

Research Monograph

On

**“Surveillance, Freedom of Expression, and Human Rights in the
Digital Age: A Bangladesh Perspective”**

This research monograph submitted in partial fulfillment of the requirements for the
degree of Master of Laws (LL.M.)

In

LL.M. (Master of Laws)

Department of Law

Sonargaon University (SU), Dhaka.

Supervised By:

Muhammad Ali

Lecturer & Coordinator

Department of Law

Sonargaon University (SU), Dhaka

Submitted By:

Real Banik

ID No: LLM2502033019

Department of Law

Sonargaon University (SU), Dhaka

Date of Submission: 2026-06-25

Letter of Transmittal

To

Muhammad Ali

Lecturer & Coordinator

Department of Law

Sonargaon University (SU)

Dhaka, Bangladesh

Subject: Submission of Research Monograph on “Surveillance, Freedom of Expression, and Human Rights in the Digital Age: A Bangladesh Perspective”

Dear Sir,

I am pleased to submit my thesis entitled “Surveillance, Freedom of Expression, and Human Rights in the Digital Age: A Bangladesh Perspective” in partial fulfillment of the requirements for the LL.M. program at Sonargaon University.

This work reflects my sincere effort to analyze the challenges posed by state surveillance to constitutional rights and human freedoms in Bangladesh. I am grateful for your guidance and support throughout this research.

Respectfully submitted,

Real Banik

ID No: LLM 2502033019

Program: LL.M. (1 year)

Department of Law

Sonargaon University (SU)

Supervisor's Certificate

This is to certify that this research monograph entitled “**Surveillance, Freedom of Expression, and Human Rights in the Digital Age: A Bangladesh Perspective**” has been prepared by **Real Banik** in partial fulfillment of the requirements for the LL.M (Master's) degree at Sonargaon University (SU), Dhaka. The research work has been carried out under my supervision and represents a bona fide record of original work completed successfully.

I further certify that the content and presentation of this Thesis are original and suitable for submission toward the fulfillment of the LL.M (Master's) program requirements.

Muhammad Ali

Lecturer & Coordinator

Department of Law

Sonargaon University (SU)

Declaration

I hereby declare that this research monograph, entitled “**Surveillance, Freedom of Expression, and Human Rights in the Digital Age: A Bangladesh Perspective,**” has been prepared solely by me and submitted to the Department of Law, Sonargaon University (SU), in partial fulfillment of the requirements for the LL.M. Master's degree. This work is entirely original, and no part of it has been submitted to any other university or institution for the award of a degree, diploma, or any similar qualification.

Real Banik

ID No: LLM 2502033019

Program: LL.M. (1 year)

Department of Law

Sonargaon University (SU)

Acknowledgement

With a mind of deep gratitude and compassion, I extend my sincere appreciation to all who have guided and supported me in completing this Research Monograph entitled **“Surveillance, Freedom of Expression, and Human Rights in the Digital Age: A Bangladesh Perspective”**.

First and foremost, I am profoundly thankful to my supervisor, Muhammad Ali, Lecturer & Coordinator, Department of Law, Sonargaon University (SU), Dhaka, whose generous guidance, patience, and insightful mentorship shaped the direction and depth of this study.

I am equally indebted to my teachers and peers, whose encouragement fostered a nurturing environment for inquiry and growth. To the women whose voices and experiences inspired this research your resilience and strength are the true foundation of this work.

I also wish to express heartfelt gratitude to my classmates, family, and friends for their unwavering support and kind presence throughout this academic journey. Your compassion provided balance during moments of challenge.

Finally, I dedicate this work to all those striving for justice and equality in Bangladesh and beyond. May this research contribute, in a modest way, to the ongoing struggle for the realization of fundamental rights and Human Dignity.

Thank you

Real Banik

ABSTRACT

This paper examines the tension between the state's security-driven cyber legislation and the protection of fundamental human rights within Bangladesh's rapidly digitizing society. It specifically scrutinizes how legislative frameworks, such as the Digital Security Act 2018, often prioritize state-led surveillance agendas at the expense of investigative journalism and individual privacy. Through an analysis of legal frameworks and rights-based literature, this study argues that such mechanisms facilitate systemic abuses, including the erosion of digital assembly and unauthorized data monitoring. Furthermore, the centralization of executive power has increasingly marginalized civil society, creating a climate where digital oversight serves as a primary tool for silencing political dissent and restricting fundamental freedoms. This regulatory environment mirrors broader regional trends, where state-led digital infrastructure initiatives are increasingly utilized to embed a politics of fear and preemptively neutralize critical discourse. By weaponizing ambiguous legal frameworks like the Cyber Security Ordinance, the state effectively bypasses constitutional safeguards, transforming the digital landscape into a space characterized by self-censorship rather than public deliberation. This trajectory necessitates a re-evaluation of the current legislative trajectory to ensure that the pursuit of national security does not permanently stifle the digital exercise of democratic rights. In particular, the enactment of the Cyber Security Act 2023 and the subsequent 2025 ordinance highlight a continued shift toward restrictive governance that complicates the realization of international human rights obligations within the nation's evolving digital infrastructure.

Table of Contents

1	Chapter 1: Introduction	1
1.1	Background: Global rise of surveillance and Bangladesh's digital transformation. ..	1
1.2	Problem Statement: Conflict between state security and freedom of expression. ..	3
1.3	Objectives: Examine constitutional guarantees, statutory laws, and human rights implications.....	4
1.4	Research Questions:	5
1.5	Research Methodology:.....	6
1.6	Literature Review:.....	7
1.7	Scope & Limitations: Bangladesh focus with selective global comparisons.....	9
2	Chapter 2: Conceptual Framework.....	11
2.1	Defining Surveillance: State vs. corporate surveillance.....	11
2.2	Freedom of Expression: Constitutional guarantees (Articles 39 & 43).....	12
2.3	Human Rights in Digital Age: ICCPR, UDHR, regional instruments.	13
2.4	Theoretical Lens: Security vs. liberty; postcolonial critiques.....	14
3	Chapter 3: Legal Framework in Bangladesh	17
3.1	Constitutional Provisions: Freedom of speech, privacy, press.	17
3.2	Statutory Laws: ICT Act, Digital Security Act, Telecommunication Act.	19
3.3	Judicial Interpretation: Supreme Court rulings on privacy/expression.	20
3.4	Policy Documents: National ICT Policy, Cybersecurity strategies.....	21
4	Chapter 4: Comparative Perspectives.....	23
4.1	India: Surveillance under IT Act and Aadhaar debates.....	23
4.2	EU: GDPR and privacy safeguards.....	24
4.3	USA: Patriot Act and free speech challenges.....	25
4.4	Regional Context: South Asian surveillance trends.	26
4.5	Lessons for Bangladesh: Balancing national security with rights.	27
5	Chapter 5: Case Studies in Bangladesh.....	29
5.1	Rohingya crisis and surveillance	29

5.2	Media regulation and censorship.	30
5.3	Digital activism and state monitoring.	31
5.4	Corporate surveillance: Telecom and social media platforms.	32
5.5	Implications for journalists, activists, and marginalized groups.	33
6	Chapter 6: Human Rights Implications & Reform Proposals	35
6.1	Impact on freedom of expression.	35
6.2	Chilling effect on journalism and activism.	36
6.3	Privacy vs. security debates.	36
6.4	Gendered and marginalized perspectives.	37
6.5	Reform Proposals:.....	38
7	Chapter 7: Conclusion	41
	Bibliography	43

1 Chapter 1: Introduction

1.1 Background: Global rise of surveillance and Bangladesh's digital transformation.

The proliferation of mobile connectivity and internet access has fundamentally altered civic participation, yet this shift has coincided with the enactment of stringent regulatory measures such as the Digital Security Act and the subsequent Cyber Security Act (Anupam Gope, 2026)¹. These legislative frameworks have increasingly come under scrutiny for their broad provisions, which critics argue prioritize governmental authority over individual liberties. This research investigates the implications of these policies on the democratic landscape, specifically analyzing how the erosion of anonymity and the potential for state-led monitoring constrain the exercise of freedom of expression and public assembly (Dr. Abdullah-Al-Monzur Hussain, 2024).² By evaluating the operational impact of these laws against the International Covenant on Civil and Political Rights, this analysis highlights the critical need for regulatory transparency that aligns with international human rights standards (Shams., 2024)³. Furthermore, this study addresses the inherent risks of algorithmic oversight and data-driven profiling, which threaten to stifle dissent and marginalize vulnerable groups within the digital public sphere. Beyond these structural concerns, the integration of artificial intelligence into state surveillance apparatuses introduces significant ethical challenges regarding discrimination and the potential for automated censorship (Islam., 2023)⁴. The consolidation of these technological capabilities facilitates the emergence of a "Dual State," where the rhetoric of national development serves as a facade for the

¹ Gope, A. (2026). *Evolving Cyber Governance and Human Rights in Bangladesh: From the Digital Security Act to the Cyber Security Ordinance, 2025*. Zenodo (CERN European Organization for Nuclear Research)

² Hussain, A. (2024). *Rethinking Human Rights in Digital Context: Bangladesh Perspective*. Journal of Dhaka International University, 13(1)

³ Shams, A. T. (2024). *Dissent under Siege: Case Studies of Repression in the Digital Era of Bangladesh*. Advances in Journalism and Communication, 12(1), 207–230.

⁴ Ashraf, S., & Islam, Md. M. (2023). *AI and the future of human rights in Bangladesh: a call for robust legal and ethical frameworks*. International Journal of Law and Information Technology, 31(4), 331–348.

systematic regulation and suppression of political opposition (Rahman., 2025)⁵. Such digital authoritarianism underscores the urgency of addressing the widening gap between domestic policy and the evolving global norms that prioritize the protection of individual privacy and civil liberties against arbitrary state intervention. Central to this examination is the concept of "digital pitfalls," which characterizes how the state utilizes surveillance and a politics of fear to neutralize critical discourse. This climate of pervasive monitoring not only induces widespread self-censorship among digital activists and journalists but also exacerbates existing power imbalances between the state and marginalized populations. These systemic vulnerabilities are exacerbated by fragmented oversight mechanisms that lack the requisite transparency to prevent potential abuses of executive authority. To address these challenges, it is imperative to investigate whether such surveillance creates a persistent "chilling effect," compelling individuals to self-censor their political expression out of fear of state retaliation. Furthermore, the deployment of such invasive monitoring mechanisms without robust judicial oversight often disproportionately targets journalists and human rights defenders, thereby undermining the essential pluralism required for democratic accountability. This phenomenon mirrors broader patterns of digital authoritarianism observed in other jurisdictions, where the deployment of intrusive monitoring tools under the guise of national security creates profound asymmetries of power that compromise personal autonomy. Such regulatory asymmetry, often characterized by executive-centric oversight, obscures the thin line between legitimate state security interests and the weaponization of personal data for political control (M. Abraham, 2024).⁶

⁵ Rahman, A. (2025). The Dual State: Artificial Intelligence, Authoritarian Control, and the Crisis of Youth in Bangladesh (2014-2024)

⁶ Abraham, M., Dev, S., & Manrique, J. I. T. (2024). Asymmetric Surveillance Governance: A Thematic Analysis of Privacy, National Security, and AI Regulation in India. *Qubahan Political Journal*, 3(1), 1–11.

1.2 Problem Statement: Conflict between state security and freedom of expression.

This investigation specifically interrogates how the strategic utilization of digital infrastructure allows the government to regulate information flow and marginalize opposition, thereby eroding democratic accountability within the nation's hybrid political landscape (Drovcic, 2025)⁷. This study further examines how the lack of independent regulatory bodies facilitates the unchecked expansion of surveillance capabilities, which are frequently justified through populist narratives of national stability. By analyzing these mechanisms, the research demonstrates how surveillance is increasingly legitimized through legal structures that weaken democratic practices and institutionalize control under the guise of security and national interest. Consequently, this technological integration necessitates a critical reassessment of how modern governance frameworks instrumentalize data as a pivotal driver of the contemporary economy while simultaneously leveraging it as a tool for political containment. Moreover, the emergence of a "private-public surveillance partnership" in Bangladesh complicates traditional accountability, as commercial data intermediaries frequently align with state interests to facilitate mass monitoring. This reliance on third-party digital intermediaries mirrors regional trends where fragmented legal frameworks, such as those observed in Pakistan, lack the necessary proportionality safeguards to check executive discretion in data acquisition. These regulatory deficiencies are further exacerbated by the absence of an omnibus data protection law, which leaves sensitive personal information vulnerable to exploitation by both state actors and private entities. Although recent initiatives such as the 2025 Personal Data Protection Ordinance signal an attempt to formalize these protections, they remain constrained by systemic legal and institutional barriers that prevent meaningful oversight (P. Saha, 2026)⁸. This legislative stagnation underscores a broader concern regarding the Digital Security Act of 2018, which remains a primary instrument for criminalizing online dissent despite calls for its repeal by international observers (Hasan., 2023)⁹. Consequently, the interaction between these legislative frameworks

⁷ Drovcic, C. (2025). Surveillance Capitalism and the New Social Order: Rethinking Freedom in the Digital Age. *OTS Canadian Journal*, 4(9), 16–16.

⁸ Saha, P., Chan, A. S., & Sultana, S. (2026). When Data Protection Fails to Protect: Law, Power, and Postcolonial Governance in Bangladesh. In *arXiv (Cornell University)*. Cornell University.

⁹ Hasan, A. R. (2023). Digital Security Act 2018: From the Lens of Investigative Journalism and Freedom of Expression. *Perspectives in Social Science*, 17.

and the broader sociopolitical climate reflects a concerted effort to institutionalize state surveillance, thereby creating a hybrid media system where traditional and digital platforms are increasingly subsumed under the state's apparatus of political control. This institutionalization is further entrenched by the state's capacity to process large-scale personal data, which, despite the introduction of recent ordinances, remains largely unchecked by independent judicial or civil society monitoring. This regulatory ambiguity allows state actors to leverage public-private hybridisation to circumvent established legal safeguards, effectively co-opting commercial data infrastructures to monitor political activity under the veneer of administrative efficiency. This convergence of interests obscures the accountability gap between state intelligence agencies and private information companies, effectively shielding invasive practices from the more stringent constraints often applied to governmental bodies. Such integration of state power and corporate technical infrastructure mirrors regional trajectories toward digital authoritarianism, where legal frameworks are leveraged to prioritize state control over individual constitutional protections.

1.3 Objectives: Examine constitutional guarantees, statutory laws, and human rights implications.

Furthermore, this research seeks to determine if the existing legal regime in Bangladesh provides protections for personal data that align with international standards, given the country's lack of comprehensive privacy legislation. Additionally, the study aims to evaluate how current legislative gaps impede the protection of identity and autonomy, particularly in an era where personal data serves as the primary currency for both commercial and political surveillance. Moreover, the study intends to analyze the discrepancies between domestic statutory instruments and international human rights benchmarks, such as those articulated in the International Covenant on Civil and Political Rights, to identify the systemic failures that permit ongoing privacy infringements (The Right to Privacy in the Digital Age: State Concerns and Initiatives in Bangladesh., 2025) Finally, the analysis seeks to propose a roadmap for legislative reform that prioritizes the explicit recognition of privacy as a fundamental right, thereby reconciling the current tension between state-led technological integration and the

constitutional preservation of individual liberty. By bridging the gap between emerging South Asian privacy jurisprudence and localized legal standards, this roadmap addresses the critical need to harmonize economic data initiatives with the protection of core fundamental rights. This research contends that without explicit and robust constitutional safeguards, the potential for rights violations will continue to escalate as rapid technological advancements persistently outpace existing legal reforms (AllahRakha., 2024)¹⁰. Such a trajectory risks cementing a domestic environment where the lack of clear data subject ownership—a common shortfall in the regional legislative landscape—leaves citizens structurally vulnerable to algorithmic disenfranchisement (Md. Z. Haq, 2025)¹¹. Furthermore, the persistent exploitation of these statutes to stifle public discourse has drawn significant condemnation from global human rights entities, which characterize such measures as draconian impediments to online freedom of expression. These critiques highlight an urgent need to re-evaluate the intersection of ICT dependence and individual privacy, as personal data currently functions as the primary currency for digital-age governance.

1.4 Research Questions:

- i. How does state surveillance in Bangladesh affect the constitutional guarantee of freedom of expression under Articles 39 and 43?
- ii. To what extent do existing laws such as the ICT Act and Digital Security Act adequately protect human rights in the digital age?
- iii. How have Bangladeshi courts interpreted privacy and freedom of expression in the context of digital surveillance?
- iv. What lessons can Bangladesh draw from comparative jurisdictions such as India, the EU, and the USA in balancing surveillance with human right?
- v. How have specific incidents (e.g., Rohingya crisis monitoring, media censorship, digital activism) illustrated the tension between surveillance and rights in Bangladesh?

¹⁰ AllahRakha, N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, 2(4), 31–43.

¹¹ Haq, Md. Z., Ayub, Z. A., & Abdel-Rahman, A. B. (2025). GDPR and Bangladesh's data privacy laws: a comprehensive analysis. *International Journal of Public Law and Policy*, 11(2), 192–209.

- vi. What are the broader human rights implications of surveillance practices in Bangladesh, particularly for journalists, activists, and marginalized communities?
- vii. What constitutional, legislative, and policy reforms are necessary to ensure that surveillance practices in Bangladesh align with international human rights standards?

1.5 Research Methodology:

This study adopts a doctrinal, comparative, and case-study based methodology to critically examine the intersection of surveillance, freedom of expression, and human rights in Bangladesh's evolving digital landscape. The doctrinal approach involves a systematic analysis of constitutional provisions, statutory instruments such as the Digital Security Act 2018, Cyber Security Act 2023, and the 2025 Cyber Security Ordinance, alongside relevant judicial interpretations of Articles 39 and 43 of the Constitution of Bangladesh. This method enables a rigorous evaluation of how existing legal frameworks both safeguard and restrict fundamental rights in the digital age.

Complementing this doctrinal inquiry, a comparative method is employed to situate Bangladesh's surveillance practices within broader global and regional contexts. Jurisdictions such as India, the European Union, and the United States are examined to identify best practices and lessons in balancing national security imperatives with international human rights obligations. This comparative lens highlights divergences and convergences in legal standards, particularly regarding privacy, data protection, and freedom of expression, thereby offering a roadmap for potential reform in Bangladesh.

Additionally, the research integrates a case-study approach to ground theoretical analysis in practical realities. Specific incidents—including state monitoring during the Rohingya crisis, censorship of digital media, and the targeting of journalists and activists—are examined to illustrate how surveillance mechanisms operate in practice and how they affect vulnerable communities. These case studies provide empirical

depth, demonstrating the lived consequences of surveillance beyond abstract legal discourse.

The methodology is primarily qualitative, relying on textual analysis of legislation, judicial decisions, policy documents, and scholarly literature. Secondary sources such as reports from international human rights organizations, UN resolutions, and regional policy papers are also incorporated to ensure a holistic understanding of the subject matter. The study consciously avoids quantitative measurement, as the focus lies on normative legal evaluation rather than statistical generalization.

Finally, the research is guided by the tripartite human rights test of legality, necessity, and proportionality, as articulated in international jurisprudence. This evaluative framework ensures that surveillance practices are assessed against globally recognized standards, thereby bridging the gap between domestic legal realities and international human rights commitments. By synthesizing doctrinal analysis, comparative insights, and case-based evidence, the methodology provides a comprehensive foundation for assessing the compatibility of Bangladesh's surveillance regime with constitutional guarantees and international obligations.

1.6 Literature Review:

The scholarly discourse on surveillance and freedom of expression in the digital age reveals a persistent tension between state security imperatives and the protection of fundamental rights. In the Bangladeshi context, much of the literature critiques the Digital Security Act 2018 and the Cyber Security Act 2023 for their broad and ambiguous provisions, which enable state-led monitoring and criminalization of dissent (Hasan, 2023; Shams, 2024). These statutes are frequently characterized as instruments of digital authoritarianism, where surveillance infrastructures are deployed not merely for national security but as mechanisms to silence political opposition and constrain journalistic freedom (Rahman, 2025).

Globally, scholars have emphasized the risks of algorithmic governance and predictive surveillance, noting that opaque decision-making systems undermine accountability and erode democratic safeguards (Kouroutakis, 2024; Khalaileh,

2023). Comparative studies from the European Union highlight the importance of proportionality and necessity standards in surveillance law, particularly under the General Data Protection Regulation (GDPR), which provides a robust framework for balancing privacy with legitimate state interests. In contrast, jurisdictions such as India have struggled with fragmented data protection regimes, where surveillance practices often bypass judicial oversight, mirroring the challenges faced in Bangladesh (Grover & Singh, 2024).

The literature also underscores the role of international human rights instruments—notably the ICCPR and UDHR—in setting normative benchmarks for privacy and freedom of expression. However, scholars argue that these standards remain aspirational in many developing contexts, as weak institutional capacity and executive dominance hinder effective implementation (Cheong, 2024; Khasawneh et al., 2025). This gap between normative ideals and practical enforcement has been described as a “chilling effect,” where pervasive monitoring induces self-censorship among activists, journalists, and marginalized communities (Ashraf & Islam, 2023).

Finally, critical perspectives rooted in postcolonial theory highlight how surveillance in South Asia is often justified through developmental rhetoric, masking its function as a tool of political containment (Belayet et al., 2025). These critiques emphasize the need for human-rights-by-design frameworks that embed transparency, contestability, and accountability into digital governance systems. Without such reforms, scholars warn that surveillance risks becoming normalized as a structural feature of governance, thereby undermining democratic pluralism and civil liberties.

Taken together, this body of literature establishes the foundation for interrogating Bangladesh’s surveillance regime. It highlights the urgent need to reconcile domestic legal frameworks with international human rights standards, while also drawing lessons from comparative jurisdictions that have attempted to balance security imperatives with civil liberties.

1.7 Scope & Limitations: Bangladesh focus with selective global comparisons.

The study prioritizes an analytical framework that synthesizes qualitative legal assessments with comparative insights from South Asian jurisdictions to highlight systemic vulnerabilities in existing regulatory architectures (Singh, 2024)¹². This comparative approach specifically evaluates whether existing surveillance mandates adhere to the tripartite standards of legality, necessity, and proportionality as articulated in international human rights jurisprudence. By examining these benchmarks against the prevailing legal landscape, this analysis seeks to expose the persistent discordance between the state's expansive surveillance capabilities and the requirements of democratic accountability (Dutt., 2026)¹³. This research further interrogates how the deployment of artificial intelligence and facial recognition technologies by state authorities exacerbates these vulnerabilities, often functioning beyond the reach of established judicial oversight mechanisms. Given the dual-use potential of these technologies, the lack of transparency in their procurement and deployment raises profound concerns regarding their compliance with global human rights norms. Furthermore, the integration of these sophisticated tools into public services necessitates a rigorous assessment of algorithmic fairness to prevent the systemic infringement of civil liberties and individual autonomy. Consequently, the absence of a comprehensive regulatory mechanism to govern these digital interventions creates a persistent environment of impunity that threatens to normalize the erosion of personal privacy. This systemic failure to establish clear oversight facilitates an environment where data is increasingly weaponized to stifle dissent rather than foster public service, effectively transforming the digital sphere into a tool for state-centric control. Such dynamics reflect a broader regional trend where the absence of unified data protection frameworks allows algorithmic profiling and cross-border data flows to operate without meaningful legislative checks. Consequently, this regulatory void exposes citizens to pervasive surveillance architectures that lack the requisite proportionality and necessity standards essential for a rights-respecting democratic society. Addressing this deficit

¹² Grover, D. J., & Singh, R. (2024). THE LAW OF RIGHT TO PRIVACY IN INDIA: PROTECTING PRIVACY IN THE DIGITAL ERA: CHALLENGES. *ShodhKosh Journal of Visual and Performing Arts*, 5(1).

¹³ Tyagi, R., & Dutt, O. (2026). Privacy vs. National Security: Balancing Surveillance and Data Protection in India. *International Journal For Multidisciplinary Research*, 8(1).

requires a fundamental shift toward robust legislative frameworks that prioritize individual dignity and autonomy over unfettered state data collection. Integrating such safeguards remains essential for ensuring that the transition to digital governance does not undermine the foundational principles of privacy and democratic participation. Such reform must explicitly address the tension between the state's drive for technological modernization and the necessity of maintaining transparency in algorithmic decision-making. To achieve this, policymakers should implement mandatory algorithmic impact assessments and audit requirements to mitigate the risks of bias and unauthorized surveillance inherent in automated governance. Establishing these accountability mechanisms requires the adoption of polycentric governance models that mandate the disclosure of data processing logic, thereby ensuring that automated systems remain subject to public scrutiny rather than opaque state control. Beyond internal oversight, fostering a culture of public participation and multi-stakeholder engagement is essential to align AI deployment with democratic values rather than strictly computational efficiency. Effective governance in this context necessitates the creation of independent, well-resourced data authorities empowered to perform regular audits and sanction abuses, thereby curbing the normalized expansion of bulk data collection. Such institutional reforms must be complemented by the adoption of privacy-enhancing technologies, such as encryption and anonymization, to ensure that service delivery remains distinct from state oversight. By prioritizing human-centric design, policymakers can ensure that digital identity systems serve as foundations for democratic agency rather than mechanisms of state-centric surveillance (Matta., 2026).¹⁴

¹⁴ Matta, D. (Daoud). (2026). The Digital Social Contract: Protecting Identity in the Age of AI. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research.

2 Chapter 2: Conceptual Framework

2.1 Defining Surveillance: State vs. corporate surveillance.

The former involves the direct exercise of coercive state power to monitor political activity, while the latter characterizes the commercial extraction of behavioral data for algorithmic profiling, both of which erode the boundaries of individual autonomy. This conceptual tension highlights the importance of "constrained democratic agency," where digital systems serve as conduits for political intervention rather than deterministic instruments of control. This framework posits that governance, rather than the underlying technology itself, remains the primary determinant of whether digital identification systems empower citizens or entrench authoritarian oversight. To move beyond this dichotomy, the framework adopts the "capillaries of power" lens to analyze how specific algorithmic architectures—such as epistemic opacity and embedded bias—displace accountability and bypass established legal safeguards. This structural opacity functions as a "black-box" mechanism that intentionally shields state decisions from meaningful judicial and public scrutiny. This concentration of power among centralized state actors, combined with the lack of institutional visibility, effectively weakens public trust and exacerbates the vulnerability of marginalized groups to political manipulation. Furthermore, these surveillance practices often ignore the critical need for enforceable data protection standards, allowing for the deployment of invasive systems without the necessary technological or legal oversight required to prevent human rights abuses. Consequently, a shift toward a human-rights-by-design framework is essential to ensure that administrative efficiency does not supersede the fundamental legal protections guaranteed to all citizens (Victor., 2025)¹⁵. This mandate necessitates recognizing that digital identity infrastructures inherently function as apparatuses of control, where the centralization of sensitive data facilitates the potential for state-led exclusion. Moreover, the core platform properties of these digital identification systems often prioritize the extraction of actionable intelligence over individual user agency, effectively forcing citizens into binary conditions of compliance or social exclusion. This structural imbalance suggests that without comprehensive normative constraints, digital development initiatives risk reconfiguring

¹⁵ Daniel, L. O., & Victor, N. O. C. (2025). Digital Identity Policy-Making in Africa (pp. 233–260).

social participation in ways that systematically undermine individual dignity. Such risks are particularly acute in contexts where biometric systems are deployed in the absence of comprehensive data protection laws, effectively granting state entities and technology providers unchecked authority over the digital footprints of vulnerable populations.

2.2 Freedom of Expression: Constitutional guarantees (Articles 39 & 43).

These must be governed by principles that ensure explainability, contestability, and the preservation of human dignity, effectively re-anchoring digital governance within the rule of law. This normative realignment must move beyond mere transparency, acknowledging that the affordances of automated systems within existing power structures inherently disrupt traditional legal safeguards. The emergence of responsibility gaps within these autonomous architectures underscores the urgent need for a regulatory shift that treats algorithmic opacity not as a technical constraint, but as a direct challenge to the rule of law. Such challenges require enforcing an obligation for reason and explainability in automated decision-making to mitigate the risk of systemic bias (Kouroutakis., 2024)¹⁶. Furthermore, since the internal logic of learning-based systems frequently remains non-transparent and non-explainable, the lack of contestability hinders the ability of public officials to meaningfully assess the justifiability of algorithmic outcomes. The inherent opacity of these “black box” models complicates the assignment of responsibility, as it becomes nearly impossible for developers or deploying entities to provide a clear justification for specific, rights-impacting outcomes. This lack of accountability creates a significant regulatory gap that prevents individuals from challenging adverse decisions, thereby undermining the democratic necessity of legal redress. To mitigate these risks, implementing adversarial procedures that introduce friction into dominant filtering systems is essential to restore the public interest and ensure meaningful oversight. By shifting from a framework of post hoc procedural redress to one that embeds structural contestation, these interventions move beyond soft-law recommendations to provide citizens with the

¹⁶ Kouroutakis, A. E. (2024). Rule of law in the AI era: addressing accountability, and the digital divide. *Discover Artificial Intelligence*, 4(1).

power to challenge the latent hierarchies and bias-replicating thresholds inherent in automated decisions. Ultimately, this transition toward institutionalized contestability forces a departure from the "black-box" model, requiring that all automated adjudications meet rigorous interpretability thresholds to preserve the ontological integrity of legal authority.

2.3 Human Rights in Digital Age: ICCPR, UDHR, regional instruments.

These foundational texts provide the normative bedrock for challenging state-sponsored algorithmic surveillance that threatens the core tenets of privacy and freedom of expression. However, in the absence of robust judicial mechanisms, these international standards often remain aspirational, failing to curb the deployment of predictive systems that undermine the individual's right to be free from arbitrary interference (Cheong., 2024)¹⁷. Consequently, the lack of meaningful contestability in these systems effectively nullifies the practical utility of these human rights instruments, as citizens cannot effectively challenge automated outcomes that lack procedural transparency. Addressing this accountability deficit requires shifting the focus toward the scope and implementation of State obligations to ensure that businesses and public entities are held to rigorous standards of prevention and remedy. Specifically, achieving such accountability necessitates granting affected parties access to the underlying evidentiary data, as explanations alone often prove insufficient to enable meaningful legal challenges. Furthermore, international oversight bodies must move toward a systemic governance approach that incorporates prospective benchmarking and risk-based regulatory frameworks to mitigate the proliferation of algorithmic harms before they are integrated into administrative state functions. This transition necessitates the intellectualization of administrative law, where core principles such as due process and reasoned decision-making are redefined to address the sociotechnical complexities of automated governance (F. S. Al Khasawneh, 2025)¹⁸. This re-conceptualization must prioritize the "Principle of Refutability,"

¹⁷ Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*,

¹⁸ Khasawneh, F. S. Al., Amoush, M. A. M., & Khwaileh, K. M. (2025). GOVERNING ALGORITHMS: THE INTELLECTUALIZATION OF ADMINISTRATIVE LAW AND EMERGING

ensuring that every automated administrative outcome remains subject to the incorporation of contradiction and revision through reasoned legal argument (Isotalo., 2026)¹⁹. By formalizing these mechanisms, policymakers can address the structural asymmetries where existing legal doctrines, designed for human agency, struggle to interpret harms originating from opaque and adaptive systems. This necessitates a paradigm shift in legal doctrine to redefine victimhood and agency, as traditional frameworks fail to account for the "obscurity" inherent in AI-driven surveillance. This challenge is compounded by the fact that AI systems can generate unforeseen conclusions that preclude individuals from even identifying that their rights have been violated, thereby preventing them from seeking necessary redress (Khalaileh., 2023)²⁰. To address these impediments, current governance initiatives must pivot from soft-law rhetoric toward substantive accountability by imposing direct legal obligations on entities deploying these technologies.

2.4 Theoretical Lens: Security vs. liberty; postcolonial critiques.

In the Bangladeshi context, this theoretical tension is exacerbated by the securitization of digital space, where state-mandated surveillance architectures are frequently justified as essential for national stability despite their erosive impact on individual dissent. This climate of pervasive monitoring is further complicated by the absence of a comprehensive legal framework for data governance, which leaves citizens vulnerable to unaccountable algorithmic liabilities (H. Belayet, 2025)²¹. Such regulatory fragmentation necessitates an alignment of local data protection standards with the National AI Policy, 2024, to ensure that technological integration does not bypass fundamental democratic safeguards. Moreover, the integration of these systems must be grounded in an integrated legal-technological governance framework that explicitly

INTERNATIONAL-LAW CONSTRAINTS. *Veredas Do Direito Direito Ambiental e Desenvolvimento Sustentável*, 22(3).

¹⁹ Isotalo, G. (2026). From Jurisprudence to Infrastructure: Algorithmic Governance and the Ontological Displacement of Law. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research.

²⁰ Khalaileh, Y. (2023). Accommodating Artificial Intelligence in International Law: An Overview and New Frontier. *Journal of Human Security*, 19(1).

²¹ Belayet, H., Mohammad, Matin, C., Mohammad Abdul, Abdullah, F., Muhammad, Mohammad, A. T., & Monzur, H., Abdullah Al. (2025). Evaluating the legal accountability of artificial intelligence (AI) in Bangladesh: beyond regulatory frameworks. Monash University Research Portal (Monash University).

prioritizes procedural fairness and the protection of fundamental rights over administrative expediency. Furthermore, given the significant gaps in institutional readiness, the development of context-sensitive regulatory frameworks must address specific sectoral vulnerabilities to ensure that technological advancements do not inadvertently facilitate discriminatory surveillance practices. In this regard, establishing autonomous oversight bodies is critical to evaluate the ethical implications of these tools, ensuring that national security objectives do not supersede the protection of civil liberties. Such mechanisms must mandate transparency in algorithmic deployments, requiring agencies to provide accessible data concerning the operational parameters of surveillance tools to facilitate public scrutiny. This is particularly pressing given that the rapid deployment of these technologies in Bangladesh, ranging from digital public services to cyber-monitoring, has often outpaced the evolution of existing instruments like the Cyber Security Act 2023. Indeed, the ambiguity inherent in such legislation risks transforming cybersecurity mandates into tools for curtailing individual liberties rather than fostering public safety. Recent reports indicate that state-led surveillance initiatives, such as the National Telecommunication Monitoring Centre's acquisition of advanced spyware capable of intercepting encrypted communications, underscore the urgent need for stringent judicial oversight (Shams, 2024)²². Ultimately, bridging the gap between ambitious digital strategies and human rights protection requires moving beyond reactive legislation to develop robust, context-aware frameworks that explicitly regulate the ethical deployment of AI. This entails reconciling the aggressive enforcement mechanisms of the Cyber Security Ordinance 2025 with the constitutional protections afforded to personal privacy and freedom of expression. Such a reconciliation demands that legal reforms address the existing technological divide and regulatory fragmentation to prevent the normalization of mass digital surveillance under the guise of national security. Proactive legislative reform must therefore prioritize the creation of independent, multi-stakeholder auditing mechanisms that hold state agencies accountable to international human rights standards. Furthermore, fostering a culture of algorithmic accountability requires the implementation of robust governance frameworks that mandate clear lines of responsibility for cybersecurity solutions, ensuring that oversight mechanisms can effectively address potential

²² Shams, A. T. (2024). Dissent under Siege: Case Studies of Repression in the Digital Era of Bangladesh. *Advances in Journalism and Communication*, 12(1), 207–230.

systemic errors. Moreover, establishing these accountability benchmarks requires a shift toward radical algorithmic transparency, ensuring that the logic underpinning surveillance tools remains accessible for judicial and public scrutiny (Engelmann, 2023)²³. Such transparency initiatives are essential to mitigate the risk of algorithmic prejudice and to ensure that digital interventions do not exacerbate existing social inequalities or facilitate state-sanctioned censorship. To achieve this, policymakers and industry leaders must adopt a collaborative approach that embeds human-centered ethical considerations into the core of digital innovation, effectively narrowing the gap between security imperatives and civil rights. This transition towards multi-stakeholder governance must also address the asymmetric power dynamics inherent in state-corporate surveillance, where behavioral analytics and predictive tools often operate beyond the reach of traditional public accountability. Consequently, the implementation of mandatory algorithmic impact assessments is necessary to institutionalize checks on executive discretion, mirroring efforts to standardize regulatory oversight in comparable jurisdictions.

²³ Engelmann, A. G. (2023). Algorithmic transparency as a fundamental right in the democratic rule of law. *Brazilian Journal of Law Technology and Innovation*, 1(2), 169–188.

3 Chapter 3: Legal Framework in Bangladesh

3.1 Constitutional Provisions: Freedom of speech, privacy, press.

These guarantees face ongoing challenges as legislation such as the Cyber Security Act, 2023, increasingly reflects state-centric norms that prioritize control and reputational management over the protection of individual dissent. - Legislative Ambiguity: The broad and often vague language within the Information and Communication Technology Act, 2006, and subsequent amendments creates significant legal uncertainty that complicates the interpretation of protected digital conduct (Mallika, 2025)²⁴. - Corporate Responsibility: The role of internet intermediaries remains largely unaddressed, necessitating clear liability regimes that align with international benchmarks for platform accountability and human rights. Adopting a multi-stakeholder governance model—incorporating government, industry, and civil society—is vital to ensure that these technological shifts enhance, rather than undermine, the digital rights of citizens. Furthermore, integrating comprehensive digital literacy programs and critical thinking initiatives is essential to equip the public against the algorithmic catalysts of communal and moral panic that have increasingly characterized the post-2024 information landscape. Ultimately, a rights-based approach to policy-making must reconcile the nation's rapid technological integration with the necessity of protecting individuals from the risks of systemic misuse and unauthorized data monitoring. In this context, the recent introduction of the Personal Data Protection Ordinance and the National Data Governance Ordinance in 2025 serves as a critical, albeit incomplete, attempt to codify these protections within the evolving digital ecosystem. However, the efficacy of these new instruments remains curtailed by significant structural and political barriers that hinder their ability to enforce genuine institutional accountability. Specifically, the lack of an independent regulatory body—comparable to the data protection authorities observed in other jurisdictions—prevents these ordinances from transitioning beyond symbolic legal frameworks into functional mechanisms of redress. Without a centralized and autonomous oversight entity, the enforcement of these ordinances remains fragmented, leaving citizens with limited

²⁴ Hossain, M. S., & Mallika, M. (2025). Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview. *International Journal of Research and Innovation in Social Science*, 3796–3811.

recourse against unauthorized data processing and state surveillance. This legislative inertia highlights a broader paradox where the state promotes digital transformation to drive economic growth while simultaneously maintaining archaic control mechanisms that stifle civic participation. Addressing this dichotomy necessitates a comprehensive review of judicial precedent to clarify the extent to which executive surveillance directives may supersede fundamental constitutional safeguards. Such an analysis must concurrently emphasize the necessity of normative harmonization to eliminate regulatory ambiguity, ensuring that disparate sectoral laws do not facilitate the erosion of civil liberties. Moreover, the institutionalization of robust data protection demands a shift away from fragmented, sector-specific regulations toward a unified legal architecture that aligns with global standards of privacy and human rights. This transformation requires not only the formalization of legal definitions but also the empowerment of a data protection authority capable of conducting independent, risk-based impact assessments that address the specific vulnerabilities inherent in the country's digital administrative systems. Learning from regional challenges, policymakers must critically analyze how exemptions for state agencies—often invoked under the guise of national security—can undermine the integrity of such oversight bodies. Establishing a truly autonomous regulatory framework requires explicit safeguards against political interference, ensuring that data protection officers are legally protected while performing their oversight functions. Furthermore, the current absence of an independent supervisory authority threatens to create a regulatory vacuum, diminishing public trust and exacerbating the legal uncertainties that already plague the digital rights landscape. Establishing an independent oversight entity is therefore critical to mandate institutional accountability, prevent the misuse of population data, and ensure that enforcement mechanisms are not subordinated to the executive branch's broad discretionary powers. Such reforms must also prioritize the integration of victim-oriented redress mechanisms, which are essential for addressing the significant weaknesses in current institutional capacity and law enforcement efficacy. By mandating clear legal standards and transparent oversight, Bangladesh can better balance national security imperatives with the protection of fundamental human rights. Such initiatives should be accompanied by the repeal of restrictive media laws and the strengthening of parliamentary supremacy to foster a legal environment that is truly conducive to the preservation of civil liberties. Beyond these structural adjustments, fostering a digital environment that respects fundamental human rights

necessitates a cultural shift toward transparency, where both state and private actors are held accountable to the principles of necessity and proportionality (Islam, 2022; “The Right to Privacy in the Digital Age: State Concerns and Initiatives in Bangladesh,” 2025).

3.2 Statutory Laws: ICT Act, Digital Security Act, Telecommunication Act.

These frameworks, while foundational to the nation's information society, currently operate within a regulatory landscape where the absence of harmonized oversight complicates the enforcement of constitutional protections. These existing statutes often prioritize state-centric control over individual privacy, frequently leading to the systematic suppression of dissenting voices in the digital sphere. Consequently, the lack of a specialized data protection law leaves these regulations to function as instruments of state surveillance rather than safeguards for fundamental human rights. This misalignment underscores the urgency of establishing an independent supervisory agency capable of conducting objective oversight, thereby preventing the administrative misuse of personal data that has become increasingly prevalent. While the Constitution theoretically guarantees the privacy of correspondence under Article 43, the lack of a comprehensive data protection regime renders these fundamental rights largely unenforceable against state-sanctioned intrusion (Haque, 2019)²⁵. This systemic deficiency creates an environment where personal data acts as a digital commodity subject to pervasive tracking, yet lacks the necessary legal barriers to prevent unauthorized state access. Furthermore, the proliferation of these technologies necessitates a rigorous legal audit to ensure that government cyber-governance aligns with international obligations, particularly regarding the proportionality of technical surveillance measures. In this context, the shift toward a privacy-centric regime is imperative to counter the trend of data-driven surveillance, which currently prioritizes administrative convenience over individual autonomy. Adopting a structured proportionality test—requiring legality, legitimate aim, and necessity—would serve as a vital constraint against the opaque exercise of executive power in the digital domain

²⁵ Haque, A. B. (2019). NEED FOR CRITICAL CYBER DEFENCE, SECURITY STRATEGY AND PRIVACY POLICY IN BANGLADESH - HYPE OR REALITY? *International Journal of Managing Information Technology*, 11(1), 37–50.

(Singh A. , 2026)²⁶. Moreover, this normative refinement must address the inherent risks of identity theft and unauthorized access that emerge when personal data is treated merely as a fuel for economic innovation rather than a protected extension of individual dignity.

3.3 Judicial Interpretation: Supreme Court rulings on privacy/expression.

The judiciary has increasingly grappled with the tension between state-mandated digital oversight and the evolving jurisprudence of fundamental rights, as courts struggle to reconcile analog-era constitutional protections with the realities of algorithmic governance. These judicial inquiries must now confront the failure of traditional legal doctrines to account for the opaque, automated nature of big data analytics and biometric identification, which often operate beyond the reach of conventional oversight (M. Kaur, 2026).²⁷ By applying established legal tests of proportionality to these emerging technologies, the judiciary can better assess whether such monitoring methods constitute a justifiable interference with the individual's right to privacy and freedom of expression. Such a framework must explicitly address the "chilling effect" that ubiquitous surveillance exerts on public discourse, ensuring that judicial remedies provide meaningful protection against the encroachment of state-driven digital monitoring on democratic participation. In this pursuit, the judiciary should adopt a restrictive approach toward executive claims of national security, ensuring that surveillance infrastructures do not become normalized tools for managing political dissent. Furthermore, the judiciary must draw inspiration from comparative regional jurisprudence, such as the constitutional shift toward recognizing individual autonomy and self-determination of information as fundamental to democratic governance. This judicial maturation requires incorporating principles of digital constitutionalism to ensure that privacy, proportionality, and due process are not merely abstract concepts but binding constraints on algorithmic state power. Drawing upon the landmark judicial reinterpretation of the right to privacy as an intrinsic component of human dignity,

²⁶ Singh, A. (2026). Right to Privacy and State Surveillance: Procedural Safeguards and Accountability. *International Journal of Criminal Common and Statutory Law*, 6(1), 27–30.

²⁷ Kaur, M., Sharma, N., Mehta, P. K., Dhanoa, M. K., & Anegbe, B. (2026). Data Protection Laws and Privacy Rights in the Digital Age: Legal Challenges and Emerging Frameworks. *Indian Journal of Law*.

courts must move beyond static constitutional readings to address the complex challenges posed by state-led digital governance. Such a shift would require the judiciary to treat constitutional norms as living instruments capable of curtailing the opaque and unaccountable nature of modern algorithmic governance. Integrating this "Regulatory Judicialism" into the national legal framework would empower courts to serve as adaptive co-regulators, ensuring that technological deployment remains subordinated to the constitutional mandates of fairness and accountability. Ultimately, this evolution necessitates a re-evaluation of the state action doctrine, ensuring that human rights protections extend beyond state agencies to encompass the private platforms that facilitate pervasive digital surveillance. Moving forward, aligning national policy with emerging regional precedents—such as the conceptualization of a digital bill of rights—is essential to curbing the unchecked integration of state and corporate data-gathering apparatuses. Such a framework would necessitate the establishment of robust institutional mechanisms, potentially modeled after independent digital commissions, to provide the oversight currently absent in existing analog-based legal structures.

3.4 Policy Documents: National ICT Policy, Cybersecurity strategies.

These frameworks often prioritize state-led developmental goals and administrative efficiency, yet they fail to explicitly integrate a rights-based approach to mitigate the risks of digital profiling and algorithmic bias. This lack of oversight perpetuates a fragmented regulatory landscape, where current statutes—like the Information Technology Act—remain insufficient to address the unique complexities of AI-driven surveillance and automated decision-making. Consequently, the absence of binding oversight mechanisms allows state agencies to bypass due process, as technical systems increasingly perpetuate structural biases without transparent justification. To address these systemic vulnerabilities, legislative reform must prioritize the establishment of an enforceable accountability framework that mandates algorithmic impact assessments and auditability for all automated systems deployed in the public sector. Such reforms should explicitly incorporate principles of non-discrimination and procedural fairness to counteract the opacity often inherent in autonomous risk assessment and resource

allocation models. Beyond these immediate reforms, policymakers must ensure that the design of automated infrastructure incorporates human-in-the-loop protocols to mitigate the risks of exclusionary outcomes and rights violations. Furthermore, this paradigm shift requires moving away from reactive, post-facto legal remedies toward a proactive regulatory model that addresses the probabilistic and evolving nature of AI-mediated systems. This proactive approach necessitates a transition from traditional, evidence-based liability models to regulatory frameworks capable of monitoring the continuous, autonomous outputs of machine learning systems. Such a transition demands that legislators look beyond mere technical efficiency to codify the principles of dignity and non-discrimination as foundational requirements for the lifecycle of any algorithmic deployment.

4 Chapter 4: Comparative Perspectives

4.1 India: Surveillance under IT Act and Aadhaar debates.

In this context, the integration of predictive analytics and biometric frameworks like Aadhaar has faced significant scrutiny for potentially infringing upon the constitutional right to privacy established in “Justice K.S. Puttaswamy v. Union of India”²⁸, which highlights the critical tension between national security imperatives and fundamental privacy rights. The Indian experience underscores the regulatory deficit in addressing algorithmic accountability and transparency, where current legal structures often struggle to provide sufficient oversight for automated decision-making systems (Vaishali, 2026)²⁹. Similarly, the absence of clear legislative mandates regarding the traceability of algorithmic outputs in India continues to exacerbate risks of data privacy erosion and discriminatory profiling (A.V. & -, 2024). Moreover, the reliance on opaque, "black box" models in social welfare and law enforcement complicates the ability of individuals to contest administrative decisions, necessitating a move toward standardized requirements for human oversight and the duty to provide meaningful reasons for algorithmic outcomes.

- Comparative Analysis: By examining these cross-border regulatory trajectories, it becomes evident that while jurisdictions like the European Union prioritize a rigorous, risk-based classification system to safeguard human dignity, other regions continue to grapple with reconciling digital public infrastructure inclusivity with effective algorithmic accountability. Specifically, India's evolving strategy emphasizes inclusive digital public infrastructure, yet it lacks the formal, rights-centric enforcement mechanisms characteristic of the EU's comprehensive legislative approach. This divergence highlights the urgent necessity for Bangladesh to synthesize international best practices, such as the EU's risk-based scrutiny and Australia's transparency-focused ethical frameworks, into a localized, human-centric surveillance governance model. By shifting the regulatory focus toward ex-ante impact assessments, Bangladesh could mitigate the risks posed by the current trend of executive-centric oversight, which often favors administrative efficiency over the protection of individual civil liberties. Furthermore, integrating principles of

²⁸ Justice K.S. Puttaswamy v. Union of India, 10 SCC 1 (Supreme Court of India, 2017).

²⁹ Vaishali. (2026). AlgorithmicGovernanceThroughPredictiveAnalytics:LegalAccountabilityAnd Decision-MakingChallengesInIndia. Zenodo (CERN European Organization for Nuclear Research).

proportionality and privacy-by-design into the legislative process would provide the necessary safeguards to reconcile national security imperatives with the fundamental rights of citizens.

4.2 EU: GDPR and privacy safeguards.

The General Data Protection Regulation serves as a foundational benchmark by codifying the right to explanation, ensuring individuals can challenge the logic behind automated decisions that significantly impact their personal lives (O. Reis, 2024)³⁰. Furthermore, this framework mandates strict limitations on the processing of sensitive biometric data, establishing a high threshold for consent and transparency that restricts the potential for arbitrary mass surveillance (I. Researcher, 2026)³¹. By establishing such rigorous normative standards, the EU model contrasts sharply with regions where digital governance often prioritizes systemic data collection over individual autonomy, thereby providing a template for balancing technological progress with fundamental rights. This comparative analysis reveals that while normative frameworks offer essential protection for civil liberties, the global rise of algorithmic censorship and predictive surveillance necessitates a broader shift toward legal mechanisms that restrict the control of information and collective behavior (Freitas, 2026)³². Indeed, the disparity between these approaches reflects a broader tension in Bangladesh, where current legislative efforts emphasize compliance-heavy controls at the expense of independent supervision and ethical oversight. This imbalance creates a systemic vulnerability where the concentration of coercive power inhibits the development of an innovation-friendly environment, effectively discouraging the adoption of privacy-by-design architectures. Consequently, addressing these legislative gaps requires the establishment of an independent regulatory body tasked with ensuring that data-driven

³⁰ Reis, O., Eneh, N. E., Ehimuan, B., Anyanwu, A., Olorunsogo, T., & Abrahams, T. O. (2024). PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, 6(1), 73–88.

³¹ Researcher, I., Gupta, T., & Junghare, V. (2026). Privacy and Data Protection in AI: A Comparative Analysis of EU and Indian Regulatory Frameworks. *International Journal of Social Science and Human Research*, 9(2).

³² Freitas, J. G. D. (2026). The challenges of AI regulation: data protection, civil rights, and landmark cases. *Frontiers in Political Science*, 8.

technologies remain subordinate to constitutional rights, rather than serving as instruments for state-led surveillance. Such an oversight body must prioritize the codification of rights-based, precautionary standards that align with international benchmarks for algorithmic accountability (Habibulloh, 2025)³³. This institutional shift is essential for operationalizing the principles of informational self-determination, thereby ensuring that emerging technologies do not outpace the legal protections designed to uphold individual agency (He & Zhang, 2025).

4.3 USA: Patriot Act and free speech challenges.

The expansion of surveillance authorities under the Patriot Act has historically prioritized national security objectives over the protections afforded by the First Amendment, often creating a landscape where private sector data sharing facilitates extensive government monitoring. This legislative approach has set a precedent where the convergence of corporate data harvesting and state security mandates complicates the enforcement of consumer privacy, as seen in the ongoing debates surrounding the California Consumer Privacy Act's efficacy. Consequently, this regulatory fragmentation reflects the inherent difficulties in reconciling domestic surveillance practices with international human rights norms, particularly regarding the systemic protection of metadata and digital anonymity (M. Huda, 2024)³⁴. In the context of Bangladesh, this suggests that without robust safeguards against the misuse of surveillance technologies, the country risks infringing upon the democratic processes and individual autonomy that define a rights-respecting society. Moreover, the deployment of AI-driven tools for public safety often blurs the line between legitimate crime prevention and the infringement of individual freedoms, threatening to cultivate a pervasive atmosphere of surveillance-induced anxiety. This chilling effect is further compounded by the lack of institutional safeguards, which leaves citizens in developing nations particularly vulnerable to potential surveillance abuse compared to those in

³³ Habibulloh, M. (2025). Digital Governance And The Right To Privacy: A Comparative Analysis Of AI Regulation In Southeast Asia And The European Union. *Journal of Law Policy and Global Development*, 1(1), 19–35.

³⁴ Huda, M., Awaludin, A., & Siregar, H. K. (2024). Legal Challenges in Regulating Artificial Intelligence: A Comparative Study of Privacy and Data Protection Laws. *International Journal of Social and Human*

more established democratic jurisdictions. To counter this trend, Bangladesh must prioritize the adoption of proactive, rights-based governance models that mitigate the dangers of unchecked state power and systemic data overreach. Establishing such frameworks requires a critical assessment of how algorithmic tools, when left unregulated, foster discriminatory profiling and exacerbate existing social fissures. Moreover, the omnipresent nature of these technologies risks chilling political participation, as the fear of being targeted for peaceful assembly or dissent may suppress the vibrant public discourse essential for a healthy democracy.

4.4 Regional Context: South Asian surveillance trends.

In the broader South Asian landscape, states are increasingly adopting intrusive digital monitoring tools under the guise of public security, often lacking the judicial oversight mechanisms present in more democratic legal traditions. This regional trend toward securitized governance frequently undermines privacy, as the absence of stringent oversight permits the unchecked deployment of surveillance technologies that lack accountability. Such unchecked expansion reflects a broader regional drift toward the normalization of digital authoritarianism, where the integration of predictive policing and mass biometric monitoring is prioritized over the preservation of constitutional guarantees. Within Bangladesh, this trajectory manifests as a "Dual State" where digital advancements designed to project economic modernization are repurposed to consolidate control and suppress dissent (Rahman, 2025)³⁵. This trend mirrors challenges seen elsewhere in the region, where legislative exemptions for state security often override nascent data protection frameworks, effectively shielding law enforcement from necessary algorithmic accountability. Furthermore, the lack of algorithmic transparency is compounded by a reliance on foreign-procured surveillance platforms, which creates a strategic dependency that limits local oversight of data governance and algorithmic logic. As these technologies are integrated into public services, the absence of robust accountability mechanisms for automated decision-making risks entrenching social biases and magnifying historical injustices. By

³⁵ Rahman, A. (2025). *The Dual State: Artificial Intelligence, Authoritarian Control, and the Crisis of Youth in Bangladesh (2014-2024)*

embedding these automated systems into the social fabric without rigorous public deliberation, the state risks transforming citizens into "algorithmic subjects" whose rights are perpetually mediated by opaque computational logics rather than established legal principles. This shift is particularly evident in the utilization of the Digital Security Act, which has been operationalized alongside advanced interception capabilities—such as spyware deployment and the acquisition of equipment to monitor encrypted communications—to systematically dismantle spaces for legitimate dissent. This reliance on foreign-built surveillance infrastructure further exacerbates national security risks, as the absence of access to source code or algorithmic parameters grants external vendors potential influence over sensitive domestic information.

4.5 Lessons for Bangladesh: Balancing national security with rights.

To navigate this challenge, the government must transition from expansive, security-centric legislative models toward human-centric frameworks that prioritize constitutional protections for privacy and freedom of expression. This shift necessitates the development of comprehensive regulatory standards, such as those proposed in the National AI Policy 2024, to ensure that technological integration remains aligned with ethical governance and public accountability. Furthermore, fostering diversity within AI development teams and engaging stakeholders in the decision-making process is essential to identify and rectify biases inherent in these systems (A. O. Aderibigbe, 2023)³⁶. Establishing independent, multi-disciplinary oversight bodies is critical to evaluate the deployment of these tools against international human rights obligations, ensuring that legislative frameworks evolve at a pace commensurate with technological advancement. Additionally, implementing mandatory algorithmic impact assessments will facilitate the identification of potential harms before deployment, thereby addressing the current gap in accountability for automated decision-making processes. Such proactive measures are essential to ensuring that AI deployment in crisis

³⁶ Aderibigbe, A. O., Ohenhen, P. E., Nwaobia, N. K., Gidiagba, J. O., & Ani, E. C. (2023). ARTIFICIAL INTELLIGENCE IN DEVELOPING COUNTRIES: BRIDGING THE GAP BETWEEN POTENTIAL AND IMPLEMENTATION. *Computer Science & IT Research Journal*, 4(3), 185–199.

interventions and public safety remains subject to rigorous ethical scrutiny, ultimately safeguarding the fundamental rights of the population. By formalizing these regulatory pathways, Bangladesh can mitigate the risks of data-driven discrimination while fostering a digital environment that prioritizes individual autonomy over mass monitoring (Ashraf & Islam, 2023; Belayet et al., 2025). Ultimately, fostering this institutional resilience requires a concerted shift toward algorithmic sovereignty, enabling the state to exercise independent control over the critical infrastructure that defines its digital governance. Developing such sovereignty necessitates the implementation of adaptive legal structures that regulate the lifecycle of predictive analytics and biometric monitoring, thereby ensuring that state security efforts do not override democratic values. To achieve this, policymakers must confront the systemic opacity of machine learning models that currently obstruct legal requirements for transparency and individual redress. Moreover, the implementation of routine audits and the adoption of explicit ethical standards are necessary to reduce algorithmic bias and ensure that automated systems do not disproportionately impact underrepresented populations. Establishing these accountability structures necessitates the creation of redress mechanisms that allow citizens to challenge automated decisions and seek remedies for potential rights violations. Member States must ensure that these remedies are accessible and effective, providing individuals with meaningful information regarding the role of AI systems in the justice and law enforcement sectors, particularly when these technologies influence decisions that significantly impact their lives. In this context, public participation should be formalized through mandatory, publicly accessible impact assessments that delineate the scope and methodology of any algorithmic tool implemented within the public sphere. Such frameworks must mandate clear lines of responsibility, ensuring that agencies remain accountable for outcomes generated by cybersecurity and surveillance solutions. Furthermore, introducing comprehensive safeguards for the explainability of data processing methods serves as a vital prerequisite for maintaining judicial independence, thereby preventing algorithmic outputs from circumventing existing oversight.

5 Chapter 5: Case Studies in Bangladesh

5.1 Rohingya crisis and surveillance

The humanitarian response and management of refugee settlements have increasingly incorporated biometric data collection and facial recognition technologies, raising significant concerns regarding the protection of vulnerable populations from potential data breaches and state-sponsored monitoring. These technologies, if repurposed for mass profiling, jeopardize the safety of asylum seekers and necessitate strict democratic control to prevent the weaponization of sensitive humanitarian data. Furthermore, the integration of these systems necessitates a robust legal framework that mandates transparency and independent oversight to mitigate the risks of automation bias and discriminatory algorithmic outcomes. Establishing such protections is particularly urgent given that the lack of institutional transparency in humanitarian data management can facilitate unauthorized surveillance, thereby infringing upon the fundamental right to privacy and human dignity of displaced persons, (B. A. Riswandi, 2025)³⁷. Consequently, policymakers must implement rigorous data minimization protocols and secure storage standards to ensure that humanitarian assistance remains distinct from security-oriented data harvesting (A. Y. Abdurakhmanov, 2025).³⁸ Moreover, adopting participatory governance models—wherein feedback from affected communities informs the design of oversight mechanisms—is vital to strengthening the legitimacy of digital infrastructure within these settlements. Institutionalizing these safeguards ensures that algorithmic interventions remain contestable, preventing the normalization of surveillance as a precondition for access to essential aid. Beyond the immediate context of refugee management, similar ethical quandaries emerge in the deployment of maritime security technologies, where the integration of AI-driven surveillance requires strict adherence to human-centric principles of accountability and transparency (Islam, 2024)³⁹. Given that technological safeguards often prove insufficient due to inherent structural flaws, it is imperative that policymakers prioritize

³⁷ Riswandi, B. A., Ahmed, S., Raghav, A., Singh, B., Sangal, A., Arora, M. K., Lal, S., & Chandra, S. (2025). Computational Intelligence in Human Rights Protection (pp. 31–42).

³⁸ Abdurakhmanov, A. Y., Boltayev, A., Urazmetov, M., & Ahmad, M. (2025). Civil Rights in the Age of AI (pp. 1–28).

³⁹ Islam, M. S. (2024). Maritime Security in a Technological Era: Addressing Challenges in Balancing Technology and Ethics. *Mersin University Journal of Maritime Faculty*, 6(1), 1–16.

robust regulatory frameworks over mere efficiency-driven deployments. Future legislative efforts must explicitly address the risks of “black box” algorithms, which prevent meaningful audits and obstruct the identification of discriminatory patterns within sensitive humanitarian datasets ((IOM), 2021)⁴⁰. Furthermore, the procurement of these proprietary systems from external vendors must be conditioned upon the disclosure of source logic to prevent the erosion of due process.

5.2 Media regulation and censorship.

The digitalization of media oversight has increasingly leveraged AI-driven content moderation tools to identify and restrict speech, often under the justification of maintaining social harmony and preventing the spread of misinformation. However, the lack of clearly defined criteria for automated flagging risks the arbitrary suppression of dissent, as algorithms often struggle to distinguish between legitimate political criticism and malicious disinformation, thereby creating a chilling effect on freedom of expression (Okonkwo, 2023)⁴¹. This systemic reliance on opaque moderation models allows state actors to leverage technological limitations to marginalize critical voices, effectively rendering them invisible within the digital public sphere. This phenomenon demonstrates how the lack of a human-centric oversight mechanism transforms neutral moderation into an instrument of state-sanctioned silencing, where values are implicitly shaped by the cognitive biases of the underlying programming. Consequently, the lack of transparency in these recommendation systems can amplify controversial content and distort public opinion, further shrinking the space for pluralistic discourse (Nuredin, 2023)⁴². To counter this trend, it is essential to mandate regular, independent audits of these moderation algorithms to expose embedded biases and ensure alignment with international human rights standards. Such proactive regulatory measures should be complemented by fostering collaborations between the state, academia, and civil society to establish a digital ecosystem that prioritizes public interest over opaque,

⁴⁰ Migration, I. O. for. (2021). World Migration Report 2022. In World Migration Report. Wiley.

⁴¹ 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.

⁴² Nuredin, A. (2023). The Legal Status Of Artificial Intelligence And The Violation Of Human Rights. *International Scientific Journal*

efficiency-driven algorithmic governance. By requiring developers to replace "black box" models with interpretable frameworks, regulators can ensure that algorithmic decisions remain subject to meaningful human review and consensus. Specifically, facilitating the disclosure of source codes to trusted, neutral experts remains a critical step for reconciling the protection of proprietary trade secrets with the fundamental necessity of due process and accountability. In this regard, aligning domestic legislation with international standards remains essential to ensure that algorithmic moderation does not function as an indiscriminate tool for prior censorship.

5.3 Digital activism and state monitoring.

The proliferation of automated surveillance tools has significantly increased the risks of pre-emptive monitoring for activists, whose digital footprint often makes them primary targets for state-sanctioned tracking. This systematic monitoring utilizes advanced predictive analytics to identify potential dissenters, effectively chilling participatory engagement and creating an environment where online advocacy is perceived as inherently subversive (Manitra, 2025)⁴³. This convergence of data harvesting and algorithmic profiling creates an atmosphere of pervasive insecurity, where the fear of reprisal compels individuals to engage in self-censorship to avoid being flagged by state security apparatuses. This dynamic is further exacerbated by the integration of biometric identification and pattern-recognition software, which enables real-time tracking of movement and association patterns at unprecedented scales. Such extensive data collection, often conducted without informed consent, fundamentally undermines the right to privacy and obscures the legal boundaries between legitimate public safety measures and unauthorized state intrusion. This shift toward predictive oversight necessitates a critical re-examination of whether such algorithmic interventions in the public domain are compatible with the international obligations to protect individual liberty. Moreover, the reliance on automated hash-matching and predictive machine learning to categorize user behavior often fails to account for the nuanced socio-political context inherent to local activism.

⁴³ Manitra, R. R. M. (2025). "Am I Being Silenced by a Machine?" AI-Driven Content Moderation and The Chilling Effect on Freedom of Expression. *Alauddin Law Development Journal*, 7(2), 109–125.

5.4 Corporate surveillance: Telecom and social media platforms.

These entities increasingly operate as intermediaries that manage vast repositories of user data, often facilitating state surveillance through opaque information-sharing agreements that lack sufficient judicial oversight. These private digital infrastructures essentially enable a regime of widespread surveillance where the absence of transparency and accountability safeguards exposes individuals to potential rights violations. This "private/public surveillance partnership" complicates the legal landscape, as commercial actors harvest extensive data—ranging from browsing history to geolocation—that is subsequently accessible to state authorities under the guise of national security. Such data-driven surveillance, frequently justified by security or counterterrorism mandates, often circumvents established privacy protections to facilitate intrusive user profiling and real-time monitoring (O. A. Ajala, 2024)⁴⁴. This entanglement between telecommunications providers and state security apparatuses facilitates the weaponization of metadata, transforming private commercial data into an expansive mechanism for political repression and the suppression of dissent (IONESCU, 2025). Furthermore, the commercialization of sophisticated surveillance technologies, often developed by private firms and exported to state entities, frequently bypasses the rigorous necessity and proportionality tests required by international human rights frameworks (A. Pūraitė, 2020)⁴⁵. These collaborative infrastructures effectively shift the burden of rights protection onto private intermediaries, which often lack the requisite legal mandate to challenge government data requests that threaten fundamental civil liberties (Kumari, 2026)⁴⁶. Consequently, the blurred line between corporate data management and state security mandates renders traditional mechanisms

⁴⁴ Ajala, O. A., Arinze, C. A., Ofodile, O. C., Okoye, C. C., & Daraojimba, O. D. (2024). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. *World Journal of Advanced Engineering Technology and Sciences*, 11(1), 294–300.

⁴⁵ Pūraitė, A., Adamonienė, R., & Žemeckė, A. (2020). Sustainable Digitalization in Public Institutions: Challenges for Human Rights. *European Journal of Sustainable Development*, 9(3), 91–91

⁴⁶ Kumari, Dr. R. (2026). Digital Age Human Rights: Privacy, Surveillance, and Global Governance. In Zenodo (CERN European Organization for Nuclear Research). European Organization for Nuclear Research.

of accountability insufficient, necessitating a robust legal framework that defines the limits of private-sector participation in surveillance (Ahammed, 2024)⁴⁷.

5.5 Implications for journalists, activists, and marginalized groups.

These vulnerable cohorts are increasingly subjected to targeted digital attacks, where the combination of metadata analysis and biometric surveillance facilitates the de-anonymization of protected sources and the erosion of digital safe havens (Cohen, 2017)⁴⁸. The normalization of this pervasive monitoring disproportionately targets dissenting voices, effectively constraining the democratic space by transforming the act of digital communication into a potential liability for the user (Teo, 2023)⁴⁹. This convergence of state-corporate monitoring enables authorities to resignify commercial data for security goals, transforming routine digital activity into evidence for pre-emptive legal or extra-legal action. Ultimately, this hybridisation of public and private surveillance undermines the collective capacity for assembly and free expression, as the distinction between state-sanctioned oversight and commercial data exploitation collapses. This legislative void encourages a climate where metadata and content are treated as interchangeable assets for state-sanctioned profiling, further distancing the digital experience from constitutional guarantees. Consequently, the international community has increasingly recognized the imperative for stricter export controls on surveillance technologies to prevent corporations from supplying repressive regimes with the infrastructure required for such systematic rights violations. Beyond these export constraints, there is an urgent need to establish domestic legal safeguards that explicitly prohibit the use of private sector data in criminal proceedings unless stringent judicial warrants are obtained. Without such regulatory recalibration, the consolidation of state and corporate power threatens to establish a permanent architecture of digital dominance that renders meaningful dissent impossible. Addressing this systemic

⁴⁷ Ahmed, M. W., & Ahammed, M. M. (2024). Human Rights and Technology: Exploring How Technological Advancements Impact Human Rights, Particularly in Surveillance and Data Collection. *International Journal of Arts and Humanities Studies*, 4(4), 19–27.

⁴⁸ Cohen, J. E. (2017). Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt. *Critical Analysis of Law*, 4(1)

⁴⁹ Teo, S. A. (2023). *Towards Human Rights 2.0? : A meta-theoretical analysis of the disruptions to human rights foundations by artificial intelligence*. Lund University Publications (Lund University)

challenge requires the implementation of a shared responsibility regime that holds both surveillance firms and state actors accountable for human rights violations under an international oversight framework. Such a framework must specifically address the proliferation of cyber-surveillance spyware, ensuring that multinational corporations face legal liability for facilitating abuses like arbitrary detention and privacy violations (Chan, 2019). Furthermore, drawing upon emerging regulatory models such as the European Commission's proposed Corporate Sustainability Due Diligence Directive, there is a clear impetus to compel firms to conduct rigorous human rights impact assessments, thereby institutionalizing corporate accountability for the technologies they deploy. By mandating such assessments, jurisdictions can begin to mitigate the "surveillance asymmetry of regulation," where transnational technology flows outpace the capacity of fragmented domestic legal systems to impose constitutional checks.

6 Chapter 6: Human Rights Implications & Reform Proposals

6.1 Impact on freedom of expression.

The pervasive nature of algorithmic surveillance creates a "chilling effect," where the constant threat of real-time monitoring compels individuals to engage in self-censorship to avoid potential repercussions. This environment of systemic opacity and algorithmic bias risks normalizing the erosion of civil liberties, as individuals alter their digital behavior to preempt state-sanctioned scrutiny. Such predictive monitoring mechanisms further exacerbate the power imbalance between the state and the individual, effectively transforming autonomous digital engagement into a landscape of constant, performative conformity. This shift undermines the fundamental presupposition of agency in digital environments, as the anticipation of surveillance overrides the user's capacity for authentic democratic participation (Kosta, 2020)⁵⁰. Moreover, the integration of artificial intelligence into state governance introduces complex challenges regarding algorithmic bias and discrimination, which necessitate a transition toward a more transparent and accountable regulatory framework. To address these challenges, policymakers should prioritize the harmonization of legal frameworks across jurisdictions to ensure consistent standards for algorithmic transparency and data protection, thereby safeguarding human rights against the discriminatory potential inherent in automated decision-making systems. Such efforts must emphasize the integration of human rights doctrine into the AI lifecycle to prevent the "supercharging" of existing socioeconomic inequalities through biased predictive modeling (Omotoso, 2025).⁵¹

⁵⁰ Kosta, E. (2020). Algorithmic state surveillance: Challenging the notion of agency in human rights. *Regulation & Governance*, 16(1), 212–224.

⁵¹ AHA, R., & OMOTOSO, S. (2025). THE HUMAN RIGHTS CRISIS IN AI DEVELOPMENT AND USE: DOES THE EUROPEAN FRAMEWORK PROVIDE AN ADEQUATE PROTECTION? *International Journal of Law Politics and Humanities Research*.

6.2 Chilling effect on journalism and activism.

The increasing deployment of sophisticated surveillance tools enables the real-time tracking of sensitive communications, which systematically undermines the confidentiality essential for investigative reporting and the protection of whistleblowers. This digital erosion of confidentiality effectively disincentivizes the disclosure of state misconduct, as the threat of automated surveillance facilitates the identification and potential persecution of critical sources. Furthermore, the normalization of such intrusion risks creating a permanent digital enclosure, where the technical capacity for state-led surveillance overrides the fundamental right to anonymity in political discourse. In this context, the integration of advanced machine learning systems introduces a "black box" effect that exacerbates the potential for illegal, arbitrary censorship and the degradation of information integrity (Wang, 2025)⁵². In this light, the deployment of artificial intelligence must be reconciled with international human rights law to prevent the complete erosion of privacy and autonomy in public spaces. To mitigate these systemic risks, it is imperative to implement robust ethical design principles and independent oversight mechanisms that prioritize the protection of individual data rights within the digital governance lifecycle.

6.3 Privacy vs. security debates.

The discourse surrounding these competing interests often posits national security as a justification for the expansion of mass surveillance, yet this frequently overlooks the foundational human rights requirements for necessity and proportionality (Krishnakumariamma, 2025)⁵³. The reliance on these justifications often obscures the long-term impact on democratic autonomy, necessitating a move toward global governance frameworks that center human dignity rather than solely state-driven efficiency (Metzger, 2019)⁵⁴. Moreover, the deployment of emotion recognition and

⁵² Wang, X. (2025). A Review of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *Journal of Politics and Law*, 18(4), 68–68.

⁵³ Kunjukrishnan, R. P., & Krishnakumariamma, S. (2025). Artificial Intelligence and Human Rights in the Era of Digital Governance: Exploring Promises and Challenges. *International Journal of Advances in Social Sciences and Humanities*, 4(2), 64–71.

⁵⁴ Donahoe, E., & Metzger, M. M. (2019). Artificial Intelligence and Human Rights. *Journal of Democracy*, 30(2), 115–126.

biometric analysis in urban environments further threatens to undermine human dignity and autonomy, extending surveillance into the very sphere of individual physical and behavioral integrity. In this context, the shift toward a "Panopticon society" reveals how the pursuit of urban security through ubiquitous data collection frequently prioritizes state control over the protection of individual privacy. Such oversight systems often suffer from a lack of technical expertise among designers, leading to ethical boundaries being compromised in favor of broad data aggregation. Furthermore, the pervasive integration of these technologies into smart infrastructure often bypasses existing individual information self-determination, centralizing control within opaque algorithmic systems that prioritize commercial and state utility over citizen protection (Esposito, 2024)⁵⁵.

6.4 Gendered and marginalized perspectives.

Algorithmic monitoring disproportionately affects vulnerable groups by embedding historical biases into automated systems, thereby intensifying existing socioeconomic disparities. These surveillance architectures often compromise spatially grounded rights, such as freedom of assembly and association, by disproportionately tracking marginalized populations within urban environments. This technological stratification facilitates predictive profiling and behavioral nudging, which effectively enforce social sorting that reinforces the systemic exclusion of these communities from equitable digital access. Consequently, the deployment of such technologies is frequently tested on low-income groups without robust checks and balances, effectively turning smart city infrastructure into a tool for the targeted marginalization of vulnerable populations. Such initiatives often neglect the broader sociopolitical contexts of urban life, ultimately curtailing opportunities for diverse civic perspectives and fostering a technocratic governance model that ignores historical disparities. Furthermore, the rise of "biocriminology" threatens to deepen these divisions by labeling certain demographics as inherently pathological based on opaque biometric signifiers. These discriminatory logics often reflect a broader "techno-solutionism," where complex

⁵⁵ Mantelero, A., & Esposito, M. S. (2024). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. arXiv (Cornell University).

social conflicts are reduced to computable problems that ignore the lived realities of equity-seeking communities (Pilo', 2023)⁵⁶.

6.5 Reform Proposals:

- Constitutional reforms (privacy rights). These mandates must explicitly codify the right to digital privacy and data sovereignty as fundamental protections against unwarranted state interference, thereby limiting the scope of pervasive surveillance technologies. Additionally, legislative bodies should establish legal frameworks that empower citizens to exert sovereignty over their metadata, including the adoption of tools for communication encryption and data obfuscation to counter the reach of surveillance capitalism (Makanadar, 2024)⁵⁷. Furthermore, these reforms should mandate the institutionalization of procedural justice in the implementation of smart technologies, ensuring inclusive decision-making processes that protect marginalized communities from being subjected to opaque data collection practices.
- Legislative reforms (Digital Security Act amendments). These measures should include the enactment of strict data protection laws that require proactive human rights impact assessments prior to the deployment of any municipal surveillance infrastructure, specifically addressing the risks of predictive profiling. Moreover, such legislation must mandate transparent algorithmic audits to dismantle the top-down, centralized implementation models that currently preclude meaningful citizen participation. Furthermore, such policies must advocate for technological sovereignty, enabling local communities to co-design infrastructure that reflects human-centric social values rather than merely optimizing for commercial or administrative extraction. Ultimately, these reformative efforts must acknowledge that smart city initiatives often absorb and reproduce the dominant cultural values of the existing political economy, necessitating a critical shift toward architectures that prioritize

⁵⁶ Jaffe, R., & Pilo', F. (2023). Security technology, urban prototyping, and the politics of failure. *UvA-DARE (University of Amsterdam)*, 54(1), 76–93.

⁵⁷ Makanadar, A. (2024). Digital surveillance capitalism and cities: data, democracy and activism. *Humanities and Social Sciences Communications*, 11(1).

community accountability over biopolitical management. This transition requires moving beyond technocratic "smart city" models that treat urban issues as apolitical, instead favoring deliberative, slow-governance frameworks that center citizen expertise and democratic legitimacy.

- Judicial activism (expanding interpretation of rights). Courts must increasingly serve as a bulwark against the erosion of fundamental rights by adopting an expansive interpretation of constitutional privacy that challenges the legality of invasive urban monitoring tools. By mandating that municipal authorities demonstrate the necessity and proportionality of surveillance measures, the judiciary can force a reconciliation between urban innovation and the preservation of anonymity. Additionally, establishing independent oversight bodies is critical to ensuring that the utilization of automated technologies remains subject to continuous review, thereby preventing the normalization of intrusive monitoring.
- Policy recommendations (transparency, accountability, oversight). Municipalities should prioritize the establishment of comprehensive data stewardship frameworks that clarify government responsibilities as both data platforms and regulatory authorities. These frameworks must require city departments to identify existing gaps in their privacy architectures, compelling an evaluation of the potential chilling effects that persistent data collection may exert on the exercise of public expression. In this context, it is imperative that local public authorities maintain firm control over policy initiatives, ensuring that the involvement of stakeholders—including citizens and local businesses—remains central to the deployment of technological solutions.
- International alignment (ICCPR, UN guidelines). Bangladesh should synchronize its digital governance with international human rights standards, such as the EU's General Data Protection Regulation, to establish rigorous accountability for smart city vendors and prevent the exploitation of citizens. By mandating that private sector providers adhere to these global benchmarks, the state can effectively mitigate the negative externalities associated with pervasive surveillance. Such alignment also necessitates a shift toward a justice-based, participatory framework that moves beyond symbolic compliance to ensure that human rights and democratic accountability remain central to the state's "Smart Bangladesh" vision. This approach necessitates the adoption of

privacy-enhancing technologies—such as anonymization, pseudonymization, and unlinkability—which must be fully tested and instantiated within their specific operational environments to guarantee their efficacy against data-driven threats. Furthermore, policymakers should implement data minimization strategies to ensure that the collection of citizen information is strictly limited to the operational requirements of essential public services.

7 Chapter 7: Conclusion

This concluding section synthesizes the preceding analysis to advocate for a human-centric approach to digital governance, emphasizing that the protection of fundamental rights must supersede the uncritical adoption of automated surveillance technologies. Rather than viewing technological innovation as an inevitability, policymakers must foster recursive engagement strategies that invite ongoing, multidisciplinary feedback to ensure that governance remains transparent, accountable, and aligned with international human rights norms. By centering human agency in the design process, the state can avoid the pitfalls of civic paternalism that often reduce citizen participation to mere symbolic gestures. Integrating these participatory mechanisms will enable the nation to transcend the current digital divide and cultivate a resilient infrastructure that respects individual dignity and autonomy. Ultimately, this paradigm shift serves to mitigate the systemic vulnerabilities inherent in smart city development, where developers often overlook human rights risks in favor of neoliberal, technology-centric objectives. By adopting a rights-based framework, Bangladesh can transform its digital landscape into an ecosystem that prioritizes sustainable development and the safeguarding of civil liberties (Hussain, 2024)⁵⁸. This evolution requires reconciling the recent legislative trajectory—marked by the Information and Communication Technology Act 2006 and the subsequent Cyber Security Act 2023—with constitutional mandates to ensure that digital expansion does not come at the cost of democratic discourse.

Moving forward, it is essential to prioritize a human-centric approach to cybersecurity that aligns technical security requirements with the proactive removal of structural vulnerabilities. Such a strategy must specifically address the heightened cyber-vulnerability inherent in retrofitting traditional infrastructure with smart technologies, ensuring that the integration of new systems does not exacerbate risks to privacy or civic security. Furthermore, local governance must integrate bottom-up, grassroots-led initiatives to prevent the imposition of externally-funded surveillance models that often bypass essential social inclusion criteria. To realize the “Smart Bangladesh” vision effectively, policymakers must ensure that data-driven progress does not compromise the security of the very citizens it intends to empower. Consequently, achieving this

⁵⁸ Hussain, A. (2024). Rethinking Human Rights in Digital Context: Bangladesh Perspective. *Journal of Dhaka International University*, 13(1).

balance requires the robust integration of cybersecurity resilience and transparency, ensuring that the transition to a smart nation does not inadvertently facilitate the erosion of civil liberties. Ultimately, the success of this transition depends on fostering a secure digital ecosystem that balances technical innovation with rigorous legal protections to uphold fundamental rights.

Bibliography

- (IOM), I. O. (2021). *World Migration Report 2022*. Wiley, for IOM.
- A. O. Aderibigbe, P. E. (2023). Artificial Intelligence in Developing Countries: Bridging the Gap Between Potential and Implementation. *Computer Science & IT Research Journal*,, 185–199.
- A. Pūraitė, R. A. (2020). Sustainable Digitalization in Public Institutions: Challenges for Human Rights. *European Journal of Sustainable Development*,, 91.
- A. Y. Abdurakhmanov, A. B. (2025). Civil Rights in the Age of AI. IGI Global.
- Ahammed, M. W. (2024). Human Rights and Technology: Exploring How Technological Advancements Impact Human Rights, Particularly in Surveillance and Data Collection. *International Journal of Arts and Humanities Studies*,, 19–27.
- AllahRakha., N. (2024). Constitutional Safeguards for Digital Rights and Privacy. *International Journal of Law and Policy*, 31–43.
- Anupam Gope, L. D. (2026). Evolving Cyber Governance and Human Rights in Bangladesh: From the Digital Security Act to the Cyber Security Ordinance, 2025. doi:10.5281/zenodo.18793146
- B. A. Riswandi, S. A. (2025). Computational Intelligence in Human Rights Protection. 31–42.
- Cheong., B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. *Frontiers in Human Dynamics*,.
- Cohen, J. E. (2017). Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt. *Critical Analysis of Law*.
- Dr. Abdullah-Al-Monzur Hussain, A. P. (2024). Rethinking Human Rights in Digital Context: Bangladesh Perspective. *Journal of Dhaka International University*, Vol. 13, Issue 1.

- Drovic, C. (2025). Surveillance Capitalism and the New Social Order: Rethinking Freedom in the Digital Age. *OTS Canadian Journal*,, 16.
- Dutt., R. T. (2026). Privacy vs. National Security: Balancing Surveillance and Data Protection in India. *International Journal for Multidisciplinary Research*,.
- Engelmann, A. G. (2023). Algorithmic transparency as a fundamental right in the democratic rule of law. *Brazilian Journal of Law, Technology and Innovation*, , 169–188.
- Esposito, A. M. (2024). An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA) in the Development of AI Data-Intensive Systems.
- F. S. Al Khasawneh, M. A. (2025). Governing Algorithms: The Intellectualization of Administrative Law and Emerging International-Law Constraints. *Veredas Do Direito: Direito Ambiental e Desenvolvimento Sustentável*,.
- Freitas, J. G. (2026). The challenges of AI regulation: data protection, civil rights, and landmark cases. *Frontiers in Political Science*,.
- H. Belayet, C. M. (2025). Evaluating the legal accountability of artificial intelligence (AI) in Bangladesh: beyond regulatory frameworks.
- Habibulloh, M. (2025). Digital Governance and the Right to Privacy: A Comparative Analysis of AI Regulation in Southeast Asia and the European Union. *Journal of Law, Policy and Global Development*, , 19–35.
- Haque, A. B. (2019). Need for Critical Cyber Defence, Security Strategy and Privacy Policy in Bangladesh – Hype or Reality? *International Journal of Managing Information Technology*,, 37–50.
- Hasan., A. R. (2023). Digital Security Act 2018: From the Lens of Investigative Journalism and Freedom of Expression. *Perspectives in Social Science*.
- Hussain, A. (2024). Rethinking Human Rights in Digital Context: Bangladesh Perspective. *Journal of Dhaka International University*.
- I. Researcher, T. G. (2026). Privacy and Data Protection in AI: A Comparative Analysis of EU and Indian Regulatory Frameworks. *International Journal of Social Science and Human Research*.

- Islam, M. S. (2024). Maritime Security in a Technological Era: Addressing Challenges in Balancing Technology and Ethics. *Mersin University Journal of Maritime Faculty*, 1–16.
- Islam., S. A. (2023). AI and the future of human rights in Bangladesh: a call for robust legal and ethical frameworks. *International Journal of Law and Information Technology*, Vol. 31, Issue 4, pp. 331–348.
- Isotalo., G. (2026). From Jurisprudence to Infrastructure: Algorithmic Governance and the Ontological Displacement of Law.
- Khalaileh., Y. (2023). Accommodating Artificial Intelligence in International Law: An Overview and New Frontier. *Journal of Human Security*, .
- Kosta, E. (2020). Algorithmic State Surveillance: Challenging the Notion of Agency in Human Rights. *Regulation & Governance*,, 212–224.
- Kouroutakis., A. E. (2024). Rule of law in the AI era: addressing accountability, and the digital divide. *Discover Artificial Intelligence*.
- Krishnakumariamma, R. P. (2025). Artificial Intelligence and Human Rights in the Era of Digital Governance: Exploring Promises and Challenges. *International Journal of Advances in Social Sciences and Humanities*, 64–71.
- Kumari, D. R. (2026). Digital Age Human Rights: Privacy, Surveillance, and Global Governance.
- M. Abraham, S. D. (2024). Asymmetric Surveillance Governance: A Thematic Analysis of Privacy, National Security, and AI Regulation in India. *Qubahan Political Journal*, .
- M. Huda, A. A. (2024). Legal Challenges in Regulating Artificial Intelligence: A Comparative Study of Privacy and Data Protection Laws. *nternational Journal of Social and Human*, 116–125.
- M. Kaur, N. S. (2026). Data Protection Laws and Privacy Rights in the Digital Age: Legal Challenges and Emerging Frameworks. *Indian Journal of Law*, 72–82.
- Makanadar, A. (2024). Digital Surveillance Capitalism and Cities: Data, Democracy and Activism. *Humanities and Social Sciences Communications*.

- Mallika, M. S. (2025). Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview. *International Journal of Research and Innovation in Social Science*, 3796–3811.
- Manitra, R. R. (2025). “Am I Being Silenced by a Machine?” AI-Driven Content Moderation and the Chilling Effect on Freedom of Expression. *Alauddin Law Development Journal*, 109–125.
- Matta., D. (2026). he Digital Social Contract: Protecting Identity in the Age of AI.
- Md. Z. Haq, Z. A.-R. (2025). GDPR and Bangladesh’s data privacy laws: a comprehensive analysis. *nternational Journal of Public Law and Policy*, 192–209.
- Metzger, E. D. (2019). Artificial Intelligence and Human Rights. *Journal of Democracy*, 115–126.
- Nuredin, A. (2023). The Legal Status of Artificial Intelligence and the Violation of Human Rights. *International Scientific Journal Sui Generis*,, 7–28.
- O. A. Ajala, C. A. (2024). Reviewing advancements in privacy-enhancing technologies for big data analytics in an era of increased surveillance. *World Journal of Advanced Engineering Technology and Sciences*, 294–300.
- O. Reis, N. E. (2024). Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences*, 73–88.
- 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*,, 222–238.
- Omotoso, R. A. (2025). The Human Rights Crisis in AI Development and Use: Does the European Framework Provide an Adequate Protection? *International Journal of Law Politics and Humanities Research*.
- P. Saha, A. S. (2026). When Data Protection Fails to Protect: Law, Power, and Postcolonial Governance in Bangladesh.
- Pilo’, R. J. (2023). Security Technology, Urban Prototyping, and the Politics of Failure. *Security Dialogue*,, 76–93.

- Rahman, A. (2025). The Dual State: Artificial Intelligence, Authoritarian Control, and the Crisis of Youth in Bangladesh (2014–2024).
- Rahman., A. (2025). The Dual State: Artificial Intelligence, Authoritarian Control, and the Crisis of Youth in Bangladesh (2014–2024).
- Shams, A. T. (2024). Dissent under Siege: Case Studies of Repression in the Digital Era of Bangladesh. *Advances in Journalism and Communication*, 207–230.
- Shams., A. T. (2024). Dissent under Siege: Case Studies of Repression in the Digital Era of Bangladesh. *Advances in Journalism and Communication*, .
- Singh, A. (2026). Right to Privacy and State Surveillance: Procedural Safeguards and Accountability. *International Journal of Criminal Common and Statutory Law*., 27–30.
- Singh, D. J. (2024). The Law of Right to Privacy in India: Protecting Privacy in the Digital Era: Challenges. *ShodhKosh Journal of Visual and Performing Arts*.
- Teo, S. A. (2023). Towards Human Rights 2.0? A Meta-Theoretical Analysis of the Disruptions to Human Rights Foundations by Artificial Intelligence.
- The Right to Privacy in the Digital Age: State Concerns and Initiatives in Bangladesh. (2025). *sian Journal of Social Sciences and Legal Studies*, 279–289.
- Vaishali. (2026). Algorithmic Governance Through Predictive Analytics: Legal Accountability and Decision-Making Challenges in India.
- Victor., L. O. (2025). Digital Identity Policy-Making in Africa. IGI Global.
- Wang, X. (2025). A Review of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. *ournal of Politics and Law*., 68.