Page 1047 - 1066 **DOI:** *https://doi.org/10.63108/IJLMH.13267*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Is AI Governing Us? A Deep Dive into the Regulatory Gaps in Bangladeshi AI Governance

TANJILA CHOWDHURY* AND ASSADEKA TABASSUM JAMAN**

ABSTRACT

Artificial intelligence (AI) is widespread throughout the world and is used, knowingly and unknowingly, because of the speed of its services. People live under an illusion about AI's advancement, which creates profound barriers to human security in the digital world, harms people in the real world and creates risks to fundamental human rights. In response to this risk, the European Union has adopted a significant regulatory model, Regulation (EU) 2024/1689 (the EU AI Act). The Act prohibits several AI practices, such as manipulation, and provides risk-based protection so that AI systems are transparent and accountable to people and governments. As a result, AI systems can be reconciled with human safety, security and the protection of fundamental rights. However, incidents of AI manipulation have occurred, including the violation of a child's right to life, and many other incidents are taking place, especially affecting vulnerable AI users, because many countries lack binding legal protection. Legislation on AI is not limited to technological innovation but also concerns human security, transparency and accountability. Bangladesh produced the draft National Artificial Intelligence Policy 2024 (NAIP) and later the National AI Policy 2026–2030 (Draft v2.0), which provides some important protections for human lives against AI manipulation, including data protection and cybersecurity, grounded in Bangladeshi culture. However, the policy focuses on public services, innovation and economic growth, primarily to fulfil the technological ambitions of Vision 2041 in line with the Sustainable Development Goals (SDGs). Consequently, human security and protection from AI remain an option rather than a primary goal among the policy's commitments. Not only Bangladesh but most South Asian countries lack protection for people, especially the vulnerable, against AI manipulation. This qualitative legal research therefore examines the adequacy of AI governance and enforcement in Bangladesh in protecting digital security and fundamental rights. Drawing comparative insights from the EU AI Act, it examines gaps in Bangladesh's digital legislation and institutional practice and identifies best practices. It also compares practice in the neighbouring countries of India and Pakistan to assess Bangladesh's position within South Asia's regional AI governance framework. Through a

* Author holds an LL.M. from the UNESCO Madanjeet Singh South Asian Institute of Advanced Legal and Human Rights Studies, University of Asia Pacific, Dhaka, Bangladesh. ORCID: https://orcid.org/0009-0006-5246-6293
** Author is a Legal Associate at Capital Law Chamber, Dhaka, Bangladesh.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

critical analysis of primary and secondary sources, it finds that Bangladesh and its neighbours have adopted policies but lack adequate protections and binding laws to govern AI systems, leaving people living blindfolded.

Keywords: *Artificial intelligence (AI), Human rights, AI governance, Algorithmic equality, Bangladesh*

I. INTRODUCTION

Artificial intelligence (AI) is expanding rapidly across the world, beyond the transnational boundaries of technical innovation, into day-to-day social, professional, economic, institutional and individual life.[1] These automated systems are used in matters that bear directly on people's lives, so AI can benefit people and harm them at the same time, and people everywhere now experience both the blessings and the curses of AI algorithms.[2] In Bangladesh, according to the Bangladesh Bureau of Statistics, 54.8% of households had internet access in 2025, and more than half of the population reaches the internet through smartphones, so a significant share of the population already uses AI products.[3] AI systems are not solely a matter of technology, and they should not be left unregulated, because they bear on human dignity, personal autonomy, equality and several other fundamental rights.[4] Not everyone is technologically literate enough to recognise discrimination and bias, and many fall into the loop and suffer afterwards. A 2024 report of the Bangladesh Bureau of Statistics and the United Nations Population Fund (UNFPA) found that nearly 89% of women who use social media in Bangladesh had experienced online violence at least once, and AI makes such abuse easier and faster to commit.[5]

Internationally, the UNESCO Recommendation on the Ethics of Artificial Intelligence and Regulation (EU) 2024/1689 (the EU AI Act) address AI systems through human rights protections and risk-based safeguards. The Fundamental Rights Impact Assessment (FRIA) required by the EU AI Act is a significant tool for measuring how far rights are protected and

---

[1] Teemu Birkstedt et al., *AI Governance: Themes, Knowledge Gaps and Future Agendas*, 33 INTERNET RESEARCH 133 (2023), https://doi.org/10.1108/INTR-01-2022-0042; Sameer Hinduja & Justin W. Patchin, *Risks and Harms of Conversational Artificial Intelligence (CAI) Chatbot Use Among US Youth*, 98 JOURNAL OF ADOLESCENCE 1597 (2026), https://doi.org/10.1002/jad.70164; Amna Batool, Didar Zowghi & Muneera Bano, *AI Governance: A Systematic Literature Review*, 5 AI AND ETHICS 3265 (2025), https://doi.org/10.1007/s43681-024-00653-w.

[2] Birkstedt et al., *supra* note 1; Batool, Zowghi & Bano, *supra* note 1; Hinduja & Patchin, *supra* note 1.

[3] INFO. & COMMC'N TECH. DIV., GOV'T OF BANGL., BANGLADESH NATIONAL AI POLICY 2026–2030 (DRAFT V2.0) §§ 1.1–1.2 (Feb. 9, 2026), https://aipolicy.gov.bd/docs/national-ai-policy-bangladesh-2026-2030-draft-v2.0.pdf [hereinafter NAIP V2.0].

[4] Batool, Zowghi & Bano, *supra* note 1.

[5] Hiren Pandit, *Comprehensive Efforts Needed to Counter TFGBV in Bangladesh*, ASIAN AGE (Bangl.) (June 26, 2026), https://dailyasianage.com/news/354066/comprehensive-efforts-needed-to-counter-tfgbv-in-bangladesh; *89% Women Face Online Abuse in Bangladesh: National Consultation Calls for Urgent Action*, UNITED NEWS OF BANGLADESH (Apr. 17, 2026), https://unb.com.bd/category/Bangladesh/89-women-face-online-abuse-in-bangladesh-national-consultation-calls-for-urgent-action/183853; NAIP V2.0, *supra* note 3, § 4.5.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

where they are left unprotected.[6] By contrast, Bangladesh's South Asian neighbours, India and Pakistan, have not enacted binding AI laws. This regional gap creates significant challenges for the protection of human rights.

Against this international and regional backdrop, Bangladesh began its AI governance with the draft National AI Policy 2024 (NAIP 2024), which did not regulate AI systems but offered guidance for commercial development in certain areas.[7] Two years later, another policy followed, the National AI Policy 2026–2030 (Draft v2.0) (NAIP V2.0), which addresses risks to people better than its predecessor.[8] However, chapters 1 and 2 of NAIP V2.0 emphasise economic growth and the development targets of Vision 2041, which, as a matter of policy, makes human rights a secondary concern at an urgent moment for AI governance.[9] Two years after the 2024 draft, a strict and binding law might have been expected; the optional approach to human rights in NAIP V2.0 leaves the position no better. Bangladesh's earlier digital laws were also used against online speech: Human Rights Watch documented 1,271 charge sheets filed by the police between 2013 and April 2018, most of them under section 57 of the Information and Communication Technology Act, 2006, and many of them against people who had criticised the government or political leaders.[10]

The question this paper asks is how far the inadequacy of AI governance in Bangladesh affects the protection of people's fundamental rights. It is a qualitative legal study of primary sources, namely international instruments, national statutes, rules, policies and guidelines, and of secondary literature. It first takes the EU AI Act as the best-practice benchmark and then compares the AI frameworks of India and Pakistan as regional and neighbouring practice. Using a three-tier theoretical framework, it assesses the state's accountability for protecting human rights, and finally it measures the adequacy and effectiveness of AI governance in Bangladesh against international and national frameworks. Vulnerable people, such as women, children and

---

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art. 27, O.J. L, 2024/1689 (July 12, 2024), https://eur-lex.europa.eu/eli/reg/2024/1689/oj [hereinafter EU AI Act]; Nathalie A. Smuha, *Regulation 2024/1689 of the Eur. Parl. & Council of June 13, 2024 (EU Artificial Intelligence Act)*, 64 INTERNATIONAL LEGAL MATERIALS 1234 (2025), https://doi.org/10.1017/ilm.2024.46.

[7] INFO. & COMMC'N TECH. DIV., GOV'T OF BANGL., NATIONAL ARTIFICIAL INTELLIGENCE POLICY 2024 (DRAFT) (2024) [hereinafter NAIP 2024]; *see also Govt Drafts AI Policy to Tap Its Potential, Tackle Concerns*, DAILY STAR (Bangl.) (July 9, 2024), https://www.thedailystar.net/business/news/govt-drafts-ai-policy-tap-its-potential-tackle-concerns-3653106.

[8] NAIP 2024, *supra* note 7; NAIP V2.0, *supra* note 3.

[9] NAIP V2.0, *supra* note 3, §§ 1.1, 2.1.

[10] HUMAN RIGHTS WATCH, NO PLACE FOR CRITICISM: BANGLADESH CRACKDOWN ON SOCIAL MEDIA COMMENTARY (2018), https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary.

those with little technological literacy, face the greatest challenges, and the gaps in the policy instruments examined here leave their rights the least protected.

II. AI GOVERNANCE: CONCEPTS AND MODELS

Governance of AI refers to the set of rules, practices, ethics, organisational roles and goals, and stakeholder interests aligned with legal frameworks.[11] It can be organised around a few specific questions: who is accountable, what is governed, when governance enters the AI lifecycle, and how laws are implemented through standards, audits and enforcement. These questions matter because AI systems are rapidly being adopted for decision-making in health care, public administration, education and digital finance.[12] In these sectors errors scale faster, and they affect rights, opportunities and access to services.

The literature identifies a stable normative core: fairness, transparency, accountability, explainability, privacy and trustworthiness.[13] These principles form the ethical foundation of governance; without them AI can become a means of discrimination and opaque decision-making, which in turn weakens human control.[14] AI decision-making can also reproduce existing social inequalities. Governance is, moreover, more developed at the level of principle than at the level of enforceable practice, and this leaves a wide gap between ethical expectations and real-world practice.

In practice, both hard law and soft law govern AI: soft law works through ethical guidelines, standards and voluntary frameworks, and hard law through regulation and legislation.[15] Soft law remains attractive because of its flexibility, but it carries weak enforceability and the risk of ethics washing, where stakeholders adopt ethical language without accepting binding obligations.[16] A central point of AI governance is that it must cover the whole AI lifecycle rather than only the expansion of AI.[17] Bias and harm can arise at every stage: when data are gathered,

[11] Birkstedt et al., *supra* note 1; Batool, Zowghi & Bano, *supra* note 1.
[12] Birkstedt et al., *supra* note 1; Batool, Zowghi & Bano, *supra* note 1.
[13] Hinduja & Patchin, *supra* note 1.
[14] Hinduja & Patchin, *supra* note 1.
[15] Birkstedt et al., *supra* note 1; Frederic Heymans & Rob Heyman, *Identifying Stakeholder Motivations in Normative AI Governance: A Systematic Literature Review for Research Guidance*, 6 DATA & POLICY e58 (2024), https://doi.org/10.1017/dap.2024.66.
[16] Heymans & Heyman, *supra* note 15; Batool, Zowghi & Bano, *supra* note 1.
[17] Ibrahim Habli, Tom Lawton & Zoe Porter, *Artificial Intelligence in Health Care: Accountability and Safety*, 98 BULLETIN OF THE WORLD HEALTH ORGANIZATION 251 (2020), https://doi.org/10.2471/BLT.19.237487; Birkstedt et al., *supra* note 1; Yingjie Wang, Matthew Wilchek & Feras A. Batarseh, *From Data to Policy: A Systematic Review of AI in Water Regulations and Compliance*, 9 NPJ CLEAN WATER art. 33 (2026), https://doi.org/10.1038/s41545-026-00555-w.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

when models are trained, when outputs are interpreted and when systems are used inside institutions.[18]

At present the EU AI Act is the most developed model. It follows a risk-based structure that prohibits harmful practices and imposes strict requirements on high-risk systems.[19] Yet risk classification does not fully answer questions of fairness, accountability and contextual suitability.[20] The EU AI Act is also designed as a complete governance system rather than a mere statute, with an AI Office, an AI Board, a scientific panel and national authorities implementing it across the member states.[21] The model matters because it is intended to shape regulation beyond Europe.

Of Bangladesh's neighbours, India has the more developed structure of AI governance, a development-oriented and sector-led model that emphasises innovation, infrastructure and economic growth rather than a single comprehensive law.[22] Pakistan has moved beyond general discussion to formal policy. Its National AI Policy 2025 has a stronger architecture than earlier soft-governance approaches, combining financing, centres of excellence, human-capital goals and an AI regulatory directorate with sectoral sandboxes.[23] Pakistan nonetheless lacks binding AI law, has weak data protection and has no risk-classification system.[24] This leaves people's rights exposed, especially the rights of those with little literacy in AI, cybersecurity and the internet.

Bangladesh lacks the implementation needed for effective AI regulation, and no binding framework has been established to give effect to the national policy.[25] This gap leaves citizens

---

[18] Habli, Lawton & Porter, *supra* note 17; Birkstedt et al., *supra* note 1; Wang, Wilchek & Batarseh, *supra* note 17.
[19] Oskar J. Gstrein, Noman Haleem & Andrej Zwitter, *General-Purpose AI Regulation and the European Union AI Act*, 13 INTERNET POLICY REVIEW, no. 3, 2024, https://doi.org/10.14763/2024.3.1790; Ceyhun Necati Pehlivan, *The EU Artificial Intelligence (AI) Act: An Introduction*, 5 GLOBAL PRIVACY LAW REVIEW 31 (2024), https://doi.org/10.54648/GPLR2024004.
[20] Gstrein, Haleem & Zwitter, *supra* note 19.
[21] Gstrein, Haleem & Zwitter, *supra* note 19.
[22] Divij Joshi, *AI Governance in India: Law, Policy and Political Economy*, 10 COMMUNICATION RESEARCH AND PRACTICE 328 (2024), https://doi.org/10.1080/22041451.2024.2346428; Avinash Agarwal & Manisha J. Nene, *A Federated Architecture for Sector-Led AI Governance: Lessons from India*, 20 TRANSFORMING GOVERNMENT: PEOPLE, PROCESS AND POLICY 1043 (2026), https://doi.org/10.1108/TG-09-2025-0310; Deepak Kumar & Chinmaya Kumar Sahu, *Artificial Intelligence Governance and Social Policy Divergence: A Comparative Political Economy Perspective on Global AI Regulation*, INTERNATIONAL JOURNAL OF SOCIOLOGY AND SOCIAL POLICY 1 (2026), https://doi.org/10.1108/IJSSP-02-2026-0129.
[23] Sohail Rao, *Pakistan's National AI Policy 2025: A Comparative Appraisal, Advantages, Risks, Execution Pathways, and Regional Benchmarks*, 1 INNOVAPATH 12 (2025), https://doi.org/10.63501/2P23R912; Muhammad Shahzad Basra, Muhammad Shoaib Jamil & Aisha Warraich, *The Brussels Effect, the EU AI Act, and Pakistan's AI Policy Choices: Aligning Global Market Access with Digital Sovereignty*, 4 RESEARCH JOURNAL FOR SOCIAL AFFAIRS 103 (2026), https://doi.org/10.71317/RJSA.003.06(A).0761.
[24] Basra, Jamil & Warraich, *supra* note 23.
[25] Tasmiah Tahsin Mayeesha, Farzana Islam & Nova Ahmed, *AI4Bangladesh: AI Ethics for Bangladesh: Challenges, Risks, Principles, and Suggestions*, *in* PROCEEDINGS OF THE 13TH INTERNATIONAL CONFERENCE ON INFORMATION & COMMUNICATION TECHNOLOGIES AND DEVELOPMENT 260 (2024), https://doi.org/10

exposed to serious AI-related harm and affects many of their human rights. The lack of accountability, together with algorithmic bias, leads to discrimination in equal treatment.[26] In particular, the lack of public accountability makes risk-scoring algorithms opaque, so that they can automate caste, class or gender bias.[27]

These shortcomings may affect human rights to a considerable extent, yet little disaggregated data from these countries is available. The countries lack precautions on the use of AI at both the institutional and the consumer end. They also lack remedies after harm, as no policy provides for accountability. This lack of access to justice may lead to violations of a range of rights, extending as far as the right to life. This paper therefore draws on predictable harms identified in studies from developed countries with robust, binding laws, and uses them to show how far such harms can affect countries that lack a legal framework for protection against AI.

III. Theoretical Framework

This paper uses a three-tier theoretical framework to examine the gravity of human rights violations caused by the lack of AI governance, especially unrestricted manipulation and data exploitation. Bangladesh is the main focus; regional developments in India and Pakistan are compared, with the EU AI Act as the normative benchmark. The framework links three theories: the human security approach associated with the United Nations Development Programme (UNDP); the capability approach of Amartya Sen and Martha Nussbaum; and Sandra Fredman's work on substantive equality together with Kimberlé Crenshaw's work on intersectionality.[28]

Human security theory forms the foundation of the framework. It was introduced in the UNDP's Human Development Report 1994 and developed by scholars such as Mary Kaldor.[29] It moves the object of security from state sovereignty to individual human dignity.[30] Applied to AI governance, human security provides the macro-level justification for state regulation: AI-

.1145/3700794.3700820.

[26] Mayeesha, Islam & Ahmed, *supra* note 25.

[27] Ruotong Wang, F. Maxwell Harper & Haiyi Zhu, *Factors Influencing Perceived Fairness in Algorithmic Decision-Making: Algorithm Outcomes, Development Procedures, and Individual Differences*, *in* Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems 1 (2020), https://doi.org/10.1145/3313831.3376813; Sejin Paik et al., *Who Benefits from AI? Examining Different Demographics' Fairness Perceptions Across Personal, Work, and Public Life*, 5 Discover Artificial Intelligence art. 39 (2025), https://doi.org/10.1007/s44163-025-00235-7.

[28] Kimberlé Crenshaw, *Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color*, 43 Stanford Law Review 1241 (1991), https://doi.org/10.2307/1229039; Amartya Sen, Development as Freedom (1999); Mary Kaldor, Human Security: Reflections on Globalization and Intervention (2007); Martha C. Nussbaum, Creating Capabilities: The Human Development Approach (2013); Sandra Fredman, *Substantive Equality Revisited*, 14 International Journal of Constitutional Law 712 (2016), https://doi.org/10.1093/icon/mow043.

[29] Kaldor, *supra* note 28.

[30] Kaldor, *supra* note 28.

driven behavioural manipulation and predatory profiling are not mere bugs but a breach of the state's affirmative duties towards citizens under international human rights law and under constitutional and domestic law. For instance, when an AI system manipulates consumers, it can induce psychological distress and may even lead to self-harm. Left ungoverned, such behaviour can violate the right to health and, eventually, the right to life. AI also creates opportunities to harvest data and to produce false information, which is inconsistent with the rights to privacy, to information and to freedom of expression.

Macro-level security must be made enforceable through binding legal guarantees, which is why it is supported by the second theory, the capability approach of Amartya Sen and Martha Nussbaum.[31] The approach can be read as a constitutional lens: it does not judge laws as they stand in the books but asks whether individuals are actually empowered to exercise their rights.[32] From this perspective, individuals' agency and mental competence are core constitutional goods that states must protect. AI systems undermine them by delivering biased and unequal information to different users and by compromising their integrity. "Conversion factors" in the capability approach describe a person's ability to turn resources into real opportunities.[33] Fragmented and biased information prevents that conversion and produces behavioural control instead, which violates the rights to dignity, to freedom of thought and conscience, and to civic participation.

The third tier is a socio-legal operational framework drawn from Sandra Fredman's multidimensional model of substantive equality and Kimberlé Crenshaw's theory of intersectionality.[34] The theory holds that treating all people identically can itself be a form of inequality.[35] South Asia has many pre-existing inequalities and forms of discrimination, and people in the region face structural differences such as unequal literacy, gender divisions and rural-urban gaps in access. For people already facing such disadvantages, unrestricted AI systems compound discrimination, and the harm grows with its gravity, in violation of the protection against discrimination. Crenshaw's intersectionality is also relevant to the differences between AI language models as they operate in countries such as Bangladesh, India and Pakistan and as they operate in Western jurisdictions.[36]

[31] SEN, *supra* note 28; NUSSBAUM, *supra* note 28.
[32] SEN, *supra* note 28.
[33] SEN, *supra* note 28; NUSSBAUM, *supra* note 28.
[34] Crenshaw, *supra* note 28; Fredman, *Substantive Equality Revisited*, *supra* note 28.
[35] Crenshaw, *supra* note 28.
[36] Crenshaw, *supra* note 28.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Bangladesh, India and Pakistan are gradually moving towards AI regulation, and all three have adopted or drafted AI policies. However, AI frameworks grounded in human security have yet to be enacted. Compact and robust AI legislation that protects human integrity is essential for the well-being, rights and security of people in these countries.

IV. International legal framework for the protection of human rights in the context of AI systems

The rapid integration of AI into social, economic and governmental decision-making has turned AI governance from a question of technology policy into an international human rights imperative. AI systems increasingly determine access to essential services such as information, employment, finance, healthcare, education, public services and political communication. State regulation therefore goes beyond technological innovation. Governance depends on safeguarding individuals from arbitrary interference, guarding against algorithmic discrimination and cognitive manipulation, and preventing the loss of human agency. This part examines the emerging international legal and normative framework governing AI, followed by a comparative analysis of the European Union (EU), India and Pakistan, so that rights-based approaches become visible and comparable for Bangladesh in assessing its own legislation and implementation.

A. International human rights framework for AI governance

AI governance is increasingly a human rights imperative rather than merely a matter of technological development. Although the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) predate contemporary AI systems, their principles provide a normative framework for regulating AI-driven practices. Together, these instruments set standards safeguarding life, security, privacy, equality, freedom, health and participation in scientific advancement. As a State Party to the ICCPR and the ICESCR, Bangladesh is obliged to take the legislative, administrative and other measures needed to protect and fulfil these rights.

Article 3 of the UDHR (life, liberty and security of person) and Article 6 of the ICCPR (the right to life) are relevant where AI creates foreseeable risks of serious physical or psychological harm.[37] The human security approach adopted in this paper accordingly treats high-risk AI not

[37] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 3 (Dec. 10, 1948) [hereinafter UDHR]; International Covenant on Civil and Political Rights art. 6, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

simply as a technological failure but as an actionable threat to human security.[38] The Human Rights Committee has recognised that the obligation of States Parties to respect and ensure the right to life extends to reasonably foreseeable threats and life-threatening situations, including deprivations of life caused by persons or entities whose conduct is not attributable to the State.[39] Bangladesh must therefore take preventive measures where AI systems risk exposing individuals, especially vulnerable users, to serious harm.

The right to privacy is likewise engaged by AI-driven data collection, behavioural profiling and automated inference. Article 12 of the UDHR and Article 17 of the ICCPR protect against arbitrary or unlawful interference with privacy.[40] Effective AI governance must therefore safeguard personal data and individual autonomy, and it must guarantee meaningful control over personal information and over automated processing. As a State Party to the ICCPR, Bangladesh must enact strong statutory and regulatory safeguards against interference through emerging technologies.

Substantive equality and non-discrimination are equally important, because algorithmic systems trained on biased or unrepresentative datasets risk entrenching structural inequalities in employment, education, welfare and public services.[41] The substantive equality and intersectionality approaches require attention to how AI applications disproportionately affect vulnerable groups.[42] Bangladesh is bound to ensure that technological growth does not worsen its existing socio-economic disparities. Compliance is also required because Article 19 of both the UDHR and the ICCPR protects freedom of opinion and expression, which AI influences significantly through algorithmic content curation, recommendation systems and behavioural manipulation.[43] Transparency, explainability and meaningful human oversight are therefore indispensable legal requirements. The ICESCR further ties AI governance to socio-economic rights such as the right to health, and it guarantees the right to enjoy the benefits of scientific progress (Articles 12 and 15).[44] This normative approach aligns with the capability approach, which asks whether individuals have genuine opportunities and agency in the face of

[38] KALDOR, *supra* note 28.
[39] Hum. Rts. Comm., General Comment No. 36 (2018) on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life, ¶ 7, U.N. Doc. CCPR/C/GC/36 (Sept. 3, 2019).
[40] UDHR, *supra* note 37, art. 12; ICCPR, *supra* note 37, art. 17.
[41] Crenshaw, *supra* note 28; SANDRA FREDMAN, DISCRIMINATION LAW (2d ed. 2011); Fredman, *Substantive Equality Revisited*, *supra* note 28.
[42] Crenshaw, *supra* note 28.
[43] UDHR, *supra* note 37, art. 19; ICCPR, *supra* note 37, art. 19.
[44] International Covenant on Economic, Social and Cultural Rights arts. 12, 15, Dec. 16, 1966, 993 U.N.T.S. 3 [hereinafter ICESCR].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

technological innovation.[45] Bangladesh is obliged to ensure that advances in AI do not create new barriers for vulnerable and marginalised groups.

Taking a narrower focus on individual rights, UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence sets out a global framework built on risk- and rights-based approaches that seek to secure human dignity and safety.[46] It gives particular content to privacy, equality and non-discrimination, transparency and accountability in relation to AI. NAIP V2.0 refers to internationally recognised ethical frameworks, including those advanced by UNESCO, and commits the government to adopt the values set out in the Recommendation on AI Ethics, a human-rights-centred step for future governance.[47]

B. International framework on artificial intelligence: the European Union as a rights-based benchmark

The European Union (EU) has a robust AI framework in Regulation (EU) 2024/1689, commonly known as the Artificial Intelligence Act (EU AI Act).[48] The EU AI Act aims to protect human rights and human security by prohibiting harmful practices and controlling risks.[49] Its rights-centred agenda seeks to make trustworthy AI systems available to the public. It does not prohibit all AI systems; rather, it works systematically and regulates specified systems.[50] This is a sound approach, under which rights such as freedom of movement, expression and opinion are protected, with reasonable restrictions on risky uses that may harm people or infringe the rights of others.

Article 5 of the EU AI Act is a significant rights-protective feature. It prohibits specified harmful AI practices involving manipulation, deception and the exploitation of vulnerabilities, including vulnerabilities due to age, disability or a specific social or economic situation, where significant harm is caused or is reasonably likely.[51] The provision explicitly recognises human autonomy and the position of vulnerable communities.[52] It also intersects with the human security risk-based approach and with substantive equality theory.[53] The EU links these ideas to risk management (Articles 6 and 9, on classification and risk management) and to strict data governance under Article 10, which requires training, validation and testing data to be relevant

[45] SEN, *supra* note 28; NUSSBAUM, *supra* note 28.
[46] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (Nov. 23, 2021), https://unesdoc.unesco.org/ark:/48223/pf0000381137.
[47] NAIP V2.0, *supra* note 3, §§ 1.3, 4.10.
[48] EU AI Act, *supra* note 6.
[49] Smuha, *supra* note 6.
[50] EU AI Act, *supra* note 6.
[51] EU AI Act art. 5(1)(a)–(b).
[52] EU AI Act art. 5.
[53] Crenshaw, *supra* note 28; KALDOR, *supra* note 28; Fredman, *Substantive Equality Revisited*, *supra* note 28.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

and sufficiently representative and to be examined for possible biases that may lead to discrimination.[54] The Act also keeps humans in control of major decisions made with AI: Article 14 requires human oversight of high-risk systems, which preserves human autonomy against algorithmic bias and allows people to exercise their judgement properly.[55]

Article 13 requires high-risk AI systems to be sufficiently transparent and to come with instructions for use, including information on their accuracy, which supports transparency and accountability.[56] The capability approach is relevant here as well, because governance of this kind protects human empowerment by giving people power over AI, and it prioritises that empowerment over algorithmic bias and state surveillance.[57] The Act also requires deployers of high-risk systems to attend to the outcomes they deliver, imposes disclosure duties and, for certain deployers, requires a Fundamental Rights Impact Assessment (Articles 26, 27 and 50).[58] It thus addresses risks before any harm occurs. These provisions reflect a governance system that prioritises its people and the protection of fundamental rights.

The EU AI Act also operates alongside other legislation rather than excluding or replacing it: it expressly does not affect the General Data Protection Regulation (Regulation (EU) 2016/679), so data protection law continues to apply to AI-related risks.[59] Even so, harms continue to surface in both the physical and the digital world. In the United States, a 14-year-old boy in Florida died by suicide in February 2024 after months of conversations with a Character.AI chatbot, according to a wrongful-death lawsuit filed by his mother in October 2024.[60] If harm of this kind occurs in technologically advanced jurisdictions, people with less protection in the digital world may suffer far more. Bangladesh needs comprehensive, sustainable and systemic protection for its people, with adaptable normative standards on manipulation, risk classification and, above all, human oversight. Bangladesh already has data protection and cybersecurity legislation, and alongside those laws it can govern AI systems and safeguard people's rights through the institutions that develop and deploy them.

---

[54] EU AI Act arts. 6, 9, 10.
[55] EU AI Act art. 14.
[56] EU AI Act art. 13.
[57] SEN, *supra* note 28; NUSSBAUM, *supra* note 28.
[58] EU AI Act arts. 26, 27, 50.
[59] EU AI Act art. 2(7).
[60] Angela Yang, *Lawsuit Claims Character.AI Is Responsible for Teen's Suicide*, NBC MIAMI (Oct. 23, 2024), https://www.nbcmiami.com/news/national-international/lawsuit-claims-character-ai-is-responsible-for-teens-suicide/3453420/; *see also* Van-Han-Alex Chung, Pénélope Bernier & Alexandre Hudon, *Mass Media Narratives of Psychiatric Adverse Events Associated With Generative AI Chatbots: Rapid Scoping Review*, 13 JMIR MENTAL HEALTH e93040 (2026), https://doi.org/10.2196/93040.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

C. The better neighbour for Bangladesh to follow: a comparison between India and Pakistan in AI governance

India follows a sectoral and discovery-based approach to governance, reflected in the Digital Personal Data Protection Act, 2023 (DPDP Act), and has no comprehensive AI-specific law. The DPDP Act acts as a shield through data protection: it requires consent from users and reasonable security safeguards, and it gives children special protection through verifiable parental consent (sections 6, 8 and 9).[61] These provisions affect AI systems that rely on behavioural profiling, personal data and automated personalisation. The Ministry of Electronics and Information Technology (MeitY) has since notified the Digital Personal Data Protection Rules, 2025, which implement the DPDP Act, and it has issued the India AI Governance Guidelines, 2025, which set out a human-centric, technology-agnostic framework anchored in seven guiding principles (sutras).[62] India thus shows how privacy, data protection and child protection can be integrated into existing digital legislation without a standalone AI Act. Importantly, India does not adopt the EU model: the Guidelines conclude that a separate AI law is not needed at this stage, rely on existing laws, and were shaped through public consultation and committee review.[63] These measures are, however, sometimes treated as ethical and self-regulatory rather than as legal, rights-based solutions, which leaves a gap between policy and practice.[64]

Pakistan, on the other hand, goes a step further with a policy-driven, institution-based approach. Its National Artificial Intelligence Policy 2025 promises ethical AI with commitments on privacy, human rights, fairness, transparency and literacy.[65] The policy introduces administrative mechanisms such as an AI Regulatory Directorate, a National AI Fund, Centres of Excellence and regulatory sandboxes. However, it remains soft law and does not constitute a comprehensive binding AI statute. Pakistan also lacks an enacted general personal data protection law, as the Personal Data Protection Bill, 2023 has not been passed.[66] Pakistan has the Prevention of Electronic Crimes Act, 2016 (PECA), which criminalises cybercrimes and

---

[61] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023, §§ 6, 8, 9 (India), https://www.meity.gov.in/content/digital-personal-data-protection-act-2023 [hereinafter DPDP Act].

[62] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) (Nov. 13, 2025) (India); MINISTRY OF ELECS. & INFO. TECH., GOV'T OF INDIA, INDIA AI GOVERNANCE GUIDELINES: ENABLING SAFE AND TRUSTED AI INNOVATION (2025) [hereinafter India AI Governance Guidelines]; Press Release, Press Info. Bureau, MeitY Unveils India AI Governance Guidelines under IndiaAI Mission (Nov. 5, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2186639.

[63] India AI Governance Guidelines, *supra* note 62.

[64] Joshi, *supra* note 22.

[65] MINISTRY OF INFO. TECH. & TELECOMM., GOV'T OF PAK., NATIONAL ARTIFICIAL INTELLIGENCE POLICY 2025 (2025).

[66] Personal Data Protection Bill, 2023 (Pak.) (Ministry of Info. Tech. & Telecomm.).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

certain online harms,[67] but PECA does not regulate AI-related decision-making or prohibit algorithmic discrimination. Pakistan therefore shows a gap between policy recognition and enforceable safeguards, particularly on privacy, transparency, institutional oversight and effective remedies. Bangladesh can nonetheless learn from its institutional models for AI governance.

The comparison shows that neither South Asian model provides a complete solution to Bangladesh's AI governance challenges. Bangladesh can, however, adopt some mechanisms from each according to its own circumstances. India's existing framework could be made stricter for AI, as it still relies mainly on data protection law, while Pakistan's focus is sharper in establishing institutional policies and bodies. From these, Bangladesh can see how comprehensive a policy can be, even without a specific AI law, in setting out how a government protects people's rights with institutional transparency and accountability. This paper concludes that both India and Pakistan should follow the principles of the EU AI Act to create a coherent legal system for AI, while building on their own cultural and structural foundations. Similar legislative action in India, Pakistan and Bangladesh may help resolve regional and jurisdictional conflicts in cyberspace.

V. National Legal Framework: Protection of Human Rights in the Era of Artificial Intelligence

Drawing on the benchmark and on the comparison of India and Pakistan, this part examines the national legal framework for AI. Bangladesh is a party to the core international human rights treaties and has committed itself to human rights and fundamental freedoms since its independence in 1971. Under the fundamental rights guaranteed by the Constitution of Bangladesh, the Government of Bangladesh has pursued several technological initiatives and, to regulate and develop the AI sector, has produced the draft National Artificial Intelligence Policy 2024 and then the National AI Policy 2026–2030 (Draft v2.0).[68] Despite these policies and the wider digital framework, Bangladesh lacks a binding statute on AI. This part identifies the legal gaps in Bangladesh's AI framework and the obstacles to securing AI-related rights.

A. Constitutional rights to protect human rights against AI

The Constitution of Bangladesh is the supreme law, and all laws and policies are subject to it. Article 11, in Part II (Fundamental Principles of State Policy), declares that the Republic shall

[67] Prevention of Electronic Crimes Act, 2016, Act No. XL of 2016 (Pak.), https://www.na.gov.pk/uploads/documents/1470910659_707.pdf.
[68] NAIP 2024, *supra* note 7; NAIP V2.0, *supra* note 3.

be a democracy in which fundamental human rights and freedoms and respect for the dignity and worth of the human person shall be guaranteed. Part III (Fundamental Rights) guarantees equality before the law (article 27), protection against discrimination (article 28), protection of the right to life and personal liberty (article 32), the prohibition of forced labour (article 34) and freedom of thought, conscience and speech (article 39).[69] These rights apply equally in the digital space, and their violation there is unconstitutional.

The capability approach reinforces this, because it places on the state a responsibility to enable individuals to act on their own choices.[70] Substantive equality requires rights to be secured according to people's needs; otherwise the result is discrimination.[71] The state must therefore secure these fundamental and other constitutional rights equitably, since discrimination deepens with each violation. Under human security theory, the state must also protect people from foreseeable risks.[72] Intersectionality ties these strands together in requiring equality among people in the digital space as well.[73] People in Bangladesh therefore need protection in the digital space from algorithmic and automated discrimination, behavioural manipulation, gender-based violence and violence against vulnerable groups carried out through AI systems.

B. Policy evolution of artificial intelligence and statutory gaps

Within the framework of rights guaranteed by the Constitution, the Government of Bangladesh has adopted various laws and policies. For the development of technology, the Information and Communication Technology (ICT) Division prepared the draft National Artificial Intelligence Policy 2024.[74] For an emerging digital space, the policy might have been expected to secure personal data and security and to prohibit AI manipulation that treats people inequitably. Even developed countries with robust laws were facing many challenges from AI, but the dangers of AI in Bangladesh received little attention because there was little research on them. Although NAIP 2024 reads like an AI governance policy, it was designed mainly to promote economic development and commercialisation through AI in areas such as agriculture, public administration and education.[75]

In February 2026 the ICT Division published the extended policy, the National AI Policy 2026 –2030 (Draft v2.0) (NAIP V2.0), which includes human security provisions addressing

[69] BANGL. CONST. arts. 11, 27, 28, 32, 34, 39, http://bdlaws.minlaw.gov.bd/act-367.html.
[70] SEN, *supra* note 28; NUSSBAUM, *supra* note 28.
[71] Fredman, *Substantive Equality Revisited*, *supra* note 28.
[72] KALDOR, *supra* note 28.
[73] Crenshaw, *supra* note 28.
[74] NAIP 2024, *supra* note 7.
[75] NAIP 2024, *supra* note 7.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

algorithmic harms.[76] Section 4.5 of NAIP V2.0 provides for accountability measures against disinformation, online harassment and AI-manipulated media.[77] It strictly prohibits creating, sharing or distributing sexualised, abusive or compromising AI-generated media without consent, a common form of technology-facilitated gender-based violence (TFGBV).[78] It also prohibits AI deepfakes portraying minors in any sexual or exploitative form and the use of AI media to harass, blackmail or intimidate women or minors.[79] Section 4.6 sets out a rights-based framework for automated decision-making, giving individuals a right to an explanation and to human review of decisions that affect them.[80] Sections 4.9 and 4.11 direct the government to develop a risk management framework for existing and future AI use and to establish a liability and redress framework, with strict liability for high-risk systems.[81]

Despite these positive features, the policy has major loopholes. The primary objective of NAIP V2.0 remains the same as that of NAIP 2024: macroeconomic commercialisation, industrial capacity-building and digital sovereignty.[82] Sections 1.1 and 2.1 of NAIP V2.0 present AI as an engine for achieving the Sustainable Development Goals (SDGs) and for Bangladesh's path towards middle-income status under the Vision 2041 plan.[83] By valuing commercial gain and market expansion, the policy treats human rights as an option rather than as a fundamental and non-negotiable requirement.

This commercial emphasis disadvantages people already harmed under Bangladesh's statutory landscape, in which earlier laws gave priority to state control over individual rights. Section 57 of the Information and Communication Technology Act, 2006 penalised the electronic publication of material deemed false and obscene, defamatory, likely to harm the image of the state or likely to hurt religious belief, and it was widely used to prosecute online expression, including criticism of the government, until it was repealed by the Digital Security Act, 2018.[84] People in Bangladesh have thus experienced restrictions on digital expression for a long time. NAIP V2.0 relies on other digital-space instruments, such as the Personal Data Protection Ordinance, 2025 and the Cyber Security Ordinance, 2025, and this dependence makes the whole

[76] NAIP V2.0, *supra* note 3.
[77] NAIP V2.0, *supra* note 3, § 4.5.
[78] NAIP V2.0, *supra* note 3, § 4.5.
[79] NAIP V2.0, *supra* note 3, § 4.5.
[80] NAIP V2.0, *supra* note 3, § 4.6.
[81] NAIP V2.0, *supra* note 3, §§ 4.9, 4.11.
[82] NAIP 2024, *supra* note 7; NAIP V2.0, *supra* note 3.
[83] NAIP V2.0, *supra* note 3, §§ 1.1, 2.1.
[84] Information and Communication Technology Act, 2006, § 57 (Act No. 39 of 2006) (Bangl.), *repealed by* Digital Security Act, 2018, § 61(1) (Act No. 46 of 2018) (Bangl.); HUMAN RIGHTS WATCH, *supra* note 10.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

framework vulnerable.[85] According to the Bangladesh Bureau of Statistics, as cited in NAIP V2.0, 54.8% of households in Bangladesh had internet access in 2025, and the people in them remain unprotected in the digital space.[86] This should be a priority for the government. Long-standing restrictions on digital expression already burden these users, and reforms that prioritise commercialisation within a long-term plan risk compounding that disadvantage.

Policies are advisory and laws are obligatory, so the uncertain protection offered by policy leaves digital rights hard to secure, and that inaccessibility brings multiple forms of discrimination with it. Section 7.5 of NAIP V2.0 provides that the Ministry of Law, Justice and Parliamentary Affairs shall initiate the drafting of a comprehensive Artificial Intelligence Act by 2028.[87] Until then, people are left with non-binding executive policy, which cannot provide judicial remedies or impose binding duties on technology actors.

C. Challenges faced by Bangladeshi people in AI incidents

Because there is no binding law and the AI Act is delayed, people, especially vulnerable people, are directly exposed to serious algorithmic harms across gender, class and geography. Recognising and addressing these harms is difficult because of the lack of socio-legal research and because digital victimisation has severe offline consequences. In Bangladesh in particular, empirical data on AI incidents are inadequate. In the 2023 Oxford Insights AI Readiness Index, Bangladesh ranked 82nd in the world, reflecting significant gaps in research and in institutional technological capacity.[88] Bangladesh has historically focused on the technical implementation of machine learning, while socio-legal questions such as human rights impact, algorithmic bias and ethical governance were left out of academic work.[89] This neglect also helps explain why Bangladesh has been slow to legislate and to address the true scale of algorithmic discrimination.

Developed states have enacted AI-related laws to protect human rights, yet many AI-related incidents still occur there, so Bangladesh must take account of the results of unregulated AI in other jurisdictions. Worldwide, the use of generative AI to create deepfake pornography has become a recognised form of technology-facilitated abuse, and its victims suffer anxiety and

[85] NAIP V2.0, *supra* note 3, § 4.1; Personal Data Protection Ordinance, 2025 (Ordinance No. 61 of 2025) (Bangl.); Cyber Security Ordinance, 2025 (Bangl.) (gazetted May 21, 2025).
[86] NAIP V2.0, *supra* note 3, § 1.1.
[87] NAIP V2.0, *supra* note 3, § 7.5.
[88] Sharifa Sultana et al., *Bangladesh's AI Readiness: Perspectives from the Academia, Industry, and Government*, *in* EXTENDED ABSTRACTS OF THE 2026 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1 (2026), https://doi.org/10.1145/3772363.3798581.
[89] Sultana et al., *supra* note 88.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

depression.[90] The problem arises in cyberspace, but its effects reach into real life. In South Korea, a highly digitised country, deepfake sexual images of women and girls, generated with AI and shared in Telegram chatrooms, targeted more than 500 schools and universities in 2024, many of the victims were believed to be under 16, and fear spread among teenage girls and young women across the country.[91] The harm does not stay online: victims also suffer humiliation in real life.

The crisis is growing in Bangladesh, where AI is increasingly used to create deepfake images and videos for image-based abuse.[92] According to a 2024 report of the Bangladesh Bureau of Statistics and UNFPA, nearly 89% of women who use social media in Bangladesh have experienced online violence at least once.[93] The report shows the urgency of regulating for a safe digital space. A NETZ Bangladesh study found that over 78% of Bangladeshi women have experienced some form of technology-based abuse in their lifetime.[94] In 2024 alone, the Police Cyber Support for Women (PCSW) received more than 60,000 complaints, most of them involving doxxing, the hacking of social media accounts and blackmail.[95] AI makes such offences easier to commit: freely available generative AI tools can turn a simple photograph into explicit content, and deepfakes spread faster than they can be removed.[96] Victims suffer anxiety, depression, job loss and withdrawal from education, and some die by suicide.[97] This evidence understates the reality, as many victims do not report. Still, it shows how unregulated systems affect many fundamental rights, with women especially vulnerable. The lack of data from affected people compounds the inaccessibility of rights: no data disaggregated by gender, age or race has been found that would identify the groups most affected by particular harms and most in need of attention. Against this pattern of exploitation, the absence of binding law leaves individuals exposed to systematic discrimination.

---

[90] Amith Kumar Malaker, *We Must Tackle Digital Violence to Fight Gender Inequality*, DAILY STAR (Bangl.) (Nov. 25, 2025), https://www.thedailystar.net/opinion/news/we-must-tackle-digital-violence-fight-gender-inequality-4042721.

[91] Jean Mackenzie & Leehyun Choi, *Inside the Deepfake Porn Crisis Engulfing Korean Schools*, BBC NEWS (Sept. 3, 2024), https://www.bbc.com/news/articles/cpdlpj9zn9go.

[92] Pandit, *supra* note 5.

[93] Pandit, *supra* note 5; *89% Women Face Online Abuse*, *supra* note 5.

[94] Malaker, *supra* note 90.

[95] Pandit, *supra* note 5; Surja Mandal, *Defeating Digital Violence Against Women Requires a Unified Front*, DAILY STAR (Bangl.) (July 29, 2026), https://www.thedailystar.net/opinion/news/defeating-digital-violence-against-women-requires-unified-front-4235041.

[96] NAIP V2.0, *supra* note 3, § 4.5; Pandit, *supra* note 5; Malaker, *supra* note 90.

[97] Malaker, *supra* note 90.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

VI. FINDINGS

This paper finds that, because AI governance in Bangladesh is inadequate, people face systematic barriers in securing their fundamental rights. AI is approached through ethics rather than rights, so people are not protected from its harms by mandatory rules. There is a fundamental gap between national policy goals, their implementation and the constitutional protection of fundamental rights such as equality, non-discrimination, freedom of thought and expression, and even the right to life.

International frameworks show the importance of binding statutory law rather than non-binding executive policy. The EU AI Act is the clearest benchmark: a binding, risk-based framework centred on human rights, with provisions on non-discrimination, data governance and human oversight, Fundamental Rights Impact Assessments, and an express relationship with existing data protection law.

This paper has also examined two neighbouring countries, India and Pakistan, and found significant gaps in both, as in Bangladesh. India has folded AI governance into existing data protection law and guidelines, and Pakistan has adopted a separate AI policy built around institutional capacity, but neither has a binding, rights-centred AI law. Given their economic diversity and early stage of development, each country needs dedicated legislation suited to its own context, so that people face fewer harms and can live with equality despite long-standing inequalities.

In Bangladesh, the national framework shows a persistent pattern of prioritising commercial development, with risk-based protections and fundamental rights treated as optional. NAIP 2024 concentrated on the use of AI in education, public administration and agriculture for economic development and said little about AI bias, algorithmic harm or mechanisms for managing risks to people. NAIP V2.0, published by the ICT Division two years later, again opens in chapters 1 and 2 with economic growth, industrial capacity and Vision 2041, although it adds protections against algorithmic bias and discrimination and for women, children and vulnerable groups. Those protections remain less developed than the commercial agenda. Meanwhile the harms are real: nearly 89% of women who use social media in Bangladesh have experienced online violence at least once,[98] and AI makes doxxing, deepfakes and fabricated content easier and faster to produce. Most people are not technologically literate enough to protect themselves from algorithmic bias or to protect their data unless the state regulates the institutions that build and deploy AI. TFGBV causes psychological trauma, social stigma and

[98] Pandit, *supra* note 5; *89% Women Face Online Abuse*, *supra* note 5.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

suicide attempts, and manipulated or biased AI outputs produce discrimination online and offline, engaging rights guaranteed by the Constitution. No disaggregated data on victims has been found, and it falls to the state to collect it. NAIP V2.0 envisages only that the drafting of an AI Act will begin by 2028, a delay that may allow further violations in a country where rights in the digital space, including data protection, have long been weakly protected. With these shortcomings in the policy instruments, people are left blindfolded by the ribbon of economic development.

VII. Recommendations

The governance of AI is not merely an ethical matter; it bears directly on fundamental human rights. International guidelines and the Constitution of Bangladesh both call for human rights guarantees to be secured through legislation where necessary. The present challenges make the case for a strict, robust law urgent, and the 2028 timeframe in NAIP V2.0 for beginning to draft one is too long to wait. In a new AI law, the government should prioritise human security and safety, data protection, freedom from algorithmic bias, and strict protection against deepfakes and doxxing, supported by the institutions that run AI systems. The AI Act should follow the core principles of the EU AI Act and the UNESCO Recommendation on the Ethics of AI, with a specific mandate for Fundamental Rights Impact Assessments (FRIAs). It should interlock with existing technology laws so that no loopholes remain in people's rights. Women, children and other vulnerable groups should be prioritised specifically and explicitly. As a developing country, Bangladesh may face many loopholes and sources of harm from weak or vague laws, and these deserve particular care. For accountability and transparency, the government should publish complaints and their resolution regularly and release disaggregated data at regular intervals. Finally, given the lack of socio-legal research on AI, researchers should examine the existing gaps regularly, and the government should encourage them to do so. With these measures, people can secure their human rights in relation to AI systems and have a safer digital world.

VIII. Conclusion

This paper has examined the inadequacy and fragility of Bangladesh's AI governance framework and its effects on people's lives. Despite broad constitutional protections, the absence of AI governance leaves fundamental rights exposed to AI malfunction, which is also inconsistent with international human rights standards. AI systems create algorithmic biases that produce inequality, and deepfakes and data harvesting threaten people's rights to information and to freedom of expression. Both policies, NAIP 2024 and NAIP V2.0, fail to

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

prioritise human rights over commercialisation. Neighbouring countries are attempting to address AI governance, yet they too lack protections against risks to people and against AI malfunction. The EU AI Act and the UNESCO Recommendation on the Ethics of AI establish a benchmark to follow. Because delay in securing rights is itself a denial of them, it is high time for Bangladesh to enact an AI Act that protects human rights and closes the long-standing gaps in the protection of its people's rights.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]