
SURVEILLANCE CAPITALISM AND HUMAN DIGNITY: EVALUATING THE ETHICAL AND LEGAL IMPLICATIONS OF BIOMETRIC DATA COLLECTION

Savita S Pattanshetti, Research Scholar, Department of Law, Mansarovar Global
University, Sehore, Madhya Pradesh

Tai Chourashiya, Associate Professor, Dean, Faculty of Law, Mansarovar Global
University, Sehore, Madhya Pradesh

ABSTRACT

The expansion of surveillance capitalism and biometric governance has transformed the relationship between technology, human autonomy, and democratic society. Digital platforms increasingly rely on the extraction and commodification of biometric and behavioral data through artificial intelligence, facial recognition systems, predictive algorithms, and surveillance infrastructures. Traditional privacy frameworks remain inadequate because they primarily address informational harms while failing to protect cognitive autonomy, psychological integrity, and human dignity. This paper argues that surveillance capitalism no longer merely invades privacy but actively shapes human behavior, emotions, and decision-making through algorithmic prediction and behavioral modification.

Drawing upon theories of surveillance capitalism, constitutional dignity, informational self-determination, and cognitive liberty, the study examines how biometric governance creates asymmetrical power between individuals, corporations, and the state. Using a doctrinal and comparative methodology, the paper analyzes legal and regulatory frameworks in India, the European Union, the United States, and China. It evaluates whether existing laws adequately address AI-driven behavioral governance and biometric surveillance. The paper proposes “Cognitive Sovereignty” as a legal framework to protect mental autonomy and behavioral independence, while advancing “Biometric Constitutionalism” as a model for safeguarding human dignity, democratic accountability, and constitutional values in increasingly algorithmic societies.

Keywords: Surveillance Capitalism, Cognitive Sovereignty, Biometric Governance, Human Dignity, Algorithmic Societies

Introduction

The twenty-first century has seen a remarkable change in the interplay between technology, governmentality, and human agency. In today's digital age, technology is dependent on the harvesting, processing, and commoditization of personal as well as biometric data via artificial intelligence techniques, predictive analysis, and surveillance apparatuses. As described by Shoshana Zuboff, this form of capitalism is referred to as "surveillance capitalism," in which human experience becomes data for commercial prediction and control purposes.¹ "The proliferation of such technological innovations as facial recognition, emotion AI, and biometric identification systems has raised concerns about privacy, democratic accountability, and human dignity".² In the current world of surveillance, people are not just monitored but predicted and influenced by way of behavior-modifying means.³

The greater embedding of biometric governance in the fabric of social and political activity has dramatically changed conventional notions of privacy and autonomy. The state and business have acquired unprecedented capabilities to track, classify, and exert control over individuals via massive data harvesting and predictive modeling.⁴ "The deployment of facial recognition systems by law enforcement agencies, tech companies, immigration services, and government bodies reveals how biometric features play an increasingly important role in contemporary governance arrangements".⁵ This poses a serious problem of constitutionality and ethics since biometric markers are inextricably tied to human identity and freedom from constant surveillance and classification.⁶ In contrast to regular personal data, biometric markers have unique, unalterable properties.

Current frameworks for privacy are, nevertheless, inadequate in solving these new problems. The current legal framework concentrates mostly on information privacy and data protection based on consent but fails to provide adequate control over the use of algorithms for influencing

¹ Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization," 3 *Organization Theory* 26317877221129290 (2022).

² "The ethical application of biometric facial recognition technology | AI & SOCIETY | Springer Nature Link," available at: <https://link.springer.com/article/10.1007/s00146-021-01199-9> (last visited May 22, 2026).

³ Yahya Alshamy et al., "Surveillance capitalism and the surveillance state: a comparative institutional analysis" *Constitutional Political Economy* (2024).

⁴ Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization," 3 *Organization Theory* 26317877221129290 (2022).

⁵ Marcus Smith and Seumas Miller, "The ethical application of biometric facial recognition technology," 37 *AI & SOCIETY* 167–75 (2022).

⁶ "A Taxonomy of Privacy - Intellectual Life @ PCL," available at: <https://repository.law.upenn.edu/Documents/Detail/a-taxonomy-of-privacy/153988> (last visited May 22, 2026).

people's choices, their emotional states, and political behavior.⁷ The modern artificial intelligence systems operate in the way of predictive behavioral analysis and influence people's decisions, emotions, and politics, without making people aware of what is happening.⁸ Therefore, surveillance capitalism becomes not just about invading privacy but rather about cognitive governance of human beings.

The objective of this paper is to show that the legal discourses need to go past the usual privacy safeguards into realizing the need for “cognitive sovereignty” as a new dimension of constitutionalism and human rights. “Cognitive sovereignty” may be viewed as the entitlement of people to have control over their mental processes, behavior, cognition, and feelings without any external algorithmic manipulations. The problem being examined in this study is how well the existing laws on privacy can ensure that human dignity and autonomy are respected in algorithmic societies. Also, does biometric surveillance pose any threat to democracy by means of asymmetrical information/behavioral power?

The major goals of this research include the exploration of the connection between surveillance capitalism and biometric governance, the analysis of the constitutional restrictions within current laws on privacy, and the development of cognitive sovereignty as a potential instrument for addressing the problem of algorithmic behavior regulation. Besides, the project includes the examination of biometric regulation in India, Europe, the US, and China. Research questions to be addressed within the paper include whether there is an adequate legislation in relation to privacy issues, the constitutional aspects of biometric surveillance, and the need to address cognitive autonomy. The research is based on the following assumptions: surveillance capitalism turns biometric data into tools of governance, and privacy rights are not sufficient for protecting human dignity and cognitive autonomy.

The research methodology employed in this work will be doctrinal and comparative, drawing upon the fields of constitutional law, human rights, data protection, and recent scholarship in surveillance capitalism and artificial intelligence ethics. This study will confine itself to the field of biometric surveillance technology, behavioral prediction algorithms, and the constitutional ramifications of AI governance. By addressing the issue of surveillance

⁷ Shoshana Zuboff, “Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization,” 3 *Organization Theory* 26317877221129290 (2022).

⁸ “A Taxonomy of Privacy - Intellectual Life @ PCL,” available at: <https://repository.law.upenn.edu/Documents/Detail/a-taxonomy-of-privacy/153988> (last visited May 22, 2026).

capitalism in the context of wider discussions on democracy, dignity, and autonomy, the paper hopes to make some contribution toward the development of a framework to safeguard cognitive liberty.

Surveillance Capitalism and Biometric Governance

The arrival of surveillance capitalism has altered the way digital economies and governing laws are structured. Shoshana Zuboff states that surveillance capitalism represents a new economic model in which the human experience is collected as a "raw commodity" to be transformed into behavioral data.⁹ Unlike traditional capitalism, which based itself on making and exchanging things like goods and services, surveillance capitalism is in effect putting a value on human behaviour by collecting, analysing and turning into money information about individuals.¹⁰ Surveillance capitalism uses a data-based architecture to track what individuals do, what they like or don't like, how they are feeling, and how they are going to behave to make predictions into the future.¹¹ As a result, the human experience is sold as a commodity within the world of algorithms that have the ability to predict and control what will happen next.

Zuboff identifies a number of significant features of this theory with the concept of "behavioral surplus" as its epiphany, which Becker describes as excessive behavioral data harvested from people in excess of what is necessary for service improvement.¹² Corporations like Google, Meta, Amazon, and other digital platforms amass an unprecedented amount of information via search histories, location tracking, browsing patterns, online communications, and biometrical identifiers.¹³ This is thus algorithmically processed by AI-ML systems to predict, nudge, and manipulate human behavior for commercial and political interests.¹⁴ Surveillance capitalism thus goes well beyond acts of surveillance into behavioral governance: a technique whereby predictive systems manipulate users' conduct through algorithmic interventions.

Biometric governance has emerged as one of the most prominent features in this idea of

⁹ Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization," 3 *Organization Theory* 26317877221129290 (2022).

¹⁰ "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School," *available at*: <https://www.hbs.edu/faculty/Pages/item.aspx?num=56791> (last visited May 22, 2026).

¹¹ *Ibid.*

¹² *Ibid.*

¹³ Yahya Alshamy et al., "Surveillance capitalism and the surveillance state: a comparative institutional analysis" *Constitutional Political Economy* (2024).

¹⁴ *Ibid.*

surveillance capitalism. Biometric technologies such as facial recognition systems, iris scans, gait recognition, voice analysis, and emotion AI enable the identification and categorization of individuals.¹⁵ Facial recognition technology advantages public surveillance infrastructures and private digital platforms by providing mass real-time monitoring and identification of individuals without any material consent.¹⁶ Visual AI creates a greater extent of surveillance by trying to determine emotional states, psychological tendencies, and behavioral vulnerabilities through facial expressions, voice patterns, and bodily movements.¹⁷ Such systems are ever so increasingly deployed within workplaces, educational institutions, law enforcement agencies, immigration series, and others, normalizing overt biometric surveillance as a way of life. Predictive algorithms have greatly enhanced the possibility of utilizing big data for governing society. By processing huge amounts of biometric and behavioral data, predictive analytic systems can identify behaviors, feelings and preferences for individuals before they are actually displayed.¹⁸ A fine example of this comes from recommendation algorithms which serve social media platforms, streaming services, and digital ads. These algorithms will present your data to you through content that's tailored specifically for you, changing the way in which you consume, see political views, and develop habits.¹⁹ Because of this; algorithms function not solely as technology that passively serves a purpose, but rather as mechanisms of modification.

It has become increasingly difficult to discern any differences between a nation-state that conducts surveillance versus the capitalistic surveillance that is conducted through surveillance capitalism. Whereas surveillance capitalism mostly uses the market to extract and commodify behavioral data, the state uses the same technologies to conduct government surveillance, policing, and social control.²⁰ When governmental and corporate surveillance have been able to merge; this has created an unprecedented way of managing people and governing them digitally. For example, China's social credit system is one of the largest examples of data-driven governance, using behavioral surveillance, biometric surveillance, and prediction to govern

¹⁵ "The ethical application of biometric facial recognition technology | AI & SOCIETY | Springer Nature Link," available at: <https://link.springer.com/article/10.1007/s00146-021-01199-9> (last visited May 22, 2026).

¹⁶ *Ibid.*

¹⁷ "Atlas of AI," available at: <https://yalebooks.yale.edu/book/9780300264630/atlas-of-ai/> (last visited May 22, 2026).

¹⁸ "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School," available at: <https://www.hbs.edu/faculty/Pages/item.aspx?num=56791> (last visited May 22, 2026).

¹⁹ *Ibid.*

²⁰ Yahya Alshamy et al., "Surveillance capitalism and the surveillance state: a comparative institutional analysis" *Constitutional Political Economy* (2024).

how people act socially and politically.²¹ Liberal democracies have utilized technologies to increase their surveillance abilities through biometric identification, predictive policing, and digital surveillance that claim to provide safety and government administered efficiency.²²

In contemporary digital society, the power of platforms has become one of the most important things about them. Big technology companies can decide what will be seen and what will not, and they influence the democratic process and the flows of information/ideas via their algorithms.²³ Social media platforms can decide how visible political content will be and what social interaction is allowed to take place and what information will be available via their recommendation systems that are opaque but designed to drive user behaviour and profit via collecting data.²⁴ This is often done by increasing the level of polarization, along with increasing the rate of disinformation, affecting people's thoughts and emotions, and increasing addiction behavior. Therefore; the use of algorithms to manipulate an individual's behavior through these platforms has now been structurally embedded in these platforms, which have now turned every single person into a constant object of predicting, trial and error and influencing.

The expansion of surveillance capitalism and biometric governance is evidence that technology does not just gather data anymore; rather; technology now has a hand in shaping human behavior and creating social realities. The merging together of biometric surveillance/measurement, predictive analytics, and modifying behavior as it relates to governing people now creates major threats to democracy, autonomy, and constitutional rights. As technological infrastructures continue to mediate how people will openly participate in the political process while impacting their emotional state, it will be extremely critical that we find a way to protect cognitive liberty and human dignity through our current constitutional discourse.²⁵

Human Dignity, Privacy and Cognitive Sovereignty

Privacy law development corresponds to the dynamic interplay between individuals,

²¹ "How will the vulnerable be protected from Covid? And other questions," *available at*: <https://www.bbc.com/news/world-asia-china-51176409> (last visited May 29, 2026).

²² "The ethical application of biometric facial recognition technology | AI & SOCIETY | Springer Nature Link," *available at*: <https://link.springer.com/article/10.1007/s00146-021-01199-9> (last visited May 22, 2026).

²³ Shoshana Zuboff, "Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization," 3 *Organization Theory* 26317877221129290 (2022).

²⁴ *Ibid.*

²⁵ "warren-brandeis,"

technology, and state authority. Privacy as it was originally conceived was defined as the right to be protected from the violation of one's body and the disclosure of one's personal information. The advent of new technologies like computerization, biometric surveillance devices, and AI has rendered the definition of the harm that results from the violation of individual privacy obsolete. Modern forms of surveillance can no longer be described simply as information-based but also involve the impairment of people's mental, emotional, and behavioral autonomy.²⁶

The theory of informational self-determination was born primarily through German constitutional law, especially from the Census Act Case of 1983 when the Federal Constitutional Court determined that it is one's right to control his/her own personal information's usage and release.²⁷ "Informational self-determination became a key element within modern data protection, such as within the European Union's General Data Protection Regulation".²⁸ Within such regulation, the notions of informed consent, "purpose limitation, data minimization, transparency, and accountability become essential to regulate how personal information is processed and collected".²⁹ However, despite being crucial measures that prevent unlawful data processing, these frameworks do not emphasize mental and cognitive privacy and freedom of thought.

The 'Constitution of India' has addressed the issue of privacy with dignity and has placed them as key concepts in addressing the protection of fundamental rights in Indian law. The 'Supreme Court found in Justice K.S. Puttaswamy v. Union of India that privacy is a right that is guaranteed under the Constitution, based on Articles 14, 19, and 21'.³⁰ Privacy involves the right of individuals to make their own decisions (decisional autonomy), protect their physical bodies (bodily integrity), determine how their own private information will be used (control of one's private information), and provide their individual dignity through privacy.³¹ Increasingly, however, the implementation of facial recognition, biometric identification systems, and predictive technology within government structures creates issues much larger than simply

²⁶ Daniel J. Solove, "A Taxonomy of Privacy," 154 *University of Pennsylvania Law Review* 477 (2006).

²⁷ "A landmark judgment turns 40: The German Census judgment of 1983. • EFDPO - European Federation of Data Protection Officers," available at: <https://www.efdpo.eu/a-landmark-judgment-turns-40-the-german-census-judgment-of-1983/> (last visited May 29, 2026).

²⁸ "Regulation - 2016/679 - EN - gdpr - EUR-Lex," available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (last visited May 29, 2026).

²⁹ *Ibid.*

³⁰ "Justice K.S. Puttaswamy (Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017," available at: <https://indiankanoon.org/doc/91938676/> (last visited May 29, 2026).

³¹ *Ibid.*

protecting personal data privacy and consent. Biometric identification systems will be able to determine the emotional state of the individual, make inferences about their psychological traits and ultimately affect future behavior or actions through algorithmic analysis.³² Therefore, privacy protections based solely on consent and data collection will not adequately account for the additional depths of privacy implications created by cognitive manipulation and behavioral governance based on the individual's use of biometrics.

In light of these changes, the notion of “cognitive sovereignty” appears as a crucial human rights and constitutional law principle. Cognitive sovereignty can be described as an individual's right to exercise autonomous control over their thoughts, emotions, behavioral actions, and other mental functions without any coercive influences through algorithms. As opposed to the right to informational privacy, cognitive sovereignty implies not only the control of one's information but the ability to preserve the psychological environment needed to maintain democratic practices and critical thinking skills.³³ It is based on the fact that advanced algorithmic systems pose serious dangers to human autonomy and constitutional democracy.

The importance of recognizing cognitive sovereignty for democratic values cannot be overestimated. Democratic regimes presuppose the presence of autonomous individuals who can think and act independently.³⁴ When algorithmic systems manage to alter the psychological environment of individuals, the process of democratic self-governance turns into an object for manipulation. The rise of surveillance capitalism poses a challenge to the constitutional principles of free society since people are deprived of the opportunity to engage in any kind of autonomous activity.

Comparative Legal Analysis and Regulatory Challenges

The regulatory frameworks surrounding the use of biometric surveillance technologies and artificial intelligence technologies are quite diverse among the countries. This variation stems from different approaches taken towards issues of privacy, security, and human rights. Europe can be seen as having taken the lead in regulating technology in a way that prioritizes human rights and freedoms. GDPR, for instance, identifies biometric information as a sensitive type

³² “The ethical application of biometric facial recognition technology | AI & SOCIETY | Springer Nature Link,” available at: <https://link.springer.com/article/10.1007/s00146-021-01199-9> (last visited May 22, 2026).

³³ “The Battle For Your Brain,” Nita Farahany available at: <https://www.nitafarahany.com/the-battle-for-your-brain> (last visited May 29, 2026).

³⁴ “Mill, On Liberty.”

of personal data that must be protected under certain criteria when processed.³⁵ In addition to GDPR, the new EU Artificial Intelligence Act also places considerable emphasis on the regulation of such AI applications as biometric identification through obligations around transparency, accountability, and human oversight.³⁶ It is also worth mentioning the restrictions placed by the EU Artificial Intelligence Act on remote biometric identification systems due to potential threats to individuals' rights.³⁷ Despite the apparent strengths of the European approach, some critics suggest that it still pays little attention to cognitive control and manipulation.³⁸

On the other hand, the US has a segmented and sectoral approach to its regulation of information. There is no overarching national data protection act like the GDPR, and the regulation of biometrics is mostly done through state laws and sectoral regulations.³⁹ For instance, while states like Illinois have introduced robust biometric privacy legislation through the Biometric Information Privacy Act (BIPA), the overall federal government's involvement is relatively weak. Big technology companies also have considerable freedom in the use of behavioural and biometric data, raising issues about surveillance capitalism, platform power, and algorithmic exploitation.⁴⁰ The lack of an overarching framework to govern AI systems is another area of concern.

China stands out in its approach since it is more focused on the implementation of comprehensive state-centered surveillance systems. Biometric identity systems, facial recognition technology, predictive policing techniques, and social credit systems have been embedded in governance systems for the purpose of social management and administrative

³⁵ "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC" (General Data Protection Regulation) (Text with EEA Relevance), OJ L, 2016, CXIX.

³⁶ "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU", (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA Relevance), 2024.

³⁷ *Ibid.*

³⁸ Orla Lynskey and Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press, Oxford, New York, 2015).

³⁹ Woodrow Hartzog and Daniel Solove, "Breached!: Why Data Security Law Fails and How to Improve It" *Books* (2022).

⁴⁰ "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School," available at: <https://www.hbs.edu/faculty/Pages/item.aspx?num=56791> (last visited May 22, 2026).

governance.⁴¹ While China has enacted the Personal Information Protection Law (PIPL), it still functions in a political setting where the interests of the state usually triumph over the individual's rights.⁴² The Chinese social credit system is a case in point as far as data-driven governance systems are concerned in that they may be used for behavioral manipulation, monitoring, and regulation.

India is placed in between the two extremes of the regulatory approach based on the principle of rights and technological advancement. DPDP Act is considered a major development towards ensuring data protection through principles concerning consent, data processing, and duties of a data fiduciary.⁴³ At the same time, DPDP Act grants exemptions in case of use by public authorities and does not impose any limitations on biometric surveillance and AI-based behavioral prediction.⁴⁴ With the increase in the number of identity management projects, facial recognition systems, and smart policing schemes, there are worries about surveillance and information imbalance.⁴⁵ Although the Indian Supreme Court has declared privacy a fundamental right, current laws do not provide a comprehensive solution to cognitive, affective, and algorithmic governance problems.⁴⁶

A comparative evaluation indicates that current regulatory regimes are more concerned about data privacy, consent, and informational privacy. While this is an important aspect, it does not go to the extent required to address the constitutional implications of behavioral predictions and psychological profiling. Dignity of the human being and autonomy of cognition are at stake not just because of data harvesting, but also because of technology that can manipulate and influence decisions. Thus, current regimes need a more comprehensive constitutional perspective that takes care of mental autonomy and democratic self-governance.

⁴¹ nathan, "Engineering global consent: The Chinese Communist Party's data-driven power expansion" *ASPI*, 2019 available at: <https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion/> (last visited May 29, 2026).

⁴² "Personal Information Protection Law of the People's Republic of China," *PIPL* available at: <https://personalinformationprotectionlaw.com/> (last visited May 29, 2026).

⁴³ "DPDP Act 2023 and DPDP Rules 2025: Compliance Guide | EY - India," available at: https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 (last visited May 29, 2026).

⁴⁴ *Ibid.*

⁴⁵ "#PrivacyofthePeople: The boom of facial recognition technology in private spaces," *Internet Freedom Foundation (IFF)*, 2022 available at: <https://internetfreedom.in/facial-recognitiontechnologyinprivatespaces/> (last visited May 29, 2026).

⁴⁶ "Justice K.S.Puttaswamy(Retd) And Anr. vs Union Of India And Ors. on 24 August, 2017," available at: <https://indiankanoon.org/doc/91938676/> (last visited May 29, 2026).

Towards Biometric Constitutionalism: Legal and Policy Recommendations

Because of the inadequacies of existing privacy regimes, there is a need for a better and more complete legal framework that would be able to cope with issues raised by biometric governance and surveillance capitalism. This essay suggests the introduction of “Cognitive Sovereignty,” as a new concept in constitutional and human rights law. Cognitive sovereignty entails the right to exercise self-governance over one’s thinking processes, emotions, beliefs, and decision making without any manipulative intervention by algorithms. In contrast to existing privacy, which is mainly concerned with information, cognitive sovereignty attempts to ensure conditions of autonomy and independent thinking.

The recognition of cognitive sovereignty calls for better biometric governance regimes. Laws need to provide explicit limits on the acquisition, retention, distribution, and use of biometric information especially when there is likelihood that it can be employed in predictive and behavioral analysis. The use of biometrics ought to be guided by necessity, proportionality, audit, and consent. Additionally, the law ought to give citizens rights to access, dispute, and delete any automated profile created using their biometrics.

Transparency in algorithm use ought to be an essential element in regulatory design too. Any AI system whose purpose is to influence decisions, recommendations, or behaviors of the user’s needs to provide details on how it works, what its objective is, and what impact it may have on the user. Transparency rules should apply to both recommendation engines, targeted advertising tools, and predictive algorithms irrespective of whether they are used by government or business.

There needs to be the concept of “right against cognitive manipulation” acknowledged as part of constitutional and human rights law. Specifically, such a right would prevent the use of AI systems designed to take advantage of psychological weaknesses, emotional reactions, and secret manipulation of decision-making processes. Restrictions would have to be placed on the use of micro-targeting in politics, emotion recognition tools, and behavioral modification mechanisms.

Real-time facial recognition tools must be subject to strict controls because of the significant impact they might have on privacy, free speech, and participatory democracy. Moreover, independent AI oversight agencies need to be created to monitor compliance, conduct

investigations into abuses, and analyze new risks related to emerging technology.

All these proposals constitute the core of “Biometric Constitutionalism,” which can serve as a way to integrate ideas about dignity, autonomy, accountability, and democracy into rules governing the use of biometric and AI systems. Biometric Constitutionalism acknowledges the reality that future challenges related to constitutionality will emerge from actions by private parties who develop technological infrastructure that can influence cognitive functions and human behavior rather than just from governmental actions.

Conclusion

The rapid proliferation of surveillance capitalism and biometric governance has significantly affected the connection between technology, autonomy, and democratic governance. As has been established above, modern surveillance operates beyond mere data collection and now functions via means such as predictive analysis, biometric identification, behavioral profiling, and algorithmic persuasion. Using the theoretical framework provided by concepts of surveillance capitalism and biometric governance, this paper demonstrates how human behavior itself becomes an economic resource due to the operation of digital economies based on data exploitation and prediction.

However, the paper shows that the current regulatory regime is insufficient when it comes to solving constitutional problems related to the use of artificial intelligence and biometric technologies. In particular, the EU, US, Chinese, and Indian approaches to regulating information security emphasize informational privacy, consent, and data processing. Although such measures are necessary, they do not provide adequate protection against the loss of mental autonomy, psychological integrity, and behavioral autonomy due to algorithmic persuasion. Thus, the threats posed by modern surveillance technologies are more cognitive than informational.

In conclusion, the present paper proposes that cognitive sovereignty be recognized as a novel constitutional and human right principle intended to secure citizens from any manipulation by algorithms. It can be achieved within the context of biometric constitutionalism, which can allow for the extension of core constitutional values like dignity, autonomy, accountability, and participation into new technological contexts. This is important because new threats to freedom will stem more often from invisible behavioral manipulation than coercion.

In summary, the fate of constitutional democracy in the future will rest not only in the securing of people's privacy but also in safeguarding their cognitive freedom and dignity from behavioral manipulation algorithms.