DOĞUŞ ÜNİVERSİTESİ DERGİSİ
DOGUS UNIVERSITY JOURNAL
e-ISSN: 1308-6979
https://dergipark.org.tr/tr/pub/doujournal

DIGITAL SURVEILLANCE AND ALGORITHMIC POWER: A THEORETICAL READING THROUGH FOUCAULT, WEBER, AND ZUBOFF

DİJİTAL GÖZETİM VE ALGORİTMİK GÜÇ: FOUCAULT, WEBER VE ZUBOFF ÜZERİNDEN KURAMSAL BİR OKUMA

Büşra YİĞİTOL[(1)]

Abstract: This study offers a theoretical framework for the digital age of surveillance by reconciling Foucault's theory of disciplinary power, Weber's idea of rational bureaucracy and Zuboff's concept of surveillance capitalism. Moving beyond descriptive accounts, the study introduces the concept of "algorithmic power" to conceptualize contemporary digital surveillance as a form of governance operating at the intersection of discipline, bureaucratic rationality, and data-driven economic processes.

The study demonstrates that digital technologies, including artificial intelligence, big data, the Internet of Things (IoT), blockchain, and digital twins, not only collect data but also predict, shape, and assign economic value to individual behavior. In this context, Foucault's model of self-discipline transforms into automated algorithmic control; Weber's rationalization transforms into data-driven bureaucratic governance; and Zuboff's surveillance capitalism provides the economic logic that commodifies behavioral data.

By combining classical social theory with contemporary digital infrastructures, this study contributes to the literature by offering an integrated conceptual perspective for understanding how power is restructured in data-driven societies. It also examines the functional dimensions of digital surveillance (such as efficiency, security, and predictive capacity) and its critical consequences, including the erosion of privacy, the ethical uncertainty, and the weakening of individual autonomy.

Keywords: Digital Surveillance, Artificial Intelligence, Digital Panopticism, Algorithmic Management, Surveillance Capitalism

***JEL*:** *M10, L10, L20, O30*

Öz: *Bu çalışma, Foucault'nun disiplin gücü teorisini, Weber'in rasyonel bürokrasi fikrini ve Zuboff'un gözetim kapitalizmi kavramını uzlaştırarak, dijital gözetim çağı için teorik bir çerçeve sunmaktadır. Tanımlayıcı açıklamaların ötesine geçen çalışma, çağdaş dijital gözetimi, disiplin, bürokratik rasyonellik ve veri odaklı ekonomik süreçlerin kesişim noktasında işleyen bir yönetim biçimi olarak kavramsallaştırmak için "algoritmik güç" kavramını ortaya koymaktadır.*

Çalışma, yapay zekâ, büyük veri, Nesnelerin İnterneti (IoT), blok zinciri ve dijital ikizler de dahil olmak üzere dijital teknolojilerin yalnızca veri toplama araçları olarak işlev görmekle kalmayıp, aynı zamanda bireysel davranışları tahmin etmede, şekillendirmede ve ekonomik olarak değerlendirmede aktif olarak rol aldığını göstermektedir. Bu bağlamda, Foucault'nun öz disiplin modeli otomatikleştirilmiş algoritmik kontrol biçimlerine dönüşür; Weber'in rasyonelleştirmesi veri odaklı

[(1)] Necmettin Erbakan Üniversitesi, Havacılık ve Uzay Bilimleri Fakültesi, Havacılık Yönetimi Bölümü; busra.yigitol@erbakan.edu.tr, ORCID: 0000-0002-7846-3393
Geliş/Received: 09-11-2025; Kabul/Accepted: 05-05-2026

Atıf bilgisi: Yiğitol, B. (2026). Digital surveillance and algorithmic power: A theoretical reading through Foucault, Weber, And Zuboff. *Doğuş Üniversitesi Dergisi*, *27*(1), 1141-1159, DOI: 10.31671/doujournal.1820379.

bürokratik yönetime dönüşür ve Zuboff'un gözetim kapitalizmi, davranışsal verilerin metalaştırıldığı ekonomik mantığı sağlar.

Klasik sosyal teoriyi çağdaş dijital altyapılarla birleştirerek, bu çalışma, veri odaklı toplumlarda gücün nasıl yeniden yapılandırıldığını anlamak için bütünleşik bir kavramsal bakış açısı sunarak literatüre katkıda bulunmaktadır. Ayrıca, dijital gözetimin işlevsel boyutlarını (verimlilik, güvenlik ve tahmin kapasitesi gibi) ve mahremiyetin aşınması, etik belirsizlik ve bireysel özerkliğin zayıflaması gibi kritik sonuçlarını da incelemektedir.

Anahtar Kelimeler: *Dijital gözetim, yapay zekâ, dijital panoptisizm, algoritmik yönetim, gözetim kapitalizmi*

1. Introduction

In our age, where digital technologies transform daily life, institutional processes, and public administration, surveillance is redefined not only as a monitoring technique but also as a form of governmentality intertwined with the production of information, the circulation of power, and the creation of economic value (Sreekumar & Balakrishnan, 2025; Werbin & Shade, 2025). Technologies such as artificial intelligence, big data analytics, the Internet of Things (IoT), blockchain, and digital twins, by making behavior visible, classifying it, and predicting it, are both strengthening the quest for order and security in modern society and generating new ethical tensions around privacy, autonomy, and justice (Capurro, 2017; Graglia et al., 2021; Royakkers et al., 2018). This necessitates a re-reading of classical socio-theoretical frameworks in the digital age.

This study develops an integrative theoretical framework for understanding surveillance in the digital age by bringing together Foucault's concept of disciplinary power, Weber's notion of rational bureaucracy, and Zuboff's theory of surveillance capitalism. Accordingly, the study conceptualizes contemporary digital surveillance as a form of "algorithmic power" operating at the intersection of discipline, bureaucratic rationality, and data-driven economic processes. By re-evaluating classical social theory in relation to contemporary digital infrastructures, the article moves beyond descriptive analyses and offers a conceptual lens for understanding how power is reconfigured in data-driven societies, while also addressing the associated risks, opportunities, and ethical tensions. In this context, algorithmic power emerges not merely as a technological phenomenon, but as a multi-layered form of governance that directs behavior, organizes information, and generates economic value.

The analysis proceeds in two steps. First, it brings together three complementary perspectives—Foucauldian discipline, Weberian rationalization, and Zuboff's surveillance capitalism—to establish a unified conceptual foundation for understanding surveillance. Second, it connects this theoretical framework to contemporary digital technologies, including artificial intelligence, big data, IoT, blockchain, and digital twins. Together, these perspectives and technologies demonstrate how surveillance has evolved into a pervasive infrastructure that operates across both spatial and temporal dimensions.

2. Perspectives on Surveillance

Understanding the forms of surveillance in the digital age cannot be achieved by focusing solely on technological tools or data infrastructures; rather, it requires a discussion of the power, rationality, and economic dynamics underlying this phenomenon at a conceptual level. Therefore, to understand the phenomenon of surveillance, this study presents the three basic theoretical approaches that address surveillance from different perspectives.

Foucault's Panopticon

Michel Foucault considers surveillance not only as a mechanism limited to the function of monitoring, controlling, or repressing, but also as a fundamental knowledge-power technology that enables modern society to operate at micro-levels of power (Foucault, 2005). In this sense, surveillance signifies the penetration of power into the entire social body through decentralized forms. Therefore, Foucault's understanding of surveillance is not only a form of control exercised by the state or institutions, but also a set of mechanisms of self-discipline that individuals exercise on themselves (Manokha, 2018).

In Discipline and Punish: The Birth of the Prison (1979), which marked a turning point in the understanding of modern forms of power, Foucault considered the Panopticon metaphor the most functional model of modern power (Foucault, 1979). Foucault's conceptualization is based on the Panopticon design developed by Jeremy Bentham in the 18th century. Bentham's proposed structure is a circular architectural model designed to maintain order and control in prisons. Thanks to the central watchtower, the guard can see all the prisoners, while the prisoners cannot see the observer (Bentham, 2011). This asymmetrical relationship of visibility transforms the Panopticon from a mere architectural arrangement into a technique of power.

What is decisive in this model is not constant surveillance itself, but the internalization of the possibility of being observed. Surveillance does not require external force to regulate behavior. In Bentham's model, the observer is invisible; however, its presence is constantly felt (Bentham, 2016). Therefore, even if the individual does not know whether they are being watched, they are compelled to act as if they were constantly being watched. This is precisely where the importance of the Panopticon emerges for Foucault: this model shows that power operates not only through oppression and coercion, but also through visibility and self-discipline (Özdemir, 2020). For Foucault, power is therefore productive: it functions by inducing individuals to participate in practices and activities they come to perceive as being in their own interest (Greco, 1993). Therefore, the Panopticon becomes an explanatory metaphor for understanding not only prisons, but also the entirety of the modern social order, including schools, hospitals, factories, and bureaucratic institutions (Foucault, 1979, 2002, 2012).

Additionally, Foucault conceptualizes the Panopticon as a space in which power and knowledge production converge, in contrast to Bentham's utilitarian intent. Surveillance not only punishes; it also produces knowledge (Manokha, 2018). Every observation, record, and statistic collects data about individuals' behavior; these data produce new norms, and norms lead individuals to evaluate themselves according to these criteria(Matzner, 2017).In this sense, surveillance operates as a cyclical process that reproduces power through the management of information. This interpretation is further supported by Giddens' conceptualization of surveillance as a fundamental

institutional characteristic of modernity, whereby states and organizations monitor populations to administer, coordinate, and regulate social life(Giddens, 1986).Consequently, surveillance in modern societies serves not only as a disciplinary mechanism but also as an informational infrastructure essential to governance.

When viewed from this perspective, the surveillance order of the digital age can be seen as a data-driven continuation of Foucault's panoptic model. Surveillance is no longer limited to physical spaces; it now extends beyond them to include smartphones, social media interactions, sensors, and artificial-intelligence-supported security cameras, with many digital devices functioning as panoptic cells that observe individuals' behavior. Today's individual lives under the constant awareness of being "monitored". This awareness enables the individual to regulate their own behavior, reproducing the self-discipline mechanism described by Foucault (Manokha, 2018)

In Foucault's analysis of disciplinary society, power is a networked (diffuse) structure rather than a hierarchical structure; that is, it is reproduced everywhere by everyone (Brown, 2006). Digital panopticism is also, in this sense a form of “decentralized” surveillance. There is no longer a single overseer; on the contrary, surveillance operates automatically through data. Individuals are both the observed and the observer at the same time. For example, on social media, users both monitor others' behavior and knowingly create a “digital showcase” by allowing their own behavior to be monitored.

Foucault's emphasis on the "knowledge–power" relationship also helps to explain digital surveillance. Digital technologies have the capacity to predict, classify, and direct individuals' behavior by processing large datasets. These data have become the most important form of capital in modern power structures. Information produces power; power produces information. Therefore, digital surveillance is not only an act of observation but also a process of information production. Individuals' online movements, purchasing preferences, social relationships, and even emotional reactions become raw materials for algorithms. Thus, Foucault's disciplinary societies have given way to the "data society" in the 21st century. However, this transformation should not be understood as the complete disappearance of disciplinary society. Rather, disciplinary mechanisms persist while being reconfigured through data infrastructures, continuous tracking, and predictive modulation. In this respect, Deleuze’s (2017) notion of the “society of control” provides an important bridge for understanding how surveillance has evolved from enclosed disciplinary institutions toward more fluid, continuous, and networked forms of monitoring in the digital age.

Weber’s Bureaucracy

Surveillance has always existed in social life, but its scope has expanded significantly with the rise of modernity and the emergence of the centralized bureaucratic state. Surveillance has become a fundamental tool for the maintenance of capitalist production relations, the functioning of the bureaucratic apparatus, and the legitimization of state power. In fact, 19th-century understandings of modernism and rationality attribute their motivations for order and control to eliminating uncertainty and to ensuring sustained efficiency, or, in other words, stability (Jarvis, 2005). This perspective is consistent with Max Weber's theory of bureaucracy. The most distinctive feature of modern society, as defined by Max Weber (Sean and Joshua, 2007), is the process of rationalization. According to Weber, modernization is the process of purifying social life of emotions and beliefs and of making it calculable,

measurable, and controllable. This is the most advanced form of rational-legal authority, and this understanding gave rise to a new form of governance characterized by bureaucracy and technical rationality (DiMaggio and Powell, 1983). Bureaucratic administration requires a knowledge-based control and inspection system at its core (Weber, 1995). Although the contemporary experience of bureaucratic organizations is often negative (people see them as slow, impersonal and inefficient, full of too much "bureaucracy"), Weber saw bureaucracy as a rational administrative structure that will manage and regulate the human nature of employees (Gould and Howson, 2021).

However, Weber's observations reveal that this rational structure also creates an “iron cage” (Mitzman, 2002). The successful operation of a bureaucracy depends on several factors (for example, clear lines of authority and written rules), but its capacity to monitor and control its members is particularly important. (Gould and Howson, 2021) This monitoring, known as surveillance, is enabled by knowledge and direct control. Individuals surrender their free will to the dominance of rules in the name of effectiveness and efficiency and lose it within the bureaucratic order (Preston, 1987).

Within this framework, the 'iron cage' approach seeks an individual who is a 'soldier'. This figure represents a mechanical soldier who operates under temporal and movement constraints and follows instructions. The system regards each individual in relation to their own efficiency and responsibility and attributes their success and happiness to their effectiveness (Özcan, 2014).

The iron cage approach not only sees people as soldier-like figures within organizational boundaries but also extends this characterization beyond the organization. In other words, it has also affected individuals' social lives. The management approach, characterized by hierarchy, rules and principles within the organization, standardization, and efficiency, has shifted from people's work lives to their lives outside of work (Milton, 1962; Wolin, 2004; Orwell, 2019). Bauman describes this approach, which focuses on control and supervision, as 'gardening' (Bauman, 1998). To ensure order and efficiency, a garden with defined boundaries requires ongoing design. Otherwise, a disease state arises. Therefore, monitoring, observation, and control are considered necessary practices to ensure discipline and order.

This understanding of Weber has become even more visible in the digital age. Today’s digital surveillance mechanisms have transformed the bureaucratic rationality that Weber envisioned into an algorithmic, automated form (Muellerleile and Robertson, 2018). Artificial intelligence, big data, and automation systems have transformed decision-making processes in organizations from being “human-centered” to “data-centered”. These systems use statistical models and algorithmic evaluations to measure employee performance, customer behavior, or citizen mobility. Thus, advances in modern technology seem to strengthen the core qualities of bureaucracy (Newman et al., 2022). The rational-bureaucratic form of power described by Weber is being reproduced through digital technologies; a numerical bureaucracy is emerging in which algorithms, rather than humans, control, measure, and direct.

While this situation has positive consequences such as “objectivity of decisions” and “increased efficiency”, it also raises serious ethical and social questions. The instrumental reason conceptualized by Weber brings with it the risk of “instrumentalizing humans” through data-driven decision mechanisms in the digital age (Rosa and Antonino, 2025). Individuals are no longer merely subjective, governed beings but are also data objects transformed into inputs for algorithms. In this context,

digital surveillance systems represent a new version of Weber's “iron cage”: a social structure that is smarter, more efficient on the surface, but at its core more determined and less free (Jorna and Wagenaar, 2007; Lee, 2020; Zuurmond, 1998).

From the perspective of Weber's typology of legitimate authority (traditional, charismatic, and rational-legal), digital surveillance can be interpreted as an automated form of rational-legal authority. In this context, legitimacy is not based on charisma or belief, but on trust in data, algorithms, and numerical accuracy. Society confers a new form of legitimacy by believing in the “neutrality” of technological systems rather than in that of rulers. However, this legitimacy is superficial because algorithms are coded by humans and thus reflect value-laden biases.

From a Weberian perspective, digital surveillance is both the culmination and paradox of modern society's “ideal of rationalization”:

• On the one hand, it provides measurability, effectiveness and order;

• Conversely, it restricts individual autonomy by confining him to the system's rules.

Zuboff's Surveillance Capitalism

Shoshana Zuboff (2023), in her work The Age of Surveillance Capitalism, introduces the concept of “surveillance capitalism” by adapting Foucault's disciplinary society and Weber's bureaucratic rationality to the logic of the digital age. This concept clarifies the economic logic underlying contemporary surveillance. According to Zuboff, contemporary forms of surveillance are no longer merely tools of political or institutional control; they have also become a fundamental source of economic accumulation (Zuboff, 2023). Zuboff (2019a) defines the most distinctive feature of the digital age as the constant monitoring and recording of individuals' behavior and the transformation of these data into economic value. It states that digital surveillance has become not only a mechanism of power but also a new economic production model. Behavioral data have become not only a tool of control but also a commodity that can be converted into capital (Zuboff, 2016).

While classical capitalism creates value through physical labor and material means of production, surveillance capitalism transforms human behavior and digital traces into a commodity that serves as a basic input to the production process (Wallace, 2022). Digital platforms collect individuals' clicks, location data, social-media activity, and search histories, which they analyze and process using behavior-prediction algorithms. In this process, the human experience itself becomes an economic commodity. According to Zuboff, this new production style converts “human behavioral surplus(into)economic gain”, that is, the digital traces left behind without individuals' awareness (Zuboff, 2023).

Surveillance capitalism reproduces Foucault's notion of panoptic power through market logic. Surveillance is no longer used solely to discipline or control; it is also employed to maximize profit. Digital platforms (such as Google, Meta, Amazon, TikTok) monitor user behavior and predict personal preferences; these predictions are used in advertising, product recommendation, and political guidance processes (Zuboff, 2019b). In this way, surveillance capitalism centralizes information and power, turning individuals into marketing objects without their awareness (Cheney-Lippold, 2017; Prey, 2018). Digital platforms reconceptualize capitalism by transforming into infrastructural intermediaries that extract value from data generated by users, employees, and partners. Indeed, in the literature, platform capitalism is

closely linked to surveillance capitalism: the accumulation, processing, and monetization of behavioral data under platform business models (Langley & Leyshon, 2017; Srnicek, 2017).

Another important consequence of surveillance capitalism is that individuals' behavior is not only monitored but also directed. According to Zuboff, contemporary digital systems operate not merely through the extraction of behavioral data, but through mechanisms of behavioral modification designed to influence future preferences and actions (Darmody and Zwick, 2020). In other words, this behavioral modification process can also be presented as a softened version of "digital totalitarianism" (Zuboff, 2019a). In this sense, digital platforms do not simply register users' desires; they actively participate in producing and organizing them. For example, online recommendation systems and targeted advertising guide users' preferences in an algorithmically determined, rather than random, manner (Thaler and Sunstein, 2009). While individuals voluntarily engage with platforms, they constantly produce data and contribute to the commercialization of their own behavior through these data.

Zuboff's concept of surveillance capitalism provides a powerful framework for understanding the economic logic of data extraction. This approach has been further developed by academics. Couldry and Mejias (2019) introduce the concept of "data colonialism," arguing that contemporary data applications represent a new form of resource extraction where human life itself becomes a raw material for economic accumulation. Similarly, Thatcher et al. (2016) conceptualize data as a power field, highlighting how data infrastructures reshape social, spatial, and economic relations. Collectively, these perspectives demonstrate that digital surveillance is not merely a control mechanism but also a system of resource extraction, accumulation, and structural transformation.

3. Digital Technologies and Surveillance: Re-reading Classical Theories of Control

The defining feature of the digital age is the widespread automation and algorithmic processing of information and data. This transformation has not only expanded surveillance quantitatively but also transformed it qualitatively. Surveillance is no longer a visible “monitoring” activity; it has become an invisible digital infrastructure woven with continuous, predictive data flows. In other words, we are now living in an era of “ubiquitous” or “liquid” surveillance(Bauman and Lyon, 2013).

The basic technologies used in today's surveillance systems perform data collection, analysis, and behavior prediction functions simultaneously (Wong, 2023). Modern surveillance systems are becoming increasingly integrated with other security measures, creating comprehensive security ecosystems that protect assets, information, and individuals more effectively than ever before (Ibrahim, 2016). Although these technologies are developed with the aim of increasing social order, security, and efficiency, they are also part of a powerful network that shapes individual behavior. From facial recognition systems at airports to location tracking on our smartphones, surveillance technology is shaping the way we behave and even changing the way our brains work (Jorna and Wagenaar, 2007). While these innovations offer advantages such as increased security, they also raise significant concerns, especially regarding privacy and personal freedoms(Wheatley, 2024).The amount of data collected by these technologies is staggering, and questions about the

ethical use of this data are at the heart of ongoing debates about digital rights (Stovpets et al., 2023; Wong, 2023).

3.1. Artificial Intelligence: Automated Surveillance and Algorithmic Discipline

Among the primary technologies in digital surveillance systems, artificial intelligence stands out as particularly revolutionary. Artificial intelligence has become one of the most influential components of contemporary digital surveillance systems. The integration of artificial intelligence into surveillance infrastructure represents a paradigm shift in security technology. By analyzing large volumes of data from multiple sources, machine-learning algorithms can identify patterns and anomalies that human operators cannot detect in real time (Aloisi and Gramano, 2019). This capability has the potential to prevent incidents by providing proactive threat detection.

Algorithms used in applications such as image recognition, face matching, behavior analysis, and emotion detection are deployed across a wide range of contexts, from security cameras to social media platforms, and algorithmically categorize individuals according to their online activities(Pasquale, 2015).AI algorithms can identify potential security risks in real time. AI-powered behavior analysis goes beyond simple motion detection by analyzing complex human behavior patterns to detect potentially suspicious activity (Muzaffar and Mazher, 2024). It improves the accuracy and speed of facial recognition systems and can learn to recognize suspicious behavior patterns. Intelligent systems can distinguish between real threats and harmless events. False alarm reduction is a critical application of artificial intelligence in surveillance, addressing one of the most significant challenges in traditional systems. By accurately distinguishing between real threats and harmless events (such as animals triggering motion sensors), AI-powered systems significantly reduce the burden on human operators and increase overall system reliability (Malik, 2024). AI technology in surveillance provides speed and accuracy in crime prevention, crisis management, and public safety processes, reduces human error, and produces data-driven decisions. In addition to these benefits, it brings a number of challenges and risks. When the main difficulties and risks are examined, algorithmic biases can replicate discriminatory outcomes (Sahakyan et al., 2025).

Algorithmic bias can lead to serious ethical issues, especially in areas such as surveillance, hiring, and performance scoring, and create a false perception of “data-driven objectivity” as neutral (Kirkpatrick, 2016). The lack of transparency in decision-making processes leads to the “black box” problem (Pasquale, 2015). Our inability to see how deep learning systems make their decisions, known as the "black box problem"," poses a significant challenge. Continuous analysis of individuals' emotional and behavioral profiles may cross ethical boundaries. As these systems become increasingly powerful and widespread, it is vital to strike a balance between security needs and privacy rights (Wong, 2023). The development and deployment of surveillance technologies must be supported by robust legal frameworks and ethical guidelines to ensure their responsible use (Kirkpatrick, 2016).

In all these ways, AI-supported surveillance systems automate Foucault's concept of "self-discipline", by shifting the regulation of individual behavior from conscious self-control to algorithmic feedback loops. For example, digital platforms that constantly measure employee performance or social media algorithms that optimize user interactions confine the individual to an invisible normative framework, and the

individual voluntarily learns to behave in accordance with the system's expectations. Thus, Foucault's notion of the "internalization of power" is rendered as an automated form of discipline by machine learning. At the same time, these systems translate Weber's ideal of "rationalization" into an algorithmic mind: the goals of efficiency, predictability, and measurability are achieved by transferring bureaucratic control over human judgment to the management of numerical models. Thus, Weber's "iron cage" becomes a digital cage operating within databases, in which algorithms are governed by probabilities rather than rules.

3.2. Big Data: From the Disciplinary Society to the Datafied Society

Artificial intelligence systems do not derive their capacity for decision-making and behavior prediction from "intelligence" alone, but from the huge data pools they feed on (Wong, 2023). In other words, the "intelligence" of artificial intelligence is derived from data. Algorithms can perform learning, prediction, and classification only if sufficient, appropriately varied data are collected. Therefore, human observational capacity but data-based knowledge production (Manokha, 2018). This situation concretely reflects Foucault's "knowledge–power" relationship in the digital age: surveillance redefines power by producing data as a form of knowledge. If artificial intelligence is the analytical mind of this power, then big data is its memory and infrastructure.

Big data is not merely a large volume of information; it is also a digital ecosystem defined by the four Vs: volume, variety, velocity, and veracity (Emmanuel and Stanier, 2016). This ecosystem is fueled by a constant flow of data generated by individuals' digital interactions, sensors, social media activities, financial transactions, and public surveillance systems(Matzner, 2016).These data are collected according to the logic of total monitoring rather than by classical statistical sampling: society becomes a continuously observed population rather than a sample(Hintz et al., 2018).Referring to big data means not only that databases contain much more information than in the past(although this is true),but also that the new forms of "actionable intelligence" that have emerged through analysis of ever-expanding sets of these data and their areas of use are taken into account (Andrejevic and Gates, 2014). These forms of intelligence enable a wide range of applications, from algorithmic models predicting individual behavioral patterns to real-time response strategies in domains such as security, marketing, and public administration. At this point, big data and predictive analytics technologies come to the fore (Ongsulee et al., 2018). Predictive analytics estimates risk by modeling the possible behavior of individuals or groups based on historical data (Montasari, 2023). These predictions shape decision-making processes across fields, from security and the economy to politics and human resources (Andrejevic, 2014; Matzner, 2016).

Big data has become a tool of economic and political power. It is a new form of "behavioral capital (behavioral surplus)" (Zuboff, 2015). Who owns the data, who has access to it, and who can analyze it now determine economic superiority and political influence (Keddell, 2021). Weber's concept of "legitimate authority" is transformed in this context: In the contemporary world, authority is no longer derived from legal texts but from data architectures and algorithmic infrastructures. This indicates the evolution of modern power from a rational to a digital-bureaucratic form.

The measurement and predictive capacities provided by big data technologies also bring serious ethical and social risks. The constant collection of data eliminates the individual's "right to be invisible. These systems carry biases from past data into the

future (Kirkpatrick, 2016; Wong, 2023). Crime prediction algorithms can reproduce social stigma, for example, by labeling certain areas as “risky”. Thus, Foucault's idea of "the spatialization of discipline" is carried over into the digital sphere: surveillance no longer confines only individuals but also entire social geographies within normative frameworks. There are no clear boundaries regarding who collects, stores, and uses the data. In addition, individuals experience mental fatigue due to constant monitoring and data-sharing demands. As a result, big data technologies are not only tools for the production of information, but also a fundamental component of the rational surveillance regime of modern society. Weber's rational order, Foucault's logic of visibility, and Zuboff's data economy come together through these technologies to take their most concrete form in digital panopticism.

3.3. The Internet of Things (IoT): The Sensory Network of Surveillance

Big data is crucial for digital surveillance (Andrejevic, 2014; Cobbe, 2019). However, this data pool can remain continuously up-to-date and meaningful by connecting the points at which data are generated — i.e., objects, sensors, and devices — within the network (Baptist Andrews et al., 2023; Lulla et al., 2021). This is where the Internet of Things (IoT) becomes relevant. When the memory function of big data is combined with the sensory nervous system of IoT, surveillance becomes a system that focuses not only on information but also on instantaneous behavior. Thus, surveillance becomes a “living system” that monitors the present and predicts the future, rather than interpreting the past (Chen and Chen, 2018).

The Internet of Things (IoT) is a digital ecosystem in which physical objects are connected to each other through sensors, software, and network connections, producing and sharing data(Memos et al., 2018).This technology makes not only devices but also spaces, processes, and behavioral patterns digitally visible. This visibility transforms traditional surveillance, creating a form of continuous, pervasive, and autonomous monitoring.

In smart cities, Traffic cameras, air quality meters, home assistants, and wearable devices have become surveillance elements that continuously produce data (Baptist Andrews et al., 2023; Chen and Chen, 2018; Lulla et al., 2021). These devices expand the surveillance network by collecting location, voice, and image data, as well as biometric and environmental information, often without the user being aware of it. Thus, Foucault’s “panoptic tower” takes on a new form in the digital age: there is no longer a single eye watching from a central point; rather, every object becomes an observer, and every user becomes a data source. Surveillance is no longer confined to physical spaces but has become a pervasive digital environment, present ubiquitously and continuously (Memos et al., 2018; Muellerleile and Robertson, 2018).

IoT systems work in concert with big data and artificial intelligence to create a fully integrated surveillance architecture. In this architecture, every sensor, device, and user becomes a “data node”, and the flow of information operates in an uninterrupted, continuous, and self-feeding system. Surveillance is no longer based on a central authority, but on a distributed and automated algorithmic network structure (Deleuze, 2017; Sahakyan et al., 2025). Foucault’s panoptic discipline has become automated in this network, Weber’s bureaucratic order has become digitized, and Zuboff’s surveillance capitalism has become infrastructural. It produces the raw material for Zuboff’s data-mining economy. In effect, the Internet of Things functions as the nervous system of a digital surveillance society. Every data stream is transformed into

information that both describes and directs an individual's behavior. This structure elevates modern society's ideal of "rational order" to a level of technical perfection, while redefining the realm of human freedom within the limits imposed by algorithmic surveillance.

3.4. Blockchain: Transparency, Privacy, and the Temporal Dimension of Surveillance

The intense data flows generated by the Internet of Things (IoT) and big data ecosystems have not only expanded the operational capacity of surveillance systems, but have also deepened structural concerns related to data security, ownership, and control (Khan et al., 2020). Blockchain technology emerges as a new paradigm for surveillance processes. A blockchain is a system in which data are stored not in a single central location but across a distributed network, with each record cryptographically linked to every other record. This structure promises a fairer and more accountable framework for surveillance processes, based on the principles of transparency, security, and immutability (Rachamadugu and Thota, 2025). However, this transparency also creates a new paradox of visibility: the secure protection of data and individual privacy do not always align.

Blockchain technology has been developed as an infrastructure for trust and verification to mitigate the risks of "data manipulation", which arise especially in big data and IoT-based systems. The data are not stored on a central server; they are stored on each node of the network (Khan et al., 2020). This structure redefines Weber's notion of the rational-bureaucratic system in the digital realm rather than relying on a central authority, it operates through a distributed and automated order. In a Weberian sense, this is a form of government in which authority can function without "centralization" and the "rule" becomes independent of the individual. However, this decentralization does not lead to the dispersion of power; rather, it implies that power is embedded in algorithms. In Foucault's panoptic model of power, the observing subject is invisible; in the blockchain era, the subject of surveillance is not human but the distributed protocol. Surveillance is no longer the result of intention but rather of system design.

Blockchain systems stand out for their decentralization, immutability, and shared data structure, all of which contribute to a high level of transparency (Bin Saif et al., 2024). Each transaction is added to the chain with a timestamp and can be verified by all users on the network (Mohanta et al., 2021). This feature confers a substantial advantage in both accountability and fraud prevention. However, this transparency conflicts with privacy. The records stored on the blockchain are not completely confidential, because transactions can be permanently viewed on a public ledger (Joshi et al., 2018). This creates a particularly complex tension with the European Union's General Data Protection Regulation (GDPR), especially regarding the "right to be forgotten." Once added to the chain, the data can no longer be retrieved; therefore, the individual becomes infinitely responsible for his digital traces (Yassein et al., 2019). In Foucault's panoptic metaphor, the effect of surveillance operates through the individual's "possibility of being seen"; within blockchain systems, however, individuals are confronted with the permanent visibility of their past actions. Surveillance thus acquires a temporal rather than spatial dimension: the past is transformed into a persistent data record that constitutes individual identity and cannot be modified or removed.

According to Weber, blockchain digitizes the “rule-based order” principle of modern bureaucracy. The rule supplants human will in this context; processes become mechanized, and rational management aligns with technical reason. For Foucault, this system produces an invisible form of “disciplinary power”: the individual is no longer directly monitored but cannot avoid leaving traces. Zuboff, on the other hand, interprets this configuration as an advanced stage of surveillance capitalism: data is no longer only a commercial resource but an ontological one — the individual's identity, behavior, and history become fixed records in the chain. In this respect, blockchain technology reopens the debate on the “ethical boundaries of surveillance” and demonstrates that data can function both as a mechanism of assurance and as a tool of control (Joshi et al., 2018; Yassein et al., 2019).

3.5. Digital Twins: The Simulation Phase of Surveillance

While blockchain systems are primarily designed to ensure decentralized verification, security, and trust through immutable and distributed records, digital twin technology monitors the present and predicts the future (Duman, 2022; Grieves, 2016). However, digital twin technologies alone do not accomplish this. A multi-layered technological architecture is required, ranging from everyday digital interactions to complex predictive systems. At the most basic level, tracking technologies such as cookies and mobile applications enable the continuous collection of user data by recording browsing behavior, location information, and interaction patterns (Taşkaya and Talay, 2019; Değermen and Mohammadabbasi, 2023). These mechanisms form the basis of what is often described as data surveillance, where individuals are constantly monitored through digital traces created in routine activities. On a broader level, digital platforms function as central nodes of surveillance by collecting, analyzing, and monetizing large amounts of user data (Srnicek, 2017). More advanced surveillance infrastructures are clearly seen in emerging technologies such as augmented reality (AR), virtual reality (VR), mixed reality (MR), and metaverse environments (Mystakidis, 2022). These systems extend surveillance beyond screens into immersive and interactive spaces where users' movements, gestures, biometric responses, and spatial interactions can be continuously monitored and analyzed. Within this continuum, digital twin technologies represent one of the most advanced forms of surveillance infrastructure.

Digital twin logic is based on simulation and predictive control. While digital twin models simulate public transportation density, energy usage, or emergency scenarios in advance at the city scale, many parameters—ranging from health data and mental state to consumption habits and social interactions— become predictable at the individual level (Babaoğlu and Memiş, 2024; Mohammadi and Taylor, 2017; He et al., 2018; Ölmez, 2025). In the age of digital twins, surveillance serves as a tool for controlling the future. The individual is subject to the system's control, not only because of what he does but also because of what he can do. In this context, digital twins extend the temporal dimension of panoptic power, thereby transforming surveillance into a form of “domination that extends into the future”.

While digital twin technology offers significant opportunities for risk management, sustainability, and resource efficiency, it also raises new new ethical, ontological, and epistemological challenges. The most fundamental risk is that simulation replaces reality (Grieves, 2016). Data-driven models not only represent the world but increasingly shape it over time. This transformation destabilizes the final stage of Weber's rationalization process, the invisible form of Foucault's disciplinary power,

and the self-reproducing structure of Zuboff's surveillance capitalism. Surveillance is no longer merely about monitoring the individual; it also involves modeling the individual's future.

Digital twins are at the intersection of artificial intelligence, big data, IoT, and blockchain technologies. This convergence is also evident in metaverse environments, where virtual replicas of physical spaces, services, and even individuals can be created, monitored, and interacted with in real time. In this sense, the metaverse represents an additional layer in which digital twins operate through immersive simulation, platform governance, and, in some cases, blockchain-based infrastructure (Yitmen et al., 2023). The intersection of all these technologies creates a fully automated form of digital panopticism. Weber's "iron cage" has now become a digital prison composed of invisible layers of data. Foucault's panopticon has taken on a new digital form, consisting of sensors, networks, and simulations. Zuboff's surveillance capitalism has turned this structure into a market order that feeds on the economy and establishes dominance through data. As a result, digital twin technologies have freed surveillance from the constraints of time and space, opening the door to a new social order grounded in the ideal of human predictability. This configuration destabilizes the ethical boundaries of knowledge and prediction and blurs the distinction between "knowing" and "managing."

4. Conclusion

This study offers a perspective on the opportunities and challenges of applying digital technologies across various dimensions of surveillance. Technologies such as artificial intelligence, big data, IoT, blockchain, and digital twins are transforming the governance mechanisms in modern society while redefining individual behavior, privacy, and freedom. The integration of digital technologies into surveillance processes has radically transformed the power relations, ethical values, and power balances within the individual–state–company triangle of modern society.

Contemporary surveillance systems no longer merely observe individuals' behavior; they also predict, direct, and convert this behavior into economic value. Thus, surveillance has transformed from a technological tool into a multidimensional management paradigm. This transformation reflects the convergence of Weberian rationalization, Foucauldian discipline, and Zuboff's surveillance capitalism. The rational-bureaucratic order described by Weber has evolved into an automated digital regime driven by algorithmic systems, while Foucault's notion of self-discipline is now reinforced through the internalization of continuous monitoring. As Zuboff emphasizes, human experience itself has become a source of economic value within surveillance-based market structures.

This emerging form of "digital panopticism" represents a new configuration of power that operates through algorithmic networks rather than centralized observation. It is diffuse yet pervasive, shaping behavior, redefining social norms, and directing economic activity. In this system, individuals not only become objects of surveillance but also active participants who internalize and reproduce control mechanisms. Consequently, surveillance increasingly functions as both a governance tool and a form of self-regulation.

However, this transformation raises critical ethical concerns regarding the balance between security and individual freedom. While digital technologies offer efficiency, predictive capacity, and enhanced social coordination, they also risk eroding privacy,

intensifying control, and undermining autonomy. Questions such as the limits of data collection and the responsibilities of states and corporations are becoming increasingly urgent.

Ultimately, the technological rationality of the digital age produces a hybrid form of power—algorithmic power—that combines instrumental reason (in the Weberian sense), Foucauldian discipline, and Zuboffian market logic. This form of power is invisible but omnipresent; it shapes not only the social order but also the individual's intellectual and emotional spheres. Therefore, the ethical, legal, and social boundaries of digital surveillance technologies need to be redefined, and the concepts of privacy, data sovereignty, and digital justice need to be strengthened to serve as the new normative framework for the digital age.

References

Al-Sahan, L., Al-Jabiri, F., Abdelsalam, N., Mohamed, A., Elfouly, T., and Abdallah, M. (2020). Public security surveillance system using blockchain technology and advanced image processing techniques. *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 104–111). https://doi.org/10.1109/ICIoT48696.2020.9089523

Andrejevic, M. (2014). Surveillance in the big data era. In K. D. Pimple (Ed.), *Emerging pervasive information and communication technologies(PICT):Ethical challenges, opportunities and safeguards* (pp. 55–69). Springer. https://doi.org/10.1007/978-94-007-6833-8_4

Andrejevic, M., and Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society, 12*(2),185–196.

Babaoğlu, C., ve Memiş, L. (2024). *Dijital ikiz ve akıllı şehirler.* SETA Yayınları.

Baptist Andrews, L. J., D, S., and Raj, R. A. (2023). IoT based surveillance camera with GPS module. *2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science(SCEECS)* (pp. 1–3). https://doi.org/10.1109/SCEECS57921.2023.10062961

Bauman, Z. (1998). *Sosyolojik düşünmek* (A. Yılmaz, Çev.). Ayrıntı Yayınları.

Bauman, Z., and Lyon, D. (2013). *Liquid surveillance: A conversation.* John Wiley & Sons.

Bentham, J. (2011). *The panopticon writings.* Verso Books.

Bentham, J. (2016). *Panoptikon Gözün İktidarı* (B. Çoban & Z. Özarslan, Trans.). Su Yayınevi.

Bin Saif, M., Migliorini, S., & Spoto, F. (2024). Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain. Future Internet, 16(3), 98.

Brown, W. (2006). Power after Foucault. In J. Dryzek, B. Honig, and A. Phillips (Eds.), *The Oxford handbook of political theory* (pp. 65–84). Oxford University Press.

Capurro, R. (2017). Digitization as an ethical challenge. *Ai & Society*, 32(2), 277–283.

Chen, N., and Chen, Y. (2018). Smart city surveillance at the network edge in the era of IoT: Opportunities and challenges. In Z. Mahmood (Ed.), *Smart cities: Development and governance frameworks* (pp. 153–176). Springer. https://doi.org/10.1007/978-3-319-76669-0_7

Cheney-Lippold, J. (2017). *We are data: Algorithms and the making of our digital selves.* New York University Press.

Cobbe, J. (2019). *Big data, surveillance, and the digital citizen*. Belfast: Queen's University.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & new media*, *20*(4), 336-349.

Darmody, A., and Zwick, D. (2020). Manipulate to empower: Hyper-relevance and the contradictions of marketing in the age of surveillance capitalism. *Big Data & Society, 7*(1), 2053951720904112. https://doi.org/10.1177/2053951720904112

Değermen, A., & Mohammadabbasi, M. (2023). Using big data in analysis of consumer behavior: A qualitative study. *Kırklareli Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *12*(1), 100-122.

Deleuze, G. (2017). Postscript on the societies of control. In D. Lyon (Ed.), *Surveillance, crime and social control* (pp. 35–39). Routledge.

DiMaggio, P. J., and Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2),147–160.

Duman, M. Ç. (2022). İşletmeler için yeni bir verimlilik teknolojisi: Dijital ikiz. *Verimlilik Dergisi*, 189–206. https://doi.org/10.51551/verimlilik.981349

Emmanuel, I., and Stanier, C. (2016). Defining big data. *Communications in Science and Technology, 1*(1), 1–6.

Foucault, M. (1979). Part three: Discipline. In *Discipline and punish: The birth of the prison* (pp. 135–230). Vintage.

Foucault, M. (2002). *The birth of the clinic.* Routledge.

Foucault, M. (2005). *Özne ve iktidar* (İ. Ergüden vd., Çev.). Ayrıntı Yayınları.

Foucault, M. (2012). *Discipline and punish: The birth of the prison.* Vintage.

Giddens, A. (1986). The nation-state and violence. *Capital & Class*, *10*(2), 216-220.

Gould, M., and Howson, A. (2021). Bureaucratic surveillance. *EBSCO Research Starters.* https://www.ebsco.com

Graglia, M. A. V., Huelsen, P., & Lazzareschi, N. (2021). The growing moral challenge in the face of technologies: Internet, social networks, IoT, blockchain and artificial intelligence. *Journal on Innovation and Sustainability RISUS*, *12*(2), 17–29.

Greco, M. (1993). Psychosomatic subjects and the 'duty to be well': Personal agency within. *Economy and Society, 22*(3),357–372.

Grieves, M. (2016). *Origins of the digital twin concept.* Florida Institute of Technology/NASA.

He, Y., Guo, J., and Zheng, X. (2018). From surveillance to digital twin: Challenges and recent advances of signal processing for industrial internet of things. *IEEE Signal Processing Magazine, 35*(5), 120–129. https://doi.org/10.1109/MSP.2018.2842228

Hintz, A., Dencik, L., and Wahl-Jorgensen, K. (2018). *Digital citizenship in a datafied society.* John Wiley & Sons.

Ibrahim, S. W. (2016). A comprehensive review on intelligent surveillance systems. *Communications in Science and Technology, 1*(1).

Jarvis, T. (2005). The digital cage: Digital surveillance and bureaucratic governance. *On Politics, 1*(1),5–16.

Jorna, F., and Wagenaar, P. (2007). The 'iron cage' strengthened? Discretion and digital discipline. *Public Administration, 85*(1), 189–214. https://doi.org/10.1111/j.1467-9299.2007.00640.x

Joshi, A. P., Han, M., and Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing, 1*(2).

Keddell, E. (2021). "Make them dance": Shoshana Zuboff's surveillance capitalism, behavior modification and Fraser's "abnormal justice."

Khan, P. W., Byun, Y.-C., and Park, N. (2020). A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics, 9*(3), 484. https://doi.org/10.3390/electronics9030484

Kirkpatrick, K. (2016). Battling algorithmic bias: How do we ensure algorithms treat us fairly? *Communications of the ACM, 59*(10), 16–17. https://doi.org/10.1145/2983270

Langley, P., & Leyshon, A. (2017). Platform capitalism: The intermediation and capitalisation of digital economic circulation. *Finance and Society*, *3*(1),11-31.

Lee, R. L. (2020). Charisma and the digital age: Mass re-enchantment online and networking the new iron cage. In I. M. Sacks and W. M. Smith (Eds.), *Routledge international handbook of charisma* (pp. 457–467). Routledge.

Lulla, G., Kumar, A., Pole, G., and Deshmukh, G. (2021). IoT based smart security and surveillance system. *2021 International Conference on Emerging Smart Computing and Informatics(ESCI)* (pp. 385–390). https://doi.org/10.1109/ESCI50559.2021.9396843

Malik, S. (2024). Using AI for behavioral analytics in cybersecurity: Detecting anomalies and insider threats. *Journal of Cybersecurity Research, 5*(2), 45–60.

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance and Society, 16*(2). https://ora.ox.ac.uk/objects/uuid:a8f5e604-0e3e-42d2-b373-a4e650b39dcb

Matzner, T. (2016). Beyond data as representation: The performativity of big data in surveillance. *Surveillance & Society, 14*(2), 197–210. https://doi.org/10.24908/ss.v14i2.5831

Matzner, T. (2017). Opening black boxes is not enough: Data-based surveillance in discipline and punish and today. *Foucault Studies*, 27–45.

Memos, V. A., Psannis, K. E., Ishibashi, Y., Kim, B.-G., and Gupta, B. B.(2018). An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. *Future Generation Computer Systems, 83*, 619–628. https://doi.org/10.1016/j.future.2017.04.039

Milton, F. (1962). *Capitalism and freedom.* University of Chicago Press.

Mitzman, A. (2002). *The iron cage: An historical interpretation of Max Weber.* Transaction Publishers.

Mohammadi, N., and Taylor, J. E. (2017). Smart city digital twins. *2017 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1–5). https://doi.org/10.1109/SSCI.2017.8285439

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., and Gandomi, A. H. (2021). Addressing security and privacy issues of IoT using blockchain technology. *IEEE Internet of Things Journal, 8*(2), 881–888. https://doi.org/10.1109/JIOT.2020.3008906

Montasari, R. (2023). The application of big data predictive analytics and surveillance technologies in the field of policing. In R. Montasari (Ed.), *Countering cyberterrorism: The confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity* (pp. 81–114). Springer. https://doi.org/10.1007/978-3-031-21920-7_5

Muellerleile, C., and Robertson, S. L. (2018). Digital Weberianism: Bureaucracy, information, and the techno-rationality of neoliberal capitalism. *Indiana Journal of Global Legal Studies, 25*(1), 187–216. https://doi.org/10.2979/indjglolegstu.25.1.0187

Muzaffar, J., and Mazher, N. (2024). AI-powered behavioral analysis for insider threat detection in enterprise networks. *Baltic Journal of Multidisciplinary Research, 1*(2),1–11.

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486-497.

Newman, J., Mintrom, M., and O'Neill, D. (2022). Digital technologies, artificial intelligence, and bureaucratic transformation. *Futures, 136*, 102886. https://doi.org/10.1016/j.futures.2021.102886

Ölmez, M. (2025). Yerel sürdürülebilirlikte dijital ikiz teknolojisi ve doğal afetleri önlemede etkisi: Japonya örneği. *İşletme, 6*(1), 103–127.

Ongsulee, P., Chotchaung, V., Bamrungsi, E., and Rodcheewit, T. (2018). Big data, predictive analytics and machine learning. *IEEE Conference Proceedings,* 1–6.

Orwell, G. (2019). *1984* (C. Üster, Çev.). Can Yayınları.

Özcan, K. (2014). Yönetsel kontrol ve örgütsel düzen: Michel Foucault ve Zygmunt Bauman ekseninde bir tartışma. *Amme İdaresi Dergisi, 47*(2), 45–67.

Özdemir, M. (2020). Foucault sosyolojisinde iktidarın serüveni: Pastoral iktidar, disiplinci iktidar, biyo-iktidar. *Türkiye Siyaset Bilimi Dergisi, 4*(1), 109–133.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press.

Preston, L. M. (1987). Freedom and bureaucracy. *American Journal of Political Science, 31*(4), 773–795. https://doi.org/10.2307/2111224

Prey, R. (2018). Nothing personal: Algorithmic individuation on music streaming platforms. *Media, Culture & Society, 40*(7), 1086–1100.

Rachamadugu, S. K., and Thota, S. K. (2025). Enhancing CCTV surveillance with blockchain and AI integration. *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS, 7)* (6), 7.

Rosa, F., and Antonino, V. (2025). Humanism, dehumanization, integral human development: An overview of boundaries and capabilities of human-centered artificial intelligence in business and organizations. In *Humanism and artificial intelligence* (pp. 3–28). Springer.

Royakkers, L., Timmer, J., Kool, L., & Van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*, 20(2), 127–142.

Sahakyan, H., Gevorgyan, A., and Malkjyan, A. (2025). From disciplinary societies to algorithmic control: Rethinking Foucault's human subject in the digital age. *Philosophies, 10*(4), 73. https://doi.org/10.3390/philosophies10040073

Sean, H., and Joshua, G. (2007). *The surveillance studies reader.* McGraw-Hill Education.

Semple, J. (1992). Foucault and Bentham: A defence of panopticism. *Utilitas, 4*(1), 105–120.

Sreekumar, T. T., & Balakrishnan, S. (2025). Digital governmentality and the algorithmic state: ai surveillance in comparative perspective. *Journal of Literary and Cultural Inquiry* (ISSN: 2349-8064), *12*(1), 17–31.

Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model. *Juncture*, *23*(4), 254-257.

Stovpets, O., Borinshtein, Y., Babenko, I. Y., Kozobrodova, D., Madi, H., and Honcharova, O. (2023). Digital technologies and human rights: Challenges and opportunities. *Revista Amazonia Investiga, 12*(72), 17–30.

Taşkaya, M., & Talay, Ö. (2019). Dijital gözetimin pazarlama amaçlı aracıları: "Çerezler" ve çerez kullanımında "açık rıza". *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*, *31*, 356-376.

Thaler, R. H., and Sunstein, C. R. (2009). *Nudge: Improving decisions about health, wealth, and happiness.* Penguin Books.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990-1006.

Wallace, J. H. (2022). Surveillance capitalism, the commodification of personal behavioral data, and how it factors into our response. *Journal of Ethics & Technology, 2*(1), 11–30.

Weber, M. (1995). Bürokratik teşkilatlanmanın esasları (İ. Sezal, Çev.). Ekin Yayınları.

Werbin, K. C., & Shade, L. R. (2025). Revisiting governmentality: Collapsing information silos and emerging biopolitical economies of circulation. *Canadian Journal of Communication*, *50*(4), 762–776.

Wheatley, M. C. (2024). Ethics of surveillance technologies: Balancing privacy and security in a digital age. *Premier Journal of Data Science, 1*, 100001.

Wolin, S. (2004). *Politics and vision: Continuity and innovation in Western political thought* (Expanded ed.). Princeton University Press.

Wong, W. H. (2023). *We, the data: Human rights in the digital age.* MIT Press.

Yassein, M. B., Shatnawi, F., Rawashdeh, S., and Mardin, W. (2019). Blockchain technology: Characteristics, security and privacy issues and solutions. *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications(AICCSA)* (pp. 1–8). https://doi.org/10.1109/AICCSA47632.2019.9035216

Yitmen, I., Alizadehsalehi, S., Akiner, M. E., & Akiner, I. (2023). Integration of digital twins, blockchain and ai in metaverse: Enabling technologies and challenges. In *Cognitive Digital Twins for Smart Lifecycle Management of Built Environment and Infrastructure* (pp. 39–64). CRC Press.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*(1), 75–89.

Zuboff, S. (2016). The secrets of surveillance capitalism. *Frankfurter Allgemeine Zeitung, 5.*

Zuboff, S. (2019a). Surveillance capitalism and the challenge of collective action. *Philosophy & Technology, 28*(1), 10–29.

Zuboff, S. (2019b). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Public Affairs.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203–213). Routledge.

Zuurmond, A. (1998). From bureaucracy to infocracy: Are democratic institutions lagging? In T. J. A. B. Bekke and K. Perry (Eds.), *Public administration in an information age: A handbook* (Vol. 6, pp. 259–273). IOS Press.