Revista Lusófona de Estudos Culturais / Lusophone Journal of Cultural Studies, Vol. 12, No. 1, 2025, e025002
https://doi.org/10.21814/rlec.6294

Among the (Many) Meanings of Big Data: History, Surveillance, Control, and Criminalisation

Laura Neiva
Centro de Estudos de Comunicação e Sociedade, Instituto de Ciências Sociais, Universidade do Minho, Braga, Portugal/Centro de Estudos Jurídicos, Económicos e Ambientais, Universidade Lusíada Norte, Porto, Portugal

Abstract

This article critically analyses surveillance in the era of big data, exploring the multiple meanings attributed to it over time and tracing its historical evolution. Drawing on surveillance studies, it examines how surveillance practices have been shaped by socio-technical and security dynamics — ranging from early efforts focused on population management and policing to the consolidation of algorithmic infrastructures grounded in mass datafication. Rather than representing a definitive rupture, big data is shown to reconfigure and expand historical mechanisms of control, fostering a convergence between mass and targeted surveillance. The analysis demonstrates how monitoring technologies are embedded in techno-optimistic narratives that legitimise their proliferation while simultaneously reinforcing the collectivisation of suspicion and reorienting criminal investigation towards predictive and statistical models. Through a brief examination of the Portuguese context, the article discusses how the adoption of such technologies reflects a political aspiration for security modernisation, framed by discourses that portray technology as an inevitable response to crime. It concludes that algorithmic surveillance not only restructures policing and criminal justice but also raises profound ethical and political concerns. The increasing opacity of automated decision-making and its naturalisation within security discourse underscores the need for critical scrutiny to ensure that technological efficiency does not become an unquestioned principle of governance — at the expense of fundamental rights and the reproduction of structural inequalities.

Keywords

surveillance, big data, police, security, history

Entre os (Muitos) Sentidos de *Big Data*: A História, a Vigilância, o Controlo e a Criminalização

Resumo

Este artigo analisa criticamente a vigilância na era de *big data*, explorando os múltiplos sentidos que lhe são atribuídos ao longo do tempo e traçando um mapeamento histórico da sua evolução. Sustentado nos estudos da vigilância, examina como estas práticas foram moldadas por dinâmicas sociotécnicas e securitárias, desde os seus primórdios associados à gestão populacional e ao policiamento, até à consolidação de infraestruturas algorítmicas baseadas na datificação massiva. Ao longo desta trajetória, argumenta-se que, longe de representar uma rutura absoluta, *big data* reconfigura e amplia mecanismos históricos de controlo, promovendo a fusão entre vigilância em massa e vigilância direcionada.

A análise desenvolvida evidencia como as tecnologias de monitorização se inscrevem em narrativas tecno-otimistas que legitimam a sua expansão, enquanto reforçam a coletivização da suspeição e deslocam a lógica da investigação criminal para um modelo preditivo e estatístico. Através do estudo sumário do caso português, discute-se como a adoção de tecnologias reflete uma vontade política de modernização securitária, enquadrada por discursos que apresentam a tecnologia como solução incontornável para a criminalidade. Conclui-se que a vigilância algorítmica não só reestrutura o policiamento e a justiça criminal, mas também levanta desafios éticos e políticos significativos. A crescente opacidade dos processos de decisão automatizados e a sua naturalização no discurso securitário impõem a necessidade de um escrutínio crítico, de modo a evitar que a eficiência tecnológica se torne um princípio incontestado de governação, comprometendo direitos fundamentais e reproduzindo desigualdades estruturais.

Palavras-chave
vigilância, *big data*, polícia, segurança, história

1. Introduction

Big data — understood as a set of tools developed to process and analyse large volumes of heterogeneous data, identifying correlations and patterns — has been widely promoted as an effective solution for decision-making across various domains of social life. In the realm of public security and criminal investigation, these technologies are frequently legitimised through techno-optimistic narratives that emphasise their potential to enhance police efficiency and risk management. However, a historical perspective on surveillance reveals that the expansion of these infrastructures does not signify a rupture with the past. Rather, it reflects the adaptation and amplification of pre-existing security practices, which continue to reinforce the logic of control and processes of differential criminalisation.

This paper sets out to map the history of surveillance and its associated technologies, analysing how their development has both shaped and been shaped by social, political, and economic contexts. Drawing on the concept of "surveillance capitalism" (Lyon, 2019), it argues that the increasing centrality of algorithmic surveillance reflects enduring power dynamics. This evolution fosters a convergence of mass and targeted surveillance, intensifies the collectivisation of suspicion, and redefines the contours of public safety.

To this end, it draws on the work of sociologist David Lyon (2014a), a leading figure in surveillance studies, to explore how the multiple meanings of surveillance have been reconfigured over time. As Lyon (2014a) notes, "today's technologies grow out of yesterday's" and, therefore, "a sense of history is badly needed to grasp the context of the contemporary" (p. 33). Through this perspective, this paper seeks to deepen the understanding of the emergence of big data by analysing its role in contemporary surveillance and its broader social implications — particularly in relation to the shift from reactive policing to predictive, algorithm-based models.

In this context, the paper also examines the incorporation of these technologies into the Portuguese security landscape, showing how their adoption reflects both a strategy of modernisation and an alignment with global discourses on the inevitability

of technological advancement. Accordingly, it is argued throughout the paper that algorithmic surveillance not only reconfigures the boundaries between security and social control but also presents significant ethical and political challenges. These developments call for critical scrutiny of the promises, limitations, and risks associated with such technologies.

2. The Historical Trajectory(ies) of Surveillance and Big Data: From State Control to Algorithmic Datafication

Analysing the evolution of surveillance over the past three decades enables the identification of two principal axes of development that continue to shape both the current landscape and future trajectories of big data. First, there has been a notable expansion of state surveillance, historically oriented towards the collection, processing, and analysis of population data with the aim of monitoring, regulating, and influencing social and political behaviour (Haggerty & Ericson, 2007; Lyon, 2001a). Second, the proliferation of new digital technologies has made it increasingly feasible to operationalise this surveillance through more sophisticated means, including intelligent sensors, predictive algorithms, and data mining[1] techniques, which are employed to generate strategic intelligence (Gandy, 2006).

This process of techno-scientific innovation has contributed to what Corbett and Marx (1991) termed the "new surveillance", characterised by the integration of digital, biometric, and predictive technologies within the security domain. These developments were further accelerated by the global fight against terrorism and cross-border crime (Bigo, 2006), gaining political and institutional legitimacy in the process. The terrorist attacks in the United States (2001), Madrid (2004), London (2005), Paris (2015), and Brussels (2016) significantly intensified the widespread adoption of such technologies, fuelling increasing enthusiasm for their purported efficiency in identifying individuals and preventing criminal threats (Beck, 2002; Bunyan, 2010; Monahan, 2010; Monar, 2008).

The global security response to these threats has fostered increased transnational police and judicial cooperation, establishing digital surveillance as a central component of public security policies. However, it is crucial to avoid what Corbett and Marx (1991) term "the fallacy of explicit agendas" (p. 402) — the misconception that these technologies emerge solely for technical purposes, devoid of political or structural motivations. As Lyon (2015) argues, the extensive collection of data and the deployment of advanced analytical tools are not mere by-products of technological progress; they represent strategic risk management approaches within the security industry, where entire populations are statistically categorised, even in the absence of concrete suspicions (Norris & McCahill, 2006). This form of surveillance is directed not only at identified individuals but also at categories of people, networks, and geographical or temporal spaces deemed to be at risk (Marx, 2002), marking a significant departure from traditional surveillance models.

[1] A computational process designed to detect anomalies, patterns, and correlations across data sets, with the aim of predicting outcomes (Pramanik et al., 2017).

The growing public and political legitimisation of surveillance networks has driven the proliferation of interconnected systems aimed at identifying, classifying, and controlling individuals and groups. Paradigmatic examples include the European Dactyloscopy (EURODAC), established in 2003 to compare the fingerprints of asylum seekers; the Visa Information System (VIS), operational since 2011, which facilitates the sharing of visa data among Schengen member states; and the Prüm Decisions (Decision 2008/615/JHA; Decision 2008/616/JHA), which govern the exchange of genetic data, vehicle registration information, and fingerprints as part of a broader strategy to combat terrorism and organised crime.

The convergence of previously dispersed systems has intensified this panorama of integrated surveillance into a complex assemblage of surveillance (Deleuze & Guattari, 1987; Haggerty & Ericson, 2007; Lyon, 2022), marked by the abstraction of physical bodies and their transformation into invisible data flows (Haggerty & Ericson, 2000). The datafication of societies (Cukier & Mayer-Schoenberger, 2013) has recast individuals as statistical entities, with far-reaching implications for how they are categorised, monitored, and governed. As Strauß (2018) observes, this digital reconfiguration fragments subjects into discrete "data points" (p. 56), thereby reshaping the thresholds and logic of contemporary surveillance.

The rise of big data has significantly intensified dataveillance (Clarke, 1988; Garfinkel, 2000; Lyon, 2022) — the systematic monitoring of actions and interactions through extensive data collection and processing infrastructures. This development has contributed to the consolidation of an ecosystem in which pattern recognition and algorithmic categorisation not only inform the regulation of individual behaviour but also underpin a market logic driven by the commercial exploitation of personal information — what Zuboff (2019) terms "data capitalism". As Esposti (2014) notes, this digitised surveillance extends beyond the realm of security, permeating the data economy, where profile segmentation and the prediction of behavioural trends serve both commercial and political agendas.

In this way, surveillance and crime control have become inextricably linked to the constitution of modern subjectivities, operating through the mediation of information flows circulating between computers, databases, and interconnected networks (Machado, 2021). In the United States, the massification of surveillance has extended beyond institutions traditionally tasked with criminal control into sectors such as health and education, contributing to what Garland (2001) describes as a culture of control. This logic of permanent monitoring, once confined to specific policing contexts, has gradually become globalised, establishing itself as a core socio-technical infrastructure of contemporary governance. As Lyon (1994, 2001a) highlights, this trajectory culminates in the emergence of a society marked by continuous surveillance and pervasive states of heightened vigilance (Corbett & Marx, 1991; Norris & Armstrong, 1999), in which the boundaries between security and social control are increasingly blurred.

Mapping this trajectory allows us to understand that the evolution of surveillance and big data is neither neutral nor merely technical. Rather, it reflects deep structural transformations that reconfigure the boundaries between public and private, visible

and invisible, permitted and prohibited. The datafication of society has not only expanded mechanisms of observation and regulation but also relocated decision-making processes to algorithmic systems that operate with growing opacity. These technologies do not simply replace human decision-making; more insidiously, they seek to shape or even determine decisions at the individual level, conditioning choices, behaviours, and life paths in subtle and continuous ways (Zuboff, 2019). Consequently, grasping the nature of contemporary surveillance demands a critical examination of its historical roots, its continuities and ruptures, and, above all, its implications for the constitution of future societies.

3. Surveillance in the Age of Big Data: Expanding Networks, Risk Management, and New Technologies

Contemporary transformations in surveillance reflect a paradigmatic shift from disciplinary practices to security strategies centred on risk management (Cunha, 2008; Maciel & Machado, 2014). This transition entails a reorientation from a model focused on eradicating crime through disciplinary mechanisms to one that prioritises the anticipation and prediction of crime, structuring security policies around the identification and minimisation of risks (Garland, 2001; Lyon, 2004). Within this framework, emerging surveillance technologies and techniques have been promoted under the banner of enhanced efficiency in securing public order (Bygrave, 2002; Lyon, 2001b), legitimising increasing investment in their deployment.

The tables that Foucault (1975/1999) identified as key instruments of disciplinary power in the 18th century have now been transformed into vast digital databases, eliminating the need for physical, visible mechanisms of discipline. As surveillance evolves from discipline to security (Cunha, 2008), control (Deleuze & Guattari, 1987), and risk management (de Laat, 2019), it has firmly established itself as a technology of power. Widely funded, praised, and defended for its symbolic and functional role in social regulation (Baird, 2018; Monahan, 2010), this valorisation has facilitated substantial investments in infrastructures designed for identifying, monitoring, and analysing individual data (Monahan, 2010).

With its growing expansion, private companies specialising in security began integrating advanced algorithms to cross-reference data from various sources, such as bank records, medical files, and web browsing cookies (Lyon, 2015; Miller, 2014). This process has led to the integration of databases as a crucial tool in police operations (Durão, 2009; Ericson & Haggerty, 1997; Van Brakel & De Hert, 2011), enabling the centralisation, storage, and extensive processing of information on suspects and convicted individuals (Durão, 2009; Haggerty, 2012; Van Brakel & De Hert, 2011). For instance, we are witnessing the gradual replacement of physical archives and in-person intelligence gathering (Marx, 1988) with pervasive mass surveillance systems (Ball & Webster, 2003), where the quantification of risk (Machado & Santos, 2016) now drives predictive policing interventions.

Although often perceived as recent innovations, the practices of quantifying risk and predicting crime have historical roots. McQuade (2021) emphasises that "a longer historical perspective, however, suggests that this contemporary change in policing may be more cyclical than singular, a return to an earlier moment, not a definitive break from the past" (p. 113), highlighting the historical continuity between modern predictive models and earlier crime management approaches. This continuity is evident in examples such as the Chicago School of 1925 (Park & Burgess, 1925), which introduced a probabilistic model to predict criminal recidivism in the context of probation. In the 1970s and 1980s, U.S. courts began employing data quantification as a criterion for decision-making (Afzal & Panagiotopoulos, 2024), cementing actuarial approaches that use numerical indicators to manage criminal risk (McCahill, 2022; Neiva, 2020). By 1994, the CompStat programme was developed in New York as a system to analyse criminal patterns and guide the allocation of police resources (Afzal & Panagiotopoulos, 2024; Creemers, 2021).

The integration of these approaches into the criminal justice system has catalysed the growth of predictive policing, which uses statistical analysis to identify emerging crime trends (Amoore, 2011; Lyon, 2004). This development has reinvigorated what Feeley and Simon (1992) describe as "actuarial justice" or "new penology", characterised by the use of data to assess individual and collective risks. This shift has been accompanied by the advancement of intelligence technologies that enable the large-scale classification and monitoring of individuals, using the data analysed to inform social control strategies (Garland, 2001; Innes et al., 2005; Kirby & Keay, 2021; Newburn, 2012). The integration of such technologies has given rise to new surveillance paradigms, where the absence of physical barriers and the invisibility of monitoring processes have become defining features. As Poster (1990) noted over 35 years ago — and his insight remains pertinent today — "a system of surveillance without walls, windows, towers, or guards" (p. 93) has become the norm, eliminating the need for direct physical contact with those under surveillance (Marx, 2006).

In this logic, contemporary surveillance incorporates the principles of biopower conceptualised by Foucault (2003), operating not only on individual bodies but on entire populations (Ericson & Haggerty, 1997). The categorisation of individuals according to risk criteria reflects the rationality of biopower, which seeks to regulate social flows by separating "good" and "bad" circulation (Foucault, 2008, p. 34). Big data thus emerges as a paradigmatic technology of security management, wherein crime control is enacted through population segmentation and the statistical quantification of threat, legitimising police interventions based on risk profiles. The deployment of algorithms to classify and predict future behaviour has engendered a process of digital segregation, whereby geographic spaces and demographic groups are designated according to danger indices generated by mathematical models (Duxbury & Andrabi, 2022; Graham, 2006). Simultaneously, predictive policing and risk assessments reinforce the normalisation of algorithmic surveillance (Ericson & Haggerty, 1997; Feeley & Simon, 1992; Garland, 1997), consolidating it as a defining mechanism of contemporary societies.

In practical terms, this transformation reorients the focus of the criminal justice system, from investigating the causes of crime to identifying potential suspects (Andrejevic

et al., 2020). Rather than addressing the structural conditions underlying criminal behaviour, the emphasis shifts towards anticipating which individuals or groups are statistically more likely to offend in the future. Consequently, the large-scale analysis of population data increasingly supplants traditional methods grounded in concrete evidence, reinforcing the use of predictive assessments as tools of social control (Dencik, 2022). A pertinent example is the Harm Assessment Risk Tool employed by the Durham Constabulary in the United Kingdom, designed to estimate the probability of an individual committing an offence within a two-year timeframe (Justice and Home Affairs Committee, 2022). Such practices exemplify a surveillance paradigm predicated on the massive aggregation of data, in which the categorisation of individuals according to assessed security risk becomes a central organising principle.

These contemporary dynamics prompt renewed reflections on the panopticon, originally conceived by Jeremy Bentham in the 18th century[2] (Innes, 2003; Mathiesen, 1997). Although critiqued by scholars such as Bogard (1996, 2006) and Haggerty (2006), the panopticon remains a valuable analytical lens through which to understand the reconfigurations of digital surveillance. Nevertheless, the classical model has been superseded by what Cunha (2008) terms a technological panopticon, marked by the mobility and decentralisation of surveillance devices, whose omnipresence infiltrates everyday life and extends well beyond bounded physical spaces (Corbett & Marx, 1991). Within this framework, big data emerges as the contemporary embodiment of this logic of vigilance — what the War Studies Department at King's College London (War Studies KCL, 2022) identifies as the next generation of security — reshaping policing practices, redefining social boundaries, and institutionalising a security *ethos* grounded in large-scale data collection and algorithmic processing.

4. The Convergence of Traditional Surveillance and Big Data: New Paradigms and Socio-Technical Tensions

The advent of big data promotes the intersection between two traditionally distinct types of surveillance: mass surveillance and targeted surveillance. The former, as conceived by Lyon (2014b, 2015), assumes that any individual can be detected within the vast surveillance ecosystem, while the latter aims to identify and monitor specific suspects. However, with the expansion of big data, these categories are becoming increasingly blurred, leading to a methodological and operational merger (Brayne, 2014, 2022). Although big data enables the mass collection of information, it ultimately operates under the logic of targeted surveillance, as its primary objective is to identify subjects considered suspicious (Lyon, 2015). In this context, Margaret Hu (2015) argues

[2] Originally proposed by Bentham (1995), the panopticon was an architectural structure designed for prisons, enabling continuous and permanent control of the inmate population through the strategic use of space and light as surveillance mechanisms. As part of a broader disciplinary system rooted in hierarchical observation (Foucault, 1975/1999), this design featured a central watchtower surrounded by a ring of cells, allowing guards to observe inmates without being seen. This visual asymmetry induced inmates to internalise the sense of constant surveillance, thereby functioning as a mechanism of discipline and self-regulation. Extending beyond the prison context, Foucault (1975/1999) expanded the concept to illustrate how panoptic principles underpin wider structures of power and surveillance in society, revealing the pervasive reach of disciplinary mechanisms across social institutions.

that these technologies construct a world of potential suspects, where the indiscriminate collection of data on all citizens makes it possible to establish digital associations between individuals and past or future criminal events (Hu, 2015; Van Brakel & Govaerts, 2024). This logic extends the surveillance network (Joh, 2016), shifting from a model based on monitoring previously identified suspects to a broader approach that places the entire population under potential scrutiny (Miranda, 2020). Within this framework, control is no longer focused on specific events. It becomes continuous, unlimited and modular, aligning with what Deleuze (2006) described as "societies of control" — contexts in which suspicion ceases to be a transitory state and evolves into a latent and permanent condition.

Schafer et al. (2011) argue that this new security ecosystem transforms the traditional logic of the presumption of innocence — where only a few individuals are monitored — into a paradigm of presumption of guilt, in which all citizens are, at least superficially, subject to constant scrutiny[3]. Big data enables these two modes of observation to converge, linking digital representations of individuals to their physical presence (Hu, 2015) and creating profiles based on algorithmic projections that influence police actions (Blount, 2024). The goal is no longer simply to investigate a target individual based on well-founded suspicions but to anticipate and shape the future by developing predictive models that, using aggregated data, project risk scenarios and inform social control strategies (Hu, 2015). As Latour (1987) notes, the construction of these calculation centres — databases and algorithmic systems — facilitates the collection and processing of dispersed information, which is reconfigured remotely and transformed into operational knowledge for police and security institutions (Haggerty & Ericson, 2000). Thus, big data surveillance not only operates with an increasing abstraction of physical bodies but also reinforces a model of security governance based on algorithmic risk management.

Despite the apparent distinctions between traditional surveillance and surveillance based on big data, both share a common core: the monitoring and control of individuals. While traditional surveillance relies on patrols and direct observation, big data replaces physical proximity with a digitalised monitoring and categorisation system, creating a symbolic distance in the act of surveillance. This allows for the inference of behavioural patterns and the construction of future scenarios based on previously collected data (Lyon, 2022). This phenomenon translates into a model of remote control, operated by algorithmic processes that transform individuals into numerical representations, categorising them under a depersonalised digital framework (Frois, 2008). As Brayne (2022) observes, the massive digitisation of information is "the main secular trend shaping surveillance in recent decades" (p. 372). This transformation shapes a new monitoring regime that is increasingly embedded in technological infrastructures (Lyon, 2022). The proliferation of these new forms of surveillance has expanded to the global and European levels, becoming a structural component of social control systems (Machado, 2021). The knowledge generated by computer analyses is progressively taking precedence over

[3] Some forensic databases exemplify this logic by retaining genetic profiles of unconvicted individuals, who are identified and can be permanently traced in future investigations. This biometric inscription acts as a marker of continuous suspicion, where the presumption of innocence is increasingly replaced by a logic of latent and automated surveillance (Kruse, 2010).

the practical experience of police officers, creating tensions between decision-making models based on algorithmic ontology and those rooted in traditional interpretative narratives (Machado, 2021).

This context helps to understand how big data fits into a techno-security governance model, where necessity, authority, and truth are exploited to legitimise mass surveillance (Skinner, 2018). Unquestioning trust in technologies, underpinned by a discourse of scientific infallibility (Costa et al., 2002), contributes to the subjugation of individuals, jeopardising fundamental rights such as freedom, equality, the presumption of innocence, and identity self-determination (Blount, 2024; Sachoulidou, 2023). The widespread dissemination of laudatory narratives about the role of digital technologies in public safety has been a key factor in the social acceptance of these practices, embedding in the collective imagination the belief that technological power is indispensable for crime prevention (see also Prainsack & Toom, 2010). This narrative is reinforced by popular fictional representations such as Person of Interest (Grondin & Hogue, 2024) or CSI: Crime Scene Investigation (Machado & Santos, 2012; Schweitzer & Saks, 2007), which glorify the use of intelligent surveillance and investigation systems. This security imaginary has influenced the development of increasingly automated surveillance infrastructures. For instance, at the Los Angeles Police Department, Brayne (2017) documents that, since 2015, police consultation systems have been complemented by automated alerts. Rather than relying solely on officers manually searching for information, databases now generate real-time notifications whenever algorithms detect patterns considered anomalous. As Elizabeth Joh (2016) notes, this transformation represents "an important expansion in the powers of the police" (p. 16), significantly enhancing their operational capabilities (Volkwein, 2022) and deepening the intersection between surveillance and the exploitation of big data (Rowe & Muir, 2021).

In this scenario, police functions undergo a substantial change, moving from a logic of repression and punishment to a control model based on collecting, analysing and managing information (Ericson & Haggerty, 1997). Thus, the adoption of surveillance technologies as structuring instruments of police action reflects a belief in the infallibility of technology, forming part of a security *ethos* that redefines penal culture and the administration of justice in contemporary times (Machado, 2021). For example, speeches in the Assembly of the Republic (Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, 2021) emphasised the acceptance of video surveillance as a useful tool in preventing and fighting crime, reflecting the authorities' confidence in technology to maintain public order and security. At national and international police events, such as the "AIDA Information Day" and the "VI Congresso de Investigação Criminal da Polícia Judiciária" (VI Congress of the Criminal Investigation Police) in 2023, where participants highlighted the benefits and potential of big data in criminal contexts, underscoring that it "will reduce investigation time", "will empower law enforcement agencies with promising solutions", and that there is "a need to make the most of technology". These events also framed the technology as part of "a brave new world", bringing "opportunities for criminal investigation" (Neiva, 2024, p. 28).

5. The Modernisation of Surveillance in Portugal: Navigating History, Technology, and the Legitimisation of Control

The evolution of surveillance in Portugal has been profoundly influenced by technological advancements and their growing integration into policing and criminal investigation systems. The national trajectory reflects a shift from traditional paper files and typewriters to digital systems for storing and processing police data. This transition has encompassed not only new forms of communication and transportation but also the digitisation of criminal information-sharing methods, solidifying an ongoing process of modernisation and technological innovation (Miranda, 2020). From the early use of anthropometric techniques for characterising individuals based on physical traits to the establishment of forensic fingerprint and DNA databases, Portugal has kept pace with global transformations in surveillance, albeit in a somewhat fragmented manner (Machado & Frois, 2014). Within this framework, the computerisation of police systems has emerged as a key tool, enabling increasingly automated collection, recording, and internal sharing of criminal information (Durão, 2009).

Despite the aspiration for modernisation, the adoption of surveillance technologies in Portugal did not occur in a linear fashion or without significant obstacles. A historical analysis highlights how the discontinuities between the past, present, and future of technology have influenced the implementation of innovations in this field. One of the most decisive factors was the dictatorship of António de Oliveira Salazar (1926–1974), which placed Portugal under a conservative, repressive political model that was hostile to technological advancement. The Estado Novo regime, supported by a system of censorship and a robust political surveillance apparatus operated by the International and State Defence Police, rejected any innovation that could undermine its mechanisms of control and repression (Pimentel, 2024).

The Carnation Revolution of 1974 marked a decisive turning point from the authoritarian regime, but the technological modernisation of surveillance and public security infrastructures did not occur immediately. The real impetus came three decades later, with the organisation of the European Football Championship — Euro 2004[4]. The scale of the event required a substantial reinforcement of security measures, which led to the adoption and expansion of surveillance technologies in public spaces. This development mirrors similar processes in other countries, such as Greece, where the implementation of CCTV (Closed-Circuit Television) during the Olympic Games reflected a highly technocratic security model, prioritising technological dominance over traditional policing strategies (Frois & Machado, 2016).

The implementation of public video surveillance systems in Portugal began in 2005, expanding a practice that had previously been limited to enclosed spaces (Frois, 2014). However, despite the political enthusiasm surrounding its adoption, the spread of this technology encountered significant resistance. By 2010, only three locations had authorised and operational video surveillance systems — Porto, Coimbra, and the Sanctuary of

[4] Although just two years after the Revolution of April 25, 1974, some changes were already underway, notably with the establishment of a central civil and criminal identification archive, created by Decree-Law 63/1976 of January 24 (Miranda, 2020).

Fátima — and by 2012, just two systems remained active due to obstacles imposed by the data protection authority[5] (Machado & Frois, 2014).

The year 2005 also marked the introduction of a proposal to create a national genetic database with a universal scope, presented in the programme of the 17th Constitutional Government of Portugal. This database was intended for both civil identification and criminal investigation purposes. Under the argument of improving efficiency in the fight against crime, the database was established and legislated in 2008[6]. This development is part of a broader European trend towards the adoption of digital forensic technologies, exemplified by the Council of Europe's Recommendation No. R (92) 1 (1992) on the use of genetic data in criminal justice, as well as the Prüm Treaty, which governs the exchange of genetic data between European Union member states. In this regard, the Portuguese case reflects a transnational alignment with technological security policies, where the deployment of advanced forensic technologies is seen as a key instrument for enhancing policing and public security.

This evolution of surveillance technologies in Portugal must be understood, as Helena Machado and Catarina Frois (2014) argue, in the context of a "policy formulation in the broadest sense" (p. 75), which reflects a collective ambition for security modernisation. This modernising narrative is driven by a political discourse that frames technology as the solution to combating crime, positioning it as central to creating a safer and more efficient society (Frois, 2014; Miranda, 2020). Thus, both the implementation of video surveillance systems and the creation of the genetic database reflect the national desire to align with practices regarded as technologically advanced, often driven by a worldview from the centre, where the institutional and technical models of central countries are seen as an indispensable reference for progress and modernity (Ribeiro, 2004). In this context, there is a reinforced belief that these tools are more effective than traditional criminal investigation methods.

More than just security tools, these technologies serve as symbolic representations of the country's progress and its capacity to align with international standards. As Diana Miranda (2020) points out, "the modernisation enabled by technology (...) and the need for development contrast, in political discourse, with the acknowledgement of backwardness, a certain 'inferiority complex', and a perception of Portugal's peripheral and underdeveloped status" (p. 6; see also Frois, 2013; Nunes & Gonçalves, 2001). In this sense, the adoption of these technologies not only addresses practical security needs but also reflects a broader ambition to transcend Portugal's peripheral position, positioning technology as a marker of progress and sophistication in surveillance and social control.

[5] "The Portuguese Data Protection Authority (CNPD) is an independent administrative body (...) endowed with administrative and financial autonomy, with authority to work alongside the Assembly of the Republic. The CNPD monitors and supervises compliance with the General Data Protection Regulation, Law 58/2019, Law 59/2019, and Law 41/2004, as well as other legal and regulatory provisions related to the protection of personal data. Its role is to safeguard individuals' rights, freedoms, and guarantees in relation to the processing of their personal data." (Comissão Nacional de Proteção de Dados, n.d.).

[6] Law No. 5/2008, of February 12, established the creation of a DNA profile database for civil and criminal identification purposes (Procuradoria-Geral Regional de Lisboa, n.d.).

6. Conclusion

The analysis presented here sheds light on how surveillance and the technologies associated with big data have become foundational infrastructures in contemporary policing and criminal investigation. The historical evolution of control practices reveals a trajectory marked by both continuity and disruption, where traditional mechanisms of power are reconfigured and adapted to new socio-technical contexts. Surveillance, far from being a solely contemporary phenomenon, stands as a structuring element of modernity, evolving into increasingly sophisticated and invisible forms. In this process, the datafication of everyday life emerges as the new paradigm of security.

This article has highlighted how optimistic imaginaries surrounding the transformative potential of technologies have been constructed, shaping both present-day experiences and future projections of security and policing. The belief in algorithmic infallibility and big data neutrality underpins narratives that legitimise their widespread integration into security dynamics while obscuring the associated risks and social implications. The proliferation of this techno-optimistic logic contributes to the normalisation of algorithmic surveillance as an inevitable practice, pushing critical discussions on fundamental rights, privacy, and structural inequalities into the background.

The historical mapping of surveillance technologies enables us, drawing on Foucault's (1975/1999) work, to craft a history of the present that illuminates how surveillance becomes embedded in institutions and social practices. The legacy of control technologies does not vanish; rather, it remerges in new forms, integrated into increasingly sophisticated and opaque infrastructures — often black-boxed (Latour, 1987), meaning enclosed in systems whose operating logic is inaccessible to public scrutiny. The rise of predictive policing and risk analysis tools driven by big data, therefore, does not mark a complete rupture with previous models but rather their adaptation to a context of hyperconnectivity and the proliferation of global databases.

In this context, it is essential to critically examine the ethical and political ramifications of this emerging surveillance architecture. The convergence of mass surveillance with targeted surveillance blurs the lines between suspects and non-suspects, fostering a security model based on the collectivisation of suspicion and continuous monitoring. The consequences of this shift are far-reaching: the transformation of policing into an algorithmic process of crime prediction diverts attention from the social and structural factors that contribute to crime, replacing it with a probabilistic model that categorises individuals and areas based on perceived risk. This shift carries the significant risk of reinforcing historical inequalities, as algorithms, often trained on past data, tend to perpetuate existing systemic biases and discriminatory patterns (Brayne, 2017).

A brief analysis of the Portuguese case demonstrates that the adoption of these technologies is not a detached event but is embedded within a broader historical process of security modernisation, where technology is often presented as the panacea for addressing structural and political challenges. The establishment of genetic databases and the expansion of video surveillance networks in the country not only enhance social control but also reflect a desire to conform to international security norms, often with little critical reflection on the social and ethical consequences.

In this context, it is crucial to critically consider the future trajectories being constructed regarding the use of big data in policing and criminal investigations. What kind of society are we creating when security decisions are made by algorithmic calculations that function opaquely, beyond democratic oversight? How can we ensure that the promises of increased efficiency and predictability do not lead to sophisticated forms of exclusion and criminalisation of certain social groups? Paradoxically, this covert and automated surveillance may coexist with overt and highly visible forms of control targeting racialised or marginalised populations, as evidenced by police interventions in urban spaces linked to cultural differences, such as Rua do Benformoso in Lisbon (Neves, 2024).

Current trends indicate that we are moving towards a model of security governance marked by an escalation of digital surveillance, which is increasingly embedded in technical infrastructures beyond the direct control of citizens and, at times, even security personnel themselves. However, it is crucial to acknowledge that this logic of invisibility and automation is juxtaposed with public and highly visible forms of control, often targeting marginalised populations. This duality reveals a security landscape marked by significant asymmetry, where different regimes of visibility are selectively imposed. Nevertheless, it is equally important to recognise the emergence of counter-surveillance or *sousveillance* (Mann et al., 2003), in which citizens use technology to monitor the actions of security forces. A paradigmatic example is the use of bodycams, whose ambivalence has been explored by scholars such as Diana Miranda (2022), who highlights how these technologies can both enhance transparency and amplify surveillance. Simultaneously, phenomena such as citizen journalism — where citizens document and disseminate police interactions — have been altering the visibility of policing and reshaping the relationship between surveillance and power (Goldsmith, 2010; Huey & Broll, 2012).

It is, therefore, essential to advocate for a robust public debate on the limits of digital surveillance, the transparency of algorithmic systems, and the necessity of establishing regulatory and accountability mechanisms. If algorithmic surveillance is reshaping the landscape of policing and criminal justice, it is our responsibility to critically examine its consequences and resist its uncritical adoption. The history of surveillance is not merely a history of power and control but also a history of struggles for freedom, privacy rights, and the construction of more just societies. By understanding the past of surveillance, we can question its future and, more importantly, challenge the technological determinism often presented to us as unquestionable progress.

Translation: Anabela Delgado

Acknowledgements

The author would like to express her sincere gratitude to Professor Helena Machado, the scientific supervisor of the doctoral research that provided the foundation for the analysis presented in this article, as well as to the reviewers, whose constructive feedback greatly enhanced the quality of the text.

This work was funded by FCT – Foundation for Science and Technology, I.P., through the award of a doctoral scholarship (reference 2020.04764.BD and DOI 10.54499/2020.04764.BD) from the national budget and the EU budget via the European Social Fund (ESF).

This work is supported by national funds through FCT – Foundation for Science and Technology, I.P., under projects UIDB/00736/2020 (base funding) and UIDP/00736/2020 (programme funding).

References

Afzal, M., & Panagiotopoulos, P. (2024). *Data in policing: An integrative review. International Journal of Public Administration*, 1–20. https://doi.org/10.1080/01900692.2024.2360586

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society*, *28*(6), 24–43. https://doi.org/10.1177/0263276411417430

Andrejevic, M., Dencik, L., & Treré, E. (2020). From pre-emption to slowness: Assessing the contrasting temporalities of data-driven predictive policing. *New Media & Society*, *22*(9), 1528–1544. https://doi.org/10.1177/1461444820913565

Baird, T. (2018). Interest groups and strategic constructivism: Business actors and border security policies in the European Union. *Journal of Ethnic and Migration Studies*, *44*(1), 1–19. https://doi.org/10.1080/1369183X.2017.1316185

Ball, K., & Webster, F. (2003). The intensification of surveillance. In K. Ball & F. Webster (Eds.), *The intensification of surveillance: Crime, terrorism and warfare in the information era* (pp. 1–15). Pluto Press.

Beck, U. (2002). The terrorist threat: World risk society revisited. *Theory, Culture & Society*, *19*(4), 39–55. https://doi.org/10.1177/026327640201900400 3

Bentham, J. (1995). *The panoptic writings*. Verso Trade.

Bigo, D. (2006). Globalized (in)security: The field and the ban-opticon. In D. Bigo & A. Tsoukala (Eds.), *Terror, insecurity and liberty. Illiberal practices of liberal regimes after 9/11* (pp. 10–48). Routledge.

Blount, K. (2024). Using artificial intelligence to prevent crime: Implications for due process and criminal justice. *AI & SOCIETY*, *39*, 359–368. https://doi.org/10.1007/s00146-022-01513-z

Bogard, W. (1996). *The simulation of surveillance: Hyper-control in telematic societies*. Press Syndicate of the University of Cambridge.

Bogard, W. (2006). Welcome to the society of control: The simulation of surveillance revisited. In K. Haggerty & R. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 55–78). ACUP.

Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review*, *79*(3), 367–391. https://doi.org/10.1177/0003122414530398

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brayne, S. (2022). The banality of surveillance. *Surveillance & Society*, *20*(4), 372–378. https://doi.org/10.24908/ss.v20i4.15946

Bunyan, T. (2010). Just over the horizon: The surveillance society and the state in the EU. *Race & Class*, *51*(3), 1–12. https://doi.org/10.1177/0306396809354162

Bygrave, L. A. (2002). *Data protection law. Approaching its rationale, logic, and its limits*. Kluwer Law International.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias. (2021). P*arecer sobre a Proposta de Lei n.º 111/XIV/2.ª (GOV) – Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança*. Assembleia da República.

Comissão Nacional de Proteção de Dados. (n.d.). *O que somos e quem somos*. Retrieved November, 3, 2022, from https://www.cnpd.pt/cnpd/o-que-somos-e-quem-somos/

Corbett, R., & Marx, G. T. (1991). Critique: No soul in the new machine: Technofallacies in the electronic monitoring movement. *Justice Quarterly*, *8*(3), 399–414. https://doi.org/10.1080/07418829100091111

Costa, S., Machado, H. C., & Nunes, J. A. (2002). O ADN e a justiça: A biologia forense e o direito como mediadores entre a ciência e os cidadãos. In M. E. Gonçalves (Ed.), *Os portugueses e a ciência* (pp. 199–233). Dom Quixote.

Creemers, N. (2021). *The policing assemblage: On the co-evolution of technology, knowledge, and policing in New York City*. Technische Universität Berlin.

Cukier, K. N., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, *92*(3), 28–40.

Cunha, M. I. (2008). Disciplina, controlo, segurança: No rasto contemporâneo de Foucault. In C. Frois (Ed.), *A sociedade vigilante: Ensaios sobre privacidade, identificação e vigilância* (pp. 67–81). Imprensa de Ciências Sociais.

de Laat, P. B. (2019). The disciplinary power of predictive algorithms: A Foucauldian perspective. *Ethics and Information Technology*, *21*, 319–329. https://doi.org/10.1007/s10676-019-09509-y

Decisão 2008/615/JAI do Conselho, de 23 de Junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. (2008). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32008D0615

Decisão 2008/616/JAI do Conselho, de 23 de Junho de 2008 , referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras. (2008). Jornal Oficial da União Europeia. https://eur-lex.europa.eu/eli/dec/2008/616/oj/?locale=pt

Deleuze, G. (2006). Postscript on the societies of control. In D. Wilson & C. Norris (Eds.), *Surveillance, crime and social control* (pp. 35–39). Routledge.

Deleuze, G., & Guattari, F. (1987). Introduction: Rhizome. In G. Deleuze & F. Guattari (Eds.), *A thousand plateaus* (pp. 3–28). University of Minnesota Press.

Dencik, L. (2022). The datafied welfare state: A perspective from the UK. In A. Hepp, J. Jarke, & L. Kramp (Eds.), *New perspectives in critical data studies: The ambivalences of data power* (pp. 145–166). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-96180-0_7

Durão, S. (2009). La producción de mapas policiales: Prácticas y políticas de la policía urbana en Portugal. *Intersecciones en Antropología*, *10*(1), 43–61.

Duxbury, S. W., & Andrabi, N. (2022). The boys in blue are watching you: The shifting metropolitan landscape and big data police surveillance in the United States. *Social Problems*, *71*(3), 912–937. https://doi.org/10.1093/socpro/spac044

Ericson, R. V., & Haggerty, K. D. (1997). *Policing the risk society*. University of Toronto Press.

Esposti, S. D. (2014). When big data meets dataveillance: The hidden side of analytics. *Surveillance and Society*, *12*(2), 209–225. https://doi.org/10.24908/ss.v12i2.5113

Feeley, M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, *30*(4), 449–475. https://doi.org/10.1111/j.1745-9125.1992.tb01112.x

Foucault, M. (1999). *Vigiar e punir: Nascimento da prisão* (R. Ramalhete, Trans.). Vozes. (Original work published 1975)

Foucault, M. (2003). *Society must be defended: Lectures at the Collège de France, 1975-76*. Picador.

Foucault, M. (2008). T*he birth of biopolitics: Lectures at the Collège de France, 1978-79*. Palgrave Macmillan.

Frois, C. (2008). Vigilância e identidade: Para uma nova antropologia da pessoa. In C. Frois (Ed.), A *sociedade vigilante: Ensaios sobre identificação, vigilância e privacidade* (pp. 175–191). Imprensa de Ciências Sociais.

Frois, C. (2013). *Peripheral vision. Politics, technology and surveillance*. Berghahn Books.

Frois, C. (2014). Video-surveillance and the political use of discretionary power in the name of security and defence. In M. Maguire, C. Frois, & N. Zurawski (Eds.), *The anthropology of security: Perspectives from the frontline of policing, counter-terrorism and border control* (pp. 45–61). Pluto Press.

Frois, C., & Machado, H. (2016). Modernization and development as a motor of polity and policing. In B. Bradford, B. Jauregui, I. Loader, & J. Steinberg (Eds.), *The SAGE handbook of global policing* (pp. 391–405). SAGE.

Gandy, O. (2006). Data mining, surveillance, and discrimination in the post-9/11 environment. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 363–384). University of Toronto Press.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. O'Reilly.

Garland, D. (1997). Governmentality and the problem of crime: Foucault, criminology, sociology. *Theoretical Criminology*, *1*(2), 173–214. https://doi.org/10.1177/1362480697001002002

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. Oxford University Press.

Goldsmith, A. (2010). Policing's new visibility. *The British Journal of Criminology*, *50*(5), 914–934. https://doi.org/10.1093/bjc/azq033

Graham, S. (2006). *Constructing 'Homeland' and 'Target' - Cities in the 'War on Terror'*. Public Culture.

Grondin, D., & Hogue, S. (2024). Person of interest as media technology of surveillance: A cautionary tale for the future of the national security state with diegetic big data surveillance, algorithmic security, and artificial intelligence. *Television & New Media*, *25*(4), 334–351. https://doi.org/10.1177/15274764231210280

Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In D. Lyon (Ed.), *Theorizing surveillance* (pp. 23–45). Willan.

Haggerty, K. D. (2012). Book review: The New Social Control: The Institutional Web, Normativity and the Social Bond. *Theoretical Criminology*, *16*(4), 527–531. https://doi.org/10.1177/1362480612454951

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. B*ritish Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Haggerty, K. D., & Ericson, R. V. (2007). The new politics of surveillance and visibility. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 3–26). University of Toronto Press.

Hu, M. (2015). Small data surveillance v. big data cybersurveillance. *Pepperdine Law Review*, *42*(4), 773–844.

Huey, L., & Broll, R. (2012). 'All it takes is one TV show to ruin it': A police perspective on police-media relations in the era of expanding 'citizen journalism'. *Policing and Society*, *22*(4), 384–396. https://doi.org/10.1080/10439463.2011.641556

Innes, M. (2003). *Understanding social control: Deviance, crime and social order*. Open University Press.

Innes, M., Fielding, N., & Cope, N. (2005). "The appliance of science?": The theory and practice of crime intelligence analysis. *British Journal of Criminology*, *45*(1), 39–57. https://doi.org/10.1093/bjc/azh053

Joh, E. (2016). The new surveillance discretion: Automated suspicion, big data, and policing. *Harvard Law & Policy Review*, 1–33.

Justice and Home Affairs Committee. (2022). *Technology rules? The advent of new technologies in the justice system*. Westminster.

Kirby, S., & Keay, S. (2021). *Improving intelligence analysis in policing*. Routledge.

Kruse, C. (2010). Forensic evidence: Materializing bodies, materializing crimes. *European Journal of Women's Studies*, *17*(4), 363–377. https://doi.org/10.1177/1350506810377699

Latour, B. (1987). *Science in action. How to follow scientists and engineers through society*. Harvard University Press.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*. Polity Press.

Lyon, D. (2001a). Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology*, *3*(3), 171–180. https://doi.org/10.1023/A:1012227629496

Lyon, D. (2001b). *Surveillance society: Monitoring everyday life*. Open University Press.

Lyon, D. (2004). Globalizing surveillance: Comparative and sociological perspectives. *International Sociology*, *19*(2), 135–149. https://doi.org/10.1177/0268580904042897

Lyon, D. (2014a). Situating surveillance: History, technology, culture. In K. Boersma, R. Van Brakel, C. Fonio, & P. Wagenaar (Eds.), *Histories of State surveillance in Europe and beyond* (pp. 32–46). Routledge.

Lyon, D. (2014b). Surveillance, Snowden, and big data: Capacities, consequences, critique. B*ig Data and Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance and Society*, *13*(2), 139–152. https://doi.org/10.24908/ss.v13i2.5363

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics* (pp. 64–77). Routledge. https://doi.org/10.4324/9781315167305-4

Lyon, D. (2022). Surveillance. *Internet Policy Review*, *11*(4), 1–19. https://doi.org/10.14763/2022.4.1673

Machado, H. (2021). O futuro incerto e as turbulências da vigilância genética na Europa. In H. Machado (Ed.), *Crime e tecnologia: Desafios culturais e políticos para a Europa* (pp. 23–40). Afrontamento.

Machado, H., & Frois, C. (2014). Aspiring to modernization: Historical evolution and current trends of State surveillance in Portugal. In K. Boersma, R. Van Brakel, C. Fonio, & P. Wagenaar (Eds.). *Histories of State surveillance in Europe and beyond* (pp. 65-78). Routledge.

Machado, H., & Santos, F. (2012). Entre a polícia ficcional e a polícia real: Os usos do DNA na investigação criminal em Portugal. In S. Durão & M. Darck (Eds.). *Polícia, segurança e ordem pública: Perspetivas portuguesas e brasileiras* (pp. 201–216). Imprensa de Ciências Sociais.

Machado, H., & Santos, F. (2016). Culturas de objetividade, epistemologias cívicas e o suspeito transnacional. Uma proposta para mapeamentos teóricos em estudos sociais da genética forense. In C. Fonseca, F. Rohden, P. S. Machado, & H. S. Paim (Eds.), *Antropologia da ciência e da tecnologia: Dobras reflexivas* (pp. 179–203). Editora Sulina.

Maciel, D., & Machado, H. (2014). Biovigilância e governabilidade nas sociedades da informação. In H. Machado & H. Moniz (Eds.), *Bases de dados genéticos forenses: Tecnologias de controlo e ordem social* (pp. 141–166). Coimbra Editora.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331–355. https://doi.org/10.24908/ss.v1i3.3344

Marx, G. T. (1988). *Undercover police surveillance in America*. University of California Press.

Marx, G. T. (2002). What's new about the "new surveillance"? Classifying for change and continuity. *Surveillance & Society*, *1*(1), 9–29. https://doi.org/10.24908/ss.v1i1.3391

Marx, G. T. (2006). Varieties of personal information as influences on attitudes towards surveillance. In K. D. Haggerty & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 79–110). University of Toronto Press.

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/10.1177/1362480697001002003

McCahill, M. (2022). Theorizing surveillance in the pre-crime society. In B. A. Arrigo & B. Sellers (Eds.), *The pre-crime society: Crime, culture and control in the ultramodern age* (pp. 227–267). Bristol University Press.

McQuade, B. (2021). World histories of big data policing: The imperial epistemology of the police-wars of U.S. hegemony. *Journal of World-Systems Research*, *27*(1), 109–135. https://doi.org/10.5195/jwsr.2021.1033

Miller, K. (2014). Total surveillance, big data, and predictive crime technology: Privacy's perfect storm. *Journal of Technology Law & Policy*, *19*(1), 105–146.

Miranda, D. (2020). Identifying suspicious bodies? Historically tracing criminal identification technologies in Portugal. *Surveillance & Society*, 1–22.

Miranda, D. (2022). Body-worn cameras 'on the move': Exploring the contextual, technical and ethical challenges in policing practice. *Policing and Society*, *32*(1), 18–34. https://doi.org/10.1080/10439463.2021.1879074

Monahan, T. (2010). *Surveilllance in the time of insecurity*. Rutgers University Press.

Monar, J. (2008). The European Union as a collective actor in the fight against post-9/11 terrorism: Progress and problems of a primarily cooperative approach. In M. Gani & P. Mathew (Eds.), F*resh perspectives on the 'war on terror'* (pp. 209–234). The Australian National University Press.

Neiva, L. (2020). *Big data na investigação criminal: Desafios e expectativas na União Europeia*. Húmus.

Neiva, L. (2024). *Expectativas de agentes policiais sobre big data no sistema de policiamento e investigação criminal em Portugal* [Doctoral dissertation, Universidade do Minho]. RepositóriUM. https://hdl.handle.net/1822/93930

Neves, C. S. (2024, December 19). *Dispositivo policial reforçado. Rixa na Rua do Benformoso fez vários feridos*. RTP Notícias. https://www.rtp.pt/noticias/pais/dispositivo-policial-reforcado-rixa-na-rua-do-benformoso-fez-varios-feridos_n1626944

Newburn, T. (2012). The future of policing. In T. Newburn (Ed.), *Handbook of policing* (2nd ed., pp. 824–841). Willan Publishing.

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society: The rise of CCTV*. Berg.

Norris, C., & McCahill, M. (2006). CCTV: Beyond penal modernism? *British Journal of Criminology*, *46*(1), 97–118. https://doi.org/10.1093/BJC/AZI047

Nunes, J. A., & Gonçalves, M. E. (2001). Introdução. In J. A. Nunes & M. E. Gonçalves (Eds.), E*nteados de Galileu? A semiperiferia no sistema mundial da ciência* (pp. 13–31). Afrontamento.

Pimentel, I. F. (2024). O 25 de Abril de 1974 e a PIDE/DGS. *Revista Crítica de Ciências Sociais*, (133), 121–146. https://doi.org/10.4000/11pr5

Poster, M. (1990). *The mode of information: Poststructuralism and social context*. Polity Press.

Prainsack, B., & Toom, V. (2010). The Prüm regime: Situated dis/empowerment in transnational DNA profile exchange. *The British Journal of Criminology*, *50*(6), 1117–1135. https://doi.org/10.1093/bjc/azq055

Pramanik, M. I., Lau, R. Y. K., Yue, W. T., Ye, Y., & Li, C. (2017). Big data analytics for security and criminal investigations. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(4), e1208. https://doi.org/10.1002/widm.1208

Procuradoria-Geral Regional de Lisboa. (n.d.). *Legislação*. Ministério Público Portugal. Retrieved October, 27, 2022, from https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1506&tabela=leis

Recomendação n.º R (92) 1. (1992). Comité de Ministros aos Estados-membros sobre a utilização da análise de ADN no âmbito do sistema de justiça penal, de 10 de fevereiro de 1992.

Ribeiro, M. C. (2004). *Uma história de regressos: Império, guerra colonial e pós-colonialismo*. Afrontamento.

Park, R. E., & Burgess, E. W. (1925). *The city*. The University of Chicago Press.

Rowe, M., & Muir, R. (2021). Big data policing: Governing the machines? In J. McDaniel & K. Pease (Eds.), *Predictive policing and artificial intelligence* (pp. 254–269). Routledge.

Sachoulidou, A. (2023). Going beyond the "common suspects": To be presumed innocent in the era of algorithms, big data and artificial intelligence. *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-023-09347-w

Schafer, J. A., Buerger, M. E., Myers, R. W., Jensen, C. J., III, & Levin, B. H. (2011). *The future of policing: A practical guide for police managers and leaders*. CRC Press.

Schweitzer, N. J., & Saks, M. J. (2007). The CSI effect: Popular fiction about forensic science affects the public's expectations about real forensic science. *Jurimetrics Journal*, *47*, 357–364.

Skinner, D. (2018). Race, racism and identification in the era of technosecurity. *Science as Culture*, *29*(1), 1–23. https://doi.org/10.1080/09505431.2018.1523887

Strauß, S. (2018). Big data – Within the tides of securitisation? In A. R. Sætnan, I. Schneider, & N. Green (Eds.), T*he politics and policies of big data* (pp. 46–67). Routledge.

Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies. *Technology-Led Policing: Journal of Police Studies*, *3*(20), 163–192.

Van Brakel, R., & Govaerts, L. (2024). Exploring the impact of algorithmic policing on social justice: Developing a framework for rhizomatic harm in the pre-crime society. *Theoretical Criminology*, *24*(1) 91–109. https://doi.org/10.1177/13624806241246267

Volkwein, C. E. (2022). Digitizing the fourth amendment: Privacy in the age of big data policing. *Privacy Certificate Student Publications*, *5*, 1–21.

War Studies KCL. (2022, 19 de janeiro). *How are emerging technologies (re)shaping the security landscape?* [Video]. YouTube. https://www.youtube.com/watch?v=aQv9p6rCLDw

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

Biographical Note

Laura Neiva is an invited assistant professor in the Department of Sociology at the Institute of Social Sciences, University of Minho, Portugal. She is also a collaborating researcher at both the Communication and Society Research Centre at the same institute and the Center for Legal, Economic, International and Environmental Studies at Lusíada University – North, in Porto, Portugal. She holds a bachelor's degree in Criminology from the Faculty of Law, University of Porto (2017), a master's degree in Crime, Difference and Inequality from the Institute of Social Sciences, University of Minho (2019), and a PhD in Sociology from the same institution (2024). Neiva is the author of the book *Big Data na Investigação Criminal: Desafios e Expectativas*

na União Europeia (Big Data in Criminal Investigation: Challenges and Expectations in the European Union, Editora Húmus). Her research interests focus on the social studies of science and technology, emerging technologies in criminal investigation, big data, surveillance studies, policing, and the role of expectations.

ORCID: https://orcid.org/0000-0002-1954-7597
Email: lauraneiva@ics.uminho.pt
Address: Campus de Gualtar. Rua da Universidade, 4710-057, Braga, Portugal

Submitted: 21/02/2025 | Accepted: 31/03/2025