AI & SOCIETY (2026) 41:415–427
https://doi.org/10.1007/s00146-025-02473-w

OPEN FORUM

Rise of the algopticon: the algoptic gaze in the age of algorithmic governance and surveillance capitalism

Trent Bax[1]

Received: 5 March 2025 / Accepted: 26 June 2025 / Published online: 9 July 2025

Abstract
This paper introduces the concept of an *algopticon* to theorize surveillance in the age of algorithmic governance and surveillance capitalism. Building on earlier surveillance models— panopticon, synopticon, banopticon, and super-panopticon—the algopticon represents a qualitative transformation in how power operates through data, prediction, and automation. Drawing on Hegel's concept of sublation (Aufhebung), the paper argues that the algopticon does not simply replace these earlier frameworks but sublates them: it negates, preserves, and elevates their core logics into a new surveillance regime. Visibility becomes invisibility; discipline becomes prediction; and observation becomes algorithmic categorization. By automating control and embedding it into everyday life, the algopticon alters subjectivity, restructures agency, and deepens asymmetries of power. Through comparative analysis, this paper shows how the algopticon consolidates disciplinary, synoptic, exclusionary, and informational logics into a pervasive system of behavioral governance. It concludes by emphasizing the ethical and political stakes of this shift and calls for algorithmic accountability, transparency, and democratic oversight to ensure that emerging technologies serve justice rather than entrench inequality.

Keywords Surveillance · Algorithms · Algopticon · Panopticon · Super-panopticon · Synopticon · Banopticon

1 Introduction

From its origins in informal community oversight, surveillance has gradually become a highly structured and technologically sophisticated tool of social organization and control in contemporary societies (Lyon 2007; Marx 2016). From Victorian-era gas lamps that illuminated streets for policing to the omnipresent security cameras of the contemporary era, surveillance practices have evolved alongside advances in science and technology (Lyon 2001; Newell 2023). Surveillance theorists have developed a range of frameworks to analyze these ever-shifting surveillance practices, with each capturing the socio-technical logics of its era (Marx 2015). Key concepts in this field include: (1) the *panopticon*, introduced by Jeremy Bentham (1791) and adapted by Michel Foucault (1977) to explain the power of the few to watch the many; (2) the *synopticon*, introduced by Mathiesen (1997) to explain the gaze of the many on the few within a viewer-centric society; (3) the *banopticon*, introduced by Bigo (2008) to examine surveillance as a mechanism for risk management and exclusion of mobile populations deemed as threats; and (4) the *super-panopticon*, proposed by Poster (1990) to highlight the embedding of surveillance within digital flows and decentralized systems.

These earlier frameworks have been further challenged by the rise of algorithmic surveillance (Andrejevic 2019) and surveillance capitalism (Zuboff 2019). Algorithms operate opaquely yet pervasively to categorize, predict, and influence human behavior in ways that were once unimaginable (Pasquale 2015). This shift to an algorithm-driven surveillance paradigm calls for a new conceptual framework: the *algopticon* (Jamil 2020). Building upon these earlier frameworks, this paper will argue that the algopticon captures the unique features of algorithmic surveillance—where certainty replaces uncertainty, invisibility replaces visibility, and control becomes predictive and automated. This paper contributes to the field of surveillance studies by tracing and comparing the theoretical foundations of the panopticon, synopticon, banopticon, and super-panopticon concepts, and then introducing the algopticon as a novel framework for understanding algorithmic surveillance. Through this

✉ Trent Bax
trentbax@ewha.ac.kr

[1] Ewha Womans University, Seoul, Republic of Korea

analysis, this paper provides a comprehensive understanding of how surveillance practices have evolved in response to technological and societal shifts. The advent of the algorithmic gaze raises significant ethical concerns surrounding privacy, bias, and the redistribution of power in a data-driven and AI-centric society (Marx 2015; Saheb 2023).

In recent decades, surveillance studies have grappled with what Haggerty (2006) describes as the overuse and the reification of the panopticon—a concept so dominant it risks stifling analytical innovation and obscuring non-panoptic forms of surveillance. As Haggerty and Ericson (2000) argue, the model can narrow scholarly focus, thereby sidelining newer dynamics, such as rhizomatic expansion, decentralization, and data-driven abstraction of bodies into 'data doubles.' These critiques are important to surveillance theory because they open space for alternative frameworks like the surveillant assemblage (Haggerty and Ericson 2000), control society (Deleuze 1992), and social sorting (Lyon 2003). Yet while the panopticon may be exhausted in some contexts, it remains foundational in others. Jamil's (2020) analysis of Uber reveals how panoptic logics—visibility, centralization, ranking, and discipline—have not vanished but evolved. App-based control, real-time monitoring, and digital confinement reinvent the panopticon for the algorithmic age. The Uber algopticon is neither architectural nor reliant on human observers, but it retains an "all-seeing power" that automates discipline and induces self-monitoring. Far from obsolete, the panopticon persists as what Lyon (2006: 4) calls "a ghost lurking within the post-panoptic world," haunting even decentralized, data-driven systems. While Lyon (2007) rightly critiques the model's limitations—its overgeneralization and neglect of digital interactivity—he acknowledges its continued relevance in enclosed spaces like prisons and workplaces, where disciplinary architectures endure. Likewise, Foucault's insights into power, subjectification, and institutional control remain important for understanding how norms are internalized—even through algorithmic mediation. As Caluya (2010) reminds us, many critics conflate Bentham's architectural design with Foucault's broader panopticism, which is not a fixed structure but a 'machine of power' that organizes space, time, and knowledge. This paper, therefore, uses the panopticon not as an endpoint, but as a historical and conceptual starting point—an indispensable historical precursor to the algopticon. As will be shown, the algopticon sublates the panopticon—preserving its core logics while surpassing its spatial and human limitations through predictive algorithms and distributed control.

The algopticon is not merely a rhetorical addition but a dialectical development. Its conceptual justification rests on a dialectical understanding of historical development, and here Hegel's (1977) notion of *sublation* (*Aufhebung*) offers a theoretical foundation. To sublate (*aufheben*) involves a dialectical process in which earlier stages are not simply negated or discarded but are preserved and transformed, allowing development to move forward through contradiction and continuity. Thus, what is sublated (*aufgehoben*) is at the same time both preserved *and* changed (Hegel 1969). In this sense, the algopticon does not erase panopticon, synopticon, banopticon, or super-panopticon, it sublates them by integrating the logics of panoptic visibility (panopticon), mass-mediated reciprocity (synopticon), and risk-based exclusion (banopticon) into a new architecture of invisible, predictive, and pre-emptive control. This is not a lateral proliferation of metaphors, but a vertical transformation: a qualitative shift in the surveillance assemblage that requires a distinct conceptual framework. The algopticon can thus earn its place not as a novelty concept but as a dialectical culmination—a form of surveillance that negates older models' visible architectures, preserves their underlying aims—such as discipline, control, risk management—and transcends them through algorithmic automation. Without a concept like the algopticon, we risk analytically flattening a profound historical development and missing the unique characteristics of algorithmic-driven surveillance.

2 Panopticon: the few watch the many

Jeremy Bentham proposed the *panopticon* in the late eighteenth century as a design for an ideal prison based on maximum visibility and minimal force. The structure placed a central watchtower within a circular arrangement of cells, ensuring that all prisoners could be observed from a single vantage point. This design was grounded in the belief that visibility could enforce discipline, and that the uncertainty of whether one was being watched would induce self-regulation (Bentham 1791). Bentham's utilitarian-based intention was to create a cost-effective mechanism for social control that reduced the need for physical force (Weinreich 2021). Michel Foucault revitalized the concept in his seminal work *Discipline and Punish* (1977), transforming it from a prison blueprint into a broader metaphor for modern disciplinary societies. Foucault argued that the panopticon exemplified how power in modern societies operates through surveillance, normalization, individualization, and self-regulation. According to Foucault, the panopticon's ability to create uncertainty allows institutions to maintain control without direct coercion, fostering a sense of internalized discipline. For Foucault, power is not centralized solely in a singular authority but is dispersed throughout society, requiring individuals to self-regulate their behavior due to the omnipresent threat of surveillance (Lyon 2007).

The panopticon is characterized by three key features: 1. *Hierarchical Power Structure*: Power is concentrated in the hands of a few observers who control the many. This

division between observer and observed underpins social power and is reflected in modern institutions that monitor populations through surveillance mechanisms (Foucault 1977). 2. *Uncertainty and Internalized Control*: The uncertainty of being watched compels individuals to self-regulate. The mere possibility of surveillance produces a disciplinary effect, leading people to internalize the gaze of authority (Manokha 2018). 3. *Visibility as Discipline*: The panopticon's architecture emphasizes visibility. Surveillance is embedded in the structure, making authority seem omnipresent. Though individuals may not know when they are being observed, the visible potential of observation keeps them in a constant state of vigilance (Foucault 1977).

While the panopticon was conceived as a physical structure, its principles resonate in contemporary forms of surveillance. In schools, workplaces, and urban environments, surveillance technologies enforce discipline and conformity (Stacy and Rodriguez 2023). CCTV cameras, for example, replicate the panopticon's dynamics of visibility and uncertainty, as individuals modify their behavior knowing they might be watched (Koskela 2003). Moreover, digital technologies have extended the reach of the panopticon into virtual spaces. Employers monitor employees' productivity (Manokha 2020), schools track students' online activities (Pangrazio et al. 2023), and governments collect vast amounts of data through surveillance programs (Rubinstein et al. 2014). Social media platforms also use algorithms to monitor user behavior, creating a digital panopticon where individuals are aware of their visibility to tech corporations but unsure of when or how they are being watched (Zuboff 2019). The digital transformation of surveillance does not simply replace Bentham's model but rather sublates it: the logic of visibility is retained in the awareness of constant monitoring, while its spatial architecture gives way to invisible, ambient algorithmic control. In this way, the panopticon's core elements—discipline through uncertainty, visibility as control, and asymmetrical power—are both preserved and transcended, reconstituted within contemporary infrastructures, such as social media, workplace monitoring systems, and state surveillance programs.

3 Synopticon: the many watch the few

Introduced by Thomas Mathiesen (1997), the *synopticon* concept inverts the top-down power dynamics of the panopticon, positing a society where the many watch the few. Mass media and emerging digital technologies enable the general public to scrutinize the powerful, reversing traditional surveillance models in which the few observe the many. This shift aligns with the rise of new forms of media and technology, such as television, reality shows, and social media platforms, which democratize the capacity for surveillance (Ellis 2021). Mathiesen expanded on Foucault's theories by arguing that surveillance was no longer just a tool for elites to control the masses, but was increasingly a mechanism of public accountability. It allowed ordinary people to act as active spectators and critique politicians, celebrities, and public figures (Doyle 2011).

One defining feature of the synopticon is the mass mediation of surveillance, where citizens—armed with digital devices and internet access—can participate in observing elites. Television, internet, and social media platforms allow users to watch events in real time, share them instantly, and form collective opinions about those being scrutinized (Shang et al. 2017). The scale of these mediated observations expands the power of the public gaze, transforming it from traditional passive viewership into an active, participatory model (Mundt et al. 2018). By enabling individuals to engage in the surveillance of institutions and individuals, social media has the ability to promote social accountability and democratize the process of observation.

Another key feature of the synopticon is *voluntary participation*. Unlike the panopticon, where surveillance is imposed and constant, individuals in the synopticon often choose to expose themselves to public observation (Bauman and Lyon 2013) although this participation is often driven by social, economic, or platform-specific pressures that limit true voluntariness. Politicians, celebrities, and influencers share aspects of their lives on social media, creating an illusion of accessibility, authenticity, intimacy, and transparency (Manning et al. 2017; Marwick and Boyd 2011). The desire for visibility is a powerful motivator as public figures invite observation to gain and maintain relevance, enhance their status, or gain economic capital. But while they can curate their own visibility, they also risk being subjected to public judgment as social media platforms amplify public reactions (Rost et al. 2016). From a Hegelian perspective, the synopticon sublates the panopticon—it preserves the disciplinary function of surveillance but transforms it through voluntary exposure and mass mediation, converting coercive observation into a dynamic of self-display and mutual watching.

While social movements like *#MeToo* and *Black Lives Matter* exemplify the democratic potential of the synopticon, they also reveal its constraints. The commodification of visibility and the manipulation of media narratives can reinforce elite control even within the ostensibly egalitarian space of social media (Andrejevic 2014). Moreover, the rise of surveillance capitalism (Zuboff 2019) means the platforms that enable the synopticon are exploiting the very participants they empower because they capture data about their behavior and interactions in ways that benefit corporate interests. The synopticon, therefore, remains a contested terrain, where the power of the many to watch the few is intertwined with the growing surveillance capacities of institutions and corporations. As such, the synopticon reflects

both the democratization of surveillance and the concentration of power in the hands of a few corporations and media conglomerates.

The synopticon also fosters an *illusion of accountability*, where the powerful appear to be held in check by the watchful eyes of the public. However, the deeper structural dynamics of power often remain unchallenged as the spectacle of surveillance frequently fails to disrupt entrenched social hierarchies (Bauman and Lyon 2013). While scandals may provoke public outrage, the public's capacity to substantially influence those in power is often limited because the public's gaze often takes the form of reciprocal 'social surveillance' (Marwick 2012) that fails to result in meaningful social or political change. Thus, while the synopticon holds significant potential for societal transformation, its impact is ultimately shaped by broader structural forces that determine how surveillance is mediated and who controls the narratives within these spaces. As Doyle (2011) argued, the synopticon contributes to social control not through coercion, but through distraction, seduction, and pacification. While the many are often fixated on entertainment and sensationalized news, they are less likely to become engaged in political activism or critical resistance (Bauman 2000).

Building on Mathiesen's synopticon, Serdar (2023) proposes the *omnipticon* as a further sublation that captures the shift to networked, lateral, and self-reflexive surveillance. The omnipticon describes a shift toward a networked system facilitated by digital technologies and social media, where everyone watches everyone. Unlike the panopticon——which enforces discipline through the fear of being watched——the omnipticon thrives on voluntary participation, blurring the lines between surveillance and self-display. In this "*I am seen, therefore I am*" era (Bauman 2010: 20), individuals engaging in what Andrejevic (2004b) calls 'lateral surveillance' willingly expose their private lives to others. Driven by the desire for visibility, social validation, and status, they contribute to a culture of transparency and digital exhibitionism. This transformation reinforces social control through implicit pressures rather than overt coercion, shaping a society where people perceive themselves as free while unknowingly or knowingly conforming to mass surveillance and commodified self-presentation (Bauman 2010).

4 Banopticon: the unwanted are excluded

Didier Bigo (2008) introduced the concept of the banopticon to describe a shift in surveillance from observation and discipline to risk management and exclusion. Emerging in the context of globalization, immigration, post-9/11 counterterrorism strategies, and border security regimes, the banopticon framework is concerned with how states and institutions use surveillance to pre-emptively categorize, restrict, exclude, or ban individuals identified as security threats (Bigo 2002; Huysmans 2006). The banopticon emphasizes the role of surveillance in managing borders, immigration policies, and the growing securitization of everyday life. In this framework, surveillance is not just about discipline (as in the panopticon) or distraction (as in the synopticon), it is about defining and controlling who is deemed worthy of inclusion in society—and who is not (Bauman 2004). Banoptic-like surveillance operates through tools, such as databases, biometric systems, and risk profiling, which target migrants, asylum seekers, refugees, and other 'unwelcome' individuals (Manley and Silk 2014). These systems often function in opaque ways, leaving perceived security threats vulnerable to decisions made outside normal juridical procedures, human rights conventions, and democratic norms (Macdonald and Hunter 2019).

Unlike the panopticon—where surveillance centers on normalization and inclusion—the banopticon focuses on exclusion as its primary method of control. Those deemed risky or dangerous are segregated, restricted, or blocked from certain societal privileges, such as migration, access to resources, or participation in public life (Macdonald and Hunter 2013). These exclusions can take the form of practices like the denial of visas, deportation, or placing individuals on no-fly lists (Nagra and Maurutto 2020). Often, these decisions are based on political and racial profiling, which can exacerbate inequality (Fassin 2013).

A key feature of the banopticon is pre-emption—the practice of anticipating, predicting, and preventing risks before they materialize (Bigo 2008). Surveillance technologies are not only used to monitor individuals but also to predict future actions, such as potential acts of terrorism or criminal behavior (Brayne and Christin 2021). This anticipatory approach relies on sophisticated data analysis and profiling methods, where decisions about people's movements, rights, or freedoms are made based on predicted behaviors rather than just actual events (Andrejevic 2017; Caldwell et al. 2020).

The banopticon is particularly evident in contemporary border control systems, which have become increasingly automated through technologies like biometric passports, visa application algorithms and facial recognition systems (Sanchez del Rio et al. 2016). These technologies create a digital divide by categorizing individuals as either approved or excluded based on predetermined criteria, often with limited recourse for appeal or transparency (Zuboff 2019). Denial of entry, deportation, and restrictions on movement are direct manifestations of this system, which seeks to prevent risks but may not sufficiently account for the rights, context or circumstances of those classified as 'data subjects' (Bigo et al. 2012).

The banopticon also plays a significant role in counterterrorism practices, where surveillance targets specific populations based on racial or religious profiles (Yazdiha 2023). This has sparked significant ethical debates, particularly regarding racial profiling and its disproportionate impact on marginalized communities (Sian 2017). For example, Muslims and individuals from certain countries are often disproportionately scrutinized in airport security systems (Sharma and Nijjar 2018), illustrating the intersection of surveillance, ethnicity, religion, and biopower. These racialized surveillance practices can contribute to systemic inequalities, further alienating already vulnerable populations (Alimahomed-Wilson 2019).

In Hegelian terms, the banopticon sublates the panopticon: it retains the logic of surveillance and behavioral control but transforms it by shifting the focus from internalized discipline to pre-emptive exclusion—elevating older methods into a more securitized and anticipatory regime of governance. While the panopticon focused on the internalization of norms through visibility, the banopticon preserves this monitoring impulse but transforms it into a predictive regime centered on profiling and exclusion.

More broadly, the securitization of everyday life—where security practices are applied to citizens in ways similar to the exclusion of outsiders—has become a widespread phenomenon (Bajc and de Lint 2011; Low 2017). Cities increasingly adopt 'smart' surveillance technologies that monitor not only physical borders but also social and cultural boundaries, marking the extension of the banopticon into urban spaces (Firmino and Duarte 2016). This growing trend of surveillance in the public sphere—often framed as necessary for safety and commerce (Lyon 2007)—can lead to the exclusion of those perceived as threats to societal norms (Wakefield 2005). This extension into urban life blurs the line between traditional state-led security and pervasive algorithmic surveillance, thereby foreshadowing the logics of the algopticon.

5 Super-panopticon: the networks watch the many

Mark Poster (1990) introduced the concept of the *super-panopticon* to extend Foucault's idea of the panopticon into the context of digital and information technologies. While Foucault's panopticon focuses on visibility and control of individuals within physical spaces, the super-panopticon operates through decentralized and distributed systems, such as databases and networks. Surveillance is embedded in everyday digital interactions, rather than being confined to specific institutions or physical spaces (Lyon 2007). Thus, the super-panopticon sublates the panopticon: it preserves the disciplinary logic of surveillance while transforming its operational form from architectural visibility to informational invisibility—thereby transforming surveillance into a dispersed, automated, and informational process.

The super-panopticon emphasizes collection, storage, and analysis of personal data. Control is exerted not through physical observation but through the categorization and manipulation of individuals via data profiles. Individuals in the super-panopticon are not simply disciplined into conformity, they are rather constructed as a 'data double' through the data collected about them (Haggerty and Ericson 2000). This data shapes how institutions and other entities perceive and interact with individuals (Lyon 2007). For example, Gandy (1993) showed in the 'panoptic sort' that consumer surveillance began using database marketing to produce discriminatory practices that targeted potentially valuable customers and dismissed those consumers determined to be of little value——those whom Zygmunt Bauman (2004) called 'flawed consumers.'

Unlike the panopticon, where visibility is the key mechanism of control, the super-panopticon functions more covertly. Poster (1990) argued individuals are increasingly constituted as data—as 'information subjects'—and monitored not by human eyes but by computational systems. As a result, individuals are often unaware of the extent or specifics of the data being collected, analyzed, and used to make decisions about them, shape their opportunities, or categorize them in ways that affect their social and economic lives. The rise of electronic communication technologies, such as networked computers, credit card systems, and digital media, facilitates the super-panopticon. These technologies integrate surveillance into everyday life, making it pervasive and embedded in routine activities. As Marx (1988) noted, networked technologies are less visible, often involuntary and transcend physical space and time through data storage, retrieval, combination, analysis, and communication.

In summary, the super-panopticon highlights an important shift from surveillance as a tool for disciplining (panopticon), distracting (synopticon), or excluding (banopticon), into a mechanism for managing individuals through their data, and manipulating behavior by shaping access, classification, and opportunity. This development has significant implications for privacy, data ownership, consent, autonomy, and accountability. Historically, the super-panopticon concept anticipated contemporary concerns about big data, predictive analytics, and algorithmic governance, where individuals are increasingly defined and controlled by their digital footprints (Lu 2022). The super-panopticon underscores how digital technologies transform power dynamics—not by observing physical behavior in physical spaces, but by monitoring and shaping individuals through the collection and use of their personal data. This informational turn lays the groundwork for the next evolutionary stage of surveillance—the algopticon—where algorithmic

processes not only monitor but also autonomously decide and intervene.

6 Algopticon: the algorithms watch everyone

The *algopticon* provides a new framework for understanding surveillance in the age of algorithmic and AI-driven governance. Coined by Rabih Jamil (2020) to describe Uber's use of AI tools, the concept captures how platforms like Uber deploy artificial intelligence to produce a decentralized system of continuous oversight, ranking, and discipline. Uber's algorithmic infrastructure predicts supply and demand at scale while monitoring driver behavior—what Jamil calls a form of 'digital incarceration.' This mirrors how Amazon's warehouse workers are subjected to handheld scanner surveillance (BBC News).

While the panopticon emphasizes visibility and uncertainty, the algopticon operates on principles of constant categorization and certainty. Unlike the synopticon's democratization of the gaze or the banopticon's focus on exclusion, the algopticon integrates these dynamics through algorithms that systematically track, classify, and act on data generated by individuals and systems. And while the super-panopticon centered on informational profiling through databases, the algopticon involves real-time feedback loops where behavioral data is not just stored but continuously acted upon. It is not merely the storage of data, but its predictive operationalization that defines the algopticon. The algopticon sublates these earlier surveillance paradigms: it preserves their foundational mechanisms of observation, normalization, and exclusion but transforms them into a new, automated form of algorithmic governance that is more pervasive and predictive. This *automated surveillance* (Andrejevic 2019) has given rise to post-disciplinary forms of surveillance, which do not depend upon the internalization of the monitoring gaze but rather coexist with traditional forms. Automated data collection enables predictive analytics, thereby replacing deterrence with pre-emptive intervention. In this sense, the algopticon sublates the panopticon's partial gaze—it preserves its disciplinary logic while transforming it through comprehensive, always-on sensing networks. Thus, the algopticon reflects a shift from human observation to computational processes, where algorithms continuously monitor, rank, predict, influence, and modify behaviors based on patterns in data (Zuboff 2019). For instance, by 2016, Facebook's FBLearner Flow machine learning algorithm was making "more than 6 million predictions per second" (Dunn 2016). The power of the algopticon lies not in the visibility of individuals, but in the visibility of their digital personas, which are increasingly commodified (Crawford 2023).

Unlike the human-centered gaze of the panopticon or synopticon, the algopticon relies on computers and algorithms to process information. This automation of surveillance is operating at a speed and scale that humans cannot match (Mayer-Schönberger and Cukier 2013). As algorithms work in real time, their ability to analyze and predict outcomes expands rapidly, offering unprecedented surveillance capabilities——and profit (Zuboff 2019).

A key feature of the algopticon is the *datafication of behavior*. In this system, human actions and interactions are converted into quantifiable data points (Mayer-Schönberger and Cukier 2013). Purchasing habits, social media use, biometric data, and even physical movements contribute to an individual's digital profile, facilitating predictive analytics (Chaudhary et al. 2021). These data points form the foundation of algoptic surveillance (Andrejevic 2019). As a result, researchers can access and analyze data without directly interacting with the individuals being studied. This scientific method creates a distal and abstract relationship between researchers and those *subjected to* research as algoptic research is conducted at a distance, far removed from the communities being studied (Crawford 2023).

The algopticon is fundamentally *predictive*. As exposure of Facebook's internal AI tools indicates (Biddle 2018), algorithms use past behaviors and patterns to forecast future actions, often aiming for pre-emptive control. For example, Egbert and Krasmann (2019) found predictive policing tools analyze data to identify crime hotspots or individuals likely to reoffend, creating systems of pre-emptive surveillance. But this predictive surveillance extends far beyond criminal justice into sectors, such as healthcare, finance, energy, retail, and marketing (Valli 2024).

In the algopticon, surveillance is often *invisible* or embedded in everyday systems. Social media, e-commerce platforms, and health-tracking devices often collect data without users fully realizing the extent of the monitoring (Andrejevic 2014). The normalization of surveillance, facilitated by pervasive technologies, leads to what Andrejevic (2004a, b) describes as the 'banality' of surveillance—where watching and being watched becomes routine, with individuals internalizing it as part of daily life (Lyon 2018).

While users are often aware they are being monitored through privacy policies or targeted advertisements, this awareness does not equate to transparency. Users know they are being watched but often do not understand how or by who their data are used, categorized, or acted upon (Pasquale 2015). For instance, a Pew Research Center report (Auxier et al. 2019) found many Americans believe their activities are tracked by companies and governments, yet they feel largely powerless to control how their data are collected or used, and they often don't fully comprehend the specifics of data use or the entities involved. This lack of transparency is a central feature of algoptic

surveillance, where algorithms——according to Pasquale (2015)——often function as 'black boxes' with limited accountability or oversight.

The algopticon also perpetuates systemic inequalities through biased algorithms (Kordzadeh and Ghasemaghaei 2021). For instance, hiring algorithms may replicate gender or racial biases (Andrews and Bucher 2022), and predictive tools may disproportionately target marginalized communities (Eubanks 2018; Noble 2018). Since these biases are embedded within the algorithmic decision-making processes, they amplify existing social inequalities (O'Neil 2016).

All in all, the algopticon provides a critical lens with which to understand how digital surveillance has become ingrained in everyday life through decentralized and automated systems. Social media platforms like Facebook, Instagram, and X (formerly Twitter) epitomize the algopticon. As research shows (Angwin et al. 2016a, b; Couldry and Mejias 2019), these platforms track users' interactions, preferences, and networks to create detailed profiles that can deliver hyper-targeted advertisements. Data-driven advertising influences consumer behavior, including political messaging (Hinds et al. 2020). For example, Facebook's algorithm was shown to influence users' moods through subtle manipulations (Tufekci 2015), particularly targeting emotional vulnerabilities, especially among teenagers (Levin 2017). These platforms transform personal communication into a site of algoptic surveillance, where users unknowingly or knowingly participate in the extraction and commodification of their own data (Zuboff 2019).

Retail platforms and loyalty programs also demonstrate the algopticon's focus on *behavioral modification through digital categorization*. Consumer behaviors are tracked via purchasing patterns, online activity, and membership histories, which shape personalized recommendations and marketing strategies (Verhoef et al. 2010). Platforms like Amazon, Netflix, and YouTube use data to predict user preferences, turning consumption into a site of algoptic surveillance (Helles and Flyverbom 2019).

Similarly, digital health initiatives, including wearable devices and electronic health records, reflect the algopticon's principle of embedding surveillance into daily life (Gidaris 2019). By collecting biometric data and monitoring health metrics, these systems transform individuals into a 'virtual self' or 'software self' (Lyon 2007). These devices track health metrics, which can then be shared with insurers or healthcare providers to influence treatment plans and premiums (Ajana 2017). COVID-19 tracking apps and vaccination passports exemplify how data-driven systems categorize individuals based on health status, affecting their movement and societal participation (Stacy and Rodriguez 2023). While these technologies hold potential for improving healthcare, they also pose risks to privacy, autonomy, and exploitation (Crawford et al. 2015).

More broadly, 'smart cities' rely on interconnected digital infrastructures to manage urban life in real-time, employing surveillance systems like CCTV, traffic monitoring, and public Wi-Fi (Kourtit et al. 2017). Sherman (2023) terms this urban AI-based system the *polyopticon*, which consists of a distributed network of synthetic intelligences gathering vast amounts of data to enhance urban efficiency. However, the urban-focused algoptic gaze raises concerns about privacy and civil liberties, as these systems often collect data with little transparency or consent (Kitchin 2016). As Lu (2022: 2146) argues, "the right to data privacy cannot be assured if individuals cannot understand how AI systems access, assess, and intrude upon them."

Moreover, law enforcement increasingly relies on data-driven technologies to predict criminal behavior, reflecting the algopticon's focus on *datafication for pre-emptive surveillance*. Predictive policing software aggregates crime data to predict future incidents so that limited police resources can be directed toward high-risk areas (Pearson et al. 2024). Similarly, risk prediction tools influence bail and sentencing decisions (Barnes and Hyatt 2012), and are used to predict which individuals are most likely to be involved in gun violence (Brayne 2017). However, these applications raise concerns about reinforcing biases in the data and producing false positives, thereby further entrenching systemic inequalities (Lum and Isaac 2016)—as shown by an investigation into racial bias in predictive policing (Angwin et al. 2016a, b).

In educational and professional contexts, surveillance technologies are used to track performance, attendance, and behavior, impacting both students (Kumar et al. 2019) and teachers (Heemsbergen et al. 2024). Educational algorithms assess students' academic progress, often directing them toward targeted interventions. These technologies further entrench algorithmic decision-making within sectors traditionally governed by human discretion, thereby creating opportunities for algorithmic overreach and the depersonalization of education (Binns 2022). Likewise, workplace surveillance increasingly relies on AI-driven tools, including computer monitoring, email tracking, biometric recognition, GPS tracking, and predictive analytics (Ball 2021). While companies justify these practices for security, compliance, and productivity, they raise ethical concerns about privacy, autonomy, and employee well-being (Glavin et al. 2024). These technologies illustrate how the algoptic gaze extends surveillance into traditionally personal and professional domains to reshape norms and boundaries around education and employment.

As highlighted, the algopticon raises pressing ethical concerns. The relentless and constant collection of data infringes on individual privacy, often without informed consent. For

example, many digital services require users to agree to lengthy, complex terms of service, which makes it difficult to provide genuinely informed consent and to understand the full extent of the surveillance done in-and-with one's name. Moreover, individuals often have no meaningful choice but to accept data collection to use essential services (Schneier 2015). This means the commodification of personal data challenges traditional notions of privacy, autonomy and consent (Zuboff 2019). As Couldry and Mejias (2019) argued, the datafication of personal information transforms privacy from a *right* into *raw material* for profit (i.e., a commodity), often bypassing genuine user consent.

In regard to algorithmic accountability, decisions made by algorithms are often opaque, with limited recourse for those negatively impacted (Tufekci 2015). Since decision-making processes are often hidden from the public, regulators and even those directly affected, it is difficult to challenge biased or unfair decisions (Pasquale 2015). This lack of transparency in algorithmic decision-making undermines trust in institutions and automated systems (O'Neil 2016).

Finally, access to and control over data is concentrated in the hands of a few corporations and states, creating power imbalances (Schneier 2015). These imbalances can exacerbate existing inequalities, as marginalized groups may be disproportionately surveilled or excluded from opportunities based on algorithmic decisions (Eubanks 2018).

Thus, the algopticon is a powerful framework for understanding how algorithmic technologies shape modern surveillance. By integrating automated monitoring, predictive analytics, and datafication, the algopticon moves beyond the traditional forms of surveillance to create hyper-efficient and pre-emptively reactive systems of governance. This historical development reflects Hegel's sublation process, whereby earlier forms of surveillance are not entirely discarded. Instead, they are preserved and transformed within the algopticon. The panopticon's disciplinary gaze, the synopticon's mass mutual observation, and the banopticon's exclusionary logic are all sublated into a more personalized, predictive, opaque, and automated form of social control.

7 Surveillance in transformation: sublating the opticons

The algopticon introduces a paradigm shift in surveillance by both diverging from and building upon the prior key '-opticon' concepts of panopticon, synopticon, banopticon and super-panopticon. This historical shift can be framed through the Hegelian concept of sublation: the algopticon does not merely replace these earlier models but simultaneously negates, preserves, and transforms them into a higher-order system. This section examines similarities and differences among these frameworks, focusing on their mechanisms of surveillance, power dynamics, and societal implications.

7.1 From panopticon to algopticon

The panopticon relies on centralized, visible surveillance to create a state of internalized discipline. By contrast, the algopticon decentralizes surveillance, embedding it within algorithmic systems that operate invisibly in the background. The algopticon sublates the panopticon: it preserves the goal of behavioral control but transforms the mechanism from human gaze to automated inference. The panopticon's power lies in the prisoner's awareness of the guard's potential gaze, which cultivates uncertainty. The algopticon, however, operates largely unseen, with its surveillance embedded in algorithmic processes that pervade everyday life. However, the algopticon does not eliminate uncertainty entirely—it replaces the subject's uncertainty (about being watched) with a new uncertainty about *how* they're being profiled and acted upon. This invisibility is fundamental to the control exerted by algorithmic surveillance. Whereas the panopticon depends on human observation, the algopticon automates surveillance, processing vast amounts of data at scale (Crawford and Paglen 2019). Unlike the panopticon, where human observers maintain authority, the algopticon delegates surveillance tasks to algorithms, thereby reducing direct human oversight.

Both systems aim to influence and modify behavior. In the panopticon, the threat of observation ensures compliance. The algopticon, by contrast, exerts control through data categorization and predictive analytics, shaping behavior by pre-emptively acting on perceived risks or preferences (Brayne and Christin 2021). Algorithms predict and direct individual actions before they occur, leveraging big data to construct behavioral profiles (Andrejevic 2019). While the panopticon raises concerns about autonomy and dignity, the algopticon introduces additional ethical challenges, including algorithmic bias and discrimination, lack of accountability and transparency, and the commodification of personal data (Saheb 2023). The opacity of algorithmic processes prevents individuals from fully understanding or contesting decisions made about them (Eubanks 2018; Noble 2018).

7.2 From synopticon to algopticon

The synopticon describes a society where the many watch the few, particularly through mass media and celebrity culture. While the algopticon incorporates elements of distributed observation, it sublates the synopticon by preserving its decentralized logic but repurposing it through automation and machine vision. The synopticon's focus is on collective observation of the few by the many, whereas the algopticon involves many watching everyone as algorithms

continuously analyze data from vast populations (Andrejevic 2014). Additionally, the synopticon relies on human attention and media technologies, whereas the algopticon operates through advanced computational systems (Tufekci 2015). Unlike traditional media-based observation, the algopticon automates surveillance and analysis, using algorithms to continuously monitor and categorize vast amounts of data (O'Neil 2016; Zuboff 2019).

Regarding human agency, individuals in the synopticon participate as watchers or watched, creating a dynamic interplay (Marwick 2012). The algopticon, by contrast, reduces individual agency by making decisions based on data patterns, often without the individual's awareness or consent (Couldry and Mejias 2019). Unlike the participatory nature of the synopticon, where power is dispersed across society (Peacock et al. 2023), the algopticon's automated processes diminish personal involvement, consolidating power in the hands of those who control the algorithms (Srivastava 2023).

7.3 From banopticon to algopticon

The banopticon focuses on systematic exclusion, using surveillance to determine who is included or excluded from spaces, rights, or services. The algopticon sublates this logic of exclusion: it retains the exclusionary function but embeds it into ubiquitous, automated classification systems. While the banopticon explicitly identifies and excludes individuals deemed as threats, often in migration or security contexts, the algopticon achieves exclusion subtly, using algorithms to classify individuals into risk categories or deny access to opportunities based on data profiles (Eubanks 2018; O'Neil 2016). This covert form of exclusion extends beyond physical borders to digital and social spaces, where algorithms can restrict access to loans, jobs, or social platforms without clear justification (Garcia et al. 2024).

Whereas the banopticon operates in targeted contexts—such as border control or counterterrorism—the algopticon is far broader, encompassing all aspects of life as it continuously collects and analyzes data to predict and influence personal and public behavior (Zuboff 2019). The banopticon's decisions may be overt, such as the denial of entry or asylum, whereas in the algopticon, exclusion often occurs covertly, such as algorithms rejecting a job application or denying credit based on opaque criteria (Eubanks 2018; O'Neil 2016).

7.4 From super-panopticon to algopticon

The super-panopticon and the algopticon both theorize the evolution of surveillance in the information age, yet they differ in their emphasis on algorithms, predictive processes, and ethical challenges. Both frameworks move beyond the architectural visibility of the panopticon by shifting toward decentralized, data-driven surveillance. The algopticon sublates the super-panopticon: it builds upon its foundational logic but transforms it into a more dynamic, automated, and anticipatory regime. In the super-panopticon, databases and networks operate as invisible yet omnipresent mechanisms of control, embedding surveillance into mundane systems like credit scoring and communication networks (Simon 2005). Similarly, the algopticon relies on algorithmic processes diffused across platforms, making surveillance less visible yet more intrusive. The opacity of surveillance in both frameworks means individuals rarely comprehend how their data are collected, analyzed, or used to shape their lives (Lu 2022; Noble 2018).

Both rely on data-driven control, where power emerges from collection, categorization, and analysis of personal information (Andrejevic 2019). The super-panopticon constructs individuals as 'data subjects,' shaping their identities based on stored information. The algopticon extends this process by actively using algorithmic predictions to reshape subjectivities, influencing behaviors based on anticipated futures rather than just past actions (Brayne and Christin 2021).

Despite these similarities, the algopticon introduces unique features. Whereas the super-panopticon centers on retrospective categorization—analyzing stored data to enforce discipline—the algopticon prioritizes predictive surveillance (Zuboff 2019). Algorithms anticipate and preempt future actions, shifting control from interpreting past behaviors to influencing future possibilities through the very subtle modification of behavior (ibid). This predictive capacity alters power and agency dynamics (Saheb 2023). Additionally, the super-panopticon relies on human actors to interpret and act on data, while the algopticon automates decision-making, often with minimal human oversight (Crawford and Paglen 2019). This shift raises pressing concerns about accountability, bias, and transparency that are less pronounced in the super-panopticon (Couldry and Mejias 2019; Srivastava 2023).

The scale and the pervasiveness of the algopticon exceed those of the super-panopticon. While the latter operates through identifiable technologies like credit systems, the algopticon integrates into nearly every facet of life, from personalized advertising to predictive policing and smart cities (O'Neil 2016). Its operations are frequently opaque, amplifying ethical concerns about autonomy and discrimination beyond the privacy-focused issues associated with the super-panopticon (Garcia et al. 2024).

The algopticon therefore represents a new stage in surveillance theory, best understood not as a rupture but as a sublation of prior surveillance architectures. The super-panopticon laid the groundwork for understanding digital surveillance, focusing on data collection within electronic communication systems. The algopticon extends these ideas

by incorporating algorithmic automation, predictive analytics, and the restructuring of social control. While the super-panopticon captured the early stages of information-driven surveillance, the algopticon represents a more technically advanced evolution by highlighting how algorithms and artificial intelligence now shape behavior, decision-making, and power structures in a data-saturated world.

8 Conclusion

Surveillance has always reflected the power dynamics and technologies of its era. From visibility and discipline (panopticon), to mass mutual observation (synopticon), exclusionary risk sorting (banopticon), and database-driven normalization (super-panopticon), surveillance has historically mirrored its technological and political contexts. The algopticon builds upon these foundations while introducing a new paradigm. Like the super-panopticon, it decentralizes observation, embedding surveillance into everyday systems. However, the algopticon extends beyond data storage and categorization to prediction and pre-emption, replacing deterrence with proactive control. Unlike the panopticon's reliance on visibility, the algopticon operates largely invisibly yet pervasively. In contrast to the synopticon's human gaze, the algopticon automates observation, thereby freeing it from the limitations of human attention. And while it shares the exclusionary mechanisms of the banopticon, the algopticon expands exclusion to all aspects of life, from economic opportunities to digital participation. What distinguishes the algopticon is its scale, automation, and speed—processing vast data flows in real time to continuously shape behavior before it happens.

A defining feature of the algopticon is its predictive nature, enabled by vast computational power and the commodification of personal data. This shift from uncertainty to algorithmic certainty raises critical ethical concerns, including bias, opacity, transparency, accountability, inequality, and the erosion of privacy and autonomy. The algopticon envisions a society where control is systematic, pervasive, and predictive, shaping not just present actions but also modifying future possibilities and outcomes. While algorithmic predictions promise precision and efficiency, they often obscure how certainty is manufactured—reinforcing rather than correcting the biases and inequalities of existing data.

Hegel's concept of sublation helps us to better grasp the algopticon's significance. The algopticon sublates panopticon, synopticon, banopticon, and super-panopticon. It does not discard their logics but transforms them—preserving disciplinary aims while embedding them in automated, predictive infrastructures. This dialectical movement justifies the algopticon as a distinct analytical category. It marks a qualitative shift in the architecture of observation and control.

As surveillance technologies continue to evolve, the algopticon challenges traditional notions of power and control, highlighting the need for urgent attention from scholars, policymakers, and civil society. Addressing the profound implications of data-driven and algorithmic surveillance requires robust frameworks that promote transparency, accountability, and ethical data use to prevent technological advances from entrenching inequality or diminishing personal freedoms. This demands not only critical theory but also regulatory innovations, such as algorithmic impact assessments, data transparency protocols, stronger data privacy protections, and digital rights charters.

The algopticon is obviously not the endpoint of surveillance evolution, but rather the latest chapter in an ongoing dialectical narrative. Future socio-technical developments will further transform how individuals are watched, categorized, and controlled, underscoring the need for vigilance and proactive engagement in shaping surveillance systems. As surveillance extends beyond the physical to the digital, political, psychological and emotional realms, addressing disparities in power and access to information is imperative. If left unchecked, the algopticon risks naturalizing opaque, automated forms of domination. To resist this, we must not only analyze surveillance, but actively shape its future through democratic, ethical, and transparent interventions (Zuboff 2019).

Author contributions The primary author wrote the entire manuscript.

Data availability No datasets were generated or analyzed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

Ajana B (2017) Digital health and the biopolitics of the quantified self. Digit Health 3:1–9. https://doi.org/10.1177/2055207616689509

Alimahomed-Wilson S (2019) When the FBI knocks: racialized state surveillance of Muslims. Crit Sociol 45(6):871–887

Andrejevic M (2004a) Reality TV: the work of being watched. Rowan & Littlefield Publishers, Lanham

Andrejevic M (2004b) The work of watching one another: lateral surveillance, risk, and governance. Surveill Soc 2(4):479–497

Andrejevic M (2014) Surveillance in the big data era. In: Pimple K (ed) Emerging pervasive information and communication technologies (PICT). Law, governance and technology series, vol 11. Springer, Dordrecht

Andrejevic M (2017) To Pre-empt a thief. Int J Commun 11:879–896

Andrejevic M (2019) Automating surveillance. Surveill Soc 17(1/2):7–13

Andrews L, Bucher H (2022) Automating discrimination: AI hiring practices and gender inequality. Cardozo Law Rev 44(1):145–201
Angwin J, Larson J, Mattu S, Kirchner L (2016a) Machine bias: there's software used across the country to predict future criminals and it's biased against Blacks. ProPublica
Angwin J, Mattu S, Parris T (2016) Facebook doesn't tell users everything it really knows about them. ProPublica
Auxier B, Rainie L, Anderson M, Perrin A, Kumar M, Turner E (2019) Americans and privacy: concerned, confused and feeling lack of control over their personal information. Pew Research Center: Internet, Science & Tech. United States of America
Bajc V, de Lint W (2011) Security and everyday life. Routledge, New York
Ball K (2021) Electronic Monitoring and Surveillance in the Workplace. Literature Review and Policy Recommendations. JRC125716, Luxembourg: Publications Office of the European Union
Barnes GC, Hyatt JM (2012) Classifying Adult Probationers by Forecasting Future Offending. Final Technical Report. Prepared for the U.S. Department of Justice
Bauman Z (2000) Liquid modernity. Polity Press, Cambridge
Bauman Z (2004) Wasted lives: modernity and its outcasts. Polity Press, Cambridge
Bauman Z (2010) 44 Letters from a liquid modern world. Polity Press, Cambridge
Bauman Z, Lyon D (2013) Liquid surveillance: a conversation. Polity Press, Cambridge
Bentham J (1791) Panopticon, or the inspection house. T. Payne, London
Biddle S (2018) Facebook uses artificial intelligence to predict your future actions for advertisers, says confidential document. The Intercept April 13
Bigo D (2002) Security and immigration: toward a critique of the governmentality of unease. Alternatives 27(1):63–92
Bigo D (2008) Globalised (in)security: the field and the ban-opticon. In: Bigo D, Tsoukala A (eds) Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11. Routledge, Abingdon, Oxon, pp 10–49
Bigo D, Carrera S, Hayes B, Hernanz N, Jeandesboz J (2012) Evaluating Current and Forthcoming Proposals on JHA Databases and a Smart Borders System at EU External Borders. European Parliament PE 462, Brussels
Binns R (2022) Human Judgment in algorithmic loops: Individual justice and automated decision-making. Regulat Governance 16(1):197–211
Brayne S (2017) Big data surveillance: the case of policing. Am Sociol Rev 82(5):977–1008
Brayne S, Christin A (2021) Technologies of crime prediction: the reception of algorithms in policing and criminal courts. Soc Probl 68(3):608–624
Caldwell M, Andrews JTA, Tanay T, Griffin LD (2020) AI-enabled future crime. Crime Sci 9:14
Caluya G (2010) The post-panoptic society? Reassessing Foucault in surveillance studies. Social Identities 16(5):621–633
Chaudhary K, Alam M, Al-Rakhami MS, Gumaei A (2021) Machine learning-based mathematical modelling for prediction of social media consumer behavior using big data analytics. J Big Data 8:73
Couldry N, Mejias UA (2019) The Costs of Connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press, Stanford
Crawford K (2023) Data: from the Atlas of AI. Missing links in AI governance. UNESCO, Paris, pp 111–132
Crawford K, Paglen T (2019) Excavating AI: the politics of images in machine learning training sets. AI & Soc 36:1105–1116
Crawford K, Lingel J, Karppi T (2015) Our metrics, ourselves: a hundred years of self-tracking from the weight scale to the wrist wearable device. Eur J Cult Stud 18(4–5):479–496
Deleuze G (1992) Postscript on the societies of control, vol 59. MIT Press, Cambridge, pp 3–7
Doyle A (2011) Revisiting the synopticon: reconsidering Mathiesen's 'The Viewer Society' in the age of Web 2.0. Theor Criminol 15(3):283–299
Dunn J (2016) Introducing FBLearner Flow: Facebook's AI backbone. Engineering at Meta
Egbert S, Krasmann S (2019) Predictive policing: not yet, but soon preemptive? Polic Soc 30(8):905–919
Ellis JR (2021) Policing legitimacy: Social media, scandal and sexual citizenship. Springer, Cham
Eubanks V (2018) Automating inequality: how high-tech tools profile, police, and punish the poor. Martin's Press, St
Fassin D (2013) Enforcing order: an ethnography of urban policing. Polity Press, Cambridge
Firmino R, Duarte F (2016) Private video monitoring of public spaces: the construction of new invisible territories. Urban Studies 53(4):741–754
Foucault M (1977) Discipline and punish: the birth of the prison. Pantheon Books, New York
Gandy OH Jr (1993) The panoptic sort: a political economy of personal information. Oxford University Press, Oxford
Garcia ACB, Garcia MGP, Rigobon R (2024) Algorithmic discrimination in the credit domain: what do we know about it? AI & Soc 39(4):2059–2098
Gidaris C (2019) Surveillance capitalism, datafication, and unwaged labour: the rise of wearable fitness devices and interactive life insurance. Surveill Soc 17(1/2):132–138
Glavin P, Bierman A, Schieman S (2024) Private eyes, they see your every move: workplace surveillance and worker well-being. Social Currents 11(4):327–345
Haggerty KD (2006) Tear down the walls: on demolishing the panopticon. In: Lyon D (ed) Theorizing surveillance: the panopticon and beyond. Willan, Cullompton, UK, pp 37–59
Haggerty KD, Ericson RV (2000) The surveillant assemblage. In: Surveillance C, Control S (eds) Clive Norris and Dean Wilson. Routledge, London, pp 61–78
Heemsbergen L, Krebs S, Gorur R, Maddox A (2024) Algorithmic performance management in higher education: viva! 365 ways of surveillance. Surveill Soc 22(2):73–87
Hegel GWF (1969) Hegel's science of logic (Trans. A.V. Miller). Humanities Press, Atlantic Highlands, NJ
Hegel GWF (1977) Phenomenology of Spirit (Trans. A. V. Miller). Oxford University Press, Oxford (Original work published 1807)
Helles R, Flyverbom M (2019) Meshes of surveillance, prediction, and infrastructure: on the cultural and commercial consequences of digital platforms. Surveill Soc 17(1/2):34–39
Hinds J, Williams EJ, Joinson AN (2020) "It wouldn't happen to me": privacy concerns and perspectives following the Cambridge Analytica scandal. Int J Hum Comput Stud 143:102498
Huysmans J (2006) The politics of insecurity: fear. Migration and Asylum in the EU, Routledge, Milton Park
Jamil R (2020) Uber and the making of an algopticon - insights from the daily life of Montreal drivers. Cap Class 44(2):241–260
Kitchin R (2016) The ethics of smart cities and urban science. Phil Trans R Soc A 374:20160115
Kordzadeh N, Ghasemaghaei M (2021) Algorithmic bias: review, synthesis, and future research directions. Eur J Inf Syst 31(3):388–409
Koskela H (2003) 'Cam era' – the contemporary urban panopticon. Surveill Soc 1(3):292–313

Kourtit K, Nijkamp P, Steenbruggen J (2017) The significance of digital data systems for smart city policy. Socioecon Plann Sci 58:13–21
Kumar PC, Vitak J, Chetty M, Clegg TL (2019) The platformization of the classroom: teachers as surveillant consumers. Surveill Soc 17(1/2):145–152
Levin S (2017) Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless.' The Guardian 1
Low S (2017) Security at home: how private securitization practices increase state and capitalist control. Anthropological Theory 17(3):365–381
Lu S (2022) Data privacy, human rights, and algorithmic opacity. Calif Law Rev 110:2087–2147
Lum C, Isaac W (2016) To predict and serve? Significance 13(5):14–19
Lyon D (2001) Surveillance society: monitoring everyday life. Open University Press, Buckingham and Philadelphia
Lyon D (ed) (2003) Surveillance as social sorting: privacy, risk and digital discrimination. Routledge, London and New York
Lyon D (2006) The search for surveillance theories. In: Lyon D (ed) Theorizing surveillance: the panopticon and beyond. Routledge, London and New York, pp 3–20
Lyon D (2007) Surveillance studies: an overview. Polity Press, Cambridge
Lyon D (2018) The culture of surveillance: watching as a way of life. Polity Press, Cambridge
Macdonald M, Hunter D (2013) The discourse of Olympic security: London 2012. Discourse Soc 24(1):66–88
MacDonald MN, Hunter D (2019) The discourse of security: language, illiberalism and governmentality. Palgrave Macmillan, Cham
Manley A, Silk M (2014) Liquid London: sporting spectacle, britishness & ban-optic surveillance. Surveill Soc 11(4):360–376
Manning N, Penfold-Mounce R, Loader B, Vromen A, Xenos M (2017) Politicians, celebrities and social media: a case of informalisation? J Youth Stud 20(2):127–144
Manokha I (2018) Surveillance, panopticism, and self-discipline in the digital age. Surveill Soc 16(2):219–237
Manokha I (2020) The implications of digital employee monitoring and people analytics for power relations in the workplace. Surveill Soc 18(4):540–554
Marwick AE (2012) The public domain: surveillance in everyday life. Surveill Soc 9(4):378–393
Marwick AE, Boyd D (2011) To see and be seen: celebrity practice on twitter. Convergence 17(2):139–158
Marx GT (1988) Undercover: police Surveillance in America. University of California Press, Berkeley
Marx GT (2015) Surveillance studies. Int Encycl Soc Behav Sci 23(2):733–741
Marx GT (2016) Windows into the soul: Surveillance and society in an age of high technology. University of Chicago Press, Chicago
Mathiesen T (1997) The viewer society: Michel Foucault's 'panopticon' revisited. In: Surveillance C, Control S (eds) Clive Norris and Dean Wilson. Routledge, London, pp 41–60
Mayer-Schönberger V, Cukier K (2013) Big data: a revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt, New York
Mundt M, Ross K, Burnett C (2018) Scaling social movements through social media: the case of black lives matter. Social Med Society. https://doi.org/10.1177/2056305118807911
Nagra B, Maurutto P (2020) No-fly lists, national security and race: the experiences of Canadian Muslims. Br J Criminol 60(3):600–619
Newell BC (2023) Surveillance as information practice. J Am Soc Inf Sci 74(4):444–460
BBC News. Amazon: the truth behind the click. www.bbc.co.uk/programmes/n3csvf5g
Noble SU (2018) Algorithms of oppression: how search engines reinforce racism. New York University Press, New York
O'Neil C (2016) Weapons of math destruction: how big data increases inequality and threatens democracy. Crown Publishing Group, New York
Pangrazio L, Selwyn N, Cumbo B (2023) Tracking technology: exploring student experiences of school datafication. Camb J Educ 53(6):847–862
Pasquale F (2015) The black box society: the secret algorithms that control money and information. Harvard University Press, Cambridge
Peacock V, Bruun MK, Dungey CE, Shapiro M (2023) Surveillance. In: Nieber H (ed) The open encyclopedia of anthropology. University of Oxford, Oxford
Pearson E, Bjerg Jensen R, Adey P (2024) Pred-Pol-Pov: Visibility, data flows, and the predictive policing of poverty. Surveill Soc 22(2):120–137
Poster M (1990) The mode of information: postculturalism and social context. University of Chicago Press, Chicago
Rost K, Stahel L, Frey BS (2016) Digital social norm enforcement: online firestorms in social media. PLoS ONE 11(6):e0155923
Rubinstein IS, Nojeim GT, Lee RD (2014) Systematic government access to personal data: a comparative analysis. Int Data Privacy Law 4(2):96–119
Saheb T (2023) Ethically contentious aspects of artificial intelligence surveillance: a social science perspective. AI and Ethics 3:369–379
Sanchez del Rio J, Moctezuma D, Conde C, Martin de Diego I, Cabello E (2016) Automated border control e-gates and facial recognition systems. Comput Secur 62:49–72
Schneier B (2015) Data and goliath: the hidden battles to collect your data and control your world. W. W. Norton & Company, New York
Serdar M (2023) Transformation of the surveillance society from panopticon to omnipticon: the case of black mirror's episode 'nosedive.' OPUS J Soc Res 20(53):396–409
Shang S, Wu Y, Li E (2017) Field effects of social media platforms on information-sharing continuance: do reach and richness matter? Inf Manag 54(2):241–255
Sharma S, Nijjar J (2018) The racialized surveillant assemblage: Islam and the fear of terrorism. Pop Commun 16(1):72–85
Sherman S (2023) The Polyopticon: a diagram for urban artificial intelligences. AI & Soc 38:1209–1222
Sian K (2017) Countering racism in counter-terrorism and surveillance discourse. Palgrave Commun 3(4):1–3
Simon B (2005) The return of panopticism: supervision, subjection and the new surveillance. Surveill Soc 3(1):1–20
Srivastava S (2023) Algorithmic governance and the international politics of big tech. Perspect Polit 21(3):989–1000
Stacy J, Rodriguez MC (2023) A reconfigured panopticon: COVID-19, virtual schooling, and regulation of our homes. Teach Coll Rec 125(10):31–55
Tufekci Z (2015) Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technol Law J 13:203–218
Valli LN (2024) A succinct synopsis of predictive analysis applications in the contemporary period. Int J Multidiscipl Sci Arts 3(4):25–36
Verhoef PC, Venkatesan R, McAlister L, Malthouse EC, Krafft M, Ganesan S (2010) CRM in data-rich multichannel retailing environments: a review and future research directions. J Interact Mark 24(2):121–137
Wakefield A (2005) The public surveillance functions of private security. Surveill Soc 2(4):529–545
Weinreich SJ (2021) Panopticon Inc: Jeremy Bentham, contract management, and (neo)liberal penality. Punishment Soc 23(4):497–514

Yazdiha H (2023) The relational dynamics of racialised policing: community policing for counterterrorism, suspect communities, and Muslim Americans' provisional belonging. J Ethn Migr Stud 49(11):2676–2697

Zuboff S (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs, New York