretim süreçlerindeki kategorilerle ifade etmek, enformasyonel kapitalizmin daha iyi anlaşılmasına yardımcı olmaktadır. Burada dikkat edilmesi gereken önemli hususlardan biri ise sosyal medyayı incelerken ne tekno-iyimser ne de tekno-kötümserlik bakış açısına sahip olmak gerekir. Önemli olan var olan teknolojiye odaklanmaktan ziyade kapitalizm ve sosyal medyanın etkileşimine odaklanmaktır. Bu noktada, Karl Marx'ın kapitalist üretim süreçlerinin sermaye birikim modelini anlamak isabetli bir yaklaşım sunmaktadır. Bu bağlamda, sosyal medya platformlarının ve onların şirketleşmiş yapısının sermaye birikim modelinde kullanıcı verileri önemli bir yer tutmaktadır. Kullanıcı verileri bir meta olarak kullanılmakta ve reklamcılara satılmaktadır. Ayrıca, bu modelin temelinde gözetim süreçlerinin olması da kaçınılmazdır. Nitekim, sosyal medya şirketleri bir haberleşme platformundan ziyade birer hedefli reklamcılık makinesi olarak addedilmektedir. Son olarak, sosyal medya platformları gerek katılımcı kültür gerek kamusal alan mefhumu açısından bir çelişki yaşamaktadır. Bu eleştiriler ışığında, "Fuchs'un alternatif bir sosyal medya anlayışı mümkün müdür? Mümkünse bu nasıl gerçekleşebilir?" sorularının yanıtına bakmak faydalı olacaktır.

Her şeyden önce, alternatif bir internetin mümkün olup olmadığına yönelik soruya cevap vermek gerekirse, Fuchs'a (2020) göre bu mümkündür. Bu bağlamda yalnızca internetin alternatifi değil, alternatif bir toplumun olup olmayacağı da sorgulanmalıdır. Nitekim bu ikisini birbirinden ayırmamak gerekir. Dolayısıyla hem internetin hem de toplumun temelindeki mevcut düzende birtakım değişiklikler gereklidir. Şüphesiz, bu değişimlerin gerçekleşebilmesi için mücadeleler de gereklidir.

Sosyal medya alternatifleri özelinde değerlendirme yaparken müşterekler mantığına başvurulmaktadır. Bu mantığa göre, tüm insanlar toplum içerisinde eşit haklara sahip olmalıdır. Dolayısıyla, müşterekler mantığı teknolojinin toplumun odağı olmasının aksine, onun bir parçası olduğunu öne sürerek insanların medyayı katılımcı olarak kullanması gerektiğini ifade eder. Olması gerekenler dikkate alındığında, günümüz medyası veya teknolojisi için ne yazık ki bu mantıktan söz edilememektedir. "Çünkü kapitalizm sınıflı bir toplumdur. Kapitalist internet, sınıf yapılı bir internettir."

(Fuchs, 2020, ss. 491-492). Bu bağlamda Fuchs (2020), müşterekler mantığının hayata geçirilmesi için mücadelelerin sosyalizm perspektifinden ele alınması gerektiğini öne sürerek “sosyalist gizlilik” koruma kavramını tanıtmaktadır.

Sibermekân tüketicilerinin korunmasına yönelik mücadelelerin başarıya ulaşması için yedi strateji belirlenmiştir. Bunlar; veri koruma yasaları, onaylı reklamcılığın geliştirilmesi, internet şirketlerinin gözlem platformları tarafından denetlenmesi, dijital emek sendikaları, alternatif medya platformları, kurumlar vergisi ve internet kullanımının alternatif bir toplumsal bağlamda ele alınması şeklinde ifade edilmektedir (Fuchs, 2020, s. 493).

Sosyal medya şirketleri, kâr çıkarları uğruna kullanıcı mahremiyetini göz ardı ederken, veri koruma yasalarına yönelik sıkı yaptırımlar, bu şirketlerin zorlanmasına yardımcı olabilir. Bu noktada, kullanıcı haklarını korumaya yönelik yasaların çıkarılması büyük önem taşımaktadır. Bir diğer strateji olan onaylı reklamcılık politikalarının benimsenmesi, kullanıcıların sürekli olarak bilgilendirilmesine dayanan ve onayları olmadan hedeflenmelerine imkân tanımayan bir yaklaşımdır. Her ne kadar bu strateji kapitalist medya şirketlerinin sermaye birikim sürecini sekteye uğratacağı için onların kabul etmek istemeyeceği bir model olsa da kullanıcıların gizliliğini koruma noktasında önemli bir adım olabilir. Şirket gözlem platformları ise bir karşı gözetim ve karşı mücadele stratejisi olarak değerlendirilmektedir. Bu platformlar, sosyal medya şirketlerinin olumsuz davranışları veya sorumsuzluklarıyla ilgili verileri toplayarak belgeler halinde kamuoyuyla paylaşır. Her ne kadar bu sorumsuzlukların belgelendirilmesi sömürü düzenini ortadan kaldırmasa da kamuoyuna açık hale getirilmesi karşı mücadele için etkili bir adımdır. Bu bağlamda WikiLeaks'e değinmek yerinde olacaktır. WikiLeaks, siyasal ve iktidar şeffaflığını sağlamak amacıyla belgeleri kamuoyuna sunan bir şirket gözlem platformudur. Ancak karşılaştığı “kaynak asimetrisi” nedeniyle büyük oranda engellenmiştir (Fuchs, 2020, s. 498). Sosyalist gizliliğin sağlanması için gerekliliği vurgulanan bir diğer strateji, dijital emek sendikalarının varlığıdır. Sendikalar, ağırlıklı olarak çalışanların çalışma koşullarını iyileştirmek amacıyla çaba sarf eden örgütlerdir. Geleneksel anlamda işçi sendikaları, genellikle ücretli emeğe odaklanmaktadır. Ancak dijital emek bağlamında değerlendirildiğinde, henüz tam olarak hangi konuların odağa alınması gerektiği konusunda çeşitli belirsizlikler bulunmaktadır. Bu bağlamda, Fuchs (2020), *Maddi Olmayan Emek Sendikası* fikrinin doğru bir yaklaşım olacağını öne sürmektedir: “Bir dijital emek sendikası, geçici kullanıcı grevleri düzenleyebilir, dünyanın ücret ödenmemiş işçileri adına evrensel temel gelir talebi biçiminde ücret talep edebilir, alternatif, ticari olmayan platformları destekleyen fonlar oluşturmayı savunabilir” (Fuchs, 2020, s. 500). Alternatif internet platformlarının mümkün olabileceğine dair öngörüler mevcuttur. Şüphesiz bu öngörülerin temelinde, kâr amacı gütmeyen platformların varlığı yatmaktadır. Örneğin, Wikipedia, kâr amacı gütmeyen bir alternatif

platformun var olabileceğini gösteren başarılı örneklerden biridir. Bununla beraber, Facebook'a bir alternatif olarak geliştirilen Diaspora ve bir sosyal paylaşım sitesi olan Kaioo, ticari olmayan alternatif internet platformlarına örnek olarak gösterilebilir. Ancak, kâr amacı gütmeyen dijital platformların kapitalist medya ekonomisinde karşılaştığı iki temel problem bulunmaktadır. Bunlar, garantisi olmayan kaynaklar ve garantisi olmayan emek gerçeğidir. Bu bağlamda, alternatif sosyal medya platformlarını destekleyen sivil toplum örgütlerinin varlığı önemlidir, ancak tek başına yeterli değildir. Fuchs (2020), kaynakların alternatif medyaya yönlendirilmesi için sivil toplum kuruluşlarının sol siyasi partilerle iş birliği içinde olması gerektiğini savunmaktadır. Stratejilerin bir diğer ayağı, büyük medya şirketlerinin vergilendirilmesi yönündedir. Google, Facebook ve birçok medya platformu, dünyanın pek çok yerinde neredeyse hiç vergi mükellefiyetine sahip değildir. Yeterince adil olmayan bu durum, vergi mevzuatlarının uygulanmasıyla önlenmeli ve katılımcı medya ücretinin tesis edilmesi sağlanmalıdır. Son olarak, eşitsizliğin ve sömürünün hüküm sürdüğü bir sosyal medyanın üstesinden gelebilmek için, öncelikle eşitsizliğin ortadan kaldırıldığı bir toplum gereklidir. Bu noktada, gizliliğin sağlanmasına yönelik yapılan çağrılara dair yüzeysel olduklarına yönelik eleştiriler dile getirilmektedir: “Şirketleşmiş İnternet’in hâkimiyeti ışığında, gizliliğin güçlenmesi için yapılan çağrılar dar görüşlü ve yüzeyseldir. Çünkü gizlilik, insanları zarardan korumak için düşünülür; bu zararlara neden olan yapıların ve koşulların üstesinden gelmek için değil.” Bu bağlamda, katılımcı bir demokrasiyi ifade eden “açık toplum” çağrısına kulak verilmelidir. Bu başarıldığı takdirde sömürünün ve gözetimin olmadığı bir medya, bir toplum olması mümkündür (Fuchs, 2020, s. 506).

2.3.2. Nick Couldry ve Ulises Mejias’ın Veri Sömürgeciliği Yaklaşımı

Nick Couldry ve Ulises Mejias, büyük veri çağında kapitalist üretim süreçlerinde kullanıcı verilerinin toplanmasını ve işlenmesini ekonomik, toplumsal ve etik açılardan eleştirel bir bakışla inceleyen önemli düşünürlerdendir. Kapitalist üretim ilişkilerinin insan doğasını kullanarak bireyin özerkliğini tehdit ettiğini savunmakta ve bu sürecin veri sömürgeciliğine işaret ettiğini vurgulamaktadırlar. Kapitalist üretim süreçlerinde kullanıcı verilerinin kullanımına yönelik eleştirilerini tarihsel kapitalizm ile dijital kapitalizm arasındaki bağlantılar üzerinden temellendirmektedirler. Özellikle tarihsel sömürgecilik ile veri sömürgeciliği arasında yapısal benzerlikler bulunduğunu ortaya koymaktadırlar. Bunun yanı sıra, bulut imparatorluğu, veri ilişkilerinin kolonyallığı, postkolonyalizm ve neoliberalizm gibi kavramları da inceleyerek geniş bir çerçeve sunarlar. Ancak, Couldry ve Mejias’ın yaklaşımı geleneksel veri çalışmalarıyla sınırlı kalmamaktadır. Yalnızca Marksist, postkolonyal ya da Foucault’cu analizlerle yetinmek yerine, veri çalışmalarının geniş perspektifinden faydalanarak çok disiplinli bir bakış açısı geliştirmektedirler (Couldry & Mejias, 2022, s. 25).

Kapitalist üretim süreçlerinde veri kaynakları çok katmanlı bir yapıya sahiptir. Bu kaynaklar yalnızca süreçler, nesneler veya bireylerden oluşmakla kalmaz, aynı zamanda bu unsurlar arasındaki etkileşimleri, yani bağlantıları da içerir. Dolayısıyla, veri çıkarma sürecinin gerçekleşebilmesi için insanların, nesnelerin ve bilgisayarların birbirine bağlı olması gerekmektedir. Ancak, bu bağlantılar belirli bedelleri de beraberinde getirir. Bu bedellerin en önemlisi ise insan özerkliğini tehdit eden ve genişleyen gözetim rejimleridir. Sömürgecilik, tarih boyunca daima bir “şeyi” temellük etmeye dayanmıştır. Verinin bir sömürü aracı haline gelmesi ile yeni hammadde biçimlerinin keşfedilmesi arasında bir ilişki bulunmaktadır. Bu bağlamda nasıl ki tarihsel sömürgecilik bölgesel kaynakları sömürü amacıyla ele geçirerek genişlediyse veri sömürgeciliği de insan yaşamının her anını temellük ederek genişlemektedir. Dolayısıyla şimdiye kadar yapılan birçok çalışma, daha çok dijital emeğin sömürüsü üzerine yoğunlaşmıştır. Ancak veri sömürgeciliği yaklaşımını önceki çalışmalardan ayıran temel nokta, insan yaşamının yalnızca ekonomik üretim süreçleriyle değil, günlük pratikler de dahil olmak üzere birçok özel yönüyle sömürgeleştirildiğini vurgulamasıdır. Başka bir ifadeyle, bireylerin yaşamından elde edilen verilerin, ticari kazanç sağlamak amacıyla temellük edilmesi üzerine odaklanmaktadır. Her ne kadar tarihsel sömürgecilik ile veri sömürgeciliği arasında güçlü bir bağ bulunsu da bu iki sömürü biçiminin birebir aynı süreci paylaştığını iddia etmek yanıltıcıdır. Tarihsel sömürgecilik, gezegendeki doğal kaynakların ve insan nüfuslarının fiziksel olarak yok edilmesine dayalı bir süreçtir ve bu anlamda verinin sömürülmesiyle tam olarak aynı yapıyı paylaşmaz (Couldry & Mejias, 2022).

Couldry ve Mejias (2022) bu noktada şu açıklamayı yapmaktadır:

Eğer sömürgecilik, bir tarafın diğerinin yaşam alanını işgal etmesine ve kaynaklarını temellük etmesine izin veren ideolojik rasyonalizasyonlar ile teknolojik araçların (gözetim ve tahakküm mekanizmaları dahil) birleştiği bir süreç olarak anlaşılabiliriyorsa, o halde yeni bir sömürgecilik aşamasına girdiğimizi söyleyebiliriz (s. 83).

Couldry ve Mejias’ın (2022) en önemli iddiası, insan yaşamının sınırsızca sermayeleştirildiği yönündedir. Henüz yirmi yılı aşkın bir geçmişe sahip olan bu yeni sermaye modelinde veriler merkezi bir rol oynamaktadır. Dünyayı farklı kategoriler, ölçütler ve çeşitli temsil biçimleriyle soyutlayarak oluşturulan bir yapı olan veri, bilginin temel yapı taşlarını oluşturur. Burada asıl vurgulanan nokta insan yaşamının, özellikle de sosyal etkileşimlerin, kâr odaklı veri üretimini teşvik edecek şekilde yeniden yapılandırılmasıdır. Bu dönüşüm sürecinde bireylerin yaşamları kişisel alan ile dış müdahale arasındaki sınırların giderek belirsizleştiği bir biçimde tasarlanmakta, sosyal hayat sürekli olarak izlenmekte denetlenmekte ve ekonomik kazanç sağlamak amacıyla temellük edilmektedir.

Artan veri yoğunluğunun kapitalist üretim kaynaklarını sürekli genişletmesi, dikkat çeken bir diğer noktadır. Veri, sermaye olarak kullanıldığında yalnızca statik bir değer olmanın aksine, sürekli hareket halinde olan bir değere dönüşmektedir. Bu durum, dijital izlerin kesintisiz dolaşımını sağlayarak veri ticaretini mümkün kılar. Bunu gerçekleştirmek için bireylerin daha fazla bağlantılı hale getirilmesi ve çeşitli bağlantılı teknolojilerle çevrelenmesi gerekmektedir. Kapitalizm, insan yaşamını ve dünyayı bir sermaye girdisi olarak konumlandığından, üretim süreçlerinin arka planındaki gündelik insan pratiklerinin kontrol edilmesini kolaylaştırır. Üstelik bu kontrol mekanizması artık yalnızca çevrimiçi sosyal medya uygulamalarıyla sınırlı kalmayıp çok daha geniş bir alana yayılmaktadır (Couldry & Mejias, 2022).

Yeni bir sömürü biçimi olan veri sömürgeciliği aynı zamanda yeni ideolojilerin ortaya çıkmasına zemin hazırlamaktadır. Bunların başında bağlantı ideolojisi ile verileştirme ideolojisi gelir. Bağlantı ideolojisi, nesnelerin, insanların ve süreçlerin birbirine bağlanmasının doğal ve kaçınılmaz bir olgu gibi sunulmasına dayanır. Bu bağlamda, Facebook'un kurucusu Mark Zuckerberg'in şirketin kuruluş amacının yalnızca bir şirket yaratmak değil, "dünyayı daha açık ve bağlantılı hale getirmek" olduğunu ifade etmesi, bu ideolojiyi pekiştiren önemli bir örnek olarak öne çıkar. Bağlantı ideolojisinde vurgulanmak istenen asıl nokta yalnızca teknik olarak bir bilgisayar ağına bağlanmaktan ibaret değildir. Asıl önemli olan bu bağlantılar kurulduktan sonra şirketlerin devasa verileri toplarken önlerinde hiçbir engel bulunmamasıdır (Couldry & Mejias, 2022, ss. 46-47).

Couldry ve Mejias (2022), kapitalist üretim süreçlerine insan yaşamlarının dahil edilmesini eleştirirken, literatürde yaygın olarak kullanılan gözetim kapitalizmi, enformasyonel kapitalizm, iletişimsel kapitalizm veya platform kapitalizmi gibi kavramlara özellikle başvurmazlar. Bunun nedeni, veri sömürgeciliğinin kendine özgü ve benzersiz bir model oluşturmasıdır. Mevcut terimlerin, gözetimin kapitalist üretim sürecinin ayrılmaz bir parçası olduğunu kabul etmekle birlikte, bu süreci tam anlamıyla tanımlamak için yetersiz kaldığını savunurlar. Nitekim, "Bugün kapitalizmin her zamankinden farklı bir şey olduğuna dair henüz ikna edici bir argüman ortaya konmuş değil" ifadesiyle, bu dönüşümün mevcut kavramlarla tam olarak açıklanamadığını vurgularlar (Couldry & Mejias, 2022, s. 68). Veri sömürgeciliği yaklaşımını tanımlarken kullanılan metaforlardan biri olan *Bulut İmparatorluğu* kapitalist üretim süreçlerinin dayandığı teknolojik altyapıları simgeleyen bir kavramdır. Bu metafor, veri sömürgeciliği ekonomisiyle pek çok ortak noktaya sahip olup, "imparatorluk" kelimesinin burada geniş çaplı sömürünün hızlı ve etkili bir temsili olarak kullanılması, yazarın bu terimi bilinçli ve stratejik bir seçim olarak benimsediğini gösterir (Couldry & Mejias, 2022, s. 74).

Bulut İmparatorluğu'nun ortaya çıkışını tetikleyen üç temel sorunun altını çizmek önemlidir. Birincisi, artan eşitsizlik nedeniyle bireylerin harcama yapabilecekleri alanların daralması ve bu

bağlamda kapitalizmin insanlara ücretsiz sosyal etkileşim alanları sunarak varlığını sürdürmesidir. İkincisi, üretim süreçlerinde işçilerin yerini giderek makinelerin alması ve bu sayede üretim maliyetlerinin düşmesidir. Üçüncüsü ise, doğal kaynakların tükenmeye başlamasıyla birlikte kapitalizmin yeni sömürü alanları arayışına girmesi ve sosyal yaşamı en büyük kaynak rezervi olarak konumlandırmasıdır. Bu sebeple, Bulut İmparatorluğu kendini sürekli yeniden üreten ve sona ermeyen bir süreç olarak varlığını sürdürmektedir (Couldry & Mejias, 2022). Bu bağlamda, büyük teknoloji şirketlerinin yaşamı sınırsızca sermayeleştirmesi, Philip Stern'in (2011), "şirket devleti" kavramının hayata geçmesi yönünde bir gösterge olarak değerlendirilebilir. Stern'e (2011) göre, şirket devleti yalnızca ticareti değil, aynı zamanda hukuku, toprağı ve bireysel özgürlükleri düzenleme gücüne sahip olup, genel anlamda yaşamı kontrol eden bir otorite konumundadır. Bu noktada, Amazon, Apple, Facebook (günümüzde Meta), Google ve Microsoft gibi "beş büyükler" olarak anılan dev şirketlere dikkat çekilmektedir. Örneğin, çevrimiçi mağaza olarak bilinen Amazon, aynı zamanda bulut bilişim altyapısının %44'ünü sağlayan önemli bir web hizmetleri sağlayıcısıdır. Apple ise yalnızca kendi işletim sistemlerini kullanan cihazlar üretmesi ve medya endüstrisiyle yaptığı tüketici aleyhine gizli anlaşmalar nedeniyle eleştirilmektedir. Öte yandan, Facebook'un iş modeli tamamen kullanıcı verilerini toplamak ve bunları reklam verenlere satmak üzerine kuruludur. Ayrıca, WhatsApp ve Instagram gibi platformları bünyesine katarak kârını artırmayı hedeflemektedir. Google ise dünyanın en büyük ve en çok kullanılan arama motoru olmanın yanı sıra, e-posta hizmetleri, haritalar, iletişim araçları, bulut bilişim çözümleri ve YouTube gibi alt platformlarıyla milyarlarca kişiye ulaşmaktadır. Son olarak, Microsoft Windows işletim sistemi ve internet tarayıcısıyla öne çıkarken, Google ile rekabet edebilmek için her yıl yaklaşık 5 milyar dolar yatırım yapmakta ve dünyanın en büyük ikinci bulut hizmeti sağlayıcısı konumundadır. Tüm bu veriler doğrultusunda, bu şirketlerin kapsamlı etkisi ve devasa gücü göz önüne alındığında, adeta modern şirket devletler ortaya çıkmaktadır.

Beş büyük teknoloji şirketinin geniş pazar payına sahip olmasının yanı sıra, alt şirketleri ve bağlantılı firmalarla kurdukları etkileşimlerin de büyük önem taşıdığı vurgulanmalıdır. Örneğin, Google yalnızca bir donanım ve yazılım üreticisi olmanın ötesinde, aynı zamanda bir veri analizcisi ve simsarı olarak da değerlendirilmektedir. Benzer şekilde, Cambridge Analytica skandalından önce Facebook'un Acxiom ile ortaklık kurması, bu şirkete veri sağladığını göstermektedir. Otomasyonun hayatımızda giderek yaygınlaşması, geçmişte olduğu gibi bugün ve gelecekte de önemli dönüşümlere yol açacaktır. İnsan iş gücünün azalacağı yönündeki yaygın inanç, dolaylı olarak teknoloji şirketleri ile devletler arasında bir ittifakın oluşmasına neden olmaktadır. İş gücündeki bu azalma, toplumsal denetim mekanizmalarının daha da güçlenmesine yol açarken, devlet ve özel sektör arasındaki iş birliğini de pekiştirmektedir. Bu iş birliği, bir yandan gözetim teknolojilerinin geliştirilmesini ve uygulanmasını teşvik ederken, diğer yandan hükümetlerin kalıcı gözetim tedbirlerini yaygınlaştırma yetkisini

artırmaktadır. Burada eleştirilmesi gereken temel nokta, güvenlik ve terörle mücadele adı altında toplanan verilerin kullanım amacının şeffaf olmaması ve bu süreçlerin demokratik değerlere uygun olup olmadığının sorgulanmamasıdır. Bunun yanı sıra, Bulut İmparatorluğu'nun özellikle savunmasız sosyal grupları hedef alması da dikkat edilmesi gereken bir diğer önemli meseledir. Tarihsel sömürgecilikte olduğu gibi, en ağır bedeli yine ezilen gruplar ödemektedir. Son olarak, Bulut İmparatorluğu'nun çeşitli uygulamalar, platformlar ve akıllı teknolojiler aracılığıyla bireylerin yaşamlarını kuşatarak, bu yaşamları metalaştırılmış bir biçimde yeniden sunma gücü göz ardı edilirse, mevcut sistem giderek doğal bir olgu gibi algılanacak ve bu süreçler olağanlaştırılacaktır (Couldry & Mejias, 2022).

Veri sömürgeciliği argümanını gözetim bağlamında ele alan Couldry ve Mejias (2022), geleneksel gözetim ile verilere dayalı gözetim arasında ortak bir bağ bulunduğunu ve bu bağın insanın temel benliğini işgal ettiğini savunmaktadır. Veri toplama süreçlerinin temelinde yatan en derin sorun, bireyin benliğine yönelik bir şiddet biçimi olarak tanımlanır ve şu ifadeyle desteklenir: “Sürekli izlenebilir bir yaşam, alanı sürekli olarak dış bir güç tarafından işgal edilip sömürülen, mülksüzleştirilmiş bir yaşamdır” (Couldry & Mejias, 2022, s. 224). Bu bağlamda, veri sömürgeciliği yalnızca bireysel mahremiyeti değil, aynı zamanda insan yaşamının bütünlüğünü ve özerkliğini de ciddi şekilde tehdit eden bir olgu olarak karşımıza çıkmaktadır.

Verilerin sömürgeleştirildiği iddiasına karşı, bu durumdan nasıl kurtulabileceğine dair çeşitli yaklaşımlar da ortaya konmaktadır. Veri sömürgeciliğine karşı geliştirilen mevcut çözümlere yönelik çeşitli eleştiriler bulunmaktadır. Bu eleştirilerden biri medya okuryazarlığına yöneliktir. Medya okuryazarlığı, sosyal yaşamı verileştiren teknolojilere karşı nasıl mücadele edileceği sorusuna yanıt arayan ve giderek büyüyen bir endüstri olarak değerlendirilmektedir. Bu yaklaşımın bazı faydaları olduğu kabul edilse de veri sömürgeciliğine karşı etkili bir mücadele yöntemi olarak görülmesi yanıltıcıdır ve eleştirilmelidir. Bir diğer eleştiri, düzenleme ve mevzuatlara yöneliktir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) gibi gizlilikle ilgili düzenlemeler, veri sömürgeciliğine dayalı iş modellerine karşı belirli kısıtlamalar getirmiş olsa da yetersiz kalmaktadır. Kişisel verilerin kullanımında rıza alma ilkesi getirilmiş olsa da veri iktidarı varlığını korumakta ve daha kapsamlı düzenlemeler gerekmektedir. Ayrıca, dijital platformların sivil direniş ve eylemcilik alanı olarak değerlendirilmesi de eleştirilmektedir. Hacktivizm gibi protesto türleri, veri iktidarlarının meşruiyetine geçici olarak meydan okuyabilse de bu yöntemlerin tek başına yeterli olmadığı vurgulanmaktadır. Bu bağlamda, “Hacktivizm, veri iktidarıyla yaşamak için genelleştirilebilir bir model olamaz; genelleştirilirse, sonuçları hesaplanamaz bir veri savaşı ortaya çıkacaktır” (Couldry & Mejias, 2022, s. 273). İfadesi bu eleştiriyi desteklemektedir. Son olarak, verilerin sömürgecilikten kurtarılması sürecinde sivil hareketlerin tek başına yeterli olmadığı, bu mücadelenin etkili olabilmesi için kolektif eylemler ve

bilinçlenmenin kaçınılmaz olduğu belirtilmektedir. Bu doğrultuda direniş stratejileri pek çok açıdan değerlendirilebilir. Özellikle bazı stratejiler veriyle doğrudan ilişkili görünmese de aslında onunla bağlantılıdır. Çünkü verilerin gaspını engellemek yalnızca teknolojik stratejilerle değil, aynı zamanda politik, toplumsal ve eğitsel çözümlerle mümkündür. Özellikle feminist gruplar ile ırkçılığa karşı harekete geçen grupların mücadelelerinden çok şey öğrenilmesi gerektiği vurgulanmaktadır (Couldry & Mejias, 2024). Yazarların bu bağlamda, Meksikalı feminist akademisyen Paola Ricaurte ile birlikte kurdukları *Tierra Común* adlı girişim, adalet ve onur mücadelesinin bir parçası olarak incelenmeye değerdir (*Tierra Común*, 2020).

2.3.3. Shoshana Zuboff'un Gözetim Kapitalizmi Yaklaşımı ve Eylem Ekonomileri

Zuboff (2021), “gözetim kapitalizmi” (surveillance capitalism) kavramını ortaya koyarak dijital ekonominin ve büyük teknoloji şirketlerinin gizli işleyişini gözler önüne sermiştir. Gözetim kapitalizmini eleştirel bir bakış açısıyla analiz eden Zuboff, bunun yalnızca yeni bir kapitalist birikim modeli olmadığını, aynı zamanda mahremiyet ve demokratik değerler üzerinde ciddi olumsuz etkiler yarattığını savunmaktadır. Mevcut kapitalizmin yerleşik kavramlarını yeterli görmeyerek, *gözetim kapitalizmi*, *davranışsal artı değer* (Behavioral Surplus) ve *eylem ekonomisi* (Economies of Action) gibi yeni kavramsallaştırmalar geliştirmiştir. Bu yaklaşımıyla, gözetim kapitalizminin eşi benzeri görülmemiş bir özgünlüğe sahip olduğunu ve mevcut teorik çerçevelerle tam olarak anlaşılamayacağını vurgulamaktadır (Zuboff, 2021).

Gözetim kapitalizmi, temel gelir kaynağı insan deneyimi olan yeni bir pazaryeri modeli olarak tanımlanmaktadır. Bu yeni birikim sürecinde, insan deneyimleri bir tür hammadde olarak toplanmakta, çeşitli işlemlerden geçirilerek davranışsal verilere dönüştürülmektedir. Elde edilen bu davranış verileri hem hizmetlerin geliştirilmesi hem de makine öğrenmesi süreçlerinin beslenmesi amacıyla kullanılmaktadır. Davranışsal eylemlerin toplanması, analiz edilmesi ve işlenmesiyle, bireylerin gelecekteki hareketlerine dair öngörüler sunan *tahmin ürünleri* oluşturulmaktadır. Bu öngörü ürünleri, kapitalist birikimin yeni aşaması olan pazaryerinde ticari bir meta haline gelmektedir. Bu yeni birikim modelinin öncüsü tartışmasız şekilde Google'dır. Google tarafından keşfedilen ve sıfır maliyetle kullanıcı eylemlerinin ticari bir değere dönüştürülmesi olarak ifade edilebilecek bu süreç, zamanla yalnızca Google ile sınırlı kalmamış, birçok şirkete yayılmıştır. Zuboff'un (2021), özellikle vurguladığı en önemli noktalardan biri, *davranışsal artı değer* kavramının aslında gözetim mekanizmasının bir parçası olarak görülmesi gerektiğidir. Şirketlerin kâr maksimizasyonu stratejilerinin temelinde, gözetim odaklı bir ekonomik mantık olan gözetim kapitalizmi yatmaktadır. Bu nedenle, bu süreçleri *gözetim ekonomisi* çerçevesinde değerlendirmek mümkündür.

Gözetim kapitalizminin tarihsel gelişimine bakıldığında, bu yeni ekonomik modelin ortaya çıkmasında Google'ın büyük bir rolü olduğu vurgulanmalıdır. Zuboff'a göre (2021), kitle üretimi temelli kapitalizmde Ford Motor Company ve General Motors ne kadar kritik bir öneme sahipse, gözetim kapitalizminin oluşumunda da Google aynı derecede önemli bir rol oynamış ve bu modelin mucidi olmuştur. Google'ın kapitalist düzende oynadığı önemli rol, yeni bir kâr maksimizasyonu modelinin keşfiyle şekillenmiştir. Başlangıçta, kullanıcılar için hizmet geliştirme amacıyla gerçekleştirilen veri toplama süreçleri zamanla kâr elde etme hedefine dönüşmüş ve bu doğrultuda veri toplama süreçleri genişlemiştir. Dolayısıyla Google, kullanıcılar için ücretli hizmetler sunmak yerine, reklam odaklı bir iş modeli benimsemiştir. Geliştirilen algoritmalar sayesinde veriler analiz edilerek reklamlar, uygun kullanıcılara hedeflenmiştir. Bu bağlamda, Google'ın kullanıcıların ne yaptıklarıyla doğrudan ilgilenmediği, ancak ürettikleri verilerin analiz edilerek anlamlı sonuçlara dönüştürüldüğü sonucu ortaya çıkmaktadır (Zuboff, 2015). Hedefli reklamcılığın temel amacı, reklamın etkinliğini artırmak ve kullanıcıların ilgisini çekecek içeriklerle daha yüksek dönüşüm oranları elde etmektir. Reklamların hedeflenmesi noktasında açığa çıkan önemli unsurlardan biri de kişiselleştirmedir. Kullanıcıların davranış verileri, demografik özellikleri veya geçmiş aramaları sayesinde reklamlar kişiye özel olarak hedeflenmektedir. Örneğin bir kullanıcının ilgi duyduğu herhangi bir nesne ile ilgili arama yapması sonucu farklı bir web sayfasında o nesne ve benzeri ile ilgili reklam görmesi ve reklamın kişiselleştirilmiş olması sebebiyle kullanıcının reklama tıklama olasılığı yüksek bir ihtimaldir. Dolayısıyla Google'ın kullanıcı verisi çıkarması artık yalnızca kullanıcılar için hizmet gelişimi amaçlı değil temelde kullanıcıların ilgi alanlarıyla uyumlu reklamların eşleşmesi noktasında kullanıcıların akıllarını okumak için yapılmaktadır. Tüm bu girişimler sonucu ortaya bir kullanıcı profil bilgisi çıkarılarak tahmin ürünleri yerine matematiksel kesinlik yaratılmakta ve böylelikle reklam bütçesinde daha az kayıplar yaşanmaktadır. Kullanıcılar, Google arama motorunda arama eylemlerini gerçekleştirdikçe, birincil davranış verilerinin yanı sıra ikincil davranış verileri de ortaya çıkmaktadır. Örneğin, kullanıcı aramalarındaki anahtar kelimelerden ziyade arama düzenleri, arama sıklıkları, kelimelerin ifade biçimleri, bekleme ve yazma süreleri, konum, noktalama işaretleri gibi ikincil veri kaynakları oluşmaktadır. Başlangıçta yan ürün olarak nitelendirilen bu veriler, gelişigüzel depolanmış ve herhangi bir amaca hizmet etmemiştir. Bu süreçte kritik olan nokta, ikincil kaynak olarak nitelendirilen bu davranış verilerinin değerinin keşfedilmesidir. Esasında “atık veri” olarak adlandırılan bu davranışsal yan ürünler, süreç içerisinde yeniden anlamlandırılarak bir dönüşüm safhasına girmiştir. Bu noktada Zuboff (2021), Google'ın erken gelişim aşamasında yaşanan geri besleme döngülerinin bir güç dengesi ortaya çıkardığını öne sürmektedir. Bu güç dengesi ise aramanın ve insanların birbirlerine olan ihtiyacından doğmuştur. Arama, öğrenmek için insanlara ihtiyaç duyarken insanlar da öğrenmek

için aramaya ihtiyaç duymaktadır. Dolayısıyla bu denge sayesinde Google, daha uygun ve daha kapsamlı sonuçlar üretme yolunda kendini geliştirmiştir.

Kapitalizm özelinde *artı değer* kavramı temel bir dinamik oluştururken gözetim kapitalizminde *davranışsal artı değer* temel bir dinamik oluşturmaktadır. Bu iki aşamada da artı değer kavramları değer yaratma süreçlerini ifade etmektedir. Artı değer teorisi işçi sınıfının emeği ile üretilen ancak karşılığının işçiye ödenmediği bir değer üretimine karşılık gelir. İşçi belli bir süre emek harcadıktan sonra işveren bu emek karşılığında kâr elde eder. Elde edilen bu kâr fazla kısım olarak görülür ve artı değer kavramına işaret eder. Buradan hareketle artı değer fiziksel emek ile ilişkilidir. Davranışsal artı değer kavramı ise kullanıcıların dijital verilerini içermektedir. Kullanıcıların dijital ortamda ürettikleri verilerin şirketler tarafından toplanarak işlenmesi sonucunda kar elde edilmesi davranışsal artı değeri ortaya çıkarmaktadır. Dolayısıyla Zuboff (2021), davranışsal artı değeri gözetim kapitalizminin bir değer yaratma süreci olarak görmektedir.

Gözetim kapitalizmi, kullanıcıların yalnızca çevrimiçi ortamda gerçekleştirdiği eylemleri değil çevrimdışı fiziksel ortamdaki eylemleriyle de ilgilenir. Gözetim kapitalistlerinin rekabetçi dinamikleri dolayısıyla daha fazla ve kesin öngörü sağlayan kaynaklara ulaşma çabası onları el değmemiş ormanlara itmiştir. Bu el değmemiş ormanlar insanların fiziksel dünyadaki tüm eylemlerine karşılık gelmektedir. En fazla ve daha kesin sonuçlar getireceği yolun ise kişinin davranışlarına müdahaleden geçtiğini öne süren Zuboff (2021), şu şekilde açıklamaktadır: “Gözetim kapitalistleri en öngörü vadeden davranışsal verinin gidişata müdahil olmaktan geçtiğini keşfederek davranışları manipüle etme yoluyla kar etmeye başladılar. Otomatikleştirilmiş makine süreçleri davranışlarımızı bilmekle kalmayıp onları büyük ölçüde şekillendirir oldu” (Zuboff, 2021, s. 21). Dolayısıyla rekabetçi baskıların bir sonucu olarak gözetim kapitalizmi kullanıcının arama motoru eylemleri, sosyal medya paylaşımına dair tüm eylemleri veya internette gezindiği her türlü çevrimiçi eylemle sınırlı kalmayarak gündelik pratiklerin sınırsız örneklerini içinde barındıran çevrimdışı bir dünyaya doğru büyüme elde etmiştir. Örneğin, Google üçüncü bir partiye erişim hakkı satabilir ve bu üçüncü partinin bir sigorta şirketi olması muhtemeldir. Bu sigorta şirketi, kullanıcının davranışına müdahale etme hakkını satın almış olur. Risk taşıyan hastalıklara sahip iseniz veya taşıma ihtimaliniz varsa ve zararlı besleniyorsanız, buzdolabınız aniden kilitlenebilir. Bunun sonucunda ise sigortasız kalma veya daha yüksek miktarda sigorta ücreti ödeme yaptırımıyla karşılaşılabilir. Kullanıcıların bu tür yaptırımlarla karşılaşması ise bir güç asimetrisinin doğmasına zemin hazırlamakta ve yeni bir egemenlik biçiminin oluşması adına eleştirilmektedir (Zuboff, 2015).

Kullanıcıların yalnızca çevrimiçi ortamda değil, fiziksel dünyadaki eylemlerini de kapsayan ve gerçek zamanlı davranışların manipülasyonu yoluyla gelir elde etmeyi amaçlayan eylem ekonomisi,

yalnızca kullanıcıların zevklerini tahmin etmeyi hedeflemez. Aynı zamanda, kullanıcıların nerede, ne zaman ve ne yaptıkları konusunda bilgi sahibi olmayı ve bununla kalmayıp bu davranışları değiştirmeyi amaçlar. Davranışları değiştirme hedefinin arkasında yatan en önemli neden ise, en yüksek öngörülebilirliği sunan kaynaklara erişmek ve yüksek oranda garanti edilen kazançlar elde etmektir. Eylem ekonomisi, insan davranışlarının biyolojik doğasından beslendiği gibi, psikolojik süreçlerden de yararlanmaktadır. Davranışsal eylemlerin manipülasyonu, “hareketlendirme kabiliyeti” olarak adlandırılan yeni bir başarımın sonucudur. Bu sistemlerin başarıya ulaşmasında, şüphesiz kullanıcıların bilişsel fonksiyonları da dikkate alınarak davranış değiştirme süreçleri devreye sokulmaktadır (Zuboff, 2021, s. 364).

Eylem ekonomisinin fiziksel mekâna yayılan kuşatıcı etkisini birçok farklı örnekle incelemek mümkün olduğu gibi bunlardan biri konum tabanlı mobil oyunlardan biri olan Pokémon Go oyunudur. Pokémon Go oyunu, gerçek zamanlı yaşam ile dijital ara yüzü buluşturan oyunlardan biridir. Oyuncular yalnızca dijital ortamda kalmaz aynı zamanda belirli lokasyonlara yönlendirilerek gerçek zamanlı davranışlar üretmeleri sağlanmaktadır. Pokémon avına çıkan oyuncular, sınır tanımaksızın sürekli hareket ettirilmekte ve yukarıda bahsi geçen hareketlendirme kabiliyeti aracılığıyla kesintisiz bir şekilde veri üretmektedir. Bu oyun sayesinde geniş bir GPS koordinat ağı oluşturularak evler ve sokaklar, mahremiyet sınırlarının tanınmadığı gözetim temelli kapitalist düzene entegre edilmektedir. Zuboff (2021), Pokémon Go oyununu şu şekilde tanımlar: “Pokémon Go, ölçek, kapsam ve hareketlendirmeyi birleştiren, davranışsal artı değerini sürekli kaynağını çıkaran ve iç, dış, özel ve kamusal alanların haritalanmasını detaylandırmak için taze veri sağlayan gözetim kapitalistlerinin gerçekleşen rüyasıydı” (Zuboff, 2021, s. 386). Dolayısıyla, oyunlaştırma aracılığıyla davranışsal veri üretimi hızlı ve verimli bir şekilde gerçekleştirilmiştir. Son olarak, Pokémon Go oyununun kurucularının ticari iş birliklerine de değinmek gerekir. Örneğin McDonald’s veya Starbucks gibi markalar, Pokémon Go’ya ödeme yaparak kendi şubelerini bir “PokéStop” ya da “Gym” haline getirebilmektedir. Oyuncular bu markaların bulunduğu lokasyonlara yönlendirilerek markaların müşteri çekme olasılığı arttırılmaktadır. Bu bağlamda, markalara bir tür davranış satışı gerçekleştirilerek kâr elde edilmektedir (Zuboff, 2021).

Son olarak, Apple’ın “Error 53” olayı dijital mülkiyet, güvenlik söylemi ve kurumsal tahakküm ilişkisini gözler önüne seren dikkat çekici bir örnektir. Bu olayda, iPhone 6 serisi cihazlarda parmak izi sensörü (Touch ID) yetkili olmayan bir servis tarafından değiştirildiğinde, kullanıcılar cihazlarını yazılım yoluyla güncellemeye çalıştıklarında sistem tarafından “Error 53” hatası ile karşılaşmış ve cihazları tamamen kullanılamaz hale gelmiştir. Apple bu durumu, kullanıcıların biyometrik verilerinin güvenliğini sağlamak amacıyla alınmış bir önlem olarak açıklamıştır. Ancak bu müdahale, güvenlik gerekçesinin ötesinde, kapitalist üretim ilişkileri bağlamında değerlendirildiğinde, onarım sürecinin

şirket tekeline alınması ve kullanıcıların üçüncü taraf servis sağlayıcılarına yönelmesinin engellenmesi anlamına gelmektedir. Bu da beraberinde dijital ürünlerin mülkiyetinin gerçekten kullanıcıda olup olmadığını sorgulatan bir durumu ortaya çıkarmaktadır. Kullanıcı, satın almış olduğu bir cihaz üzerinde tam kontrol hakkına sahip değilse, bu durum yalnızca bir "kullanım izni" çerçevesinde şekillenen mülkiyet ilişkilerine işaret eder. Böylece Error 53 olayı, gözetim kapitalizminin yalnızca kullanıcı verilerinin toplanmasıyla değil, aynı zamanda fiziksel cihazlar üzerindeki teknik ve işlevsel kısıtlamalar yoluyla da kullanıcıları pasifleştirdiğini ve dijital özneliği şirket çıkarları doğrultusunda biçimlendirdiğini göstermektedir.

Üç önemli eleştirel yaklaşım ele alındığında, gözetim konusunun günümüz teknoloji dünyasında daha derin tartışmaların ortasında olduğu görülmektedir. Bu yaklaşımların hepsi bir araya geldiğinde, büyük veri çağında kişilerin verilerinin türlü kılıflarla elde edildiği ve elde edilme yollarının ise anti-demokratik bir görüntü oluşturduğu belirtilmelidir. Hem bilgi hem de güç asimetrisinin ortaya çıkmasına yol açan bu gözetim rejimlerine karşı geliştirilen hem kişisel çözümler hem de hukuki çözümler ne yazık ki yeterli değildir. Bu minvalde, önce çevrimiçi düzende başlayan bu yeni düzen, zamanla kullanıcıları bilgisayar başından kaldırmış ve fiziksel yaşamı da içine alarak kuşatıcı hale gelmiştir. Artık daha fazla bağlantılı nesne ve daha fazla bağlantılı kullanıcı ortaya çıkmıştır. Bu yaklaşımları bir adım daha ileriye taşıyarak ve genelden daha öze doğru giderek bu bağlantılı dünyayı nesnelerin interneti çerçevesinde incelemek çok makul olacaktır. Veri sömürgeciliği ve eylem ekonomileri argümanlarını nesnelerin interneti dünyasında, daha doğru ifade etmek gerekirse bağlantılabilir bir dünyanın örnekleri içerisinde incelemek önem arz etmektedir. Bir sonraki bölümde, nesnelerin interneti konusunun kavramsal çerçevesi incelenecek ve gözetim odağında örnekleri ele alınacaktır. Bu bağlamda, fiziksel yaşamın her alanına yerleşen bu gözetim rejimlerine karşı geliştirilen gizlilik çözümleri değerlendirilecektir.

3. NESNELERİN İNTERNETİ ve GİZLİLİK ÇÖZÜMLERİ

Gözetim kapitalizmi, sınırları sürekli olarak genişleyen bir sermaye birikim modelidir. Önceki bölümde de görüldüğü üzere, kullanıcıların çevrimiçi ortamda bıraktıkları tüm dijital ayak izleri, onların kolayca tanımlanmasına yol açmaktadır. Kapitalist ideolojiye büyük oranda hizmet eden veri işleme süreçleri, makine zekâsının kendini geliştirmesi için sürekli olarak yeni yöntemler üretmeye devam etmektedir. Bunun en belirgin örneği, kullanıcı verilerinin artık yalnızca çevrimiçi ortamlardan değil, sınırlarını aşarak fiziksel mekâna taşmasıdır. Zuboff'un "eylem ekonomileri" kavramında da görüldüğü üzere, davranışların ve bu davranışlardan elde edilen duyguların bile kapitalist ideolojide veri olarak önemli bir karşılığı bulunmaktadır. Şüphesiz, fiziksel mekâna taşan ve davranışsal verilerin yoğun biçimde toplanabildiği bir dünya inşa edilmekte; bu inşa sürecini hızlandıran ve katkı sunan önemli teknolojiler bulunmaktadır. Bu bağlamda, Nesnelerin İnterneti ekosistemi, gözetim kapitalizminin çok daha kârlı ve yoğun bir şekilde işlemesine katkı sağlamaktadır. Nitekim, Nesnelerin İnternetinin her şeyi bağlanabilir kılma özelliği ve her şeyi akıllılaştırarak fiziksel mekânı kuşatan yapısı, gözetim kapitalizmini daha da güçlendirmektedir. Dolayısıyla, Nesnelerin İnterneti ekosistemini gerek teknolojik altyapısıyla gerekse gözetim kapitalizmini destekleyen uygulama alanlarıyla birlikte incelemek önem arz etmektedir.

3.1. Nesnelerin İnterneti: Tarihsel ve Kavramsal Çerçeve

Nesnelerin İnterneti (IoT) kavramı sürekli olarak devam eden bir gelişim sürecine sahip olması sebebiyle standart bir tanıma sahip değildir ve farklı şekillerde tanımlanmaktadır. Nesnelerin interneti kendi kendini organize edebilen, bilgiyi, veriyi ve kaynakları paylaşabilen, ortam içerisinde olası değişiklikler ve durumlar karşısında tepki verebilme potansiyeline sahip akıllı nesnelerin açık ve kapsamlı bir ağı olarak tanımlanmaktadır (Madakam vd., 2015, s. 165). Bu genel tanıma ek olarak daha özel bir bakış açısıyla nesnelerin interneti, RFID etiketleri aracılığıyla bilgisayarların nesneleri otomatik olarak tanımlaması, takip etmesi, izlemesi ve yönetme kabiliyetine sahip olmasıdır (Meloan, 2003). Nesnelerin interneti terimi yalnızca insanlar için değil her zaman ve her yerde bağlantı sağlayan fiziksel nesnelerin küresel altyapısı vizyonunu yansıtmakla beraber sanal veri ve ortamların aynı uzay ve zamanda etkileşim kurabildiği bir dünyayı ifade etmektedir (Kosmatos vd., 2011).

Nesnelerin interneti kavramı resmi olarak ilk kez 2005 yılında ITU (International Telecommunication Union-Uluslararası Telekomünikasyon Birliği) tarafından tanımlanmıştır ve mobil vericilerin nesnelere yerleştirilmesiyle zaman ve mekan fark etmeksizin insanlar ile nesneler arasında etkileşim sağlayan insan-nesne ve nesne-nesne etkileşimini mümkün kılan teknolojik bir devrim olarak ifade edilmiştir (I.T.U. Strategy, 2005).

Nesnelerin interneti terimi için farklı kavramlar da kullanılmaktadır. Örneğin “Nesnelerin Web'i, gömülü zeka, bağlı aygıtlar ve her şeye gücü yeten, hesaplama ve fiziksel süreçlerin bütünleştirilmesi, gerçek ve sanal dünyaları bir araya getiren, her yerde bilişim ve sakin teknoloji, ortam zekası, makine-makine etkileşimi” gibi Nesnelerin İnterneti terimine karşılık gelen kavramsallaştırmalar yer almaktadır (Madakam vd., 2015, s. 166). Bu çeşitlilik, kavramın hem teknik hem de toplumsal bağlamlarda geniş bir anlam spektrumuna sahip olduğunu gösterirken; aynı zamanda nesnelerin internetinin yalnızca nesneler arası bağlantıyı değil, insan, veri, süreç ve cihaz etkileşimini kapsayan daha bütüncül bir çerçeve olan “Her Şeyin İnterneti” (Internet of Everything) anlayışına doğru evrildiğini de ortaya koymaktadır.

İnternet bağlantılı ilk cihaz 1980'li yılların başında icat edilen Carnegie Melon Üniversitesi'ndeki bir kola makinesidir. Bu cihazda programcılar yazdığı bir sunucu programı sayesinde makinedeki depolama alanının ne kadar süredir boş olduğu takip edilmiştir. Ayrıca programcılar, internet aracılığıyla makineye bağlanarak makinenin durumunu uzaktan kontrol edebilmiş ve makine içerisindeki içeceklerin ısı durumunu tespit edebilmiştir (Teicher, 2018).

Nesnelerin interneti terimi ilk kez 1999 yılında Kevin Ashton tarafından ortaya atılmıştır. IoT teknolojisinin öncüsü olarak kabul edilen Ashton, Radyo Frekans Tanımlama-Radio frequency identification (RFID) teknolojisi üzerine yaptığı çalışmalarla nesnelerin birbiriyle bağlantı kurmasını sağlamayı amaçlamıştır (Tao vd., 2016).

3.1.1. Nesnelerin İnternetinin Özellikleri

Nesnelerin interneti platformunun tanımlanma biçimlerinin arkasında aynı zamanda altyapıları yer almakta ve özelliklerine vurgu yapılmaktadır. Bir yandan Nİ platformunun veri toplama ve analizi, cihaz yönetimi ve kontrolü özelliğine vurgu yapılırken öte yandan merkezi yönetim hizmetleri, depolama, işleme, analiz ve görselleştirme özelliklerine de vurgu yapılmaktadır (Asemani vd., 2019, s. 173).

Nesnelerin İnterneti temel özellikleri birçok farklı bakış açısına sahiptir. Bir yandan Nİ platformunun açıklık (Openness), geçerlilik (Viability), güvenilirlik (Reliability), ölçeklenebilirlik (Scalability), birlikte çalışabilirlik (Interoperability), veri yönetimi (Data Management) ve güvenlik sorunları (Security Issues) özelliklerine vurgu yapılırken öte yandan karmaşıklık (Complexity), Yeni 3c Teknolojisi (The new 3c technical), bileşik ekosistem (Compound ecosystem) ve dinamiklik (Dynamics) özelliklerine de dikkat çekilmektedir.

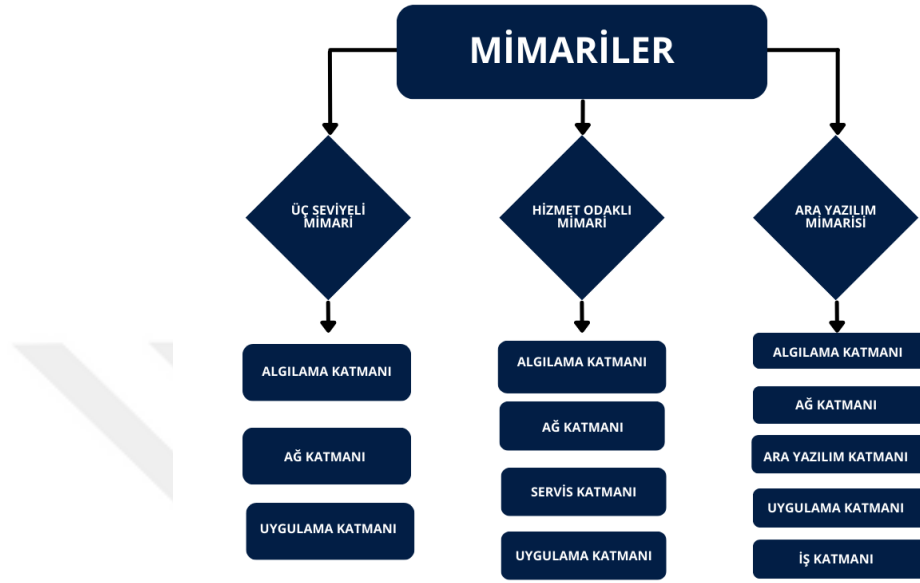
Nesnelerin İnterneti platformunun açıklık özelliği, ham veri ve diğer özel hizmetleri sunmanın dışında esnek bir yapıya sahip olması gerektiğini vurgular. Bunun gerçekleşebilmesi ise bir API (Uygulama Programlama Ara Yüzü) sağlanarak mümkün olmaktadır. Diğer taraftan platformun geçerlilik özelliği iş modeli ve satıcıya bağımlılık bileşenlerine dayanmaktadır. Önerilen teknolojinin pazara sürülmesinin uygunluğu analiz edilmektedir. Güvenilirlik özelliği ise Nİ içerisinde belli bir erişilebilirlik seviyesine ulaşma ve ihtiyaçlara uygun performans sağlaması adına kritik bir öneme sahiptir. Ölçeklenebilirlik, artan cihaz sayısı ve üretilen veri miktarının ölçekli olarak düzenlenebilmesine vurgu yapmaktadır. Nİ'nin heterojen bir yapıya sahip olması, birlikte çalışabilirlik özelliğini ortaya çıkarır, çünkü birden fazla bileşenin etkileşim kurabilmesi için birlikte çalışabilirliğin sağlanması gerekmektedir. Diğer bir özelliği veri yönetimidir. Üretilen verilerin düzenlenmesi noktasında yapılan tasarımları içermektedir. Son olarak güvenlik sorunlarıyla mücadele etme özelliğine vurgu yapılmaktadır. Burada güvenilir bir Nİ'ye ulaşmak için iletişim güvenliği, kimlik doğrulama ve erişim kontrolü gibi çeşitli sorunlar dikkate alınmaktadır (Roman vd., 2013, s. 8).

Nesnelerin İnternetinin 3c teknolojisi olarak adlandırılan önemli bir özelliği bulunmaktadır. 3c, iletişim (communication), bulut bilişim (cloud computing) ve kontrol (control) kavramlarını içinde barındırmaktadır. Bu üç teknoloji etkileşimi sayesinde algılama teknolojisi, gelişmiş ağ teknolojisi, yapay zekâ teknolojisi ve otomasyon birlikte çalışarak Nİ'nin temel hedeflerinden biri olan nesne-insan bağlantısını mümkün kılmaktadır. Bir diğer özellik ise platformun karmaşık (Complexity) bir ağ yapısına sahip olmasıdır. Nİ'nin karmaşık ağ yapısı toplanan veri miktarının fazla ve çeşitli olmasının bir sonucudur. Nİ aynı zamanda bileşik ekosistem (Compound ecosystem) özelliğine de sahiptir. Nİ'nin zaman ve mekân fark etmeksizin her ortama uyum sağlama amacı ile sosyo-ekonomik-doğal kompleks ekosistem teorisi arasında ilişki kurulmaktadır. Bu teoride “sürdürülebilir gelişimin özü, yaşam ve yaşam alanının, iş, toplum, kültür ve maddi üretim ortamının uyumlu bir şekilde gelişmesi” amacı yer almaktadır. Bu amaç doğrultusunda Nİ ile özellik bakımından ilişki kurulmaktadır. Son olarak Nesnelerin İnterneti dinamik bir özelliğe sahiptir. Bu özelliği sayesinde sistem bileşenlerinin gerekmesi halinde yeniden yapılandırılmasına olanak sağlar (Tao vd., 2016, s. 3).

3.1.2. Nesnelerin İnterneti Mimarisi

Nesnelerin internetinin çok sayıda nesneyi birbirine bağlayabilme yeteneği büyük bir ağ trafiğinin oluşmasına ve devasa ölçekte veri kapasitesine ihtiyacın doğmasına sebep olmaktadır. Bununla birlikte gizlilik ve güvenlik sorunları, sürdürülebilirlik ve hizmet kalitesi gibi temel faktörlerin ele alınması gerekmektedir. Ayrıca, sadece ağ trafiği değil depolama kapasitesinin de elverişli olması gereksiniminden dolayı Nİ platformunun maksimum gelişim ve ilerleme göstermesi çeşitli mimariler ve protokollerin uygulanmasına bağlı olmaktadır (Kraijak & Tuwanut, 2015).

Nesnelerin interneti mimarisi tek bir standarda bağlı değildir dolayısıyla birçok farklı değişkene sahip farklı Nİ mimarileri mevcuttur. Ancak genel hatlarıyla en yaygın kullanılan Nİ mimarilerini üç ayrı grupta incelemek mümkündür. Bunlar; üç seviyeli mimari, hizmet odaklı tabanlı mimari ve ara yazılım mimarisi olarak adlandırılmaktadır (Lombardi vd., 2021).



Şekil 1. Yaygın IoT Mimarileri

Üç seviyeli mimari içerisinde nesnelerin fiziksel ve tüm özelliklerini içinde barındıran algılama katmanı, belirli teknolojiler ve protokoller aracılığıyla verilerin uygulama katmanına iletilmesini sağlayan ağ katmanı ve son olarak yazılımın fiziksel dünyaya adım atmış halini temsil eden bir uygulama katmanı yer almaktadır. Algılama katmanı, topladığı bilgiyi işleyerek çevrelediği ortamla etkileşime girmektedir. Bu katmanda fiziksel mekanla etkileşime girebilen ve yüksek hesaplama yeteneklerine sahip olan "akıllı" nesneler yer almaktadır. Akıllı nesnelerin teknolojik yönleri ve kendi kendini tanımlama, kendi kendini teşhis etme ve kendi kendini test etme gibi işlevsel yönlerine odaklanılmaktadır. Mimarinin ikinci seviyesinde bulunan ağ katmanı, algı katmanı aracılığıyla elde edilen verileri uygulama katmanına iletmekle görevlidir. Bu iletişimi sağlayan bağlantı içerisinde neredeyse tüm teknolojiler ve protokoller yer almaktadır. Son seviyede yer alan uygulama katmanı ise hizmetlerin hayata geçirilmesini mümkün kılan yazılımları içermektedir. Bu seviyede toplanan tüm veriler düzenlendikten sonra gerçek zamanlı akıllı nesnelere sunulur. Uygulama katmanında yaygın olarak kullanılan yazılım teknolojilerinden biri dağıtık biçimde yapılandırılabilen ve uzak erişimin sağlanabildiği bulut bilişim ve uç bilişim teknolojileridir. Nesnelerin interneti uygulamalarının hayata geçirilmesinde rol oynayan Amazon AWS, Microsoft Azure, Xively, Firefox WebThings Gateway vb. önemli platformlardır (Lombardi vd., 2021).

Nesnelerin interneti yaygın mimari stillerinden biri de hizmet odaklı mimaridir. Bu modelde üç seviyeli mimarinin içinde yer alan katmanlara ek olarak dördüncü bir katman bulunmaktadır ve servis odaklı katman (SoA) mimarisi olarak adlandırılmıştır.

Son olarak en yaygın kullanılan Nesnelerin İnterneti mimarilerinden biri ara yazılım mimarisi veya beş katmanlı mimari olarak adlandırılan stildir. Nİ mimarilerinde ölçeklenebilirlik, güvenilirlik ve birlikte çalışabilirlik gibi kritik faktörleri destekleyen bir yapının olması önem arz etmektedir. Dolayısıyla ara yazılım mimarisi bu faktörlerin verimli bir şekilde uygulanmasını sağlayan bir yapıya sahiptir ve bu katmanda yer alan uygulamalar veriler ve kullanıcılar arasında bir bağlantı işlevi görmektedir (Gang vd., 2011). Ara yazılım mimarisi; algılama katmanı, ağ katmanı, ara yazılım katmanı, uygulama katmanı ve iş katmanı olmak üzere toplamda beş katmanlı bir mimaridir. Bu mimaride kritik bir öneme sahip olan ara yazılım katmanı aygıtlardan topladığı verileri filtreleme ve uygulamalar için aygıtlara erişim kontrolü sağlayabilmektedir. Son olarak ara yazılım mimarisinin “Çeşitli uygulamaları desteklemesi, çeşitli işletim sistemi ve platformlarda çalışması, dağıtık bilgi işlem ve heterojen ağlar, cihazlar ve uygulamalar arasındaki hizmetlerin etkileşimi, standart protokolleri desteklemesi ve uygulamalar için kararlı, üst düzey bir ara yüz sağlaması” gibi avantajları bu mimarinin yaygın kullanılmasını destekleyen faktörlerdir (Lombardi vd., 2021, s. 6).

3.1.3. Nesnelerin İnternetinde Kullanılan Teknolojiler

Nesnelerin çeşitli hedefleri gerçekleştirebilmesi için kullanılan birçok teknoloji mevcuttur. Yaygın olarak kullanılan teknolojiler genel olarak Radyo Frekanslı Tanımlama (RFID), Kablosuz Sensör Ağları (WSN), Ara Katman Yazılımı (Middleware), Bulut Bilişim, Yakın alan iletişimi (NFC), Bluetooth, Wİ-Fİ ve yapay zeka teknolojilerini içermektedir (Lee & Lee, 2015).

3.1.3.1. Radyo Frekanslı Tanımlama (RFID)

Nesnelerin interneti platformunun önemli bileşenlerinden biri olan RFID teknolojisi, sahip olduğu etiketler aracılığıyla otomatik olarak kimlikleri tanımlamakta ve verilerin yakalanmasını sağlamaktadır. RFID etiketleri, basit barkodlara nazaran çok daha fazla veri depolayabilme potansiyeline sahiptir (Lee & Lee, 2015).

RFID teknolojisi kablosuz iletişim sistemlerinin önemli bir parçasını oluşturmaktadır. Özellikle fiziksel nesneleri tanımlamak için kullanılan bu teknoloji, okuyucu, etiket ve anten bileşenlerinin radyo frekansı ile haberleşmesi sonucu sürecini tamamlamaktadır. RFID teknolojisinin geliştirilebilir ve esnek bir yapıya sahip olması onun kullanım alanlarını genişletmektedir. Akıllı park uygulamaları, Akıllı trafik denetimi ve yönetimi için RFID ile elektronik plaka uygulaması, e-sınav uygulaması, Aktif RFID kullanarak iç mekânda yer algılaması (LANDMARC), Radyo frekans kimlik tanıma sistemleri ile

elektronik para uygulamasının gerçekleşmesi, ve HGS (Hızlı geçiş sistemi) RFID teknolojisinin önemli uygulamalarını içermektedir (Maraşlı & Çıbuk, 2015).

3.1.3.2. Kablosuz Sensör Ağları (WSN)

Nesnelerin interneti için önemli bir unsur olan kablosuz sensör ağları, fiziksel veya çevresel koşulları izleyerek ortam koşulları hakkında veri toplamaktadır. Örneğin bir ortamdaki sıcaklık, ses, titreşim ve basınç değerleri gibi veriler çeşitli sensörlerin kullanımıyla elde edilmektedir. Ayrıca bu ağlar, birçok fiziksel ortama entegre edilmesinden dolayı birçok farklı uygulamaya dahil edilmiştir. Örneğin bir hastanın vücuduna yerleştirilen sensörler doktorların uyguladığı tedaviye ne ölçüde tepki verdiğini açıklayabilmektedir (Madakam vd., 2015). Bu durum ise kablosuz sensör ağlarının giyilebilir teknolojilerde oldukça yaygın kullanılmasını açıklayabilmektedir. Nitekim akıllı saatlerin kişi vücudu hakkında çeşitli veriler sağlaması bunun en güzel örneklerindendir.

3.1.3.3. Ara Katman Yazılımı (Middleware)

1980'lerden itibaren eski ve yeni teknolojiler arasında güçlü entegrasyon özelliği sayesinde popüler olan ara katman yazılımı, iletişimi kolaylaştıran yazılım uygulamaları arasında yer almaktadır. Nesnelerin İnterneti uygulamalarında önemli bir yere sahip olan ara katman yazılımı, Nİ'nin dağıtık heterojen yapısına uyumlu bir şekilde eşlik etmektedir. Buna en güzel verilebilecek örneklerden biri Global Sensör Ağlarıdır (GSN). Herhangi bir programlama çabası gerektirmeden sensör hizmetleri geliştirilmekte ve dağıtılmaktadır (Lee & Lee, 2015).

3.1.3.4. Bulut Bilişim

Bulut bilişim, birçok uygulama ve verilerin depolanmasını sağlayan sanal bir sunucudur. Ortam fark etmeksizin internete bağlanarak cihazlar aracılığıyla verilere kolay bir şekilde ulaşım sağlanabilmektedir. Karşılaştırmalı bir analiz olarak verilerin hard disklerde depolanması yerine internet ortamında yer alan sanal sunucularda depolanması bulut bilişimi ifade etmektedir. Bulut bilişimin olumlu özellikleri arasında yer alan geniş depolama alanı, hızlı olması ve maliyet açısından tasarruflu olması avantajları bulut bilişimin daha fazla kullanılmasına olanak tanımaktadır. Dolayısıyla Nİ uygulamalarında ortaya çıkan devasa büyüklükteki veri ihtiyaçlarının karşılanması açısından bulut bilişim önemli bir avantaj sunmaktadır (Gündüz & Daş, 2017).

3.1.4. Nesnelerin İnterneti Uygulama Alanları

Nesnelerin interneti teknolojisinin kullanım alanları gittikçe genişlemekte ve çeşitli alanları kapsamaktadır. Akıllı şehir ve akıllı ev uygulamaları, pazarlama, lojistik, ticaret vb. alanlarda Nİ teknolojileri oldukça yaygın kullanılmaktadır. Nesnelerin interneti kullanım alanları sağlık, tarım, eğitim, ulaşım ve kamu sektörü gibi başlıca sektörlerde kendine yer bulmaktadır.

3.1.4.1. Akıllı Şehir Uygulamaları

Nesnelerin internetinin en çok kullanım alanlarından biri akıllı şehirlerdir. Akıllı şehirlerin hem kendi bünyesinde birçok uygulama barındıracak potansiyelde olması hem de büyük şirketlerin daha çok bu alana yatırım yapması akıllı şehirlerin en yaygın kullanım alanlarından biri olmasına zemin hazırlamıştır. Akıllı şehirlerde teknolojilere bağlı çeşitli sistemler toplum için önem arz eden sağlık, kamu hizmetleri, ulaşım vb. hizmetlerin sağlanması için birbirine bağlanmaktadır (Al-Fuqaha vd., 2015). Bilgi ve iletişim teknolojilerinin birbirine entegre edildiği akıllı şehirler, yaşam kalite standartlarını iyileştirmeyi amaçlayan bir kentsel gelişim vizyonu olarak tanımlanmaktadır (Lombardi vd., 2021).

3.1.4.2. Akıllı Ev Uygulamaları

Nesnelerin interneti teknolojisinin yayılımı genişledikçe mikro uygulamalar daha da artmaktadır. Bunun en güzel örneklerinden biri de kişilerin yaşam alanları olan evlerdir. Otomasyona sahip bir ev kişinin günlük yaşamındaki pek çok eylemi daha konforlu ve sistematik bir hale getirebilmektedir. Günümüzde evin içinde yer alan nesnelerin birçoğu birbiriyle haberleşerek insan müdahalesini ya hiç gerektirmeyecek şekilde ya da çok az müdahalenin bulunduğu şekilde varlığını sürdürmektedir.

Bir akıllı ev prototipinde birden fazla akıllı uygulama örneği verilebilir ve bu uygulamalar esnek yapısı nedeniyle sürekli olarak geliştirilebilmektedir. Akıllı evler, uzaktan kumanda ile kontrol edilebilen evler, programlanabilir evler, senaryolandırılmış evler ve yapay zekaya sahip evler olarak çeşitlilik göstermektedir. Bu çeşitlilik teknolojik gelişmelere bağlı olarak sürekli değişime uğramıştır. Önceleri insan müdahalesi olmadan çalışmayan uygulamalar şimdi yapay zekâ aracılığıyla daha da ileri bir safhaya taşınmıştır. Yapay zekaya sahip evlerde insan müdahalesine gerek kalmadan kişilerin ev içi hareketleri izlenerek analiz edilmekte ve yapay zeka kişi davranışlarına göre eylemlerini devreye sokabilmektedir (Avcı, 2022).

3.1.4.3. Akıllı Sağlık Hizmetleri

Nesnelerin interneti uygulamalarının etkilediği önemli alanlardan biri de sağlık sektörüdür. Nesnelerin İnterneti teknolojileri kullanılarak birçok sağlık uygulaması geliştirilmekte ve olası sorunlara etkili çözümler üretilmektedir.

Nesnelerin internetinin önemli teknolojilerinden biri olan sensörler akıllı sağlık hizmetlerinin önemli bir bileşenini oluşturmaktadır. Örneğin parkinson vb. nörolojik hastalıklara sahip olan hastalar izleme sensörleri aracılığıyla izlenmekte ve vücut içerisinde gelişen birtakım belirtiler kolayca teşhis edilmektedir. Vücuda yerleştirilen sensörler arasında Elektromiyografi (EMG), Elektroensefalografi

(EEG) ivmeölçer gonyometre (eklem hareket açıklığı ölçer) ve optik hareket yakalama sistemleri bulunmaktadır (Delrobaei vd., 2018). Akıllı sağlık sistemlerinde sensörlerin yanı sıra giyilebilir teknolojiler de yaygın bir şekilde kullanılmaktadır. Giyilebilir teknolojiler insan vücuduna dair gerekli verileri toplayarak ilgili kişi ya da kurumlara iletmekte ve hasta takibi zaman aşımına uğramadan anlık bir şekilde yapılmaktadır. Örneğin akıllı bileklikler ve saatler, akıllı gözlükler, akıllı ayakkabılar ve hasta takip yamaları hem dünyada hem de ülkemizde kullanımı yaygınlaşmaya başlayan giyilebilir teknolojilerdir. Bu cihazlar kişilerin tansiyon, şeker, nabız ve kandaki oksijen derecesi gibi klinik değeri olan bilgileri ortaya koyarak özellikle erken teşhis noktasında önemli bir avantaj sunmaktadır (Kılıç & Tosun, 2021).

3.1.4.4. Giyilebilir Cihazlar

Giyilebilir cihazlar, bir önceki konu başlığında da değinildiği gibi akıllı sağlık uygulamalarında yaygın kullanılmaktadır ancak giyilebilir teknolojiler yalnızca sağlık sektörüyle sınırlı kalmamaktadır. Moda, endüstri, spor, eğlence vb. sektörlerde de kullanım alanı olan giyilebilir teknolojiler, birçok sektöre entegre edilebilmektedir. Günlük hayatta çok sık rastladığımız akıllı saatler giyilebilir cihazların en yaygın örneklerinden biridir. Wİ-Fİ, Bluetooth ve GPS gibi teknolojilerin bu saatlere entegre edilmesiyle akıllı saatler bir telefonun sahip olduğu birçok işlevi yerine getirebilmektedir. Bunun yanı sıra içerisinde bulunan temel sensörler aracılığıyla akıllı saat kullanıcılarının günlük davranış eylemleri ve fiziksel aktivitelerine dair veriler kaydedilmektedir. Örneğin uyku esnasında gerçekleşen hareketlilikler, nabızın ölçülmesi, kalp ritim hareketleri, spor esnasında adımların sayılması vb. eylemlerin verileri kaydedilmektedir.

3.1.4.5. Endüstriyel Nesnelerin İnterneti Uygulamaları

Nesnelerin interneti teknolojilerinin endüstriyel ortamda kullanılması endüstriyel nesnelerin interneti (IIoT) gibi yeni bir kavramın ortaya çıkmasına yol açmıştır. Endüstriyel alanlarda nesnelerin interneti uygulamalarının kullanılması bazı avantajlar sunmaktadır. Bunlar, üretim süreçlerinin otomatikleştirilmesi ve insan müdahalesinin olabildiğince en aza indirgenmesi sonucu maliyetlerin azalması ve verimlilik oranının artmasıdır. (Turkyılmaz, 2024). Ancak burada önemli bir ayrım gözetilmelidir. Nesnelerin internetinin diğer uygulamalarında merkezde çoğunlukla birey yer almakta ve bu bağlamda bireyin izlenmesi ve gözetimi ön plana çıkmaktadır. Oysa endüstriyel nesnelerin internetinde durum daha farklıdır; burada bireyden çok süreçler, makineler ve üretim ağları odaklıdır. Bu çalışmada özellikle kâr potansiyeli yüksek, dolayısıyla sermaye birikimine dönüştürülebilen IIoT uygulamaları ele alınmıştır. Zira bazı tarımsal ya da kamusal uygulamalarda olduğu gibi, her IIoT kullanımının doğrudan ekonomik kazanca dönüşmediği görülmektedir. Bu nedenle analiz, ağırlıklı olarak ekonomik değer üretimiyle bağlantılı kullanım örnekleri üzerinden ilerletilmiştir.

3.2. Nesnelerin İnterneti ve Büyük Veri Gözetimi

Her akıllı obje bir çeşit kukladır; tüm akıllılığıyla kuklacının saklı ekonomik zorunlulukları için talihsizce dans eden bir kukla olarak kalır. Ürünler, hizmetler ve uygulamalar kaçınılmazlığın davul sesiyle, bizim gerçekliği evim, yaşamım ve bedenim dediğimiz hala vahşi alanlardan yontulan gözetleme gelirleri vaadine doğru yürüyüşe geçer. Her akıllı ürün vazgeçilmez sorularımızı tekrarlar: Akıllı ürün neyi bilir ve bunu kime söyler? Kim bilir? Kim karar verir? Kimin karar verdiğine kim karar verir?

Shoshana Zuboff (2021, s. 296)

Teknolojinin hızlı gelişimi hayatımıza dahil olan akıllı cihazların sayısında büyük bir artışın yaşanmasına sebep olmuştur. Akıllı cihazlar ve nesnelerin interneti tabanlı uygulamalar, sahip olduğu teknolojiler sayesinde günlük hayatta yaşanan birçok probleme büyük ölçüde çözüm getirmiştir. Nesnelerin interneti uygulamalarının sağladığı avantajların yanı sıra elbette dezavantajları ve tartışılması gereken küresel ölçekli sorunları mevcuttur. Nesnelerin interneti uygulamalarında tartışılması gereken önemli konular şüphesiz gizlilik, güvenlik, mahremiyet ve gözetim konularıdır. Nesnelerin interneti tabanlı uygulamalarda kullanılan teknolojiler aracılığıyla çok büyük miktarda veri toplanmakta ve bu veriler çeşitli işlemlerden geçerek yeniden düzenlenmektedir. Özellikle her yerde bulunan sensörler veri gözetiminin gerçekleşmesinde büyük bir rol oynamaktadır. Dolayısıyla nesnelerin interneti platformunun hem özellikleri ve teknolojileri hem de her yerde bulunma ve her şeyi bağlantılı kılma paradigması büyük veri gözetiminin gerçekleşmesini mümkün hale getirmektedir.

Nesnelerin interneti platformunun fiziksel mekâna yayılması ve coğrafi alanların derinliklerine doğru gittikçe genişlemesi bu kavramın yeniden tanımlanmasına yol açmaktadır. Kişinin en özel sayılabilecek ortamlarından biri olan evi, bedeni veya toplumlar için kentler ve sokaklar artık akıllı olarak nitelendirilen bir kisveye bürünerek sensörler ve aktüatörler ile izlenebilen bir ortama dönüşmüştür (Ahn, 2021). Kevin Ashton bilgisayarların şeyler hakkında bilinebilecek her şeyi bilme ihtimalinin yaratacağı faydayı vurgulayarak her şeyin takip edilebilir olmasının israf ve maliyetleri azaltacağı yönünde olumlu bir gelecek hayal etmiştir. Ahn (2021), ise Ashton'ın nesnelerin interneti ile ilgili bu düşüncesinde veri toplama her ne kadar insan dışı uygulamaları işaret ediyorsa bile bu konunun insan mantığıyla doğrudan ilişkili olduğu noktasında önemli bir sorunun bir kenara bırakıldığını ve basitçe kullanılan “her şey” ifadesinin her şeyi izleme ihtiyacına karşılık geldiğini ifade etmektedir.

Fiziksel mekânın her alanına yayılan bağlanabilir teknolojiler aracılığıyla birçok alan verileştirilmekte ve çeşitli amaçlar için kullanılmaktadır. Verileştirmenin muazzam gücünü keşfeden aktörler, sürekli olarak deneyler yapmakta ve kullanıcıları adeta birer deneme tahtası olarak kullanmaktadır. Bu bağlamda, sigorta şirketlerinin ekonomik değer anlayışlarını geliştirme sürecinde verileştirme keşfi oldukça anlamlıdır. Sigorta şirketleri, ekonomik deneyler yürüterek potansiyel

müşterileri onların davranışsal tepkilerini ölçerek belirleyebilmektedir. Ayrıca, sadece potansiyel müşterilerin belirlenmesi açısından değil, ürün özelliklerinin test edilmesi ve ürünler hakkında sürekli taze bilgi üretilmesi açısından da önemli bir imkân sunmaktadır. Örneğin, otomobil sigortacıları, potansiyel kaza yapma riski taşıyan sürücülerini belirlemek amacıyla araç motoruna takılan sensör ve cihazları ya da daha düşük maliyetli olması açısından akıllı telefonlar aracılığıyla hız ve GPS takibini kullanmaktadır. Bu teknolojiler, hem davranışa dayalı kişiselleştirmeye hem de “davranışsal manipülasyona” hizmet etmektedir (Meyers & Hoyweghen, 2020).

Nesnelerin İnterneti paradigmasının her şeyi bağlanabilir kılma hedefi doğrultusunda veri gözetiminin gerçekleştiği örnekler ele alındığında, yukarıda bahsi geçen sigorta şirketlerinin verileştirme aracılığıyla yürüttüğü ekonomik deneyler yalnızca küçük bir örnek teşkil etmektedir. Ancak bu ekosistem içinde gerçekleştirilen veri gözetimi örnekleri çok boyutlu ve karmaşıktır. Bu nedenle mevcut örnekleri sınıflandırarak aktarmak, çok daha makul ve sistematik bir incelemeye olanak tanımaktadır. Bu bağlamda, nesnelerin interneti dünyasında önemli ve geniş ölçüde yer tutan akıllı şehirler, akıllı evler, giyilebilir teknolojiler ve konum tabanlı teknolojiler aracılığıyla gerçekleştirilen veri gözetimi örneklerine, bunların odak noktalarına ve literatürdeki mevcut gözetim pratiklerine değinilmesi gerekli görülmüştür.

3.2.1. Akıllı Şehirlerde Veri Gözetimi

Kentsel veriler hem kapsam hem de ayrıntı bakımından tipik küçük verilerden farklı bir konumda yer almaktadır. Örneğin, toplu ulaşım turnikelerinden geçen kartların sayıları, araç plaka tanıma kameraları ve yayaların sensörlerle kolayca izlenmesi gibi uygulamalar bu veriler arasında yer almaktadır. Veri odaklı kentleşme, otomatik olarak veri gözetimine zemin hazırlamakta ve özellikle akıllı şehirler bağlamında coğrafi gözetimin yoğunlaşmasına yol açmaktadır. Coğrafi gözetim ise kişilerin, nesnelerin ve tüm hareketliliğin izlenmesine olanak tanıdığı gibi aktörler arasındaki etkileşimlerin de gözlenmesini mümkün kılmaktadır. Akıllı şehirler bir yaşam laboratuvarı olarak inşa edilmekte ve geleneksel şehirlerden farklı olarak daha öngörülebilir, kontrol edilebilir ve yönlendirilebilir bir yaşam akışını amaçlamaktadır. (Fabrègue & Bogoni, 2023). Akıllı şehirlerde veri gözetimi örneklerini incelerken Google’ın şehirler üzerinde aktif bir şekilde rol oynamasına değinmek yerinde olacaktır.

Dünyada en çok kullanılan arama motoru misyonuna sahip olan Google, zihinlerde daha çok arama faaliyetlerinin baş aktörü olarak yer alsa da üst çatısı Alphabet olan şirketin farklı projelere imza atan birçok alt kuruluşu yer almaktadır. Bu şirketler Google’ın arama motoru kalitesinin iyileştirilmesi amacıyla farklı olarak fiziksel ve gerçek zamanlı uygulamaları içinde barındıran projelere imza atmaktadır. Bu projeler şehirlerde yaşanan olası sorunlara yönelik tasarlanan akıllı şehir ve evlerdeki

konforun sağlanması üzerine tasarlanan akıllı ev teknolojileri, otonom araçların düzenine yönelik geliştirilen çalışmalar, nesnelerin interneti ile uyumlu çalışabilen dijital asistan ve sağlık-spor ilişkisi üzerine tasarlanan projeleri içermektedir.

Google'ın gerçekleştirdiği şehir merkezli projeler arasında akıllı trafik uygulamaları, internet erişim noktaları, akıllı sürdürülebilir şehirlerin inşası ve daha birçok fiziksel gerçek zamanlı uygulamalar yer almaktadır. Şehir içerisinde birbirine bağlanılabilir nesneler ve bağlantılı nesneler ile Google uygulamaları arasında da kurulan bağlantı ilişkisi Google'ın birçok noktada gerçek zamanlı veri hakimiyeti kurmasına yol açmaktadır.

2015 yılında çatısı Alphabet holding şirketi olarak yeniden organize edilen Google, kısa bir süre sonra alt şirketlerinden biri olan Sidewalk labs'ı kurmuştur. Sidewalk Labs, Google'ın şehir üzerine tasarlanan çözümleyici projelerinin daha iyi işleyebilmesi için kurulmuş ve Google City adına önemli bir varlık haline gelmiştir. Nitekim şirketin ilk taahhütlerinden biri New York City'de “dijital eşitsizlik” sorunuyla savaşmak adına herkesin ücretsiz internet erişim sağlayabileceği dokunmatik ekranların kurulması olmuştur. Ancak Google'ın internete herkesin erişme hakkının olmasına yönelik bu girişiminin altında yatan ve göz ardı edilen önemli bir sorun bulunmaktadır. Kullanıma sunulan dokunmatik ekranlar kullanıcılar hakkında verilerin toplanmasına yol açıyorken ekranları kullanmayanlar için dahi Wİ-Fİ ağı aracılığıyla çeşitli kişisel veriler toplanmakta ve bu eylem adeta “veri çeşmeleri” olarak adlandırılmaktadır (Zuboff, 2021, s.283).

Google'ın Sidewalk Labs önderliğinde 2017 yılında geliştirmek istediği ancak çeşitli nedenlerle 2020 yılında iptal edilen bir başka projesi de Toronto'da Quayside adlı akıllı bir kasaba kurma çabası olmuştur. Yüksek teknoloji tabanlı tasarlanan bu projede şehirlerde görülen birçok problemin olmadığı ve seçilen bölgenin her noktasına yerleştirilmiş teknoloji aracılığıyla günlük hayatta çeşitli altyapı, trafik sorunları, kirli hava vb. karşılaştığımız kaos görüntüsünden arındırılmış kusursuz bir şehir hayal edilmiştir. Oldukça heyecanlandırıran ve masumane görünen bu projede birtakım mahremiyet ihlali gerçeklerinin açığa çıkması bu projeye karşı bakış açılarının olumsuz yönde değişmesine yol açmıştır. Hem projede yer alan uzmanların eleştirileri hem de kamusal bir ayaklanmanın çıkması ise bu projeye olan negatif bakışların birer göstergesi olmuştur. Nitekim verilere dayalı olan şehir hizmetlerinin işleyişinde mahremiyetin korunmasına yönelik projenin başında işe alınan gizlilik uzmanı Ann Cavoukian CBC'ye verdiği röportajda yaptığı açıklamalarla mahremiyet ihlallerinin üzücü gerçeklerini açığa çıkarmıştır.

Ontario eski gizlilik komiseri olan Cavoukian, Toronto'da kurulmak istenen akıllı bölge projesinde mahremiyetin sağlanmasına yönelik çalışmalar yürütmüştür. Şehrin tüm noktalarında

bulunacak sensörler, kameralar ve bağlantılı birçok cihazın her zaman aktif olacağı planlanan bu tasarımda ise her türlü verinin vakumlanması kaçınılmaz olacaktır. Bu minvalde toplanan veriler yalnızca nesnelerden değil aynı zamanda kişilerden ve kişilerin tüm hareketliliklerinden elde edilmektedir. Gizlilik uzmanının mahremiyetin her şeye dahil edilmesi gerektiği ve en önemlisi veriler toplanırken kimlik gizlemenin (anonimleştirmenin) önemli bir gereklilik olduğuna dair hedefi başta Google tarafından kabul edilebilir olsa da projenin yürütücülüğünü üstlenen diğer kurumlar ve şirketler bunun kabul edilemez olduğunu öne sürmüş ve bunun üzerine Google'ın herhangi bir şey yapamayacağını belirtmesi sonucu gizlilik uzmanı projeden istifa ederek geri çekilmiştir. Gizlilik uzmanının “burada akıllı şehir inşa edilmiyor gözetimin akıllı şehri inşa ediliyor” vurgusu ise projeye karşı olumsuz bakış açısını çok net bir şekilde ortaya koymaktadır (CBC, 2020).

Akıllı şehirlerin daima ekolojik dengeyi sağlayabileceği ve sürdürülebilir olacağı yönündeki vaatlere eleştirel bir bakış açısıyla yaklaşmakta fayda vardır. Bu şehirlerin gerekli sistemleri karşılayabilmesi için çok büyük miktarda enerji tüketmesi gerekmektedir. Aynı zamanda, bu teknolojilerin üretimi yoğun endüstriyel faaliyetler gerektirdiğinden, doğrudan çevresel tahribata yol açmaktadır. Bununla birlikte, akıllı şehirler üzerine geliştirilen çözümler mevcut şehir sistemlerini olumsuz yönde etkileyebilmekte ve akıllı şehir sakinlerine ekolojik bir yaşam sunulurken, aynı kentin diğer sakinleri daha fazla olumsuz sonuçlara katlanmak zorunda kalmaktadır. Ayrıca, akıllı şehirlerin gerçek ekolojik maliyeti küresel ölçekte değerlendirildiğinde, sunduğu faydaya kıyasla çok daha yüksek olduğu görülmektedir (Pitron, 2023). Bu durum, akıllı şehirlerin yalnızca ekolojik bir yaşam kurma amacını taşımadığını; aksine, sürdürülebilirlik sağlanamadığında bu yapıların zamanla birer atık kente dönüştüğünü göstermektedir. Dolayısıyla, akıllı şehirlerin ekolojik olmaktan çok, ekonomik ve gözetim odaklı yapılar olduğu söylenebilir.

3.2.2. Akıllı Ev Ürünlerinde Veri Gözetimi

Günümüzde giderek yaygınlaşan akıllı evler (smart home), bünyelerinde bulunan teknolojik aygıtlar sayesinde ev sakinlerine daha konforlu bir yaşam sunmaktadır. Akıllı termostatlar, temizlik robotları, mutfak gereçleri, mobilyalar ve diğer birçok nesneyi içeren bu evler, hayatı kolaylaştıran ve yaşam standartlarını yükselten çözümler sunmaktadır. Ev içinde kullanılan cihazların sunduğu bu çözüm odaklı yaklaşımlar, büyük ölçüde veri analizi döngüsünün işleyişine dayanmaktadır. Hizmet odaklı stratejik gelişimlerde verilerin kullanılması ve bu sayede kalitenin artırılması, kullanıcıya çeşitli avantajlar sağlamaktadır. Ancak bu bölümün odak noktası, bu süreçte mahremiyet ihlallerinin yaşanması ve teknolojiyi elinde bulunduranların bu uygulamaları kapitalist bir yaklaşımla gerçekleştirmesidir.

Akıllı ev ürünlerinde veri gözetimini mümkün kılan çeşitli teknolojiler bulunmaktadır. Bu teknolojiler, kullanıcıların kontrol ve kolaylık gibi iki temel unsura erişimini sağlayarak, teknoloji sahiplerinin veri gözetimini meşru bir çerçeveye oturtmasına olanak tanımaktadır. Nitekim kullanıcılar adına kontrol ve kolaylığın sağlanması için gözetim vazgeçilemez bir gereklilik olarak addedilmiştir. Bu alanda başarılı bir örnek, şüphesiz Google Nest teknolojisidir. Nest, ev içi güvenlik sistemleri, sıcaklık kontrolü ve ışık ayarlarının otomatik olarak yönetilmesini sağlayan bir akıllı ev teknolojisi sunmaktadır. Bu süreç, çeşitli sensörler, kameralar ve diğer ileri teknolojilerin entegrasyonu sayesinde gerçekleştirilmektedir (White & Gilmore, 2022).

Londra Üniversitesi araştırmacıları, Nest teknolojilerinin sözleşmelerini hukuki açıdan incelediklerinde, bu sözleşmelerin kişilerin anlayabileceği makul bir dilden yoksun olduğunu ve verilerin yaklaşık bin kez üçüncü taraflarla paylaşıldığını ortaya koymuştur. Ayrıca, bu durumun Nest kullanıcılarının sözleşmeleri detaylı bir şekilde okumadıkları gerçeğiyle örtüştüğü tespit edilmiştir. Sonuç olarak, Nest teknolojilerinin hukuki ve etik standartlara uygun olmadığı ve yeterli şeffaflık sağlamadığı ifade edilmiştir (La Diega & Walden, 2016).

Kişinin belki de en mahrem sayılabileceği alanlardan biri olan evinin yatak odasında yer alan bir akıllı yatak teknolojisini örnek vermek yerinde olacaktır. Birçok moda uyarlanabilen Sleep Number akıllı yatak teknolojisi, kullanıcıların uyku kalitelerini gözetleyebildiği gibi ortam içerisindeki hava koşulları hakkında da bilgi sahibi olabilmektedir. Bununla beraber bağlanılabilir olma özelliği sayesinde hem evde bulunan herhangi bir akıllı cihaza hem de bir uygulamaya kolaylıkla bağlanabilmektedir. Sleep Number akıllı yatak teknolojisinin sözleşmesi dikkate alındığında ise kullanıcı verilerinden açıkça faydalanabileceği ve ürün kullanıcı profilinin iptal edilmesi durumunda dahi kişisel bilgilerin paylaşılacağına dair önemli bilgiler yer almaktadır (Zuboff, 2021, s. 293).

Günümüzde kullanımı hızla artan akıllı ev ürünlerinden biri de robot süpürgelerdir. Robot süpürgeler, evin içinde bir harita oluşturarak buna uygun şekilde hareket etmektedir. Ancak bu süpürgelerin potansiyel birer gözetim aracı olabileceğine dair çeşitli eleştiriler bulunmaktadır. Yakın geçmişte yayımlanan bir makalede, dünyaca ünlü şirket iRobot'un Roomba robot süpürgelerinin evde bulunan kişilere ait uygunsuz görüntüleri internete sızdırdığı ve bu görüntüleri üçüncü taraflarla paylaştığı belirtilmiştir. Esasında test aşamasında, gönüllü kullanıcıların katıldığı bir projede yaşanan bu skandalda, görüntülerin kaydedilmesi ve paylaşılmasına dair katılımcıların yeterince bilgilendirilmediği anlaşılmıştır (Guo, 2023). Bu durum, özellikle kameralı robot süpürgelerin ev içi yaşamı sürekli olarak izleyebildiğini ve aktif biçimde veri toplayabildiğini göstermektedir. Bir test aşamasında böyle bir mahremiyet ihlalinin yaşanması, gelecekte daha büyük sorunların ortaya çıkabileceği yönünde kaygılar doğurmaktadır.

Akıllı ev ürünleri, veri gözetimi için tek başına başarılı olsa da bir başka uygulama ile birleştğinde çok daha fazla veri hazinesine ulaşılabilir. Bu cihazların, farklı uygulamalarla entegrasyonu verilerin izlenmesi ve analiz edilmesi açısından önemli sonuçlar doğurur. Bunun en dikkat çekici örneklerinden biri, dijital asistanlar ile nesnelerin interneti cihazları arasındaki uyumlu birleşmedir. Örneğin, Google'ın kişisel asistanını Google Home ile entegre olarak kullanmayı önermesi buna iyi bir örnektir. Kullanıcıların sesli komutlarla ev içerisindeki akıllı cihazları kontrol edebilmesi, kullanıcı deneyimini kolaylaştırmanın yanı sıra, daha büyük bir veri kaynağı oluşturarak gözetim süreçlerini güçlendirmektedir. Bu durum yalnızca Google ile sınırlı değildir. Benzer şekilde, Amazon'un Alexa'sı, Apple'ın Siri'si ve daha sonra geliştirilen Viv ses sistemi gibi dijital asistanlar da bu entegrasyonu başarıyla gerçekleştiren örnekler arasında yer almaktadır (Zuboff, 2021, s. 334). Bu bağlamda Amazon'un akıllı kapı zili olan Ring de aynı örnek içerisinde değerlendirilebilir. Ring, Amazon'un akıllı kişisel asistanı Alexa ile kolayca entegre edilebilmektedir. Dolayısıyla her akıllı ürün bir diğerine bağlanarak yayılmacı bir politika benimsemektedir. Bu bağlamda akıllılığın giderek bağlanılabilir ve yayılabilir özelliği bir enfeksiyon olarak nitelendirilmektedir: “Böylece hem Ring hem de Alexa, birer enfeksiyon vektörüne dönüştü; her biri belirli bir noktada yayılmak ve diğer enfekte noktalarla birleşmek üzere konumlandırılmıştır” (Wood & Steeves, 2021, s. 150).

Akıllı evler ve evlere yerleştirilen akıllı ürünlerin gözetimini sağlayan başlıca aktörler, Google ve Amazon gibi büyük teknoloji şirketleri olsa da bu durum yalnızca bu şirketlerle sınırlı değildir. Bu büyük şirketlerin evler özelinde yürüttüğü stratejiler, üçüncü tarafların da evlere dâhil olmasını sağlamaktadır. Bunun en çarpıcı örneklerinden biri ise finans, emlak ve sigorta firmalarının büyük teknoloji şirketlerine eşlik etmesidir (Maalsen & Sadowski, 2019).

Sigorta firmaları, akıllı evlere dâhil olarak ev sahiplerinin ev içindeki gündelik pratiklerini izleyip veri gözetimi gerçekleştirmektedir. Bir tür ödüllendirme stratejisi kullanarak kullanıcılara cazip teklifler sunmaktadırlar. Bu bağlamda, büyük teknoloji şirketleriyle yaptıkları iş birlikleri dikkate değerdir. Örneğin, Liberty Mutual şirketi, kullanıcıların sahip oldukları cihazları izlemelerine izin vermeleri hâlinde Nest Protect duman dedektörünü ücretsiz olarak kullanma vaadinde bulunmaktadır. Öte yandan, yalnızca iş birliğiyle sınırlı kalmayan bazı sigorta şirketleri, daha kolay veri toplayabilecekleri kendi akıllı cihazlarını üretmeye yönelik yatırımlar da yapmaktadır. Bu duruma Progressive'in “Snapshot” ve Admiral'ın “Black Box” gibi araç içi sistemleri örnek olarak verilebilir. Sigorta firmaları dışında emlak sektörü de akıllı teknolojiler konusunda hayli iştahlı bir tutuma sahiptir. Bir tür derecelendirme sistemine sahip olan Rentberry kiralama platformu kiracıların geçmiş ödeme bilgileri ile ilgili verileri toplayarak bir puanlama gerçekleştirmektedir. Böylelikle daha kusursuz ve iyi

kiracıların ortaya çıkmasına zemin hazırlamaktadır. Sonuç olarak daha güvenilir ve kontrol edilebilir bir insan profili oluşturulmaktadır (Maalsen & Sadowski, 2019).

3.2.3. Giyilebilir Teknolojilerde ve Konum Tabanlı Teknolojilerde Veri Gözetimi

Giyilebilir teknolojiler ve konum tabanlı teknolojiler ortak bir ekosistemi paylaşarak birbirini tamamlayan teknolojiler olarak gün yüzüne çıkmaktadır. Bundan dolayıdır ki bu iki önemli teknolojiyi aynı çatı altında toplamak ve veri gözetimi ekosistemi açısından birer paydaş olarak değerlendirmek önemlidir.

Gözetim kapitalizmi ekosisteminde şüphesiz ki insan bedenleri önemli bir aktör olarak belirmiştir. Her zaman her yerde veri toplama paradigması daha da derinleşerek insan bedenine doğru bir yol almış ve bedenin duygu durumundan ve tüm hareketliliğinden beslenmiştir. Zuboff (2021) bu durumu “Bedenin icrası” (the rendition of the body) olarak kavramsallaştırmıştır. Her zamankinden daha fazla sensörlerle donatılan ve algoritmalarla çevrelenmiş hareketli bir alan bedenin her ayrıntısına odaklanarak biyometrik gözetimin gerçekleşmesine zemin hazırlamaktadır. Bu hassas gözetim teknikleriyle bedenin duygularına ve ruh haline çok kolay bir şekilde erişilebilmekte ve analiz edilmektedir. Giyilebilir cihazlar-konum tabanlı teknolojiler ile beden ilişkisini ele alırken bahsi geçen biyometrik gözetim konusuna da temas etmek bağlamın daha iyi anlaşılmasına olanak tanımaktadır.

Biyometrik veri, kişilerin fiziksel özellikleri ve davranışsal özelliklerini içinde barındıran kişilere özel benzersiz verileri içermektedir. European Parliament and Council (2016), biyometrik veriyi “bir gerçek kişinin fiziksel, fizyolojik veya davranışsal özelliklerine ilişkin olarak belirli teknik işlemler sonucunda elde edilen ve söz konusu gerçek kişinin benzersiz bir şekilde tanımlanmasına olanak tanıyan veya bunu doğrulayan yüz görüntüleri veya daktiloskopik veriler” olarak tanımlamaktadır. s.34

Biyometrik veriler üzerinden duygu algılama ise aslında çok da yeni var olan bir çalışma alanı değildir. 1990'lardan bu yana duygu algılama çalışmaları yapılmaktadır ve “duygusal bilişim” çatısı altında yer almaktadır (Picard, 2000). Kişinin duygusal yaşamını görmek, anlamak veya dinlemenin çeşitli makine öğrenmesi teknikleriyle mümkün olduğunu öne süren Andrew McStay (2020), bu durumu “duygusal yapay zekâ” olarak adlandırmıştır. Duygusal yapay zekâ vücut içerisinde gerçekleşen her türlü olayın verisini kaydetmekte ve analiz edebilmektedir. Bu veriler “kalp atış hızı, vücut sıcaklığı, solunumu ve cildin elektriksel özelliklerini kapsayan kelimeler, görüntüler, yüz ifadeleri, bakış yönü, jestler, sesler ve daha birçok biyolojik geri bildirim” öğelerini içermektedir (McStay, 2020, s. 2). Toplanan kapsamlı veriler, kişisel özelliklerin belirlenmesi ve yapay zekâ algoritmalarının da etkili rolüyle adeta bir dijital fenotipleme gerçekleştirilmekte ve gerek davranışsal bilimler alanında gerekse pazarlama alanında etkili bir şekilde kullanılmaktadır.

Kişilere ait fizyolojik veya duygusal veriler, çeşitli amaçlarla toplanmaktadır. Bu amaçlar arasında cihaz-kullanıcı etkileşim oranını artırma, davranışların optimizasyonu ve risk değerlendirmeleri yer almaktadır. Özellikle sigorta şirketleri, müşterilerden elde edilen tepkisellik verileri sayesinde önemli iyileştirmeler gerçekleştirebilmektedir. Ayrıca, bu tür verilerin toplanması, pazarlamacıların hedefli reklamcılık faaliyetlerini kolaylaştırmaktadır (McStay, 2020).

Yaygın teknolojiler, genelden özele doğru bir ilerleme göstererek önce şehirlere, ardından evlerimize ve nihayetinde bedenlerimize entegre edilmektedir. Bu sürecin en etkili araçlarından biri ise giyilebilir teknolojiler ve biyoteknolojilerdir. Giyilebilir teknolojilerin özellikle sağlık uygulamaları içerisindeki kullanımı oldukça yaygındır. Bu bağlamda, giyilebilir teknolojiler, bireylerin fiziksel aktivitelerini, uyku düzenlerini ve sağlık durumlarını sürekli izleyerek kişiselleştirilmiş sağlık çözümleri sunmaktadır. Örneğin, akıllı saatler ve fitness takip cihazları, kalp atış hızı, kan, oksijen seviyesi ve adım sayısı gibi verileri ölçerken, tıbbi sensörler hastalıkların erken teşhisinde kullanılabilmektedir. Biyoteknoloji ise genetik analizden implant teknolojilerine kadar geniş bir alanda yenilikler sunarak, bedenin dijitalleşme sürecine katkı sağlamaktadır. Giyilebilir teknolojilerin arka planda yer alan en önemli özelliği ise bedenlerin sayısallaştırılarak hesaplanabilir hale getirilmesidir.

Giyilebilir teknolojiler, sağlık ve spor uygulamalarında oldukça etkin bir rol oynamaktadır. Özellikle akıllı saatler ve fitness takip cihazları, bir önceki paragrafta belirtildiği gibi, bireylerin biyolojik verilerini kaydetme işlevi görmektedir. Bu cihazlar yalnızca fiziksel aktiviteleri izlemekle kalmayıp aynı zamanda zihinsel sağlık durumlarını analiz ederek bu bilgileri veri haline getirebilmektedir. Bu cihazlar, parmak izi ve yüz tanıma gibi hassas biyometrik verileri tanımlama yetenekleriyle daha da geliştirilmiştir. Bu gelişmeler, cihazların kullanımını artırırken aynı zamanda toplanan verilerin bir araya getirilip analiz edilmesine olanak tanır. Bu süreç sonucunda, kullanıcıların davranış ve tercihlerine dayalı ayrıntılı bir tüketici profili oluşturulmaktadır (Sifaoui & Eastin, 2024).

Giyilebilir akıllı cihazların, özellikle sağlık amaçlı kullanımda ticari bir boyut kazanması, yeni eleştirilerin ortaya çıkmasına neden olmaktadır. Bu cihazların tıbbi amaçlardan ziyade tüketim odaklı kullanıma sunulması, güvenilirlik konusunda çeşitli zorluklara yol açmaktadır. Bu bağlamda, Amerikan Tabipler Birliği (AMA) ve FDA, sağlık profesyonellerini ve tüketicileri yalnızca bu cihazlardan elde edilen verilere dayanarak tanı koymamaları konusunda uyarılmaktadır. Örneğin, FDA (Food and Drug Administration), akıllı saatler ve yüzüklerin geleneksel tıbbi cihazlar kadar hassas ve doğru sonuçlar vermeyebileceğini belirterek bu cihazların kan şekeri ölçümü gibi amaçlarla kullanılmasına karşı dikkatli olunması gerektiğini ifade etmektedir (Evenson vd., 2015).

Zuboff (2021), bedeninin icrasının çok kolay bir şekilde önce akıllı telefonlarla başladığını öne sürmektedir. Nihayetinde cep telefonları sürekli olarak kişilere eşlik eden ve bir noktada bedenin bir parçası olarak yaşamlarımıza katılan cihazlardır. Bu minvalde bulunduğumuz şehirler veya evler akıllı olmasa bile ve hatta söz konusu büyük teknoloji şirketleri tarafından ele geçirilmemiş olsa bile davranışsal veriler üzerinde işlem yapmaya hazır olan birçok aktör bulunmaktadır. Birbiriyle iç içe geçen ve giyilebilir cihazlar gibi bedenin hareketliliğinden faydalanan konum tabanlı gözetim için de bu durum geçerlidir. Konum verilerinin birincil olarak toplandığı cihazlar akıllı telefonlardır. Örneğin telefonda yer alan GPS uygulamalarının yanı sıra birçok mobil uygulama konum verilerine erişim izni istemektedir. Bu erişim izni kabul edilmediği takdirde ise kullanıcı tarafından uygulamaya ya hiç erişim sağlanamamakta ya da kısıtlı erişim sağlanmaktadır.

Konum tabanlı gözetim, tıpkı giyilebilir cihazlar gibi birçok farklı amaç için kullanılmaktadır. Bu amaçlardan biri, aynı zamanda bu çalışmanın temel odak noktalarından birini oluşturan konum tabanlı pazarlama faaliyetleridir. Markalar, müşterilerden elde ettikleri konum verilerini kullanarak, doğru kişiye doğru zamanda ve doğru yerde reklam hedeflemesi yapmakta ve stratejik avantajlar elde etmektedir. Üstelik markaların bunu gerçekleştirebilmesi için tüketicilerin yalnızca konum tabanlı uygulamaları kullanması gerekmez; kullanıcıların konum verisine erişim izni olan herhangi bir uygulamayı kullanması yeterlidir. Bu bağlamda, birçok kullanıcının konum erişim izinlerine dair sözleşmeleri okumaması yaygın bir davranış olduğundan, bu durum genellikle gözden kaçırılan bir meseledir (Tokgöz, 2018).

Konum tabanlı pazarlamanın başarısı, kullanıcıya anlık bildirimler gönderebilmesi, QR kodların kullanımı, içerik yönetim sistemleri, yüksek performanslı coğrafi eşleme motorları gibi çeşitli özelliklere dayanmaktadır. Ayrıca, satış noktası verilerini bireysel veya toplu olarak düzenleme, üçüncü parti haritalama araçlarını destekleme, alışveriş planlama imkanı sunma, hem cihazlardan hem de şebekelerden alınan konum bilgilerini kullanabilme yeteneği ve yalnızca mobil uygulamalar üzerinden değil, tüm mobil tarayıcılar aracılığıyla erişim sağlama gibi özellikler, bu pazarlama stratejisini daha etkili hale getirmektedir (Dilmen, 2020).

Kullanıcıların konum verilerine ne sıklıkla erişildiğini inceleyen birçok araştırma yapılmıştır ve bu araştırmalarda Google'ın önemli bir rol oynadığı açıkça görülmektedir. Özellikle Android tabanlı cihazlardan toplanan konum verileri, Google'ın herhangi bir hizmeti etkinleştirildiğinde otomatik olarak kullanılan bu hizmetlerden elde edilmektedir. Bu durum, Android tabanlı bir mobil cihaz kullanmanın bile veri gözetimine kapı araladığı anlamına gelmektedir. Ayrıca, yalnızca Android değil, iOS da nokta atışı konum belirleme yeteneğine sahiptir. Her iki işletim sistemi de konum verilerini GPS, yerel Wi-Fi ağları ve diğer kaynaklarla birleştirerek, kullanıcıların genellikle yüksek doğrulukla hedeflenmesini

mümkün kılmaktadır. Ancak, konum verilerinin toplanması ve kullanılması konusunda Apple ve Google arasında dikkate değer farklılıklar bulunmaktadır. Apple, kullanıcıların açık rıza vermediği durumlarda konum verilerini anonim bir şekilde toplama politikasını benimsemektedir (Brandom, 2016).

2017 yılında *Quartz* tarafından yayımlanan bir haber makalesinde, “Google, konum servisleri kapalı olsa bile Android kullanıcılarının konumlarını topluyor” şeklinde dikkat çekici bir başlık yer almıştır. Makalede, Android kullanıcılarının konum servislerini etkinleştirmemeleri veya telefonlarında SIM kart bulunmaması durumunda bile, baz istasyonları aracılığıyla hücresel veri veya Wİ-Fİ ağına bağlandıklarında toplanan verilerin Google'a gönderildiği belirtilmektedir. Google'ın bu uygulaması, özellikle konum hizmetlerini kapatmayı tercih eden askeri personel veya şiddet mağduru kişiler gibi, izlenmeyi istemeyen bireyler için bir sorun teşkil ettiği yönünde eleştirilmektedir. “Google'a gönderilen veriler şifrelenmiş olsa da telefon casus yazılım veya diğer bilgisayar korsanlığı yöntemleriyle tehlikeye atılmışsa, potansiyel olarak üçüncü bir tarafa gönderilebilir. Her telefonun konum verilerinin ilişkilendirilebileceği benzersiz bir kimlik numarası vardır.” Öte yandan Google, topladığı konum verilerini üçüncü taraflarla paylaşmadığını belirtse de reklamcıların bu verileri kullanarak tüketicileri hedeflemesine olanak tanımaktadır. Bu yaklaşımın, açıkça ticari bir değeri olduğu görülmektedir (Collins, 2017).

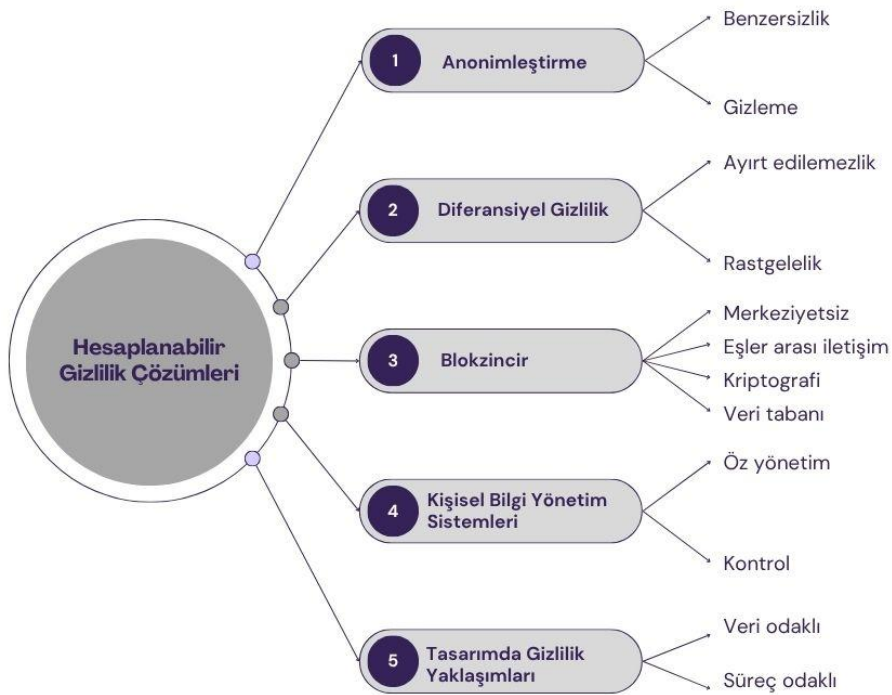
Carnegie Mellon Üniversitesi tarafından yapılan bir diğer çalışma, uygulamaların kullanıcıların konum verilerine erişimini incelemektedir. Bu çalışmada, toplamda 23 katılımcının konum bilgilerine erişim sağlayan uygulamalar detaylı bir şekilde analiz edilmiştir. Çalışma, reklam verenler, sigorta şirketleri, perakendeciler, pazarlamacılar ve konut kredi kuruluşları gibi çeşitli aktörlerin, sırasıyla 4.182, 5.398 ve 356 kez gibi şaşırtıcı sıklıklarla kullanıcıların konum verilerine eriştiğini ortaya koymuştur. Esasında bir farkındalık çalışması olan bu araştırmanın sonucunda, katılımcıların veri paylaşımı konusundaki farkındalıklarının belirgin şekilde arttığı gözlemlenmiştir (Almuhimedi vd., 2015).

Akıllı şehirler, akıllı evler, giyilebilir teknolojiler ve konum tabanlı teknolojiler, nesnelerin interneti uygulama alanları içerisinde yaygın bir şekilde kullanılmaktadır. Bu teknolojiler aracılığıyla veri gözetimi, fiziksel mekânın daha fazla alanına yayılmış ve dijital gözetim aktörlerinin kapitalist düzende sahip oldukları konumu daha da güçlendirmiştir. Artık daha öngörülebilir ve kontrol edilebilir kullanıcı profilleri ortaya çıkmaktadır. Bu bağlamda, mahremiyet ihlali olarak değerlendirilebilecek bu eylemlere karşı geliştirilen güvenlik önlemleri ve gizlilik çözümleri incelenmeye değerdir. Bir sonraki başlıkta, hesaplanabilir yaşam akışı temelinde en çok kullanılan hesaplanabilir gizlilik çözümleri ele alınacaktır.

3.3. Hesaplanabilir Gizlilik Çözümleri

Gizliliğin hesaplanması, gizlilik kavramının yalnızca teknik bir çatı altında ele alınması anlamına gelmemektedir. Nitekim, gizlilik meselesi teknik bir konu olmanın ötesine geçerek sosyo-kültürel bir boyut kazanmıştır. Bu nedenle, teknolojinin sürekli değişen dinamikleri, gizlilik kavramının konumunu da sürekli olarak değiştirmekte ve hatta belirsizleştirmektedir. Sonuç olarak, gizliliğin matematiksel olarak korunması mümkün görünse de toplumsal olarak nasıl korunması gerektiği hâlâ tartışılmaktadır (Munn vd., 2019).

Kişisel veri mahremiyetinin sağlanması adına hem teknolojik hem de hukuki çözümler geliştirilmektedir. Teknik çözümler arasında, anonimleştirme, diferansiyel gizlilik, blokzincir tabanlı güvenlik sağlayıcılar, kişisel bilgi yönetim sistemleri (PIMS) veya kişisel veri depoları (PDS), tasarım yoluyla gizlilik yaklaşımları ve kullanıcı ara yüzlerinin gizlilik kontrolünü sağlayacak şekilde tasarlanması gibi önemli girişimler yer almaktadır. Bu başlık altında, geliştirilen teknolojilerin özellikle nesnelerin interneti bağlamındaki konumu değerlendirilecektir. Bu çerçevede, bu teknolojilerin başarılarına ve sınırlarına değinilecektir.



Şekil 2. Hesaplanabilir Gizlilik Çözümleri

3.3.1. Anonimleştirme

Veri güvenliği ve kullanıcı mahremiyetinin sağlanması için alınan önemli önlemler arasında anonimleştirme teknikleri yer almaktadır. Anonimleştirme, bireyleri tanımlayan verilerin silinmesi veya değiştirilmesi yoluyla, bireylerin doğrudan tanımlanmasını önlemeyi amaçlar. Anonimleştirme sürecinde çeşitli yöntemler kullanılarak kişisel verilerin kimlikle ilişkilendirilemez hâle getirilmesi amaçlanır. Bu bağlamda, verilerin daha geniş kategoriler altında gruplanması, belirli bilgilerin sembollerle gizlenerek görünmez kılınması, hassas içeriklerin ayrı veri tablolarına dağıtılması, veri sıralarının değiştirilerek orijinal yapıdan uzaklaştırılması ve mevcut verilere belli oranda rastlantısal değişiklikler eklenerek orijinalliğin bozulması gibi yöntemler öne çıkar. Bu tür uygulamalar, bireylerin tanınmasını engellemek ve mahremiyetin korunmasını sağlamak açısından önemli araçlar olarak değerlendirilmektedir. (Gümüş & Eyüpoğlu, 2022).

Bir veri koruma yöntemi olarak anonimleştirme, görünürde güçlü bir yöntem olarak değerlendirilmektedir. Ancak, anonimleştirmenin genel karakteri göz önüne alındığında bazı özellikleri suistimal edilebilir ve bu durum koruma kapasitesini zayıflatır. Sonuç olarak, veri koruma amacıyla anonimleştirme tekniklerine başvurulmasının güvenilirliği konusunda şüpheler oluşması kaçınılmazdır.

Anonimleştirilmiş veri kümelerinin yeniden tanımlanabilir olduğunu ispatlayan birçok çalışma mevcuttur. Bu çalışmaların çoğunda, makine öğrenmesi tekniklerine başvurulmasının yanı sıra anonimleştirmenin kendi karakteristik özelliklerinden yola çıkılarak da yeniden tanımlanabilmeye yol açtığı gösterilmektedir (De Montjoye, 2015; Narayanan & Shmatikov, 2008). Anonimleştirilmiş büyük veri kümeleri, yeterli harici verilerle birleştirildiğinde kullanıcı kimlikleri yeniden tanımlanabilmektedir. Bununla birlikte, kullanıcıların ayırt edici özellikleri, sosyal ağ bağlantıları veya arama geçmişleri gibi kolayca saptanabilen veriler bir araya geldiğinde yeniden tanımlama işlemi daha da kolaylaşmaktadır. Bu iki durumun gerçekleşmesi, özellikle büyük veri kümeleri söz konusu olduğunda anonimleştirmenin yetersiz olduğunu göstermektedir (Narayanan & Shmatikov, 2008).

Anonimleştirmenin bir diğer zafiyet noktası, benzersizlikten yola çıkılarak yeniden tanımlamanın kolaylaşmasıdır. İnsanların hareketleri ne kadar benzersizse tanımlanmaları da o kadar kolay hale gelmektedir. De Montjoye (2015), bir kişinin hareket izini benzersiz hale getirmek için ortalama kaç adet yer ve zaman bilgisi gerektiğini araştırmıştır. Araştırma sonucunda, herhangi bir kişinin hareket izine dair ortalama dört adet yer ve zaman bilgisinin saptanmasının, bu kişinin %95 gibi yüksek bir olasılıkla yeniden tanımlanabilmesine yol açtığı bulunmuştur:

Örneğin, bir kişinin sabah 9-10 arasında A bölgesinde ve öğlen 12-1 arasında B bölgesinde olduğu biliniyorsa, bu bilgi tek başına onu kesin olarak tanımlamaya yetmeyebilir. Ancak, üçüncü bir nokta

(örneğin, saat 3-4 arasında C bölgesinde olması) eklendiğinde, bu kişi artık veri tabanında benzersiz hale gelebilir (s. 22).

Sonuç olarak anonimleştirmenin zafiyetini ortaya koyan bu maddeler, verileri anonim hale getirmenin tam anlamıyla gizliliği korumadığını ve veri koruma noktasında anonim tekniklerinin tek başına yeterli bir çözüm olmadığını göstermektedir.

3.3.2. Diferansiyel Gizlilik

Diferansiyel gizlilik modeli matematiksel olarak diğer birçok modele kıyasla daha güvenilir bir güvenlik modeli sağlamaktadır. Önemli bir mahremiyet veri koruma modeli olarak değerlendirilen diferansiyel gizlilik kavramı aynı zamanda diferansiyel mahremiyet kavramı olarak da ifade edilmektedir (Dwork, 2006). Geleneksel bir koruma yöntemi olarak değerlendirilen anonimleştirme yönteminde yaşanan en önemli zafiyetlerden biri arka plan saldırılarına tam anlamıyla karşı koyamamasıdır. Bu önemli zafiyete karşı diferansiyel gizlilik modeli ise tam bir veri koruma garantisi sunmaktadır (Canbay & Sağıroğlu, 2020).

Diferansiyel gizlilik, genel bir tanım olarak veri tabanları üzerinde yapılan analizlerde gürültü ekleyerek tam gizlilik koruması sağlayan bir gizlilik sağlama modelidir. Özetle diferansiyel gizlilik, “rastgele bir mekanizma aracılığıyla yanıtların kontrollü (olasılıksal) gürültüye eklenmesiyle sorgulara verilen yanıtlar ile kişisel veriler arasındaki bağlantıyı gizleme fikrine dayanmaktadır.” (Castiglioni vd., 2020, s. 2).

Diferansiyel gizlilik, teoride bireylerin verilerinin hiçbir şekilde ifşa edilmeyeceğine dair tam bir koruma garantisi sunsa da bunun pratikte zor olduğu belirtilmektedir. Ancak yine de veriye rastgele eklenen gürültü sayesinde yayımlanan bilgilerin belirli bir bireyle ilişkilendirilmesi önlenmektedir. Diferansiyel gizliliğin matematiksel tanımı aşağıdaki şekildedir (Ahmadzai & Nguyen, 2023).

$$\Pr[A(D1) \in S] \leq \epsilon * \Pr[A(D2) \in S]$$

3.3.3. Blok zinciri

Merkeziyetsiz bir yapıya sahip olan blok zinciri teknolojisi, esasen bir veri tabanı rolü üstlenmektedir. Daha çok kripto varlıklar üzerinden ismi anılan bu teknoloji, sıklıkla finans alanında (Bitcoin, Ethereum vb.) duyulmakta ve çoğu zaman da bu varlıklarla karıştırılmaktadır. Ancak blok zinciri, bu varlıkların arkasındaki temel teknoloji olmakla birlikte, yalnızca finans sektöründe değil, birçok alanda kullanımı mevcut olan bir kod yapısıdır. Kriptografik yapısı sayesinde gizlilik ve güvenliğin sağlanması noktasında da işlevseldir. Nesnelerin interneti uygulamaları içerisinde güvenliği sağlamak adına çeşitli denenmiş örnekleri bulunmaktadır. Dolayısıyla blok zinciri, doğası gereği

merkeziyetsiz olması bakımından hem ekonomi politik açıdan hem de gizliliğin sağlanmasında sunduğu kriptografik olanaklar bakımından incelenmeye değer bir teknolojidir.

Blok zinciri teknolojisi, işlemleri ve verileri bloklar içinde tutan bir yapıya sahiptir. Bu işlemleri kriptografik yöntemlerle güvence altına alan blok zinciri, esasında bir veri tabanı özelliğine sahiptir ve veriler bloklara kaydedilmektedir (Türker & Tanyeri, 2024). Nesnelerin interneti uygulamalarında ve bağlı cihazlarda yüksek oranda güvenlik açığı tespit edilebilmektedir. Yaşanan gizlilik ve güvenlik sorunlarına yönelik birçok koruyucu yaklaşım ve çözüm önerisi geliştirilmektedir. Bu çözümlerden biri de blok zinciri teknolojisidir. Blok zinciri, potansiyel olarak nesnelerin interneti uygulamalarında gizliliği koruyan çeşitli çözümler sunmaktadır.

Nesnelerin interneti özelinde potansiyel blok zinciri çözümleri; veri bütünlüğü ve entegrasyonu, kimlik doğrulama, yetkilendirme, gizlilik ve güvenli iletişim başlıkları altında toplanabilmektedir. Herhangi bir bağlı cihazda meydana gelen tüm işlemler, dağıtık yapıya sahip blok zincirine kaydedilmekte ve takip edilebilmektedir. Ayrıca, blok zincirinde kullanılan akıllı sözleşmeler, bağlı cihazlara merkeziyetsiz kimlik doğrulama ile daha esnek ve detaylı yetkilendirme kuralları sunarak, veri gizliliği ve cihaz yönetimini daha güvenli ve etkili hâle getirmektedir (Kösesoy, 2019).

Nesnelerin İnterneti uygulamalarında, blok zinciri kullanılarak güvenliğin sağlanmasına yönelik yapılan birçok deneysel çalışma, kötü niyetli saldırganların engellenmesi amacıyla gerçekleştirilmektedir. Bu bağlamda, kapitalist şirketlerin kullanıcı davranışlarını analiz etmesi ve manipüle etmesi doğrultusunda geliştirdiği sömürü sisteminin de bir güvenlik ihlali olarak değerlendirilmesi durumunda, “blok zinciri bu noktada bir çare olabilir mi?” sorusunun sıklıkla göz ardı edildiği görülmektedir. Teknik düzlemde, mahremiyet ihlallerini engellemeye yönelik blok zinciri uygulamaları halihazırda mevcuttur; ancak kapitalist şirketlerin neden olduğu mahremiyet ihlallerine yönelik somut başarıya ulaşmış bir çalışma bulunmamaktadır. Bu bağlamda, blok zinciri teknolojisinin merkeziyetsiz yapısı çerçevesinde, tekelleşen internet yapısının incelenmesi değerli olabilir.

Blok zinciri teknolojisinin merkeziyetsiz yapısı, internetin tekelleşmesi sorununa çözüm olma potansiyeline sahip olmakla birlikte, bu potansiyel çift yönlü bir karakter taşımaktadır. Blok zincirinin merkeziyetsizlik ilkesi; Google, Facebook, Amazon gibi kurumsallaşmış teknoloji şirketlerine alternatif oluşturma imkânı sunmaktadır. Görünürde, veri sahipliğini kullanıcıya vermesi, şeffaflık sağlaması ve araçları ortadan kaldırması, dijital kapitalist sömürü sistemine karşı gelme veya güç ve bilgi asimetrisini azaltma yönünde olumlu bir karakter taşır. Ancak bu özellikler, teknolojinin kapitalist şirketler tarafından kendi çıkarları doğrultusunda yönlendirilemeyeceği anlamına gelmez. Nitekim şirketlerin, blok zinciri teknolojisini özelleştirerek yeniden merkezileştirme ihtimali de söz konusudur. Sonuç

olarak blok zinciri teknolojisinin tekelleşmeye karşı potansiyelini gerçekleştirebilmesi yalnızca teknik bir mesele değil aynı zamanda sosyal ve politik düzeyde de desteklenmesi gereken bir süreçtir. Aksi takdirde, internetin merkezileşme kaderi blok zinciri için de geçerli olabilir.

3.3.4. Kişisel Bilgi Yönetim Sistemleri

Kişisel Bilgi Yönetim Sistemleri (PIMS), aynı zamanda Kişisel Veri Depoları (PDS) olarak da ifade edilen, kullanıcının kendi verilerini yönetmesine olanak tanıyan teknik sistemler bütünüdür. Bu teknik araçlar, kullanıcının verileriyle ilgili gerçekleşen senaryolar hakkında bilgilendirilmesini sağlar ve verileri üzerinde kontrol gücünü artırır. Bu sayede, verilerin kim tarafından toplandığı, hangi tür hesaplamaların gerçekleştirildiği, yapılan analizlerin sonuçları ve verilerin üçüncü taraflarla paylaşımı gibi süreçler, şeffaf bir şekilde veri sahibinin kontrolü altına alınmayı amaçlamaktadır (Janssen vd., 2020).

PDS'lerin verilerin metalaştırılması sürecine karşı duruşu farklı bir dinamiğe sahiptir. PDS'ler, veri metalaştırmasına doğrudan karşı çıkmak yerine, sayısallaştırmayı yoğunlaştırır ve bunun hem kaçınılmaz hem de kullanıcı için faydalı olduğunu savunur. Dolayısıyla PDS'ler, gözetim kapitalizmine müdahale etmeyi amaçlar; ancak bunu, kararların şirketler lehine değil kullanıcı lehine alınabileceği bir yapı kurarak ve kullanıcıyı verinin kaynağı olmaktan çıkarıp sağlayıcısı konumuna getirerek gerçekleştirmeyi hedefler. Öte yandan, PDS'ler tüketici odaklı yeni bir pazar yapısının doğmasına yol açarak tekelciliğin zayıflamasına da katkı sağlayabilir (Lehtiniemi, 2017).

Kişisel veri depolarının temel amacı, verilerin yüksek olasılıkla korunmasını sağlamaktır. Bu noktada, Genel Veri Koruma Yönetmeliği (GDPR) ile aralarında sıkı bir ilişki bulunmaktadır. Denetleyiciler, veri işleyiciler ve veri sahipleri ekseninde çeşitli roller ve sorumluluklar tanımlanmaktadır. Kişisel veri depolarının aktif olarak çalışabilmesi için fiziksel bir cihaza ihtiyaç duyulmaktadır. Bu bağlamda, uygulama geliştiricilerinin veri işleme faaliyetini gerçekleştirebilmesi için cihaz kullanıcılarından onay alması gerekmektedir. Bu durum yasal bir dayanak gerektirdiğinden GDPR devreye girmekte ve “rıza” ile “açık rıza” kavramları önem kazanmaktadır. GDPR'ın veri sahiplerinin haklarını koruma konusunda önemli bir rol üstlendiğini belirtmek gerekir. PDS bağlamında, kişisel verilerin işlenmesini kısıtlama, veriler üzerinden profillemeye izin vermeme, iptal, düzeltme ve silme gibi haklar tanınmaktadır. Dolayısıyla PDS'lerin hem teknik hem de yasal veri koruma mekanizmaları sağladığı söylenebilir (Janssen vd., 2020).

PDS'lerin kullanıcıya daha fazla kontrol ve şeffaflık sağlama vaadi değerlidir. Ancak dijital altyapıların her geçen gün artan bilgi ve güç asimetrisi çok boyutlu ve oldukça karmaşıktır. Bu nedenle, veri işlemenin yapısal sorunları, PDS'lerin vaatlerini yalnızca sınırlı ölçüde hayata geçirmesine neden

olmaktadır. PDS'lerin sınırlı başarıya ulaşması, aynı zamanda gözetim kapitalizminin temel işleyişinin sorgulanmamasıyla da doğrudan ilişkilidir. Bu sorgulama yapılmadığı sürece, kullanıcılar daha fazla güçlenmek yerine mevcut sisteme entegre olmaktadır. Nitekim, PDS'nin kullanıcıya daha fazla kontrol ve özyönetim sağlama vaadi, kullanıcıyı daha fazla veri üretmeye teşvik etmektedir. Bu durum ise, kullanıcının gizliliğini korumak yerine, sömürü sistemine daha fazla hizmet etmesine yol açmaktadır (Janssen vd., 2020). Bununla beraber, PDS'lerin bireysel güçlendirme stratejisi belirli açılardan eleştirilmelidir. Çünkü kullanıcıların yeterli kontrol gücüne sahip olması, teknik bilgiye, karar verme kapasitesine ve rasyonel değerlendirme becerilerine sahip olmayı gerektirir. Ayrıca, davranışsal yönlendirmeyi tamamen engellediği söylenemeyeceği gibi, veri kontrolünün davranış kontrolüne dönüşme ihtimali de söz konusudur. Sonuç olarak, PDS'lerin gizli gözetim biçimlerine zemin hazırlama ihtimali de bulunmaktadır (Lehtiniemi, 2017).

3.3.5. Tasarım Yoluyla Gizlilik Yaklaşımı (Privacy by Design-PBD)

Tasarım yoluyla gizlilik yaklaşımı anlatılırken Jaap-Henk Hoepman'ın (2022) *Privacy Design Strategies (The Little Blue Book) Gizlilik Tasarım Stratejileri* kitabına başvurulmuştur. Söz konusu kitabın tasarım stratejilerinin ayrı bir başlık altında aktarılması uygun görülmüştür.

Tasarımda gizlilik yaklaşımı, 2018 yılından itibaren yasal olarak bir zorunluluk haline gelmiştir. Yasal çerçevede gizliliğin en baştan itibaren sağlanması önemli bir gereklilik olarak kabul edilmektedir. Bu bağlamda, tasarımda gizlilik yaklaşımı yalnızca teorik bir çerçeve olarak görülmemeli, esasen uygulama aşamasında değer kazanmaktadır. Dolayısıyla söz konusu kitap, “Nereden ve nasıl başlanmalı?” sorusuna büyük ölçüde yanıt vermekte ve kişisel bilgi işleyen kuruluşlar, sistemleri tasarlayan mühendisler ve sistem sorumlularını büyük oranda ilgilendirmektedir. Sonuç olarak belirsiz yasal normların somut hale getirilmesi ve sistem tasarımının keşfedilmesi adına önemli adımlar sunmaktadır (Hoepman, 2022).

Gizlilik stratejileri, veri odaklı ve süreç odaklı olmak üzere iki gruba ayrılmaktadır. Toplamda sekiz gizlilik stratejisi sunulmakta olup bu stratejiler dörderli gruplar halinde sınıflandırılmaktadır. Aşağıdaki tabloda gizlilik stratejileri yer almaktadır.

**VERİ ODAKLI
STRATEJİLER****SÜREÇ ODAKLI
STRATEJİLER**Minimize Etmek (Minimise)Bilgilendirmek (Inform)Ayırmak (Separate)Kontrol Sunmak (Control)Soyutlamak (Abstract)Uygulamak (Enforce)Gizlemek (Hide)Kanıtlamak (Demonstrate)**Tablo 1. Gizlilik Stratejileri**

Veri odaklı stratejiler ağırlıklı olarak teknik bir niteliğe sahiptir ve verilerin gizliliğe uygun bir şekilde işlenmesini sağlamaktadır. Süreç odaklı stratejiler ise organizasyonel prosedürlere odaklanmaktadır (Hoepman, 2022).

Veri odaklı stratejiler, verinin işlenmeden önceki sürecinde alınması gereken önlemleri ifade etmektedir. Örneğin minimize etme işlemi olabildiğince az veri toplanması ve gereksiz verilerin toplanmasından kaçınmayı ifade etmektedir. Gizleme, uygun teknik yöntemler ile üçüncü taraflarla veri paylaşımını engellemeyi amaçlamaktadır. Ayırma, verilerin mümkün olduğunca merkezden uzak bir yerde toplanmasını ve tek bir yerde toplanmamasını amaçlar. Soyutlama ise ayrıntılı bilgi yerine özet bilginin kullanılmasıdır.

Süreç odaklı stratejiler ise veri işleme sırasında ve sonrasında alınması gereken önlemleri ifade etmektedir. Örneğin bilgilendirme, kullanıcıların verilerin nasıl ve neden işlendiğine dair bilgi sahibi olmasını amaçlamaktadır. Kontrol, tıpkı kişisel bilgi yönetim sistemleri gibi kullanıcıların verileri üzerinde öz yönetim ve kontrol sahibi olmasını amaçlamaktadır. Uygulama, gizlilik politikalarının zorunlu kılınmasını ifade etmektedir. Kanıtlama ise denetimin önemli bir mekanizma olduğunu ve gizlilik stratejilerinin uyumluluğunun kanıtlanabilir olması gerektiğini ifade etmektedir.

3.3.6. Veri Minimizasyonu

Veri minimizasyonu verilerin mümkün olduğunca en az olacak şekilde toplanmasını amaçlar ve toplanan verilerin yalnızca gerekli veriler olmasını önceler. Dolayısıyla veriler ne kadar az toplanırsa

gizlilik riski de o kadar düşük olmaktadır. Örneğin herhangi bir çevrimiçi uygulamada veya bir cihazda kullanıcının ilgili olmayan tüm verilerinin toplanması veri minimizasyonunu gerektirmektedir.

Akıllı bir cihazda yalnızca gerekli veriler toplanarak da amacına ulaşabilmektedir. Buna bazı pnömatik yol tüpleri ve hatta yaklaşık yirmi yıl önce tasarlanan aware home örnek verilebilir. Bununla beraber Londra'daki bazı alışveriş merkezlerinde kullanılan kinetik zemin teknolojileri, bireylerin kimlik bilgilerini ya da dijital izlerini toplamadan, yalnızca fiziksel hareketi enerjiye dönüştürmektedir. Pavegen gibi girişimlerin geliştirdiği bu sistemler, gözetimden arındırılmış, anonim ve çevresel olarak sürdürülebilir bir teknoloji modelini temsil etmektedir. bu

Veri minimizasyonu ilkesinin bir nesnelerin interneti cihazına uygulanmasına yönelik bir senaryo kurulabilir. Örneğin, Google'ın akıllı termostat ürünü üzerinden bir değerlendirme yapılabilir. Nitekim, önceki bölümlerde de değinildiği üzere Google Nest teknolojisi, akıllı ürünlerde veri gözetiminin sıkça yaşandığı örneklerden biri olarak karşımıza çıkmaktadır.

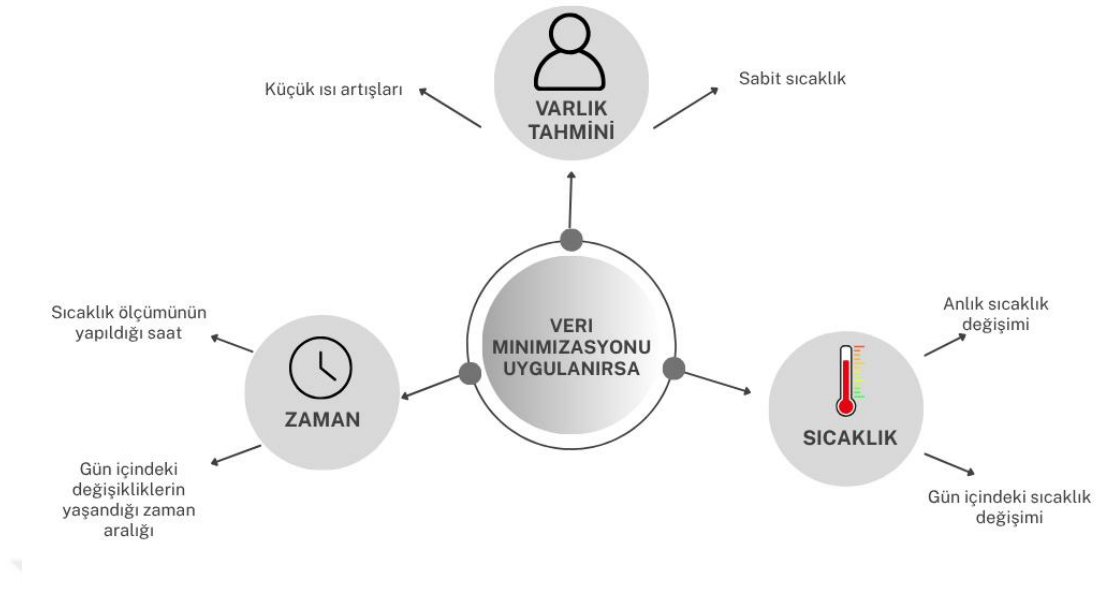
Akıllı termostatın, veri minimizasyonu uygulanmadan önceki hâli değerlendirildiğinde, kullanıcıların ev içerisindeki tüm eylemleri, evdeki sıcaklık geçmişinin tamamı toplanarak analiz edilmektedir. Ancak veri minimizasyonu uygulandığında, yalnızca sıcaklık ve zaman verileri toplanır ve böylece kullanıcıların diğer alışkanlıklarına dair veriler toplanmaz. Verilerin minimize edilmesi stratejisi, gözetim kapitalizmi şirketlerinin veri toplama yüzdeliğini azaltarak daha az kullanıcı verisi ile modelleme yapmasına ve daha az hedefli reklam gelirlerine sahip olmasına yol açabilir. Örneğin Shaowang ve arkadaşları (2025) nesnelerin interneti veri akışları üzerinden yaptıkları algoritmik küçültme çalışmasında kullanıcı tanımlanabilirliğini %16,7 oranında azaltmayı başarmıştır. Üstelik yaptıkları deneysel çalışmada doğruluk kaybını %1'in altında tutmayı da başaramışlardır (Shaowang vd., 2025).

Aşağıda, iki farklı model üzerinden bir kıyaslama yapılmaktadır. İlk model, mevcut gözetim kapitalizmi yaklaşımıyla çalışan bir termostat tasavvurudur. Burada örnek olarak sunulan veri çeşitliliği, sadeleştirilmiş bir biçimde verilmiştir. Dolayısıyla bir şirketin topladığı tüm verilere dair açık bilgiler bulunmayabilir. Bu nedenle, gerçekte toplanan veri miktarı burada gösterilen çeşitlilikten çok daha fazla olabilir. Ancak karşılaştırmanın anlaşılabilirliği açısından sunulan veri çeşitliliğinin yeterli olduğu düşünülmektedir. İkinci modelde ise veri minimizasyonu ile tasavvur edilmiş bir termostat işleyişidir. İki model arasında bir karşılaştırma yapılarak aralarındaki veri çeşitliliği farkına dikkat çekilmeye çalışılmıştır.



Şekil 3. Kapitalist Termostat Modeli

Bu modele dikkatle bakıldığında, termostatin kullanım amacı doğrultusunda toplanması gereken verilere ek olarak kullanıcıya ve ortama ilişkin verilerin de toplandığı görülmektedir. Kullanıcıların konum verileri, tercihleri, termostat özelinde elde edilmesi gereken veriler ve sıcaklık değerleri gibi bilgiler toplanmaktadır. Örneğin, ağ verileri bağlamında, kullanıcının Wi-Fi bağlantısı kesildiğinde ve bu durum konum verileriyle eşleştirildiğinde, kullanıcının evde olup olmadığına dair bir veri ortaya çıkarılabilir. Bununla birlikte, kullanıcının uyku saatleri, sıcaklık ayarlarının değiştirildiği zaman dilimleri gibi zaman verileri de toplanmaktadır. Ayrıca, kullanıcının davranışsal farklılıkları ve tercihlerine dayalı olarak gelişen eylemlerine ilişkin veriler de kayıt altına alınmaktadır. Üstelik bu davranışlar zaman ekseninde filtrelenebilmekte; örneğin, hafta içi ve hafta sonu arasındaki davranış farklılıklarına ilişkin veriler toplanarak analiz edilmektedir. Tüm bu veriler, kullanıcıya yönelik davranış profilleri oluşturmak, reklam hedeflemesi yapmak, yönlendirmelerde bulunmak ve daha ayrıntılı profillemeler geliştirmek amacıyla kullanılabilir.



Şekil 4. Minimize Edilmiş Termostat Modeli

Bu modele bakıldığında ise, oda sıcaklığı, zaman bilgisi ve kullanıcının evde bulunma durumu, minimum veri kullanımıyla belirlenebilmektedir. Örneğin, zaman bilgisinde yalnızca sıcaklık ölçümünün yapıldığı saatler; sıcaklık verisinin, o anki oda sıcaklığına ya da yalnızca hava koşullarına dayanarak ayarlanması; son olarak da kullanıcının evde olup olmadığı bilgisinin sıcaklık verilerine göre tahmin edilmesi gibi kategorilerden bahsedilebilir. Örneğin kullanıcı eve geldiğinde küçük ısı artışları sebebiyle kullanıcının eve geldiğinin anlaşılması veya sabit ısının olması sebebiyle kullanıcının evde olmadığı anlaşılması gibi örnekler verilebilir. Bir önceki modelden farklı olarak, burada GPS, hareket sensörleri ve kameralar gibi aygıtlar kullanılmadan da cihaz işlevini yerine getirebilmektedir. Kullanıcının yaptığı her değişikliğin verisi kaydedilmemekte, böylece profil çıkarımı da önemli ölçüde azalmaktadır. Dolayısıyla, veri minimizasyonu uygulandığında bir akıllı cihazın işlevini yerine getirmesi için kullanıcının kim olduğu, eve ne zaman gelip gittiği ya da günlük pratiklerine ilişkin verilerin toplanmasına gerek kalmaz. Bu durum ise, kapitalist şirketlerin davranışsal eylemleri yönlendirme, detaylı profillemeler yapma ve hedefli reklamcılık faaliyetlerinde bulunma kapasitelerini büyük ölçüde kısıtlar.

Bu bölümde, birinci bölümde ele alınan ve araştırmanın ana teorik çerçevesini oluşturan gözetim kapitalizmi daha da özelleştirilerek nesnelerin interneti uygulama alanları üzerinden incelenmiştir. İlk olarak, nesnelerin interneti tarihsel ve kavramsal açıdan ele alınmış, ardından genel özellikleri ve yaygın teknolojileri üzerinde durulmuştur. Sonrasında, taranan literatüre dayanarak nesnelerin internetinin en

yaygın uygulama alanları belirlenmiş ve başlıklar halinde tartışılmıştır. Nesnelerin internetinin genel hatlarıyla ele alınmasının ardından, araştırmanın odak noktasını oluşturan veri gözetimi konusu işlenmiştir. Buradaki veri gözetimi, birinci bölümde ele alınan veri gözetimi kavramına kıyasla daha özelleştirilmiş olup nesnelerin interneti özelinde değerlendirilmiştir. “Her zaman her yerde bağlantılabilirlik” paradigmasından yola çıkılarak, önce şehirde, sonra evde ve daha derine inerek nihayetinde bedene sirayet eden bağlantılabilir teknolojilerin veri gözetimi örnekleri açıklanmıştır. Son olarak gözetim rejimlerine karşı geliştirilen hesaplanabilir gizlilik modelleri olan gizliliği arttırmaya yönelik geliştirilen teknolojilere değinilmiştir.



4. GİZLİLİK ÇÖZÜMLERİ ÜZERİNE BİR ARAŞTIRMA

Bu çalışmada, gözetim kapitalizminin genişleyen sınırları, nesnelerin interneti üzerinden incelenmiştir. Eleştirel ekonomi politik çerçevede yürütülen bu çalışmada, her zaman ve her yerde gözetimin yaygınlaşması sorunsalı ele alınmıştır. Bu bağlamda gizlilik çözümlerinin incelenmesi gerekli görülmüştür. Her ne kadar çeşitli teknik gizlilik çözümleri ve bazı yasal düzenlemeler mevcut olsa da ekonomi politik düzlemde büyük veri odaklı ciddi bir güç eşitsizliği söz konusudur. Bu bağlamda, mevcut gizlilik çözümlerinin bu güç asimetrisini gidermedeki yeterliliğinin sorgulanması, ortaya çıkan ihtiyaçların belirlenmesi ve bu ihtiyaçların değerlendirilmesi amacıyla bir araştırma tasarımı geliştirilmiştir. Gizlilik çözümleri üzerine nitel bir araştırma gerçekleştirilmiş ve uzmanlarla derinlemesine görüşmeler yapılmıştır. Bu bölümde, araştırmanın amacı ve kapsamı, yöntemi, bulguları ve sonuçları sunulmaktadır.

4.1. Araştırmanın Amacı ve Kapsamı

Araştırma, gözetim kapitalizmi yaklaşımının nesnelerin interneti uygulamalarıyla daha da yoğunlaştığı yönündeki eleştirisine temellenmektedir. Bu bağlamda çalışma, nesnelerin interneti cihazlarının ürettiği büyük verinin nasıl toplandığını, işlendiğini ve bu süreçte hangi mahremiyet ihlallerinin ortaya çıktığını, söz konusu ihlallere yönelik gizlilik önerilerini analiz etmeye odaklanmaktadır. Araştırma, bu teknolojik gelişmelerin yalnızca teknik boyutlarıyla değil, aynı zamanda sosyo-politik ve etik sonuçlarıyla da ele alınmasını hedeflemektedir. Bu doğrultuda, nesnelerin interneti uygulamalarında yaşanan mahremiyet ihlallerine karşı geliştirilen gizlilik artırıcı sistemlerin mevcut potansiyelinin ne ölçüde işe yaradığını ve daha güvenli çözümlerin nasıl geliştirilebileceğini sorgulamaktadır. Bu araştırma, gözetim kapitalizmi çerçevesinde, nesnelerin interneti teknolojilerinin mevcut kullanım biçimlerinin gizlilik ve veri güvenliği bağlamında ne tür riskler barındırdığını ortaya koymayı ve bu risklere yönelik alternatif çözümlerin teknik, yasal ve ekonomi-politik düzlemde tartışılmasına katkı sunmayı amaçlamaktadır.

4.1. Metodoloji

Araştırma kapsamında nitel araştırma yöntemi tercih edilmiş olup uzman görüşmesi veri toplama tekniği kullanılmıştır. Araştırmada, veri toplama tekniği olarak uzman görüşmelerinin tercih edilmesinin önemli nedenleri bulunmaktadır. Bunlardan ilki, şirketler veya resmi kurumlar tercih edildiğinde, nesnelerin interneti üzerine yürüttükleri veri toplama süreçlerine ya da gizlilik uygulamalarına dair açık veriye ulaşmanın güç olmasıdır. İkinci olarak, kullanıcılar nezdinde yapılacak bir araştırmanın, teknik bilgi sunmak veya ekonomi-politik bir değerlendirme yapmak açısından uygun olmadığı düşünülmektedir. Dolayısıyla, araştırmanın uzman görüşlerine dayandırılması; hem mevcut güç ve bilgi asimetrisinin ortaya konulmasında hem gizlilik stratejilerinin yeterliliğinin sorgulanmasında

hem de geleceğe yönelik projeksiyonlar sunulmasında daha anlamlı sonuçlar vereceği düşüncesiyle tercih edilmiştir.

Bu konuda çalışan uzmanların tespiti için veri tabanlarında bulunan bilimsel yayınlar incelenmiş ve çalışmaya uygun olduğu düşünülen isimler belirlenmiştir. Uzmanlara ulaşmak için dijital iletişim kanalları kullanılmış ve ağırlıklı olarak e-posta yoluyla iletişim kurulmuştur. İlk gönderilen e-postada araştırmanın amacı belirtilmiş ve ikinci bir teyit amaçlı ilgili uzmanın çalışmaya uygun olup olmadığı sorulmuştur. Uzmandan olumlu yanıt alındığı takdirde, hazırlanan beş adet soru Word dosyası şeklinde kendisine iletilmiştir. Ulaşılan uzmanlardan bazıları ise ya araştırma konusunun uzmanlık alanlarına girmediğini ya da konuya ilgili olsalar da yeterli zamana sahip olmadıkları için çalışmaya katılamayacaklarını belirtmiştir.

Uzmanlar, spesifik ilgi alanlarından dolayı dünyanın farklı coğrafyalarından katılımcı olduğu için ve fiziksel olarak da bir araya gelmek mümkün olmadığı için yazılı metin ve video konferans aracılığıyla iletişim kurulmuştur. Dolayısıyla iletişim dili de İngilizce dilinde gerçekleşmiştir. Bundan dolayı uzmanlardan elde edilen verilerin betimsel analizini gerçekleştirmeden önce Türkçe diline çevrilmiştir.

Elde edilen veriler, betimsel analiz yöntemiyle değerlendirilmiştir. Literatür taramasından hareketle öngörülen temalar ışığında sorular hazırlanmış olup görüşmelerden sonra yanıtlar incelenerek mevcut temalar revize edilmiş ve yeni temalar eklenmiştir. Bu temalar altında belirli kavramsal kategoriler geliştirilmiştir. Böylelikle uzman görüşlerinden elde edilen veriler, yapılandırılmış ve sistematik bir biçimde yorumlanarak, araştırmanın kuramsal çerçevesiyle ilişkilendirilebilecek anlamlı sonuçlara ulaşılması hedeflenmiştir.

4.2. Araştırmanın Örneklemi ve Veri Toplama Tekniği

Araştırmanın örneklemi, Nesnelerin İnterneti ve gizlilik konularında uzmanlaşmış kişiler oluşturmaktadır. Nitel araştırmalarda sıkça kullanılan amaçlı örneklem yöntemine başvurularak çalışma konusuna dair derinlemesine bilgi sunabilecek, bu alanda akademik ya da pratik uzmanlığı bulunan katılımcıların seçilmesi hedeflenmiştir. Başlangıçta, örneklem Türkiye sınırları içerisindeki uzmanlarla sınırlı tutulmuştur. Ancak bu çerçevede yapılan görüşme taleplerinden yeterli düzeyde detaylı geri dönüş alınamaması nedeniyle, coğrafi kısıtlama kaldırılmış ve örneklem uluslararası düzeyde genişletilmiştir. Bu doğrultuda, dünya genelinde Nesnelerin İnterneti ile gizlilik kesişiminde çalışan uzmanlara ulaşılmıştır. Uzmanlara e-posta yoluyla ulaşılmadan önce, ilgili kişilerin bilimsel yayınları, akademik profilleri ve varsa araştırma laboratuvarlarına ait web siteleri ayrıntılı biçimde incelenmiştir. Bu süreçte, özellikle literatür taraması ve uzman arayışında “IoT”, “privacy”, “IoT and surveillance” gibi anahtar

kelimeler kullanılarak konuya özel çalışma yürüten araştırmacılara ulaşılması hedeflenmiştir. Ulaşılan uzmanlar, araştırma disiplinleri ve bulundukları ülkeler temelinde kategorize edilmiştir. Araştırmaya toplam 10 uzman katılmış olup, bu uzmanlardan üç kategori ikiyeşerli olarak aynı ülkeden; kalanlar ise farklı ülkelere olmak üzere toplamda yedi farklı ülkeden katılım sağlanmıştır. Uzmanlarla yapılan görüşmeler, Aralık 2024 ile Mayıs 2025 tarihleri arasında gerçekleştirilmiştir. Görüşmelerde uzmanlardan birebir yanıtlar alınmış olup bu sayede araştırma kapsamında doğrudan birincil veri elde edilmiştir.

UZMANLARIN DÜNYA ÜZERİNDE BULUNDUKLARI ÜLKELER



Şekil 5. Uzman Haritası

Tablodan hareketle araştırmaya Almanya'dan iki, ABD'den iki, Avustralya'dan iki; Finlandiya, Hollanda, Macaristan ve İspanya ülkelerinden birer uzman katılım sağlamıştır.

UZMANLAR	GÖRÜŞMENİN TÜRÜ	ARAŞTIRMA ALANI	ÜLKE
UZMAN 1	Yazılı Metin	IoT ve Gizliliği Arttıran Teknolojiler	Hollanda
UZMAN 2	Yazılı Metin	Bilgisayar Bilimi/Gizlilik Tasarımları	ABD
UZMAN 3	Yazılı Metin	Bilgisayar Bilimi/Biyoenformatik	ABD
UZMAN 4	Yazılı Metin	Ağ Sistemleri	Finlandiya
UZMAN 5	Video Konferans	Akıllı Sistemler ve Veri Koruma Hukuku	Macaristan
UZMAN 6	Yazılı metin	Büyük Veri, Gizlilik ve Veri Koruması	Almanya
UZMAN 7	Yazılı Metin	Kişisel Veri Hukuku	Almanya
UZMAN 8	Yazılı Metin	Akıllı Teknolojilerin Politik Ekonomisi	Avustralya
UZMAN 9	Yazılı Metin	Kent ve Hesaplamalı Teknolojiler	Avustralya
UZMAN 10	Yazılı Metin	Teknolojide Gizlilik	İspanya

Tablo 2. Uzmanların Araştırma Alanları

Bu tablodan hareketle uzmanlar, nesnelerin interneti, veri gizliliği, güvenlik teknolojileri ve veri koruma hukuku gibi alanlarda çalışmalar yapan araştırmacılardan oluşmaktadır. Uzmanların seçiminde, çalışmanın konusuna ilişkin kuramsal ve uygulamalı bilgi birikimine sahip olmaları esas alınmış, disiplinler arası bir bakış açısı sağlamak amacıyla bilgisayar bilimi, hukuk, mühendislik ve sosyal bilimler gibi çeşitli alanlardan akademisyen ve araştırmacılara ulaşılmıştır. Uzmanlar, araştırmada kimlik bilgilerinin açıkça ifade edilmesini istemediği için kimlik bilgileri ve gerçek isimleri anonimleştirilerek uzman 1, uzman 2 şeklinde kodlanmıştır.

Veri toplama tekniği olarak nitel araştırma yöntemlerinden derinlemesine görüşmenin bir türü olan uzman görüşmesi tercih edilmiş ve görüşmeler çoğunlukla yazılı metin yoluyla, bir tanesi ise video konferans yöntemiyle gerçekleştirilmiştir. Uzmanlara ulaşmak için öncelikle e-posta yoluyla iletişime geçilmiş, görüşmeyi kabul eden katılımcılara araştırma amacını açıklayan bir bilgilendirme metni ve beş açık uçlu soru içeren bir Word dosyası iletilmiştir.

Hazırlanan beş adet soru; uzmanların büyük teknoloji şirketlerinin kişisel veriler üzerinden gelir elde etme modelleri hakkındaki görüşlerini, bağlı akıllı cihazların kullanıcı verilerini toplama ve işleme biçimlerine dair düşüncelerini, akıllı cihazların fiziksel mekâna yayılmasının gözetimi nasıl

yoğunlaştırdığına ilişkin değerlendirmelerini, bu cihazların kişisel veri mahremiyetini ihlal etmemesi için ne tür önlemler alınması gerektiğini ve somut örneklerin mevcut olup olmadığını, mevcut gizlilik tasarımlarının gerçekten işe yarayıp yaramadığını ve son olarak da ilgili uzmanın bu bağlamda önerdiği çözüm yollarını içermektedir.

Uzmanlara sorulan soruların orijinal hali aşağıdaki tabloda yer almaktadır.

Uzmanlara Sorulan Sorular

1.soru	Büyük teknoloji şirketlerinin kişisel veriler üzerinden gelir elde etme modelleri hakkındaki görüşleriniz hangi konumdadır? Bu bağlamda Internet of Things (IoT) cihazlarının (Akıllı şehirler, akıllı evler, giyilebilir teknolojiler ve bağlanılabilir birçok akıllı cihazlar vb.) kullanıcı verilerini toplama ve işleme yöntemlerini nasıl değerlendiriyorsunuz?	
2.soru	IoT ile fiziksel mekandaki hareketlerimize, mobilite/hareketliliğe yönelik veriler toplayabiliyorlar. Söz konusu verilerin kişisel veri havuzuna dahil olması teknoloji şirketlerinin kullanıcıyı daha detaylı profilelemesine olanak tanıdığını düşünüyor musunuz? Söz konusu durum gelirlerine katkı sağlar mı? IoT aracılığıyla toplanan verilerin çeşitliliğinin artmasını gözetimi yoğunlaşması olarak değerlendirebilir miyiz? Konuyu mahremiyet odağında değerlendirebilir misiniz?	
3.soru	IoT ile toplanan ve işlenen kişisel verilerin mahremiyet ihlaline yol açmaması için nasıl veri güvenliği ve gizlilik önlemleri alınabilir? Bu konuda bildiğiniz örnekler nelerdir?	
4.soru	IoT uygulamalarında kullanılan gizlilik tasarımları sahiden kişisel verilerin güvenliğini sağlıyor mu?	
5.soru	IoT cihazlarının kişisel verileri koruyan ve kullanıcının mahremiyet hakkını gözeticek şekilde geliştirilmesi için sizce neler yapılabilir? Çözüm önerileriniz var mı?	

Tablo 3. Araştırma Soruları

4.3. Temalar ve Bulgular

Uzmanlara yöneltilen soruların cevapları beş ayrı tema altında sınıflandırılarak analiz edilmiştir.

4.3.1. Ekonomi Politik Bağlamda Nesnelerin İnterneti

Bu araştırmada, uzmanların gizlilik çözümlerine yönelik değerlendirmeleri ekonomi politik bir çerçevede ele alınmaktadır. Bu doğrultuda belirlenen ilk tema, uzmanların nesnelerin interneti ve gizlilik çözümlerine ekonomi politik bağlamda nasıl yaklaştıklarını ve bu iki olguyu söz konusu bağlamla nasıl ilişkilendirdiklerini analiz etmeyi amaçlamaktadır. Bu doğrultuda, uzman görüşlerinden yola çıkarak

veri temelli ekonomik gelir elde eden şirketlerin nesnelerin interneti alanındaki yansımalarına dikkat çekilmiş ve bu konudaki görüşler ekonomi politik bağlamda analiz edilmiştir.

Araştırmanın ilk sorusu, uzmanların teknoloji şirketlerinin veri temelli gelir modelleri hakkındaki görüşlerine odaklanmaktadır. Özellikle nesnelerin interneti cihazları üzerinden veri toplanması ve işlenmesine dair değerlendirmeleri incelenmiştir. Çoğu uzman, şirketlerin veri toplama süreçlerini kapitalist sistemle ilişkilendirerek eleştirmekte ve bu uygulamaların mahremiyet ihlali taşıdığını düşünmektedir. Örneğin uzman 1 bu konuda şu ifadeleri kullanmıştır:

“Davranışsal verileri kâr amacıyla işleyen büyük teknoloji şirketleri, geniş çaplı ve sürekli gizlilik ihlalleri gerçekleştirmektedir. Hizmetleri kullanıcılara göre uyarlamak için onları yoğun şekilde takip etmek ve profillemek, ne yazık ki günümüz dijital hizmetlerinde yaygın bir uygulamadır. Nesnelerin İnterneti cihazları ve hizmetleri de bu durumdan farklı değildir.”

Kullanıcı verilerinin farkında olunmadan ve çoğunlukla rıza alınmadan toplanmasının etik dışı olduğu konusunda genel bir uzlaşa vardır. Ayrışan görüşlere bakıldığında ise bazı uzmanlar veri toplamanın tamamen olumsuz olmadığını savunmakta, kişiselleştirilmiş hizmetlerin geliştirilmesi açısından faydalı olabileceğini belirtmektedir. Özellikle küçük ölçekli geliştiriciler için veri kullanımının daha meşru olabileceği dile getirilmiştir. Ayrıca verilerin sadece reklamcılık değil, ürün geliştirme gibi olumlu amaçlarla da kullanılabileceği ifade edilmiştir. Genel olarak uzmanlar, büyük teknoloji şirketlerinin veri toplama süreçlerini eleştirmekle birlikte, veri kullanımının bağlama göre anlam kazanabileceğini de göz önünde bulundurmaktadır.

Öncelikle, şirketlerin kullanıcı verilerini hizmet geliştirme amacıyla kullanmasının meşruiyetine bakıldığında, gelir modeli ile kamu yararı arasında bir gerilim olduğu söylenebilir. Nitekim kâr ile kamu yararının bir arada bulunması, politik ve etik meşruiyet arasındaki sınırları belirsizleştirmektedir. Dolayısıyla bu durum, değer üretiminin toplumsal fayda kisvesi altında ticarileştirilmesi anlamına gelmektedir. Bu duruma bir ek olarak nesnelerin interneti teknoloji sağlayıcılarının veri toplama ve analiz etme konusunda diğer şirketlere kıyasla daha meşru haklara sahip olması gerektiğini düşünen uzmanlar bulunmaktadır. Örneğin uzman 2 bu durum hakkında şunları söylemektedir:

“Daha küçük nesnelerin interneti geliştiricilerinin, mühendislik süreçlerini finanse edebilmek ve rekabet gücü kazanabilmek için davranışsal verileri kullanmalarının daha meşru bir çıkar olduğunu savunabiliriz. Oysa Google, Meta, Apple gibi büyük şirketler hâlihazırda önemli bir pazar gücüne sahiptir ve faaliyetlerini başka yollarla finanse edebilecek kaynaklara sahiptirler ya da davranışsal

verilerin işlenmesiyle elde edilen değeri, daha gizlilik dostu tekniklerle de sağlayabilecek yatırım kapasitesine sahiptirler.”

Buradan yola çıkarak kaynakların ve güç ilişkilerinin asimetrik bir yapıya sahip olduğu görülmektedir. Bu durum ise ne yazık ki tekelleşmeyi kolaylaştırmakta ve piyasadaki rekabeti bastırmaktadır. Sonuç olarak da küçük bağlanılabilir teknoloji firmaları varlığını sürdürmek için daha agresif bir veri toplama sürecine dahil olmaktadır.

Nesnelerin interneti ekonomi politiği çoğunlukla gözetim kapitalizmi çerçevesinden ele alınmaktadır. Ancak, nesnelerin interneti ekosistemi doğası gereği yalnızca kapitalist gözetimle açıklanamayacak dinamiklere de sahiptir. Bu durum, bazı uzmanlar tarafından özellikle vurgulanmaktadır. Örneğin Uzman 1 bu durumu şu şekilde açıklamaktadır:

“Her bağlı cihaz gözetim kapitalizmini destekliyor gibi görünse de nesnelerin internetinin etkileri yalnızca bu çerçeveden değerlendirilemeyecek kadar geniştir.”

“Benim gözlemlediğim iki temel eksiklik şunlardır: Gözetim kapitalizmi yaklaşımı, genellikle sadece kullanıcılarla büyük teknoloji şirketleri arasındaki ilişkilere odaklanmaktadır. Ancak, diğer şirketler ya da devletler de birbirlerinin mahremiyetini etkileyebilir; bu yön yeterince ele alınmamaktadır. Bu yaklaşım, tüm şirketlerin kişisel verileri doğrudan topladığını varsaymaktadır. Oysa günümüzde bazı nesnelerin interneti hizmetleri, kişisel veriye doğrudan erişmeden, diğer şirketleri kendi sistemlerine entegre ederek de veri temelli iş modelleri geliştirebilmektedir.”

Bu açıklamalar, nesnelerin interneti teknolojilerinin gözetim üzerindeki etkisinin yalnızca birey-şirket ilişkisinden ibaret olmadığını; aksine katmanlı ve karmaşık bir yapının var olduğunu göstermektedir. Nitekim gözetim aktörleri çeşitlenmekte, yalnızca bireyler değil, şirketler ve devletler de birbirlerinin verilerini kullanarak gözetim uygulamakta ve çok taraflı bir gözetim hakimiyeti ortaya çıkmaktadır. Bununla birlikte, meseleyi yalnızca kişisel veri odağında ele almak yetersiz görünmektedir. Gözetim kapitalizmi, işleyişin genellikle kişisel veriler üzerinden yürüdüğünü ifade etse de nesnelerin interneti sistemlerinde şirketler arası veri paylaşımı ve altyapı bağımlılığı da önem kazanmaktadır. Bu durum, doğrudan kişisel veriye ihtiyaç duyulmadan da gözetim ve kontrolün mümkün olduğunu göstermektedir. Son olarak, yeni güç ilişkilerinin doğduğu da ifade edilebilir. Nesnelerin interneti hizmet sağlayıcıları, diğer şirketleri kendi sistemlerine bağımlı hale getirerek yeni bir tür ekonomik ve teknolojik hakimiyet kurabilmektedir.

4.3.2. Nesnelerin İnterneti ile Gözetimin Yaygınlaşması ve Derinleşmesi

Araştırmanın ikinci teması, nesnelerin interneti cihazlarının yaygınlaşması ile gözetim arasındaki ilişkinin analizini kapsamaktadır. Uzmanların çoğu, bu cihazların topladığı çeşitli verilerin gözetimi daha derin ve yaygın hâle getirdiği görüşündedir.

Ortak görüşlere bakıldığında akıllı cihazların yaygınlaşmasıyla beraber yalnızca çevrimiçi değil, fiziksel ortamlardan da veri toplanmakta ve bu durum gözetimi hem yoğunlaştırmakta hem de derinleştirmektedir. Toplanan veri çeşitliliği sayesinde kullanıcılar daha detaylı bir şekilde profillenebilmektedir. Genel olarak uzmanlar, nesnelerin interneti cihazlarının hem veri çeşitliliğini hem de gözetim yoğunluğunu arttırdığını kabul etmektedir.

Örneğin Uzman 2, çevrimiçi gözetim ile fiziksel mekâna yayılan gözetim arasındaki farkı şu şekilde açıklamaktadır:

“Bir web sitesi sağlayıcısının ya isteyerek verdiğimiz ya da hassas kategorileri kolayca ortaya çıkarmayan (örneğin IP adresi gibi) kişisel bilgileri işlemesi başka bir şeydir; bir de bileğimizde taşıdığımız ve sürekli olarak (sağlık verileri dâhil) çok çeşitli sensörlerden veri toplayan, bu verileri bulutta işlemek üzere gönderen ve bunun sonucunda çok güçlü öngörücü modeller geliştiren bir akıllı saatin yaptığı veri işlemesi bambaşka bir şeydir. Üstelik çoğu zaman kullanıcı bu işlemlerin farkında bile değildir.”

Dolayısıyla bir akıllı cihazın veriyi toplama ve işleme kapasitesinin çevrimiçi sistemlerden çok daha büyük olduğu söylenebilir. Sonuç olarak akıllı cihazlar daha yoğun bir gözetim gerçekleştirerek öngörülebilir modeller ortaya çıkarmaktadır.

Çevrimiçi gözetimden farklı olarak, nesnelerin interneti gözetimi daha sınırsız ve yayılmış bir doğaya sahiptir. Bu nedenle burada dikkat edilmesi gereken unsurlardan biri, bağlamın değişmesi ve aynı zamanda karmaşıklaşmasıdır. Çünkü akıllı teknolojiler (akıllı evler, akıllı şehirler, giyilebilir teknolojiler vb.) veri yoğunluğu açısından çok daha etkindir. Akıllı cihaz teknolojilerinin yaygınlaşması ise, bağlama göre değişen bir ekonomik varlık sınıfının oluşmasına yol açmaktadır. Bu durum, veriden elde edilen statik değerden farklı olarak, yaşamın her alanının hatta bağlamsal ilişkilerin bile ekonomik değere dönüştürüldüğü daha kapsamlı bir ortam yaratmaktadır.

Nesnelerin interneti ekosisteminin gittikçe genişlemesi, kullanıcılar üzerinde bazı önemli etkilere yol açmaktadır. Örneğin, yine uzman 2 bu durumla doğrudan ilişkili olabilecek şu açıklamayı yapmaktadır:

“Amerika Birleşik Devletleri'nde, bir kişinin yasal olmayan bir eyalette kürtaj yaptırıp yaptırmadığının ortaya çıkarılması, hatalı bir yüz tanıma algoritmasının bir şüpheliyi yanlış tanımlaması ya da çevrimiçi toplanan sağlık bilgilerine dayanarak bir sağlık sigortası başvurusunun reddedilmesi gibi vakalar yaşanmıştır. Bu tür örnekler sonucunda bir tür “soğutucu etki” (chilling effect) ortaya çıkmaktadır; insanlar artık gündelik faaliyetlerde bulunmaktan daha çok çekinebilir, çünkü daha önce özel sayılan ortamlarda kendilerini güvende hissetmeyebilirler.”

Bu durum, bireysel özgürlüğün sınırlanmasına neden olabileceği gibi, insanların izlendiklerinin farkında olmaları nedeniyle doğal davranışlarını değiştirmelerine de yol açmaktadır. Kendisini güvenli saydığı ortamlarda bile birey artık güven duygusunu kaybetmeye başlayabilir.

Nesnelerin internetinin giderek yaygınlaşmasının gözetimi yoğunlaştırdığı iddiası, genellikle verinin nicel olarak artmasıyla ilişkilendirilmektedir. Ancak Uzman 7, bu konuda daha farklı bir bakış açısına sahip olup şu açıklamayı yapmaktadır:

“Nesnelerin interneti cihazları aracılığıyla toplanan verilerin niteliği ve niceliği, bu faaliyetin gözetim olarak nitelendirilip nitelendirilemeyeceğini belirlemede önemlidir. İşlenen verilerin gerçek kişilerle ilişkilendirilebilir olması halinde, çeşitliliğinin ve miktarının artmasını gözetimin yoğunlaşması olarak değerlendirebiliriz. Ancak işlenen verilerin anonimleştirilmiş olması, gerçek kişiyle ilişkili olmaması veya ilişkilendirilemeyecek nitelikte olması gibi durumlarda kişisel veri işleme faaliyetinden söz edilemeyeceğinden, gözetimin yoğunlaşmasından da bahsedilemez.”

Bu açıklamaya benzer olarak uzman 3, şu açıklamada bulunmuştur:

“Bazı nesnelerin interneti cihazları, belirli bir bireyi tanımlamadan insanların toplu davranışlarına dair faydalı veriler toplayabilir. Eğer toplanan verilerden belirli bir kişiyi tanımak mümkün değilse, bu oldukça güvenli sayılabilir.”

Bu durum, tıpkı büyük veri kavramının sadece verinin devasa miktarda olduğu anlamına geldiği yönündeki yanıltıcı algıyı hatırlatmaktadır. Dolayısıyla nesnelerin interneti ekosisteminin genişlemesiyle gözetimin derinleşip derinleşmediği yalnızca toplanan verinin miktarına değil, aynı zamanda kişisel veri olup olmadığına ve kişisel veriye dönüştürülebilirliğine bağlı olduğu sonucunu ortaya çıkarmaktadır.

4.3.3. Nesnelerin İnterneti ve Mahremiyet Sorunsalı

Günlük hayatta nesnelerin interneti teknolojilerinin giderek daha fazla yer edinmesi, kişilerin evi ve bedeni gibi en mahrem sayılabilecek ortamlarda var olması bazı mahremiyet ihlallerinin

yaşanmasına sebep olmaktadır. Uzman görüşlerinden elde edilen verilere göre, genel olarak Nİ cihazlarının doğası, kullanıcıların ve hatta kullanıcı olmayan kişilerin bile mahremiyetini riske atmaktadır. Bu durum bazı uzmanlar tarafından, kullanıcıların farkında olmadan mahremiyet ihlali yaşadığı şeklinde yorumlanırken; bazı uzmanlar ise kullanıcıların bu durumun farkında olduğunu, ancak hizmet karşılığında bir tür “veri takası” yaptıklarını kabul ettiklerini ifade etmektedir.

Hizmet karşılığında kullanıcı verilerinin paylaşılmasına dair farklı görüşler mevcuttur. Örneğin, Uzman 10 bunun kabul edilebilir bir model olduğunu şu şekilde açıklamaktadır:

“Hepimiz Google Haritalar gibi ücretsiz hizmetlerden, kişiselleştirilmiş önerilerden ve veri toplama sayesinde mümkün olan birçok kolaylıktan büyük ölçüde faydalaniyoruz. Eğer kullanıcılar neyi feda ettiklerinin farkındaysa ve bu takastan memnunsa, bunun kabul edilebilir olduğunu düşünüyorum.”

Bu açıklama, kullanıcının bilinçli onamına bağlı olarak veri takasının kabul edilebilir olduğunu ifade etmektedir. Ancak burada dikkat edilmesi gereken önemli konulardan biri, kullanıcı onamının sınırlı bir yapıya sahip olmasıdır. Dolayısıyla, söz konusu olan gerçek bilinçli davranış biçimlerinin tartışılması gerekmektedir. Buna ek olarak, bilgilendirilmiş rızanın gerçekten var olabilmesi için kullanıcıların verilerinin nasıl işlendiği, kimlerle paylaşıldığı ve ne kadar süreyle saklandığı gibi konularda tam bilgi sahibi olmaları gerekir. Ancak bu, uygulamada neredeyse hiç gerçekleşmeyen bir durumdur. Bu durum ise başlı başına bir mahremiyet sorunsalını doğurmaktadır.

Kullanıcıların mahremiyetlerinin risk altında olduğu, genel bir kanı olarak ifade edilmiştir. Ancak bu durum daha da detaylandırıldığında, yalnızca kullanıcıların değil, kullanıcı olmayan üçüncü tarafların da mahremiyetlerinin ihlal edildiği sonucuna ulaşılmaktadır. Bu duruma özellikle dikkat çekmek isteyen Uzman 1, 2 ve 3 sırasıyla şu açıklamaları yapmaktadır:

“Bir kişinin evine Ring marka bir akıllı kapı zili taktığını düşünelim. Gözetim kapitalizmi merceğinden bakıldığında, Amazon’un bu kullanıcıyı nasıl profilleyebileceği ve davranışlarını nasıl etkileyebileceği analiz edilir. Bu, elbette kullanıcının gizliliğini etkiler ve geçerli bir eleştiridir. Ancak aynı zamanda Ring, çevredeki insanların gizliliğini de etkiler. Bu cihazı kullanan kişi, artık kullanıcı olmayanların da mahremiyetini etkiler. Daha fazla insan Ring kameraları kullanmaya başladığında, mahallelerde bir tür gözetim ağı oluşur.”

“Burada ayrıca “izleyicilerin” (bystander) gizliliğine dair bir tartışmaya da yer vermek gerekir. Yani sadece cihazın birincil kullanıcılarının değil, örneğin bir Airbnb’de akıllı hoparlör bulunan bir evde konaklayan misafirlerin ya da otonom bir internet bağlantılı arabanın yakınından geçen yayaların da gizliliği risk altındadır.”

“Nesnelerin interneti cihazları söz konusu olduğunda, cihazı satın alıp kuran kişi –tıpkı bir akıllı telefon kullanıcısında olduğu gibi– neler olup bittiği konusunda bir miktar bilgiye sahiptir. Ancak Nİ cihazları, cihazı kurmayan ve hatta cihazın orada olduğunu bile bilmeyen “masum” üçüncü kişilerin verilerini de toplayabilir.”

Sonuç olarak, nesnelerin interneti teknolojileri yalnızca kullanıcıların değil, kullanıcı olmayan üçüncü tarafların da mahremiyetini tehdit eden bir yapıya sahiptir. Bu durum, mahremiyetin bireysel bir mesele olmaktan çıkıp toplumsal bir sorun haline geldiğini göstermektedir.

Nesnelerin interneti ve mahremiyet sorunsalına farklı açılardan yaklaşan uzmanlar da bulunmaktadır. Örneğin Uzman 7, bu duruma hukuki açıdan yaklaşarak şu açıklamayı yapmıştır:

“Hukukun diğer tüm alanlarında olduğu gibi, veri koruma kapsamında da hukuka uygunluğun her zaman etik ve adil olan ile eş anlamlı olmadığı haller ile karşı karşıya kalınmaktadır. Örneğin bir veri işleme faaliyeti hukuka uygun olabilir ancak bireylerin mahremiyet ve gizlilik algısını tehdit etmeye devam edebilir. Bu durumun en temel örneklerini mevcut düzenlemelerde yer alan istisna hükümlerinde görmekteyiz. Milli güvenliğe ilişkin istisnalar, bireyin devlet tarafından gözetlenmesine olanak tanıyabilir. Nesnelerin interneti cihazları söz konusu olduğunda da hukuka uygun veri işleme faaliyetleri, gözetimin yoğunlaşmasını tetikleyebilir.”

Bu açıklamaya dayanarak iki önemli sonuca ulaşılabilmektedir. İlk olarak, mahremiyetin yasal olarak korunabilirliğinin sınırlı olduğu çıkarımı yapılmaktadır. İkinci olarak ise gözetimin yasal yollarla da gerçekleştirileceği ancak denetimsiz biçimde artabileceği ve özellikle kamu-özel sektör iş birliklerinde (örneğin akıllı şehir projelerinde), yasal fakat denetlenmeyen veri akışının mahremiyetin sistematik olarak aşındırılmasına neden olabileceği sonucuna ulaşılmaktadır.

Nesnelerin interneti teknolojileri ile mahremiyet riski arasındaki ilişki her zaman sınırları net bir şekilde belirlenmiş bir duruma işaret etmeyebilir. Bu noktada, Uzman 3’ün konuya ilişkin görüşlerine dikkat çekmekte fayda vardır:

“Eğer toplanan verilerden belirli bir kişiyi tanımak mümkün değilse, bu oldukça güvenli sayılabilir. Örneğin, bir cihaz bir sokakta yoğun trafik olup olmadığını belirleyebilir. Eğer bir kamera kullanılıyorsa ve video kaydediliyorsa, o zaman bireysel araçlar ve sürücüler sonradan tespit edilebilir – bu kötü sonuçlar doğurabilir. Ancak onlarca yıldır kullanılan başka tür cihazlar da vardır ki bunlar kişisel veri sızdırma riski olmadan trafik akışını ölçebilir – mesela, yola yerleştirilen kalın bir hortumdan geçerken araç sayısını tespit eden sistemler (bunlara bazen “pnömatik yol tüpleri” denir).

Yani, nesnelerin interneti cihazları ve bunların topladığı veriler hakkında genelleyici ifadeler kullanmak kolay değildir.”

Bu açıklamadan yola çıkarak iki önemli çıkarım yapmak mümkündür. İlk olarak, nesnelerin interneti cihazları her zaman mahremiyet riski oluşturmaz. İkinci olarak ise bazı mevcut örneklerde bu cihazlar, kişisel verileri tanımlamadan da amaçlarına ulaşabilmektedir.

4.3.4. Çözüm Önerileri Bağlamında Teknik ve Yapısal Görüşler

Bu bölümde, akıllı cihazlar aracılığıyla veri toplanırken kullanılan mevcut gizlilik tasarımlarının ne kadar etkili olduğu ve veri toplanırken mahremiyetin nasıl korunabileceği ele alınmıştır. Uzmanlar, bu konuda hem teknik hem de yapısal sorunlara dikkat çekmektedir.

Uzmanların ortak görüşleri, mevcut gizlilik tasarımlarının belli bir düzeyde koruma sağlasa da bu korumanın genellikle sınırlı olduğu, anonimleştirmenin tek başına yeterli olmayıp tahmine dayalı saldırılarla geri döndürülebileceği, kullanıcı rızasının gizlilik politikalarının merkezinde yer almasına rağmen çoğu zaman güncel olmadığı ve geri alınamaz nitelikte olduğu, kullanıcı ara yüzlerinin gizlilik tercihlerini yönetmeye genellikle elverişli olmadığı, şeffaflık ve erişilebilirlik eksikliklerinin bulunduğu ve gizlilik tasarımlarının başarılı olabilmesi için sistemlerin en başından bu prensiplere göre geliştirilmesi gerektiği yönünde birleşmektedir.

Uzmanlar ağırlıklı olarak dört gizlilik çözümüne odaklanmıştır. Bunlar anonimleştirme, diferansiyel gizlilik, veri minimizasyonu ve tasarımda gizlilik yaklaşımlarını içermektedir.

Anonimleştirme

Mevcut gizlilik sağlayıcı yöntemlerinden biri anonimleştirmedir. Verilerin anonimleştirilmesi kullanıcıyı tanımlayabilecek herhangi bir bilginin açığa çıkarılmadan şifrelenmesi ve gizliliğin sağlanmasıdır. Uzmanlar genel olarak anonimleştirmenin etkili bir gizlilik sağlayıcı olduğunu düşünmemektedir. Ancak belirli bir noktaya kadar güvenliği sağlayabileceği görüşü hakimdir. Örneğin uzman 2 şu görüşü belirtmektedir:

“Güvenli çalışma alanları (secure enclaves), güvenilir yürütme ortamları (trusted execution environments), anonim kimlik bilgileri (anonymous credentials) ve takma ad kullanımı (pseudonymization) gibi yöntemler de düşünülebilir.”

Uzman 10 ise şu görüşlerini aktarmaktadır:

“İdeal olarak, veriler takma adlandırma (pseudonymization) yöntemiyle işlenmeli ve özellikle üçüncü taraflarla paylaşım ihtimali varsa, k-anonimlik gibi gizlilik koruma teknikleri uygulanmalıdır.

Ayrıca verilerin hem iletim sırasında hem de saklanırken şifrelenmesi, yetkisiz erişimden korunması açısından gereklidir.”

Anonimleştirmenin yetersiz bir yöntem olduğunu düşünen uzman 6, şu görüşünü belirtmektedir:

“Anonimleştirme ve benzeri hesaplamalı gizlilik yöntemleri genellikle yetersizdir; geçmişte yapılan araştırmalar, örneğin Sweeney (1997), Narayanan ve Shmatikov (2019), bu tekniklerin çeşitli saldırılarla aşılabileceğini göstermiştir. Bu saldırılar genellikle anonimleştirilen veri kümesinde yer alan bireyleri hedef alır. Ancak daha da önemli olan, gizliliğin yalnızca anonimlik ihlaliyle değil, veri çıkarımı ve profillemeye yoluyla da ihlal edilebilmesidir. Kimi durumlarda kişi veri kümesindedir ama bazı bilgileri silinmiştir (çıkartım), kimi zaman ise kişi veri kümesinde bile değildir fakat benzer örüntüler üzerinden tahmin yapılabilir (profillemeye). Günümüzde asıl tehlikenin, yeterince üzerinde durulmayan bu ikinci tür gizlilik ihlallerinde olduğu söylenebilir.”

Buradan hareketle anonimleştirmenin gerçek anlamda gizliliği garanti etmediği sonucuna ulaşılmaktadır.

Tasarımda Gizlilik

Anonimleştirme dışında, mevcut gizlilik tasarımları hakkında da çeşitli görüşler belirtilmiştir. Örneğin, tasarımda gizlilik yaklaşımları üzerine hem ortak hem de ayrışan görüşler mevcuttur. Bazı uzmanlar, bu yaklaşımların yüksek düzeyde koruma sağladığını belirtirken; bazıları ise bu yöntemlerin yalnızca belli bir noktaya kadar mahremiyeti koruyabileceğini, ancak tam anlamıyla garantili sonuçlar sunamayacağını ifade etmektedir. Hatta bazı uzmanlar, bu yaklaşımların şirketlere daha fazla kontrol gücü sağlayabilecek araçlar olduğunu da savunmaktadır. Örneğin uzman 1 şöyle ifade etmektedir:

“Birçok örnekte, teknoloji şirketlerinin mahremiyet artırıcı teknolojileri (PETs) stratejik biçimde kullandığını görüyoruz. Örneğin: Rekabet avantajı sağlamak için (Apple Find My, App Tracking Transparency, Google Privacy Sandbox), hükümetlerin karar alma yetkilerini kendi üzerlerine çekmek için (Google Apple Exposure Notification Framework) ve üçüncü taraf şirketlerin cihaz ve hizmet üretim biçimlerini yeniden şekillendirmek için (Amazon Sidewalk). PET’ler kullanılsa bile, bu hizmetler yeni gizlilik sorunları yaratmakta ve bu sorunlar PET’lerin kendileri tarafından çözülememektedir.”

Bu durum gizlilik artırıcı teknolojilerin yeni bir gizlilik endişesi yarattığı noktasında bir paradoks oluşturmaktadır. Bu görüşe ek olarak uzman 7 de şu görüşü savunmaktadır:

“Mevcut gizlilik tasarımlarının büyük bir kısmının yeterince kullanıcı dostu olmadığı ve hatta manipülatif nitelikte olduğu kanaatindeyim. Kullanıcıların aktif eylemleri olmaksızın veri işleyecek şekilde tasarlanmış cihaz ve uygulamalar, mevcut veri koruma ilke ve kuralları ile çelişmektedir ve ne yazık ki sıklıkla kullanılmaktadır.”

Tasarımda gizlilik yaklaşımı hakkında uzman 2'nin şu görüşüne de dikkat çekmekte fayda vardır:

“Mükemmel bir tasarımda gizlilik (PbD) uygulaması varsayımı altında bile, nesnelerin interneti uygulamalarında kişisel verilerin güvenliğiyle ilgili genel bazı zorluklar devam etmektedir. Nİ cihazları genellikle sınırlı kaynaklara sahiptir, bu nedenle bazı güvenlik mekanizmalarını destekleyemeyebilirler. Donanım ve yazılım tedarik zincirinde güvenlik açıkları olabilir ve bunlar tamamen önlenmesi zor olan risklerdir. Ayrıca kullanıcı faktörü de önemlidir: bireyler Nİ cihazlarına gerekenden fazla bilgi sağlayabilir veya sınırlı kullanıcı ara yüzü nedeniyle verilerini yeterince güvenli hale getiremeyebilirler. Bu tür sorunlar, en iyi gizlilik uygulamalarıyla bile tamamen önlenemeyebilir.”

Bu açıklama, yalnızca gizlilik tasarımının iyi işleminin yeterli olmadığını; nesnelerin interneti cihazlarının doğası gereği sınırlı kaynaklara sahip olmasının, gizlilik yaklaşımlarının bütüncül bir şekilde uygulanmasını engellediğini göstermektedir. Dolayısıyla gizlilik yaklaşımlarının uygulanması bağlamın ve cihazın türüne göre değişiklik gösterebilir. Sonuç olarak etkili gizliliğin sağlanması için cihazların buna uygun tasarlanması da önem arz etmektedir.

Veri Minimizasyonu

Uzmanlar, teknik olarak uygulanabilecek etkili yöntemlerden biri olarak veri minimizasyonunu önermektedir. Uzmanlar, bu yöntemin başarılı sonuçlar verebileceğini düşünmektedir. Mümkün olduğunca az veri toplanması ve verilerin cihaz içinde işlenip saklanması gerektiği savunulmaktadır. Örneğin Uzman 2 şu görüşü belirtmektedir:

“Tasarımda gizlilik ilkeleri arasında, nesnelerin interneti bağlamında en önemlilerinden biri veri minimizasyonudur. Mümkün olduğunca az veri toplayın. Verileri buluta göndermek yerine cihazda işleyin ve depolayın.”

Uzman 4 şu ifadeleri kullanmaktadır:

“Gizlilik yöntemleri bir cihazın türüne ve bağlamına göre değişiklik gösterebilir ancak veri minimizasyonu (gereksiz veri toplamamak), gizlilik odaklı tasarım gibi ilkeler izlenirse gizliliği sağlamak mümkün olabilir.”

Diferansiyel Gizlilik

Bir başka görüş ise diferansiyel gizlilik yönündedir. Örneğin Uzman 3 şu şekilde ifade etmiştir:

“Elde veri varsa, bunu anonimleştirmeye yönelik çeşitli teknikler uygulanabilir fakat bu çabalar çoğunlukla başarısız olur. Diferansiyel gizlilik gibi daha resmi ve kanıtlanabilir mekanizmalar bazı uygulamalarda –örneğin 2020 ABD Nüfus Sayımında– kullanılmaya başlanmıştır. Ancak –bu önemli bir nokta– orijinal veri bir yerlerde saklanıyorsa, bu verilerin bir gün sızma ihtimali her zaman vardır.”

Bu görüşe dayanarak diferansiyel gizlilik veya herhangi teknik geliştirilen bir gizlilik yöntemi her ne kadar başarılı olsa da orijinal verilerin bir yerlerde tutuluyor olması risklerin her zaman var olduğu sonucunu ortaya çıkarmaktadır.

Uzman 7 ise hem anonimleştirme hem de diferansiyel gizliliğin gizliliği sağlamada uygun yaklaşımlar olabileceğini ifade etmektedir:

“Veri güvenliği hususunda diferansiyel gizlilik, homomorfik şifreleme, etkili olabildiği hallerde anonimleştirme gibi yöntemlerden istifade edilebilir. Nesnelerin interneti cihazları arasında kolaylıkla ve hızla gerçekleşen veri aktarımının güvenliğini tesis etmek önemlidir. Bu sebeple gelişmiş şifreleme teknikleri başta olmak üzere fiziksel (yangın, sel, deprem gibi hallerde server güvenliğinin sağlanması vb.) ve siber güvenlik (zararlı yazılımların önlenmesi, güvenlik duvarı vb.) önlemlerinin alınması elzemdir.”

4.3.5. Devlet Politikaları Bağlamında Yapılabilecek Uygulamalar

Mevcut gizlilik tasarımlarının etkililiği, uzmanlar tarafından tartışılmış ve bazı teknik yöntemler önerilmiştir. Ancak bu yöntemlerin büyük ölçüde politikalarla desteklenmesi gerektiği düşünülmektedir. Dolayısıyla, etkili gizlilik çözümlerinin geliştirilmesi, uygulanabilir politikalar bağlamında da ele alınmalıdır.

Uzman görüşlerinde, çözüm önerileri ya da mevcut gizlilik tasarımlarının başarımlarının belirlenmesi bağlamında yasal çerçeve ön plana çıkmaktadır. Hem kullanıcılar için hazırlanan yasal sözleşmeler hem de teknik çözümlerin uygulanması açısından yasaların belirli ve şeffaf şekilde hazırlanması ve denetlenmesi büyük önem arz etmektedir. Dolayısıyla teknik çözümlerin yasal çözümlerle sıkı sıkıya bağlı olduğu gerçeği de vurgulanmaktadır. Buna ek olarak kullanıcı farkındalığının artması da gizliliğin sağlanması noktasında önemli bir yer tutmaktadır. Dolayısıyla kullanıcı farkındalığının arttırılması için gerekli eğitimlerin hazırlanması da bir zaruret olarak görülmektedir.

Kişisel verilerin işlenmesi konusunda mevcut yasal çerçevenin ortaya konulması önem arz etmektedir. Daha önce teknik görüşlerde yer alan tasarımda gizlilik yaklaşımı Genel Veri Koruma Tüzüğü'nün (GDPR) tasarımda ve varsayılanda gizlilik ilkesi konsepti özelinde de incelenilmektedir.¹

Tasarımda gizlilik yaklaşımı ilkesi, her ne kadar mahremiyetin korunması açısından önemli bir adım olsa da özellikle yenilikçi girişimlerde (örneğin yapay zekâ, nesnelerin interneti vb.) gizliliğin korunmasına yönelik uygulanabilir yöntemler sunma ve rehberlik etme konusunda yetersiz kalmaktadır. Dolayısıyla gizlilik stratejilerinin gerekliliği, yalnızca teorik düzeyde ele alındığında yeterli olmaz; bu stratejiler uygulanabilir hâle geldiğinde anlamlı ve başarılı sonuçlar doğurur. Aksi takdirde, yalnızca gerekliliğini ifade etmekle sınırlı kalır.

Tasarımda gizlilik yaklaşımı, sorunların yalnızca teknik çözümlerle değil, aynı zamanda kültürel ve organizasyonel dönüşümlerle de ele alınması gerektiğini benimsemektedir. Ancak uygulama aşamasında mühendislik ve hukuk disiplinleri arasında büyük ölçüde uyumsuzluk ortaya çıkmaktadır. Mühendisler, genellikle soyut ve yoruma açık hukuki gereklilikleri somut uygulamalara dönüştürmekte zorlanırken; hukukçular ise teknolojik sınırlamaları ve sistem tasarımının pratik kısıtlarını yeterince göz önünde bulunduramamaktadır. Bu durum, gizliliğin sağlanması sürecinde çelişkilerin doğmasına yol açmakta ve sürdürülebilir gizlilik çözümlerinin geliştirilmesini engellemektedir (Gustavsson, 2020).

Hukuk ve mühendislik arasındaki bu gerilim, mevcut araştırmamızda da kendini göstermektedir. Örneğin, veri koruma hukuku alanında uzman kişiler, gizliliğin en iyi şekilde sağlanabilmesi için gereken önlemleri sıralarken, teknik açıdan önerilen çözümlerin uygulanabilirliği hakkında yeterli bilgiye sahip olamayabilir. Bu durum bir mühendis özelinde incelendiğinde ise, gizliliği sağlamaya yönelik görüşler genellikle kötü amaçlı yazılımlardan korunmaya odaklanmakta ve veri mahremiyeti, ekonomi-politik düzlemde uzak kalmaktadır.

Tasarımda gizlilik ilkesi doğrultusunda bazı uzmanlar görüş belirtmektedir. Örneğin uzman 1 bu konu hakkında şöyle bir açıklama yapmaktadır:

¹ 2018 yılında GDPR'ın yürürlüğe girmesiyle birlikte, kişisel verilerin korunması yasal bir zorunluluk hâline gelmiş ve bu bağlamda “varsayılan olarak gizlilik” ilkesi bir standart olarak belirlenmiştir. Veri işleme süreçlerinde, en başından itibaren kullanıcıların gizliliğini esas alacak şekilde sistemlerin tasarlanması bir şart olarak kabul edilmiştir. Bu gelişme, özellikle gizliliğin temel bir hak olarak görülmesi ve mahremiyetin korunması açısından önemli bir adım olarak değerlendirilmektedir (Gustavsson, 2020).

“Bence veri koruma düzenlemeleri sadece “tasarım ve varsayılan olarak veri koruma” (örneğin GDPR madde 25) öngörmekle kalmamalı, aynı zamanda PET’lerin nasıl uygulandığına dair şeffaflık konusunda daha katı olmalıdır. Bu, kullanıcıların daha uzun gizlilik politikaları okumaya zorlanması anlamına gelmemelidir; bunun yerine, bağımsız araştırmacıların ve aktivistlerin denetim yapabilmesi sağlanmalıdır.”

Bu açıklamadan yola çıkarak, devlet politikaları bağlamında uygulanabilecek birçok düzenleme önerisi çıkarımı yapılabilir. İlk olarak, yalnızca teknik çözümlerin değil, şeffaflığın da düzenlenmesi gerekmektedir. İkinci olarak, şirketlerin gizlilik tasarımlarının yalnızca varlığına güvenilmemeli, bunların etkili ve uygun bir şekilde uygulanıp uygulanmadığı mutlaka denetlenmelidir. Son olarak, sivil denetimin kurumsallaşması gerektiği vurgulanmaktadır. Devlet, şeffaflık mekanizmalarını kurumsallaştırarak sivil toplumun katılımını teşvik etmeli ve kolaylaştırmalıdır. Bu bağlamda, bağımsız etik denetim kurullarının oluşturulması gibi politikaların hayata geçirilmesi önerilmektedir.

Uzmanların, çevrimiçi uygulamaların veya akıllı cihazların kullanımı sırasında kullanıcılar için hazırlanan sözleşmelere ilişkin çeşitli görüşleri bulunmaktadır. Uzmanlar, bu sözleşmelerin genellikle uzun, okunması güç ve sade bir dilden uzak olması nedeniyle eleştirmektedir. Bu durum, kullanıcıların sözleşmeleri anlamak için zaman ve çaba harcamaktan kaçınmasına ve doğrudan kabul etmelerine neden olmaktadır. Ayrıca sözleşmelerin çok sık değişiyor olması ve güncelliğini korumaması da önemli etkenlerden biridir. Dolayısıyla bu sorun ciddi bir şekilde ele alınmalı ve çözüm önerileri geliştirilmelidir.

Uzmanlar, sözleşmelerin daha anlaşılır bir şekilde hazırlanması, sade ve açık bir dil kullanılması gerektiğini vurgulamaktadır. Ayrıca bu sözleşmelerin düzenli olarak güncellenmesi ve içeriklerinin denetlenmesi de önemli görülmektedir. Örneğin uzman 7 bu konu ile ilgili şöyle bir açıklama yapmaktadır:

“Nesnelerin interneti cihazları kullanılarak gerçekleştirilen veri işleme faaliyetlerinde yaşanan ilk problem, aydınlatmanın gereği gibi yerine getirilememesidir. Bu kapsamda katmanlı aydınlatma başta olmak üzere video, QR kod, sesli betimleme gibi çeşitli yöntemlerle aydınlatma yükümlülüğünün yerine getirilmesi desteklenebilir. Kullanıcıların hem veri işlemeye ilişkin güncel gizlilik politikalarını görüntüleyebildiği hem de tercihlerini yönetebildiği dijital platformların kurulması, rızanın güncelliği başta olmak üzere şeffaflığı da teşvik edebilir.”

Bu konuda uzman 10 da görüşlerini belirtmektedir ve şu ifadeleri kullanmıştır:

“Bir nesnelerin interneti sisteminin hangi verileri topladığını, bu verilerin nasıl korunduğunu ve nasıl kullanılacağını kullanıcıya açık ve sade bir dille anlatmak çok önemlidir. Kullanıcıların bu temel noktaları anlamak için karmaşık yasal ifadeleri çözümlemesine gerek olmamalıdır. Buna ek olarak, hizmetin ISO 27000 serisi gibi tanınmış güvenlik standartlarına uyduğunu belirten güvenilir bir beyan ya da sertifika sunulmalıdır.”

Yine aynı konu üzerine uzman 9 da görüş belirtmektedir:

“İnsanlar genellikle sayfalarca küçük yazıları okumaz ve eğer bunu telefon üzerinden yapıyorsanız, bu daha da zor hale gelir. Bu tür sözleşmelerin, insanların anlayabileceği ve erişebileceği şekilde iletilmesi faydalı olacaktır. Ayrıca, seçim eksikliğine de dikkat çekmek isterim. Çoğu zaman bir hizmeti kullanmak için tek seçenek katılmayı (opt-in) kabul etmektir ve eğer bu hizmete erişmenin başka bir yolu yoksa, kullanıcıların aslında gerçek bir seçeneği kalmamaktadır.”

Bununla birlikte, bir sözleşmenin “anlaşılır” olup olmadığını belirleyen ölçütlerin ne olduğu ve kime göre belirleneceği konusu da tartışmalıdır. Örneğin uzman 5 bu konuya ilişkin şöyle bir açıklama yapmaktadır:

“Kullanıcıların yaşları, eğitim düzeyleri veya dijital okuryazarlık seviyeleri göz önünde bulundurularak farklı kullanıcı gruplarına hitap eden sözleşmelerin hazırlanması, metinlerin daha erişilebilir ve anlaşılır hâle gelmesini sağlayabilir.”

Bu yaklaşım, sözleşmelerin seri üretim mantığıyla hazırlanmasının önüne geçerek, daha kişiselleştirilmiş ve kapsayıcı bir sözleşme tasarımı ihtiyacını ortaya koymaktadır.

Bir diğer önemli konu kullanıcının ürünü kullanmak için vermiş olduğu rızadır. Kullanıcı bir kez rıza verdikten sonra genellikle rızasını geri çekebilme hakkına sahip değildir. Daha doğrusu rızasını geri çekmek istediğinde gerekli bir muhatap bulamama sorunuyla karşı karşıyadır. Dolayısıyla büyük veri analizleri geleneksel gizlilik ilkelerini ve rıza mekanizmalarını geçersiz kılmaktadır.

Rızanın etkili bir koruma aracı olmamasının önemli sebepleri bulunmaktadır. Bunlar genellikle kullanıcıların verilerin hangi amaçla kullanılacağını tam olarak anlamadan onay vermeleri, büyük veri sistemlerinde verilerin sıklıkla ikincil ve öngörülemez amaçlarla yeniden kullanılması, verilerin bir kez depolandıktan sonra uzun vadeli analizlerde ve farklı bağlamlarda kullanılabilmesi (örneğin Google Nest örneğinde olduğu gibi) ve rızanın anlık bir işlem olmasına karşın veri kullanımının sürekli ve dinamik bir şekilde gerçekleşmesi nedeniyle, kullanıcının veri koruma üzerindeki kontrolü neredeyse imkânsız hâle gelmektedir (Barocas & Nissenbaum, 2014). Dolayısıyla bu önemli soruna karşı durmak

için rızanın ötesine geçmek gerekmektedir. Gizlilik korunmasının yalnızca bireysel rızaya dayandırılmaması, yapısal ve kurumsal önlemlerin alınması gerekmektedir. Bu da veri işleme ilkelerinin yasal olarak sınırlandırılması anlamına gelmektedir.

Uzmanlık alanı mühendislik olan katılımcılar, yasal çerçevede düzenlenebilecek gizlilik yöntemlerini ağırlıklı olarak kötü amaçlı saldırılara karşı geliştirilebilecek teknikler çerçevesinde ele almaktadır. Bu durum, aynı zamanda mühendislerin sosyal bilimler perspektifinden uzak olmaları nedeniyle güvenlik ihlallerini yalnızca kötü niyetli saldırılar bağlamında değerlendirmelerine; şirketlerin kişisel verileri işlemesine yönelik eylemleri ise birer güvenlik ihlali olarak görmemelerine neden olmaktadır. Dolayısıyla mühendislerin ekonomi-politik bir çerçeveden uzak oldukları gözlemlenmektedir. Bu durumu desteklemek adına bazı uzman görüşlerine yer vermek önemlidir. Örneğin Uzman 2, hükümetlerin ve politika yapıcıların nesnelerin interneti cihazlarının güvenliğine ilişkin standartlar ve düzenlemeler geliştirmeye odaklanmaları gerektiğini, Avrupa Birliği'nin *Cyber Resilience Act* girişiminin ise buna iyi bir örnek oluşturduğunu belirtmektedir. Buna ek olarak, ABD'de bazı sözleşmeli firmalar için *Software Bill of Materials (SBOM)* zorunluluğu getirilmiş olup, bu uygulamanın Nİ cihazlarındaki tedarik zinciri risklerini azaltmak amacıyla kullanılabileceği ifade edilmektedir. Her iki örnek dikkate alındığında, ağırlıklı olarak siber güvenliği sağlamaya yönelik uygulamalar oldukları görülmektedir. Bu uygulamalar her ne kadar kapitalist yöntemlerle kazanç elde eden şirketleri engelleme potansiyeline sahip olmasa da kötü amaçlı saldırıları önleme ve güvenliği sağlama açısından önem taşımaktadır.

Uzmanların bir kısmı, kullanıcıların farkındalık seviyesinin gizliliğin sağlanması yolunda önemli bir kısıt oluşturduğunu belirtmektedir. Bu nedenle, kullanıcı farkındalığının artırılmasının, çeşitli okuryazarlık eğitimlerinin sağlanması koşuluyla mümkün olabileceği yönünde görüşler dile getirilmektedir. Örneğin uzman 7 bu konuyla ilgili şu ifadelerle yer vermektedir:

“Hem gizlilik hem de teknolojik cihazların kullanımı hususunda okuryazarlığın artırılması önemlidir. Bireylerin hak ve özgürlükleri başta olmak üzere cihaz tasarımları ve minimum gereklilikler konusunda bilinçlendirilmesi, büyük teknoloji şirketlerini de uyumlu olmaya ve daha iyi uygulamalara itecektir. Zira bilinçli kullanıcılar, daha iyi ve bilinçli tercihler yaparak sektörün aktörlerini daha iyi uygulamalar ve politikalar benimsemeye zorlayabilecektir.”

Kullanıcıların bilinçlendirilmesi hususunda uzman 5'in de görüşleri bulunmaktadır:

“Kullanıcıların bilinçlenmesi için eğitimler gereklidir. Gizlilik ve teknoloji okuryazarlığı eğitimlerinin verilmesi gerektiğini hatta bu eğitimlerin ilkökul seviyesinden itibaren verilmesi gerektiğini düşünüyorum.”

Bu doğrultuda, dijital okuryazarlık, veri okuryazarlığı ve mahremiyet bilinci gibi konuların erken yaşlardan itibaren eğitim sistemine entegre edilmesi gerektiği vurgulanmaktadır. Özellikle kişisel verilerin ne şekilde toplandığı, işlendiği ve paylaşılacağına dair temel bilgilerle donatılan bireylerin, gizlilik tercihlerini daha bilinçli şekilde yönetebileceği savunulmaktadır. Ayrıca, kullanıcıların yalnızca teknik bilgilere değil, aynı zamanda veriye dayalı iş modellerinin etik ve toplumsal etkilerine dair bilgiye de sahip olmaları, veri koruma süreçlerine aktif katılımlarını mümkün kılacaktır.

Genel olarak kullanıcıların farkındalık seviyelerinin yüksek olması gizliliğin dolaylı olarak sağlanabileceğine dair argümanlar yer almaktadır. Ancak bir uzman bu konuda şüpheleri olduğunu dile getirmiştir. Dolayısıyla onun görüşlerini de belirtmek önemlidir. Uzman 3 şöyle ifade etmektedir:

“Elbette, çoğu tüketicinin teknoloji şirketlerinin hangi verileri topladığı ya da bu verileri nasıl kullandığı hakkında tam bilgi sahibi olmadığı söylenebilir, fakat her şeyi bilselerdi bile farklı bir karar verip vermeyecekleri konusunda emin değilim.”

4.4. Araştırmanın Sonucu

Bu araştırmada, gözetim kapitalizmi modelinin nesnelerin interneti üzerinden nasıl işlediği ve uzmanların bu konuya ilişkin bakış açıları ortaya konulmaya çalışılmıştır. Ayrıca, gözetimin artık yalnızca çevrimiçi ortamda değil, her zaman ve her yerde yayılmasına olanak tanıyan nesnelerin interneti gözetimi sorununa karşı hangi gizlilik çözümlerinin mevcut olduğu, bu çözümlerin başarı düzeyleri ve hangi çözümlerin geliştirilebileceği ele alınmıştır. Buna ek olarak, nesnelerin interneti teknolojileri yoluyla gerçekleşen gözetim olgusu, uzmanların görüşleri doğrultusunda hem ekonomi-politik hem de mahremiyet sorunsalı perspektiflerinden incelenmiştir. Veriler, toplamda 10 katılımcı ile yapılan ve derinlemesine görüşmenin bir türü olan uzman görüşmelerinden elde edilmiştir.

Toplamda beş adet açık uçlu soru oluşturulmuştur. Bu sorular, içerik olarak gözetim kapitalizmi ekseninde nesnelerin interneti, fiziksel mekâna yayılan nesnelerin interneti uygulamaları, nesnelerin interneti gözetimine karşı geliştirilen mevcut gizlilik yöntemleri ve uzmanların önerdiği mahremiyet çözümlerini içermektedir. Uzmanlardan elde edilen veriler doğrultusunda tematik bir sınıflandırma yapılmıştır. Bu sınıflandırma; ekonomi-politik çerçevede nesnelerin interneti, nesnelerin interneti teknolojileriyle gözetimin yaygınlaşması ve derinleşmesi, nesnelerin interneti ile yaşanan mahremiyet sorunları, çözüm önerileri bağlamında teknik ve yapısal görüşler ile devlet politikaları bağlamında yapılabilecek uygulamalar temalarını içermektedir.

Öncelikle teknoloji şirketlerinin veri temelli gelir modelleri değerlendirilmiş ve bunun nesnelerin interneti üzerindeki yansımalarına dikkat çekilmiştir. Bu bağlamda ortaya çıkan etik,

ekonomik ve toplumsal sonuçlar analiz edilmiştir. Uzmanların büyük çoğunluğu, şirketlerin bu gelir modellerini eleştirmiş ve gelir elde etme biçimlerinin kapitalist bir yapıya dayandığını belirtmiştir. Ancak veri toplamanın bağlama bağlı olarak olumlu kullanım alanlarının da olabileceği; özellikle küçük ölçekli geliştiricilerin bu süreçte daha meşru motivasyonlara sahip olabileceği yönünde farklı görüşler de dile getirilmiştir.

Şirketlerin veri toplama ve işleme şekillerinin olumsuz olmadığını düşünen uzmanlar çoğunlukla bu eylemlerin kamu yararını amaçladığını ifade etmektedir. Ancak şirketlerin çıkarları ile kamu yararının bir arada bulunması etik meşruiyet ile ekonomik çıkarlar arasında bir belirsizlik doğurmakta ve bu durum, toplumsal fayda adı altında gerçekleştirilen veri temelli ticarileşmeyi ortaya koymaktadır. Buna ek olarak küçük ölçekli bağlanılabilir teknoloji firmaları ile büyük teknoloji şirketleri arasında var olan güç asimetrisi onların daha agresif veri işleme yöntemlerine başvurmasına yol açmakta ve bu durum meşru bir zemine oturtulmaktadır. Sonuç olarak bu durum piyasadaki tekelleşmeyi daha da hızlandırmaktadır.

Her şeyin daha fazla “akıllılaştırılması” ve gündelik yaşamın her ayrıntısına entegre edilmesi, gözetim pratiklerinin artmasına ve derinleşmesine zemin hazırlamaktadır. Nesnelerin interneti teknolojilerinin yaygınlaşmasıyla birlikte gözetimin daha da derinleştiği iddiasına uzmanlar genel olarak katılmaktadır. Ancak bazı uzmanlar, gözetimin derinleşmesi konusunun verinin niceliği ve niteliği bakımından ele alınması gerektiğini vurgulamaktadır. Dolayısıyla gözetim yoğunlaşmasının yalnızca verinin miktarıyla değil, verinin kişisel olup olmadığı ve bireylerle ilişkilendirilebilirliği gibi unsurların da dikkate alınması gerektiği ifade edilmektedir. Ayrıca, konu nesnelerin interneti özelinde incelendiğinde, eleştirinin yalnızca gözetim kapitalizmi odağından değerlendirilmesinin yetersiz olduğu belirtilmektedir. Zira gözetim kapitalizmi ağırlıklı olarak birey-şirket ilişkisi üzerinden ele alınmakta ancak nesnelerin interneti gözetimi, şirketler arası ve hatta devlet aktörleri arasındaki ilişkileri de içeren çok taraflı bir yapıya sahiptir.

Nesnelerin İnterneti teknolojileri, sunduğu kolaylıklar ve hizmetlerin yanı sıra ciddi mahremiyet sorunlarını da beraberinde getirmektedir. Hem kullanıcıların hem de kullanıcı olmayan kişilerin mahremiyetini etkilemesiyle bu sorun artık yalnızca bireysel değil aynı zamanda toplumsal bir mesele haline gelmiştir. Dolayısıyla Mahremiyetin korunması, sadece bireylerin değil toplumun bütününe dijital geleceği açısından stratejik bir gereklilik hâline gelmiştir. Öte yandan her nesnelerin interneti cihazının mahremiyet riski taşıdığı da söylenemez. Mevcut bazı örnekler kullanıcı verileri veya tanımlanabilecek veriler olmadan da cihazların amaçlarına ulaşabildiğini göstermektedir.

Uzmanların çözüm önerileri dikkate alındığında, 'teknik çözümler' ve 'devlet politikaları bağlamında yapılabilecek uygulamalar' olmak üzere iki ana tema oluşturulmuştur. Uzmanların çoğu, mevcut teknik çözümlerin tam anlamıyla gizlilik garantisi sunmadığını ifade etmekte; özellikle anonimleştirme yöntemini eleştirerek, bu yöntemin tahmini modelleme yoluyla tersine çevrilebileceğini savunmaktadır. Tasarımda gizlilik yaklaşımlarından biri olan *veri minimizasyonu* ilkesi, etkili bir gizlilik stratejisi olarak önerilmektedir. Bu doğrultuda, mümkün olduğunca az veri toplanması ve verilerin cihaz içinde işlenip saklanması gerektiği vurgulanmaktadır. Sonuç olarak, uzmanlar teknik çözümlerin tek başına yeterli olmadığını, bunların hukuki, yapısal ve toplumsal düzenlemelerle desteklenmesi gerektiğini belirtmektedir. *Kullanıcı bilinci ve teknoloji okuryazarlığının artırılması*, bireylerin verilerini korumada daha etkin olmalarını sağlayacaktır. Birçok uzman, kullanıcılara verileri üzerinde *doğrudan kontrol* sağlanması, sade bir dille hazırlanmış sözleşmelerin sunulması ve *şeffaflık* ilkelerinin benimsenmesi gerektiğini ifade etmektedir.

5. SONUÇ

Gözetim olgusu, tarih boyunca çeşitli nedenlerle varlığını sürdürmüştür. Kimi zaman iktidarların kontrol ve tahakküm arzusu doğrultusunda, kimi zaman güvenlik kaygısıyla, kimi zaman ise şirketlerin gelir modellerine katkı sağlamak amacıyla uygulanarak kapitalist sermaye birikiminin bir aracı olmuştur. Sanayi toplumunda işçi üretkenliğini arttırmak için gözetim bir araç olarak kullanılarak artı değerın maksimize edilmesi hedeflenmiştir. Benzer şekilde dijital kapitalizmde de kullanıcıların daha detaylı profillenmesi ve daha iyi kişiselleştirilmesi verimliliği ve artı değeri arttırarak sermaye birikimini maksimize etmektedir. Bu çarkın döndürülebilmesi için de olabildiğince veri toplanması gerekmektedir. Bu durum ise kullanıcıların daha fazla gözetlenmesiyle sonuçlanmaktadır.

Kapitalizmin önemli bir aracı haline gelen gözetim teknolojileri, günümüzde özellikle makine öğrenmesi, yapay zekâ ve gelişmiş algoritmalar aracılığıyla kullanıcı ve ortam verilerini toplayarak büyük ölçüde beslenmektedir. Tarihsel olarak kapitalizm, sürekli olarak bir şeyi metalaştırarak varlığını sürdürmüştür. Bugünün gözetim kapitalizmi bağlamında ise veri, yeni bir meta haline gelmiştir. Kesintisiz biçimde üretilen ve akan veriler, gözetim kapitalizminin bitmek bilmeyen kârlı sonuçlarını beslemektedir.

İnsan davranışlarını bir tür hammaddeye dönüştürerek sermaye birikimi sağlayan gözetim kapitalizmi modeli; çevrimiçi ortamda kullanıcıların gerçekleştirdiği aramaların, bu aramalar üzerindeki davranış biçimlerinin izlenmesi, buradan verilerin elde edilmesi, analiz edilmesi ve işlenmesi süreçlerine dayanmaktadır. Bu süreç sonunda kullanıcıya dair bir profil çıkarılarak, doğru zaman ve doğru yerde hedeflenmiş reklamların sunulması temel amaçlardan biri haline gelmiştir. Başlangıçta çevrimiçi alanla sınırlı olan bu gözetim süreci, zamanla genişleyerek fiziksel mekâna da sızmıştır. Webde var olan gözetim, zamanla keşfedilecek bir alanın kalmamasına işaret ederken gözetim teknolojilerinin fiziksel mekânı içerisine alacak şekilde genişlemesi hem sermaye sahiplerinin çıkarları ile uyumlu olmuş hem de devletlerin denetim mekanizmalarını güçlendiren bir ekosistemin doğmasına yol açmıştır.

Gözetim teknolojilerinin fiziksel mekâna yayılmasıyla birlikte zaman ve mekân sınırları ortadan kalkmış, gözetim daha da yoğunlaşmıştır. Özellikle nesnelerin interneti teknolojilerinin yaygınlaşmasıyla bu durum daha belirgin hale gelmiştir. Şehirlere, evlere ve hatta bedenlere nüfuz eden akıllı teknolojiler, kullanıcı ve ortam hakkında her an ve her yerde verileri toplanabilir hâle getirmiştir. Bu gelişmeler, kapitalizmin yeni bir biçimi olarak insan yaşamının her anının sermayeye dönüştürülmesiyle sonuçlanmıştır.

Nesnelerin İnterneti teknolojilerinin fiziksel mekânı kuşatması, mahremiyet sorunlarının yaşanmasına neden olmaktadır. Üstelik mahremiyet ihlali riskleri yalnızca akıllı cihaz kullanıcılarını

değil kullanıcı olmayan üçüncü şahısların da mahremiyetini risk altına alarak bu meselenin yalnızca bireysel değil toplumsal bir düzlemde ele alınması gereken bir mesele olduğunu ortaya koymaktadır. Bu teknolojilerin mekânı, bedeni ve insan hareketliliğini içine alacak şekilde genişlemesi kullanıcı tarafından mahremiyet meselesinin ele alınmasını gerektirmektedir. Güvenlik sorunları yalnızca kötü amaçlı saldırılar çerçevesinde değerlendirilmemeli; şirketlerin kullanıcı verilerini işlemesi ve bu veriler üzerinden kullanıcıları tanımlaması da bir gizlilik ihlali olarak ele alınmalıdır. Buradan hareketle nesnelerin internetini ekonomik politik bağlamda incelemek önem arz etmektedir. Dolayısıyla nesnelerin interneti ile gözetim kapitalizminin daha da derinleşmesi sorunsalı bu araştırmanın temelini oluşturmaktadır. Bu durum önemli bir sorun olarak görülmüş ve buna karşı alınabilecek önlemlerin araştırılması gerekli bulunmuştur. Bu araştırmanın hedeflerinden biri ortaya konulan mahremiyet sorunsalına karşı mevcut gizlilik çözümlerinin ne derece çare olup olmadığını anlamaktır. Bu bağlamda gizlilik çözümlerinin güç eşitsizliğini gidermedeki yeterliliğini sorgulamak, yöntemlerin yetersiz olduğu düşünülen yanlarını ortaya koymak ve teknik olarak gizlilik çözümleri yeterli olsa dahi bu yöntemlerin uygulanmasının ardındaki toplumsal etkiyi ve ekonomi politik ilişkileri daha açık hale getirmek amaçlanmaktadır. Araştırma kapsamında nitel araştırma yöntemi tercih edilmiş olup uzman görüşmesi veri toplama tekniği kullanılmıştır. Uluslararası düzeyde bir katılımcı listesi oluşturulmuş ve dünyanın farklı ülkelerinden toplam 10 uzmanla görüşülmüştür. Uzmanlar, ABD, Hollanda, Almanya, Macaristan, Finlandiya, İspanya ve Avustralya ülkelerinden katılım sağlamıştır. Uzmanlar, nesnelerin interneti, veri gizliliği, güvenlik teknolojileri ve veri koruma hukuku gibi alanlarda çalışmalar yapan akademisyen ve araştırmacılardan oluşmaktadır.

Araştırma sonucunda çıkan bulgulara göre uzmanlar, genel olarak nesnelerin interneti teknolojilerinin gözetim kapitalizmini yoğunlaştırdığı iddiasını kabul etmektedir. Ayrıca mevcut gizlilik çözümlerinin teknik olarak teoride yeterli olduğunu, ancak bu çözümlerin verimli bir şekilde uygulanamamasını ve bilgi ile güç asimetrilerini giderememesini ekonomik ve politik nedenlere dayandırmaktadır.

Öncelikle uzmanlardan, veri temelli ekonomik gelir elde eden şirketlere bakış açılarını ve bu bağlamda nesnelerin internetini nasıl değerlendirdiklerini açıklamaları istenmiştir. Sonuçlara göre, uzmanların bir kısmı şirketlerin sermaye birikim modellerini kapitalist bir sistem çerçevesinde değerlendirmenin doğru olacağını belirtirken bir kısmı ise kullanıcı verilerinin kullanılmasını hizmetlerin geliştirilmesi açısından gerekli görmektedir.

Birçok cihaz ve uygulamalarda kullanıcılara hizmet gelişimi için verilerin kullanıldığı bilinmektedir. Hatta Google'ın erken dönemlerinde atık veri olarak görülen kullanıcı davranışlarına ilişkin veriler, zamanla büyük bir ekonomik potansiyel taşıdığı fark edilerek sistemli bir şekilde

toplanmaya ve analiz edilmeye başlanmıştır. Google'ın bu verileri keşfetmesi, şirketin iş modelinde köklü bir dönüşüm yaratarak reklam odaklı gelir stratejilerinin merkezine bu verileri yerleştirmesine yol açmıştır. Böylece veri, yalnızca hizmet kalitesini artırmanın bir aracı olmaktan çıkmış, doğrudan ekonomik değeri olan bir sermaye unsuruna dönüşmüştür. Bu dönüşüm, özel şirketlerin veri üzerinde kurduğu tahakküm karşısında kamu yararı ile şirket çıkarları arasındaki dengenin sorgulanmasını gerektirmektedir. Kullanıcı verilerinin hizmet gelişimi için kullanılmasının meşrulaştırılması kapitalist gelir modeliyle kamu yararı arasında bir gerilim ortaya çıkarmaktadır. Çünkü kâr ile kamu yararının bir arada bulunması etik ve politik meşruiyet sınırlarını bulanıklaştırmaktadır. Dolayısıyla bu durum, değer üretiminin toplumsal fayda kisvesi altında ticarileştirilmesi sonucunu ortaya koymaktadır.

Diğer yandan nesnelerin interneti teknolojilerinin yayılan ve sınır tanımayan yapısının, gözetim kapitalizmi kavramını da aşan bir dünyayı temsil ettiğiidir. Çünkü bu teknolojilerin gözetim üzerindeki etkisi, yalnızca birey-şirket odağında ele alınamayacak kadar geniş, katmanlı ve karmaşıktır. Örneğin, toplumsal olaylarda ya da kriz anlarında dünyanın pek çok yerinde olduğu gibi COVID-19 pandemisi sırasında da devletlerin vatandaşlarını fiziksel mekânda izleme pratiklerinin önemli bir kısmı, nesnelerin interneti tabanlı teknolojiler üzerinden gerçekleştirilmiştir. Bununla birlikte, bu gözetim ilişkileri yalnızca devlet ve vatandaş arasında değil; teknoloji şirketleri, altyapı sağlayıcıları, güvenlik kurumları ve hatta uluslararası platformlar gibi birçok farklı aktör arasında da şekillenmektedir. Bu durumda, bireyin mahremiyetinin ve özgürlüklerinin sınırlarını kimin belirleyeceği önemli bir soru olarak gündeme gelmektedir. Bu noktada devreye hukukun girmesi kaçınılmazdır. Elbette sınırları yasaların çizmesi beklenir ancak mevcut yasal düzenlemeler çoğu zaman teknolojik gelişmelerin gerisinde kalmakta, uygulamada yetersiz kalmakta veya çok uluslu teknoloji aktörlerinin baskın gücü karşısında etkisizleşmektedir. Bu nedenle, yalnızca teknik değil aynı zamanda etik, toplumsal ve hukuki açıdan da yeni bir denge ve denetim mekanizmasına duyulan ihtiyaç her geçen gün daha da belirginleşmektedir.

Hukuki düzenlemelerin gözetim ilişkilerini denetlemedeki rolü tartışılırken, ekonomi politik bir çerçeveden bakıldığında iki temel nokta öne çıkmaktadır. Birincisi, uzmanlar gözetim uygulamalarını sınırlamak ve şirketleri denetlemek için yasaların gerekliliğine işaret etse de bu yasaları koyan devletler aynı zamanda gözetimin baş aktörleridir. Yani hem toplum üzerinde denetim kurmak adına gözetim teknolojilerini kullanan hem de vatandaşın mahremiyetini korumakla yükümlü olan aktör devlettir. Bu çelişki, yasa koyucunun aynı zamanda gözetleyen iktidar olması gerçeğini yansıtmaktadır. Dahası, devlet ile teknoloji şirketleri arasındaki güç ilişkisi, yasaların nasıl biçimlendirileceği konusunda kritik bir rol oynamaktadır. Örneğin Elon Musk ile ABD devleti arasındaki yakın iş birlikleri, şirket-devlet ilişkilerinin şeffaflıktan uzak ve güç temelli yapısını gözler önüne sermektedir. Bu durum, yasaların tarafsız bir denetim mekanizması olma potansiyelini sorgulamakta, hukukî düzenlemelerin sınırlarını

görünür kılmaktadır. İkinci olarak ise, şirket çıkarlarının kamusal yarar karşısında sistematik olarak öncelik kazanmasının ardında Neo-liberal politikaların etkisi yatmaktadır. Neo-liberalizmle birlikte sosyal devlet anlayışı zayıflamış, kamu kurumları özelleştirilmiş ve devletin birçok alandaki düzenleyici rolü piyasanın lehine geri çekilmiştir. Bu koşullar altında çıkarılan yasalar da kaçınılmaz olarak sermaye sahiplerinin mülkiyet haklarını korumaya odaklanmakta; bireyin mahremiyet hakkı ise ikincil bir mesele hâline gelmektedir. Dolayısıyla, gözetim ve hukuk arasındaki ilişkiyi anlamak için yalnızca normatif düzenlemelere değil, bu düzenlemelerin arkasındaki iktidar ilişkilerine ve ideolojik altyapıya da dikkatle bakmak gerekmektedir.

Mevcut gizlilik yaklaşımlarının mahremiyet ihlallerini engelleme olasılıkları tartışılmıştır. Bu bağlamda teknik birçok yaklaşımın belli bir yere kadar güvenliği sağlayabileceği ancak tam anlamıyla güvenlik garantisi sunmayacağı sonucuna ulaşılmıştır. Özellikle anonimleştirme tekniklerinin tahmine dayalı saldırılarda kolay bir şekilde tersine çevrilebileceği tespit edilmiştir. Yaşanan mahremiyet ihlallerine karşı gizliliğin sağlanmasına yönelik farklı bağlamlarda çözüm önerileri sunulmuştur. Teknik yaklaşımlar çoğunlukla veri minimizasyonu ve kullanıcı ara yüzlerinin doğru tasarlanması yönünde olmuştur. Bununla beraber tasarımda gizlilik yaklaşımları ve diferansiyel gizliliğin de cihazın türüne göre başarılı sonuçlar verebileceği yönünde görüşler belirtilmiştir. Bu tür teknik gizlilik çözümleri mevcut varlıklarıyla her ne kadar değerli olsa da gözetim kapitalizmi şirketlerinin agresif bir şekilde veri çıkarma ve işleme operasyonlarını engelleme noktasında yetersizdir. Dolayısıyla bu soruna yalnızca teknik çözümler odağında yaklaşmak ve etkili teknik yöntemler geliştirmeye devam etmek sürecin sonu değildir. Çünkü zaman ve mekân sınırlarını aşan bu gözetim biçimi, geniş ekonomik ve politik bağlamlarla ilişkili olduğu için, gizlilik çözümlerinin tek bir yönetime indirgenmesi etkili olmayacaktır. Sonuç olarak uzmanların birçoğunun da belirttiği üzere teknik çözümler ne kadar başarılı olursa olsun yasal uygulamalarla desteklenmesi gerekmektedir. Böylelikle gizliliği sağlama ve veri koruma noktasında hem teknik hem de yasal düzlemde ele alınacak çözümler bir araya getirilmeli ve iş birliği yapılmalıdır.

Gizliliğin sağlanması ve veri koruma alanında geliştirilebilecek çözüm önerilerinden biri de politikalar ışığında yapılması gereken dijital ve gizlilik okuryazarlığı eğitimlerinin yaygınlaşmasıdır. Bu tür eğitimlerin önemli farkındalıklar oluşturduğu kabul edilmelidir çünkü kapitalist birikim modelinin arka planda nasıl işlediğine dair bilgi sahibi olmanın, kullanıcıların verilerini sahiplenme konusunda daha bilinçli olmalarını sağlayacağı düşünülmektedir. Ancak bu eğitimlerin bireysel düzlemde ele alındığını hatırlatmak gerekir. Bu tür bireysel girişimlerin yapısal sorunları tek başına çözebileceğini varsaymak özellikle ekonomi politik bir perspektiften bakıldığında oldukça sınırlı bir yaklaşımdır. Çünkü mevcut dijital ekosistemde birey ile büyük teknoloji şirketleri ve devlet kurumları arasında ciddi

bir güç asimetrisi bulunmaktadır. Bu denli derinleşmiş bir eşitsizlik ortamında bireyin farkındalık geliştirmesi elbette değerli olsa da bu çabanın sistemdeki yapısal açıkları kapatması mümkün değildir. Ayrıca, eleştirel bir dünya görüşüne sahip olmadan edinilen teknik bilginin, örneğin bir gizlilik ayarını nasıl değiştireceğini bilmenin, bireyi bütüncül olarak güçlendirmesi beklenemez. Gizlilik okuryazarlığı bu anlamda önemli bir araçtır ancak politik bilinçle birleştiğinde anlamlı ve dönüştürücü olabilir. Bu bağlamda, bağımsız araştırmacıların, sivil toplum kuruluşlarının ve dijital haklar aktivistlerinin rolü büyük önem taşımaktadır. Nitekim uzmanlardan biri de yalnızca bireysel farkındalık değil, kolektif bilinç ve eleştirel yaklaşımın da bu mücadelede temel olduğunu vurgulamıştır.

Diğer taraftan, nesnelerin interneti cihazlarının, kullanıcılarına veri toplama ve işleme faaliyetleri hakkında yeterli aydınlatma yapma yükümlülüğü dikkate alınmalıdır. Kullanıcıların hem veri işlemeye ilişkin güncel gizlilik politikalarını görüntüleyebildiği hem de tercihlerini yönetebildiği dijital platformların kurulmasının hem rızanın güncelliğini hem de şeffaflığı teşvik edeceği düşünülmektedir. Aynı zamanda, kullanıcıların cihazı kullanmak için bilinçli rıza göstermesi ve gerçek rıza koşullarının sağlanması önemlidir. Yalnızca “kabul et” seçeneğinin sunulması ve bu seçenek kabul edilmediğinde cihazın kullanımına izin verilmemesi, kullanıcının özgür iradesiyle rıza göstermediği sonucunu ortaya çıkarmaktadır. Bir sorun olarak ele alınması gereken bu duruma karşı, politik karşı duruşların geliştirilmesi gerekmektedir. Yine aynı bağlamda, çözüme kavuşturulması gereken bir diğer sorun, kullanıcı sözleşmelerinin anlaşılması güç ifadelerle hazırlanması ve kullanıcının sözleşmeyi okumaya yeterli zamanı ayırmaması nedeniyle doğrudan kabul etmesidir. Sözleşmelerin daha açık ve sade bir dille hazırlanması gerekmektedir. Ayrıca araştırmada ortaya çıkan sonuçlardan biri, sözleşmelerin sade bir dille hazırlanması anlayışının kime ve neye göre belirleneceğinin önemli olduğudur. Kullanıcı sözleşmelerinin yaş, eğitim düzeyi veya meslek gruplarına göre hazırlanmasının önemine dikkat çekilmektedir.

Bu tezde nesnelerin interneti, gözetim kapitalizminin derinleşen yapısıyla ilişkili olarak, eleştirel bir ekonomi politik perspektiften değerlendirilmiştir. Dijital gözetimin yalnızca çevrimiçi ortamlarla sınırlı kalmayıp fiziksel mekâna, bedene ve hareketliliğe kadar genişlemesi, veri temelli kapitalist birikim süreçlerinin yeniden şekillendiğini göstermektedir. Nesnelerin interneti teknolojilerin işlevselliği ve potansiyeli inkâr edilmese de bu teknolojilerin sermaye birikimini ve devletin denetim kapasitesini artıran yönleri baskın hâle gelmekte ve mahremiyet hakkı giderek daha karmaşık bir sorun alanına dönüşmektedir. Bu bağlamda gizlilik çözümleri teknik açıdan belirli imkânlar sunsa da güç asimetrisini ortadan kaldırmak için yetersiz kalmaktadır. Bu çözümlerin etkililiği, mevcut ekonomik ve siyasi yapılarla yakından ilişkilidir. Öte yandan bireysel bilinçlenme ve dijital okuryazarlık çabaları önemli olmakla birlikte, çözümün yalnızca bireye yüklenmesi, yapısal eşitsizlikleri göz ardı etmek

anlamına gelmektedir. Sonuç olarak bu tez, gizlilik çözümlerinin etkinliğini yalnızca teknik düzeyde değil, aynı zamanda bu çözümleri şekillendiren iktidar ilişkileri, mülkiyet yapıları ve yasal çerçeveler bağlamında sorgulayan eleştirel bir perspektif sunmaktadır.

Çalışmanın teorik kısmında hesaplamalı gizlilik yaklaşımları bölümünde bulunan blok zinciri ve kişisel bilgi yönetim sistemleri hakkında görüş belirtilmemiştir. Dolayısıyla gelecek çalışmalarda bu iki konu özelinde durulması hedeflenmektedir. Blok zincirinin merkeziyetsiz yapısı ve kendine özgü karakterinin veri koruma açısından ne derece başarılı olabileceğinin araştırılması hedeflenmektedir. Bir diğer yandan gözetim kapitalizmi ekosisteminde kullanıcı davranışlarının manipüle edilmesine yönelik disiplinler arası faaliyetleri gün yüzüne çıkarmak hedeflenmektedir. Özellikle davranışların manipüle edilmesinde psikolojik süreçlerin etkili olduğunu ispat eden bilişsel bilim çalışmaları ve nöro-ekonomik çalışmalara yer verilerek ekonomi-psikoloji-teknoloji birlikteliğinin gelecek çalışmalarda bulunacağı öngörülmektedir. Son olarak yapay zekâ teknolojilerinin hızlı gelişimi birçok unsuru ve kavramı değiştirdiği gibi nesnelerin interneti kavramına da sirayet etmiştir. Özellikle yeni çıkan AIoT kavramı AI (yapay zekâ) ile IoT (nesnelerin interneti) kavramlarının birleşimini ifade etmektedir ve yapay zekâ destekli nesnelerin interneti gün geçtikçe daha da hızlı gelişmeye devam edecektir. Dolayısıyla bu kavramsallaştırma özelinde gelecek çalışmalara yer verilmesi hedeflenmektedir.

KAYNAKLAR

- Ahmadzai, M., & Nguyen, G. (2023). Federated Learning with Differential Privacy on Personal Opinions: A Privacy-Preserving Approach. *Procedia Computer Science*, 225. <https://doi.org/10.1016/j.procs.2023.10.039>
- Ahn, S. (2021). Stream your brain! Speculative economy of the IoT and its pan-kinetic dataveillance. *Big Data & Society*, 8(2). <https://doi.org/10.1177/20539517211051973>
- Al-Fuqaha, A., Guizani, M., Mohammedi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE*, 17(4). <https://doi.org/10.1109/COMST.2015.2444095>
- Almuhimedi, H., Schaub, F., & Sadeh, N. (2015). Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 787-796. <https://doi.org/10.1145/2702123.2702210>
- Aradau, C., & Blanke, T. (2015). The (Big) Data-security assemblage: Knowledge and critique. *Big Data & Society*, 2(2). <https://doi.org/10.1177/2053951715609066>
- Asemani, M., Abdollahei, F., & Jabbari, F. (2019). *Understanding IoT Platforms Towards a comprehensive definition and main characteristic description*. International Conference on Web Research (ICWR), Tehran. <https://doi.org/10.1109/icwr.2019.8765259>
- Avcı, İ. (2022). Akıllı Evlerde IoT Teknolojileri ve Siber Güvenlik. *Avrupa Bilim ve Teknoloji Dergisi*, 34. <https://doi.org/10.31590/ejosat.1080228>
- Barocas, S., & Nissenbaum, H. (2014). Big Data's End Run Around Procedural Privacy Protections. *Communications of the ACM*, 57(11), 31-33. <https://doi.org/10.1145/2668897>
- Bogost, I. (2015). The Cathedral of Computation. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2015/01/the-cathedral-of-computation/384300/>
- Boyd, Danah, & Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication & Society*, 15(5). <https://doi.org/10.1080/1369118X.2012.678878>
- Bozkurt, V. (2001). Gözetim ve İnternet: Özel Yaşamın Sonu mu? *İş, Güç Endüstri İlişkileri ve İnsan Kaynakları Dergisi*, 3(2).
- Brandom, R. (2016). Police are filing warrants for Android's vast store of location data. *The Verge*. <https://www.theverge.com/2016/6/1/11824118/google-android-location-data-police-warrants>
- Canbay, Y., & Sağiroğlu, Ş. (2020). Derin Öğrenmede Diferansiyel Mahremiyet. *ULUSLARARASI BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ DERGİSİ*, 6(1), 1-12. <https://doi.org/10.18640/ubgmd.750310>

- Castiglioni, V., Chatzikokolakis, K., & Palamidessi, C. (2020). A logical characterization of differential privacy. *Science of Computer Programming*, 188. <https://doi.org/10.1016/j.scico.2019.102388>
- CBC (Direktör). (2020). *I resigned in protest from Sidewalk Labs' "smart city" project over privacy concerns* [Video recording].
- Cheshire, T. (2016). Behind the scenes at Donald Trump's UK digital war room. *Sky news*. <https://news.sky.com/story/behind-the-scenes-at-donald-trumps-uk-digital-war-room-10626155>
- Collins, K. (2017). Google collects Android users' locations even when location services are disabled. *Quartz*. <https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled>
- Couldry, N., & Mejias, U. A. (2022). *Bağlantının Bedelleri* (G. Boztepe, Çev.; 1. bs). Nota bene bilişim.
- Couldry, N., & Mejias, U. A. (2024). *Q and A with Nick Couldry and Ulises A Mejias on Data Grab* [Mülakat]. https://eprints.lse.ac.uk/123475/1/lsereviewofbooks_2024-4-30--q-and-a-with-nick-couldry-and-ulises-a-mejias-on-data-grab.pdf
- Çubukcu, Z. (2024). Dijital Çağda Kişisel Verilerin Korunmasında Veri Koruma Otoritelerinin Rolü. *TOPLUM, EKONOMİ VE YÖNETİM DERGİSİ*, 5(3). <https://doi.org/10.58702/teyd.1485163>
- De Montjoye, Y.-A. (2015). *Computational Privacy: Towards Privacy-Conscientious Uses of Metadata* [Media Arts and Sciences]. Massachusetts Institute of Technology.
- Delrobaei, M., Memar, S., Pieterman, M., Stratton, T. W., McIsaac, K., & Jog, M. (2018). Towards Remote Monitoring of Parkinson's Disease Tremor using Wearable Motion Capture Systems. *Journal of the Neurological Science*, 384, 38-45.
- Dilmen, N. E. (2020). *Konumsal Medya Dijital Çağda Mekan Üzerine Disiplinlerarası Tartışmalar* (C. Tokgöz & B. Aydoğan, Ed.). Siyasal Kitabevi.
- Dolgun, U. (2008). *Şeffaf Hapishane yahut Gözetim Toplumu*. Ötüken.
- Dwork, C. (2006). Differential privacy. İçinde M. Bugliesi & B. Preneel (Ed.), *ICALP'06: Proceedings of the 33rd international conference on Automata, Languages and Programming—Volume Part II*. Springer-Verlag. https://doi.org/10.1007/11787006_1
- European Parliament and Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

- Evenson, K. R., Goto, M. M., & Furberg, R. D. (2015). Systematic review of the validity and reliability of consumer-wearable activity trackers. *International Journal of Behavioral Nutrition and Physical Activity*, 12(1). <https://doi.org/10.1186/s12966-015-0314-1>
- Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. *Smart Cities*, 6. <https://doi.org/10.3390/smartcities6010027>
- Foucault, M. (1995). *Deliliğin Tarihi* (2. bs). İmge kitabevi.
- Fuchs, C. (2014). Bilişsel Kapitalizm ya da Enformasyonel Kapitalizm? Enformasyonel Ekonomide Sınıfın Rolü (D. Saraçoğlu, Çev.). İçinde M. A. Peters & E. Bulut (Ed.), *Bilişsel Kapitalizm! Eğitim ve Dijital Emek*. NotaBene.
- Fuchs, C. (2020). *Sosyal Medya Eleştirel Bir Giriş* (D. Saraçoğlu & İ. Kalaycı, Çev.; 2. bs). Nota bene bilişim.
- Fuchs, C. (2021). *Dijital Kapitalizm Çağında Marx'ı Yeniden Okumak* (D. Saraçoğlu, Çev.). Nota bene bilişim.
- Gang, G., Zeyong, L., & Jun, J. (2011). *Internet of Things Security Analysis*. International Conference on Internet Technology and Applications. <https://doi.org/10.1109/itap.2011.6006307>
- Gellman, B., & Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post*. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
- Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. <https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>
- Guo, E. (2023). Roomba testers feel misled after intimate images ended up on Facebook. *MIT Technology Review*. <https://www.technologyreview.com/2023/01/10/1066500/roomba-irobot-robot-vacuum-beta-product-testers-consent-agreement-misled/>
- Gustavsson, S. (2020). *An Assessment of Privacy by Design as a Stipulation in GDPR* [Uppsala Universitet]. <https://www.diva-portal.org/smash/get/diva2:1446745/FULLTEXT01.pdf>
- Gümüş, H. T., & Eyüpoğlu, C. (2022). BÜYÜK VERİDE ANONİMLEŞTİRME TEKNİKLERİ VE SALDIRI TÜRLERİ: UYGULAMA ÖRNEKLERİ. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi*, 21(42).
- Gündüz, M. Z., & Daş, R. (2017). Nesnelerin interneti: Gelişimi, bileşenleri ve uygulama alanları. *Pamukkale Üniversitesi Mühendislik Bilimleri Dergisi*, 24(2). <https://doi.org/10.5505/pajes.2017.89106>

- Harbath, K., & Fernekes, C. (2023). History of the Cambridge Analytica Controversy. *Bipartisan Policy Center*.
- Hoepman, J.-H. (2022). *Privacy Design Strategies (The Little Blue Book)*. <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>
- Hu, M. (2020). Cambridge Analytica's black box. *Big Data & Society*, 7(2). <https://doi.org/10.1177/2053951720938091>
- I.T.U. Strategy. (2005). *ITU Internet Reports 2005: The Internet of Things*.
- Janssen, H., Cobbe, J., & Singh, J. (2020). Personal information management systems: A user-centric privacy utopia? *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1536>
- Jenkins, H. (2006). *Convergence Culture Where Old and New Media Collide*. New York University.
- Kılıç, T., & Tosun, N. (2021). Akıllı Sağlık Ekosistemi ve Güncel Uygulama Örnekleri. *İşletme Bilimi Dergisi (JOBS)*, 9(3). <https://doi.org/10.22139/jobs.1019007>
- Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. *Big Data & Society*, 1(1). <https://doi.org/10.1177/2053951714528481>
- Kosmatos, E. A., Tselikas, N. D., & Boucouvalas, A. C. (2011). Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. *Advances in Internet of Things*, 1(1), 5-12. <https://doi.org/10.4236/ait.2011.11002>
- Kösesoy, İ. (2019). Nesnelerin İnterneti Güvenliğinde Blok Zinciri Uygulamaları. *Veri Bilimi Dergisi*, 2(1), 1-9.
- Kraijak, S., & Tuwanut, P. (2015). *A Survey On IoT Architectures, Protocols, Applications, Security, Privacy, Real-World Implementation and Future Trends*. 11th International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai. <https://doi.org/10.1049/cp.2015.0714>
- La Diega, G. N., & Walden, I. (2016). Contracting for the 'Internet of Things': Looking into the Nest. *European Journal of Law and Technology*, 7(2).
- Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58(4).
- Lehtiniemi, T. (2017). Personal Data Spaces: An Intervention in Surveillance Capitalism? *Surveillance & Society*, 15(5), 626-639.
- Lomas, N. (2018). Cambridge Analytica's Nix said it licensed "millions of data points" from Acxiom, Experian, InfoGroup to target US voters. *Tech Crunch*.
- Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of Things: A General Overview between Architectures, Protocols and Applications. *information*, 12(2).

- Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2). <https://doi.org/10.1177/2053951714541861>
- Maalsen, S., & Sadowski, J. (2019). The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance. *Surveillance & Society*, 17(1/2), 118-124.
- Madakam, S., Ramaswamy, R., & Tripathy, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, 3(5), 164-173. <https://doi.org/10.4236/jcc.2015.35021>
- Manokha, I. (2023). gdpr as an Instance of Neoliberal Governmentality: A Critical Analysis of the Current 'Gold Standard' of Data Protection. *BRILL*. https://brill.com/view/journals/pari/4/2/article-p173_004.xml
- Maraşlı, F., & Çıbuk, M. (2015). RFID Teknolojisi ve Kullanım Alanları. *BEÜ Fen Bilimleri Dergisi*, 4(2).
- McDermott, Y. (2017). Conceptualising the right to data protection in an era of Big Data. *Big Data & Society*, 4(1). <https://doi.org/10.1177/2053951716686994>
- McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data & Society*, 7(1). <https://doi.org/10.1177/2053951720904386>
- Meloan, S. (2003). Toward a Global" Internet of Things. *Sun Develop*, 6(11), 32-35.
- Meyers, G., & Hoyweghen, I. V. (2020). 'Happy failures': Experimentation with behaviour-based personalisation in car insurance. *Big Data & Society*, 7(1). <https://doi.org/10.1177/2053951720914650>
- Munn, L., Hristova, T., & Magee, L. (2019). Clouded data: Privacy and the promise of encryption. *Big Data & Society*, 6(1). <https://doi.org/10.1177/2053951719848781>
- Mühlhoff, R. (2023). Predictive privacy: Collective data protection in the context of artificial intelligence and big data. *Big Data & Society*, 10(1). <https://doi.org/10.1177/20539517231166886>
- Narayanan, A., & Shmatikov, V. (2008). *Robust De-anonymization of Large Sparse Datasets*. 2008 IEEE Symposium on Security and Privacy, USA. <https://doi.org/10.1109/SP.2008.33>
- Picard, R. W. (2000). *Affective Computing*. The MIT Press.
- Pitron, G. (2023). *Dijital Cehennem* (A. Tümertekin, Çev.). Türkiye İş Bankası.
- Roman, R., Zhou, J., & Lopez, J. (2013). On the Features and Challenges of Security & Privacy in Distributed Internet of Things. *Computer Networks*, 57.
- Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, 6(1). <https://doi.org/10.1177/2053951718820549>

- Shaowang, T., Liu, S., Marques, J., Feamster, N., & Krishnan, S. (2025). Algorithmic Data Minimization for Machine Learning over Internet-of-Things Data Streams. *arXiv*.
- Sifaoui, A., & Eastin, M. S. (2024). “Whispers from the Wrist”: Wearable Health Monitoring Devices and Privacy Regulations in the U.S.: The Loopholes, the Challenges, and the Opportunities. *cryptography*, 8(2). <https://doi.org/10.3390/cryptography8020026>
- Stern, P. (2011). *The Company-State: Corporate Sovereignty and the Early Modern Foundations of the British Empire in India*. Oxford University Press Inc.
- Sütcü, C. S., & Aytekin, Ç. (2018). *Veri Bilimi*. Paloma.
- Tao, F., Wang, Y., Zuo, Y., Yang, H., & Zhang, M. (2016). Internet of Things in product life-cycle energy management. *Journal of Industrial Information Integration*, 18(2). <https://doi.org/10.1016/j.jii.2016.03.001>
- Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. İçinde K. E. Himma & H. T. Tavani (Ed.), *The Handbook of Information and Computer Ethics* (ss. 131-164). John Wiley.
- Teicher, J. (2018). *The little-known story of the first IoT device*. IBM. <https://www.ibm.com/think/topics/iot-first-device>
- Tierra Común. (2020). Tierra Común. <https://www.tierracomun.net/en/home>
- Toffler, A. (1980). *The Third Wave*. Bantam.
- Tokgöz, C. (2011). *Bilişim Çağında Toplumsal Denetim Aracı Olarak Gözetim Olgusu ve Yeni İletişim Ortamlarında Bireyin Gözetim Farkındalığı Üzerine Bir Araştırma* [Yüksek Lisans]. Marmara Üniversitesi.
- Tokgöz, C. (2018). Mekân ve Beden Bağlamında Gözetim ve Direniş. *Kültür ve İletişim*, 41.
- Turkyılmaz, S. (2024). Endüstri 4.0 ve endüstriyel nesnelerin interneti: Uygulama, fırsat ve zorluklar-literatür taraması. *Doğuş Üniversitesi Dergisi*, 25(2). <https://doi.org/10.31671/doujournal.1310736>
- Türker, G. F., & Tanyeri, K. (2024). Blokzincir Teknolojisi ile Nesnelerin İnterneti Tabanlı (IoT) Sistemlerin Veri Güvenliğinin Sağlanması. *Gazi Üniversitesi Fen Bilimleri Dergisi*, 12(1), 80-91. <https://doi.org/10.29109/gujsc.1194653>
- Uluk, M. (2022). *Gözetim Kapitalizminde Kişisel Verilerin Kullanımı: Etik Web Çerçevesinde Web Siteleri ve Mobil Uygulamalar Üzerine Bir Araştırma*. İstanbul Üniversitesi.
- University of Cambridge. (2018). *Statement from the University of Cambridge about Dr Aleksandr Kogan*. <https://www.cam.ac.uk/notices/news/statement-from-the-university-of-cambridge-about-dr-aleksandr-kogan>
- Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5).

Weiser, M. (1999). The Computer for the 21st Century. *Association for Computing Machinery*, 3(3).

Westin, A. (1967). *Privacy and Freedom*. Altheneum.

White, C., & Gilmore, J. N. (2022). Imagining the thoughtful home: Google Nest and logics of domestic recording. *Critical Studies in Media Communication*, 40(1). <https://doi.org/10.1080/15295036.2022.2143838>

Wood, D. M., & Steeves, V. (2021). Smart Surveillance. *Surveillance & Society*, 19(2), 150-153.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 75-89. <https://doi.org/10.1057/jit.2015.5>

Zuboff, S. (2021). *Gözetleme Kapitalizmi Çağı* (T. Uzunçelebi, Çev.; 1. bs). Okuyan Us.