Victims of AI: Addressing the Legal Response Gap to AI-Related Crimes in Bangladesh

M Sabbir Ahmed Shihab[1], Mostafizur Rahaman[2], Md. Omar Faruk Shakib[3], Md. Easin[4*]

[1]Lecturer, Department of Computer Science and Engineering, CCN University of Science and Technology, Cumilla, Bangladesh

[2]Assistant Professor and Chairman, Department of Law, CCN University of Science and Technology, Cumilla, Bangladesh

[3] Undergraduate Student, Department of Law, CCN University of Science and Technology, Cumilla, Bangladesh

[4]Lecturer in Public Administration, Department of Law, CCN University of Science and Technology, Cumilla, Bangladesh

[*]Corresponding Author

DOI: https://dx.doi.org/10.51244/IJRSI.2026.130200194

Received: 04 February 2026; Accepted: 10 March 2026; Published: 21 March 2026

ABSTRACT

AI technologies improving rapidly in Bangladesh have eased the path to novel forms of digital harm, such as deepfake harassment (using manipulated videos or images to create false representations), AI-assisted impersonation (using AI to mimic someone's identity), extortion, phishing, and algorithmic discrimination (bias in automated decision-making processes). This scenario raises doubts about the robustness of our current legal system in safeguarding individuals from AI-induced harm. The study examines the absence of a legal response to violence against women in Bangladesh by asking if laws are sufficient, whether institutions are prepared and capable of assisting victims and how accessible justice is for them. Using a mixed-methods approach, we analyzed survey data from 435 respondents aged 18–35 and two case studies of AI-generated deepfake harassment and blackmail. Overall, the results show that a majority of respondents (55%) perceive AI misuse as "very common," with women and children being perceived as particularly vulnerable groups. In addition, most respondents (65%) believe that existing laws and regulations are inadequate at preventing new harms caused by AI. The report also says that most people support new or updated laws and that digital literacy is a good way to stop problems before they happen. The paper concludes that to address the legal response deficit and ensure robust protection in an AI-driven society, Bangladesh requires victim-centered legal reform, enhanced digital forensic capabilities, clear liability regulations, and a more cohesive framework for AI governance.

Keywords: Artificial Intelligence, AI-related Crime, Deepfake, Cybercrime, AI Governance, Legal Response, Bangladesh.

INTRODUCTION

The swift incorporation of artificial intelligence (AI) into contemporary social, economic, and administrative frameworks has significantly reshaped the functioning of digital communication and modern governance. Bangladesh's push to modernize its digital infrastructure, a key part of its development strategy, has fueled the rapid integration of AI technologies across various industries. This includes areas such as social media, e-governance, healthcare, telecommunications, and financial services. These emerging technologies could very well supercharge productivity, fuel economic expansion, and spark a wave of new ideas.

However, the rise of AI-related crimes presents complex legal and regulatory challenges, especially in places where current laws are designed to address traditional cybercrimes or offenses committed by individuals.

Machine learning algorithms, generative AI systems, and automated decision-making tools can be used in ways that lead to fraud, identity theft, the spread of false information, the misuse of surveillance, and algorithmic bias. For example, deepfake technologies can make very realistic audio and video that then undermines the reliability of digital evidence. The laws that govern criminal accountability are mainly the 1860 Penal Code, the 2023 Cyber Security Act (formerly the 2018 Digital Security Act) and various other ICT-related laws, all of which maintain a focus on particular identifiable individuals and purposeful malfeasance. But these provisions are poorly equipped to address cases involving AI systems that can operate independently or with very limited human oversight or monitor algorithms and international technology providers. Pinpointing blame becomes increasingly complex, as does identifying the cause and assigning responsibility. When algorithmic outputs lead to negative consequences, it's a real challenge to determine who bears the fault. Is it the developer, the entity that deployed the algorithm, the user who interacted with it, or the platform that served as the intermediary?

Furthermore, the standards governing evidence and investigative methodologies often prove inadequate when addressing digital content generated or modified by artificial intelligence, leading to challenges in holding responsible parties accountable for the harm caused by these technologies. Furthermore, the algorithmic processes that drive public service provision, credit assessments, and employment practices can yield unfair or biased results, particularly when those impacted lack the necessary expertise to initiate legal proceedings. People who experience problems related to artificial intelligence often face obstacles in the legal system, receive insufficient help from relevant organizations, or don't know what legal options are available to them.

This systemic shortcoming not only erodes public trust in digital systems and regulatory entities but also impedes access to justice. Such changes capture the large-scale "legal response gap" embedded in Bangladesh's existing regulatory system. The laws that govern criminal accountability are mainly the 1860 Penal Code, the 2023 Cyber Security Act (formerly the 2018 Digital Security Act) and various other ICT-related laws. All of that maintains a focus on particular identifiable individuals and purposeful malfeasance.

Conversely, these stipulations are less effective in addressing scenarios involving autonomous AI systems or those necessitating minimal human intervention, given their insufficient capacity to navigate the intricacies of accountability when machines, rather than humans, initiate actions. Current investigations indicate that a legal framework emphasizing victim protection and proactively considering future advancements is essential for mitigating the escalating risks linked to artificial intelligence.

Rationale of the study:

As the trend of using the internet and digital services in the digital economy increases in Bangladesh, traditional works as well as artificial intelligence-based crimes also increase rapidly. That, of course, implies that victims are exceptionally fragile and there’s been an immeasurable chasm in how the judicial system has responded. At the beginning of 2024, Bangladesh had well over 77 million internet users, and that number is rapidly increasing as social media becomes more accessible and business goes online.

Cybercriminals always have an advantage because they can reach millions of online communities to deceive individuals; national cybercrime data indicates a significant increase in incidents of this nature, such as app-based fraud and online scams. Some statistics go as far as to reveal that the rate of some types of cybercrime is up by 382% in a single year, which only goes to show how widespread digital victimization is. The critical dangers from AI are growing even faster across the board (The Daily Star). To illustrate, deepfake cases went from hundreds of thousands in 2023 to millions by 2025. Next year, identity fraud with AI content will occur at a frequency of every five minutes; AI-powered cyberattacks actually increased by more than 47% in 2025. Generative AI tools were increasingly leveraged in advanced phishing and impersonation schemes (SQ Mag). While these trends are concerning, there isn't much in the way of guidance from current laws about who should be held accountable when AI systems go wrong, how to define an AI-related crime, or what different ways a person can get justice if they were hurt. In other words, people and groups don't walk through crowded streets looking for justice.

This basic research is needed to make a map of the risks that come from AI, find holes in the law that let these harms happen without being fixed, and come up with regulatory and legal solutions that will protect victims in

a digital age driven by AI.

Conceptual Framework:

The Present study utilizes Victim Protection & Access to Justice as the main dependent variable. The framework examines how the widespread availability of technology and gaps in legal-regulatory spaces exacerbate victims' vulnerability (most importantly to access legal remedies), focusing on Bangladesh.

Independent variables	Dependent Variables
• Nature and Complexity of AI-related Crimes	**Level of Victim Protection & Access to Justice in AI-related Crimes**
• Adequacy of Existing Legal Framework	
• Institutional and Enforcement Capacity	
• Regulatory and Policy Governance of AI	
• Legal Response Gap	
• Legal Framework Inadequacy	
• Weak Institutional Capacity	
• Limited AI Governance	
• Clarity level in defining AI-generated offences	
• AI-assisted phishing and financial scams	
• Level of algorithmic discrimination	
• Availability of victim compensation mechanisms	

There are many crimes related to AI in Bangladesh, as per the framework. and it is not so much the crimes themselves that command how much protection victims get from existing laws and institutions but rather how well these entities respond to those crimes. When technology is ahead of regulation, there is a gap in the law and leads to less accountability and sub remediations being offered at the expense of protecting the victim. Specialized legal reform, institutional fortification and formalized renditions of AI governance can close the response gap significantly and provide far superior protections for victims.

Research Objectives

Broad Objective

- Evaluate the sufficiency of Bangladesh's legal framework to deal with AI-related offences and ensure effective protection for victims combat the crimes.

Specific Objectives

a. To reveal new types of AI-assisted crimes in Bangladesh.
b. To explore the gaps that may exist in current laws regarding harms related to AI.
c. List challenges around liability, enforcement, and remedies for victims;
d. To suggest legal and policy reforms to enhance victim protection.

LITERATURE REVIEW

(Ward et al., 2024) stated that people are concerned about AI risks when a specific person is presented as a victim in the story or presents the description of the incident. Present, true, or recognizable victims are more powerful than numerical victims. To raise awareness, this method is also used in the judgement of criminal justice cases and the evaluation of AI-generated sexual content. While (Falade, 2023) expressed that innovative models like ChatGPT and other new chatbot tools introduce us to creative opportunities and also bring us many challenges. Cybercriminals use this huge opportunity to control public opinion via social media and use deepfake videos and images, making realistic and individualized phishing messages. These new creative tools are used illegally for attacks on social engineering for spreading misinformation.

However, (Minhas et al., 2022) asserted authentic information is a necessary part of forensic investigation. In many cases, information given by the witnesses and victims is a primary source. When an incident occurs, the investigation authority should first collect the evidence because there's a risk of eliminating the information. To collect this information, some of the tools are used. If there's use of AICI tools, it is better than other tools like Free Recall and CI Basic chatbot. Whereas (Sutarya et al., 2025) reported AI-based child pornography means such a crime is based on the illegal use of fake images and videos and AI chatbots, which affects victims' mental, physical, and social growth. Even with the Child Protection Act, the relationship between the use of AI and the lagging of law is making new challenges in today's time. Legislative reform and inter-sectoral cooperation are necessary to address this issue.

(Mayeesha et al., 2024) explained developed countries recognize AI in ethical and accountable development and implementation of guidance of the discussion is continuing, but Bangladesh and other developing countries are ignored in this program. Bangladesh's citizens are unskilled and lack knowledge about data ethics in AI. It is a failure of the government. In contrast (Kupriianova & Kupriianova, 2023) describe that AI sexual models make women's dignity a "human desire" or "enjoyable thing." Scientific analysis said that the social media accounts that offer to upload sexual content, more than half of the total social media accounts, getting content by swap of money are either collected illegally from the people, making them victims, or, with proper use of AI tools, they created sexual models via the face substitute technique. This model has taken access to a social media account. Alternatively, (James, 2024) prescribed to protect victims' rights and give compensation for serious damage, both the Civil Act and the Criminal Act need remedy. For dealing with these issues, a federal law should be adopted and formulated, which will give fair remedies in these two of the Civil and Criminal Acts.

(Blauth et al., 2022) declared that especially, there are four types of misuse and harmful use of AI. The misuses are the following: data integrity invasion, unexpected outcomes of AI, systematic trade, fellowship presumption attacks, harmful use of independent weapons, cracking (data/system), false news, and control of social media. Conversely, (King et al., 2020) opined that AI can lead to autonomous fraud by targeting members on social platforms along with AI-empowered manipulation copies (simulated) exhibited in the markets. AI crime is now comparatively new and naturally a part of many branches that started socio-legally and widely spread into science. How AI crime will be in the future is a clear idea that we don't have at present. Nevertheless, (Caldwell et al., 2020) explained an 'AI upcoming crime' program organized for 2 days where law enforcement agencies, scholars, defence, government, and private authorities participated. They marked and evaluated a total of 18 main upcoming threats, where 6 threats are highly rated. Among them, 5 threats are society-wide influenced. Like, making deep fakes by AI-reliance activities or big crimes systematized by AI, and the 6th threat is misusing technology- using AI-driven vehicles (without drivers) for terrorist attacks.

(Liu et al., 2024) stated that at the time of natural disaster, any loan recipient who applies for a loan to AI-authorized lenders after the disaster is well positioned to reduce the delinquency percentage. However, (Biana & Domingo, 2024) described transport as one of the most violent and risky systems for women and young girls. To keep women safe, a modern system launched an AI-powered vehicle. This platform separated women from passengers and drivers. The initiative is not properly applicable for ensuring women are safe from harassment. Present AI tools are not handling the basic issue of gender inequality. Such separation makes it difficult to achieve equality between men and women in the society. Consequently, (Whittaker et al., 2018) analysed the day-by-day growth of the government's use of machine-created decision methods that instantly affect human beings and society without creating a responsibility framework. Increasing unauthorized and uncontrolled systems of AI research on mankind as well as liability lagging in AI, which benefits the one group that created and uses these tools at the cost paid by the suffering people.

In the same way (Schank, 1987) delivered that AI is a practice that finds the accurate system to utilize in presenting knowledge. AI's basic target is to create innovative tools, and another target is to search out the genesis of creativity. Subsequently, (Zhang et al., 2021) presented AI funding in the medicine sector remarkably increasing to above USD 13.8 billion, growing 4.5 times larger than in 2019. In Northern America, 65% of AI PhD graduates entered into industry in 2019. AI platforms can now create ordinary text, pictures, and audio, and humans have difficulty determining between man-made or natural outcomes for certain technological limitations. Civil society and scholars' perspective is that AI ethics are stronger than industrial corporations.

According to (Taddeo & Floridi, 2018) they assessed by completing the task, AI provides great advantages to society. Because of its lower costs, minimized risks, continuation, and responsibility, as well as the innovative explanations it introduces us to, e.g., AI technology can reduce 85% of diagnostic mistakes in breast cancer, and the AI cybersecurity framework can decrease the usual time to recognize and nullify the cyberattacks from a period of 101 days to a couple of hours.

Eventually, (Furman & Seamans, 2019) interpreted that AI has the capability to change the economy. When AI is combined with robotics, it can boost efficiency, which is especially necessary when there is a continuing decrease in productivity development. It may obstruct labour fields and reduce existing labor work participation, which would worsen the situation.

(Reed, 2018) scrutinized that AI poses risks that present laws and rules are not able to lead with sufficiently. Thus, modern rules shall be wanted. In many cases, the present system can perform beneficially if the creator of AI technology can give effective clarity in defining how AI actions are created. In the following section, (Tao et al., 2025) explored if, for mistakes committed by AI, citizens provide soft blame for the government, while they highly reproach the government for mistakes by human administrators. When people think that it is important that the capability of victims needs remedy, at that time they more highly reproach the government for their liability. The government is less responsible when the occurrence is made by AI; the victim's ability is considered for less remedy.

As a result (Maslej et al., 2025) assessed that day by day AI is progressively attached to daily life. From the medical sector to transit, AI is quickly evolving from the laboratory to everyday life. In 2023, AI-empowered 223 healthcare technology accepted by FDA, 6 times up from 2015. In vehicle technology, human-driven cars have stopped being an experiment, and U.S. technicians give more than 150,000 without-human-driver journeys in a week. In 2024, U.S.-founded organizations generated 40 innovative AI models, as opposed to China’s 15 and Europe's 3. In 2024, U.S. national authority provided 59 AI-associated rules and regulations, which was two times higher than in 2023.

METHODOLOGY

A mixed-methods (combination of qualitative and quantitative) approach has been used in the current study to explore AI-associated criminal activity and its legal issues for Bangladesh. The mixed-methods design enables a statistical examination of awareness, exposure and perceptions but also richly illuminates victim experiences and perspectives regarding legal protections. Multiple methods were combined as to increase the reliability and analytical rigor of the study.

Study Population and Sample

The study's participants were students in Bangladesh; aged range was between 18 to 35. This age group was chosen because of their significant use of digital technologies such as social media, and AI tools which increases their potential exposure to AI-related crime risks. A total of 435 respondents participated in the study. This paper also contained also two case studies related on AI related crimes in Bangladesh. Participants were drawn from different educational levels, including higher secondary, undergraduate, and postgraduate students. The initial selection process indeed took into account several factors.

Data was primarily collected using a semi-structured questionnaire via online. The sampling process was conducted by random sampling method. This questionnaire included both closed-ended and open-ended questions. The data collection process has been completed, and responses were compiled systematically for analysis.

Data Analysis

The quantitative data underwent analysis via SPSS (Statistical Package for the Social Sciences), facilitating the generation of descriptive statistics such as frequency distributions, percentages, and pertinent cross-tabulations. However, Microsoft Excel and Google Sheets were utilized for data analysis, organization, tabulation, and the graphical representation of the study's results.

Qualitative responses will be analyzed using a thematic analysis approach, to identify common themes relating to victimization patterns, awareness gaps identified and assessment of the effectiveness of the legal framework. An integrated interpretation will be accomplished through combining the outcomes obtained from both quantitative and qualitative analyses.

Ethical Considerations

Participation in this study was voluntary. Before taking part, participants were informed about the study's purpose. All data were used strictly for academic purposes; confidentiality and anonymity were ensured.

Limitations of the Study

This investigation constrained by several limitations that could potentially affect the breadth and depth of its conclusions. The study's temporal constraints curtailed the possibility of conducting comprehensive empirical research and longitudinal analyses of AI-related criminal activities within Bangladesh.

Funding for the project was limited and, as such, it constricted opportunities for large scale fieldwork, thorough technical reviews and access to specific databases and digital forensic analysis tools. We note that the very small number of respondents will impact how broadly the results are applicable across sectors and populations. Different participants also had varying levels of AI literacy, which posed challenges in obtaining technically detailed responses (Some respondents seemed to have little knowledge about AI technologies or their legal consequences). Lastly, Bangladesh's regulation of AI is still in its nascent and evolving stages, with a lack of official statistics and judicial rulings making it difficult to build a robust data set for analytical purposes.

Data Analysis

Age	Frequency	Percentage
18-24	417	96
25-35	18	4
18-35	435	100

Table 1: Age of the respondents

Table 1 presents the background, showing that 435 individuals (100%) took part in the investigation. Out of 435 respondents, the most participants belong to18–24 years age group (96%) (n:417). By comparison, just 18 respondents (4%) are aged between 25–35 years.

In summary, the data show that most of the sample is consolidated in people ages 18–24 suggestive of the study overrepresents younger adults. Very few players are in the 25–35 age group.

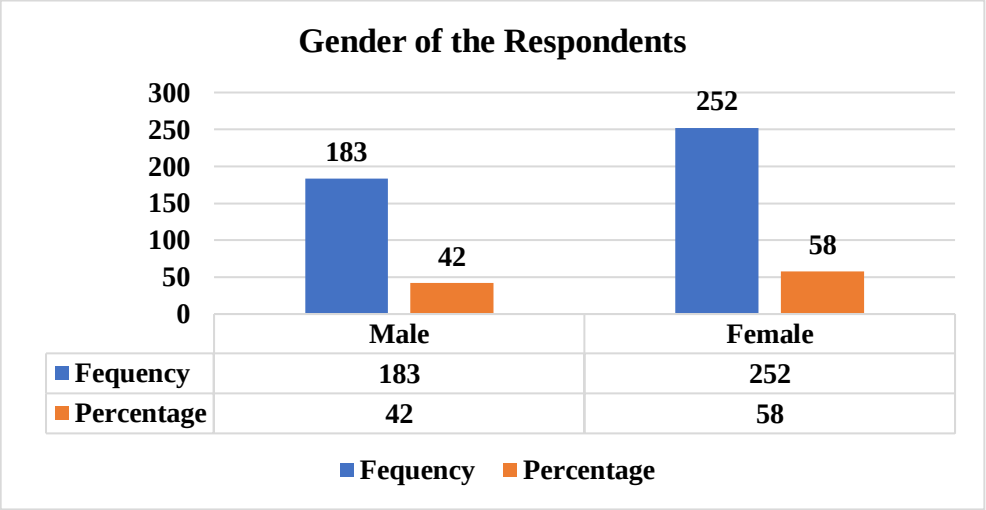
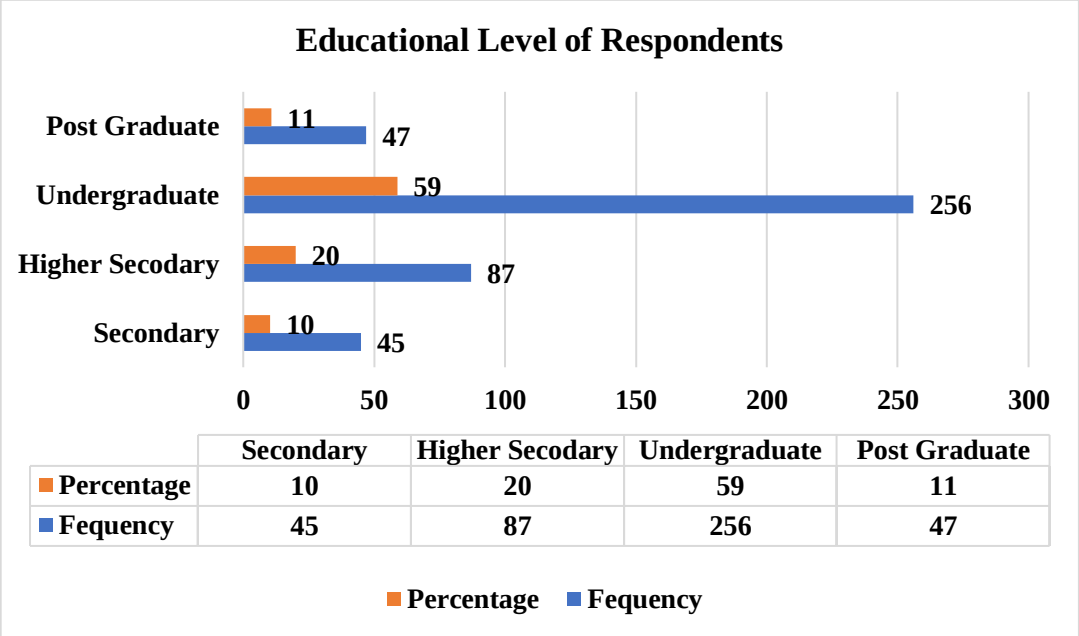


Chart 1: Gender of the Respondents

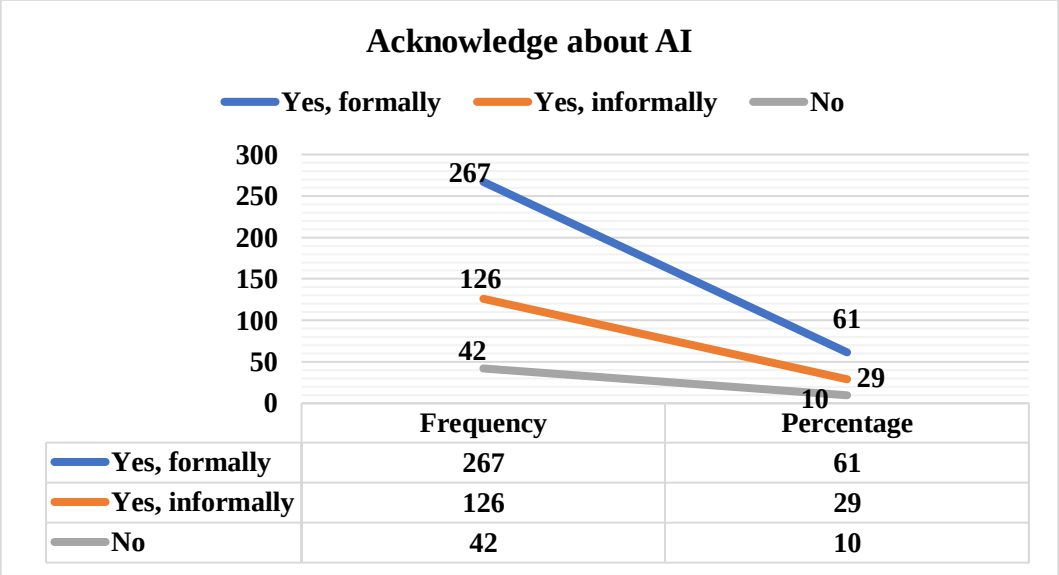
The chart 1 named "Gender of the Respondents" shows the frequency and percentage distribution of participants in terms of gender. In total, 435 responded (183 male - 42% of the sample; 252 female - 58%). However, the chart shows that there are more female respondents than male both numerically and as a percentage. This means that the sample of the study consists largely of women, but men are also a significant part of respondents.



	Secondary	Higher Secodary	Undergraduate	Post Graduate
Percentage	10	20	59	11
Fequency	45	87	256	47

Chart 2: Educational Level of Respondents

The chart 2 shows educational distribution of 435 respondents. 291 (71%) identified as students, with the majority being undergraduates: 256 (59%). The second largest group consists of 87 respondents (20%) with higher secondary education. Postgraduates consist of 47 respondents, (11%) and second-degree holders constitute the least, with only (45) 10% Descriptive statistics Overall, the sample is mainly constituted of individuals with undergraduate-level education.



	Frequency	Percentage
Yes, formally	267	61
Yes, informally	126	29
No	42	10

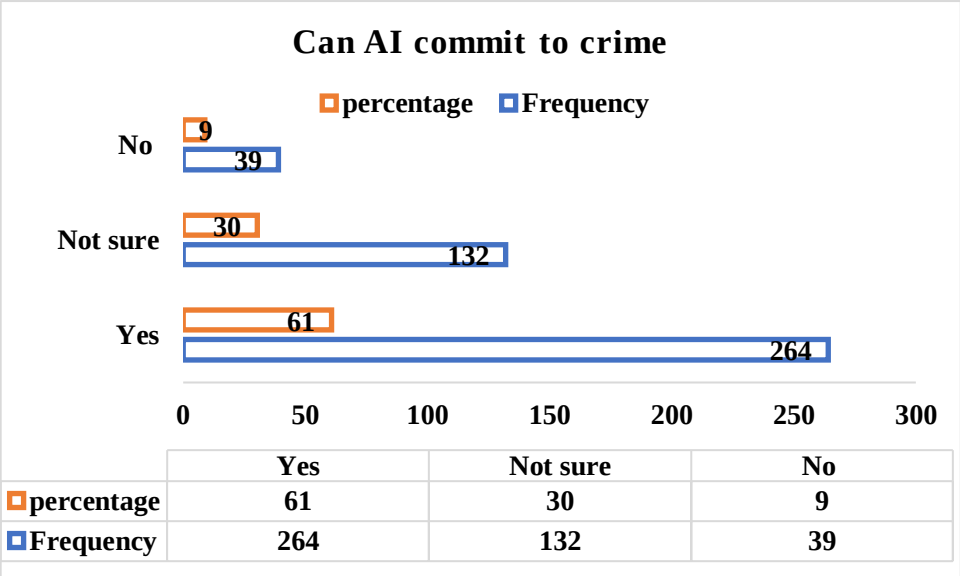
Chart 3: Acknowledge about AI

The chart 3 demonstrates the level of participation amongst respondents. The most common reported method for formal participation was: n = 267 (61%) Furthermore, 126 (29%) indicated that they participate informally. Meanwhile, 10% said they do not participate — a total of 42 respondents. There is formal participation in public engagement on either side of the divide, with further informal activity amongst a smaller group, and only a minority not left participating at all.

Level	Frequency	Percentage
don't know	18	4
not sure	57	13
somewhat familiar	195	45
familiar	145	33
very familiar	20	5

Table 2: How Familiar with AI

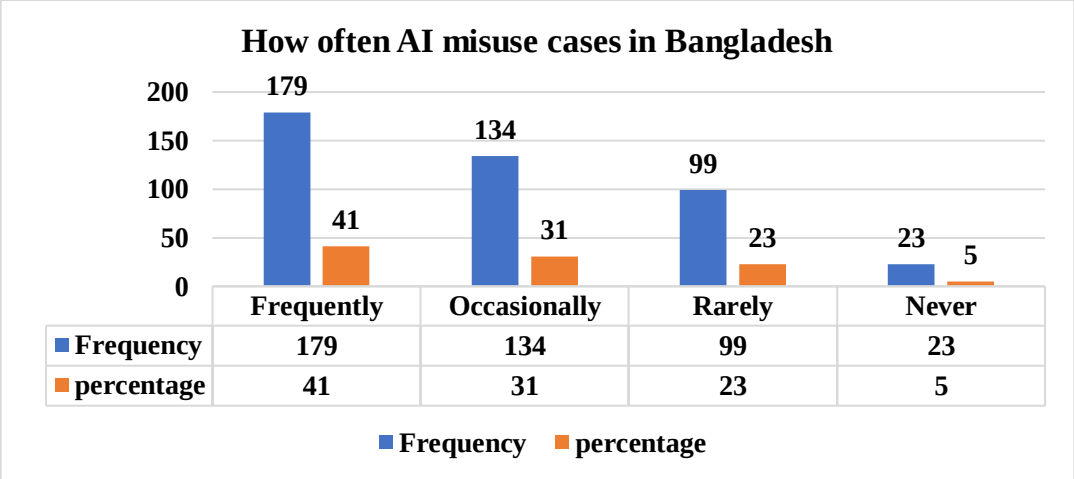
Table 2 Respondents' Familiarity with AI The majority of common respondents,195 (45%),said that they are somewhat familiar with AI compared to 145 (33%) who says they are familiar. A smaller percentage, 20 respondents (5%), said they are very familiar. 57 respondents (13%) said they were not sure, and 18 respondents (4%) said that they do not know about AI It appears that the majority of respondents have at least some levels of familiarity with AI, and few expressed a lack of knowledge.



	Yes	Not sure	No
percentage	61	30	9
Frequency	264	132	39

Chart 4: Can AI commit to crime?

The chart 4 shows how respondents think about whether AI is capable of a crime. Over half the respondents, 264 (61%), answered "Yes," signifying that they do believe AI can commit a crime. Also, 132 respondents (30%) chose not to answer this question. In contrast, 39 (9%) answered "No," which means that the majority of respondents believe in what we refer to as "AI crimes", despite a significant portion remaining doubtful and only a tiny fraction opposing this perspective.



	Frequently	Occasionally	Rarely	Never
Frequency	179	134	99	23
percentage	41	31	23	5

Chart 5: How often AI misuse cases in Bangladesh

The chart 5 shows respondent's perception about the frequency of AI misuse in Bangladesh. The biggest share of 179 respondents (41%) stated that misuse of AI occurs frequently. The next nearest option was 134 respondents (31%) that said they do this, but only sporadically. 99 (23%) respondents perceive misuse happens infrequently, and just 23 (5%) report that it doesn't happen. In terms of that finding overall, a large majority appear to believe AI abuse is, at the very minimum, an occasional occurrence with frequent occurrence being the most prevalent view.

Category of people	Frequency	percentage
Women and Children	139	32
Everyone equally	123	28
General interest users	117	27
Politician and celebrities	56	13

Table 3: Most vulnerable to AI-related crimes

The table 3 details respondents' views on who is most at-risk of being harmed by AI-generated crimes. The most common response, identified by 139 respondents (32%), was women and children as the demographic most vulnerable. The second most common response was 123 respondents (28%) saying that everybody is equally vulnerable. Seventeen respondents (27%) also pointed to regular internet users as most at risk. The least frequently cited category, with 56 respondents (13%) was politicians and celebrities. Overall, the results point to a view that women and children are particularly vulnerable, but a significant fraction of respondents agree with broad-based vulnerability.

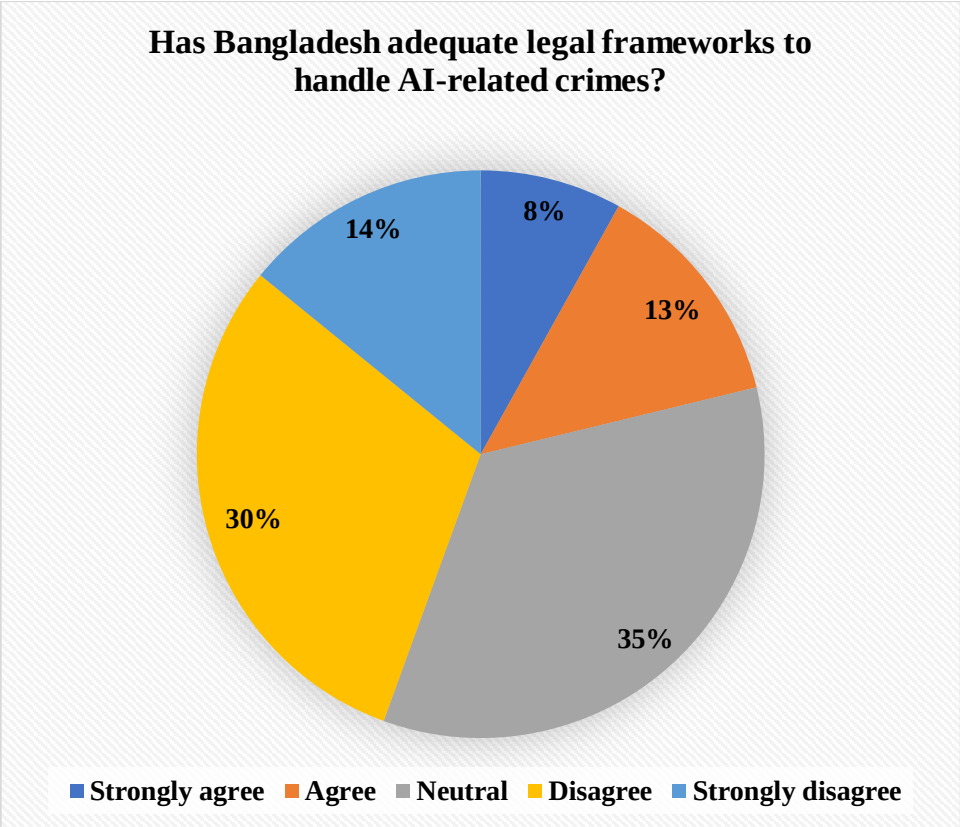


Chart 6: Has Bangladesh adequate legal frameworks to handle AI-related crimes?

The chart 6 shows whether respondents think Bangladesh has the adequate legal frameworks to combat crimes relating to AI. A plurality of respondents reporting 147 (34%) expressed a neutral stance. 132 (30%) disagreed and 63 (14%) strongly disagree, signifying that those who don't had a significant prevalence. Conversely, 57 (13%) agreed and 36 (8%) strongly agreed that existing legal frameworks are sufficient. Overall, the results indicate that neutrality is indeed the most common position but that a greater proportion (combined) of respondent's express dissatisfaction than satisfaction with the current legal framework.

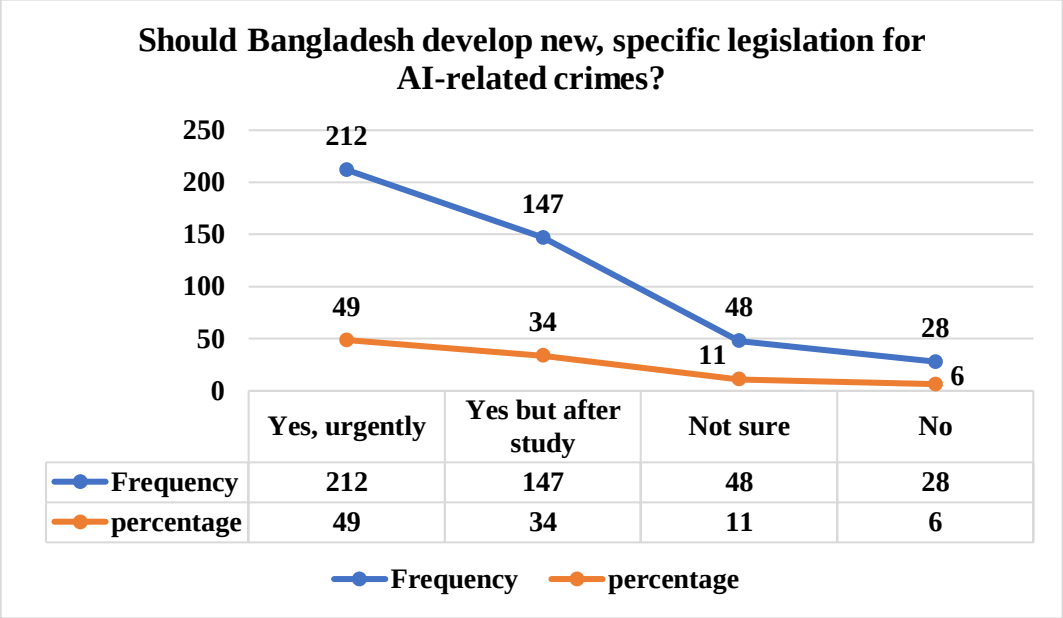
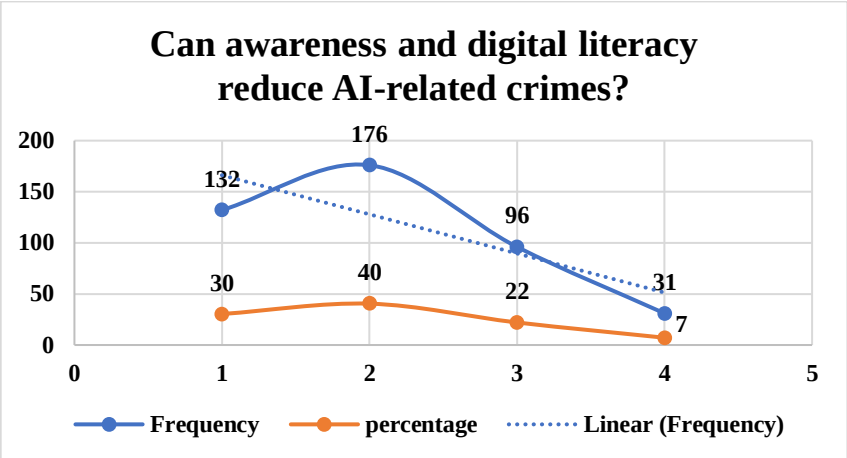


Chart 7: Should Bangladesh develop new legislation for AI-related crimes?

The chart 7 summarizes respondents' Views on if Bangladesh should draft fresh, specific legislation for AI crimes (N =435). Almost half the respondents (212, 49%) felt that new legislation needed to be developed urgently. A further 147 participants (34%) supported legislation but only following proper study. In contrast, 48 respondents (11%) did not know and 28 respondents (6%) disagreed with the creation of new legislation. Overall, results show considerable support for certain types of public policy changes; 87% call for immediate and/or studied legislation.



Can awareness and digital literacy reduce AI-related crimes?		
Level of opinion	Frequency	percentage
Strongly agree	132	30
Agree	176	40
Neutral	96	22
Disagree	31	7

Table 3 & Chart 8: Can awareness and digital literacy reduce AI-related crimes?

This chart and table show that the level of how can awareness and digital literacy reduce AI related crimes? The respondents are asked whether awareness of digital literacy can reduce crimes caused by AI, as shown in table. Notably, out of the respondents, 132 (30%) strongly agreed that awareness and digital literacy are effective preventative measures to potential threats while 176 (40%) only agreed with this statement suggesting good level of confidence in preventative power of these skills. In parallel, 96 (22%) respondents were neutral. A minority

(31 respondents, or 7 percent) disagreed and none disagreed strongly. The findings indicate that, overall, awareness and digital literacy are positively supported as preventive measures of crime related to AI.

Case Studies

Case Study 1

AI-Generated Deepfake Harassment of a University Student

In 2025, a 22-year-old university student from Chittagong, whom we'll call Israt (pseudonym), found herself targeted by an AI-generated deepfake harassment campaign.

Someone took publicly available photographs of Israt from her social media accounts and applied generative AI image-editing and face-swapping technologies to make fake images and videos of her in compromising positions. The modified photos were then posted in Facebook groups, messaging apps and private online forums related to her university. The material spread quickly, and the vast numbers of people who viewed it discounted its fanciful elements rather than the photographs.

The viral spread of these deepfakes had a huge impact on Israt's image and mental health. She said she faced social stigma, harassment online and had little motivation to go to university out of fear she would be outed again. Israt lodged a police complaint at her local station under the Information and Communication Technology Act 2006, which criminalizes some forms of online abuse as well as cyber harassment and defamation. But the detectives struggled to investigate the case. The government lacked the appropriate resources and expertise to demonstrate that the photographs were generated via AI, and there was nothing in the statute regarding deepfake technology or manipulations through AI that change someone's identity.

Moreover, much of the content had appeared on platforms not based in Bangladesh, complicating matters further as far as jurisdiction went. As a result, the investigation proceeded slowly, and the perpetrator remained at large for a long time. This case illustrates how AI-generated deepfake technology is becoming an increasing menace, while the laws in Bangladesh make little headway to counter new forms of digital victimhood.

Case Study 2

AI-Generated Deepfake Blackmail Against a University Teacher

In 2026, here in Bangladesh a university professor named "Dr. Mohsin" (pseudonym)- became the target of an A.I.-enabled blackmail campaign that used deep fake photos and videos. Dr. Mohsin had worked as a professor at a reputed university for several years and he was active on social media and professional networking sites. According to the information, people who have no direct acquaintance with him transformed his images available in public domain and used the AI-enabled image manipulation tools to fabricate images of him in indecent and shameful spots.

Shortly after the images were created, the criminals contacted Dr. Mohsin via anonymous WhatsApp accounts. They claimed to have lurid images and threatened to send them to his coworkers, the university administration and students if he didn't pay a lot of money. The attackers demanded payment in mobile money services and cryptocurrencies. They warned that if the victims didn't pay, the images would be circulated across the internet. The criminals had sent him many AI-generated photographs as proof and threatened to publish more material in order to apply even greater pressure.

Dr. Mohsin was a lot stressed out mentally as the fake photographs surfacing could have very well derailed his career and academic progress. He was worried that reporting the incident could damage his reputation, so he did not do it right away. At last, he went and filed a report to the Cyber Crime Unit of Bangladesh Police stating that he was being Blackmailed, Harassed Online and his Identity was Stolen.

But there were a series of flaws in the inquiry. It was hard to track down the people who did it because they used anonymous accounts, encrypted pathways of communication and possibly even servers outside the country.

Furthermore, although existing cybercrime laws apply to online harassment and extortion, there are no specific legal frameworks that address AI-generated deepfake extortion or identity manipulation. For the investigation it is even harder as there are not enough good digital forensic experts that can trace out AI generated media. This case shows how emerging technology in terms of AI could aid cyber extortion and emphasizes the need for Bangladesh to have clearer legislation as well as better methods of investigating AI crimes.

DISCUSSION AND FINDINGS

Inadequacy of Existing Law for AI-related Crimes

The research concludes that the existing legal framework in Bangladesh is not adequately prepared to deal with such complexities of AI-related crime.

Existing Legal Framework:

Cyber Security Act, 2023

The Cyber Security Act, 2023 is the key legislation on cybercrimes in Bangladesh.

Relevant Sections:

Section 17: Computer-related Offense: This one is after all computer related if there is using AI tools to access someone else's computer or system or data wrongfully.

Penalty: 5 (up-to) years of imprisonment or fine up-to 5 million (BDT) or with both.

Section 25: Crimes Related to Cyber Bullying and Revenge Pornography or Harassment Online: Covers the use of AI for the production of deepfake images, videos etc.

Penalty: Imprisonment for a term not exceeding two years or with a fine not exceeding 1,000,000 BDT or with both.

In case, the victim is a female or a minor, the punishment shall be increased to five years' imprisonment or a fine of a maximum of 2 million BDT.

Pornography Control Act 2012:

When it comes to using AI to create deepfake porn, nudes, or videos, this law applies.

Relevant Section:

Article 4: Pornography production, distribution or publication: Imprisonment for a term not exceeding ten years and/or a fine.

Information and Communication Technology Act 2006:

Relevant Section:

Section 57: Used to posting defamatory or false information over the net.

Previously, this section was widely used in all cybercrime cases until newer cyber laws were enacted.

Penal Code 1860:

In addition to the existing guidelines governing cyber offences, traditional criminal statutes can also be applied to cases involving an AI-based offence.

Relevant Sections:

Section 499 / 500: Defamation; Printing or publishing defamatory matter regarding a person.

Section 506: Anyone who intimidates another person – such as making a death threat – including in the digital space with the use of Artificial Intelligence

Section 420: Cheating and Fraud: The use of AI tools to cheat or commit fraud.

While existing laws such as those relating to cybercrime or the Penal Code can address certain digital offences, they are not well-suited for regulating harms caused by artificial intelligence technologies. Taken together, AI systems can produce synthetic content; mimic people and refer to digital identities in ways that upend traditional notions of intent, responsibility and authorship. As a result, legal authorities often struggle to establish liability, collect admissible evidence and groundlessly prosecute offenders.

Lack of Acknowledgement about AI in the Digital World

One contrasting implication of the study is that people abusing AI systems have not become a rarity in digital environments. Most respondents indicated that AI-related misuse occurs frequently or at least sometimes. This means that computer virus attacks powered by AI are not just theoretical concerns anymore but rather a growing threat for all people using the Internet. AI tools are becoming increasingly user-friendly, enabling anyone to modify images, create deepfakes and automate phishing attempts or other forms of spurious digital content. Such abuse amplifies the scale and speed of digital crimes, giving victims little time to respond or obtain legal remedies. The findings thus illustrate how the innovative thrust of AI technologies can also expose new vulnerabilities within digital ecosystems.

Vulnerability of Female and Child Sexual Exploitation

It also designates several groups as particularly vulnerable to AI crimes. Women and children were perceived to be the most vulnerable victim category, people who use internet in general which ultimately culminates into victims of cyber rape. This perspective is closely tied to the increasing availability of AI tools used to generate non-consensual sexually explicit images, deepfake harassment and online blackmail and identity-based impersonation. Such crimes are particularly egregious and devastating when manipulated content (i.e. pictures or videos) proliferates on social media platforms, resulting in severe psychological, social and reputational harm to the victim. The findings suggest that social vulnerabilities might aggravate challenges of digital safety, with crime or attacks by artificial intelligence likely to land first on these vulnerable individuals.

Role of Public Awareness and Digital Literacy

The results also reveal that respondents widely believe that digital awareness and literacy can help significantly reduce the risk of AI misuse. Most of the people they interviewed also believed that a more informed public surrounding AI technologies, online safety practices and preservation of digital evidence could help shield individuals from new types of cybercrime. Awareness-raising initiatives might also help victims report incidents with greater efficacy and to sue for recourse in court. This underlines that while legal measures are necessary, they can't be the only solution on the table- prevention in the shape of education, digital literacy programs and responsible technology also needs to be front and centre in terms of addressing AI-related harms.

Institutional and Enforcement Challenges

However, it also highlights other concerns related to institutional and enforcement deficiencies as not just legislative ones. Many offenders can play the role of a criminal anonymously or from behind barriers such as foreign jurisdiction, making it difficult for law enforcement to detect perpetrators. Potential actions would include investigations or prosecution of individual defendants where forensic skill and technological capacity are poor (including investigation of deepfakes, or alteration in digital evidence). Those very institutional shortcomings limit victims from pursuing justice and contribute to the growing sense that crimes facilitated by AI tech face minimal repercussions in our current legal system.

RECOMMENDATIONS

Development of AI-Specific Legal framework

In Bangladesh perspective, passing laws related to AI-based crime Amend current cyber-laws to prevent offences like impersonation of individuals using AI, deepfake blackmail, synthetic identity fraud and AI assisted black mailing. Ensuring clear legal definitions and corresponding penalties would provide a significant tool by which law enforcement agencies can them prosecute offenders and offer victims proper legal protections.

Enhancing Digital Investigation Capability

Law enforcement institutions require a more advanced technological infrastructure to monitor and apply AI-related regulations. Law enforcement agencies must invest in a robust suite of modern digital forensic capabilities using machine learning techniques that can identify when recordings have been tampered with and verify whether content is genuine and trace back the source of some autonomous AI-generated content. They should also have specialized training programs where investigators, prosecutors and judges are taught the technical aspects of evidence produced by AI systems so that those types of evidence can be properly assessed in hearings.

Establishment of Victim-Oriented Legal Aid Mechanisms

Given the psychological and reputational harms inflicted by AI crime, it is essential to develop victim-oriented legal assistance mechanisms. The mechanisms could include measures such as rapid reporting channels, removal procedures and legal assistance services for victims. If we are to create a legal system that people can trust, then establishing clear pathways for victims to seek justice is part of what it means to restore trust in our institutions and contain the long-term effects of AI-mediated victimization.

Public Awareness and Responsible usage of AI

Public information campaigns should alert citizens to the dangers of AI technologies, and how we can defend ourselves from digital manipulation and cybercrime. Help promote web safety and responsible use of AI-work together as universities, tech firms and public agencies. Such initiatives would help citizens recognize AI-generated disinformation, report suspicious activity and secure their personal information.

Strengthening International and Platform Cooperation

Not every AI-enabled crime will cross digital borders, and not all be through faceless online aggressors. Therefore, Bangladesh has to enhance its international cooperation mechanism and build linkages with global technology companies to mitigate these challenges.” By collaborating more closely with social media companies and law enforcement organizations across borders, they could streamline investigations, find bad actors out of their platforms more quickly to limit the spread of content and track perpetrators operating outside national frontiers.

CONCLUSION

As new technologies take over more of our lives, AI has grown into many new types of digital crime that can put our current legal systems to the test. This study looked at whether Bangladesh's current legal system is strong enough to stop and prosecute crimes involving AI, as well as whether there are enough protections for people who might be hurt by these crimes. As a result, while cybercrime is partially protected by law and other criminal laws do protect us in some ways, our legal system is still terribly unprepared to deal with crimes made possible by AI technologies, such as deepfake video content manipulation, AI-enabled impersonation fraud, and automated online harassment. More and more people are worried about AI technologies that could be abused or that could put women and children at risk. Some others are the ability to investigate, the knowledge of digital forensics, and meeting legal requirements that vary from country to country. The study says that Bangladesh needs a more complex paradigm along with better institutional capacity because of this.

REFERENCES

1. Ward, T., Saeri, A., & Noetel, M. (2024). Turn a Blind AI: The Impact of Compassion Fade and the Identifiable Victim Effect on AI Risk Concerns. SSRN. https://doi.org/10.2139/ssrn.4839839
2. Falade, P. V. (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. arXiv. https://doi.org/10.48550/arXiv.2310.05595
3. Minhas, R., Elphick, C., & Shaw, J. (2022). Protecting victim and witness statement: examining the effectiveness of a chatbot that uses artificial intelligence and a cognitive interview. *AI & Society, 37*(1), 265–281. https://link.springer.com/article/10.1007/s00146-021-01165-5
4. Sutarya, I. M., Prastiono, S., & Jamaludin, A. (2025). The Law's Protection Against Children as Victims of Exploitation Artificial Intelligence-Based Cyberpornography. Journal of Law, Politic and Humanities, 5(5), 3473–3487. https://dinastires.org/JLPH/article/view/1725
5. Mayeesha, T. T., Islam, F., & Ahmed, N. (2024, December). AI4Bangladesh: AI ethics for Bangladesh—Challenges, risks, principles, and suggestions. In Proceedings of the 13th International Conference on Information & Communication Technologies and Development (pp. 260–272). ACM. https://doi.org/10.1145/3700794.3700820
6. Kupriianova, L., & Kupriianova, D. (2023). The AI in the porn industry of social media: Human replacement or precursor for growing the sexual violence and human trafficking indicators? In Collection of Scientific Papers «SCIENTIA» (October 6, 2023; Valencia, Spain) (pp. 75–82). Retrieved from. https://previous.scientia.report/index.php/archive/article/view/1236
7. James, T. P. (2024). Not her fault: AI deepfakes, nonconsensual pornography, and federal law's current failure to protect victims. BYU Law Review, 50, 1159–. https://digitalcommons.law.byu.edu/lawreview/vol50/iss4/10/
8. Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. IEEE Access, 10, 77110–77122. https://ieeexplore.ieee.org/abstract/document/9831441
9. 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(1), 89–120. https://link.springer.com/article/10.1007/s11948-018-00081-0
10. Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime**.** Crime Science, 9**(**1), 14. https://link.springer.com/article/10.1186/s40163-020-00123-8
11. Liu, Y., Li, X., & Zheng, Z. (2024). Smart natural disaster relief: Assisting victims with artificial intelligence in lending. Information Systems Research, 35(2), 489–504. https://pubsonline.informs.org/doi/abs/10.1287/isre.2023.1230
12. Biana, H. T., & Domingo, R. (2024). Victim-blaming AIs. AI & Society, 39(3), 1443–1444. https://link.springer.com/article/10.1007/s00146-022-01567-z
13. Whittaker, M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., Myers West, S. M., Richardson, R., Schultz, J., & Schwartz, O. (2018). AI Now Report 2018. AI Now Institute, New York University. Retrieved from https://ainowinstitute.org/AI_Now_2018_Report.pdf
14. Schank, R. C. (1987). What is AI, anyway? AI Magazine, 8**(**4), 59–59. https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/623
15. Zhang, D., Mishra, S., Brynjolfsson, E., Etchemendy, J., Ganguli, D., Grosz, B., … & Perrault, R. (2021). The AI index 2021 annual report. arXiv. https://doi.org/10.48550/arXiv.2103.06312
16. Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. Science, 361**(**6404), 751–752. https://doi.org/10.1126/science.aat5991
17. Furman, J., & Seamans, R. (2019). AI and the economy**.** Innovation Policy and the Economy, 19**(**1), 161–191. https://doi.org/10.1086/699936
18. Reed, C. (2018). How should we regulate artificial intelligence? Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2128). https://royalsocietypublishing.org/rsta/article/376/2128/20170360/115636
19. Tao, L., Wan, J., & Wen, B. (2025). The effects of artificial intelligence and victims' deservingness information on citizens' blame attribution towards administrative errors. Public Management Review, 27**(**12), 3104–3124. https://doi.org/10.1080/14719037.2024.2411632

20. Maslej, N., Fattorini, L., Perrault, R., Gil, Y., Parli, V., Kariuki, N., … & Oak, S. (2025). Artificial intelligence index report 2025. arXiv. https://doi.org/10.48550/arXiv.2504.07139