Digital Surveillance, Biometric Governance, and the Erosion of Informational Privacy: A Constitutional Law Perspective

1. Karim Abdelnour: Department of Public Law, Cairo University, Cairo, Egypt
2. Salma Benyoussef*: Department of Political Science, Hassan II University, Casablanca, Morocco
3. Thabo Maseko: School of Law, University of the Witwatersrand, Johannesburg, South Africa

*****Correspondence: e-mail: salma.benyoussef@uh2c.ma

Abstract

The rapid expansion of digital surveillance and biometric governance has fundamentally transformed the architecture of contemporary governance, reshaping the relationship between the state, the individual, and constitutional law. This article examines how emerging surveillance infrastructures—particularly those grounded in biometric technologies and algorithmic decision-making—challenge traditional constitutional doctrines of privacy, dignity, autonomy, and democratic accountability. Using a narrative review combined with descriptive-analytical methodology, the study traces the evolution of surveillance technologies from analog observation to predictive and biometric systems, and analyzes their institutional integration within modern governance frameworks. The findings demonstrate that biometric surveillance constitutes a new mode of constitutional power characterized by data-driven governance, algorithmic sovereignty, and the redefinition of individuals as data subjects rather than legal subjects. This transformation erodes informational privacy as a structural condition of constitutional democracy and weakens established safeguards of proportionality, due process, and judicial oversight. The article further identifies key structural risks associated with biometric governance, including function creep, irreversible data compromise, normalization of permanent identification, and deepening asymmetries of power and transparency. Through a comparative examination of jurisprudential trends and human rights frameworks, the study reveals persistent doctrinal inconsistencies and unresolved constitutional tensions surrounding surveillance practices. Finally, the article proposes a normative reconstruction of constitutional limits on biometric surveillance, emphasizing the need for substantive restrictions, strengthened procedural safeguards, robust institutional oversight, and democratic governance of surveillance infrastructures. The study concludes that safeguarding informational privacy in the digital age is not merely a regulatory challenge but a constitutional imperative essential for preserving democratic legitimacy, the rule of law, and human freedom in increasingly data-driven societies.

Keywords: Digital surveillance; Biometric governance; Informational privacy; Constitutional law; Algorithmic governance; Democratic accountability

Received: date: 15 August 2023
Revised: date: 09 September 2023
Accepted: date: 22 September 2023
Published: date: 01 October 2023

Citation: Abdelnour, K., Benyoussef, S., & Maseko, T. (2023). Digital Surveillance, Biometric Governance, and the Erosion of Informational Privacy: A Constitutional Law Perspective. *Legal Studies in Digital Age*, 2(4), 48-60.

1. Introduction

The transformation of governance in the digital age has fundamentally reconfigured the relationship between the state, the individual, and information. Contemporary governance no longer relies solely on territorial authority, institutional regulation, or legal coercion but increasingly operates through data infrastructures, algorithmic decision-making systems, and continuous information extraction from social life. Digital technologies have become integral to public administration, law enforcement, social welfare systems, migration control, and national security governance, producing what scholars describe as a datafied state in which political authority is exercised through computational processes and automated classification regimes (Fathaigh et al., 2021). This transformation has also blurred traditional boundaries between public and private power, as governmental agencies increasingly depend on digital platforms, data brokers, and corporate surveillance infrastructures to achieve regulatory objectives (Kumar, 2017). As governance becomes embedded in digital architectures, legal norms developed in earlier constitutional contexts face unprecedented pressure to adapt to the new realities of algorithmic governance, predictive regulation, and networked control.

Within this emerging configuration of digital governance, mass digital surveillance has become one of the defining institutional features of contemporary states. Surveillance practices are no longer limited to targeted investigations or exceptional security measures but now operate as permanent infrastructures of monitoring, data aggregation, and behavioral analysis. Modern surveillance systems encompass bulk collection of communications data, platform-based tracking, predictive analytics, and real-time behavioral profiling across vast populations (Murray & Fussey, 2019). Governments increasingly justify such practices through discourses of counterterrorism, public safety, public health, and administrative efficiency, especially in times of crisis such as the COVID-19 pandemic, when emergency surveillance architectures were rapidly deployed on a global scale (Bentotahewa et al., 2021). Yet the normalization of mass surveillance has produced deep structural consequences for constitutional governance, as the continuous monitoring of entire populations challenges foundational legal concepts of suspicion, proportionality, and individualized justification (Abdulrauf, 2018). Surveillance is no longer an exceptional instrument but an ordinary condition of governance, shaping the everyday experiences of citizens and redefining the scope of state power.

The rise of biometric governance marks a further intensification of this transformation. Biometric governance refers to the systematic deployment of biological and behavioral identifiers—such as facial recognition, fingerprints, iris scans, DNA profiles, voice recognition, and gait analysis—within governmental and commercial infrastructures of identification, verification, and control. Facial recognition technologies have been widely adopted in law enforcement, border management, and public security operations, raising complex legal concerns regarding accuracy, discrimination, and constitutional legitimacy (Chong & Kuek, 2022). Regulatory frameworks governing biometric systems remain fragmented and inconsistent across jurisdictions, with many legal systems struggling to define adequate safeguards against misuse and abuse (Yew & Xiang, 2022). Biometric governance transforms the human body itself into a continuous data source, rendering identity a computational object permanently embedded in digital infrastructures (Ferguson, 2019). Unlike conventional identifiers, biometric data cannot be meaningfully changed or revoked, creating unprecedented risks when such data is compromised or repurposed (Kozhanovich et al., 2023). As biometric systems become central to modern governance, constitutional law faces the challenge of regulating a form of power that operates through bodily inscription rather than traditional legal documentation.

These developments have profound implications for the concept of informational privacy. Informational privacy is no longer limited to secrecy or confidentiality but increasingly concerns control over the collection, processing, circulation, and repurposing of personal data within complex socio-technical systems. The erosion of privacy in contemporary surveillance societies reflects not merely individual loss but structural transformation in the conditions of autonomy, dignity, and democratic participation (Friedman, 2019). In control societies governed by continuous data flows, the distinction between public and private life becomes increasingly unstable, as personal information circulates across governmental agencies, corporate platforms, and transnational data networks (Melis, 2019). Informational privacy thus emerges as a foundational constitutional value linked to the preservation of individual self-determination, protection against arbitrary power, and maintenance of democratic pluralism (Weinberg, 2017). Yet the prevailing architecture of digital surveillance steadily undermines these normative foundations by constructing legal regimes that prioritize data extraction, efficiency, and security over individual rights.

At the core of contemporary constitutional debate lies the growing tension between state security imperatives and the protection of constitutional rights. Governments routinely invoke national security, crime prevention, and public order to justify expansive surveillance measures, often framing privacy protections as obstacles to effective governance (Ņesterova, 2019). The legal normalization of bulk data collection, predictive policing, and biometric monitoring reflects a gradual reconfiguration of constitutional balances, in which security rationales systematically displace traditional doctrines of proportionality, necessity, and due process (Talapina, 2021). Courts and legislatures struggle to reconcile the demands of modern security governance with enduring constitutional commitments to human dignity, liberty, and the rule of law (Ziemblicki, 2023). This conflict is further intensified by the rise of digital authoritarianism in various regions, where surveillance technologies are increasingly deployed to suppress dissent, manipulate public opinion, and consolidate political control (Ziani, 2020). Even within democratic systems, surveillance architectures often operate in conditions of limited transparency and weak accountability, raising fundamental concerns regarding constitutional legitimacy and democratic oversight (Balule & Dambe, 2023).

Despite the growing body of scholarship on surveillance, privacy, and data governance, significant gaps remain in existing legal analysis. Much of the current literature addresses specific technologies, regulatory frameworks, or regional legal developments without offering a comprehensive constitutional synthesis of how digital surveillance and biometric governance collectively reshape the structure of modern constitutionalism. Studies have examined the human rights implications of bulk surveillance (Murray & Fussey, 2019), the challenges posed by electronic surveillance in developing legal systems (Abdulrauf, 2018), and the ethical tensions surrounding AI surveillance architectures (Okonkwo, 2023), yet these analyses often remain fragmented across doctrinal, technological, and normative domains. Similarly, important work on surveillance capitalism and corporate data practices has illuminated the role of private actors in the surveillance ecosystem (McGuigan et al., 2023; Stucke, 2022), but has not fully integrated these insights into constitutional frameworks of public power. The absence of an integrated constitutional theory of biometric governance and digital surveillance leaves unresolved questions regarding the future of privacy, democratic accountability, and the legitimacy of contemporary governance structures.

The present study seeks to address these gaps by offering a comprehensive constitutional analysis of digital surveillance and biometric governance through the lens of informational privacy. The central objective of this research is to examine how emerging surveillance infrastructures challenge traditional constitutional doctrines and to propose normative pathways for preserving informational privacy in the digital age. The analytical framework adopted in this study draws upon comparative constitutional law, human rights theory, and socio-legal scholarship to explore the structural transformation of governance under conditions of pervasive data extraction. By situating technological developments within broader constitutional principles of dignity, autonomy, proportionality, and democratic governance, this article aims to contribute to the reconstruction of privacy as a core constitutional value in contemporary legal systems.

Methodologically, this research employs a narrative review combined with descriptive analysis. The narrative review approach allows for the systematic integration of interdisciplinary scholarship across constitutional law, surveillance studies, information ethics, and political theory, capturing the complexity of contemporary surveillance ecosystems (Draper, 2016). Descriptive analysis is used to map the evolution of surveillance technologies, regulatory frameworks, and institutional practices, providing a detailed account of how biometric governance operates in real-world contexts (Dule et al., 2020). This methodological design facilitates the identification of normative patterns, legal tensions, and emerging doctrinal challenges that cannot be adequately captured through purely empirical or doctrinal methods. The study draws upon international legal sources, regional jurisprudence, regulatory instruments, and scholarly analyses to construct a coherent constitutional narrative of the digital surveillance age.

The structure of the article reflects this analytical progression. Following the present introduction, the second section examines the technological and institutional architecture of digital surveillance and biometric governance, tracing their evolution and operational mechanisms. The third section develops the constitutional foundations of informational privacy and explores the normative conflicts generated by contemporary surveillance practices. The fourth section offers an in-depth constitutional analysis of biometric surveillance, identifying structural risks and proposing legal constraints necessary for democratic governance. The concluding section synthesizes the findings and outlines future directions for constitutional theory and legal reform in the age of pervasive digital surveillance. Through this structured inquiry, the article seeks to illuminate the profound constitutional transformations unfolding within the digital state and to advance a principled legal response to the erosion of informational privacy.

2. Architecture of Digital Surveillance and Biometric Governance

The architecture of digital surveillance and biometric governance reflects a profound transformation in the modalities through which power, control, and regulation are exercised in contemporary societies. Surveillance technologies have evolved from rudimentary analog instruments of observation into complex computational ecosystems capable of continuous, automated, and predictive monitoring. Early forms of surveillance relied on physical observation, wiretapping, and discrete data collection practices embedded within traditional law enforcement and intelligence operations. These mechanisms were limited in scale, constrained by human labor, and largely reactive in nature. By contrast, contemporary surveillance infrastructures operate through algorithmic systems that process vast quantities of data in real time, enabling authorities to monitor populations at unprecedented levels of granularity and speed (Fathaigh et al., 2021). This shift from analog surveillance to algorithmic monitoring has altered the temporal and spatial dimensions of governance, allowing continuous observation that transcends physical boundaries and jurisdictional constraints (Ziemblicki, 2023).

The emergence of big data infrastructures constitutes a central pillar of this transformation. Modern surveillance systems rely on massive data repositories that aggregate information from telecommunications networks, social media platforms, financial transactions, biometric systems, and Internet-of-Things devices. These infrastructures enable the integration of heterogeneous data streams into unified analytical environments capable of revealing complex behavioral patterns (McGuigan et al., 2023). Big data surveillance no longer focuses merely on what individuals have done but seeks to infer what they are likely to do in the future through predictive analytics (Murray & Fussey, 2019). Such predictive capabilities are increasingly used in policing, border control, credit assessment, and social risk management, thereby transforming governance into a forward-looking enterprise grounded in probabilistic modeling rather than retrospective adjudication (Okonkwo, 2023). The expansion of predictive analytics has generated new forms of risk governance in which algorithmic assessments guide policy interventions long before any legal wrongdoing has occurred (Talapina, 2021).

Artificial intelligence further intensifies these developments by enabling automated behavioral profiling across entire populations. Machine learning systems are deployed to classify individuals based on inferred traits, social affiliations, emotional states, and potential risks, often without the knowledge or consent of the individuals concerned (Koczur, 2022). These systems continuously refine their predictive models by learning from incoming data, producing feedback loops that deepen the reach and opacity of surveillance practices (Draper, 2016). AI-driven profiling systems are now used in criminal justice, employment screening, migration control, and financial regulation, creating a pervasive environment of algorithmic evaluation that reshapes social opportunities and constraints (Hewitt, 2023). The opacity of these systems complicates legal oversight and undermines procedural fairness, as affected individuals are often unable to challenge decisions made by automated systems whose internal logic remains inaccessible (Ingel et al., 2020).

Within this technological environment, biometric governance has emerged as a dominant regulatory paradigm. Biometric governance refers to the systematic integration of biometric identifiers into governance structures for the purposes of identification, authentication, verification, and control. Unlike traditional identity documents, biometric identifiers are inherently linked to the biological and behavioral characteristics of individuals, rendering identity a permanent and inescapable feature of the body itself (Ferguson, 2019). The scope of biometric governance now encompasses a wide array of technologies, including facial recognition systems deployed in public spaces (Chong & Kuek, 2022), iris and fingerprint scanners used in border control and civil registration systems (Kozhanovich et al., 2023), DNA databases maintained by law enforcement agencies (Talapina, 2021), voice recognition technologies embedded in digital platforms (Yew & Xiang, 2022), and gait analysis tools used for remote identification in urban surveillance networks (Ziemblicki, 2023). Each of these modalities extends the reach of governance into intimate domains of human existence, transforming the body into a continuous data interface with the state and market.

Biometric ecosystems are shaped by the complex interplay between state institutions and corporate actors. Governments rely on private technology firms to design, deploy, and maintain biometric infrastructures, while corporations depend on governmental demand and regulatory frameworks to expand their markets and legitimize their technologies (Kumar, 2017). This symbiotic relationship has produced hybrid governance structures in which public authority and private commercial interests become deeply entangled (Stucke, 2022). Technology companies collect biometric data through consumer devices, social media platforms, and smart infrastructure, while public agencies integrate these data streams into law enforcement, immigration control, and national security operations (McGuigan et al., 2023). The resulting ecosystem erodes traditional distinctions between public surveillance and private data extraction, creating a surveillance environment in which multiple actors exercise overlapping forms of informational power (Basimanyane, 2022).

At the core of biometric governance lie vast databases designed to store, process, and exchange biometric information across institutional and national boundaries. Interoperability between databases allows biometric data collected for one purpose to be repurposed for multiple forms of governance, often without renewed consent or adequate oversight (Dule et al., 2020). Cross-border data flows further complicate regulatory control, as biometric information is transferred across jurisdictions with divergent legal standards for privacy protection and data security (Ņesterova, 2019). International data-sharing agreements, security partnerships, and commercial contracts enable the global circulation of biometric data, creating transnational surveillance networks that escape the effective reach of domestic constitutional constraints (Murray & Fussey, 2019). The structural irreversibility of biometric data compromise amplifies these risks, as individuals cannot meaningfully change their biometric identifiers once such data is leaked, misused, or unlawfully accessed (Bentotahewa et al., 2021).

The institutionalization of surveillance power is anchored in the expanding authority of security agencies and intelligence architectures. Modern intelligence systems operate through integrated surveillance platforms that combine signals intelligence, cyber surveillance, biometric identification, and data analytics into unified operational frameworks (Abdulrauf, 2018). These institutions increasingly rely on continuous data ingestion and automated analysis to support decision-making processes, thereby shifting intelligence work from human judgment to computational governance (Okonkwo, 2023). Emergency legislation and national security doctrines have facilitated the rapid expansion of these capabilities, often in the absence of comprehensive parliamentary oversight or transparent judicial review (Balule & Dambe, 2023). As surveillance infrastructures become embedded within routine administrative functions, exceptional security measures gradually transform into ordinary governance practices (Ziani, 2020).

Public–private surveillance partnerships further entrench these dynamics. Governments procure surveillance technologies from private vendors, outsource data processing functions, and rely on corporate platforms for the collection and analysis of personal information (Fathaigh et al., 2021). These partnerships blur lines of accountability, as private actors operate beyond the reach of traditional constitutional constraints while exercising significant influence over public governance (Koczur, 2022). Technology firms profit from surveillance contracts while expanding their data holdings and market dominance, reinforcing economic incentives that favor the continued growth of surveillance infrastructures (Stucke, 2022). The commodification of surveillance transforms personal data into an asset class, embedding surveillance practices within broader structures of digital capitalism (Kumar, 2017).

Digital platforms, data brokers, and advertising networks constitute a parallel system of corporate surveillance capitalism that intersects with state surveillance in complex ways. Platforms collect detailed behavioral data on billions of users, constructing comprehensive profiles that are monetized through targeted advertising and algorithmic manipulation (Lingel, 2019). Data brokers aggregate and trade personal information across industries, creating opaque markets in which individual identities are continuously bought and sold (Smith & Shade, 2018). Governments increasingly access these commercial data reservoirs for law enforcement, intelligence, and regulatory purposes, effectively outsourcing surveillance functions to corporate ecosystems (McGuigan et al., 2023). This convergence of state and corporate surveillance power produces a pervasive environment of continuous monitoring that transcends formal legal boundaries and erodes traditional notions of constitutional limitation (Friedman, 2019).

Collectively, these technological and institutional developments constitute a new architecture of governance in which surveillance and biometric control are not merely tools of the state but foundational mechanisms of social organization. The resulting system operates through constant data extraction, algorithmic classification, and predictive intervention, reshaping the conditions under which constitutional rights are exercised and contested. This architecture establishes the structural context within which the erosion of informational privacy unfolds, setting the stage for the constitutional analysis developed in the subsequent sections of this article.

3. Informational Privacy and Constitutional Norms

Informational privacy has gradually emerged as a core constitutional value in modern legal systems, shaped by the historical evolution of political authority, technological change, and the normative foundations of human dignity. The conceptual genealogy of informational privacy is rooted in earlier liberal traditions that emphasized the protection of personal autonomy and the inviolability of the private sphere as essential conditions of human flourishing (Weinberg, 2017). As societies transitioned from industrial to information-based economies, privacy ceased to be merely a matter of physical seclusion and became increasingly concerned with the governance of personal data, identity, and self-presentation in digital environments (Draper, 2016). The proliferation of networked communication systems and automated data processing transformed privacy into a structural condition for democratic citizenship, as control over personal information became inseparable from the capacity to participate freely in social, political, and economic life (Friedman, 2019). In this context, informational privacy came to represent a normative commitment to protecting individuals from arbitrary informational power exercised by both states and corporate actors (Ņesterova, 2019).

The relationship between privacy, dignity, autonomy, and liberty lies at the heart of this constitutional transformation. Privacy safeguards the capacity of individuals to construct their identities free from constant surveillance and external coercion, thereby sustaining personal dignity and moral agency (Melis, 2019). Without privacy, autonomy becomes illusory, as individuals modify their behavior in response to perceived observation and judgment (Hewitt, 2023). Liberty, in turn, depends upon the existence of protected spaces within which individuals can think, communicate, associate, and dissent without fear of monitoring or retaliation (Talapina, 2021). These interrelated values form the normative foundation upon which constitutional privacy protections are built, transforming privacy from an individual preference into a collective constitutional good essential for democratic order (Ziemblicki, 2023). Informational privacy thus functions as a structural safeguard against the concentration of informational power that threatens to destabilize constitutional balances (Okonkwo, 2023).

Comparative constitutional jurisprudence increasingly reflects this expanded understanding of privacy. Courts and legislatures across multiple jurisdictions have recognized informational privacy as a fundamental right closely connected to human dignity and democratic participation (Kozhanovich et al., 2023). European legal systems, drawing on human rights traditions, have articulated robust protections for personal data and informational self-determination, particularly in response to mass surveillance practices (Ziemblicki, 2023). Emerging constitutional frameworks in Africa have likewise grappled with the tension between electronic surveillance and privacy rights in rapidly digitizing societies (Abdulrauf, 2018). Even in jurisdictions where privacy protections remain fragmented, courts have increasingly acknowledged the constitutional stakes of informational governance in the digital age (Talapina, 2021). This global convergence reflects a growing recognition that informational privacy is not merely a derivative interest but a foundational constitutional principle necessary for preserving the legitimacy of modern governance.

The doctrinal frameworks that operationalize these constitutional commitments have evolved to address the challenges posed by digital surveillance. The reasonable expectation of privacy doctrine has served as a primary analytical tool for determining the scope of privacy protection in various legal systems. Originally developed to protect individuals from unreasonable intrusions into private spaces, this doctrine now faces significant strain in environments where data is continuously generated, collected, and analyzed across public and private domains (Ferguson, 2019). In networked societies, individuals often have limited awareness of the extent to which their information is harvested and repurposed, undermining the assumption that voluntary disclosure eliminates reasonable privacy expectations (McGuigan et al., 2023). Scholars increasingly argue that privacy expectations must be recalibrated to account for structural power imbalances between individuals and data collectors rather than focusing narrowly on subjective expectations (Draper, 2016).

The principles of proportionality and necessity constitute additional doctrinal safeguards designed to constrain surveillance power. These principles require that any interference with privacy must pursue a legitimate aim, be suitable to achieve that aim, and represent the least intrusive means available (Talapina, 2021). In the context of mass digital surveillance, however, proportionality analysis becomes increasingly complex, as bulk data collection operates on speculative logics of risk rather than concrete suspicions (Murray & Fussey, 2019). The preventive orientation of contemporary surveillance practices challenges traditional legal assumptions that coercive state power should be exercised only in response to individualized wrongdoing (Ņesterova, 2019). Courts struggle to assess the necessity of surveillance systems whose benefits are often asserted in abstract security terms while their harms to privacy and democratic life remain diffuse yet profound (Ziemblicki, 2023).

Due process and procedural safeguards play a critical role in preserving constitutional accountability within surveillance regimes. These safeguards include requirements of legality, transparency, independent oversight, and effective remedies for individuals whose rights are violated (Balule & Dambe, 2023). Yet the secretive nature of intelligence operations and the technical complexity of surveillance systems frequently undermine these protections (Abdulrauf, 2018). Individuals often remain unaware that they are subject to surveillance and therefore lack meaningful opportunities to challenge unlawful data collection or misuse (Ingel et al., 2020). The opacity of algorithmic decision-making further weakens procedural justice, as affected persons cannot access the logic underlying automated classifications that shape their legal and social outcomes (Koczur, 2022). Without robust procedural guarantees, constitutional privacy protections risk becoming purely symbolic.

The chilling effects of surveillance represent one of the most significant threats to democratic participation. When individuals believe that their communications, movements, and associations are subject to continuous monitoring, they are likely to censor themselves, avoid controversial expression, and withdraw from political engagement (Friedman, 2019). Empirical and theoretical analyses demonstrate that pervasive surveillance alters behavior even in the absence of direct coercion, producing a climate of conformity incompatible with democratic pluralism (Hewitt, 2023). This chilling effect undermines the very conditions of free expression and open deliberation that constitutional democracies are designed to protect (Weinberg, 2017). The erosion of these conditions through surveillance infrastructures constitutes a structural constitutional injury rather than a series of isolated rights violations (Okonkwo, 2023).

These doctrinal and normative challenges crystallize in the broader constitutional tensions generated by contemporary surveillance regimes. The conflict between surveillance and freedom of expression is particularly acute, as monitoring practices discourage dissent, investigative journalism, and political mobilization (Talapina, 2021). Surveillance also conflicts with the presumption of innocence by subjecting individuals to continuous scrutiny based on predictive assessments rather than proven wrongdoing (Murray & Fussey, 2019). Algorithmic profiling and biometric identification exacerbate these tensions by embedding suspicion within automated governance systems that operate beyond meaningful human control (Ferguson, 2019).

Surveillance further threatens equality and non-discrimination, as predictive systems often reproduce existing social biases and disproportionately target marginalized communities (Okonkwo, 2023). Biometric technologies have been shown to exhibit differential accuracy across racial, gender, and age groups, compounding structural inequalities within legal and administrative systems (Yew & Xiang, 2022). Such discriminatory effects undermine the constitutional principle of equal protection and erode public trust in legal institutions (Kozhanovich et al., 2023). Finally, the expansion of surveillance infrastructures challenges democratic accountability by concentrating informational power within executive agencies and private corporations operating with limited transparency (Stucke, 2022). As surveillance becomes embedded within the ordinary functions of governance, traditional mechanisms of legislative oversight and judicial review struggle to keep pace with technological change (Ziemblicki, 2023). These cumulative tensions reveal the urgent need to reconceptualize informational privacy as a central pillar of constitutional order in the digital age.

4. Biometric Surveillance and the Erosion of Constitutional Privacy

Biometric surveillance represents a decisive transformation in the nature of constitutional power, marking the emergence of a new mode of governance in which authority is exercised through data-driven infrastructures and algorithmic decision-making systems. Traditional constitutional models presupposed a legal subject whose rights and obligations were defined through normative rules, judicial interpretation, and institutional procedures. Contemporary biometric governance, however, increasingly reconstitutes individuals as data subjects whose identities, behaviors, and risks are continuously assessed through computational systems (Kozhanovich et al., 2023). Data-driven governance operates through real-time data extraction and automated classification, enabling authorities to anticipate, influence, and regulate social behavior before legal norms are formally invoked (Okonkwo, 2023). This transformation produces what may be described as algorithmic sovereignty, a form of power in which political authority is exercised through technical infrastructures rather than through conventional legal commands (Fathaigh et al., 2021). Algorithmic sovereignty allows surveillance systems to shape legal outcomes, social opportunities, and political participation without transparent legal justification, thereby destabilizing foundational constitutional principles of accountability and rule of law (Ziemblicki, 2023).

Within this emerging order, the shift from legal subjects to data subjects constitutes a fundamental reconfiguration of constitutional relationships. In classical constitutional theory, the individual was recognized as a bearer of rights whose legal status constrained the exercise of state power. Under biometric governance, individuals are increasingly defined by data profiles that circulate across governmental and corporate networks (McGuigan et al., 2023). These profiles function as proxies for identity, determining access to public services, employment opportunities, credit markets, and political rights (Koczur, 2022). The legal subject becomes secondary to the data subject, as decisions affecting fundamental interests are driven by algorithmic assessments rather than individualized legal evaluation (Hewitt, 2023). This transformation erodes the normative foundation of constitutional protection by shifting the locus of power from law to code, from adjudication to automation (Draper, 2016). As biometric systems proliferate, the body itself becomes a site of governance, permanently inscribed within surveillance infrastructures (Ferguson, 2019).

The rise of preventive constitutionalism further amplifies these dynamics. Preventive constitutionalism reflects a governance model in which constitutional constraints are increasingly subordinated to anticipatory security logics (Talapina, 2021). Instead of responding to concrete violations through reactive adjudication, states now rely on biometric surveillance to predict and prevent potential risks (Murray & Fussey, 2019). This shift transforms constitutional law from a framework of rights protection into an instrument of risk management, allowing surveillance practices to expand on the basis of speculative threats rather than demonstrated necessity (Ņesterova, 2019). Judicial institutions struggle to review such practices, as the predictive logic of surveillance systems resists traditional evidentiary standards and procedural scrutiny (Abdulrauf, 2018). Preventive constitutionalism thus creates a structural imbalance in which security rationales systematically override privacy and due process protections.

The structural risks of biometric surveillance compound these constitutional challenges. Function creep, whereby data collected for one purpose is gradually repurposed for additional objectives, represents one of the most pervasive dangers of biometric governance (Dule et al., 2020). Biometric databases established for border control, public health, or civil registration are routinely accessed by law enforcement, intelligence agencies, and private actors, often without renewed consent or legislative authorization (Basimanyane, 2022). Mission expansion transforms limited surveillance programs into comprehensive monitoring infrastructures, undermining the original legal justifications for data collection (Balule & Dambe, 2023). The interconnectedness of digital systems accelerates this process, as interoperable databases enable seamless data sharing across institutional and national boundaries (Murray & Fussey, 2019).

The irreversibility of biometric data compromise constitutes a further constitutional risk. Unlike passwords or identity documents, biometric identifiers cannot be meaningfully changed once exposed (Bentotahewa et al., 2021). Data breaches, unauthorized access, and misuse therefore produce permanent vulnerabilities that individuals must endure throughout their lives (Yew & Xiang, 2022). This irreversibility amplifies the power asymmetry between data collectors and data subjects, as individuals bear the long-term consequences of systemic failures over which they exercise little control (Friedman, 2019). The constitutional implications are profound, as the state's duty to protect fundamental rights becomes increasingly difficult to fulfill in the face of permanent biometric exposure (Ziemblicki, 2023).

Biometric surveillance also normalizes permanent identification as a condition of social participation. In surveillance societies, individuals are increasingly required to submit to biometric verification in order to access public spaces, social services, financial systems, and digital platforms (Chong & Kuek, 2022). This normalization erodes the presumption of anonymity that historically protected individuals from constant scrutiny (Melis, 2019). As biometric identification becomes routine, the boundary between lawful governance and continuous monitoring dissolves, transforming constitutional rights into conditional privileges contingent upon biometric compliance (Hewitt, 2023). The cumulative effect is the construction of a society in which surveillance is no longer an exceptional measure but an ordinary precondition of citizenship (Ziani, 2020).

Asymmetries of power and transparency deficits further undermine constitutional accountability. Surveillance infrastructures are typically controlled by executive agencies and private corporations operating within opaque technical and legal environments (Stucke, 2022). Individuals lack meaningful access to information regarding how their biometric data is collected, processed, shared, and retained (Ingel et al., 2020). Oversight mechanisms are often fragmented and under-resourced, limiting their capacity to scrutinize complex technological systems (Abdulrauf, 2018). This structural opacity weakens democratic control and enables the entrenchment of surveillance power beyond effective constitutional constraint (Okonkwo, 2023).

Judicial responses to these challenges reveal a landscape of conflicting doctrines and unresolved tensions. Constitutional courts in various jurisdictions have struggled to reconcile traditional privacy doctrines with the realities of biometric surveillance (Ziemblicki, 2023). Some courts have emphasized the centrality of human dignity and proportionality in restricting surveillance practices (Talapina, 2021), while others have deferred to executive claims of national security and administrative necessity (Ņesterova, 2019). Regional human rights frameworks likewise reflect divergent approaches, with some institutions articulating robust data protection standards and others prioritizing state security interests (Murray & Fussey, 2019). These inconsistencies undermine legal certainty and weaken the protective capacity of constitutional law in the face of rapidly expanding surveillance infrastructures (Balule & Dambe, 2023).

Reconstructing constitutional limits on biometric surveillance therefore requires a comprehensive normative response. Substantive limitations must restrict the scope, purpose, and duration of biometric data collection, ensuring that surveillance practices remain strictly necessary and proportionate to legitimate aims (Kozhanovich et al., 2023). Procedural safeguards must guarantee transparency, independent oversight, and effective remedies for individuals whose rights are violated (Ziemblicki, 2023). Institutional oversight models should integrate judicial review, legislative scrutiny, and specialized regulatory authorities capable of evaluating complex technological systems (Abdulrauf, 2018). Finally, democratic governance of surveillance infrastructures must be strengthened through public participation, accountability mechanisms, and normative frameworks that reaffirm informational privacy as a core constitutional value (Weinberg, 2017). Only through such comprehensive constitutional reconstruction can legal systems respond effectively to the profound challenges posed by biometric surveillance and preserve the integrity of constitutional privacy in the digital age.

5. Conclusion

The expansion of digital surveillance and biometric governance represents one of the most consequential transformations of constitutional order in the modern era. This study has demonstrated that contemporary systems of data-driven control are not merely technological developments but structural reconfigurations of political authority, legal subjectivity, and democratic governance. Surveillance infrastructures now operate as permanent features of public administration, security management, and social regulation, embedding algorithmic decision-making and biometric identification at the core of governance itself. As a result, constitutional law confronts a new environment in which power is exercised continuously, invisibly, and often beyond the reach of traditional legal constraints.

At the heart of this transformation lies the erosion of informational privacy as a foundational constitutional value. Informational privacy is no longer simply a personal interest in secrecy but a structural condition for autonomy, dignity, liberty, and democratic participation. The conversion of individuals into data subjects whose identities are continuously monitored, profiled, and evaluated undermines the normative foundations of constitutional protection. The constitutional subject, once protected through rights, procedures, and judicial review, is increasingly governed through predictive models, biometric systems, and automated classifications that operate outside conventional legal processes. This shift weakens the capacity of constitutional law to perform its core function of restraining power and protecting individual freedom.

The analysis further revealed that biometric surveillance intensifies these challenges by transforming the human body into a permanent interface of governance. The irreversibility of biometric data compromise, the normalization of constant identification, and the expansion of interoperable surveillance databases create conditions of enduring vulnerability for individuals. These developments entrench asymmetries of power between governing institutions and citizens, while simultaneously reducing transparency and accountability. Surveillance becomes not a temporary instrument but a permanent condition of social life, fundamentally altering the relationship between the state and the individual.

Constitutional doctrines developed in earlier technological contexts now struggle to contain these emerging forms of power. Traditional frameworks of privacy, proportionality, due process, and judicial oversight remain essential but insufficient when confronted with automated governance systems that operate through speed, scale, and complexity beyond the capacities of existing institutions. Preventive constitutionalism, driven by security rationales and risk management logics, increasingly displaces reactive adjudication and individualized justification. This shift threatens to convert constitutional law from a shield protecting rights into a tool facilitating governance efficiency and security administration.

The jurisprudential landscape reflects deep uncertainty and fragmentation. Courts and regulatory bodies across jurisdictions articulate competing principles, oscillating between the protection of human dignity and deference to executive authority. The absence of coherent constitutional doctrine in relation to biometric governance produces legal instability and undermines public trust. Without a unified normative framework capable of addressing the realities of algorithmic governance, constitutional protections risk becoming symbolic rather than substantive.

Yet the erosion of constitutional privacy is neither inevitable nor irreversible. This study argues that the preservation of constitutional order in the digital age requires a fundamental reorientation of legal thinking. Informational privacy must be reconceptualized as a core structural principle of constitutional democracy rather than as an ancillary individual right. Substantive limits on biometric surveillance must be clearly articulated, restricting the purposes, scope, and duration of data collection. Procedural safeguards must be strengthened to ensure transparency, independent oversight, and effective remedies. Institutional designs must evolve to equip courts, legislatures, and regulatory authorities with the technical competence and democratic legitimacy necessary to govern complex surveillance infrastructures.

Most importantly, the governance of surveillance technologies must itself become a subject of democratic deliberation. The architecture of digital surveillance shapes social relations, political participation, and the distribution of power. Decisions regarding its design and deployment therefore belong at the center of constitutional politics rather than at the margins of administrative regulation. Democratic societies must reclaim control over the technological systems that increasingly define their political futures.

In conclusion, biometric surveillance poses a profound challenge to constitutional law, not because it introduces new tools of governance, but because it transforms the very logic through which power is exercised. If constitutionalism is to remain a meaningful constraint on authority in the digital age, it must adapt to this new reality by reaffirming informational privacy as a cornerstone of democratic life and by reconstructing legal institutions capable of governing technological power. The future of constitutional democracy depends upon whether law can evolve fast enough to protect human freedom in a world where governance is increasingly written in data and enforced through algorithms.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Abdulrauf, L. A. (2018). The Challenges for the Rule of Law Posed by the Increasing Use of Electronic Surveillance in Sub-Saharan Africa. *African Human Rights Law Journal*, *18*(1). https://doi.org/10.17159/1996-2096/2018/v18n1a17

Balule, B. T., & Dambe, B. J. (2023). Surveillance Within the Law: A Critique of the Legal Framework for Surveillance of Digital Communications by Law Enforcement Authorities in Botswana. *Statute Law Review*, *44*(2). https://doi.org/10.1093/slr/hmad003

Basimanyane, D. (2022). The Regulatory Dilemma on Mass Communications Surveillance and the Digital Right to Privacy in Africa: The Case of South Africa. *African Journal of International and Comparative Law*, *30*(3), 361-382. https://doi.org/10.3366/ajicl.2022.0414

Bentotahewa, V., Hewage, C., & Williams, J. (2021). Solutions to Big Data Privacy and Security Challenges Associated With COVID-19 Surveillance Systems. *Frontiers in Big Data*, *4*. https://doi.org/10.3389/fdata.2021.645204

Chong, S. Z., & Kuek, C. Y. (2022). Facial Recognition Technology in Malaysia: Concerns and Legal Issues. 101-109. https://doi.org/10.2991/978-2-494069-59-6_10

Draper, N. A. (2016). From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates. *Policy & Internet*, *9*(2), 232-251. https://doi.org/10.1002/poi3.142

Dule, C. S., Rajasekharaiah, K. M., & Prashanth, B. (2020). Analyze the Legislative Frameworkrelating to Surveillance and Right to Privacy: Issues and Challenges. *Iop Conference Series Materials Science and Engineering*, *981*(2), 022063. https://doi.org/10.1088/1757-899x/981/2/022063

Fathaigh, R. Ó., Möller, J., & Bellanova, R. (2021). Digital Platforms and the Digitisation of Government Surveillance. *Aoir Selected Papers of Internet Research*. https://doi.org/10.5210/spir.v2021i0.12220

Ferguson, A. G. (2019). Facial Recognition and the Fourth Amendment. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3473423

Friedman, L. M. (2019). Remnants of Information Privacy in the Modern Surveillance State. https://doi.org/10.31228/osf.io/acrkq

Hewitt, B. (2023). Panoptic Employment. *Science and Technology Law Review*, *24*(2), 349-378. https://doi.org/10.52214/stlr.v24i2.11631

Ingel, S., Richards-Karamarkovich, A., Bietsch, S., & Rudes, D. S. (2020). Privacy Violations and Procedural Justice in the United States Prisons and Jails. *Sociology Compass*, *15*(2). https://doi.org/10.1111/soc4.12847

Koczur, S. (2022). Pirates of Privacy: How Companies Profit Off Your Personal Data by Using Capital Surveillance Methods in Criminal Prosecution. *Journal of Science Policy & Governance*, *21*(01). https://doi.org/10.38126/jspg210106

Kozhanovich, Z. S., Aitchanovna, A. G., & Borisovna, D. O. (2023). Protection of Personal Data in the Era of Digitalization: Constitutional and Legal Aspect. *Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan*, *3*(74), 68-76. https://doi.org/10.52026/2788-5291_2023_74_3_68

Kumar, P. (2017). Corporate Privacy Policy Changes During PRISM and the Rise of Surveillance Capitalism. *Media and Communication*, *5*(1), 63-75. https://doi.org/10.17645/mac.v5i1.813

Lingel, J. (2019). Notes From the Web That Was: The Platform Politics of Craigslist. *Surveillance & Society*, *17*(1/2), 21-26. https://doi.org/10.24908/ss.v17i1/2.12939

McGuigan, L., West, S. M., Sivan-Sevilla, I., & Parham, P. (2023). The After Party: Cynical Resignation in Adtech's Pivot to Privacy. *Big Data & Society*, *10*(2). https://doi.org/10.1177/20539517231203665

Melis, R. (2019). Anonymity Versus Privacy in a Control Society. *Journal of Critical Library and Information Studies*, *2*(2). https://doi.org/10.24242/jclis.v2i2.75

Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, *52*(1), 31-60. https://doi.org/10.1017/s0021223718000304

Ṇesterova, I. (2019). The Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security. 109-126. https://doi.org/10.1093/oso/9780198849667.003.0008

Okonkwo, O. A. (2023). Ethical Tensions Between AI Surveillance Architectures, Human Rights Preservation, and the Universal Entitlement to Digital Privacy and Dignity. *Magna Scientia Advanced Research and Reviews*, *9*(2), 222-238. https://doi.org/10.30574/msarr.2023.9.2.0179

Smith, K. L., & Shade, L. R. (2018). Children’s Digital Playgrounds as Data Assemblages: Problematics of Privacy, Personalization, and Promotional Culture. *Big Data & Society*, *5*(2). https://doi.org/10.1177/2053951718805214

Stucke, M. E. (2022). Responding to Potential Criticisms to a Ban on Surveillance Capitalism. 213-245. https://doi.org/10.1093/oso/9780197617601.003.0010

Talapina, E. (2021). Surveillance and Human Rights: New Risks in the Digital Age. *Sravnitel Noe Konstitucionnoe Obozrenie*, *30*(6), 123-136. https://doi.org/10.21128/1812-7126-2021-6-123-136

Weinberg, L. (2017). Rethinking Privacy: A Feminist Approach to Privacy Rights After Snowden. *Westminster Papers in Communication and Culture*, *12*(3). https://doi.org/10.16997/wpcc.258

Yew, R.-J., & Xiang, A. (2022). Regulating Facial Processing Technologies: Tensions Between Legal and Technical Considerations in the Application of Illinois BIPA. https://doi.org/10.48550/arxiv.2205.07299

Ziani, O. (2020). The Rise of Digital Authoritarianism in the Time of Covid-19: The Case of North Africa. *Rowaq Arabi - رواق عربي*, ٢٥(4). https://doi.org/10.53833/kcwb1783

Ziemblicki, B. (2023). Modern Technologies as a Challenge for the Right to Privacy Under the European Convention on Human Rights. *International Community Law Review*, *25*(6), 589-604. https://doi.org/10.1163/18719732-bja10116