Scholars Journal of Engineering and Technology

OPEN ACCESS

Abbreviated Key Title: Sch J Eng Tech
ISSN 2347-9523 (Print) | ISSN 2321-435X (Online)
Journal homepage: https://saspublishers.com

Artificial Intelligence and Criminal Justice in Bangladesh: Assessing Legal Readiness to Combat AI-Enabled Crimes

Anadi Bikash Chowdhury[1]*, Amzad Sadik[2], Sabekun Nahar Setu[2], Tahsin Safqat[2]

[1]Advocate, District and Sessions Judge Court, Cumilla, Bangladesh
[2]Final Year Law Students, Bangladesh Army International University of Science and Technology (BAIUST), Cumilla, Bangladesh

DOI: https://doi.org/10.36347/sjet.2026.v14i11.004 | **Received:** 02.10.2026 | **Accepted:** 23.11.2026 | **Published:** 26.11.2026

***Corresponding author:** Anadi Bikash Chowdhury
Advocate, District and Sessions Judge Court, Cumilla, Bangladesh

Abstract | **Original Research Article**

Artificial intelligence (AI) gives offenders cheaper, faster ways to commit familiar crimes, including fraud, impersonation, blackmail, and disinformation, while creating a small number of genuinely new risks, such as bias in automated judicial tools. This paper asks what AI-enabled crimes threaten Bangladesh's criminal justice system and how legally prepared Bangladesh is to combat them. It uses a qualitative-doctrinal method supported by ten case studies and a comparative analysis of world experience. The Penal Code, the Cyber Security Act 2026, the Evidence Act and the Money Laundering Prevention Act, read alongside the draft National AI Policy 2026–2030, are tested against six threat categories drawn from the literature and against ten cases from Bangladesh and five comparator countries. Bangladesh emerges as partly ready. Criminalization is improving, but attribution rules remain thin, institutional capacity is uneven, cross-border cooperation is weak in practice, and evidentiary practice is falling behind the sophistication of synthetic media. In eight of the ten cases, an existing offense or court procedure already reached the conduct, which indicates that AI works mainly as an accelerant of existing crime rather than as the architect of a new category. The paper therefore argues for calibrated, reviewable amendment of the existing framework, benchmarked against jurisdictions of comparable capacity, rather than a wholesale AI-specific criminal code.

Keywords: Artificial Intelligence, AI-Enabled Crime, Criminal Justice, Deepfakes, legal Readiness, Bangladesh.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

1. INTRODUCTION

Artificial intelligence has moved from an experimental technology to a tool that offenders can obtain cheaply and use at scale. Deepfake fraud, voice cloning, synthetic disinformation and algorithmic bias have produced documented incidents around the world, and Bangladesh is not insulated from them. Since 2023, a deepfake advertising syndicate, election-period disinformation and AI-facilitated blackmail have all surfaced within the country (section 4.3).

The legal response has been unsettled. Bangladesh's cyber-law framework has passed through four instruments in under eight years: the Digital Security Act 2018, the Cyber Security Act 2023, the Cyber Security Ordinance 2025 and the Cyber Security Act 2026. None of this has produced a settled account of whether these instruments, together with the Penal Code, the Evidence Act and the Money Laundering Prevention Act, actually reach AI-enabled conduct, or of what legal readiness requires beyond statutory text. Policy has also moved ahead of legislation. The draft National AI Policy 2026–2030 ("the Policy") proposes risk-based regulation, prohibitions, impact assessments and independent oversight, but because it is unenacted, it creates no offenses [1, 2].

Previous work has done much to define the problem. Scholars have classified AI-enabled crime as offending in which AI is an essential contributory factor [3], ranked its foreseeable forms [4] and distinguished the abuse of AI systems from their use as a criminal instrument [5]. Comparative studies of other jurisdictions show that general cybercrime and data-protection statutes often fail to anticipate synthetic media and automated attacks (section 4.2). What the literature does not offer is a doctrinal test of Bangladesh's own criminal, evidentiary and financial-crime statutes against a multidimensional standard of readiness.

This paper supplies that test. Its purpose is to identify the AI-enabled crimes that threaten the

Bangladeshi criminal justice system and to assess how ready the law is to meet them. Its scope is doctrinal and comparative: it examines four statutes and the Policy, a sample of ten documented cases and a regional benchmark, and it does not measure the prevalence of AI-enabled crime. Its novelty lies in combining a five-dimension readiness framework with a case sample drawn from Bangladesh and five comparator countries, and in using that combination to argue that AI mainly accelerates existing offenses, so that calibrated amendment is a more defensible response than a wholesale AI-specific criminal code. The paper proceeds as follows. Section 2 states the research questions, section 3 the method, and section 4 reviews the literature and the cases. Section 5 defines the key concepts, section 6 reports the results, sections 7 and 8 discuss reform and the case for calibration, and sections 9 to 11 set out the findings, future directions and conclusions.

2. Research Questions

This paper is organized around two research questions, addressed respectively especially in sections 4.1, 6.1, 7.1 and 8.1, and in sections 4.2, 6.2, 7.2 and 8.2.

1. What AI-enabled crimes threaten Bangladesh's criminal justice system?
2. How prepared is Bangladesh legally to combat AI-enabled crimes?

The first question is empirical and classificatory: it asks which categories of AI-enabled conduct are documented or plausible within Bangladesh, drawing on comparative incidents where domestic evidence is thin. The second is normative and doctrinal: it asks whether Bangladesh's existing substantive, evidentiary, and institutional framework can meet those threats, and if not, what form of reform, wholesale or calibrated, is defensible.

3. MATERIALS AND METHODS

Research design.

The study is qualitative and doctrinal. Legal readiness is a question about whether rules, procedures and institutions can define, investigate, attribute and adjudicate conduct, so it neither requires nor lends itself to numerical measurement. The doctrinal core identifies, interprets and evaluates the substantive and procedural provisions of the Penal Code, the Cyber Security Act 2026 (successor to the Digital Security Act 2018, the Cyber Security Act 2023 and the Cyber Security Ordinance 2025), the Evidence Act and the Money Laundering Prevention Act, and tests them against the categories of AI-enabled criminal conduct identified in the literature. The Policy is read as non-binding evidence of regulatory direction and not as law.

Case studies and comparative benchmark.

Bangladesh has produced little case law and almost no empirical data on AI-enabled offenses. The study therefore pairs the doctrinal analysis with ten illustrative cases and with comparative material from India, Indonesia, China, Southeast Asia, the European Union and the United States. The foreign material is not imported as law. It is used to build an analytical benchmark of what legal readiness should mean, against which Bangladesh's framework is then measured. A case was included only if AI was an essential factor, the event was documented in reliable public sources, and the case illuminated a threat category or a readiness dimension. Bangladeshi cases were prioritized, and foreign cases served as benchmarks. The sample is illustrative and not statistically representative, and outcomes are stated as at 28 September 2026.

Sources.

The material comes from peer-reviewed articles, working papers, regulatory and legislative documents, court decisions and reported incidents accessed through digital databases and online sources. Each source was assessed for currency, jurisdictional relevance and methodological transparency before being relied upon. Where a case rests on press reporting and not on a judgment, the text says so.

Scope, limits and ethics.

The study uses no interviews, surveys or quantitative analysis, and it does not claim to measure the empirical prevalence of AI-enabled crime in Bangladesh. The indices in the figures are the authors' illustrative constructs and not official measures. Because the research involves no human participants and uses only published and public materials, ethics committee approval was not required.

4. LITERATURE REVIEW

4.1 Mapping the Threat: AI-Enabled Criminal Conduct in Comparative Perspective

The literature classifies AI-enabled crime as offending in which AI is an essential contributory factor, covering phishing, fraud, identity theft, market manipulation, harassment and forgery, with AI's autonomy and learning capacity creating liability and monitoring problems that ordinary cybercrime does not [3]. Taxonomies have grown more detailed, from an eighteen-category ranking that spans deepfake impersonation, tailored phishing, AI-generated disinformation, large-scale blackmail and attacks on autonomous systems [4] to a distinction between malicious abuse of AI, such as data poisoning, and malicious use of AI to enhance social engineering, misinformation and hacking [5]. Such crime is also difficult to detect and prove because it is anonymous, transnational and often directed at intangible data, which strains traditional doctrines of theft, damage, and forgery [6].

Within cybercrime, AI supports identity theft, phishing, botnets, ransomware, cyberterrorism, and disinformation on both the offending and detection sides of cybersecurity [7]. The same capabilities enable deepfake-driven impersonation fraud, including cloned

executive voices used to induce fraudulent transfers [8]. Automated and adaptive attacks that need little human intervention also destabilize the mens rea-centered logic of criminal liability [9, 10], and similar automation supports synthetic identity fraud and cryptocurrency laundering, although regulatory capacity to counter it varies sharply with state resources [11].

Deepfakes create risks beyond identity fraud, including personality-rights infringement, synthetic child sexual-abuse material and blackmail [12], and they complicate attribution and the verification of digital evidence in criminal proceedings [13]. Generative-AI "crimebots" extend the same risks to fraud, extortion, and fabricated evidence [14], and Indonesian experience shows that general cybercrime and personal-data statutes rarely anticipate non-consensual deepfake pornography [15].

AI is also used defensively in anti-money-laundering [16] and in adverse-media screening within Bangladeshi mobile financial services, although it cannot itself determine criminal liability [17]. Within the justice system, risk-assessment tools such as COMPAS can reproduce rather than eliminate bias [18]. The only study located on unlawful AI use in Bangladesh confirms that the threat is domestic but does not establish its prevalence or legal treatment [19]. Adjacent work on copyright piracy in India shows how digital reproduction and circulation strain enforcement frameworks, but it offers context rather than evidence of AI-enabled crime [20].

The literature thus yields six recurring threat categories: AI-assisted phishing and financial fraud; deepfake-enabled impersonation and blackmail; AI-generated disinformation; AI-enhanced hacking and malware; AI-facilitated money laundering; and bias in AI tools used within the justice system itself. How each interacts with Bangladesh's existing offenses, institutions and evidentiary practice remains open, a gap addressed in Part 6.

4.2 Measuring Preparedness: Comparative Legal Responses to AI-Enabled Crime

Legal readiness is understood as more than substantive criminalization. Even where the Budapest Convention's technologically neutral drafting covers some AI-enabled conduct, readiness also depends on procedural investigative powers, preservation of electronic evidence, clear rules of attribution and liability, and cross-border cooperation [8]. Autonomous conduct fragments mens rea, actus reus, and attribution across designers, deployers, and users [3], and the principle of legality (nullum crimen sine lege) is strained where conduct does not clearly fall within an existing offense, which supports four benchmarks: substantive coverage, digital-evidence procedure, specialized institutional capacity, and international cooperation [6].

Country studies show that general cybercrime or data-protection legislation is not enough. Indonesia's statutes fail to meet the perpetrator-identification, evidentiary, and victim-protection needs of deepfake pornography, so content removal, a right to be forgotten, and restitution are needed alongside criminal sanctions [15]. Indonesia's readiness against automated cyberattacks has been scored at only forty-five out of one hundred, owing to unresolved attribution, anonymization, and jurisdictional gaps, prompting a proposed "Penal AI Attribution Spectrum" that allocates liability by degree of AI autonomy [9]. Even fragmented American AI policy benefits from judicial willingness to extend precedent to novel conduct, so readiness depends on interpretive flexibility as much as on statutory completeness [10].

Readiness also turns on forensic and evidentiary capacity, because a legal system must still authenticate and weigh AI-manipulated evidence after manipulation is technically detected [7, 13]. Technological detection capacity and legal-evidentiary adequacy are related but distinct questions [14, 16], and since regulation lags technology, readiness should be measured by capacity for adaptive governance as well as by the statute book [4, 5]. No source located assesses whether Bangladesh's criminal, cybersecurity, evidence and financial-crime statutes are adequate to AI-enabled conduct [19].

Legal readiness is therefore multidimensional, spanning criminalization, attribution and liability, evidentiary procedure, institutional and forensic capacity, and international cooperation, and no jurisdiction examined has fully resolved all five. No study yet applies this composite framework doctrinally to Bangladesh's Penal Code, Cyber Security Act 2026, Evidence Act and Money Laundering Prevention Act, which is the gap addressed in Part 6.

4.3 From Incident to Institution: Case Studies of AI-Enabled Offending and Legal Response

This section examines ten incidents and decisions in which AI was an essential factor, the event is documented in reliable public sources, and the case illuminates a threat category from section 4.1 or a readiness dimension from section 4.2. Bangladeshi cases are prioritized, and foreign cases serve as benchmarks. The cases are illustrative rather than statistically representative; several rests on press reporting rather than judgments, and outcomes are stated as at 28 September 2026.

Deepfake advertising syndicate, Dhaka (2026)

In April 2026, Dhaka police arrested ten suspects, aged 19 to 24, for using AI tools to clone the voice, face, and mannerisms of a prominent Islamic speaker and other public figures in fake advertisements for illegal sexual-enhancement drugs; the speaker first saw the videos in February 2025, and a case was registered on 23 April 2026 under sections 22 and 27 of

the Cyber Security Act 2026 [21]. That Act succeeded the Cyber Security Ordinance 2025, which had introduced offenses concerning the misuse of AI tools [22, 23]. The reported charges do not disclose whether the AI element was charged as such, a question for Part 6.

AI-generated disinformation in the 2024 and 2026 elections

Reporting before the January 2024 election found pro-government outlets and influencers using inexpensive AI tools to produce synthetic news anchors and deepfake videos, including a fake clip of an exiled opposition leader that Meta removed only after journalists' inquiries [24]. Deepfakes of former Prime Minister Sheikh Hasina and a fabricated foreign endorsement reportedly recurred around the 2026 general election [25]. The harm falls on electoral integrity rather than property, testing whether ordinary offenses of fraud, impersonation, or incitement reach coordinated synthetic manipulation.

Arup deepfake video-conference fraud, Hong Kong (2024)

A finance employee, after a video call in which the chief financial officer and colleagues were AI-generated recreations, made fifteen transfers totaling HK$200 million (about US$25 million) although no internal system was compromised [26]. Almost two years later no arrests had reportedly been announced, illustrating the attribution and cross-border tracing problems identified in the literature [27].

Baotou face-swap fraud, China (2023)

A Fuzhou company representative transferred 4.3 million yuan after a WeChat video call with an AI face-swapped impersonation of a friend, and because he checked with the real friend soon afterwards, police and the bank intercepted about 3.37 million yuan [28]. Unlike Arup, prompt victim reporting and bank–police cooperation, rather than technology, determined recovery.

Biden voice-clone robocall, United States (2024–25)

Political consultant Steve Kramer admitted commissioning a cloned-voice robocall urging New Hampshire voters to skip the January 2024 primary, for which a US$6 million fine was proposed [29]. A jury nonetheless acquitted him in June 2025 of voter suppression and impersonating a candidate [30]. Established criminal elements must therefore still be proved even where AI-enabled conduct is admitted.

Hugh Nelson, United Kingdom (2024)

Nelson used software with an AI function to convert photographs of real children into abuse imagery to order, sold the images online and encouraged others to commit child rape, and after guilty pleas was sentenced at Bolton Crown Court to 18 years' imprisonment [31]. The prosecution rested on existing offenses, including distributing indecent pseudo-photographs, showing that conduct within established categories can be prosecuted without AI-specific legislation.

Rashmika Mandanna deepfake, India (2023–24)

A deepfake placing the actress's face on another woman's video was registered on 10 November 2023 as an FIR under Indian Penal Code sections 465 and 469 (forgery) and Information Technology Act sections 66C and 66E, and a man in his early twenties was arrested in January 2024 after investigators analyzed around 500 accounts, having allegedly created it to gain social-media followers [32, 33]. Forgery, identity-theft and privacy provisions were thus extended to synthetic media, though identification took just over two months.

Telegram deepfake abuse, South Korea (2024)

Police handled over 800 cases of sexually explicit deepfakes circulated in Telegram groups by September 2024, and on 26 September 2024 the National Assembly passed a bill criminalizing possession or viewing of such material (up to three years' imprisonment or a 30 million won fine) and raising the maximum penalty for creation to seven years irrespective of intent to distribute [34]. This is a clear example of legislative gap-filling in response to AI-enabled abuse.

State v. Loomis (Wisconsin, 2016)

The Wisconsin Supreme Court permitted a sentencing court to consider the proprietary COMPAS risk score but held that it could not be determinative and required written cautions about the tool's limitations [18, 35]. Courts can thus ring-fence algorithmic tools through procedural safeguards even without legislation.

Mata v. Avianca (SDNY, 2023)

Lawyers filed a brief citing non-existent authorities generated by ChatGPT, and the court sanctioned them [36]. Although civil, the case exemplifies the authenticity risk that AI-generated material poses to courts and is directly relevant to advocates and prosecutors in Bangladesh.

Read together, the ten cases confirm four of the six threat categories from section 4.1: financial fraud and impersonation (Dhaka, Arup, Baotou), deepfake-enabled abuse (Nelson, Mandanna, Korea), disinformation (Bangladesh elections, Kramer) and unreliable AI within the justice system (*Loomis*, *Mata*), while AI-assisted hacking and money laundering are not illustrated by the sample. They also yield five readiness lessons: existing offenses can reach AI-enabled conduct where it maps onto forgery, identity or indecent-image provisions; prosecution still turns on proof of statutory elements; cross-border attribution and rapid financial tracing determine outcomes; legislatures may need to fill gaps quickly; and courts can adopt safeguards for AI in proceedings [6, 8]. The Bangladeshi cases show that the threats are already domestic, but reveal little yet about how courts will treat AI elements, which Part 6 assesses.

5. Conceptualizing AI-Enabled Crimes: A Criminological and Criminal Justice Perspective

Assessing Bangladesh's readiness requires clarity on the terms in the title. Five are defined below.

Artificial intelligence.

For legal purposes, artificial intelligence is defined functionally as computational systems that perform tasks ordinarily requiring human intelligence, such as pattern recognition, prediction, natural-language generation and autonomous decision-making, without any need to resolve philosophical debates about machine cognition. Its jurisprudential significance lies in its capacity to act with reduced or no human supervision at the moment of harm. That capacity strains the individualized, intention-based model of liability on which most criminal codes, including the Penal Code 1860, are built.

Crime and criminal justice.

Crime is conduct prohibited and sanctioned by the state under Bangladeshi statute. Criminal justice is the institutional chain of police investigation, prosecution, adjudication and evidentiary process through which that conduct is identified, proved and punished. Placing AI-enabled crime within this frame moves the inquiry beyond substantive definition (is conduct X criminal?) to the whole chain (can it be investigated, evidenced, attributed and adjudicated?), which is the logic of the multidimensional readiness criteria discussed in Part 4.

AI-enabled crime.

Following King and others and Blauth, Gstrein and Zwitter, AI-enabled crime is criminal conduct in which AI is an essential contributory factor, either as an instrument that intensifies, automates or conceals existing offending or as the object of an attack on AI systems themselves [3, 5]. The concept is deliberately broader than cybercrime. It need not involve unauthorized computer access and may occur entirely through lawful use of lawfully deployed AI tools for criminal ends, as when a deepfake is generated for extortion.

Legal readiness.

Drawing on Velasco and on Al Qatawneh and others, legal readiness is treated as a composite and not a binary condition. It has five dimensions: criminalization clear enough to satisfy the principle of legality when applied to AI-facilitated conduct; evidentiary and procedural mechanisms able to authenticate AI-generated or AI-manipulated material; coherent rules of attribution and liability where autonomous systems mediate harm; institutional and forensic capacity to investigate; and cross-border cooperation, given the transnational character of such crime [6, 8]. The Policy adds a soft-law layer of four risk tiers, outright prohibitions, algorithmic impact assessments, human oversight of high-risk uses, strict deployer liability and an independent oversight committee [1, 2, 37]. Being unenacted, it informs the doctrinal analysis but does not replace it.

Bangladesh and jurisprudential value.

Bangladesh is the object jurisdiction. It is examined against the readiness framework and the comparative benchmarks of Part 4, on the premise, consistent throughout the literature, that formal statutory coverage does not by itself establish readiness. The concepts together expose a tension between legal positivism's demand for certainty and legality (*nullum crimen sine lege*) and criminal law's reliance on human *mens rea* as the anchor of responsibility. AI-enabled crime does not necessarily require wholly new offenses, because existing offenses can often be extended by purposive interpretation [12]. Where AI mediates harm autonomously, however, attribution must be reconstructed to the designer, deployer or user without abandoning the individualized-fault principle of liberal criminal law. That tension, and not any single missing statute, is the jurisprudential core of the readiness question examined in Part 6.

6. Results: Assessing Bangladesh's Legal Readiness to Combat AI-Enabled Crimes

6.1 Threat Assessment: The Shape of AI-Enabled Crime in Bangladesh

The first research question asks which AI-enabled crimes threaten Bangladesh. Three are already documented.

Impersonation fraud is the clearest. A Dhaka syndicate cloned the voices and faces of public figures to sell illegal drugs, and the wider literature shows that such techniques scale cheaply and cross borders easily [4, 8, 21]. *Election disinformation* is the second. Pre-election reporting found synthetic news anchors and deepfakes in 2024, and later coverage records similar content around the 2026 election [24, 25]. The Election Commission has acknowledged the danger, but observers question its capacity to respond [38]. The Policy would prohibit deepfakes intended to disrupt democracy or elections, but it remains unenacted [1, 37]. *Sexual deepfakes and blackmail* are the third. One published account describes a young girl extorted with AI-generated explicit videos and threatened with acid violence, a case of old crimes acquiring new tools [39].

Two of the six threat categories from section 4.1 are not illustrated in Bangladesh. No Bangladeshi decision on algorithmic tools in courts was located, and AI-assisted hacking and laundering do not appear in the sample. The 2025 Ordinance nonetheless anticipated hacking by penalizing developers and users who knowingly use AI for unauthorized access to critical infrastructure [22], and the Policy treats law-enforcement AI as high-risk, requiring algorithmic impact assessments and strict human oversight [1, 2, 37].

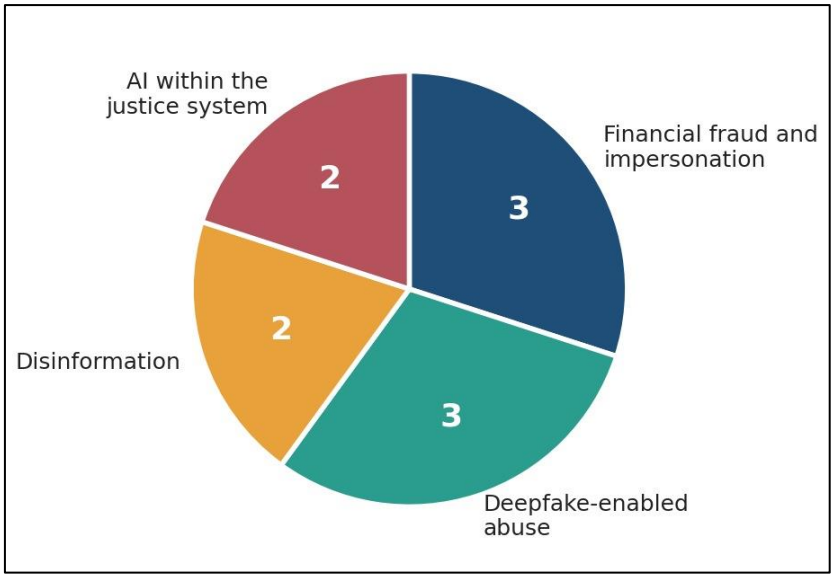


Figure 6.1: Ten-case sample by threat category (authors' classification, section 4.3)

Fraud and deepfake-enabled abuse together account for six of the ten cases. Because the sample is illustrative, this concentration suggests and does not prove that Bangladesh's most urgent exposure lies in identity-based offenses and not in autonomous attacks.

6.2 Readiness Assessment: Testing Bangladesh's Legal Framework

The second research question is tested against the five dimensions defined in Part 5. Table 6.1 reports the provisional ratings.

Table 6.1: Provisional readiness assessment [1, 21, 22, 24, 37, 40, 41]

Dimension	Evidence located	Assessment
Criminalization	AI-misuse offenses in the 2025 Ordinance; Penal Code cheating and forgery remain available; draft Policy prohibitions create no offenses	Partly ready
Evidence	None identified in sources reviewed for AI material under the Evidence Act 1872	Unresolved
Attribution	Developer and user liability for AI-assisted unauthorized access only; draft Policy proposes strict deployer liability	Partly ready
Capacity	CID cyber unit and Dhaka police traced and arrested suspects; draft Policy proposes an independent oversight committee	Developing
Cooperation	Meta removed a deepfake only after press inquiries; draft Policy commits to ratifying the Council of Europe AI Convention	Weak

Bangladesh is therefore partly ready and not fully ready. The Policy improves the picture on paper but, being unenacted, leaves these ratings unchanged. Substantive coverage is improving, yet the cyber framework has been replaced four times in under eight years, which limits settled interpretation [22, 42].

Delay is a second weakness. Figure 6.2 shows that fourteen months separated the discovery of the Dhaka fake advertisements from a registered case. An Indian deepfake case produced an arrest in about ten weeks, and the Arup fraud reportedly remained unsolved after almost two years [21, 26, 27, 32, 33].

The comparators suggest that delay is partly institutional. India, host of the February 2026 AI Impact Summit, treats deepfakes under the Bharatiya Nyaya Sanhita and the Information Technology Act, and its amended IT Rules now require labeling and a three-hour takedown [43–49]. The United States has enacted only the TAKE IT DOWN Act, and in May 2026 its evidence-rules committee declined to advance rules on AI evidence [50–54]. Figure 6.3 sets Bangladesh beside these and earlier comparators.

7. Discussion: Strengthening Bangladesh's Criminal Justice Framework against AI-Enabled Crimes

7.1 Countering the Threat: Targeted Reforms for AI-Enabled Offending

Reform should follow the threat. Figure 7.1 shows that the benchmark cases come from six countries, with Bangladesh supplying two.

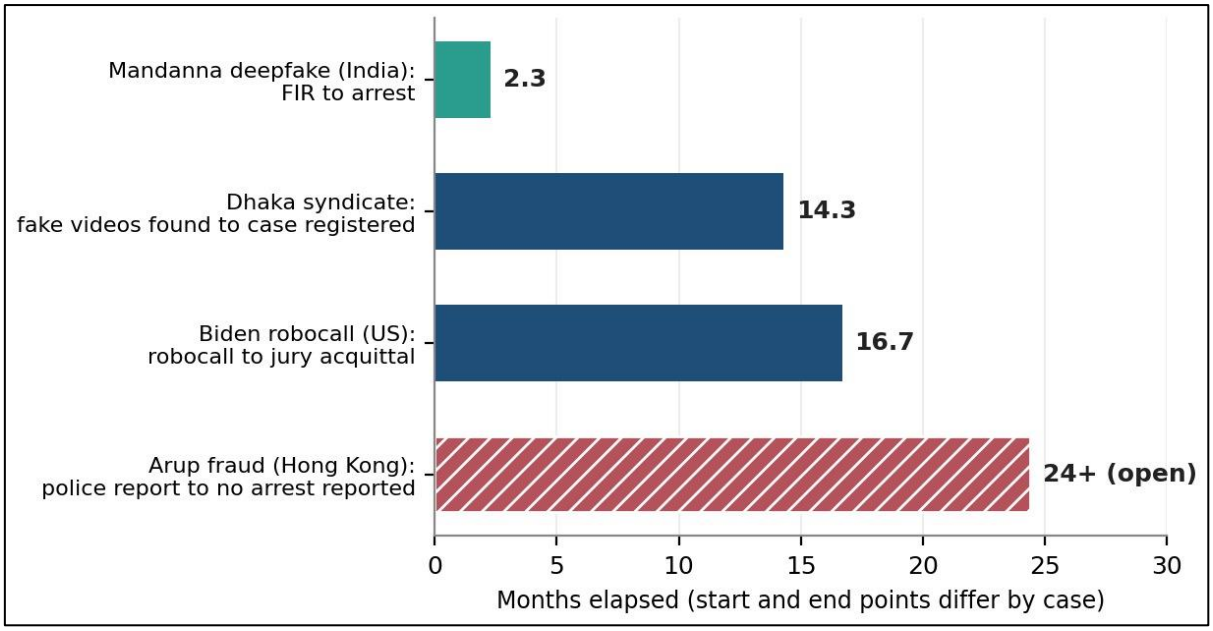


Figure 6.2: Months elapsed in four cases (start and end points differ)

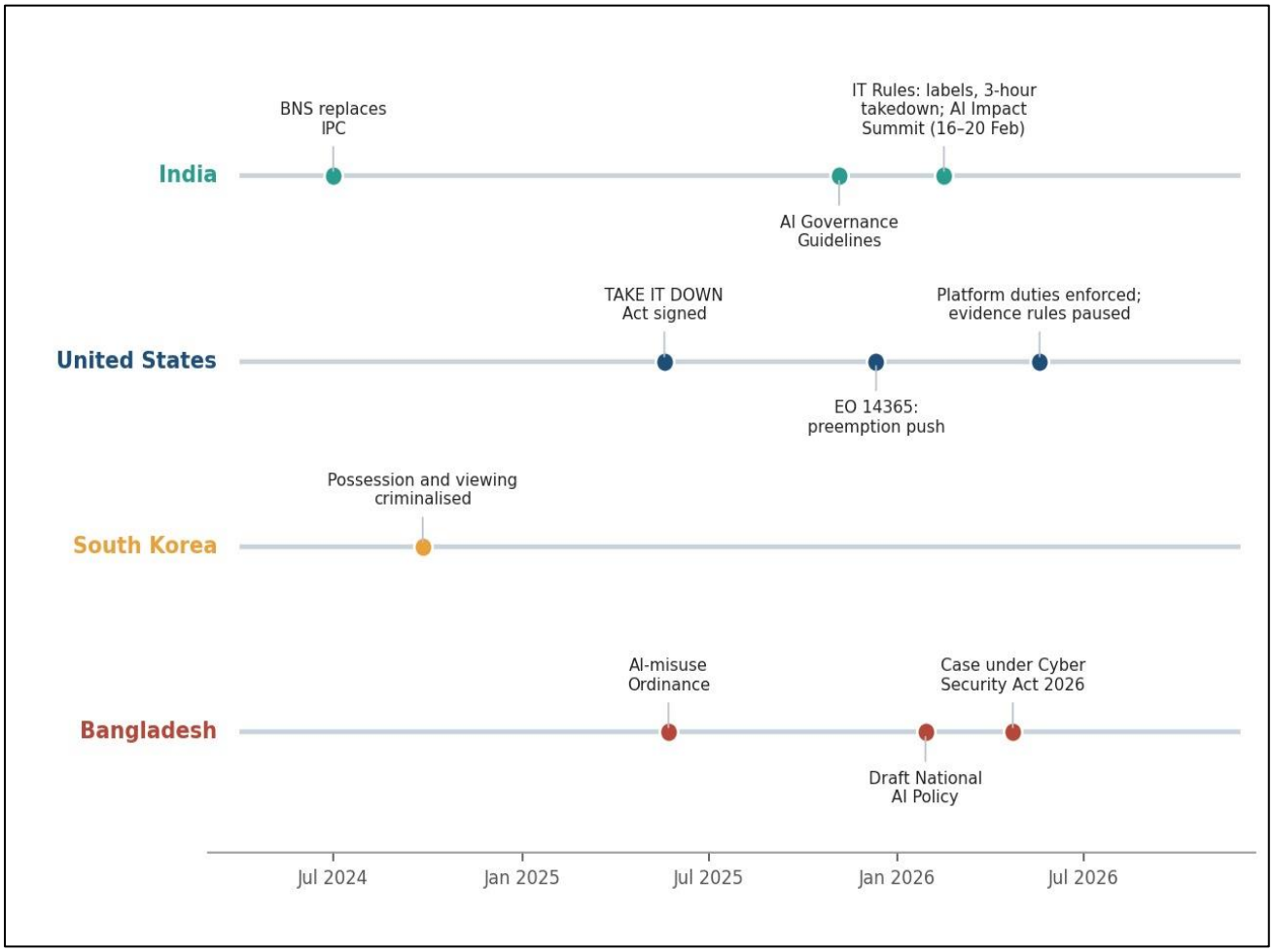


Figure 6.3: Legal-response milestones in four jurisdictions, 2024–2026 (authors' compilation) [1, 21, 22, 34, 43–54]

Readiness therefore depends on procedure and capacity as much as on statute. Part 7 addresses both.



Figure 7.1: Jurisdictions of the ten cases (Hong Kong counted with China)

Impersonation fraud demands speed. In Baotou, police and a bank intercepted about 3.37 million of 4.3 million yuan because the victim reported quickly [28]. Bangladesh should formalize a rapid-freeze protocol linking police, banks and mobile financial services, since the CID has already traced extortion payments through mobile wallets [40].

Sexual deepfakes need express treatment. Figure 7.2 widens the picture from Bangladesh and South Korea to four further countries, using the authors' illustrative index of legal-response intensity.

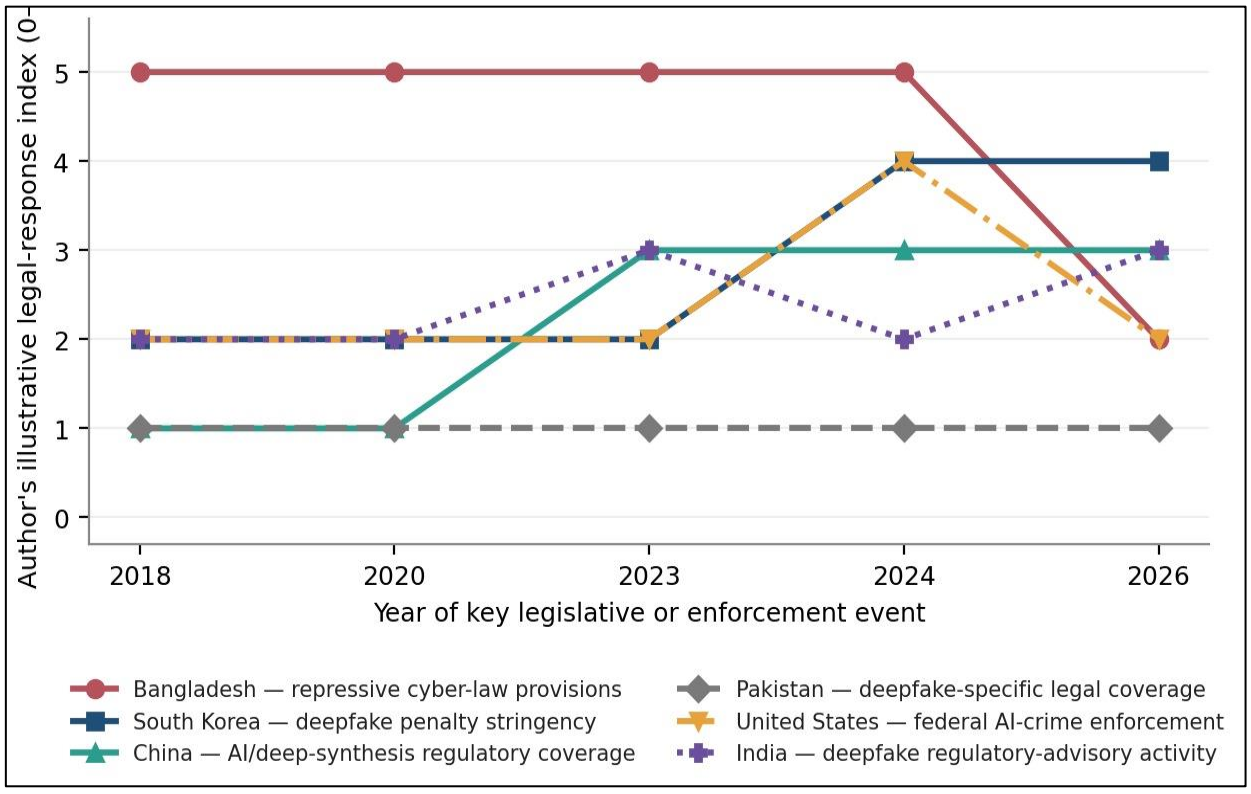


Figure 7.2: Legal-response trends in six countries, 2018–2026 (illustrative index) [22, 32, 34, 55–58]

South Korea and China tightened steadily. Bangladesh's express AI-offense clause arrived only in 2026, even as nine repressive provisions were repealed. Pakistan's 2025 amendment left deepfakes unaddressed, and enforcement in the United States and India rose and then stalled. Hugh Nelson's conviction nonetheless shows that existing indecent-image offenses can already reach synthetic material [31]. Bangladesh should therefore amend the Pornography Control Act 2012 to name synthetic imagery and add takedown and restitution rights for victims, while keeping existing offenses available, because clarity protects victims without requiring wholly new law [40, 59]. Because Bangladesh's position is best read regionally and not globally, Figure 7.3 narrows the comparison to four South Asian jurisdictions.

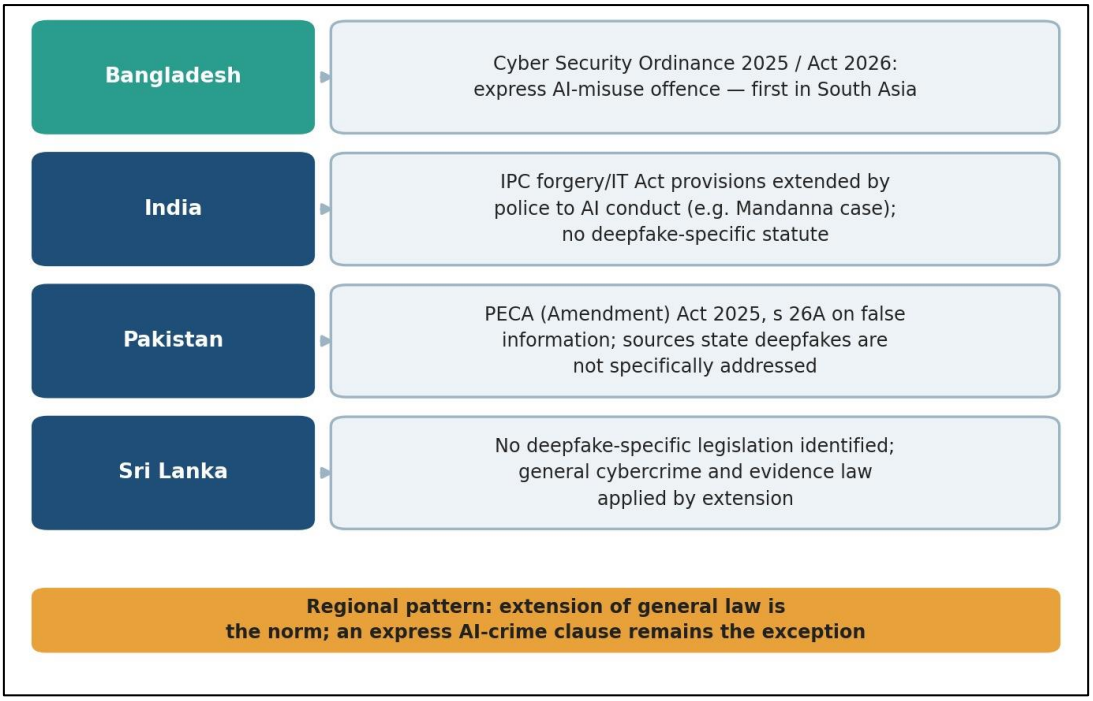


Figure 7.3: AI-crime legislative coverage across four South Asian jurisdictions [32, 60–62]

Election disinformation needs enforceable duties and not aspirations. The Election Commission's code should require labeling of synthetic content, and platforms should answer complaints within fixed time limits [24, 38]. These duties would give enforceable form to the Policy's proposed prohibition on election deepfakes [1, 37].

7.2 Building Readiness: An Adaptive Legal and Institutional Framework

Threat-specific fixes will fail without a coherent framework. Figure 7.4 sets out five linked reforms that mirror the readiness dimensions.

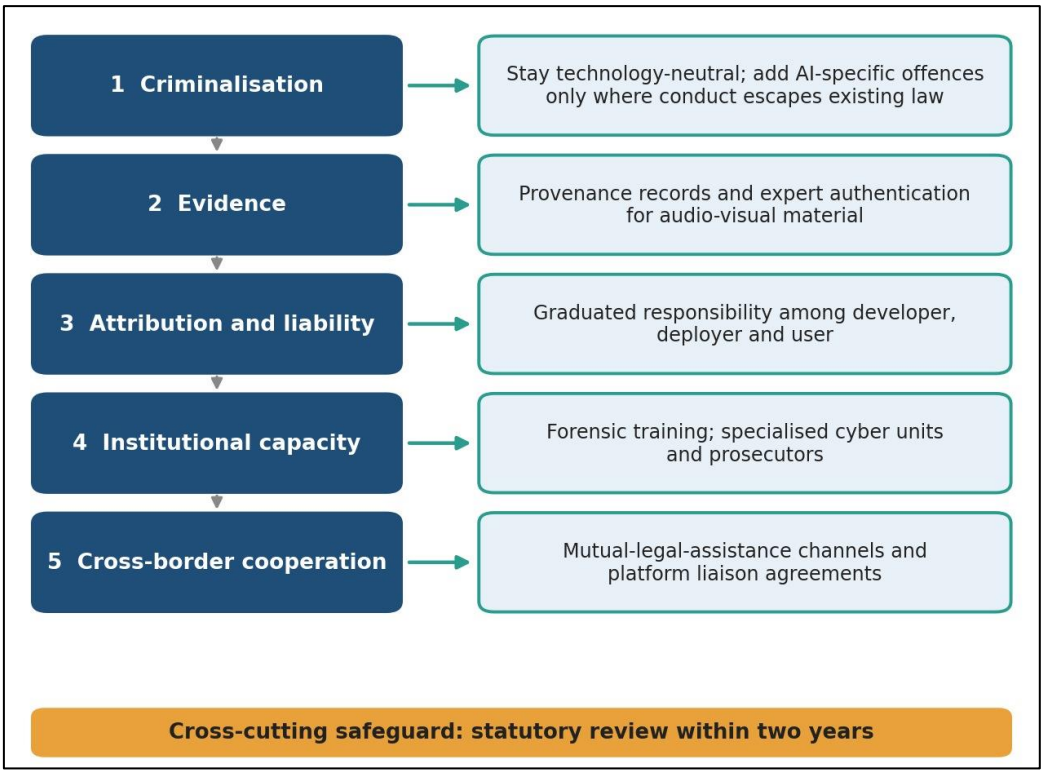


Figure 7.4: Proposed AI-responsive reform pathway

Criminalization should stay technology-neutral, adding AI-specific offenses only where conduct escapes existing law. *Evidence* rules should require provenance records and expert authentication, following the safeguards that courts adopted in *Loomis* and *Mata* [35, 36]. *Attribution* should be graduated among developer, deployer and user, as an attribution spectrum suggests, so that autonomy neither excuses nor over-criminalizes human actors [9]. The Policy's strict liability for deployers of high-risk AI suits regulatory and civil responsibility, but criminal liability should still require fault [1, 37]. *Capacity* requires forensic training and specialized units. *Cooperation* requires mutual legal assistance channels and platform liaison agreements, since a deepfake was removed in 2023 only after press inquiries [24]. The Policy's proposed oversight committee, which would audit AI systems for bias, could anchor capacity for police and judicial AI, and its commitment to ratify the Council of Europe Framework Convention on AI would support cooperation [1, 37, 41, 63].

Comparators supply working levers for these reforms. India fixes a three-hour takedown for unlawful synthetic content, two hours for intimate or impersonating imagery, and mandatory labeling [45, 64]. The United States criminalized synthetic intimate imagery and imposed a 48-hour platform takedown, enforced since May 2026, while South Korea raised its penalties [34, 50–52]. The Policy's proposed regulatory sandboxes could trial such deadlines before enactment [1, 2]. Figure 7.5 maps these levers to Bangladeshi reforms.

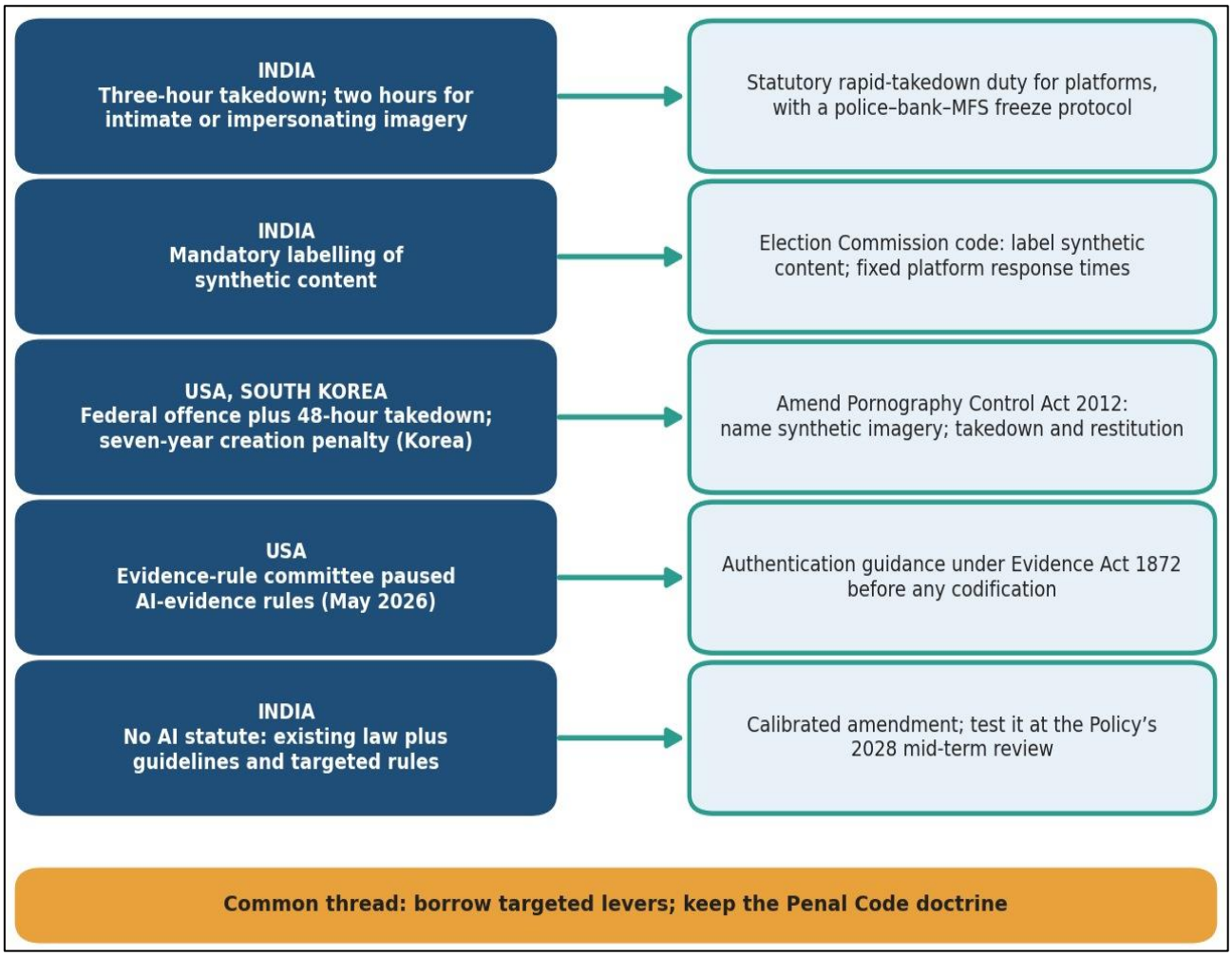


Figure 7.5: From USA and India levers to Bangladeshi reforms

Finally, because the cyber statute has been replaced repeatedly, Parliament should build in a statutory review after two years, as the Policy itself schedules a mid-term review in 2028. That would allow adaptation without another repeal [41]. These reforms close the gaps identified in Part 6 and prepare the normative argument of Part 8.

8. Discussion: Towards an AI-Responsive Criminal Justice Framework

8.1 The Amplification Path: AI as an Accelerant, Not an Architect, of Crime

This part argues and does not merely describe. On the first research question, AI is best read as an accelerant of familiar offending and not the architect of an unprecedented one. Figure 8.1 tests that claim against

the ten cases in section 4.3. In eight, an existing offense category (fraud, forgery, indecent images) or an established court procedure already reached the conduct. Only two turned on a newly enacted AI-specific provision [21, 24, 26, 28, 30–32, 34–36].

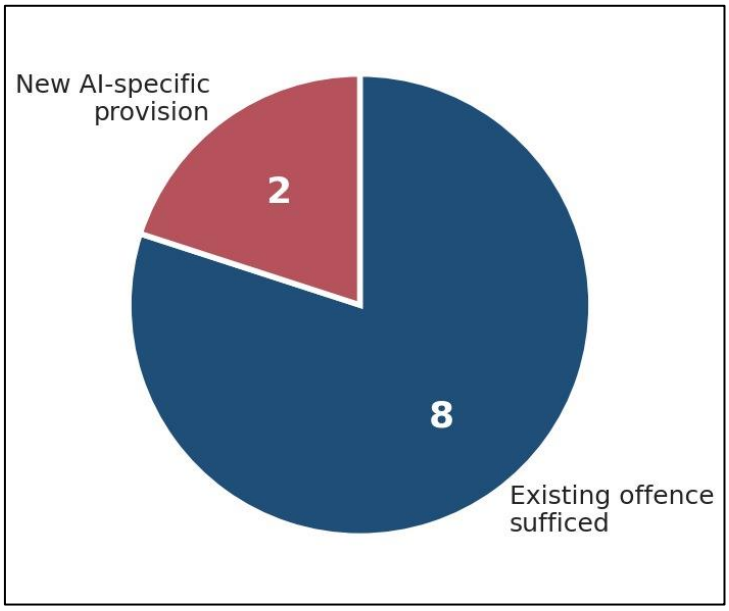


Figure 8.1: Legal basis for the ten cases in section 4.3

The exception proves the rule. Figure 8.2 scores each threat category from section 4.1 on an illustrative novelty index. Fraud, hacking and money laundering score low because AI mainly automates conduct the Penal Code already captures. Bias in judicial AI scores highest because a machine actor sits inside the adjudicative process itself, a structural novelty that no fraud or forgery provision anticipated.

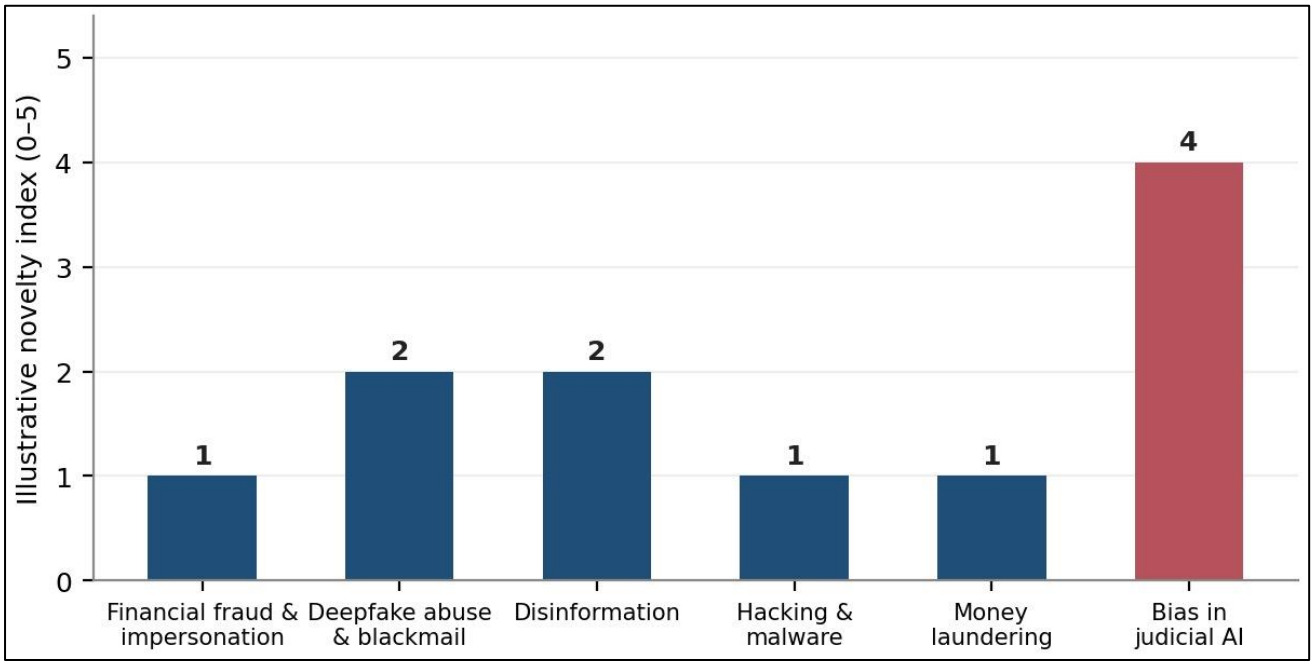


Figure 8.2: Illustrative novelty index across six threat categories (authors' classification, section 4.1)

Figure 8.3 models the continuum. Human intent (the circle) is channeled through AI instrumentality shared among developer, deployer and user (the triangle) into an existing offense category (the quadrangle). Only where the arrows cannot close, as with algorithmic bias, does new criminalization become necessary. Part 6's finding that Bangladesh's exposure concentrates in fraud and impersonation therefore favors extending, not replacing, the Penal Code and the Cyber Security Act 2026.

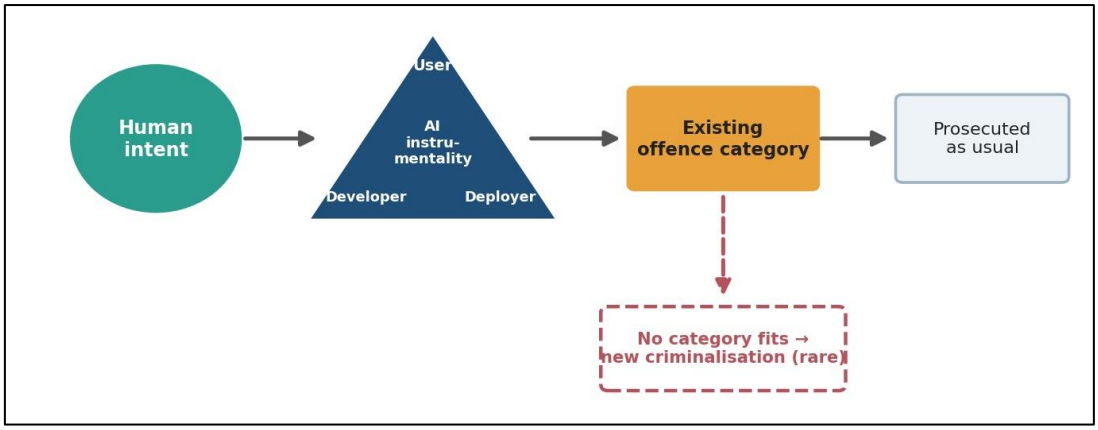


Figure 8.3: The amplification model of AI-enabled crime

8.2 The Calibration Path: Why Bangladesh Needs Adaptive Reform, Not a New Code

The second research question invites a normative choice between replacing the framework and calibrating it. Figure 8.4 tracks Bangladesh's five readiness dimensions from Table 6.1 across four legislative moments. Criminalization and cooperation commitments rise on paper, attribution stays flat, institutional capacity fluctuates because gains are not yet secured, and evidentiary readiness falls as synthetic media grows more convincing faster than authentication practice can match.

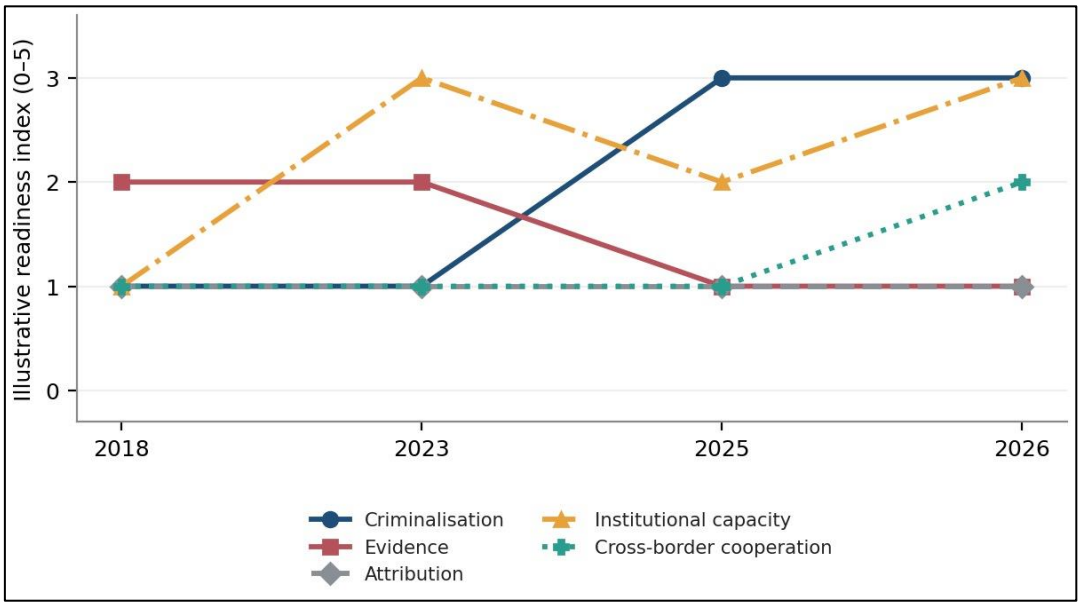


Figure 8.4: Bangladesh's five readiness dimensions, 2018–2026 (illustrative index; see Table 6.1)

Table 8.1 sets the two options side by side. A wholesale AI-crime code offers definitional clarity but risks obsolescence before enactment, given that the cyber framework has already passed through four instruments in under eight years [42]. Calibrated amendment is slower to signal but easier to revise, and it preserves the Penal Code doctrine on which prosecutors already rely.

Table 8.1: Two normative responses to Bangladesh's readiness gap

Criterion	Wholesale AI-crime code	Calibrated amendment
Speed of enactment	Slow: a comprehensive code takes years to draft and pass	Faster: targeted clauses added to existing Acts
Risk of obsolescence	High: the cyber framework has passed through four instruments since 2018	Lower: clauses can be revised without a full repeal
Institutional burden	High: new definitions, courts and training from scratch	Lower: builds on doctrine prosecutors already use
Doctrinal continuity	Weak: risks breaking from existing case law	Strong: forgery, fraud and evidence doctrine continues

The Policy itself reflects the calibrated logic. It is time-limited, subject to annual reporting and a 2028 mid-term review, and expected to give way to a permanent AI Act by 2030 [1, 37, 41]. The danger is that the 2030 Act becomes the wholesale code this section cautions against, so the 2028 review should test targeted amendments first.

Figure 8.5 places the choice geographically. Bangladesh sits closer in enforcement capacity to Pakistan and Sri Lanka than to South Korea or the United Kingdom. The more instructive comparators are therefore regional and not aspirational: calibrated reform modeled on peer capacity, reserving the fuller South Korean or British statutory approach for a later stage, once forensic and prosecutorial capacity has caught up [34, 57, 60–62].

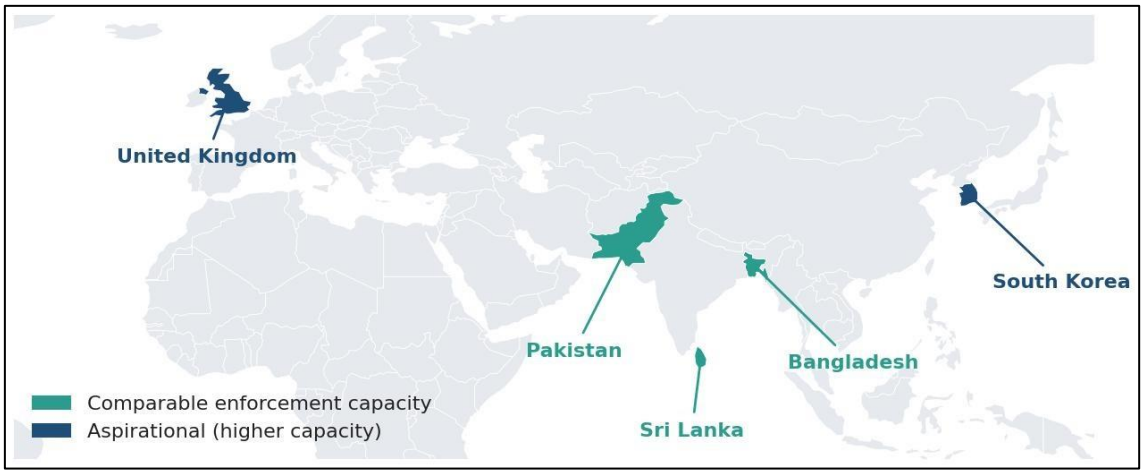


Figure 8.5: Comparator jurisdictions clustered by enforcement capacity

Two comparators illustrate the choice. India, whose February 2026 summit produced a non-binding declaration, has calibrated: it has no AI statute, but applies existing law together with targeted IT Rules [45–47]. The United States has one narrow federal statute, contested state laws, a preemption campaign and stalled evidence rulemaking [52, 54, 65]. The Policy borrows the European Union's risk tiers but, being unenacted, lacks India's enforcement rules [1, 41]. Figure 8.6 and Table 8.2 compare the three jurisdictions.

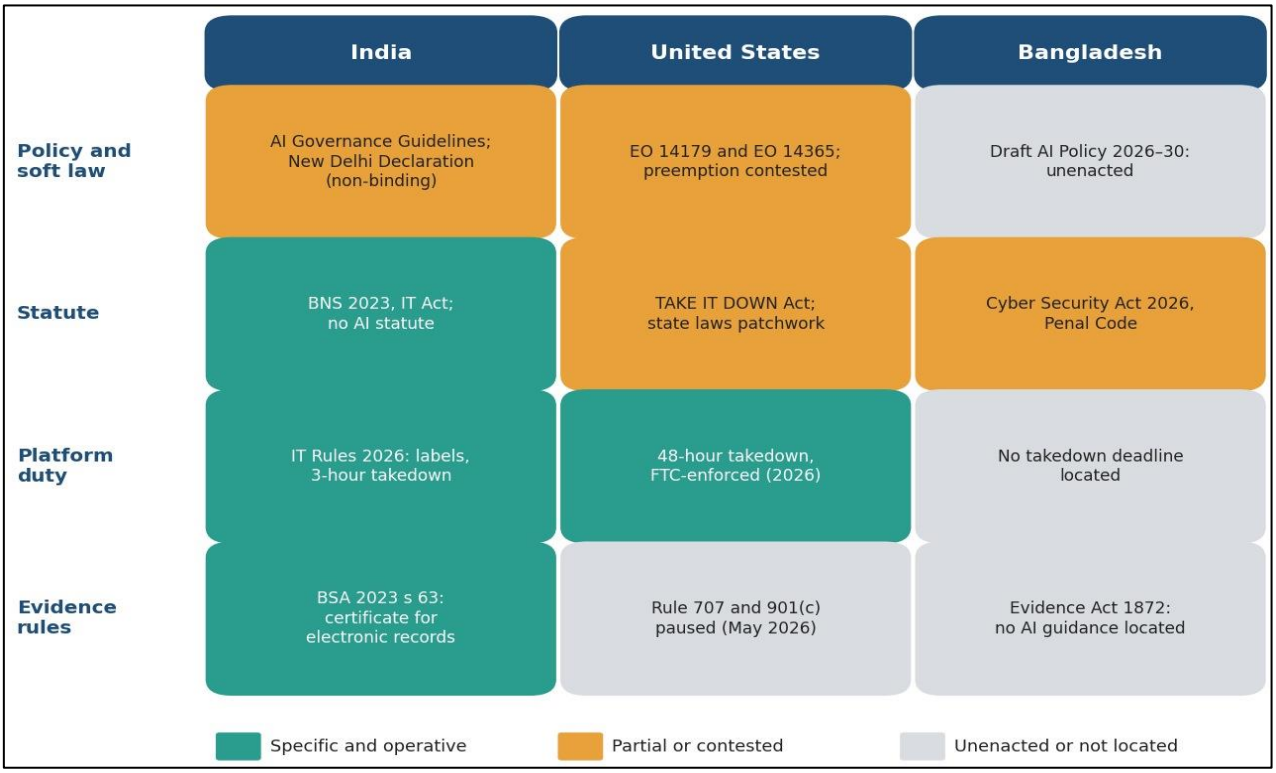


Figure 8.6: Legal architecture of India, the United States and Bangladesh [1, 43–54, 66–68]

Table 8.2: Readiness by dimension in three countries [41, 43–54, 69]

Dimension	India	United States	Bangladesh
Criminalization	Existing law plus rules	One federal statute	Existing law; Policy unenacted
Evidence	Electronic-record certificate	Rulemaking paused	Unresolved
Attribution	Graded liability proposed	Fragmented, state-led	Partly ready
Capacity	Three-hour takedown	FTC enforcement	Developing
Cooperation	Summit-led diplomacy	Rejects global AI governance	Weak; Convention pledge

Read together, sections 8.1 and 8.2 argue that Bangladesh's task is calibration on two fronts: extending existing offenses to reach AI-amplified conduct, and extending existing institutions to close the evidentiary gap, before any wholesale rewriting of the criminal code.

9. FINDINGS

Findings on the first research question. (1) Bangladesh's documented and plausible exposure concentrates in four of the six threat categories identified in section 4.1: AI-assisted financial fraud and impersonation, deepfake-enabled abuse and blackmail, AI-generated disinformation, and bias within AI tools used by the justice system itself. AI-assisted hacking and AI-facilitated money laundering are under-documented in the Bangladeshi sources reviewed. (2) Eight of the ten cases in section 4.3 were reached by existing offense categories or court procedures, and only two turned on a newly enacted AI-specific provision. This supports the amplification thesis that AI mainly intensifies familiar offending. (3) The Dhaka deepfake-advertising syndicate and the disinformation documented around the 2024 and 2026 elections confirm that these threats are already active in Bangladesh and are not merely speculative.

Findings on the second research question. (1) Table 6.1 rates Bangladesh partly ready. Criminalization and institutional capacity are improving, attribution is only partly addressed and confined to AI-assisted unauthorized access, cross-border cooperation is weak, and no settled practice for authenticating AI-generated material under the Evidence Act 1872 was located. (2) Bangladesh's enforcement capacity sits closer to Pakistan and Sri Lanka than to South Korea or the United Kingdom, so incremental amendment benchmarked against peers of comparable capacity is more defensible than importing a higher-capacity statutory model wholesale. (3) The cyber-law framework's own history of four instruments in under eight years is evidence that rapid wholesale replacement has not produced settled doctrine, which reinforces the case for calibrated, reviewable amendment over another full repeal. The Policy's risk tiers, impact assessments and oversight proposals do not alter these ratings while the Policy remains unenacted.

Together, the findings support one composite conclusion. Bangladesh's legal readiness is uneven and not absent, and it is best advanced by targeted extension of existing law, particularly on evidentiary authentication and cross-border cooperation, and not by inaction or by a wholesale AI-crime code.

10. Future Directions

Four directions extend this research.

Empirical testing. Because this paper is doctrinal and excludes interviews, future work should test the amplification and calibration theses through structured interviews with CID officers, prosecutors and judges. That would show whether the evidentiary gap identified in Part 8, which this paper infers from documented incidents, is experienced in practice.

Tracking the Cyber Security Act 2026. The Act is too recent for reported adjudication. Its application to the Dhaka deepfake-advertising case and to later cases should be followed, together with the Policy's 2028 mid-term review, because the Act's practical reach cannot be assessed from its text alone.

Authentication standards. Standards for AI-generated evidence under the Evidence Act 1872 remain unaddressed in the sources reviewed. Comparative work on provenance and expert-authentication rules, of the kind courts in *Loomis* and *Mata* improvised without legislation, would give Bangladeshi courts a firmer basis than case-by-case improvisation.

Regional coordination. The South Asian comparison in section 7.1 suggests a regional agenda. Comparable-capacity jurisdictions across SAARC face a similar readiness gap, so coordinated standard-setting under the SAARC framework may achieve more than each member state legislating alone. India's non-binding New Delhi Declaration of 2026 offers a starting forum [47, 48]. Figure 10.1 sets the four directions on an indicative timeline, from near-term monitoring to longer-term regional coordination.

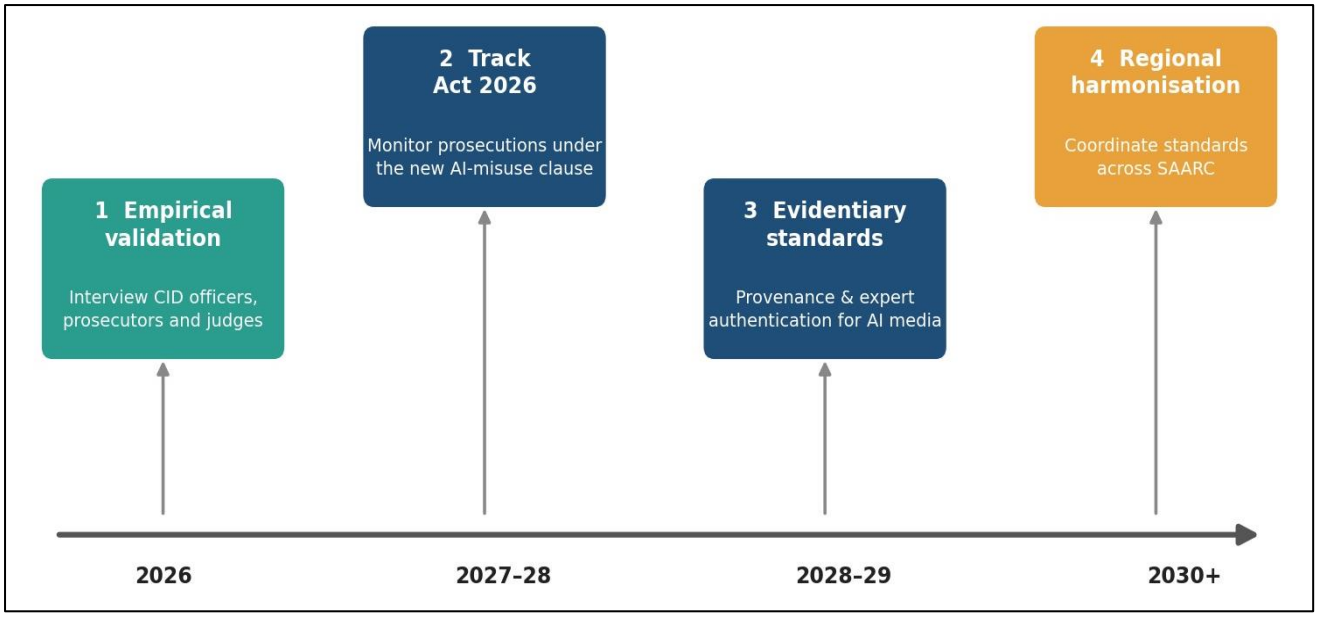


Figure 10.1: Indicative roadmap for future research, 2026–2030

11. CONCLUSIONS

This paper asked what AI-enabled crimes threaten criminal justice in Bangladesh and how prepared the legal system is to meet them. On the first question, the threat is concentrated and not diffuse. It lies in financial fraud and impersonation, deepfake-enabled abuse, disinformation and bias within judicial AI, and it is already active in Bangladesh and is not merely a foreign or future concern. On the second question, the response should be calibrated and not wholesale. The Penal Code and the Cyber Security Act 2026 already reach most AI-amplified conduct, and the more urgent gaps lie in evidentiary authentication, institutional capacity and cross-border cooperation, and not in substantive criminalization alone. The Policy offers a vehicle for this calibration, provided its proposals are enacted and tested against criminal-law doctrine.

The paper's contribution is to test these claims against ten documented cases and a regional and comparative benchmark, and not to assert readiness or its absence in the abstract. It also shows that Bangladesh's own cyber-law history, four instruments in under eight years, is itself an argument for calibration over repeated replacement. The analysis is provisional. It rests on doctrinal and comparative method and not on interviews or quantitative data, and several of its indices are the authors' own constructs and not official measures. Within those limits, the paper concludes that Bangladesh is partly and unevenly ready, and that closing the remaining gaps is a task of calibrating evidence rules, institutional capacity and regional cooperation, not of wholesale legal reinvention.

Acknowledgements

The authors declare that this research paper was conducted, written and completed entirely by the authors without financial support, grants or external assistance from any individual, institution or organization.

Conflict of Interest

The authors declare that they have no conflict of interest regarding the publication of this manuscript.

Use of AI Tools

During the preparation of this work, the authors utilized several artificial intelligence (AI) and assisted technologies to support specific stages of the research workflow. ChatGPT and Elicit were employed to assist in the initial stages of selecting the research topic, identifying relevant research gaps, and drafting initial conceptual frameworks. For the literature review, academic databases were explored alongside AI-powered discovery and synthesis tools, including Google Scholar, Elicit, and Perplexity, to locate relevant peer-reviewed studies. To enhance the clarity, grammar, and academic tone of the manuscript, text refinements were processed through ChatGPT and Grammarly. Visual aids and figures included in this paper were generated or enhanced using ChatGPT and Google Gemini. Finally, to ensure academic integrity and compliance with institutional standards, the final manuscript was evaluated for originality and AI-generated content thresholds using Turnitin. The authors reviewed, verified, and edited all outputs generated by these tools and accept full responsibility for the accuracy, authenticity, and overall integrity of the final content.

REFERENCES

1. Information and Communication Technology Division. (2026, February 9). *National AI Policy 2026–2030* (Draft v2) [Draft policy, not yet enacted].
2. The Financial Express. (2026, January 29). Draft AI policy tightens state oversight. *The Financial*

Express (Dhaka). https://thefinancialexpress.com.bd/national/draft-ai-policy-tightens-state-oversight

3. King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics, 26*, 89.
4. Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science, 9*, Article 14.
5. Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3191790
6. Al Qatawneh, I. S., Moussa, A. F., Haswa, M., Jaffal, Z., & Barafi, J. (2023). *Artificial intelligence crimes* [Working paper].
7. Dhiman, S., & Singh, S. (2025). *Cybercrime and computer forensics in epoch of artificial intelligence in India* [Working paper].
8. Velasco, C. (2022). *Cybercrime and artificial intelligence: An overview of the work of international organizations on criminal justice and the international applicable instruments* [Working paper].
9. Christina, A. M. (2026). Strengthening the criminal law system for national defense against automated cyber attacks based on "artificial intelligence." *West Science Law and Human Rights, 4*(1), 10.
10. Wisnubroto, A., & Tegnan, H. (2025). *Preventing AI crime towards a new legal paradigm: Lessons from United States* [Working paper].
11. Sun, J., Gu, S., & Su, R. (2026). *AI-empowered responsive regulation for preventing future crimes: An empirical inquiry into the regulatory pyramid to combat future crimes in China and Southeast Asia* [Working paper].
12. Ni, L. (2025). *The dimension and limit of criminal sanction thinking of artificial intelligence "deep counterfeiting"* [Working paper].
13. Sandoval, M. P., de Almeida Vau, M., Solaas, J., & Rodrigues, L. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science, 13*, Article 41. https://doi.org/10.1186/s40163-024-00239-1
14. Murray, P. E. (2025). Crimebots and lawbots: Cyberwarfare powered by generative artificial intelligence. *Transactions on Engineering and Computing Sciences, 13*(2), 29. https://doi.org/10.14738/tmlai.1302.18401
15. Ferdinal, O., & Bakir, H. (2024). *Legal protection efforts and policies to combat deepfake porn crimes with artificial intelligence (AI) in Indonesia* [Working paper].
16. Milon, M. N. U. (2024). *Gravitating towards artificial intelligence on anti-money laundering: A PRISMA based systematic review* [Working paper].
17. Roy, S. (2024). *AI adoption to combat financial crime: Study on natural language processing in adverse media screening of financial services in English and Bangla multilingual interpretation* (arXiv:2412.12171). arXiv. https://arxiv.org/abs/2412.12171
18. Malek, M. A. (2022). *Criminal courts' artificial intelligence: The way it reinforces bias and discrimination* [Working paper].
19. Nabi, M. M., Akter, M., & Fahim, M. B. (2026). The emerging threat of unlawful AI usage: A comprehensive content analysis in Bangladesh and worldwide. *Journal of South Asian Issues, 1*(1), 140. https://doi.org/10.65826/JSAI.1.1.2026.49
20. Kumar, O. K. N. (2025). Cultural loss in the shadow of copyright: Piracy and the preservation of lost media in India. *Indian Journal of Legal Review, 5*(14), 1116.
21. BSS. (2026, April 25). Ten held for using AI deepfake ads of prominent figures to sell illegal drugs. *BSS* (Dhaka). https://www.bssnews.net/others/381263
22. bdnews24.com. (2025, May 23). Bangladesh scraps controversial Cyber Security Act, introduces new AI-focused cyber safety ordinance. *bdnews24.com*. https://bdnews24.com/bangladesh/a275a547a07a
23. The Daily Star. (2026, April 8). 20 ordinances lose validity. *The Daily Star* (Dhaka).
24. The Daily Star. (2023, December 14). AI disinformation disrupting Bangladesh's election: Report. *The Daily Star* (Dhaka). https://www.thedailystar.net/news/bangladesh/elections/news/ai-disinformation-disrupting-bangladeshs-election-report-3494641
25. Global Voices. (2026, April 1). How artificial intelligence and synthetic reality shaped Bangladesh's 2026 election. *Global Voices*. https://globalvoices.org/2026/04/01/how-artificial-intelligence-and-synthetic-reality-shaped-bangladeshs-2026-election/
26. CNN Business. (2024, May 16). Arup revealed as victim of $25 million deepfake scam involving Hong Kong employee. *CNN Business*. https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk
27. saunders.co.uk. (2026, February 11). *Who is liable in a workplace deepfake fraud incident?*
28. China Daily. (2023, June 1). Authorities warn public against AI fraud. *China Daily*. https://subsites.chinadaily.com.cn/wic/2023-06/01/c_891623.htm
29. Federal Communications Commission. (2024, May 23). *FCC proposes $6 million fine for illegal robocalls that used Biden deepfake generative AI voice message* [Press release].
30. New Hampshire Public Radio. (2025, June 13). Political operative who admitted to creating fake Biden robocalls found not guilty. *New Hampshire Public Radio*. https://www.nhpr.org/nh-news/2025-06-13/political-operative-fake-biden-robocalls-nh-primary-found-not-guilty
31. The Washington Times. (2024, October 28). Hugh Nelson sentenced to 18 years for using AI to make

child sexual abuse imagery. *The Washington Times*. https://www.washingtontimes.com/news/2024/oct/28/hugh-nelson-sentenced-18-years-using-ai-make-child/
32. Business Standard. (2024, January 21). Rashmika Mandanna thanks Delhi Police after deepfake video creator arrested. *Business Standard* (New Delhi). https://www.business-standard.com/india-news/rashmika-mandanna-thanks-delhi-police-after-deepfake-video-creator-arrested-124012100166_1.html
33. The Statesman. (2024, January 20). Delhi Police arrests Andhra engineer in Rashmika Mandanna deep fake video case. *The Statesman*. https://www.thestatesman.com/india/delhi-police-arrests-andhra-engineer-in-rashmika-mandanna-deep-fake-video-case-1503261562.html
34. AsiaOne. (2024, September 27). South Korea to criminalise watching or possessing sexually explicit deepfakes. *AsiaOne*. https://www.asiaone.com/asia/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes
35. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
36. *Mata v. Avianca, Inc.*, 678 F. Supp. 3d 443 (S.D.N.Y. 2023).
37. The Daily Star. (2026, January 26). Draft AI policy targets innovation, better public services. *The Daily Star* (Dhaka). https://www.thedailystar.net/business/economy/news/draft-ai-policy-targets-innovation-better-public-services-4090431
38. The Samakal. (2025, September 20). Rising fake videos, disinformation threaten elections, EC's capacity questioned. *The Samakal* (Dhaka). https://en.samakal.com/bangladesh/170843777/rising-fake-videos-and-disinformation-threaten-elections-ec%E2%80%99s-capacity-questioned
39. The Daily Star. (2025, March 20). Reconstructing society: Lessons from a cybercrime case. *The Daily Star* (Dhaka). https://www.thedailystar.net/opinion/views/news/reconstructing-society-lessons-cybercrime-case-3853066
40. BSS. (2026, January 21). CID arrests cyber fraudster for blackmailing Bangladeshi woman in US. *BSS* (Dhaka). https://www.bssnews.net/others/353486
41. Policy Magazine. (2026, January 28). *Bangladesh's AI moment: Testing the implementation gap*. https://www.policymagazine.ca/?p=86978
42. The Daily Star. (2025). Cyber security laws in Bangladesh: The ties that bind our past and present. *The Daily Star* (Dhaka). https://www.thedailystar.net/law-our-rights/news/cyber-security-laws-bangladesh-ties-bind-our-past-and-present-3914171
43. Bharatiya Nyaya Sanhita, 2023 (India).
44. Information Technology Act, 2000 (India).
45. Hogan Lovells. (2026). *India introduces mandatory labelling for AI and 3-hour takedown for illegal content*. https://www.hoganlovells.com/en/publications/india-introduces-mandatory-labelling-for-ai-and-3hour-takedown-for-illegal-content
46. Khaitan & Co. (2025, November 11). *India AI governance guidelines*. https://www.khaitanco.com/sites/default/files/2025-11/ERGO%20-%20India%20AI%20Governance%20Guidelines%20-%2011%20November%202025.pdf
47. Basrur, A. (2026, March 30). *From dialogue to deployment: Strategic outcomes of the India AI Impact Summit 2026*. ORF. https://www.orfonline.org/expert-speak/from-dialogue-to-deployment-strategic-outcomes-of-the-india-ai-impact-summit-2026
48. NeGD. (n.d.). *AI Impact Summit 2026 concludes with adoption of New Delhi Declaration*. https://negd.gov.in/press_release/ai-impact-summit-2026-concludes-with-adoption-of-new-delhi-declaration/
49. PMF IAS. (n.d.). *New Delhi Declaration on AI Impact: Significance & challenges*. https://www.pmfias.com/?p=728103
50. TAKE IT DOWN Act, Pub. L. No. 119-12 (2025) (United States).
51. Skadden. (2025, June). *"Take It Down Act" requires online platforms to remove unauthorized intimate images and deepfakes when notified*. https://www.skadden.com/insights/publications/2025/06/take-it-down-act
52. Vorp Labs. (n.d.). *United States: AI regulatory updates*. https://vorplabs.com/ai-regulatory-updates/united-states
53. Advisory Committee on Evidence Rules. (2026, May 7). *Agenda book*. Judicial Conference of the United States. https://www.uscourts.gov/sites/default/files/document/2026-05_evidence_rules_agenda_book.pdf
54. Baker Botts. (2026, June 18). *Federal evidence rulemaking on AI hits pause: An EDVA update*. https://www.bakerbotts.com/thought-leadership/publications/2026/june/federal-evidence-rulemaking-on-ai-hits-pause-an-edva-update
55. ASIS International. (2023, May 23). *Case in China highlights the need for legal framework to deal with deepfakes*. https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2023/may/china-deepfake-fraud-and-ai-laws/
56. regulations.ai. (n.d.). *Prevention of Electronic Crimes (Amendment) Act, 2025 – Pakistan*. https://regulations.ai/regulations/RAI-PK-NA-PECA2XX-2025
57. The Friday Times. (2026, August 19). Can laws of Pakistan keep up with the misuse of AI? *The Friday Times*. https://www.thefridaytimes.com/19-Aug-2026/can-laws-pakistan-keep-misuse-ai

58. Courthouse News Service. (2025, June 13). N.H. jury acquits consultant behind AI robocalls mimicking Biden on all charges. *Courthouse News Service*. https://www.courthousenews.com/new-hampshire-jury-acquits-consultant-behind-ai-robocalls-mimicking-biden-on-all-charges/
59. Pornography Control Act, 2012 (Bangladesh).
60. The Daily Star. (2025, May 11). Combating deepfakes in Bangladesh: Legislation to public empowerment. *The Daily Star* (Dhaka). https://www.thedailystar.net/tech-startup/news/combating-deepfakes-bangladesh-legislation-public-empowerment-3892336
61. SSRN. (2026, April 2). *Synthetic media, stolen identities and silent laws: Why Pakistan's 241 million people have no legal protection against AI-generated deepfakes*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7238118
62. Deepfakes in the Global South: Understanding stakeholder perceptions. (n.d.). *tsjournal.org*. https://tsjournal.org/index.php/jots/article/download/319/106/1159
63. Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (CETS No. 225). Opened for signature 5 September 2024.
64. Freshfields. (2026). India targets deepfakes and AI-generated content: Key changes under MeitY's 2026 amendments. *Technology Quotient*. https://technologyquotient.freshfields.com/post/102mjwn/india-targets-deepfakes-and-ai-generated-content-key-changes-under-meitys-2026
65. Ensuring a National Policy Framework for Artificial Intelligence, Exec. Order No. 14365 (2025) (United States).
66. Bharatiya Sakshya Adhiniyam, 2023, § 63 (India).
67. Evidence Act, 1872 (Bangladesh).
68. Cyber Security Act, 2026 (Bangladesh).
69. RSF. (2026). *The right to reliable information: The gaping hole in India's AI Impact Summit declaration*. https://rsf.org/en/right-reliable-information-gaping-hole-india-s-ai-impact-summit-declaration