

Artificial Intelligence and Legal Reform in Bangladesh: Evaluating the Cyber Protection Ordinance, 2025

Zulfiquar Ahmed¹

¹*Department of Law, Faculty of Law, Rajshahi University, Rajshahi-6205, Bangladesh*

Abstract: This article examines the regulatory challenges posed by artificial intelligence in Bangladesh, with a critical focus on the Cyber Protection Ordinance, 2025. Using a hybrid doctrinal method, the study traces digital law's evolution from the ICT Act 2006 to CPO 2025, examining how the current framework addresses AI challenges such as accountability, automation, and rights protection within a rights-based constitutional framework. It identifies significant doctrinal gaps in the CPO especially in the absence of a functional or risk-based definition of AI, insufficient liability attribution mechanisms, and lack of enforceable ethical safeguards. The article also considers soft law instruments like the National AI Policy 2024 (Draft), AI Readiness Report 2025, and the National AI Strategy. It finds that although CPO 2025 marks progress, it lacks sufficient normative depth and institutional support for effective AI governance. By incorporating case studies of AI misuse (e.g., deepfakes, algorithmic bias in public services) and constitutional analysis (Articles 27, 31, and 39), the article situates Bangladesh's challenges within both domestic and global contexts. The article contributes to AI legal learning by offering concrete reform proposals to ensure a human-centric, rights-based regulatory regime aligned with global standards.

Keywords: *Artificial Intelligence (AI); Cyber Protection Ordinance; Cyber Statutes; AI-Based Offences; AI Accountability*

Introduction: The growing integration of artificial intelligence into social, administrative, and legal infrastructures has prompted an urgent reevaluation of existing legal frameworks. This part introduces the foundational premises of this article, which seeks to analyze the capacity of Bangladesh's newly enacted Cyber Protection Ordinance, 2025 (herein CPO, 2025), to regulate artificial intelligence in light of past legislative instruments and emerging international best practices. Drawing on both historical-comparative and normative-prescriptive doctrinal methods, the article outlines key challenges and frames the inquiry within the broader discourse on digital rights, governance, and AI ethics.

The proliferation of artificial intelligence systems capable of performing tasks that typically require human intelligence, such as reasoning, decision-making, and learning has transformed the landscape of legal, ethical, and regulatory discourse worldwide. Artificial Intelligence (AI), particularly in the form of large language models (LLMs) [1,2,3], autonomous systems, and algorithmic decision-making tools, is no longer a futuristic abstraction but an embedded reality across sectors such as finance, healthcare, governance, and national security [4]. In response, legal systems globally are grappling with how to design frameworks that both enable innovation and mitigate harms, including those to privacy, equity, autonomy, and due process [5]. The urgency to regulate AI arises from its increasing capability to act autonomously, make decisions that affect legal rights, and challenge existing norms of liability, agency, and jurisdiction [6]. The European Union's AI Act (2024) and the OECD's AI Principles (2019) offer seminal international benchmarks, aiming to guide responsible AI governance [7]. Yet, despite such global efforts, jurisdictions like Bangladesh face unique socio-legal challenges in integrating AI into their legal frameworks due to institutional, technological, and normative constraints.

Bangladesh's rapid digital transformation is underpinned by its long-standing policy trajectory from "Digital Bangladesh" to "Smart Bangladesh". Anchored in Vision 2041, the government's objective is to harness AI as a critical enabler of inclusive development, public service delivery, and industrial competitiveness [8]. The National Artificial Intelligence Policy 2024 (Draft), the AI Readiness Assessment Report (2025), and the National Strategy for Artificial Intelligence collectively articulate a roadmap for the development and deployment of AI systems across various domains. However, the absence of a comprehensive AI-specific legal framework has led to increasing tensions between technological advancement and legal safeguards. The discontinuity and inadequacy of earlier cyber legislation, such as the ICT Act, 2006, the Digital Security Act, 2018 (repealed), and the Cyber Security Act, 2023 (repealed), underscore the need for doctrinally robust, ethically grounded, and technologically adaptive legal reform.

As artificial intelligence continues to transform society, there is a growing focus on ensuring that this revolutionary technology is governed by law, regulation, human rights, ethics, and policy, providing the first comprehensive analysis of Europe's pioneering approach to AI regulation [9]. Despite the government's commitment to digital governance, the current legal infrastructure remains underdeveloped in addressing the normative and operational challenges posed by AI [10]. The recently promulgated

Article history:

Received: 11 June 2025

Received in revised form: 27 August 2025

Accepted: 23 September 2025

Available online: 15 December 2025

Corresponding author details: Dr. Zulfiquar Ahmed

E-mail address: zulfiquarcyberlaw@ru.ac.bd

Tel: +8801712534626

Copyright © 2025 BAUET, all rights reserved

Cyber Protection Ordinance (CPO), 2025, while a significant step forward, lacks explicit provisions to regulate artificial intelligence, algorithmic accountability, or ethical oversight mechanisms [11]. The key research questions guiding this article are:

- i. How have Bangladesh's cyber laws evolved in addressing AI-related risks and responsibilities?
- ii. Does the *CPO 2025* adequately capture the emerging challenges posed by artificial intelligence?
- iii. What normative principles and global best practices should inform Bangladesh's regulatory future for AI?

Literature Review:

Introducing the Cyber Protection Ordinance, 2025: The Cyber Protection Ordinance, 2025, promulgated on 21 May 2025, repealed the Cyber Security Act, 2023, in response to widespread criticism regarding its potential misuse and its failure to protect fundamental rights. The CPO introduces more refined definitions, including references to AI systems, large language models, and autonomous software agents. While it expands institutional capabilities and introduces new enforcement mechanisms, its silence on AI-specific liability [12], algorithmic discrimination, and human rights oversight reveals substantive doctrinal gaps.

Defining “Artificial intelligence” and Their Implications for Law and Society: Artificial intelligence is quite a difficult concept to unify [13]. For the purpose of this article, “artificial intelligence” refers to AI-driven systems capable of autonomous decision-making, adaptive learning, and predictive analytics ranging from chatbots and recommendation systems to autonomous drones and predictive policing tools [14]. The World Intellectual Property Organization (WIPO) defines artificial intelligence, “Artificial intelligence (AI)” is a discipline of computer science that is aimed at developing machines and systems that can carry out tasks considered to require human intelligence, with limited or no human intervention” [15]. As AI becomes embedded in judicial, administrative, and economic infrastructures, it raises critical questions about rule of law, equality before law, and the very nature of legal personhood. The assimilation of AI into legal practice presents both opportunities and challenges in the justice system [16]. However, these proliferations also raise critical questions about the role of human judgment, the protection of fundamental rights, and the need for regulatory frameworks that can keep pace with technological innovation [17]. Despite growing reliance on AI, Bangladesh's legal framework lacks a clear, consistent definition of “artificial intelligence.” The CPO 2025 introduces terms such as “AI software agent” and “large language models,” but these remain undefined or doctrinally underdeveloped. A Bangladesh-specific legal definition is needed, combining functionality (autonomous decision-making, adaptive learning) with a risk-based approach (e.g., high-risk AI in healthcare or predictive policing, low-risk AI in customer service). This would reduce ambiguity in liability and enforcement.

The Importance of Legal Regulation in the Age of AI: Legal scholars agree that the unregulated development and deployment of AI could exacerbate systemic bias, reduce transparency, and endanger democratic accountability [18]. AI is swiftly transforming the world, including the legal system [19]. Bangladesh's context is particularly vulnerable, given its infrastructural asymmetries, digital literacy gaps, and nascent data protection regime [20]. The theoretical review of the ethical insinuations of AI, as autonomous and with manipulating power in its impact on freedoms and human rights in the legal system, critically aims to evaluating the developing relationship between artificial intelligence and the law should also be considered a problem that the development of AI may violate freedoms and human rights [21]. What are the key ethical and legal challenges issued by the practicing AI technologies in the justice system and how should digital security statutes address them to reduce the negative impact on justice system in Bangladesh? However, with these encroachments originated a congregation of multifaceted legal challenges, from algorithmic bias, human rights and privacy anxieties to questions of liability and accountability for AI-driven decisions [22].

AI, Algorithms, and Discrimination: With the increasing concern that artificial intelligence could undermine fundamental rights, and ethics [23]; international bodies such as the UN, along with domestic human rights institutions and NGOs, are playing a greater role in safeguarding human rights in a future shaped by advanced AI systems. Scholars studying AI's impact on human rights warn that these technologies may replicate or even intensify existing human biases, thereby heightening the risk of discrimination [24].

Theoretical and Methodological Framework: By adopting a hybrid doctrinal approach grounded in comparative and normative analysis in assessing both statutory texts and soft-law instruments relevant to the governance of artificial intelligence. This article investigates the evolution, structure, and efficacy of AI regulation in Bangladesh's legal landscape by the analytical and methodological scaffolding in the followings:

The Legal Doctrinal Method: Forms and Application: The doctrinal method, sometimes referred to as “black-letter law” research, involves the systematic exposition, interpretation, and evaluation of legal rules, principles, and institutions. It primarily draws upon authoritative legal sources such as statutes, case law, and commentaries to determine the current state of the law and propose normative developments [25]. In the context of AI regulation, the doctrinal method allows legal scholars to interpret how emerging technologies are treated within pre-existing and evolving legal instruments—highlighting doctrinal gaps, ambiguities, and necessary reforms.

Historical-Comparative Doctrinal Method: Rationale and Tools: This sub-method traces the progression of Bangladesh's cyber legal framework across multiple legislative epochs (from the ICT Act, 2006 to CPO 2025): the Information and Communication Technology Act, 2006, the (repealed) Digital Security Act, 2018 (DSA), the (repealed) Cyber Security Act, 2023 (CSA), and the newly promulgated Cyber Protection Ordinance, 2025 (CPO).

Comparative legal analysis of legislative intent, rights-based safeguards, definitional expansions, and institutional arrangements, enriched with a SWOT Grid and Conflict Mapping tools, allows this article to:

- Chart doctrinal continuity or rupture (e.g., from ICT Act's vague enforcement to CPO's data-focused approach);
- Compare how each statute addresses key issues such as AI, data privacy, digital autonomy, and state surveillance;
- Evaluate shifts in judicial interpretation, e.g., Didarul Islam Bhuiyan Case, Jhumon Das Apon Case, Md Ruhul Amin Case, Pritom Das Case, Shanto Banik Case, Khadijatul Kubra Case, Lutfur Rahman Case, Imtiaz Ahmed Case and Mamunur Rashid Nomani Case, which criticized vague language, unclear provisions, presence of controversial sections, bizarre pattern, simply repackaging repressive provisions in cyber statutes. The inclusion of landmark cases demonstrate how Bangladeshi courts have grappled with vague statutory language and the absence of clear AI liability.
- The analysis is bolstered by global comparators such as the EU AI Act (2024) and India's Digital Personal Data Protection Act (2023).

Normative-Prescriptive Doctrinal Method: Purpose and Normative Evaluation: This normative-prescriptive analysis involves assessing the CPO 2025 against global benchmarks such as the EU AI Act (2024) and UNESCO's AI Ethics (2021), while proposing doctrinal reforms to strengthen transparency, proportionality, and due process [26]; with proposing doctrinal reforms in line with instruments like the UNESCO Recommendation on the Ethics of Artificial Intelligence [27].

Policy-Integrated Doctrinal Reading: Treating AI Strategy as Soft Law: The doctrinal method is supplemented by reading national policy instruments as quasi-normative legal materials. These include:

- Contextually interprets national policy documents such as the National AI Policy 2024 (Draft), AI Readiness Report (2025), and National Strategy for AI (2019-2024).
- Treats these instruments as quasi-normative guides to inform statutory interpretation and legislative development.

These texts, though not binding law, shape legislative intention, administrative action, and judicial interpretation. Their integration provides a contextual, governance-oriented understanding of how the legal system prepares for and conceptualizes AI regulation.

In combination, this methodology ensures an interdisciplinary, critically evaluative, and future-oriented engagement with the legal regulation of artificial intelligence in Bangladesh.

Justification for Choosing a Doctrinal Approach for This Research: The doctrinal method is most suitable for this research for the following reasons:

- It enables in-depth analysis of textual legal instruments (e.g., CPO, CSA, DSA, ICT Act);
- It supports evaluative critique grounded in legal principles and statutory interpretation;
- It bridges law and technology by assessing how emerging innovations are treated by written law;
- It aligns with the objective to propose doctrinally coherent and constitutionally sound reforms.

Research Design and Source Hierarchy: This research follows a hierarchical prioritization of sources, consistent with legal doctrinal rigour. Primary sources include statutory instruments such as the ICT Act 2006, the Digital Security Act 2018, the Cyber Security Act 2023, and the Cyber Protection Ordinance 2025, alongside case law from the DLR, BLD, and HCD/SCD jurisdictions. International legal standards such as the EU AI Act (2024), the UNESCO Recommendation on the Ethics of AI (2021), and the OECD AI Principles (2019) are also foundational to the analysis. Secondary sources comprise scholarly articles, doctrinal commentaries, and national policy documents including the AI Readiness Assessment 2025, the Draft National AI Policy 2024, and the National Strategy for AI. Together, these sources frame the doctrinal analysis within a constitutional, ethical, and policy-driven context essential for regulating AI in Bangladesh.

The Legal Adequacy Matrix, SWOC Grid, and Conflict Mapping developed in this study highlight the strengths and weaknesses of existing statutes in managing AI-related risks. Preliminary findings suggest that the ICT Act 2006 lacked specificity and enforcement mechanisms; the DSA 2018 was overly punitive and vague, leading to constitutional concerns as reflected in cases like *Dr. Shahidul Alam vs. State* (2019) [28]; *Anis Hossain Prodhan vs. State* (2020) [29]; the CSA 2023, though reformist in intent, was criticized for operational opacity [30]; and the CPO 2025, while progressive in institutional structuring, remains doctrinally silent on AI ethics and oversight. The article engages with judicial precedents more systematically. In *Didarul Islam Bhuiyan*, the court's reluctance to extend liability to autonomous systems reflects judicial caution toward AI agency; whereas in *Jhumon Das Apon* case, judicial activism indirectly addressed AI-related speech and surveillance concerns. Together, these cases reveal the judiciary's emerging but fragmented role in shaping AI governance in the absence of clear statutory guidance.

Legislative Evolution of Cyber Law in Bangladesh (2006–2025): This part critically analyzes the legislative trajectory of cyber law in Bangladesh over two decades, highlighting the evolving regulatory responses to technological developments, especially the advent of artificial intelligence. Through a doctrinal lens, it maps the transformation from foundational digital governance laws to the more nuanced, security-focused, and rights-sensitive Cyber Protection Ordinance (CPO), 2025.

ICT Act, 2006: Early Cyber Regulatory Attempts and Its Gaps: The Information and Communication Technology Act, 2006 marked Bangladesh’s first major legislative step toward digital governance. It sought to enable e-commerce, electronic signatures, and digital evidence [31]. However, it was drafted in an era when AI was not a practical concern and thus lacked provisions on emerging technologies, data protection, or algorithmic accountability. Section 57 of the Act, which criminalized online content deemed “offensive” [32] was widely criticized for its vagueness and potential misuse [33]. At least 1,271 people were reported to have been charged under Section 57 of the ICT Act before its repeal in 2018 [34]. Judicial challenges to Section 57, 63 and 66 such as *Md. Sujon Miah vs. The State*, *Alam Kiron vs. The State*, *A.P.M. Tushar vs. The State*, *Md. Anis Hossain Prodhan vs. The State*, *Anuj Chandra Majhee vs. The State*, *Sumon Mia vs. The State*, *Most. Sirajam Munira vs. The State*, *Munshi Nazrul Islam Sujan vs. The State*, and *Md. Mizanur Rahman vs. The State* [35], underscored how vague cyber provisions clashed with constitutional guarantees of free expression and due process. This demonstrated the judiciary’s early role in attempting to balance state power with rights protections [36].

Table 1. SWOT Analysis Table: ICT Act 2006.

Strengths	Weaknesses	Opportunities	Threats
Introduced legal foundation for e-governance	Lacked clarity on AI and cybersecurity	Scope for early digital law evolution	Vulnerable to misuse due to vague definitions

Table 2. Conflict Mapping: ICT Act 2006.

Conflict Source	Stakeholders Involved	Legal Issue	Outcome
Section 57 interpretation	Citizens vs. State	Ambiguity in defining offensive content	Judicial intervention and criticism

These visual frameworks serve to critically dissect the ICT Act’s doctrinal performance. The SWOT Grid and Conflict Mapping tools contextualize why and how the ICT Act failed to adequately anticipate or respond to the demands of intelligent systems and digital rights.

Digital Security Act, 2018: Over-criminalization and Cyber Surveillance: The Digital Security Act (DSA), 2018, aimed to replace the ICT Act’s controversial provisions. Section 57 has been cleverly divided into sections 25, 28, 29 and 31 of the DSA, 2018. For example, section 28 doesn’t have a clear and precise definition of crime which is a scope of being misused to criminalize free expression. There are even sections that limit expressions protected by international law, while others define additional broad restrictions by the most problematic sections are 8, 21, 25, 28, 29, 31, 32, 43 and 53. While it expanded the state’s capacity to address cyber threats, the DSA drew criticism from civil society and international observers for enabling over-criminalization and digital surveillance [37]. Sections 21–32 enabled sweeping powers of arrest for online speech. From September 2018 until January 2023, over 7,001 cases were filed under Bangladesh’s Digital Security Act (DSA) before its repeal [38]. The High Court, in *Arafat Hosen Khan v. Bangladesh* [39], questioned the proportionality of these provisions, showing an early attempt by the judiciary to apply constitutional principles to cyber law.

Table 3. SWOT Analysis: DSA 2018.

Strengths	Weaknesses	Opportunities	Threats
Expanded cybercrime definitions	Enabled overreach and censorship	Public discourse on digital rights	Undermined freedom of expression

Table 4. Conflict Mapping: DSA 2018.

Conflict Source	Stakeholders Involved	Legal Issue	Outcome
Section 29-32 enforcement	Journalists, Activists vs. Law Enforcement	Censorship and arbitrary arrest	Widespread protests and legal review

These tools help capture the DSA’s controversial enforcement history and policy failures. The SWOT Grid highlights imbalances between digital security goals and civil liberties, while Conflict Mapping outlines high-profile confrontations between the law and freedom of expression. This structured evaluation clarifies why the DSA failed to establish sustainable legitimacy and paved the way for legal reform. Yet, the Act remained silent on AI, algorithmic decision-making, or digital rights in the age of intelligent systems. This omission left future gaps in regulating emerging challenges like AI-enabled surveillance and algorithmic profiling.

Cyber Security Act, 2023: Transitional Reform and Repeal: The Cyber Security Act (CSA), 2023 aimed to refine the DSA’s harshest provisions. It introduced better definitional clarity and some safeguards. Despite these improvements, the CSA remained doctrinally weak in addressing AI liability, algorithmic accountability, or autonomous systems. It was repealed in 2025 following criticism of continued rights violations. Cases such as *Didarul Islam Bhuiyan* highlighted judicial unease with ambiguous cyber provisions, but courts did not yet develop doctrines addressing AI-driven harms or liability attribution.

Table 5. SWOT Analysis: CSA 2023.

Strengths	Weaknesses	Opportunities	Threats
Improved definitions and safeguards	Lacked independence of oversight bodies	Pathway to reform DSA flaws	Still prone to misuse due to weak enforcement

Table 6. Conflict Mapping: CSA 2023.

Conflict Source	Stakeholders Involved	Legal Issue	Outcome
Institutional Overlap	Government agencies vs. Civil Liberties Advocates	Ambiguous roles of enforcement agencies	Increased demand for repeal and rights-based reform

This structured analysis reveals the transitional character of the CSA. The SWOT Grid diagnoses both its corrective strengths and institutional deficiencies. The Conflict Mapping exposes recurring governance tensions and underscores the limited societal acceptance of the Act, which ultimately contributed to its repeal.

Cyber Protection Ordinance (CPO), 2025:

A Rights-Based Legislative Turn: The CPO, 2025 represents a deliberate attempt to integrate rights protections (Articles 27, 31, and 39 of the Constitution) while addressing cyber threats. It introduced terms such as “AI software agent” and “large language models,” marking Bangladesh’s first statutory reference to AI [40]. However, the Ordinance does not establish a functional or risk-based AI definition, nor does it specify liability frameworks for harm caused by autonomous systems. Nevertheless, it lacks AI-specific liability frameworks and oversight mechanisms for algorithmic decision-making.

Legislative Motivations and Democratic Concerns: The repeal of the CSA 2023 and the enactment of the CPO 2025 were motivated by both public pressure and democratic imperatives. The government cited the CSA’s failure to protect fundamental rights and its vague implementation guidelines [41]. The CPO aims to restore public trust by aligning digital governance with constitutional protections under Articles 27, 31, and 39 of the Constitution of Bangladesh [42]. While the CPO 2025 acknowledges Articles 27, 31, and 39 of the Constitution, its rights-based grounding remains insufficient. Article 27 (equality before law) is implicated when algorithmic bias leads to discriminatory outcomes in public service delivery; Article 31 (protection of law) raises concerns in cases where opaque AI systems undermine due process; and Article 39 (freedom of expression) is challenged by AI-generated disinformation and deepfakes. Deepfake misuse may be happened in political campaigns, non-consensual pornography, sparking public outrage, etc. [43].

Table 7. SWOT Analysis: CPO 2025.

Strengths	Weaknesses	Opportunities	Threats
Incorporates AI-specific language	Absence of ethical oversight	Opportunity for AI governance leadership	Need for algorithmic accountability and implementation

Table 8. Conflict Mapping: CPO 2025.

Conflict Source	Stakeholders Involved	Legal Issue	Outcome
AI regulation omission	Civil society, tech community vs. Lawmakers	Absence of AI liability or audit systems	Subject of legal and policy reform advocacy

These tools illustrate both promise and pressure surrounding the CPO 2025. Conflict Mapping shows ongoing tension between civil society’s demand for AI accountability and the legislature’s cautious, incomplete provisions. This dual assessment reveals that while CPO is doctrinally promising, it remains normatively incomplete.

Continuity and Disruption: Mapping the Legislative Trajectory: The legislative transformation from the ICT Act to the CPO reflects a complex interplay of continuity and disruption. The table below presents a Legal Adequacy Matrix comparing the four major statutes:

Table 9. Legal Adequacy Matrix Comparing Four Major Statutes.

Criteria	ICT Act 2006	DSA 2018	CSA 2023	CPO 2025
AI-Specific Provisions	✗	✗	✗	✓ (Partially)
Rights Safeguards	✗	✗	✓ (Limited)	✓✓
Institutional Oversight	✗	✓	✓	✓✓
Alignment with Intl. Norms	✗	✗	✓	✓✓
Procedural Clarity	✗	✗	✓	✓✓

This Legal Adequacy Matrix shows a clear pattern emerges across these laws: continuity in vague, enforcement-heavy provisions (ICT Act, DSA, CSA), and disruption in 2025 with CPO’s partial shift toward rights-based AI recognition. Yet, this disruption is incomplete: while AI is mentioned in statutory language, doctrinal clarity, accountability mechanisms, and enforceable rights remain absent. By visualizing these legal benchmarks, the matrix offers clarity on how far Bangladesh has progressed—and where it must still evolve in achieving a balanced, future-ready AI regulatory regime.

Alignment with Constitutional and International Human Rights Norms: The CPO 2025 makes a more deliberate effort to comply with national and international rights frameworks. Its language reflects compatibility with instruments such as the Universal Declaration of Human Rights, the UN Guiding Principles on Business and Human Rights, and the EU AI Act (2024). However, it remains silent on the ethical implications of AI deployment in law enforcement, predictive policing, and data-driven public administration. As such, the Ordinance would benefit from incorporating guidelines from the UNESCO Recommendation on the Ethics of Artificial Intelligence [44].

Table 10. Legal Adequacy Matrix: Human Rights Compatibility.

Legal Instrument	Freedom of Expression	Right to Privacy	Due Process	AI-Specific Human Rights Provisions
ICT Act 2006	X	X	X	X
DSA 2018	X	X	X	X
CSA 2023	✓ (Partial)	✓ (Limited)	✓	X
CPO 2025	✓✓	✓✓	✓✓	✓ (General Principles)

The Legal Adequacy Matrix assesses the extent of compliance with core human rights standards. The CPO attempts to align with human rights obligations (freedom of expression, privacy, due process).

Table 11. SWOT Analysis: Human Rights Alignment under CPO 2025.

Strengths	Weaknesses	Opportunities	Threats
Aligns with major human rights instruments	Lack of specific AI rights protection	Integrate UNESCO AI Ethics and UNGP	Operationalization in law enforcement and tech governance

Table 12. Conflict Mapping: Rights vs. Regulation in AI.

Conflict Source	Stakeholders Involved	Legal Issue	Outcome
Predictive Policing Tools	Citizens, Human Rights Orgs vs. Government	Use of AI without consent or transparency	Risk of future litigation and policy amendment

The legal matrices and visual tools in this section capture the evolving relationship between digital regulation and rights protection in Bangladesh. The SWOT Grid and Conflict Mapping expose implementation gaps and areas for reform. These instruments underscore the critical importance of grounding AI laws in constitutional and global human rights principles. However, without explicit safeguards for AI-driven surveillance (e.g., facial recognition, predictive policing), these constitutional promises risk remaining rhetorical rather than operational. By contrast, the EU AI Act (2024) and UNESCO AI Ethics (2021) embed enforceable principles of fairness, transparency, and human oversight. Bangladesh’s failure to codify similar protections highlights its lag in doctrinal readiness.

Legal and Doctrinal Challenges in Regulating Artificial Intelligence under CPO 2025: It delves into the doctrinal and operational challenges that arise in regulating artificial intelligence (AI) under the Cyber Protection Ordinance (CPO), 2025. Using a combination of statutory interpretation, doctrinal analysis, and comparative legal review, it identifies definitional ambiguities, legal gaps, enforcement limitations, and rights-based concerns embedded in the CPO’s treatment of AI technologies. The analysis engages with national and global frameworks and incorporates evidence-based legal tools, such as Legal Adequacy Matrices and SWOT Grids.

Legal Definition and Recognition of Artificial Intelligence under CPO 2025:

Defining “Artificial Intelligence” in Law: Conceptual and Doctrinal Barriers: Despite the increasing reliance on AI in both public and private sectors, Bangladesh’s legal landscape lacks a clear, consistent definition of “artificial intelligence.” The CPO 2025 introduces references to “AI software agents” and “large language models,” but these remain undefined or underdeveloped [45] Globally, legal systems have struggled with defining AI due to its evolving, interdisciplinary nature [46] As a result, legal uncertainty persists around agency, autonomy, and liability.

CPO 2025 and AI-Related Definitions: Section 2 of the CPO defines terms such as “AI software agent,” “large language models,” “digital device,” and “service provider.” However, these terms are not comprehensively integrated into the operational provisions of the Ordinance. This definitional shortfall mirrors similar issues seen in early cyber laws, such as the ICT Act 2006 and DSA 2018.

Provisions Directly or Indirectly Regulating AI Tools and Systems: The CPO 2025 addresses artificial intelligence agent or tools directly through provisions on data breaches, digital surveillance, and cyber manipulation under sections 17, 18, 21 & 25 of the CPO, 2025.

- **Section 17 of CPO, 2025:** Illegal Access or Hacking into Critical Information Infrastructure, etc. by the user of artificial intelligence tools and generation of new data through an artificial intelligence agent causing harm by any means is regulated under section 17 of CPO, 2025;
- **Section 18 of CPO, 2025:** Illegal Access to Computer, Digital Devices, Computer Systems, etc. by generating new data through an artificial intelligence agent is directly regulated under section 18 of CPO, 2025.
- **Section 21 of CPO, 2025:** Forgery in Cyber Space by a person or artificial intelligence agent to manipulate input or output of any computer or digital device, or to delete, alter, conceal data or programs, or to operate faulty data, programs, systems, or networks; or to generate or alter digital signatures, documents, or electronic files; or to create or manipulate digital money, electronic currency, or cryptocurrency; or to operate mobile banking using SIM cards registered under another person’s national identity; or to engage in hundi (informal money transfer) operations or run gambling portals without legal authority or beyond granted authority is directly regulated under Explanation, Section 21 of CPO, 2025.
- **Section 25 of CPO, 2025:** For blackmailing, sexual harassment, dissemination of revenge pornography, or creates, possesses, or stores any content related to Child Sexual Abuse Material (CSAM) or sextortion, or transmits, publishes, or broadcasts any such information, video, audiovisual material, still image, graphics, or any content captured, edited, or generated by artificial intelligence is directly regulated under Explanation, Section 25 of CPO, 2025.

However, it does not directly regulate AI development, deployment, or accountability, leading to doctrinal ambiguity in enforcement and adjudication. This ambiguity not only undermines legal clarity but also erodes public confidence in cybersecurity laws.

Legal Responsibility of AI Developers, Service Providers, and Users: CPO 2025 assigns responsibility to digital service providers for securing digital infrastructure but lacks clarity on liability attribution when harm results from autonomous AI decisions. This mirrors doctrinal debates globally regarding vicarious liability, AI agency, and negligence standards [47].

Coverage of AI-Based Offences, AI Accountability, and Limitations: While CPO 2025 recognizes AI-enabled cyber threats, it falls short of establishing clear accountability mechanisms or ethical guidelines. The law does not differentiate between human and machine actors in criminal conduct, raising issues for courts in determining culpability [48].

Table 13. Legal Adequacy Matrix: AI Recognition under CPO 2025.

Criteria	Included in CPO 2025	Adequacy Level
AI definitions	✓	Moderate
Developer liability	✗	Low
AI-based offences	✓ (Implied-Tools & Agent)	Low
Algorithmic accountability	✗	Very Low
Ethical oversight	✗	Very Low

This matrix demonstrates the partial and underdeveloped nature of AI regulation within CPO 2025. Although AI is nominally recognized, the lack of doctrinal depth and operational precision reveals significant legal inadequacies.

Challenges in Regulating AI through CPO 2025:

Scope and Limitations in Addressing AI Autonomy, Algorithmic Accountability, and Transparency: CPO 2025 does not adequately address the growing autonomy of AI systems or their capacity to make impactful decisions without human intervention. The lack of enforceable standards for algorithmic accountability and transparency limits its ability to ensure fair and just use of intelligent technologies [49]. Without legal requirements for explainability, the Ordinance leaves a gap in ensuring that automated decisions are auditable or contestable.

Absence of Specific Clauses for Ethical AI, Automated Decision-Making, or AI Bias: Ethical concerns about AI such as discrimination, profiling, and opacity—are well-documented in international literature. However, CPO 2025 lacks any mention of ethical AI principles, fairness audits, or governance frameworks to address algorithmic bias. This omission is problematic given Bangladesh’s increasing reliance on digital tools in public service delivery.

Gaps in Regulating Emerging AI Risks: The CPO 2025 inadequately addresses several pressing risks:

- **AI-generated misinformation and deepfakes:** While Section 25 addresses harmful content, it does not explicitly regulate synthetic content produced by generative AI.
- **AI in surveillance and predictive policing:** Although CPO empowers agencies to conduct surveillance, it lacks safeguards against misuse of AI-powered facial recognition and data-driven policing.

- **AI-driven cyberattacks:** The ordinance does not explicitly anticipate autonomous malware or AI-based intrusion, leaving forensic and attribution gaps.

Overlap and Contradictions between Human and Machine Agency: CPO 2025 continues to frame culpability within the traditional doctrine of human agency, neglecting the doctrinal complexities introduced by autonomous systems. This raises interpretative challenges in judicial settings, particularly around intent, knowledge, and foreseeability.

Table 14. SWOT Analysis: AI Regulation Challenges in CPO 2025.

Strengths	Weaknesses	Opportunities	Threats
Introduces AI terminology	Lacks binding ethical standards	Scope to lead South Asian AI policy	Doctrinal ambiguity on AI agency and responsibility
Expands institutional roles	No clear liability framework for AI developers	International alignment via UNESCO & OECD principles	Regulatory lag behind tech development

This SWOT grid illustrates the internal and external legal tensions within the CPO. It reflects how the ordinance, while progressive in scope, remains structurally and conceptually unprepared to handle AI’s complexities.

Doctrinal Analysis of Legal Gaps and Enforcement Challenges:

Lack of Explicit AI Ethics or Algorithmic Accountability: Unlike the EU AI Act or the UNESCO AI Ethics Guidelines, CPO 2025 does not articulate any binding obligations for fairness, non-discrimination, or explainability in automated systems. This legal vacuum leaves AI governance to discretion, risking arbitrary and unaccountable uses.

Ambiguities in Liability for Autonomous or Generative AI Actions: The doctrine of strict liability or negligence becomes complicated when causation is indirect or mediated through machine learning systems [50]. CPO’s current language does not provide judicial tools to resolve such questions, making liability attribution vague. These types of vague language used in CPO can be misinterpreted.

Evidentiary and Enforcement Challenges: Forensic and Investigative Limits: AI-generated decisions and behaviors often leave behind insufficient or non-human-readable logs. This presents forensic obstacles in proving *mens rea*, establishing causation, and securing convictions. CPO lacks provisions for digital forensic audits tailored to AI.

Infrastructural Limitations in Investigation and Redress Mechanisms: Although CPO establishes agencies like the NCERT and Cyber Security Agency, their technical capacity to audit, interpret, and regulate AI systems remains questionable [51]. Without AI-proficient personnel, enforcement becomes superficial.

Constitutional Rights and AI Governance with Digital Due Process, Privacy, and Expression:

While the CPO 2025 references constitutional protections, it fails to substantively engage with them.

- Article 27 (equality before law) is jeopardized when algorithmic bias in recruitment or public service delivery results in discriminatory outcomes.
- Article 31 (protection of law) is threatened when opaque AI decision-making denies individuals due process, for example, in automated credit scoring or predictive policing tools where affected persons cannot contest the algorithmic reasoning.
- Article 39 (freedom of expression) faces new challenges as AI-generated disinformation, deepfakes, and synthetic media can distort democratic discourse and chill legitimate speech.

CPO allows broad data collection and monitoring without sufficient procedural safeguards. The Ordinance fails to ensure digital due process rights, including notice, appeal, and review mechanisms when decisions are influenced by algorithmic tools.

Table 15. Conflict Mapping: AI, Rights, and Enforcement.

Conflict Source	Stakeholders	Legal Issue	Consequences
Predictive policing and surveillance AI	Citizens vs. State	Privacy and due process violations	Legal uncertainty and potential rights erosion
Algorithmic decision-making in governance	Bureaucracy vs. Rights Advocates	Lack of transparency and redress	Demand for judicial and legislative oversight

This mapping shows how unregulated AI in public and legal systems may exacerbate rights violations and legal fragmentation unless doctrinal reforms and safeguards are introduced. A hypothetical case study of a deepfake video used to malign a political candidate during elections illustrates how freedom of expression and electoral integrity may be undermined simultaneously.

Soft Law Instruments as Normative Guides in AI Regulation: This chapter explores the role of non-binding policy documents—commonly referred to as soft law instruments—as normative and strategic tools in shaping AI governance in Bangladesh. These documents, although not enforceable in court, influence statutory development, administrative implementation, and judicial interpretation. The analysis focuses on three major instruments: the Draft National AI Policy 2024,

the AI Readiness Assessment Report 2025, and the National Strategy for AI (2019–2024). It further assesses how well these align with CPO 2025 and what reforms may follow.

National Artificial Intelligence Policy 2024 (Draft): Legal and Ethical Frameworks: The Draft AI Policy 2024 provides ethical principles and governance goals including fairness, non-discrimination, transparency, and accountability. It proposes sector-specific guidelines and calls for the establishment of a national AI ethics board (ICT Division, 2024). However, these recommendations have not yet been legislated in binding law. Despite referencing global instruments like UNESCO's AI Ethics Guidelines and OECD principles, the draft policy lacks enforceable rights or compliance mechanisms.

Bangladesh AI Readiness Assessment Report 2025: Regulatory Gaps and International Benchmarks: The 2025 Readiness Report identifies institutional, infrastructural, and doctrinal limitations in Bangladesh's AI ecosystem. It ranks the country below regional peers in regulatory preparedness. The report recommends legislative updates to include data protection, AI accountability, and oversight authority. These recommendations provide a de facto benchmark for evaluating the adequacy of CPO 2025.

National AI Strategy (2019–2024): Legal-Industrial Synergies and Strategic Pillars: The National Strategy outlines five pillars including research, skills, infrastructure, legal frameworks, and ethics. Its sectoral focus—especially in agriculture, health, and public service—illustrates the government's intention to embed AI across development sectors. Legally, it recommends public-private regulatory collaboration and encourages anticipatory governance.

Table 16. Legal Adequacy Matrix: Soft Law vs. CPO 2025.

Evaluation Criteria	AI Policy 2024	Readiness Report 2025	AI Strategy 2019–2024	CPO 2025
Ethical AI Principles	✓	✓	✓	✗
Regulatory Recommendations	✓	✓✓	✓	✓ (General)
Enforcement Potential	✗	✗	✗	✓
Alignment with Global Norms	✓✓	✓	✓	✓ (Partial)

This matrix compares the normative depth and influence of soft law documents with CPO 2025. While CPO has legal enforceability, soft law instruments offer richer ethical and strategic frameworks that have yet to be codified.

Interpreting Soft Law through a Doctrinal Lens: Binding Potential or Guiding Norm: Soft law instruments are increasingly treated as persuasive sources in judicial and legislative interpretation [52]. In the doctrinal tradition, they act as reference tools for clarifying ambiguities, filling legislative gaps, and assessing proportionality in administrative actions. For example, if an AI ethics breach arises, courts may look to the AI Policy or UNESCO guidelines to determine standards of conduct.

How Well Do Policy Instruments Align with CPO 2025? Despite some thematic overlap, there is no formal mechanism within the CPO to incorporate policy guidance. Ethical provisions in the AI Policy 2024 and Readiness Report are not embedded in the Ordinance, leading to normative fragmentation. This weakens coherence and limits judicial capacity to apply best practices.

The Role of Policy in Shaping Future Legal Reform: Soft law will likely influence forthcoming AI legislation, either by being adopted directly or by shaping regulatory culture. Doctrinally, these instruments should be treated as quasi-normative references in both legislative drafting and judicial review.

Table 17. SWOT Grid: Normative Role of Soft Law in AI Regulation.

Strengths	Weaknesses	Opportunities	Threats
Promotes ethical standards	Not legally binding	Offers reform roadmap	Lack of institutionalization in statutes
Facilitates public-private dialogue	Unclear accountability mechanisms	Can guide case law and policy	Risk of policy inconsistency without harmonization

This SWOT grid highlights how soft law can serve as a bridge between innovation and rights-respecting regulation, if integrated into enforceable frameworks.

Normative Evaluation and Policy Reform Proposals: It provides a normative evaluation of Bangladesh's legal readiness for artificial intelligence governance under the Cyber Protection Ordinance (CPO), 2025. Building on doctrinal analysis and soft law comparisons, it identifies core ethical and regulatory deficiencies in the current legal framework and offers strategic recommendations for future reform, including the drafting of a dedicated AI law and institutional mechanisms such as an AI Ethics Commission.

Normative Evaluation of Current Legal Readiness for AI Governance:

Evaluating Bangladesh's Current Legal Readiness for AI Governance: Bangladesh's legal infrastructure from the ICT Act 2006 to the CPO 2025 has evolved but remains doctrinally underprepared for AI's complexities. Core gaps persist in liability

regimes, algorithmic accountability, and ethical safeguards. Unlike the EU AI Act (2024) or UNESCO Ethics Guidelines (2021), the CPO 2025 does not articulate enforceable obligations for fairness, transparency, or explainability. This weakens alignment with international norms and leaves AI governance largely discretionary.

Bangladesh-Specific AI Definition: A key reform is to introduce a Bangladesh-specific definition of AI that is both functional and risk-based:

- **Functional:** “Artificial Intelligence refers to digital systems capable of autonomous decision-making, adaptive learning, and predictive analytics.”
- **Risk-based:** “AI shall be classified into high-risk (e.g., healthcare, judiciary, predictive policing) and low-risk (e.g., chatbots, customer support), with stricter liability and oversight for high-risk applications.”

This dual model would allow lawmakers and courts to tailor accountability and safeguards proportionately.

Institutional Reforms: AI Oversight Authority, AI Ethics Commission: Bangladesh lacks a centralized authority to oversee AI governance. Establishing an independent AI Oversight Authority and AI Ethics Commission could fill enforcement gaps and provide interpretive clarity for courts and regulators. The establishment of an AI Ethics Commission independent of government control should oversee algorithmic audits, enforce transparency mandates, and conduct regular bias testing [53, 54]. An AI Oversight Authority, legally empowered to monitor compliance, could fill current institutional gaps, much like the role played by data protection authorities in the EU.

Table 18. Legal Adequacy Matrix: Normative Compliance Evaluation.

Criteria	Present in CPO 2025	Alignment with Global Standards
AI Ethics Principles	X	Low
Algorithmic Accountability	X	Very Low
Oversight Institutions	X	Absent
Public Redress Mechanism	X	Weak

This matrix reveals the structural gaps in Bangladesh’s current legal framework when measured against international ethical and governance standards for AI.

Judicial Role and Precedent Development: Bangladeshi courts have begun engaging with digital rights in cases such as Dr. Shahidul Alam vs. State (2019) [55]; Anis Hossain Prodhan vs. State (2020) [56]; Didarul Islam Bhuiyan Case, Jhumon Das Apon Case, Md Ruhul Amin Case, Pritom Das Case, Shanto Banik Case, Khadijatul Kubra Case, Lutfur Rahman Case, Imtiaz Ahmed Case and Mamunur Rashid Nomani Case, but their role in shaping AI liability remains underdeveloped. Future judicial activism could clarify the application of strict liability, due process, and freedom of expression to AI-related disputes [57]. For example, courts could mandate algorithmic transparency in government use of AI to protect Article 31’s guarantee of protection of law.

Implications for Law and Policy: The article underscores the urgent need for doctrinal clarity in AI definitions, liability attribution, and rights-based protections. Without algorithmic transparency and enforceable safeguards, Bangladesh risks repeating the overreach of past cyber laws under new technological guises. Policy reforms such as a dedicated AI Act, the establishment of an AI Ethics Commission, and the integration of constitutional safeguards into algorithmic decision-making are essential to ensure a human-centric approach to AI governance [58].

Recommendations for Future Legal Reform: A standalone Artificial Intelligence Act should be drafted to define AI categories and risk levels, establish AI-specific civil and criminal liability regimes, and introduce rights-based safeguards for algorithmic decision-making. In the short term, amendments to the CPO, 2025 should focus on inserting clauses addressing algorithmic transparency, explainability, and fairness, and codifying audit mechanisms for high-risk AI applications. A dedicated AI Regulatory Framework under a parliamentary statute is essential to harmonize emerging technologies with constitutional values, while a Digital Ethics Commission could independently issue binding codes of practice [59]. Bangladesh must also prioritize capacity building through legal training and active participation in international and regional AI cooperation. Future legislation in finance, health, education, and public administration should incorporate AI-specific clauses such as risk assessments and human oversight requirements. Furthermore, an AI Ethics Commission or Regulatory Authority independent and constitutionally recognized should be tasked with standard-setting, monitoring compliance, and conducting impact assessments. A unified legal framework is also necessary to align AI governance with data protection (currently absent), competition law (to prevent algorithmic monopolies), and consumer protection law (to ensure fairness in automated services). Finally, AI must be thoughtfully integrated into judicial, administrative, and governance systems not as a substitute for legal reasoning but as a tool to enhance efficiency and equity, guided by interpretative frameworks issued by constitutional courts.

Future Research Agenda: Future research should integrate empirical studies on AI’s real-world impact in Bangladesh, focusing on fintech, predictive policing, and automated welfare systems. Comparative analysis with India and Pakistan would

contextualize Bangladesh's regulatory trajectory within South Asia. An interdisciplinary approach linking law, computer science, and ethics is essential to ensure that proposed reforms are both technically feasible and normatively grounded [60].

Conclusions: As Bangladesh stands at the cusp of a technological revolution driven by artificial intelligence and AI systems, this article has sought to critically examine the readiness and effectiveness of the Cyber Protection Ordinance (CPO), 2025. The analysis demonstrates that while CPO 2025 represents a significant step beyond prior legislation such as the ICT Act 2006, the DSA 2018, and the CSA 2023 its AI-related provisions remain doctrinally incomplete and normatively underdeveloped. As artificial intelligence increasingly influences decision-making, surveillance, communication, and even public service delivery, the legal system must evolve to ensure accountability, fairness, and the preservation of fundamental rights [61].

Despite CPO 2025's improvements in institutional coordination and procedural clarity, it lacks key elements such as algorithmic transparency, human oversight obligations, and enforceable ethical safeguards. Without these, the legal framework risks enabling unchecked surveillance, discrimination, and opacity. This study affirms the importance of doctrinal legal scholarship as a tool for identifying structural gaps, proposing normative reforms, and benchmarking legal progress against international standards. Legal doctrine not only helps interpret existing statutes but also guides the development of principled, future-ready legislation. Going forward, Bangladesh must embrace a rights-based, adaptive, and interdisciplinary approach to AI regulation. This requires judicial engagement with AI-related disputes, empirical research into sector-specific applications (e.g., fintech, policing, health), and comparative studies with regional peers like India and Pakistan.

References:

- [1] S. Bayern, *A Research Agenda for Organizational Law*. United Kingdom: Edward Elgar Publishing Limited, 2024.
- [2] V. S. Anoop and J. M. Fawaz, Fine-tuning a Domain-Specific Large Language Model Using Low-Rank Adaptation Technique for Legal AI Applications-Case of India, in *Artificial Intelligence in Legal Systems: Bridging Law and Technology Through AI*, N. R. Vajjhala, B. Aslani, and E. Çela, Eds. N.p.: CRC Press, 2025.
- [3] A. P. E. D. Engelbrecht, *Artificial Intelligence: Social, Ethical and Legal Issues*. United Kingdom: IntechOpen, 2025.
- [4] R. Calo, Robotics and the lessons of cyberlaw, *California Law Rev.*103(3), 2015, pp. 513–563; V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York, NY, USA: St. Martin's Press, 2018.
- [5] L. Floridi et al., AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations, *Minds Mach.* 28(4), 2018, 689–707.
- [6] Z. Ahmed, Autonomous Artificial Intelligence and Legal Accountability in Bangladesh: Rethinking Liability and Agency, *Global J. Cybersecurity Law, Digital Ethics, Policy Innovation*, 1(3), 2022, 32–50.
- [7] OECD, *OECD principles on artificial intelligence*, 2019.
- [8] Government of Bangladesh, *National Artificial Intelligence Policy 2024 (Draft)*, Ministry of Posts, Telecommunications and Information Technology, ICT Division.
- [9] M. Varju and K. Mezei, *The Challenges of Artificial Intelligence for Law in Europe*. Springer, 2025.
- [10] Z. Ahmed, AI and Digital Governance in Bangladesh: Bridging the Gap between Policy Commitments and Legal Infrastructure, *Int. Rev. Cyber Law, Digital Governance, Human Rights*, 1(4), 2023, 1–23.
- [11] T. Tzimas, *Legal and Ethical Challenges of Artificial Intelligence from an International Law Perspective*. Switzerland: Springer International Publishing, 2021.
- [12] E. Wallingford, *Liabilities and Modern Artificial Intelligence: A Tri-Phase Model*. United Kingdom: Taylor & Francis, 2025.
- [13] E. Osaba, *Artificial Intelligence: Latest Advances, New Paradigms and Novel Applications*. United Kingdom: IntechOpen, 2021.
- [14] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Pearson, 2021.
- [15] WIPO Secretariat, *Revised Issues Paper On Intellectual Property Policy And Artificial Intelligence*, WIPO Conversation On Intellectual Property (IP) And Artificial Intelligence (Ai)- Second Session, WIPO/IP/AI/2/GE/20/1 REV.2020.
- [16] Z. Ahmed, Artificial Intelligence in Bangladesh's Justice System: Opportunities, Risks, and the Future of Legal Practice, *J. Social Justice Governance, Legal Reform, Policy Futures*, 3(3), 2022, 37–60.
- [17] S. Dash, R. Das, P. Raj, and I. Acharya, *Artificial Intelligence and Law*. N.p.: IIP Iterative International Publishers, 2025.
- [18] K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT, USA: Yale University Press, 2021; B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, The ethics of algorithms: Mapping the debate, *Big Data Soc.* 3(2), 2016, 1–21.
- [19] M. Tshilidzi and L. G. Mpedi, *Artificial Intelligence and the Law*. Germany: Springer Nature Singapore, 2024.
- [20] Z. Ahmed, Artificial Intelligence, Human Rights, and Ethical Governance in Bangladesh: Navigating Vulnerabilities in a Nascent Legal Framework, *Global J. Digital Law, Cybersecurity, Ethical Governance*, 1(2), 2021, 12–30.
- [21] Z. Ahmed, AI and the Erosion of Freedoms: Legal and Ethical Challenges in Bangladesh's Justice System, *Int. Rev. Cyber Law, Digital Governance, Human Rights*, 2(4), 2023, 43–65.
- [22] B. Adams, *Law in the Age of Artificial Intelligence: Navigating Legal Frontiers in an Evolving Technological Landscape*. N.p.: Amazon Digital Services LLC - Kdp, 2024.
- [23] D. Dennehy, A. Griva, N. Pouloudi, Y. K. Dwivedi, I. O. Pappas, et al., *Responsible AI and Analytics for an Ethical and Inclusive Digitized Society*. Springer, 2021.
- [24] W. Barfield and U. Pagallo, *Advanced Introduction to Law and Artificial Intelligence*. United Kingdom: Edward Elgar Publishing, 2020.
- [25] T. Hutchinson, Doctrinal research: Researching the jury, in *Research Methods for Law*, 2nd ed., M. McConville and W. H. Chui, Eds. Abingdon, U.K.: Routledge, 2014, pp. 7–33.
- [26] Supra note 4.
- [27] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2021.
- [28] 71 DLR (HCD) 217
- [29] 72 DLR (HCD) 312
- [30] 61 cases have been filed under CSA, 2023 accusing 372 individuals, since its enactment on 18 September 2023 to 7 July 2024.

- [31] Z. Ahmed, *A Text Book of Cyber Law in Bangladesh*, 8th ed. Dhaka, Bangladesh: Hasan Law Book, 2024.
- [32] *Anis Hossain Prodhan vs. State* (2020). 72 DLR (HCD) 312.
- [33] Z. Ahmed, *Cyber Ain: Totho O Bisleshon* (in Bengali), 5th ed. Dhaka, Bangladesh: Muhit Publications, 2025.
- [34] Dhaka Tribune, Law minister: Over 7,000 cases under DSA, Dhaka Tribune, June 5, 2023.
- [35] *Md. Sujon Miah v. The State*, Crl. Misc. Case No. 16010 of 2016; *Alam Kiron v. The State*, Crl. Misc. Case No. 48512 of 2017; *A.P.M. Tushar v. The State*, Crl. Misc. Case No. 14867 of 2016; *Md. Anis Hossain Prodhan v. The State*, Crl. Misc. Case No. 28869 of 2018; *Anuj Chandra Majhee v. The State*, Crl. Misc. Case No. 27323 of 2018; *Sumon Mia v. The State*, Crl. Misc. Case No. 24479 of 2017; *Most. Sirajam Munira v. The State*, Crl. Misc. Case No. 52359 of 2021; *Munshi Nazrul Islam Sujan v. The State*, Crl. Misc. Case No. 31376 of 2022; and *Md. Mizanur Rahman v. The State*, Crl. Misc. Case No. 46842 of 2019.
- [36] Amnesty International, *Human Rights Impact of the Digital Security Act of Bangladesh*, 2019.
- [37] M. S. Islam and T. Jahan, Gaps in Cybersecurity Legislation in Bangladesh, Dhaka Univ. Law Rev. 34(1), 2023, 88–105.
- [38] The Business Standard, Over 7,000 cases filed under DSA, Law minister, The Business Standard, June 5, 2023.
- [39] *Arafat Hosen Khan v. Bangladesh* [2010] Writ Petition no. 4719 (HC).
- [40] The Cyber Protection Ordinance, 2025, sec. 2.
- [41] Cabinet Division, *Explanatory Memorandum on the Repeal of Cyber Security Act, 2023*, Government of Bangladesh, 2025.
- [42] The preamble of the CPO, 2025 states that WHEREAS the provisions concerning the protection of citizens were inadequate in the Cyber Security Act, 2023, thereby creating grounds for misuse and oppression; and WHEREAS the said Act curtailed freedom of expression and other fundamental rights, and therefore, it is expedient to repeal the same and enact an ordinance to ensure cyber security, detect, prevent, suppress and adjudicate offences committed in cyberspace and other matters related thereto.
- [43] Ahmed Musa, *Deepfake Dilemmas: The Threats and Opportunities of AI-Generated Media*, N.p.: Recorded Books, 2025.
- [44] UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, Adopted on 23 November 2021. The United Nations Educational, Scientific and Cultural Organization, 2022.
- [45] The Cyber Protection Ordinance, 2025, sec. 2.
- [46] C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, and L. Floridi, Artificial intelligence and the 'good society': the US, EU, and UK approach, *Sci. Eng. Ethics*, 24(2), 2018, 505–528.
- [47] D. Bigo, S. Carrera, E. Guild, & V. Mitsilegas, *Controlling frontiers: Free movement into and within Europe*. Ashgate Publishing, 2020.
- [48] U. Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*. Springer, 2013.
- [49] S. Wachter, B. Mittelstadt & L. Floridi, Transparent, explainable, and accountable AI for robotics. *Science Robotics*, 2(6), 2017, eaan6080.
- [50] Supra note 17.
- [51] Supra note 47.
- [52] Ministry of Posts, Telecommunications and Information Technology, *Bangladesh AI Readiness Report, Artificial Intelligence Readiness Assessment Report April 2025*.
- [53] A. Zia-ur-Rehman, *Artificial Intelligence Ethics: A Maturity Assessment Framework*. United States: Author House UK, 2025.
- [54] A. Guru, *AI Ethics: Artificial Intelligence Beyond the Algorithm*. N.p.: Pure Water Books, 2025.
- [55] Supra note 28.
- [56] Supra note 29.
- [57] K. W. Abbott & D. Snidal, Hard and soft law in international governance. *International Organization*, 54(3), 2000, 421–456.
- [58] A. Elci and D. Ç. Ertuğrul, *Future of Digital Technology and AI in Social Sectors*. United States: IGI Global, 2024.
- [59] M. D. Baez, *AI-powered Leadership: Transforming Organizations in the Digital Age*. United States: IGI Global Scientific Publishing, 2025.
- [60] G. O. Regan, *Ethical and Legal Aspects of Computing: A Professional Perspective from Software Engineering*. Germany: Springer Nature Switzerland, 2024.
- [61] H. Bajraktari and V. Qatani, Artificial Intelligence a 'Right' or 'Violation' of Human Rights and Freedoms in the 21st Century, in *Exploration of AI in Contemporary Legal Systems*, H. Bajraktari, Ed. United States: IGI Global, 2024, pp. 43–56.