



Dijital Gözetim İzi: Yapay Zekâ Üzerine Bir Değerlendirme

Vesile Uzlu, Avrasya Üniversitesi, Pazarlama ve Reklamcılık Bölümü, Halkla İlişkiler ve Tanıtım Programı, Öğr. Gör., vesile.uzlu@avrasya.edu.tr, 0000-000-7674-2957

ÖZ

Günümüzde iletişim teknolojilerinin hızla değişim göstermesi bireylerin rutin hayatına da etki etmektedir. Bireylerin iletişim kalıpları, kendilerini ifade etme becerileri ve veriler aracılığıyla yönetilmeleri etik ilkeler bağlamında değerlendirilmelidir. Özellikle son dönemlerde popüler hale gelen yapay zekâ teknolojilerinin gelişimi birçok sorunu veya soruyu gündeme taşımıştır. Bu nedenle bu çalışmanın amacı gelişen iletişim teknolojileri ekseninde gözetim ilişkisini irdelemek ve yeni teknolojiler kapsamında yapay zekâ destekli uygulamaların etik ilkeler çerçevesinde uyumunu sorgulamak ve tartışmaktır. Bu doğrultuda bu çalışma, kavramsal analiz yöntemi ile kuramsal bir tartışma sunan teorik bir çalışmadır. Çalışma kapsamında veri kaynağını dijital gözetim ve yapay zeka ilişkisini temel alan ulusal ve uluslararası literatür oluşturmaktadır. İnceleme kapsamında ise kavramsal analiz yöntemi kullanılmıştır. Kavramsal analiz ile ilk etapta yeni iletişim teknolojilerinin süreci, gözetim toplumu, klasik gözetim kuramları, dijital gözetim sistemleri, mahremiyet ve etik kavramları incelenerek bu kavramların kuramsal temelleri ortaya konulmuştur. Bir diğer etapta ise çalışma, kuramsal tartışmayı sistematik olarak sunmak amacıyla literatür kapsamında öne çıkan kavram ve yaklaşımlardan oluşan temalar ile yapılandırılmıştır. Çalışma sonucu kapsamında, yapay zekâ destekli uygulamalar ile bireylerin verileri kaydedilerek aynı zamanda algoritmalar aracılığıyla da bireyi yönlendirerek gözetim sağlanmaktadır. Öte yandan yapay zekâ destekli sistemler, etik unsurlar bağlamında şeffaflık ve hesap verebilirlik ilkeleriyle uyusmamaktadır. Bu konuda alınan somut yaptırımların ise yetersiz olduğu sonucuna varılmıştır.

Anahtar Kelimeler : Yeni İletişim Teknolojileri, Yapay Zeka, Gözetim, Etik

Digital Surveillance Footprint: An Assessment of Artificial Intelligence

ABSTRACT

The rapid evolution of communication technologies today is also affecting people's daily lives. Individuals' communication patterns, their ability to express themselves, and the way they are managed through data must be evaluated within the context of ethical principles. In particular, the development of artificial intelligence technologies, which have gained popularity in recent years, has brought many issues and questions to the forefront. Therefore, the aim of this study is to examine the relationship between surveillance and evolving communication technologies, and to



question and discuss the alignment of AI-supported applications with ethical principles within the scope of these new technologies. In this regard, this study is a theoretical study that presents a conceptual analysis and theoretical discussion. The data source within the scope of the study consists of national and international literature based on the relationship between digital surveillance and artificial intelligence. In the scope of the examination, the conceptual analysis method was used. In the first phase of conceptual analysis, the process of new communication technologies, the surveillance society, classic surveillance theories, digital surveillance systems, and the concepts of privacy and ethics were examined to lay bare the theoretical foundations of these concepts. In the subsequent stage, the study was structured around themes consisting of concepts and approaches highlighted in the literature in order to present the theoretical discussion systematically. The findings indicate that artificial intelligence-supported applications enable surveillance by recording individuals' data while simultaneously directing individuals through algorithms. Furthermore, AI-supported systems are not fully compatible with the principles of transparency and accountability within the context of ethical considerations. It was also concluded that the concrete measures adopted to address these issues remain insufficient.

Keywords : New Communication Technologies, Artificial Intelligence, Surveillance, Ethics

Extended Abstract

When examining the stages that communication has undergone over time, it can be observed that communication, which began with drawings on cave walls, has evolved and transformed with the emergence of new communication technologies. In this context, with the emergence of new communication technologies, communication through social media, namely Web 2.0—has become interactive and more active. Web 3.0, referred to as the Semantic Web, is said to encompass intelligent applications rather than being merely interactive, and today it consists of artificial intelligence-supported applications. From this point of view, the foundation of this study is shaped around the new surveillance system brought about by digitalization and the surveillance enabled by artificial intelligence tools. Surveillance can be defined as the monitoring and tracking of individuals' behaviors; however, with new communication technologies, both surveilling and being surveilled have become easier. Particularly with the emergence of AI-supported tools, individuals have become objects of data colonialism. This situation can also be observed as a violation of individuals' privacy. Privacy refers to the state of being protected from external interference (Warren & Brandeis, 1890, pp. 193–195). However, the development of communication technologies has made this condition increasingly difficult to maintain. On the other hand, when examining the data from TÜİK, it is seen that the group using artificial intelligence applications is within the 16–24 age range, with a rate of 39% (TÜİK, 2025). In addition to the fact that individuals leave digital footprints in various AI-supported applications and are subjected to guidance as a result of their data being recorded, they are also classified and categorized in various domains through

the use of their data. From this perspective, thanks to AI-supported algorithms, individuals are digitally managed while their visibility is also controlled. On platforms such as Instagram and TikTok, while individuals' behaviors are analyzed, algorithms make similar or identical content visible based on interactions such as following a page or another individual. This situation progresses in parallel with individuals presenting their privacy-related spaces in order to become visible. Moreover, while individuals participate in these platforms through their voluntary consent, it can be said that, in the background, their data and visibility are transformed into commodities within an economic structure.

In other words, the commodification of the individual in this manner can also be referred to as data colonialism. Data colonialism scans and categorizes users through the digital footprints they leave on platforms. At this point, individuals enable data colonialism by producing data (Couldry & Mejias, 2019). Another issue is that the relationship between user experience and surveillance is legitimized within the context of user agreements. However, the extensive processing and marketing of individuals' data effectively means managing the individual. Furthermore, not only AI-supported applications but also AI platforms should be considered; for example, when examining a widely used AI application such as ChatGPT, it can be said that individuals' data are recorded. In this sense, the ethical use of AI applications by individuals is also open to debate. For instance, when users share their faces with AI applications to generate depictions of their future elderly selves, this implies that they are not only exposing their data but also their biometric data. When ethical violations are considered, the processing of data to monitor individuals and, moreover, its use as a marketing element constitutes a significant problem. Following this, when the weakening of the principle of transparency and the systematic recording of individuals' data are taken into account, it is evident that the principle of transparency in AI systems is being disregarded. On the other hand, the increase in privacy violations and the fact that algorithms guide and manage individuals through data bring about issues of accountability. The individual within the system continues to use these technologies in order not to fall behind the technological developments and the era yet lives within a technological world in which their data are processed and monitored. At this point, AI-supported applications need to be developed in a way that ensures and preserves ethical principles within the system.

As a result, it is evaluated that the individual is the primary subject of data colonialism, while AI applications have become a mechanism of control. In this sense, it is essential that this control mechanism operates within the framework of ethical principles centered on individuals. In other words, it can be clearly stated that AI applications advance the phenomenon of surveillance, that the control mechanism develops within the system along the lines of certain user agreements, and that it holds the power to direct and manage users. Therefore, renewing ethical principles within the framework of transparency will both protect users' personal rights and serve as a precaution against potential cyberattacks. This study, while addressing new surveillance perspectives, aims to raise awareness among individuals

by evaluating new forms of surveillance, ethical violations, and elements of privacy associated with widely used artificial intelligence applications today.

GİRİŞ

Günümüzde sürekli olarak gelişen iletişim yapıları, insanlar için vazgeçilmez bir etkileşim aracı olmuştur. Birey, sosyal bir varlık olduğundan iletişim kurmadan yaşamını sürdürmesi oldukça güç bir durumdur. Dolayısıyla bireylerin iletişim kurma çabası, iletişim teknolojilerinin gelişmesiyle başka bir evreye ulaşmıştır. Yeni düzende iletişim, birçok iletişim yapılarını ortaya çıkararak, iletişimi teknolojik yapı temelli hale getirmiştir (İplikçi, 2015, s. 16). İletişim, ilkel çağlarda insanların birbirleri ile iletişim kurmak için dumanı bir iletişim aracı olarak kullanmasından bu yana, internetin doğuşu ile değişmiş ve dönüşmüştür. Teknolojinin bu denli değişimi, insan hayatını kolaylaştırırken bir diğer açıdan zorlaştırdığı söylenebilir. İnternetin doğuşundan sonra, sosyal medya platformlarının artması ve birer iletişim kurma aracı haline geldikleri gözlemlenebilmektedir. Sosyal medya aracılığı ile bireyler etkileşim içerisine girerken, aynı zamanda üçüncü kişiler tarafından da gözetlendikleri açıktır. Kullanıcı deneyimleri incelendiğinde, bireyler yediklerini, içtiklerini ve hatta gezdikleri yerlerin konumunu paylaşmaktadırlar. Kısaca günlük hayatlarını ele alıp sunarak, gözetleyenler için kolaylıkla ulaşılan bir veri kaynağı oluşturmaktadırlar.

Bu çerçeveden bakıldığında, bireyler mahremiyetlerini ve verilerini gözetleyenlerin önüne kendi tercihleri doğrultusunda, kullanıcı sözleşmeleri aracılığıyla sunmaktadırlar (Pasquale, 2015, s. 143). Bu doğrultuda Web 2.0 olarak nitelendirilen sosyal medya, bir gözetlenme aracı olarak ifade edilebilir. Güncel dünyaya bakıldığında ise sosyal medyanın ötesinde dijitalleşmenin popüler aracı haline gelen yapay zekâ uygulamalarının, bireyler tarafından sıklıkla tercih edildiği görülmektedir. Sosyal medya, gözetim ve mahremiyet ihlallerini beraberinde getirirken, yapay zekâ uygulamalarının kullanımı da söz konusu ihlalleri daha ileri boyuta taşıdığı ifade edilebilir. Bu açıdan bakıldığında gözetim, dijital araçların yenilik kazanmasıyla birlikte sadece izlenme faktörünü ortaya çıkarmamaktadır. Günümüzde gözetim kavramı, yapay zekâ uygulamaları aracılığıyla bireylerin davranışlarını tahmin etme, karar süreçlerini yönlendirebilme gibi faktörleri de ortaya koymaktadır (Zuboff, 2019). Bu çerçevede, algoritmalar aracılığıyla desteklenen yeni gözetim biçimi, yapay zekâ araçlarının kullanıcılar tarafından aktif olarak kullanılması, ortaya çıkan sorunları ve etik ilişkisini incelemeye değer kılmalıdır.

Bu noktadan hareketle bu çalışmanın temeli, dijitalleşmenin getirdiği yeni gözetleme sistemi ile yapay zekâ araçlarının sağladığı gözetleme durumu üzerine şekillenmektedir. Bir diğer ifadeyle yapay zekâ uygulamaları, verileri işleyerek bir denetim mekanizması haline dönüştürdüğünü irdelemek amacıyla araştırma yürütülmüştür. Öte yandan yapay zekâ ve

etik ilişkisini incelemek önem arz etmektedir. Nitekim yapay zekâ araçları, standartlaşmış gözetimin ötesinde akıllı cihazlar, kameralar sayesinde bireyleri anlık ve mekândan bağımsız bir şekilde gözetleyerek bir veri sınıflandırması yapmaktadır. Söz konusu veriler toplumsal bir sınıflandırmaya ışık tutarak yapay zekâ tarafından bireylerin eylemleri yönlendirilebilmektedir (Asıl, 2025, s. 1419). Bu çalışmanın amacı, bireylerin mahremiyet içeren bilgilerini yapay zekâyla paylaşıırken, veriler aracılığıyla gözetlenme durumlarını tartışmak ve değerlendirmektir. Öte yandan gözetim ve yapay zekâ teknolojileri arasındaki ilişki incelenerek literatüre katkı sağlanması amaçlanmaktadır. Bir diğer ifadeyle, bu çalışmada yapay zekânın etik kullanımı eleştirel bir bakış açısıyla incelenerek, konu kuramsal çerçeve bağlamında tartışılacaktır. Bu bağlamda yeni iletişim teknolojileri kapsamında internetin gelişimi ile evrildiği noktaya temas etmek gerekir.

1. YÖNTEM

Bu çalışma, yapay zekâ, gözetim ve mahremiyet ilişkisini analiz etmeyi amaçlayan kavramsal analiz yöntemi ile ele alınmaktadır. Kavramsal analiz, sadece teorik çalışmaları sunmayı hedeflemekle kalmayıp, aynı zamanda kavramların ve çeşitli çalışmaların ilişkilerini tartışma zemininde oturtmaya olanak sağlamaktadır. Bu bağlamda bu çalışma, dijital gözetim yaklaşımlarını kuramsal temel alarak, yapay zekâ araçları kapsamında yeni gözetim sistemleri, kullanıcı deneyimleri, algoritmik yönlendirmeler ve etik konuları irdeleyen teorik bir araştırmadır. Araştırmanın temel amacı bireylerin yapay zekâ uygulamaları aracılığıyla verilerinin gözetleme unsuru olarak kullanılması, denetim ve etik ilişkisinin incelenmesidir. Bu bağlamda araştırma kapsamında veri kaynağı dijital gözetim, gözetim toplumu, yapay zekâ ve yeni gözetim sistemleri, yapay zekâ ve etik ilişkisi, yapay zekâ temelli algoritmik yönlendirmeler ve denetim ilişkisini irdeleyen ulusal ve uluslararası literatür oluşturmaktadır. Araştırmanın veri kaynakları söz konusu konulara ilişkin, kitaplar, hakemli dergilerde yayımlanan makaleler, bildiriler ve kuramsal çalışmalar oluşturmaktadır. Araştırmada inceleme süreci kapsamında kavramsal analiz yöntemi kullanılmıştır. Kavramsal analiz ile ilk etapta yeni iletişim teknolojilerinin süreci, gözetim toplumu, klasik gözetim kuramları, dijital gözetim sistemleri, mahremiyet ve etik kavramları incelenerek bu kavramların kuramsal temelleri ortaya konulmuştur. Bir diğer etapta ise çalışma, kuramsal tartışmayı sistematik olarak sunmak amacıyla literatür kapsamında öne çıkan kavram ve yaklaşımlardan oluşan temalar ile yapılandırılarak yorumlanmıştır. Bu bağlamda Mark Andrejević'in (2007) dijital gözetim kuramı, Frank Pasquale'nin (2015) algoritmik şeffaflık ve kara kutu toplumu yaklaşımı ve Shoshana Zuboff'un (2019) dijital davranış artışı yaklaşımı kuramsal çerçeve bağlamında temel alınarak sınıflandırılmış ve yorumlanmıştır. Çalışma yapay zekâ destekli iletişim teknolojileri ve uygulamalarını eleştirel bir perspektifle değerlendirerek, yapay zekâ, etik ve gözetim ilişkisini kuramsal düzeyde tartışmayı ve literatüre katkı sağlamayı amaçlamaktadır.

2. YENİ İLETİŞİM TEKNOLOJİLERİ VE DİJİTALLEŞMENİN KAVRAMSAL SÜRECİ

İletişimin teknik yapısı ele alındığında, insanların mağara duvarlarına resimler çizmesi ile başlayan süreç, televizyon, radyo gibi geleneksel medya araçları ile devam etmiştir. Bilgisayar ve internetin doğuşu ile yeni medya araçlarında da ilerleme sağlanmış ve iletişimin şekli değişmiştir. İnternet ve iletişim teknolojilerinin gelişim kaydettiği günümüzde ise, dijitalleşme de bu anlamda yeni bir boyut kazanmıştır. İletişim teknolojilerindeki değişim ve dönüşüm, yalnızca teknik altyapı sistemlerini değil, aynı zamanda bireylerin bilgiye erişimini, paylaşımını ve tüketimini de etkilemektedir. Bu nedenle yeni iletişim teknolojileri, bireyi pasif konumdan aktif konuma taşımıştır (Aydoğan, 2019, s. 57). Bu açıdan dijitalleşmenin yaşadığı dönüşümün, önceki süreçlere göre daha hızlı, daha dinamik ve etkileşim oranı daha yüksek bir yapıda olduğu söylenebilir. Dolayısıyla tarihsel çizgi içerisinde yer alan iletişim araçlarının, tek yönlüken çok yönlü ve ağ temellerine evrilmesi, mekândan bağımsız olarak zaman sınırını ortadan kaldırarak küresel süreçte eş zamanlı etkileşim sürecini olanaklı hale getirdiği ifade edilebilir. Bu noktadan hareketle dijitalleşmenin ve internetin evrimsel sürecine bakıldığında Web 1.0, Web 2.0 ve Web 3.0 süreçlerinin incelenmesi dijital evrimi anlamaya olanak tanıyacaktır.

Tablo 1: Web Süreçleri

Özellik/Boyut	Web 1.0	Web 2.0	Web 3.0
Kullanım Biçimi	Statik içerik	Etkileşimli ve dinamik içerik	Akıllı, bağlamsal ve kişisel
Kullanım Örnekleri	Web Sayfaları	Bloglar, Wikiler	Dosya Akışları
İçerik Üretimi	Firma/kurum tarafından	Kullanıcı tarafından	Veri ve bilgi odaklı akıllı üretim
İletişim	Tek yönlü	Çift yönlü	Çok yönlü, bağlantılı
Hedef	Firma	Topluluk	Kişisel
Üretim	Eğlence	Yayıncılık	Yaratıcılık
Ağ Özelliği	Hipermetin ağı	Sosyal ağ	Semantik / anlamsal ağ
Etkileşim	Web biçimleri	Web Uygulamaları	Akıllı Uygulamalar
Tarama	Dizinler	Anahtar Kelimeler	Bağlam- Uygunluk

Kaynak: (Yengin, 2014, s. 119).

Tablo 1’de görüldüğü üzere iletişim teknolojileri değişim kaydetmekle birlikte, kullanıcı ekseninde de değişikliklere yol açmıştır. Tablo 1 incelendiğinde, Web 1.0’ın etkileşimli olmadığı, durağan web sitelerini kapsadığını ve dolayısıyla iletişimin tek yönlü olduğu görülmektedir. Bu nedenle kullanıcılar pasif durumdadır. Web 2.0 ise daha gelişmiş bir versiyon olarak, etkileşimli, kullanıcının aktif ve üretim süreçlerinin içerisinde yer aldığı bir web biçimidir. Dolayısıyla Web 2.0 günümüzde sosyal medya temelli olduğu bilinmektedir. Kullanıcılar hem üretici hem de tüketici konumdadır. Web 2.0 ile kullanıcılar

duygu ve düşüncelerini paylaşarak, içerik üretimi sağlayabilmektedir (Kaplan ve Haenlein, 2010, s. 61). Web 3.0 ise teknolojinin üst versiyonu olarak çok yönlü etkileşime sahip, bilgi odaklı ve akıllı üretimin devrede olduğu bir biçimi yansıtmaktadır. Web 3.0 Anlamsal web uygulamalarını kapsamaktadır (Yengin, 2014, s. 121). Anlamsal ağ olarak bilinen Web 3.0 aynı zamanda semantik ağ anlamına gelmektedir. Semantik ağ önemli kılan unsur ağın yalnızca insanlara özgü olması değil, aynı zamanda makinelerinde söz konusu ağı okuyabilme durumudur. Bu nedenle semantik ağ küresel bir nitelikte belge ağı olarak nitelendirilebilir. (Hassan, 2017, s. 35).

Bu açıdan bakıldığında, günümüzde Web 3.0 temelli uygulamalar yapay zekâ destekli akıllı uygulamaları kapsadığı söylenebilir. Bu açıdan incelendiğinde, iletişim teknolojilerinin değişimi ve dönüşümü birey ekseninde de gelişim sağlamaktadır. Dolayısıyla YZ destekli uygulamaların, bireye sağladıkları faydalar dışında, zararları da ele alınması gereken önemli hususlar arasında yer almaktadır. Veri akışlarının yoğunlukta olduğu Web 3.0 temelli yapay zekâ araçlarının, bireylerin verilerini temel alarak gözetim unsuruna yol açmaktadır. Bu nedenle gözetim kavramının incelenmesi ve yapay zekâ ile ilişkisinin irdelenmesi elzem olmaktadır.

2.1. Gözetim Kavramı ve Dijitalleşen Gözetim

Gözetim kavramının tanımları incelendiğinde, bireyin hareket ve davranışlarını yakından izlemek, takip etmek veya kişilerin, grupların davranışlarını sistemli bir biçimde takip etmek olarak nitelendirilebilir (Clarke, 2005). Bir diğer ifadeyle, birini veya bir durumu izlemek ve kayıt altına almak anlamına gelir (Petersen, 2007, s. 10). Gözetim kavramı denilince özellikle Michel Foucault'un gözetimi ele alış biçimi dikkat çekmektedir. Foucault modern toplumu, disiplin toplumu ile bağdaştırır ve disiplinin bireyler üzerinde yararlı, itaatkâr ve üretim süreçlerinde yer almayı amaçlayan, iktidar teknikleri olarak görür. Bu tekniklerin odak noktasında ise, gözetim olduğunu ifade eder. Buradan hareketle Foucault, gözetimin bireyi sürekli görünür kıldığından bahseder. Foucault'un deyişi ile görünürlüğün bir tuzak olduğunu ileri sürer (Foucault, 2019, s. 223). Bu çerçeveden bakıldığında gözetim, sadece dışardan sağlanan bir denetim mekanizması değil, aynı zamanda bireyin kendi kendini denetlemesini sağlayan bir süreç olarak ifade edilebilir. Öte yandan Foucault, gözetim mekanizmasının mantığını açıklamak için Jeremy Bentham tarafından hazırlanan panoptikon modelini kullanır (Foucault, 2019, s. 289-293). Panoptikon modeli, merkezde bir gözetleme kulesi ve çevresinde hücreler bulunan bir hapishane modelidir. Söz konusu modelde mahkûm, gözetlenip gözetlenmediğini bilemez fakat gözetlenme ihtimaline yönelik sürekli olarak davranışlarını kontrol altında tutma ihtiyacı hisseder. Böylelikle fiziksel bir müdahaleye gerek kalmaksızın hem gözetim hem disiplin sağlanmış olmaktadır (Foucault, 2019, s. 290-291). Nitekim gözetim bireyin var olmasından bu yana bir denetim unsuru olarak, sürekli yaşamın içerisinde varlığını korumuştur. Bireyler, kendilerini yöneten kişiler tarafından veya kapitalist amaç güden iş yerleri tarafından devamlı farklı amaçlar

doğrultusunda gözetim altında tutulmuşlardır. Fakat teknolojik ilerlemeler ile dijitalleşme sürecinin de olgusu ile gözetme ve gözetilme kavramları da yeni süreçlere evrilmiştir. İletişim teknolojileri ile birçok bireyin iletişim teknolojilerinin ortaya koyduğu araçları kullanması ile gözetmek ve gözetilmek kolay bir hal almıştır (Kalaman, 2019, s. 577). Bir diğer ifadeyle gözetleme birbiri ile ilişki içerisinde olan iki farklı faktörü ele alır. İlk faktör, insanlar hakkında elde edilen eylem ve davranışları yönetmek için kodlanmış bilgi birikimi denilebilir. Gözetlemenin diğer faktörü ise, bireylerin söz konusu davranışlarının belirli konular üzerinde otorite kuran, öteki bireyler tarafından doğrudan izlenme sürecini ifade eder (Giddens, 2008, s. 24-25).

Bu çerçeveden bakıldığında dijital gözetim, bireylerin veriler aracılığıyla sürekli olarak izlenmesi ile söz konusu verilerin toplanarak yönlendirebilme gücünü kapsamaktadır. Bu sebeple teknolojik araçlara bakıldığında internet, bu verilerin başlıca kaynağını oluşturmaktadır. Sosyal medya platformları veya büyük veri teknolojilerinin içerisinde bulunan akıllı cihazlar, dijital gözetime olanak tanıyan başlıca sistemler olarak karşımıza çıkmaktadır. İletişim teknolojilerinde yaşanan gelişmeler, söz konusu olan araçlara ve son zamanlarda popüler hale gelen yapay zekâ platformlarının etkin kullanımı neticesinde, bireyler hem gözetlenmekte hem de yönlendirilmektedirler. Bu bağlamda, günümüzde gözetim olgusu sadece mekânsal alanda değil, aynı derece de zaman faktörüyle zamansal bir derinlikte kazanmıştır.

Yapay zekâ teknolojilerinin gelişimi ile söz konusu dönüşüm, bireylerin sadece olağan davranışlarını değil, oluşabilecek eylem ve davranışlarını da önceden belirleyen algoritmaları sayesinde gözetim sağlanmaktadır (Burrell ve Fourcade, 2021, s. 221-228). Oluşan yeni gözetim modeli; “Modern yaşamın bir zamanlar sorgulanması bile akla gelmeyen anlamlarının, sembollerinin ve kurumlarının gözlerimizin önünde çözülmesinden dolayı, temel özelliği parçalanma ve belirsizlik olan” (Staples, 2013, s. 85). Şeklinde dile getirilmektedir. Bu açıdan bakıldığında, toplanan veriler bireylerin hayatında, rutinleşmiş olağan bir durum olarak ele alınmaktadır. Bireyler kendi öz tercihleri ile verilerini paylaşarak, söz konusu olan gözetime olanak tanımaktadır. Öte yandan bu durum, bireylerin mahremiyet içeren bilgilerini paylaşmasına kadar uzanmaktadır. Bu sebeple dijital gözetim kavramını anlamlandırmak ve verilerin kaynağını irdelemek gerekir. Dolayısıyla bireylerin dijital gözetim kapsamında, mahremiyet unsurlarını içerisinde barındıran verilerin, paylaşılması durumu tartışılmalıdır.

2.2. Dijital Gözetim ve Mahremiyet

Günümüzde dijitalleşmenin artmasıyla birlikte gözetim unsurları fiziksel olmaktan çıkarak, veri kaynaklı olmaktadır. Gözetim, teknolojik araçların gelişmesiyle bu şekilde bir dönüşüm yaşaması toplumu da değiştirmiş ve dönüşmüştür. Öte yandan yeni evreye uğramış

olan gözetim süreci, bireyin günlük hayatının tamamına yansıdığı görülmektedir. Oluşan bu süreç, toplumsal olarak mahremiyet ve gözetim ilişkisini tartışmaya değer hale getirmiştir. Bu nedenle öncelikle mahremiyet tanımlarını ve yeni dijital gözetimin getirdiği durumun analiz edilmesi gerekmektedir.

Mahremiyet kelimesinin kökeni, Arapçaya dayanmakta ve mahrem kelimesinden hareketle doğduğu bilinmektedir. Mahremiyet kavramı incelendiğinde ise bireyin dış olgulara karşı veya şahsi durumlara yönelik, yalnız bırakılma hakkı olarak tanımlanmaktadır. Söz konusu tanımlama, bireyin dışardan müdahalelere kapalı olması durumunu anlatmaktadır (Warren ve Brandeis, 1890, s. 193-195). Bu çerçeveden bakıldığında mahremiyet, fiziksel veya mekâna bağlı olarak geliştiği görülmektedir. Fakat dijitalleşmenin artması ve veri üzerinden akması sebebiyle, bu tanım klasik bir tanım olarak kalmakla birlikte, dijitalleşmenin sağladığı gözetim söz konusu tanımın sınırlarını zorladığı söylenebilir.

Bir başka tanıma göre mahremiyet; bireylerin mahrem alanlarını ne zaman ve ne şekilde olacağını kendi belirleyecek şekilde, kontrol etme hakkı olarak tanımlanır (Westin, 1967, s. 7). Bu açıdan ele alındığında ise mahremiyet, bireyin bilgi hakkını kontrol etme durumunu kapsamaktadır. Ancak dijital gözetim ile bireyin verileri toplandığından, birey üzerinden elde edilen bilgiler vasıtasıyla kişilerin kontrol mekanizması zayıflamaktadır. Bu anlamda Lyon'a (2001, s. 2-5) göre, dijital gözetim sadece izleme veya gözetleme şeklinde değil, bireylerin ardında bıraktıkları veriler aracılığıyla profilleri kategorize etme ve sınıflandırma şeklinde olduğunu dile getirmektedir. Bu durum kapsamında değerlendirildiğinde mahremiyet, sadece bir hak ihlali değil, aynı zamanda veri kaynaklı bir profil yaratma sorununu da beraberinde getirmektedir. Mahremiyet, kişilerin özel alanlarını kapsayan kamuya açık olmayan bir alan olarak tanımlanabilir. Fakat dijitalleşme ile bu alanın silikleştiğini söylemek mümkün olmaktadır.

Nissenbaum (2009) ise mahremiyeti, bireyin verileri üzerinden tam kontrolü olarak değil, bilginin bağlama uygunluğu üzerinden değerlendirir. Örneğin sağlık, eğitim ile ilgili verilerin, uygun bağlam ile uygun kişiler arasında paylaşılması mahremiyet ihlali değildir ancak söz konusu verilerin pazarlama şirketlerine verilmesi veya uygunsuz bağlam içerisinde gerçekleşmesi mahremiyet ihlaline yol açtığından söz eder. Castells'e (2009, s. 69-75) göre, modern gözetim süreci içerisinde yer alan ağ toplumunda, bilginin temel bir üretim süreci olduğuna işaret eder. Ağ yapıları ile akan veriler ile mahremiyet, ağlar içerisinde dolaşımda olan bir kavram haline geldiğinden söz edilmektedir. Mahremiyet bireyler açısından değerlendirildiğinde, kredi kartları, kimlik kartları gibi tanıtıcı unsurlar bireyler tarafından sisteme yüklenmektedir. Aslında bu durum bile dijital bir kimlik çıkarmak için yeterli düzeydedir. Bir diğer açıdan ise, bireyler kamuya açık alanlarda sürekli kayıt altına alınarak, her davranışları biyometrik denetleme mekanizmaları aracılığıyla kontrol edilmektedir (Lyon, 2013, s. 175). Ancak sosyal medyanın bireyler tarafından aktif olarak kullanması ile devam eden süreç, gözetim şeklini de değiştirmiştir. Kullanıcılar, farklı içerikleri ve verilerini sosyal

medya platformları aracılığıyla yansıtmaktadırlar. Söz konusu kullanıcı verileri incelendiğinde, bireylerin kişisel fotoğrafları, yedikleri, gezdikleri yerler ve hatta günlük hayat akışlarını ele alarak, sosyal medya platformlarında benliklerini sundukları söylenebilir. Bu sebeple bireyler, öz tercihleri doğrultusunda kişisel verilerini paylaşmaktadırlar. Günümüzde bireylerin iletişim teknolojileri aracılığıyla özel alanını topluma açarak mahrem algısını koruması zorlaşmaktadır. Bireyler sosyal platformlarda mahrem alanlarını herkese açarken, başkaları tarafından görünür olmayı ve beğenilmeyi istemektedirler. Bireylerin sosyal ve özel hayatlarını, herkese göstermek istemeleri, mahremiyetin kamuya açılması halini almaktadır (Korkmaz, 2013, s. 112-113).

Bu bağlamda bilişim teknolojilerinin gelişimi, bireyin mahremiyetini açarken dijital gözetimi de beraberinde getirmektedir. Öte yandan yapay zekâ algoritmalarının doğurmuş olduğu gözetim süreçleri, bireyin her davranışını kayıt altına alırken, aynı zamanda algoritmalar aracılığıyla bireyin davranışını yönlendirme gücünü de eline almaktadır. Bu noktada bireylerin yapay zekâ kullanım oranları ve gözetim ilişkisine değinmek yerinde olacaktır.

3. YAPAY ZEKÂ VE DİJİTAL GÖZETİM İLİŞKİSİ: GÖZETİMİN YENİDEN İNŞAASI

Yapay zekâ araçlarının artış göstermesiyle birlikte gözetim de yeni bir evreye uğramıştır. Bireylerin yapay zekâ araçlarını kullanım durumları incelendiğinde TÜİK, Yapay Zekâ İstatistikleri 2025'e göre "Üretken yapay zekâ kullandığını beyan eden bireylerin oranı 2025 yılında %19,2 oldu. Bu oran, cinsiyete göre incelendiğinde erkeklerin %19,4'ünün kadınların %18,8'inin yapay zekâ kullandığı görüldü. Yapay zekâ kullanma oranı yaş grubuna göre analiz edildiğinde ise, en fazla %39,4 ile 16-24 yaş grubunda yer alan bireylerin yapay zekâ kullandığı, bunu %30,0 ile 25-34 yaş grubunun, %15,5 ile 35-44 yaş grubunun takip ettiği saptandı. Yapay zekâ kullanım oranının en düşük olduğu yaş grubu ise 65-74 yaş grubunda oldu." (TÜİK, 2025).

Bu açıdan bakıldığında, genç nüfusun yapay zekâyı etkin kullandığı görülmektedir. Öte yandan geleneksel gözetim süreçlerine bakıldığında, gözetimin bir denetim mekanizması olarak ele alındığı söylenebilir. Ancak dijital gözetimin getirdiği unsurlara bakıldığında, her yerde kameraların olması, akıllı cihazların bireylerin etrafını donatması veya veri gözetleme sistemleri ile bireyler sürekli olarak kolay bir biçimde gözetlenmesi durumu söz konusu olmaktadır. Dolayısıyla tıpkı panoptikon tasarımı olduğu gibi, dijital panoptikonun olduğu söylenebilir. Yapay zekâ araçlarını kullanan bireyler, tıpkı panoptikon da olduğu gibi gözetlenme hissi ile davranışlarını sınırlandırabilirler ancak verilerin kaydedildiğini bilmelerine karşın dijital ayak izi bıraktıkları da açıktır. Bu noktadan hareketle yapay zekâ

destekli algoritmaların dijital veri toplama algoritmik yönlendirme ve davranış tahmini açısından irdelenmesi gerekmektedir.

3.1. Dijital Veri Toplama, Algoritmik Yönlendirme ve Davranış Tahmini

Dijital gözetim destekli sistemler aracılığıyla bireylerin verileri kolaylıkla toplanmakta ve ekonomik bir araç olarak kullanılmaktadır. Andrevejiç'e (2007, s. 304) göre çağdaş dünyada bağlantı (ağ) bireylerin verilerinin kaydedildiği bir araçtır. Bireyler dijital platformlara erişim sağlarken aynı zamanda sunmuş oldukları veriler üzerinden hakimiyeti kaybetmektedirler. Bir diğer ifadeyle dijital erişimler bireye kolaylık sağlarken, aynı zamanda ürettikleri veriler üzerinden de kontrol sağlayarak, kişisel verilerin platformlar aracılığıyla toplanıp ekonomik bir değer sağladığından bahsetmektedir. Bu nedenle, şehrin çeşitli yerlerinde ücretsiz olarak sunulan ağ yapılarının, arka planında yatan amacına vurgu yapmaktadır. Bir diğer husus ise bireylerin verilerinin silinse dahi bir anlam ifade etmediğine yöneliktir. Andrejevic (2007, s. 306) bu konuda güçlü bir örnek vermektedir; kullanıcılar kişisel e-postaları üzerinden yaptıkları yazışmaların, kişisel iletişim bağlamında şahsa özel olduklarını düşünürler. Ancak kullanıcılar Gmail hesaplarında yer alan kullanıcı sözleşmesini incelediklerinde Google'ın verileri kopyalayarak süresiz olarak saklama hakkına sahip olduğuna ilişkin bir maddeye rastlayacaklardır. Bu bağlamda verilerin yakın gelecekte silinme garantisi olduğunu söylemek ya da düşünmek gerçekliği yansıtan bir durum değildir. Öte yandan bireylerin yeni çağda sürdürdüğü yaşam için Andrejevic "tamamen belgelenmiş bir yaşam" (2007, s. 308) ifadesini kullanmaktadır.

Bu yeni yapı ile dijital gözetim sağlanırken, aynı zamanda yapay zekâ algoritmaları aracılığıyla, bireylerin davranışları ve eğilimleri de yönlendirilebilir bir pazarlama dinamiğine dönüştüğü görülmektedir. Bu çerçeveden bakıldığında, bireyler akıllı cihazlar ve kameralar ile çevrili durumda olup, bir oto kontrol ihtiyacı hissederken aynı zamanda bıraktıkları veri izleriyle hem bir pazarlama aracı hem de veri mahremiyeti sunan bir meta haline gelmektedirler. Dolayısıyla bu durum, sabit mekanlarda gerçekleşen gözetimden ziyade, artık sürekli bir biçimde gerçekleşen veri yığınları ile bir kontrol sistemini oluşturduğu söylenebilir. Bu bağlamda yapay zekâ araçları ile gözetim, sadece görünmez kılınmamakla birlikte, aynı zamanda bireyin yaşamı içerisinde yer alan sıradan bir durum olarak görülmektedir. Öte yandan sunulan dijital izler, gözetim kapitalizmine de olanak tanımaktadır.

Bu durum Zuboff'a (2019, s. 8-12) göre, klasik düzende emeğin metalaştırma süreci hâkimken, dijital kapitalizmde bireyin verilerinin metalaştırıldığından bahsetmektedir. Bir diğer ifadeyle kullanıcıların verileri davranış tahmini ve yönlendirme bağlamında kullanılmaktadır. Dolayısıyla Zuboff bu yeni dijital ekonominin temeline dayanan davranışsal artık kavramından söz eder. Bu kavram kullanıcıların platformlarından elde edilen hizmet bağlamında, zorunlu olmayan fakat tahmin ve yönlendirme amacıyla sağlanan fazla verileri kapsamaktadır (Zuboff, 2019, s. 63-75). Nitekim söz konusu veriler yapay zekâ araçları sayesinde analiz edilerek, gelecekteki davranışlar tahmin edilmektedir. Böylelikle gözetim,

sadece izleme aracı olmaktan çıkmakta ve ekonomik bir çıktı üreten aktif bir öngörü mekanizmasına dönüşmektedir. Öte yandan Zuboff'a (2019) göre yeni gözetim yapısının getirdiği kapitalist yapı içerisinde yapay zekâ araçları yalnızca davranışları öngörmemekte, aynı zamanda bireylerin davranışlarını şekillendirmeye çalışmasıdır. Dolayısıyla Zuboff bu durumu, davranışsal geleceğe yön verme niteliğinde olduğunu dile getirmektedir (Zuboff, 2019, s. 93-100). Büyük teknolojik şirketleri veya yapay zekâ platformları aracılığı ile bireylerin söz konusu davranışları ve öngörülen tahmini eylemleri, reklam verenlere, pazarlama şirketlerine veya diğer ekonomi aktörlere satılmaktadır. Bu çerçevede, birey hem bir veri kaynağı hem de kapitalist bir özne haline gelmektedir. Bu değişim ve dönüşüm aslında gözetim kavramını klasikleşmiş olan panoptikon gözetim biçiminden farklı bir nitelikte, mekâna bağlı olmadan, zamansal derinliği olan dijital bir gözetime evrilmiştir. Modern gözetim bu yönüyle, bireylerin verilerini işleyerek, onları veri gölgeleri ile yönlendirir ve yönetir (Lyon, 1994, s. 57-65). Bu açıdan bakıldığında bireylerin akıllı cihazlar sayesinde kayıt altına tutulan etkileşimleri, arama kayıtları gibi unsurların aslında yapay zekâ algoritmaları aracılığı ile kaydedilerek bireylerin davranışları öngörülerek yönlendirilmektedir. Crawford'a (2021) göre yapay zekâ sistemleri, algoritmik bir araçtan ziyade aynı zamanda nesnel bir görüşe dayanmayan politik güç ve ideolojileri içerisinde barındıran bir yapı olduğunu ifade eder. Öte yandan yapay zekâ teknolojilerini bireyleri sınıflandırma, kategorize etme, duygu tanıma ve biyometrik veriler ile devlet iktidarıyla iç içe geçmiş bir gözetim pratiği olarak değerlendirmektedir. Bu anlamda bireyin biyometrik verileri ve duygu durumları da gözetime olanak sağlayan bir veri kaynağı olduğu söylenebilir. Dolayısıyla yapay zekâ teknolojisi Crawford (2021) tarafından bir yenilik olarak değil, bireyler arasında hak ihlallerine sebep olan eşitsizliği ve iktidar gözetimine de olanak sağlayan bir yapı olarak ele alır. Bireyin, gözetim, mahremiyet ve hak ihlalleri arasında bir meta haline geldiği söylenebilir. Sonuç olarak gözetim bu haliyle, kullanıcı deneyimlerini ve verilerini metalaştırarak sadece denetim ve güvenlik aracı olarak kullanılmamakta, aynı zamanda büyük veri şirketlerine ekonomik bir unsur sağlamaktadır. Bu anlamda bireylerin kullanıcı deneyimleri ve veri akışları irdelenmesi gereken bir diğer husus olarak karşımıza çıkmaktadır.

3.2. Kullanıcı Deneyimleri ve Dijital Gözetim

Bireylerin çeşitli yapay zekâ destekli uygulamalarda dijital ayak izi bırakması, verilerinin kaydedilmesi sonucu yapılan yönlendirme dışında, aynı zamanda bireylerin çeşitli alanlarda verileri kullanılarak sınıflandırılmakta ve kategorize edilmektedirler. Bu açıdan bakıldığında YZ destekli algoritmalar sayesinde bireyler, dijital olarak yönetilirken aynı zamanda görünürlükleri de yönetilmektedir. Instagram, Tiktok gibi platformlarda bireyin davranışları analiz edilirken, bir sayfayı veya bireyi takip etme etkileşimleri ile algoritmalar benzer veya aynı içerikleri görünür kılmaktadır. Bu durum, bireylerin mahremiyet içeren alanlarını görünür olmak amacıyla sunmaları noktasında benzer bir paralel de ilerlemektedir.

Öte yandan söz konusu platformlara bireylerin gönüllü rızaları ile katılma durumları sağlanırken, arka planda bireylerin verileri ve görünürlükleri bir ekonomik yapı içeren meta haline geldiği söylenebilir.

Bir diğer ifadeyle bireyin bu şekilde meta haline gelmesi, veri sömürgeciliği olarak da ifade edilebilir. Veri sömürgeciliği, kullanıcıların dijital platformlarda bıraktıkları ayak izleri ile taranır, kategorize edilir. Birey bu noktada, veri üreterek veri sömürgeciliğine olanak tanımış olmaktadır (Couldry ve Mejias, 2019). Bir diğer husus ise kullanıcı deneyimleri ve gözetim ilişkisi kullanıcı sözleşmeleri bağlamında meşrulaştırılarak yapılmasıdır. Oysa bireylerin verilerinin bu denli işlenmesi ve pazarlanması bireyi adeta yönetmek anlamına gelmektedir. Öte yandan sadece yapay zekâ destekli uygulamalar değil, aynı zamanda söz konusu platformlar kapsamında, örneğin ChatGPT gibi popüler kullanımda olan uygulama ele alındığında, bireylerin verilerinin kayıt altına alındığı söylenebilir. Bu anlamda bireylerin de yapay zekâ uygulamalarının etik kullanımı tartışmaya açıktır. Örneğin kullanıcıların yüzlerini, yaşlılığını tasvir ettirmesi için yapay zekâ platformları ile paylaşımları, bireylerin sadece verilerini değil, aynı zamanda biyometrik verileri üzerinden de kontrolü kaybettikleri anlamına gelir. Bu noktada bireyler veri sömürgeciliğinin birer nesnesi haline gelmektedir. Gözetimin çeşitli yollarla, görünmez duvarlarla meşrulaştırılarak şiddetinin artırıldığı ifade edilebilir.

Gözetim kavramı irdelendiğinde, panoptik gözetimin, azınlık kesimin çoğul bireyleri izlenmesi sürecini ifade ettiği dile getirilebilir. Ancak sinoptik gözetim kavramına değinecek olursak; çoğunluk tarafında yer alan bireylerin, azınlık kimseleri gözetmesi anlamını taşımaktadır. Bu kapsamda geniş kitlelerin ünlüleri, influencerları takip etmesi veya gözetlemesi örnek olarak gösterilebilir. Mathiesen'a (1997, s. 219) göre, sinoptik gözetim kavramı incelendiğinde, modern gözetim anlayışlarında sadece tepeden aşağı doğru inen bir gözetim varlığından söz etmek yetersizdir. Aşağıdan tepeye doğru, bir gözetleme anlayışı olduğunu ileri sürmektedir. Bu anlamda kitle iletişim araçları arasında yer alan televizyon ve diğer iletişim araçları sinoptik gözetimin oluşmasına temel olmaktadır. Dijital platformların artmasıyla birlikte söz konusu etkileşim ve tepedekileri gözetleme durumu daha sistematik ve kolay bir biçimde gerçekleştiği söylenebilir. Gerek politikacıları gerekse alanında ün kazanmış kimseleri, takip edip gözetlemek bu kavramın gelişmesine katkı sunmaktadır. Öte yandan sadece izleme ve gözetleme değil, aynı zamanda söz konusu kimselere yönelik dijital platformlar sayesinde yorum, beğeni, destek gibi geri dönüşlerle bireyler hem gözetlemekte hem de veri sömürgeciliğinin birer parçası olmaktadır. Bu bağlamda, önemli ölçüt görünür olma arzusunun olduğu dile getirilebilir. Bir diğer bakış açısı ise, bireyler kullanım akışı ile algoritmalar aracılığıyla yönlendirilmektedir. Öte yandan bireylerin akışta kalması sağlanarak, dikkatleri yönlendirilerek, ekran ve veri akışı uzatılmaktadır (Srnicek, 2017, s. 39-43). Bireylere öneri veya bildirimler aracılığıyla, platformda daha uzun süre kalmalarının sağlanması örnek olarak gösterilebilir. Sinoptik ve panoptik gözetimden farklı olarak Bauman ve Lyon'a (2013) göre akışkan gözetim kavramı çağdaş dünyanın en güncel gözetim biçimini

yansıtmaktadır. Panoptik gözetimde kapalı alanlarda otoriteyi ve gözetimi sağlamak amacıyla yapılan gözetim, akışkan gözetim ile artık sınırları ve duvarları olmayan ağ yollarıyla yapılan yeni gözetim biçimini ifade etmektedir. Ağ yollarıyla yapılan gözetimde bireyler resmî kurumlar ve devlet aracılığıyla değil, çeşitli pazarlama şirketleri, platformlar ve çeşitli kanallar aracılığıyla da gözetlenmektedir. Bir diğer ifadeyle Deleuze (1992) göre yeni gözetim biçimi bir modülasyona dayanmaktadır. Panoptikon modelinde olduğu gibi kapalı kurallar ve disiplin yoktur bunun yerine esnek kurallar ve günlük hayatın içerisine yerleşmiş yapılar mevcuttur. Bu anlamda modülasyon ile birlikte kontrol toplumunun ortaya çıktığı söylenebilir. Bireyler harcama yaparken kredi kartları aracılığıyla, yapay zekâ sistemlerini, internet ve sosyal medyayı kullanırken sürekli olarak veri üretir. Bu bağlamda örneğin ChatGPT gibi popüler kullanımda olan yapay zekâ sistemine bir soru sorulduğunda aradan belli bir süre geçmesine rağmen benzer bir soruyla bağlantı kurarak sorulan veya konuşulan eski mesajları yeniden sunmaktadır bu durumda üretken yapay zekanın verileri kaydetme ve işleyiş biçimini doğrudan göstermektedir. Bir diğer açıdan ise esnek bir kontrol olduğu için tek seferde veriler işlenmez yazılanlara, yönelimlere göre algoritmalar sürekli olarak güncellenir ve yeniden profillemeye çıkarmaktadır. Dolayısıyla bireylerin sistem içerisindeki dolaşımları, veri toplamak, kişiler hakkında kriter oluşturmak veya profil oluşturmak için kullanılmaktadır. Öte yandan Haggerty ve Ericson'a (2000) göre veri ikizi kavramı gözetimin başlıca unsurunu oluşturmaktadır. Veri ikizi bireylerin gerçek yaşamdaki hareketleri, bulundukları durumdan ziyade, ortaya çıkarılan veri profilini baz almaktadır. Bu çerçevede yapay zekâ sistemleri gerçek yaşantıyı değil, sunulan verileri analiz ederek bir profillemeye ulaşmaktadır. Dolayısıyla günümüzde gözetim, insanı izleyerek değil, veriyle donatılmış insanı gözetlemektedir. Bu durumu sağlamanın bir diğer yolu ise bireylerin gönüllü olarak katıldıkları sözleşmeler ve platformlar aracılığıyla gerçekleşmektedir.

Gözetim bu şekilde değerlendirildiğinde, panoptik ve sinoptik gözetim karma olarak varlığını sürdürse de günümüzde etkin olarak kullanılan, kullanıcı deneyimlerle birleşen akışkan gözetim biçimi, modülasyon gözetim ve veri ikizi ile gözetim olduğu söylenebilir. Çünkü sinoptik gözetim aracılığıyla bireyler, tepedekileri gözetleyip takip ederken, aynı zamanda veri akışları aracılığıyla panoptik gözetim ile yönetilmektedirler. Bu ikilem arasında kalan kullanıcılar ise kullanıcı deneyimleri ve veri akışlarıyla iki gözetim şekline de akışkan gözetim ile hizmet etmektedirler. Bunun yanı sıra modülasyon gözetim ile bireylerin ağlar içerisindeki tüm hareketleri yeniden analiz edilmektedir. Veri ikizi sistemi ile de bireylerin davranış kalıpları, yönelimleri baz alınarak, verilerinin takip edilerek bir profil yaratımı söz konusu olmaktadır. Bunun önemli bir sebebi ise gözetimin silikleşmesi, dijitalleşmeyle beraber görünmez hale gelmesi ve bir sistematığa dayanmasından kaynaklanmaktadır. Dolayısıyla çeşitli algoritmalar aracılığıyla kullanılan yapay zekâ destekli uygulamaların etik değerler açısından da irdelenmesi gerekmektedir.

3.3. Yapay Zekâ Gözetimi ve Etik Çerçeve

Yapay zekâ uygulamalarının, günümüz dünyasında sıkça kullanımı ileri tarihlere de etki edecek teknolojik bir yaklaşımdır. Bu nedenle bireyler, yapay zekâ uygulamalarını kullanırken etik değerleri göz önünde bulundurmalıdır. Etik, kavramsal olarak bireyin doğru ölçümlenebilir ve insani değerler bütününde, eylemlerini sürdürmesi anlamına gelmektedir. Yapay zekâ uygulamalarında etik, bazı insan davranışlarını korumaya yönelik olduğu düşünülürse bu noktada; şeffaflık, hesap verebilirlik ve siber güvenlik bağlamında teknik sağlamlık aşamaları dikkate değer unsurlar olarak ön plana çıkmaktadır (Karaağaçlı, 2025, s. 4). Bu çerçeveden bakıldığında yapay zekâ uygulamalarının, söz konusu unsurlara riayet etmesi gerektiği, önemli problemlerden birine işaret etmektedir. Yaygın olarak kullanılan yapay zekâ uygulamaları incelendiğinde ise; öneri sistemi ile çalışan yapay zekâ uygulamaları, dil çevirmenliği sistemi ile çalışan yapay zekâ uygulamaları, görüntü veya kurgu işleme ile çalışan yapay zekâ uygulamaları ve içerik yazma algoritmaları gibi birçok sistemi içerisinde barındırmaktadır (Karaağaçlı, 2024, s. 256-258). Öte yandan sosyal medya ile etkileşimli olarak, algoritmalar aracılığıyla YZ desteği ile verilerin işlendiği hususu da göz ardı edilmemelidir. Bir diğer önemli husus ise verilerin işlenirken çeşitli kullanıcı sözleşmeleri ile gerçekleşen rıza prosedürüdür. Bu çerçevede Pasquale (2015, s. 143) bu durumu şu şekilde açıklar "Web sitelerinin hizmet şartları, 'gizlilik politikaları' olmaktan çok, haklarınızı hizmetin sahibine devreden sözleşmelerdir. " Bir diğer ifadeyle kullanıcı sözleşmeleri görünürde kişisel hakları ve mahremiyeti koruyan unsurlar olmasına karşın aslında gerçekte bireylerin hakları, verileri ve mahremiyetleri söz konusu platformlara devredilmektedir. Dolayısıyla gözetim mekanizması sadece teknik olarak değil aynı zamanda hukuki bir süreç gibi görünen sözleşmeler aracılığıyla da yapılmaktadır. Öte yandan kullanıcılar ve platform sahiplerinin arasındaki güç dengesizliği şu şekilde ifade edilebilir; "Facebook veya Google gibi bir aracının hizmet şartlarını değiştirme ihtimali, neredeyse tüm kullanıcıların kapasitesinin ötesindedir." (Pasquale, 2015, s. 144) Bu çerçevede Pasquale, Facebook gibi büyük bir şirketin uymadığı vaatleri de açıklamıştır. Örneğin Facebook kullanıcı kitlesine verilerini 'sadece arkadaşlar seçeneğiyle' sınırlı kişilerle paylaşılabilirliğini dile getirdi ancak, 'sadece arkadaşlar' seçeneğini seçmek verilerinin arkadaşlarının kullanmış olduğu üçüncü taraf uygulamalarla paylaşılmasını engellemediğini ifade etmiştir (Pasquale, 2015, s. 144). Tamda bu noktada yapay zekâ ve yeni iletişim teknolojileri, verileri kaydetme, yönetme ve yönlendirme konularında etik çerçeve kapsamında sorgulanması gerekmektedir. Bu bağlamda Kişisel Verilerin Korunması Kanunu (KVKK) incelendiğinde bireylerin verilerinin işlenmesini, saklanma sürelerini ve korunmasını içermektedir. KVKK'nın 4. maddesine (2016) göre kişisel veriler işlenirken hukuka uygun ve dürüstlük temelli olmalıdır, belirli ve açık amaçlarla veriler toplanmalıdır, işlendikleri amaca uygun olarak sınırlı ve ölçülü olmalıdır ve gerekli süre kadar saklanmalıdır. Bu madde yapay zekâ destekli uygulamalar ile ele alındığında özellikle verilerin işlenme amacı ve saklanma süreleri belirsizdir. Ancak kanun maddesine göre bu belirsizlik durumu kabul edilemezdir. Bu anlamda şeffaflık ilkesi de

zedelenmektedir. Öte yandan Toplumun yaşamını kolaylaştıran söz konusu teknolojiler, aynı zamanda kullanıcıların verilerinin kaydedilmesi noktasında etik boyutu da tartışmaya dahil edilmelidir. Bu bağlamda deontolojik etik yaklaşımı bir eylemin ve davranışın ahlaki boyutunun doğurmuş olduğu sonuçlardan azade, evrensel ahlak kurallarına ve görevlerin uygunluğuna bağlı olduğu görüşüne dayanmaktadır (Kant, 2012). Bu yaklaşıma göre yapay zekâ sistemleri toplumsal açıdan fayda sağlasa da verileri kaydetmesi, paylaşması ve bireyleri yönlendirerek kişisel hakları ihlal etmesi, etik açıdan problemli olarak görünmektedir. Faydacı etik yaklaşımına göre, çok sayıda bireye çok fazla fayda üreten eylemler ahlaki olarak kabul edilmektedir (Mill , 1986, s. 19). Bu açıdan incelendiğinde yapay zekâ sistemlerinde örneğin, sağlık alanında hastalıkların erken teşhisi topluma fayda sağladığından etik olarak kabul edilebilir ancak bireylerin haklarının ihmal edilmesi bu yaklaşımın eksik yanı olarak tanımlanabilir. Sorumluluk etiği yaklaşımı kapsamında ise eylemlerin sadece mevcutta olan sonuçları değil, zaman içerisinde çıkan problemler veya sonuçların da sorumluluğunu üstlenebilme durumu ile ilişkilidir (Jonas, 1984). Yapay zekâ sistemleri ile sorumluluk etiği ilişkilendirildiğinde birtakım ilkelerin sorgulanması gerekmektedir. Bu bağlamda, yapay zekâ sistemleri çerçevesinde gelişen birtakım etik sorunlara dikkat çekmek gerekmektedir.

Bunlar;

- Verilerin işlenmesi ve pazarlanma amacı ile ilerlenmesidir.
- Şeffaflık ilkesinin zedelenmesidir.
- Gizlilik veya mahremiyet ihlallerinin görece artmasıdır.
- Hesap verebilirliğin azalması ve yaygınlaşmasıdır.
- Birey kontrolünün dışında gözetime ön ayak olmasıdır (Karaağaçlı, 2025, s. 8).

Bu çerçevede etik ihlaller ele alındığında, verilerin işlenerek bireylerin gözetlenmesi ve dahası bir pazarlama unsuru olarak kullanılması büyük bir problem olarak yer almaktadır. Bu durumu takiben şeffaflık ilkesinin zayıfladığı ve bireylerin verilerinin sistemsel olarak kaydedildiği durum göz önüne alındığında, yapay zeka sistemlerindeki şeffaflık ilkesinin yok sayıldığı görülmektedir. Öte yandan gizlilik ve mahremiyet ihlallerinin artması, algoritmaların veriler aracılığıyla bireyleri yönlendirmesi ve yönetmesi hesap verebilirlik sorununu da beraberinde getirmektedir. Sistemin içerisinde yer alan birey ise teknolojik gelişmelerin ve çağın gerisinde kalmamak amacıyla, söz konusu sistemleri kullanmakta ancak verilerinin işlendiği, gözetlendiği bir teknolojik dünyanın içerisinde yaşamını sürdürmektedir. Bu noktada YZ destekli uygulamaların sistem içerisinde etik ilkeleri sağlayarak veya koruyarak geliştirilmesi gerekmektedir.

Floridi vd. (2018, s. 700) göre, yapay zekâ sistemleri sadece verimlilik üretme açısından değil, insan toplumlarındaki yaşamın değişimi ve karar verme süreçlerindeki dönüşümün

güçlü bir faktörü olarak ele alır. Dolayısıyla yapay zekâ sistemleri sadece doğru tahmin aracı olarak değil, aynı zamanda insanlara zarar verip vermediği, sorumluluğu üstlenebilme durumu veya adil ve özerklik durumu değerlendirmelidir. Bu bağlamda Floridi vd (2018, s. 698-701) yapay zekâ etiğini beş temel ilke ile açıklar; yararlılık, zarar vermeme, özerklik, adalet ve açıklanabilirlik olarak sınıflandırır. Bu çerçevede yapay zekâ sistemleri insana fayda sağlarken gezegen sürdürülebilirliğini ve insan refahını gözetmelidir. Zarar vermeme ilkesi incelendiğinde, bireylerin mahremiyet ihlalleri ve güvenlik riskleri üretme ihtimaliyle topluma zarar vermemelidir. Özerklik ilkesine bakıldığında bireyin karar mercinin yine bireyde kalmasına yönelik olduğudur. Yani birey, yapay zekâyı karar aşamasını sevk etse bile bu durum geri alınabilir olmalı ve kontrolün insanda olması gerektiğine yöneliktir. Adalet ilkesi ile yapay zekânın haksız ayrımcılığa yol açabilecek durumları yeniden üretmemesini ifade eder. Açıklanabilirlik ilkesi ise yapay zekânın kullanımı konusunda anlaşılabilir olması ve ortaya çıkan problemlerden kimin sorumlu olduğunun belirlenmesini içermektedir. Bir diğer ifadeyle söz konusu sistemler, bireylerin yaşamını kolaylaştırırken çevresel faktörleri ve ekosistemi koruyarak hareket etmeli ve bu konuda yapılan etik ihlali de gözetmelidir. Mittelstad'a (2019) göre ise, yapay zekâ kullanımı ile ilgili etik ilkeler yayımlamak yetersizdir, bu etik ilkelerin somut çıktılar üretmesi, yaptırımlar uygulanması gerektiğini vurgulamaktadır. Bu çerçevede AB yapay zekâ yasası çeşitli risklere ve ihlallere karşı yönetmelik ve kurallar getirmiştir. Bu kurallar arasında, kişilerin mahremiyet hakkını ihlal etmesi özellikle de biyometrik veriler aracılığıyla bireyler hakkında ırk, cinsiyet yönelimi siyasi görüş, inanç gibi etmenleri işleyen yapay zeka sistemleri yasaklanmıştır. Öte yandan insan sağlığı, güvenliği ve temel haklar üzerinde büyük zarar verme potansiyeli olan sistemler yüksek riskli olarak kabul edilmiştir. Örneğin, yapay zekâ sistemleri biyometrik sınıflandırma ile kişilerin yüz detayları, ses tonları veya davranış kalıplarını takip ederek bireyleri kategorize etmektedir. Dolayısıyla söz konusu kategorize durumu kişiler hakkında ciddi ipuçları içerdiğinden bireylerin hakları ihlal edilmektedir söz konusu durum hesapverebilirlik ve şeffaflık ilkeleri bakımından yasaklanmıştır (European Parliament & Council, 2024).

Bu anlamda bireylerin toplumsal refahı, yapay zeka destekli uygulamaların insanların mesleklerinin yerine geçmesi durumu tartışmaya açık olmakla birlikte üretkenliğe destek vermek amacıyla kullanılması, kontrol mekanizması yine birey üzerinden olması elzem olmaktadır. Etik ilkeler ele alındığında, kontrol tamamen bireyde gözükmese bile veriler işlenip, pazarlanabilmektedir. Bu anlamda makineleşme durumunun artması, insanın kontrol mekanizmasının azaldığına da işaret etmektedir. Öte yandan YZ destekli uygulamaların getirmiş olduğu bir diğer problem ise, bireylerin özgün düşüncelerinin azalması ve bireylerin bu konuda pasifleşmesi olarak da değerlendirilebilir. Çünkü birey bir fikri, bir projeyi hayata geçirirken söz konusu uygulamalardan destek almaktadır. Bu nedenle bireylerin sadece verileri değil, aynı zamanda düşünme, muhakeme kurma yetenekleri de çalınmaktadır. Bir diğer bakış açısı ise, YZ destekli uygulamaların çeşitliliğinin artmasıdır. Kullanılan çoğu dijital platformlar da örneğin; Instagram, Facebook, X gibi uygulamaların davranışı yönlendirme

algoritmaları bulunmaktadır. Bu bağlamda ise bireyler, dijital gözetimin içerisinde hapsolmaktadır. Öte yandan söz konusu platformlarda bilgi kirliliğinin artması, doğru ve yanlış haber ayrımının yapılamaması da YZ destekli içeriklerin çoğalmasından kaynaklı olmaktadır. Bu sebeple etik ilkelerin uygulanması, daha sağlıklı ve güvenilir ilişkiler geliştirmek açısından, gerekli bir durum olarak görülmektedir. Ancak YZ destekli uygulamaların artması, birçok farklı konularda da yeni uygulamaların geliştirileceği ve bireylere sunulacağı öngörülebilir bir sonuç olarak ifade edilebilir.

4. TARTIŞMA VE DEĞERLENDİRME

Teknolojik gelişmelerin getirmiş olduğu yapay zekâ destekli uygulamalar ve yeni gözetim ilişkisi derinlemesine incelendiğinde, elde edilen bulgular kapsamında veri sömürgeciliğinin ve kontrol mekanizmasının yapay zekâ destekli uygulamalar ile artış gösterdiği ve etik sorunları beraberinde getirdiği önemli bir değerlendirme olarak ön plana çıkmaktadır. Literatürde yer alan birçok yapay zekâ, gözetim ve etik ilişkisi çalışmaları bu sonucu desteklemektedir. Andrejevic (2007) “Dijital ortamda gözetim” adlı çalışmada dijital teknolojilerin bireylere kolaylık sunsa da verileri üzerinden gözetim ve ekonomik çıkarım sağlandığından söz etmiştir. Öte yandan söz konusu verilerin toplanması, bireylerin gönüllü katılımı ile sağlandığını ifade etmiştir. Zuboff’un (2019) “Gözetim kapitalizmi çağı; gücün yeni sınırında insani bir gelecek için mücadele” adlı eserinde bireylerin kişisel deneyimleri çeşitli platformlar aracılığıyla depolanması, pazarlanması ve yeniden üretilmesini konu alır. Dolayısıyla Zuboff, (2019) bu durumu davranış artığı kavramıyla açıklar; kullanıcıların fazla verilerinin işlenerek tahmin, yönlendirme gibi algoritmalara hizmet ettiğini ve davranış tahmini yapılarak bireye yeniden pazarlanması durumunu ifade eder. Bireyin bilgilerinin ticari bir meta niteliği taşıdığını ve sadece mahremiyet ile sınırlı kalmadığını dile getirir. Pasquale’ın (2015) “Kara kutu toplumu; parayı ve bilgiyi kontrol eden gizli algoritmalar” eserinde, benzer bir biçimde toplanan verilerin şeffaflık ilkesinden uzak olduğunu vurgulamaktadır. Platformların sunmuş olduğu meşru gibi görünen sözleşmeler aracılığıyla gözetim sağlanırken, şirketlerin verileri ne şekilde kullandığı tıpkı bir kara kutu gibi şeffaflık ve hesap verebilirlik ilkelerine kapalı olduğunu ifade etmektedir. Floridi vd. (2018) araştırması ise yapay zekâ sistemlerinin, veri üretimi dışında, etik ilkeleri de gözetmesi gerektiğine yöneliktir. Söz konusu sistemlerin insanlara verdiği zararları, adalet ve açıklanabilirlik bakımından şeffaf olması gerektiğini vurgulamaktadır. Bu noktada AB Yapay Zekâ Yasası (2024) etik ilke sunmaktan ziyade somut çıktılar bağlamında söz konusu biyometrik verilerin her türlü ticari kullanımını genel olarak yasaklamamaktadır; ancak biyometrik verilere dayanarak bireylerin ırkı, siyasi görüşü, dinî/felsefî inancı, sendika üyeliği, cinsel yaşamı veya cinsel yönelimine ilişkin hassas çıkarımlar yapan yapay zekâ sistemlerini yasaklayarak bir para cezası ile yaptırım sağlanmaktadır ancak bu durumun yeterli bir caydırma olmadığı düşünülmektedir. Çünkü veriler aracılığıyla elde edilen miktarlar yüksek

seviyededir. Dolayısıyla bu tür yaptırımların yaygınlaşması, katı kurallara tabii olunması, sadece belirli yapay zekâ sistemlerine yönelik değil, yapay zekâ destekli uygulamaları da kapsamı gerektiği düşünülmektedir. Bir diğer açıdan KVKK'nın (2016) veri sorumlusunun aydınlatma yükümlülüğü ele alan 10. Maddesine göre veri sorumlusu kimsenin, kişilerin verilerinin hangi amaçla işlendiği, kimlere aktarılacağı, verilerin toplanma yöntemi ve hukuki sebebi net bir biçimde belirtmelidir. Dolayısıyla aydınlatma yükümlülüğünün sağlanması gerekmektedir. Ancak yapay zekâ destekli uygulamalar uzun ve karmaşık kullanıcı sözleşmeleri ile onay alırken bu soruların net bir karşılığı bulunmamaktadır. Bu anlamda mevcut olan yasalar ve yaptırımlar kişisel verilerin korunmasını yeteriz kılmaktadır.

SONUÇ

Sonuç olarak, yapay zekâ destekli algoritmalar aracılığı ile bireylerin biyometrik verileri, düşünceleri, davranışları şekillenerek bireye tekrardan pazarlanmaktadır. Bu bağlamda etik ihlallerin olduğu ve şeffaflık ilkesinin saf dışı bırakıldığı gözlemlenmektedir. Bir diğer ifadeyle, bireylerin verilerinin kullanılarak eylemlerinin kontrol edilmesi, yapay zekâ destekli uygulamaların hakimiyeti ele aldığı, etik ihlaller ve yaptırımların iyileştirilmediği şartlarda, dünyanın mekanikleştiği, insanların metalaştığı bir toplum haline gelmesi durumu söz konusu olmaktadır. Öte yandan iletişim teknolojilerinde yaşanan bu dönüşüm ile gözetim ve mahremiyet olguları da değişmiş ve dönüşmüştür. Bu nedenle bu çalışma, değişen iletişim modelinin bireyler üzerinde yaratmış olduğu etkileri, teknolojinin çok katmanlı şekilde ilerleyerek gözetimi rutin bir yaşam pratiği haline dönüştürdüğü de önemli bir değerlendirme olarak ifade edilebilir. Bir diğer ifadeyle kullanıcı deneyimleri baz alınarak, gözetim kavramı incelendiğinde panoptik gözetim ile bireylerin tepeden gözetlenme durumu yani azınlığın çoğunluğu gözetlemesi ele alınırken, sinoptik gözetimde çoğunlukta olan bireylerin azınlığı gözetleme durumu ele alınmaktadır. Bu anlamda iki kavram, akışkan gözetim ile ağlar arasında akan bir veri ve gözetlenme durumunu ifade etmektedir. Yeni gözetim şekli, yapay zekâ destekli uygulamalar ile ilişkilendirildiğinde, ağlar arasında akan akışkan gözetimin varlığını sürdürdüğü bir sistem yapısını kapsamaktadır. Çünkü bireyler dijital ayak izi bırakarak, YZ tarafından gözetlenmekte ve verileri işlenmektedir. Dolayısıyla yeni gözetim biçiminde, birey veri sömürgeciliğinin başlıca öznesiyken, YZ uygulamalarının ise bir denetim mekanizması haline geldiği değerlendirilmektedir. Bu anlamda kontrol aracının etik ilkeler çerçevesinde, insanlar üzerinden gerçekleşmesi elzem bir durum olarak görülmektedir. Bir diğer ifadeyle YZ uygulamalarının gözetim olgusunu ileriye taşıdığı, kontrol mekanizmasının sistem içerisinde belli başlı kullanıcı sözleşmeleri ekseninde geliştiği ve kullanıcıları yönlendirme ve yönetme gücünü elinde tuttuğu açıkça ifade edilebilir. Dolayısıyla şeffaflık ve hesap verebilirlik ilkeleri ekseninde etik ilkelerin ve somut yaptırımların güçlenmesi, kullanıcıların kişisel haklarını korurken, oluşabilecek siber saldırılara karşı da bir önlem niteliği taşıyacaktır.

Öneriler

Bu çalışma yeni gözetim perspektiflerini ele alırken günümüzde sıkça kullanılan yapay zekâ uygulamalarının yeni gözetlenme biçimlerini, etik ihlallerini ve mahremiyet unsurlarını değerlendirerek bireylerde farkındalık oluşturmaya amaçlamıştır. Bu çalışmanın gelecek çalışmalara perspektif sunması, YZ uygulamalarının getirmiş olduğu etik sorunlar, gözetimin dönüşmesi gibi konuların iletişim temelinde daha fazla bilimsel katkıya ihtiyaç duyduğu açıkça görülmektedir. Bu nedenle kullanıcı deneyimleri, algoritmaların işlevleri, etik sorunlar çerçevesinde belirli YZ destekli uygulamalar ve kullanıcı sözleşmesi incelenerek çalışılması önerilebilir.

KAYNAKÇA

- Andrejevic, M. (2007). Surveillance in the digital enclosure. *The Communication Review*, 10(4), 295–317.
- Asıl, S. (2025). Yapay zekâ destekli gözetim ile ilgili çalışmaların bibliyometrik analizi. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 27(4), 1418–1448.
- Aydoğan, F. (2019). Tekno-metalaşan ve "emeğe" dönüşen oyun. In F. Aydoğan (Ed.), *Endüstri 4.0 ve dijital medya* (pp. 57–71). Der Yayınları.
- Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. Polity Press.
- Burrell, J., & Fourcade, M. (2021). The society of algorithms. *Annual Review of Sociology*, 47(1), 213–237. <https://doi.org/10.1146/annurev-soc-090820-020800>
- Castells, M. (2009). *The rise of the network society*. Wiley-Blackwell.
- Clarke, R. (2005, April 30). *Have we learnt to love Big Brother?* Retrieved January 20, 2026, from <http://www.rogerclarke.com/DV/DV2005.html>
- Couldry, N., & Mejias, U. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.
- Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence*. Yale University Press.
- Deleuze, G. (1992). Postscript on the societies of control. *October*, 59, 3–7.
- European Parliament, & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
- Foucault, M. (2019). *Hapishanenin doğuşu* (M. A. Kılıçbay, Trans.). İmge Kitabevi.
- Giddens, A. (2008). *Ulus devlet ve şiddet* (C. Atay, Trans.). Kalkedon Yayınları.
- Haggerty, K., & Ericson, R. (2000). The surveillant assemblage. *The British Journal of Sociology*, 51(4), 605–622.
- Hassan, A. A. (2017). *İletişim aracı olarak akıllı telefonlarda mobil internet kullanımının incelenmesi: Somali örneği* [Unpublished master's thesis]. İstanbul Kültür Üniversitesi.
- İplikçi, H. G. (2015). İletişimde temel modeller ve kitle iletişim modelleri. *Sosyal ve Beşeri Bilimler Dergisi*, 7(2), 15–25.
- Jonas, H. (1984). *The imperative of responsibility: In search of an ethics for the technological age*. University of Chicago Press.

- Kalaman, S. (2019). Yeni medya ve dijital gözetim: Türkiye'deki sosyal medya kullanıcıları üzerine bir araştırma. *Yönetim ve Ekonomi Dergisi*, 26(2), 576–594.
- Kant, I. (2012). *Groundwork of the metaphysics of morals* (M. Gregor & J. Timmermann, Eds.). Cambridge University Press.
- Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59–68. <https://doi.org/10.1016/j.bushor.2009.09.003>
- Karaağaçlı, M. (2024). *İleti ve öğretide teknoloji*. Bizim Büro Basımevi Yayın ve Dağıtım Hizmetleri.
- Karaağaçlı, M. (2025). Yapay zeka uygulamalarında etik gereksinimi. *Uluslararası Bilişim Sistemleri ve Uygulamaları Dergisi*, 1(1), 1–18.
- Korkmaz, İ. (2013). Facebook ve mahremiyet: Görmek ve gözetlenmek. *Yalova Sosyal Bilimler Dergisi*, 3(5), 107–122.
- KVKK. (2016). 6698 sayılı Kişisel Verilerin Korunması Kanunu. Resmî Gazete.
- Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. University of Minnesota Press.
- Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Open University Press.
- Lyon, D. (2013). *Gözetim çalışmaları* (A. Toprak, Trans.). Kalkedon Yayınları.
- Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, 1(2), 215–234. <https://doi.org/10.1177/1362480697001002003>
- Mill, J. S. (1986). *Faydacılık* (Ş. Coşkunlar, Trans.). Meb Yayınları.
- Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1(11), 501–507.
- Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.
- Petersen, J. K. (2007). *Understanding surveillance technologies: Spy devices, privacy, history & applications*. Auerbach Publications.
- Srnicek, N. (2017). *Platform capitalism*. Polity Press.
- Staples, W. (2013). *Everyday surveillance: Vigilance and visibility in postmodern life*. Rowman & Littlefield.
- TÜİK. (2025). *Yapay zeka istatistikleri*, 2025. Retrieved March 12, 2026, from <https://data.tuik.gov.tr/Bulten/Index?p=Yapay-Zeka-Istatistikleri-2025-57945>

- Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, 4(5), 193–220.
- Westin, A. (1967). *Privacy and freedom*. Atheneum Publishers.
- Yengin, D. (2014). *Yeni medya ve dokunmatik toplum*. Derin Yayınları.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.