

When Algorithms Watch Us: Rethinking Privacy in a Smart Society

Stella Nandhakumar¹

¹Vinayaka Mission's Law School

Publication Date: 2026/09/29

Abstract: In the rapidly evolving age of artificial intelligence (AI) and big data, algorithmic systems increasingly govern everyday life, like predicting, influencing, and manipulating behavior across digital platforms, legal enforcement, and democratic participation. These systems are no longer limited to specialized technological environments; they increasingly participate in decisions and processes that affect how individuals communicate, access services, interact with institutions, and understand their own choices. The expansion of data-driven decision-making therefore raises questions that extend beyond technical efficiency and legal compliance. This paper explores the philosophical, political, and ethical dimensions of algorithmic surveillance and argues that privacy must be reframed as a moral and existential imperative rather than a merely legal right. Using a qualitative and comparative methodology, it analyzes AI governance and surveillance models in the United States, European Union, China, and India. The comparison highlights different approaches to innovation, accountability, state power, and individual rights. The paper further considers the implications of surveillance for autonomy, equality, democracy, and human dignity. Findings indicate that algorithmic surveillance is an ethical crisis demanding transparency, accountability, meaningful human oversight, and the reaffirmation of human dignity in smart societies. The paper concludes that responsible AI governance requires not only rules governing data and algorithms but also institutional arrangements that enable citizens to understand, question, and challenge automated forms of control.

Keywords: Privacy; Algorithmic Surveillance; Artificial intelligence; Human Dignity; Transparency.

How to Cite: Stella Nandhakumar (2026) When Algorithms Watch Us: Rethinking Privacy in a Smart Society. *International Journal of Innovative Science and Research Technology*, 11(9), 1772-1777. <https://doi.org/10.38124/ijisrt/26sep573>

I. INTRODUCTION

Artificial intelligence shapes contemporary governance, mediating access to resources, opportunities, and justice. AI systems can process enormous quantities of information and identify patterns that may not be immediately visible to human decision-makers. This capacity has created opportunities for faster administration, predictive services, automated decision-making, and more personalized digital environments. At the same time, the same capacity can make individuals continuously observable and increasingly predictable. When systems collect information about searches, movements, preferences, communications, transactions, and online behaviour, surveillance can operate without the visible presence of a traditional observer. The individual may therefore experience surveillance not as a single event but as an ongoing condition of participation in digital society.

Yet, algorithmic systems embody bias, reinforcing social and economic hierarchies. Algorithms are developed from data and institutional choices, and the outputs they produce can reflect limitations or inequalities contained in those inputs. This creates an important ethical concern: technological systems may appear neutral because decisions are expressed through automated processes, even though

those processes are designed and deployed within particular social and political environments. As Shoshana Zuboff contends, behavioral data has become the raw material of surveillance capitalism (2019). The collection and analysis of behavioural data can consequently become a source of economic value as well as a mechanism through which behaviour is observed and anticipated.

Traditional privacy law rooted in consent and data ownership is ill-suited to the pervasive, predictive nature of today's technologies. Consent may become difficult to understand when data is repeatedly collected, combined with other information, and used for purposes that an individual cannot reasonably anticipate. The problem is therefore not limited to whether a person has technically agreed to the collection of information. It also concerns whether individuals retain meaningful control over how their information is interpreted and used. In societies increasingly run by invisible algorithms, privacy must be reconceptualized as a collective moral right integral to autonomy and democracy (Mahapatra 2025).

The central concern of this paper is therefore the relationship between algorithmic surveillance and the human person. The paper does not treat AI merely as a technological innovation or privacy merely as a question of

data ownership. Instead, it examines how surveillance changes the relationship between individuals, institutions, markets, and the state. The comparative discussion of the United States, European Union, China, and India is used to identify different governance philosophies and their implications for privacy, accountability, and human dignity.

II. LITERATURE REVIEW

Bentham's Panopticon introduced the paradigm of surveillance as control, later expanded by Foucault in *Discipline and Punish* (1977) to describe internalized discipline. In the Panopticon model, the possibility of constant observation encourages individuals to regulate their own conduct. Foucault's analysis developed this idea further by showing how surveillance can become a form of discipline in which people internalize expectations and modify their behaviour even when direct coercion is absent. This provides an important foundation for understanding contemporary algorithmic surveillance because digital systems can similarly create conditions in which individuals modify their behaviour in response to the possibility of being observed, recorded, assessed, or profiled.

Deleuze's *Postscript on the Societies of Control* (1992) extended this understanding to networked systems of continuous monitoring. Unlike a fixed institution with identifiable boundaries, digital control can operate across multiple platforms and situations. The individual becomes part of a continuing stream of information that can be assessed, categorized, and acted upon. This theoretical shift from visible surveillance toward continuous digital monitoring is particularly relevant to smart societies, where data collection can be embedded in ordinary activities.

In the digital age, Zuboff's *Surveillance Capitalism* (2019) exposes how corporations monetize behavioral data. Her work draws attention to the economic dimension of surveillance and the transformation of human experience into data that can be processed and used for commercial purposes. This raises a fundamental question concerning the relationship between convenience and autonomy: individuals may receive personalized services while simultaneously contributing behavioural information to systems whose broader purposes they may not fully understand.

Yuval Noah Harari warns that "Dataism" risks subjugating human autonomy (*Homo Deus*, 2018). His discussion contributes to the wider philosophical concern that excessive reliance on data-driven systems may encourage societies to treat measurable information as more authoritative than human judgment. Collectively, these scholars establish surveillance as an ethical, political, and social challenge rather than a technological inevitability. Their work also helps explain why privacy cannot be considered only in terms of secrecy. Privacy is connected with the ability to form choices, maintain individuality, and participate in society without continuous behavioural pressure.

The literature therefore provides three connected foundations for this study. First, surveillance can operate as a mechanism of discipline and control. Second, digital technologies can transform personal behaviour into a resource for prediction and economic value. Third, the increasing authority of data-driven systems can affect human autonomy. The present paper builds upon these foundations through a comparative examination of AI governance and surveillance models in four jurisdictions.

➤ *Theoretical Framework:*

This study integrates surveillance theory from Bentham to Deleuze with economic and sociopolitical critiques from Zuboff. The framework traces power's evolution from visibility (Panopticon) to predictability (algorithmic governance). Traditional surveillance is commonly understood through the relationship between an observer and an observed person. Algorithmic surveillance changes this relationship because systems can aggregate large amounts of information and generate predictions about individuals without requiring continuous direct observation.

The framework therefore distinguishes between seeing and predicting. In the Panopticon, power is associated with the possibility of being watched. In algorithmic governance, power may increasingly operate through the capacity to anticipate behaviour, classify individuals, and influence future choices. The person is not simply observed for what he or she has already done; available data may be used to construct assumptions about what the person may do next. This creates an important ethical issue because predictions can influence opportunities and treatment even when they are uncertain or incomplete.

It posits that algorithmic systems reconfigure autonomy, where individuals internalize digital norms defined by market and state actors (Du 2025). Autonomy in this context does not mean complete freedom from all external influence. Rather, it concerns the meaningful ability of individuals to make choices without hidden systems excessively shaping the conditions in which those choices are made. If algorithms determine what information is displayed, which opportunities are presented, or how an individual is classified, the individual's decision-making environment may itself be technologically structured.

Human dignity provides the normative foundation of this framework. Treating privacy as a moral right means recognizing that individuals are not merely sources of data. Their personal information is connected with identity, relationships, preferences, vulnerability, and participation in public life. Consequently, protecting privacy also protects the conditions necessary for independent thought and democratic participation. Transparency and accountability become essential because individuals need meaningful ways to understand and question systems that affect them.

III. COMPARATIVE ANALYSIS

➤ *U.S., EU, China, and India*

Recent comparative studies reveal divergent philosophies of AI governance (Sharma & Sharma 2025; Zhao 2025). The four jurisdictions examined in this paper illustrate different relationships between innovation, individual rights, corporate power, and state authority. The comparison does not suggest that any single model completely resolves the ethical problems of algorithmic surveillance. Instead, it demonstrates how different regulatory priorities shape the protection of privacy and the governance of AI.

➤ *United States:*

A market-driven model emphasizing innovation and corporate autonomy, with fragmented state-level privacy laws. Federal initiatives such as the Blueprint for an AI Bill of Rights (White House, 2022) signal growing concern over algorithmic fairness. The United States therefore presents a governance environment in which technological development and market innovation occupy an important position, while privacy and algorithmic accountability may also be addressed through a combination of different legal and policy mechanisms. This fragmentation is significant because individuals may encounter different forms of protection depending on the applicable regulatory environment.

The American approach also demonstrates the tension between innovation and oversight. AI systems can develop rapidly in private markets, while regulatory responses may emerge through separate initiatives rather than one unified framework. From the perspective of algorithmic surveillance, this raises questions about corporate responsibility, transparency, and the ability of individuals to understand how behavioural information is collected and used. The Blueprint for an AI Bill of Rights reflects growing policy attention to issues such as automated-system fairness, although the paper's concern remains broader: whether legal and policy measures are sufficient to preserve autonomy and dignity in increasingly data-driven environments.

➤ *European Union:*

The EU AI Act (2024) and GDPR enforce rights-based accountability emphasizing human oversight and risk-based classification (Wang & Xie 2025). The European approach places greater emphasis on the protection of individual rights and on the responsibilities associated with high-risk AI systems. Human oversight and transparency are important because automated systems can have consequences beyond the immediate processing of data. The rights-based approach therefore treats AI governance as part of a broader framework of protecting individuals from harmful or unjustified uses of technology.

The European model is especially relevant to the argument of this paper because it demonstrates how privacy and AI regulation can be connected with broader ideas of accountability. Regulatory intervention does not simply concern whether information exists in a database; it also

concerns how automated systems operate and what risks they create. GDPR enforcement further demonstrates that regulatory principles require institutional mechanisms to have practical significance. The existence of legal standards is therefore only one part of effective privacy protection; enforcement and oversight remain equally important.

➤ *China:*

Adopts a state-centric model using AI for governance, surveillance, and economic planning, grounded in the Social Credit System and Data Security Law (2021). In this model, the relationship between AI and the state is particularly significant. Data and algorithmic systems can support administrative and governance objectives while also raising concerns about the extent of state surveillance and individual autonomy. The Chinese approach therefore illustrates how AI can become closely connected with public administration and state capacity.

The significance of this model for the present study lies in the question of power. When surveillance technologies are integrated into governance structures, the capacity to collect, process, and interpret information can become an important instrument of institutional authority. The ethical concern is not simply technological capability but the safeguards surrounding that capability. Questions of transparency, accountability, proportionality, and the individual's ability to challenge decisions become central to the protection of human dignity.

➤ *India:*

The Digital Personal Data Protection Act (2023) marks its first comprehensive privacy framework (Dhir & Verma 2024), though implementation challenges remain. India's position is particularly important because the country is experiencing rapid digitalization while developing its legal framework for personal data protection. The framework represents an important step toward recognizing the need for structured data governance, but the effectiveness of any legal framework depends on implementation, institutional capacity, awareness, and compliance.

The Indian context also highlights the gap that may exist between formal legal recognition and practical protection. As digital systems become more common in public and private life, citizens may not always have equal knowledge or bargaining power in relation to data collection. This makes transparency and digital literacy important complements to formal legal rights. The comparative analysis therefore treats India not merely as another regulatory model but as an example of the practical challenge of building privacy protection alongside expanding AI adoption.

IV. DATA AND FINDINGS

- **AI Adoption:** By 2024, 75 countries have formal AI strategies emphasizing ethical design (OECD AI Policy Observatory 2024). This indicates that AI governance has become a significant policy concern across jurisdictions. The increasing number of national

strategies also suggests that governments are attempting to address the social and ethical consequences of AI rather than treating it solely as an economic or technological issue.

- **Public Perception:** Pew Research (2023) reports 81 % of U.S. adults fear misuse of their data; WEF (2024) finds 68 % global distrust in AI transparency. These figures illustrate the gap between technological adoption and public confidence. Individuals may use AI-enabled services while simultaneously expressing concern about how their information is handled. This tension is relevant to the paper's central argument because privacy protection depends not only on the existence of technology but also on whether people can reasonably trust the institutions operating it.
- **Enforcement:** GDPR penalties exceeded €3.2 billion by mid-2024 (European Data Protection Board 2024). Enforcement activity demonstrates that privacy regulation can have consequences when institutions fail to meet regulatory requirements. At the same time, the existence of penalties does not by itself resolve the deeper ethical problem of algorithmic surveillance. Monetary enforcement addresses particular forms of non-compliance, whereas the broader issue concerns the continuing relationship between technology, power, autonomy, and human dignity.
- **State Surveillance:** Freedom House (2024) finds 25 of 70 countries increased biometric surveillance; China monitors 900 million citizens through facial-recognition infrastructure. These findings illustrate the growing importance of biometric and automated identification technologies within surveillance environments. Such technologies can expand the scale and speed at which individuals are identified and monitored. The ethical significance lies in the possibility that surveillance becomes routine and difficult for individuals to perceive or avoid.
- **India:** NASSCOM (2024) shows 52 % of citizens now aware of privacy rights, up from 44 % in 2023. The increase suggests growing public awareness of privacy issues in India. However, awareness alone does not guarantee effective control over personal information. Citizens also require understandable information, institutional accountability, and accessible mechanisms through which concerns can be raised and rights can be exercised.
- **Ethical Oversight:** OECD (2024) reveals only 40 % of government AI systems have independent ethics review boards. This finding is important because technological systems that influence public administration can affect individuals at a large scale. Independent ethical oversight can provide an institutional mechanism for identifying risks before or during deployment. The limited presence of such structures indicates that ethical governance remains an area requiring further development.

V. ETHICAL AND SOCIAL IMPLICATIONS

- **Autonomy Erosion** – Predictive analytics constrain free will. When algorithms predict preferences or likely behaviour and use those predictions to shape what individuals see or receive, the boundary between assistance and influence can become difficult to identify. The ethical issue is therefore not that every prediction removes freedom, but that repeated and opaque prediction can gradually shape the environment in which choices are made.
- **Bias Amplification** – Data-driven inequality persists. Algorithms can reproduce patterns present in historical or behavioural data. If those patterns contain social inequalities, automated processes may reinforce them while presenting the resulting decision as objective. This makes transparency and review necessary, particularly where algorithmic outputs affect access to opportunities, services, or institutional treatment.
- **Political Manipulation** – Algorithmic profiling endangers democracy. Political participation depends upon the ability of individuals to encounter information and form views without hidden manipulation. Profiling can make it possible to tailor messages to particular groups or individuals. The concern is therefore connected with the quality of democratic participation and the conditions under which citizens exercise political judgment.
- **Digital Inequality** – AI power centralizes among elites. Access to data, computing resources, technical expertise, and algorithmic infrastructure is not equally distributed. When a small number of institutions control large-scale data systems, the capacity to influence behaviour and make classifications may also become concentrated. Digital inequality can therefore deepen existing differences in social and economic power.
- **Psychological Impact** – Persistent monitoring induces anxiety and conformity. Awareness that behaviour may be continuously observed or assessed can affect how people communicate and act. The possibility of being profiled may encourage conformity and reduce the sense of private space necessary for experimentation, dissent, and individual development. These risks underscore the necessity of moral accountability in technological governance (Mahapatra 2025).

Taken together, these implications show why algorithmic surveillance cannot be examined only as a technical issue. A system may be accurate in processing information and still raise ethical concerns about the manner in which power is exercised. The central question is therefore whether technological efficiency is accompanied by meaningful respect for autonomy, equality, dignity, and accountability.

VI. DISCUSSION

Algorithmic surveillance constitutes a new decentralized regime of control. Unlike traditional surveillance, which may depend upon a visible institution or identifiable observer, algorithmic surveillance can be dispersed across platforms, databases, applications, and

institutional systems. This makes it harder for individuals to identify when surveillance begins, what information is being used, and how that information affects subsequent decisions.

While UNESCO's Recommendation on the Ethics of AI (2021) and OECD AI Principles (2023) stress fairness and explainability, enforcement gaps persist. The existence of principles and regulatory frameworks demonstrates growing international recognition of ethical AI, but the practical effect of such principles depends on implementation. A system may be formally governed by ethical standards while still leaving citizens without meaningful information about how automated decisions are produced or challenged.

The comparative analysis also shows that AI governance reflects broader political and institutional choices. A market-oriented approach may emphasize innovation and corporate autonomy; a rights-based approach may prioritize accountability and human oversight; a state-centric approach may place AI within broader governance and security structures; and an emerging framework such as India's may attempt to build comprehensive privacy protection while addressing implementation challenges. These differences should not be reduced to simple categories of success or failure. They demonstrate that the ethical governance of AI is closely connected with the distribution of power and responsibility.

Global convergence toward ethical AI demands institutionalized oversight, algorithmic transparency, and digital literacy programs that empower citizens (Kaya-Kasikci et al. 2025). Transparency should not be understood merely as publishing technical information that ordinary users cannot understand. Meaningful transparency requires information that allows affected individuals and institutions to understand the relevant purpose, risks, and accountability mechanisms of an AI system. Human oversight is similarly important because automated outputs should not automatically become unquestionable decisions.

Digital literacy is another important component of this approach. Individuals cannot meaningfully exercise privacy rights if they do not understand how data is collected, processed, or used. Public awareness can therefore complement legal protection by enabling citizens to make informed choices and recognize situations in which their privacy may be at risk. Institutional oversight, meanwhile, can provide a mechanism through which technological systems are assessed from an ethical perspective before their effects become widespread.

The discussion ultimately returns to the central proposition of the paper: privacy is not merely a legal entitlement concerning information. It is closely related to human dignity and autonomy. A society in which individuals are constantly predicted, classified, and influenced risks changing the meaning of personal freedom. Responsible AI governance must therefore preserve a space in which people remain subjects of rights rather than objects of data processing.

VII. CONCLUSION

Algorithmic surveillance is fundamentally an ethical dilemma. The rapid development of AI and big data has expanded the ability of governments, corporations, and institutions to observe, classify, predict, and influence human behaviour. The resulting challenges cannot be addressed solely through technological safeguards or narrow understandings of consent. Reimagining privacy as a moral right grounded in human dignity is essential to prevent AI from eroding liberty.

The comparative analysis of the United States, European Union, China, and India demonstrates that AI governance develops according to different institutional and political priorities. At the same time, the ethical concerns surrounding autonomy, bias, political manipulation, digital inequality, and psychological effects appear across these different environments. The presence of laws and policy frameworks is important, but their practical value depends upon implementation, transparency, independent oversight, accountability, and public awareness.

Smart societies must therefore embed transparency, justice, and autonomy within their digital infrastructures, ensuring AI serves humanity rather than governs it. The future of AI governance should not be measured only by how intelligent or efficient systems become, but also by whether individuals retain meaningful dignity, agency, and accountability within increasingly data-driven societies. Ethical governance requires institutions and citizens to remain capable of questioning technological power rather than accepting automated systems as inherently neutral or inevitable.

REFERENCES

- [1]. Deleuze, G. (1992). Postscript on the societies of control. October, 59, 3–7.
- [2]. Dhir, A., & Verma, S. (2024). India's Digital Personal Data Protection Act, 2023: Promise and implementation gaps. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [3]. Du, Y. (2025). Algorithmic governance and the reconfiguration of autonomy. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [4]. European Data Protection Board. (2024). Annual report 2024. <https://www.edpb.europa.eu>
- [5]. European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
- [6]. Foucault, M. (1977). Discipline and punish: The birth of the prison (A. Sheridan, Trans.). Pantheon Books.
- [7]. Freedom House. (2024). Freedom on the net 2024: The struggle for trust online. <https://freedomhouse.org/report/freedom-net/2024>
- [8]. Harari, Y. N. (2018). Homo Deus: A brief history of tomorrow. Harper Perennial.

- [9]. Kaya-Kasikci, N. et al. (2025). Institutionalizing ethical AI oversight: Transparency and digital literacy. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [10]. Mahapatra, S. (2025). Reframing privacy as a moral right in the age of algorithmic governance. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [11]. NASSCOM. (2024). Data privacy awareness in India: Annual survey findings. National Association of Software and Service Companies.
- [12]. OECD. (2023). OECD AI principles. OECD Publishing, <https://oecd.ai/en/ai-principles>
- [13]. OECD. (2024). OECD AI policy observatory. <https://oecd.ai>
- [14]. People's Republic of China. (2021). Data Security Law of the People's Republic of China.
- [15]. Pew Research Center. (2023, October 18). How Americans view data privacy. <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>
- [16]. Republic of India. (2023). The Digital Personal Data Protection Act, 2023.
- [17]. Sharma, R., & Sharma, S. (2025). Comparative philosophies of AI governance: A cross-national analysis. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [18]. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization.
- [19]. Wang, L., & Xie, Y. (2025). Rights-based accountability under the EU AI Act. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [20]. White House Office of Science and Technology Policy. (2022). Blueprint for an AI Bill of Rights: Making automated systems work for the American people.
- [21]. World Economic Forum. (2024). Global distrust in AI transparency: Survey findings.
- [22]. Zhao, X. (2025). China's state-centric model of AI governance and social control. [Author-year citation as used in the source paper — please verify exact journal/publisher details before final submission.]
- [23]. Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.