LEGAL CHALLENGES IN REGULATING AI-POWERED HACKING, PHISHING, AND IDENTITY THEFT

Tushar Krishnamani[1]

[1]Assistant Professor for Law, NMIMS Kirit P. Mehta School of Law, Mumbai

Abstract

Artificial intelligence (AI) has evolved at an extremely fast pace, both improving the security defenses and allowing cybercrime to become more complex and sophisticated. Some of the most urgent ones are AI-based hacking, phishing, and identity theft, which use machine learning, natural language processing and deepfakes technologies to avoid being noticed and attacking individuals, corporations and governments. These AI-based threats are scale-based, precise and flexible unlike conventional cybercrimes and this compounds regulation responses.

This paper discusses the issues of legal regulation of AI-based cyber-crimes, their jurisdiction, attribution, evidentiary standards, corporate liability, and human rights. It is a critical examination of current legal provisions in India, the United States, the European Union and international provisions like the Budapest Convention. The work points out the failure of the outdated laws to anticipate the risks posed by AI, and it also points out technical constraints in the enforcement agencies to investigate and prosecute those crimes.

The paper proposes a special regulation of the AI-related types of cybercrime, the internationalization of the legislative framework, and strengthening regimes of data protection. It also highlights the necessity of adaptive legal frameworks, a combination of the public and the private spheres, and law enforcement capacity building. Uniting the comparative understandings and policy recommendations, the article aims to bring a balance between innovation and security, making sure that the resilience to upcoming AI-driven cyber threats is enabled.

2. Understanding AI-Powered Cybercrimes

The use of artificial intelligence (AI) has brought a level of efficiency and flexibility to digital systems never before seen, but has also been used by malicious threat actors to be increasingly weaponized. In contrast to traditional cyberattacks, AI-enabled crimes take advantage of automation, self-education, and predictive modelling to execute attacks that are quicker, scalable, and much harder to detect. The first and most urgent are AI-related hacking, phishing, and identity theft each of which uses different technological instruments, but is characterized by the same feature a high level of sophistication.[1]

2.1. AI in Hacking – Automated Penetration Testing vs Malicious Exploitation

Conventionally, the hacking process involved skilled persons who would probe networks and use the vulnerabilities. AI has changed this dynamic, as it has introduced automated penetration testing tools capable of mapping systems, finding vulnerabilities and making attempted exploits without a human operator constantly present. The tools are ethically used by cybersecurity professionals to enhance the defense mechanisms; but in wrong hands, the technology becomes catastrophic.

Hacking tools powered by AI can process vast amounts of software code and network traffic and identify the vulnerabilities faster than human hackers do. As an example, reinforcement learning enables an artificial intelligence system to learn, through trial and error, to become better at intrusion. In addition, adversarial AI is capable of circumventing intrusion detection systems by masquerading as normal traffic, which effectively masks malics.

An example of this is the creation of malware that develops AI features that change their behavior after they are installed. These programs do not adhere to a fixed pattern but track the reactions of the system and modify their approach of attack dynamically to prevent detection.

This flexibility poses a moving target to cybersecurity defenses, making rules-based protections not effective any longer.[2]

2.2. AI in Phishing – Deepfake Voice/Video and Generative AI in Spear-Phishing

Phishing has been one of the most prevalent cybercrimes and, however, AI has radically reshaped the dimensions and consequences of phishing. The use of bulk emails comprising of generic messages in phishing was traditional. Phishing attacks in the case of AI have become hyper-personal. Social media profiles, professional networks and compromised databases can be scraped with machine learning algorithms to create messages that seem to be authoritatively credible to a specific recipient.

The large language models (LLM) of generative AI can be used by attackers to generate grammatically flawless and contextually relevant phishing emails, which removes the characteristic flaws that reveal the scam. On top of text, AI also supports deepfake audio and video information- impersonation attack is frighteningly believable. In 2020, the case of an energy company in the UK demonstrated that an alleged scam resulted in the company losing $243,000 when fraudsters impersonated the speech patterns of the CEO by using AI-based voice generation to order an immediate transfer of funds. In the same manner, deepfakes of video technology can impersonate corporate leaders in online conferences, deceiving employees into giving confidential information or making financial deals.

Spear-phishing scams have gotten more specific as well. As opposed to mailing generic messages to tens of thousands, AI applications are used to profile people and send more personalized messages, and the chances of success grow exponentially.[3]

2.3. AI in Identity Theft – Synthetic Identities and AI-Generated Documents

The identity theft has evolved well beyond stolen credit card information. AI currently allows the creation of so-called synthetic identities, in which data pieces real and fake can be joined to form believable yet entirely fictional identities. Such identities can be subjected to verification and even be given credit cards before they are discovered.

Artificial intelligence tools may also produce incredibly realistic forged documents such as government identification, passports or utility bills which is further used to commit financial fraud, illegally migrate or launder money. Compared to the traditional forged documents that usually showed obvious errors, AI-generated forgeries are realistic to pass through an automated verification.

Besides, the contribution of AI to biometric spoofing has also been a matter of concern. Ai-generated facial recognition, fingerprint scanning, or voice authentication can fool systems, compromising the trust in technologies that are previously believed to provide a safer alternative to passwords.

Case Studies of Major Incidents

A number of events around the world explain why AI-based cybercrimes have disruptive potential. Other than the deepfake voice scam case by the energy company based in the UK, cybersecurity analysts have documented that AI-driven malware has been used in cyber attacks to attack U.S. healthcare institutions. India In India, warning notices have been issued by CERT-In on multiple occasions of AI-based phishing frauds that take advantage of people during state events like the COVID-19 pandemic or through welfare programmes. In 2023, fraudsters were reported to be using AI to synthesize voices of distressed family members in distress call to defraud the victims under the guise of an emergency.

[2] Amlan Mohanty &Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment for International Peace (Nov. 21, 2024)

[3] Amlan Mohanty &Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment for International Peace (Nov. 21, 2024)

These instances indicate how AI may turn into a highly targeted, convincing, and destructive attack on ordinary cybercrimes.

Distinction Between Traditional Cybercrimes and AI-Powered Cybercrimes

The main distinction between traditional and AI-powered cybercrimes is the amount, velocity, and sophistication. Classical phishing emails were dependent on numbers, hoping that a small percentage of the recipients will succumb. In its turn, AI-powered phishing puts an emphasis on quality, i.e., the personalization of attacks to the greatest strength of credibility. In the same way, unlike in the past where hacking was labor-intensive, AI automates and optimizes intrusions at a level that is not possible by human being.AI is a source of uncertainty as well. The classical malware obeyed preprogrammed orders; AI-centered malware can evolve with the situation, which makes defense and detection exponentially more difficult. Moreover, AI drops barriers to entry by cybercriminals- people with little technical skills can now use sophisticated tools that can be bought via dark web markets.

Finally, AI-based cybercrimes are a new frontier: it is not just a more advanced version of the same but a new category of cyber threats that needs a correspondingly new legal and regulatory solution.

3. Existing Legal Frameworks (National & International)

The development of AI-driven hacking, phishing, and identity theft has compelled every legal system across the globe to re-examine the framework of cybercrime. Although the majority of jurisdictions now have laws that deal with traditional digital crimes, not many of them are tailored to the sophistication of AI. In the next section, its analysis of the strategies of India, key international frameworks, and the effectiveness of the regimes in dealing with the unique nature of the problem of AI-enabled cybercrimes is discussed.[4]

3.1. India

Information Technology Act, 2000 (IT Act)

The IT Act, 2000 is still the main law providing protection of cybercrimes in India. It makes illegal the unauthorized access to computer systems (Section 66), identity theft (Section 66C), cheating by impersonation using computer resources (Section 66D) and publication of obscene or fraudulent material online (Section 67). Although such provisions give a ground to prosecute some of the AI-based crimes, the Act does not specifically target AI generated content, adaptive malware or the creation of synthetic identities.

It has a major weakness in that it uses human attribution. To cite an example, it will be cumbersome to establish that a particular person committed a particular offence dishonestly or fraudulently as per Section 66C when autonomous AI is involved. In addition, the punishment provided is usually small when measured with the monetary and image losses caused by AI enhanced cybercrime.

Indian Penal Code (IPC) Provisions

The IPC is a supplement to the IT Act since it deals with conventional offences, which have taken a digital form. Phishing and identity thefts can be treated as cheating (Section 415), forgery (Sections 463- 465), and criminal impersonation (Section 416). Nevertheless, these lines are technology-neutral and do not suit well with any crimes that are committed by generative AI or synthetic deepfakes. As an example, forging a physical document has long-standing jurisprudence, but forging an AI-generated digital identity produces apparent uncertainties of evidence.

CERT-In Guidelines

[4] Rahul Bharati & Dr. Rahul, Navigating the Legal Landscape of Artificial Intelligence: Emerging Challenges and Regulatory Framework in India, SSRN (July 14, 2024)

The Indian Computer Emergency Response Team (CERT-In) is the nodal agency of responding to cybersecurity threats. Within its 2022 guidelines, the companies are required to disclosed phishing, identity theft, and data breach cases within six hours. This is the reason why this rapid reporting requirement needs to be enhanced to make the detection and containment of AI-driven threats stronger. However, critics complain that enforcement capabilities are limited, and, out of the fear of being reputed as bad, private actors tend to under-report cases.

In addition, AI-enabled threats are not explicitly mentioned in CERT-In guidelines, which restricts their applicability when autonomous or self-learning systems are used to deploy cyberattacks.

Data Protection Act, 2023

A new law, the Digital Personal Data Protection Act, 2023, is one of the steps in the right direction to ensure that people are not victimized by identity theft and misuse of personal data. It imposes on data fiduciaries the duty of providing security protections and disclosure to the affected individuals and the regulator in case of breaches. In the case of crimes related to AI, such safeguards are essential since the majority of phishing and identity theft campaigns are based on extensive data abuse.

Nevertheless, the Act does not target the miscreants but instead puts the emphasis on data fiduciaries. It does not hold responsible the creators of AI models that can be misused to create deepfakes or commit fraudulent impersonation, and this leaves accountability as a void.[5]

3.2 International Regimes

Relative to that, the United States has devised a patchwork of federal and state-level tools. The best-known federal law is the Computer Fraud and Abuse Act (CFAA), which violates the unauthorized access, data theft, and fraud via computer systems. Although applicable in prosecuting hacking and identity theft, the CFAA has been criticized over the years with regards to its imprecise definitions that can be broadly applied especially when it comes to AI-generated attacks. The Federal Trade Commission (FTC) has added to this by taking enforcement action against companies that do not adequately safeguard consumers against identity theft, or otherwise practice deceptive AI. The consumer protection mandate of the FTC is very wide and thus FTC is one of the most adaptable regulators in matters related to AI misuse. At the state level, there are such laws as the California Consumer Privacy Act (CCPA) and state-specific legislation on malicious deepfakes, which evidences the increased understanding of the AI threats. Nevertheless, absence of a single federal law that specifically addresses AI-related cybercrimes imposes fragmentation and gaps in implementation.[6]

The European Union on the other hand has assumed a more holistic and rights based regulatory model. The General Data Protection Regulation (GDPR) of 2016 imposes strict requirements on the collection, processing, and safeguarding of personal data. In indirect ways, GDPR also tackles identity theft and phishing with the use of AI by strengthening the rights of data subjects and providing severe penalties. It is, however, mostly applicable to legal data processors and not to fraudsters using AI beyond the EU. Network and Information Security (NIS) Directive reinforces cybersecurity resilience in the critical sectors and requires reporting on the incidents, but similarly to GDPR, it is not related to AI-related threats. Better still, the Artificial Intelligence Act proposed by the EU is the first worldwide attempt of regulating AI systems. The AI Act establishes the foundation of responsibility in the

[5] Rahul Bharati & Dr. Rahul, Navigating the Legal Landscape of Artificial Intelligence: Emerging Challenges and Regulatory Framework in India, SSRN (July 14, 2024)

[6] Olivia J. Erdélyi & Judy Goldsmith, Regulating Artificial Intelligence: Proposal for a Global Solution, arXiv (May 22, 2020)

development and deployment of AI by categorizing its applications by risk and forbidding some of its more dangerous applications. Nevertheless, its preventive impact on criminal abuse could be minimal because it mainly concerns the regulation of legitimate actors of AI.

The most important treaty on the multilateral front is the Budapest Convention on Cybercrime by the Council of Europe. It was adopted in 2001 and requires signatories to criminalize the unauthorized access, computer frauds and offences involving identity as well as assist in international cooperation in investigations. Its generalized language enables it to be used in AI-based cybercrimes, however, it existed long before the emergence of generative AI and does not consider such nuances like deepfake impersonation or adaptive malware. In addition, India is also a non-signatory with an exception based on sovereignty and data-sharing provisions, undermined its role in coordinated world enforcement. In the meantime, such international organizations like the OECD and the United Nations have also started debating responsible AI governance. Guidelines provided by the OECD focus on transparency, accountability and security whereas the negotiation of a convention on cybercrime at the UN involves discussions on AI. Nonetheless, the two attempts are still at the stage of soft law and principles of guidance, but with low binding strength.[7]

Combined, these frameworks demonstrate the pros and cons of the existing legal responses to AI-driven cybercrimes. They show readiness to change the old laws of cybercrime to suit the new threat, yet they also reveal essential gaps. The first significant drawback is the technological lag since the majority of laws are older than AI technologies and do not address the new risks of AI-generated identities and deepfakes phishing. Legal issues still exist, as crimes that are perpetrated by AI usually do not respect borders, whereas law enforcement is usually local. Another unsolved problem is attribution since the current laws are based on human intent and they are unable to handle situations in which autonomous AI implements or maximizes attacks. Furthermore, regulatory frameworks are not harmonized: the EU is moving towards wholesome regulation of AI where the U.S. has adopted a decentralized approach and India is subjected to regulations passed pre-AI. Another obstacle is the capacity of enforcement because agencies such as CERT-In, FTC, or even EU regulators have limited resources to track changing threats of AI. Lastly, not many jurisdictions place responsibilities on AI authors or service creators to curb the misuse of their technologies, despite the indications of the prevalence of criminal uses of generative models already.[8]

Conclusively, although the IT Act in India, CFAA in the United States and GDPR in the European Union offer viable points of departure, none of them is comprehensive enough to respond to the issues of AI-powered hacking, phishing and identity theft. The current regimes will remain reactive than preventive without AI-oriented adaptations and more serious international cooperation that would enable cybercriminals to stay a step further than the law.

4. Key Legal Challenges in Regulating AI Cybercrimes

Cybercrimes regulation has never been a smooth process, as they are cross-border and technology changes very fast. Artificial intelligence has added fuel to cyberattacks, which has increased and intensified these challenges. AI helps to perform hacking, phishing, and identity theft in a more sophisticated, flexible, and large-scale manner than before. Although the legal systems are available to deal with digital crime more generally, they were not structured to consider autonomous or generative systems capable of not only concealing human efforts but also dynamically changing features in response to countermeasures. Consequently, a number of major difficulties emerge in policing AI-inspired cybercrimes,

[7] The EU AI Act in a Global Perspective, Marco Almada, SSRN (June 17, 2025)

[8] Artificial Intelligence Act, Regulation (EU) 2024/1689 (EU), O.J. L, July 12, 2024 (entered into force Aug. 1, 2024).

including jurisdictional, attribution, evidence, outdated, privacy-security tensions, corporate liability and more general ethical and human rights dilemmas.

Jurisdiction is one of the most urgent problems. Artificial intelligence-driven cybercrimes are innately cross-national in nature. The source of an AI-powered phishing attack can be a machine-learning model deployed on servers in a single country, run by people in a different country, and victims who may be distributed over different jurisdictions. Conventional concepts of jurisdiction in the criminal law are based on the regionality, nationality, or the location where the injury arises. In the case of AI, however, the place of the offence is spread out and disintegrated throughout cyberspace. This is enhanced by the anonymity that is offered by virtual private networks (VPNs), the dark web and, most recently, anonymizing AI tools. Even malicious traffic that is being traced by investigators is routed through hacked servers in jurisdictions that refuse to or cannot cooperate. As an example, a fraudulent transaction started by an AI bot in Europe might go through servers in Asia, and defraud a victim in North America, and the question arises to which country should be the primary jurisdiction. The existing international cooperation mechanisms e.g. mutual legal assistance treaties tend to be too slow and politically sensitive to combat these crimes. In the absence of harmonized international norms with a specific focus on AI-enabled offences, cybercriminals will still use the lack of jurisdiction.

The question of attribution is closely related to jurisdiction. It is hard to established responsibility even with traditional cases of cybercrime, but it becomes even worse with AI. Conventional legal principles presuppose the committal or the initiation of the crime by a human agent. In AI-driven hacking or phishing, however, a great deal of the malicious will be performed automatically. The intent can be difficult to attribute as an AI malware program can modify its strategy in real-time without any human instructions. Is the responsibility to solely the programmer that created the model, or the user who implemented the model, or the site on which the model was hosted? Moreover, in certain instances, generative AI systems can unexpectedly come up with damaging results that are not necessarily meant by those who made them or their users. As an example, a broad language model to create convincing messages might, when abused, produce a series of phishing emails that are fraudulent in content. There is a problem with proving mens rea, or the guilty mind, in such contexts. The difficulty in determining whether an autonomous action performed by an AI system could meet the legal criterion of intent or knowledge is ill-equipped to the courts, and there is no clarity, which poses serious challenges to prosecutors.

Evidentiary issues also make it more difficult to regulate AI-based cybercrimes. Data integrity, data admissibility and chain of custody have always been a major problem at digital forensics. The problems are multiplied with AI. The example of deepfakes, in particular, can produce video or audio records that are almost similar to the original one. This not only concerns the use of AI evidence to convict a crime but also the ability to fight with false accusations. When an accused asserts that incriminating digital evidence is AI-generated, the courts must use expert testimony and forensic tools that can be limited at recognizing a complex AI forgery themselves. Copyright laws in most jurisdictions were based on the tangible documents and material witnesses, and it is still in progress to adjust evidentiary rules to AI-generated material. In addition, AI-generated malware may alter or delete records of its actions and make it more difficult to collect credible forensic evidence. The validity of court cases may suffer when the courts fail to be assured of the ability to differentiate genuine and AI-generated evidences.[9]

[9] Amlan Mohanty &Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment for Int'l Peace (Nov. 21, 2024)

Another problem associated with it is that most of the current laws are outdated. The majority of cybercrime laws were made in the late 20 th or early 21 st century, when AI had basic or no capabilities. They penetrate criminality of unauthorized access, data theft and fraud but hardly consider adaptive or generative systems. Consequently, prosecutors are inclined to consider the broad or far-fetched interpretations of old clauses, which may create the effect of legal uncertainty and difficulties based on the factor of vagueness. India, as an example, in its Information Technology Act, 2000, or the United States in its Computer Fraud and Abuse Act, 1986, criminalize unauthorized access to computers, but neither of these laws specifically addresses the use of AI tools that automatically perform unauthorized access without the active oversight of a human operator. Equally, several jurisdictions have identity theft laws targeting stolen personal identifiers, but do not specifically address AI-generated synthetic identities consisting of pieces of real and fake data. Without revised legislation, there is the threat that large parts of AI-specific behaviour would fall outside the criminal legal system, and would thus embolden criminals.

Adding to such legal gaps are the strains between data privacy and security protection. On the one hand, robust data protection regulations like the GDPR in the EU or the Digital Personal Data Protection Act in India, 2023, are items that can curb a mass of personal data abuse that contributes to AI-powered phishing and identity theft. Conversely, police departments usually want broad surveillance abilities that will identify and provide countermeasures to AI-based attacks on the spot. It is a fine line between these interests. Excessive surveillance can be detrimental to the rights of individuals, and extreme privacy can impair the trust of the population, whereas stringent privacy controls can reduce access to the data needed to counter AI-driven attacks in a timely fashion. As an example, requiring service providers to disclose encrypted communications or training datasets to regulators could assist in tracking criminal misuse, but also increases the probability of abuse and mission creep. Lawmakers and judges thus have to face the challenging trade-off of balancing civil liberties and security against fast-changing AI menaces.[10]

Corporate liability is yet another problem not resolved. Providers of AI services, developers, and platforms are at the middle of making or deterring misuse of their technologies. The malicious actors can use generative AI systems with little knowledge of technical expertise, which posits the question of whether providers have some liability in misuse. Nowadays, in the majority of jurisdictions the liability falls on the end-user as opposed to the developer. However, critics believe that companies that use potent AI systems ought to at least apply protection, oversight and abuse reporting regulations. The AI Act by the European Union makes such a step but it is aimed at consumer protection and not direct criminal liability of the provider of the high-risk AI systems. The Federal Trade Commission in the United States has started researching businesses due to poor protection of AI use, which is an indication of a possible transition to regard corporations as responsible. In India, Data Protection Act exerts responsibility on data fiduciaries and does not establish AI-corporate responsibilities. In the absence of better guidelines on corporate liability, AI developers can put innovation and market competition over the issue of security, leaving end-users to exploitation.

Lastly, AI cybercrimes cannot be regulated without considering ethical and human rights aspects. The fight against AI-based hacking, phishing, and identity theft is often associated with increased surveillance, algorithm-based surveillance and predictive policing software. Although these measures can boost cybersecurity, they present serious overreach concerns. Overuse of automated surveillance may violate the freedom of expression and privacy rights as well as the principle of proportionality. In the case of big data spying of communications

[10] Amlan Mohanty &Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment for Int'l Peace (Nov. 21, 2024)

to identify deepfake phishing operations, surveillance may unintentionally record legitimate communication, spiking the Internet conversation. Moreover, AI in law enforcement can be used to reinforce biases, especially when AI systems are trained with bias or discriminatory data. Government use of defensive AI can also create accountability concerns- when a governments counter-AI system mistakenly labels innocent activity as malicious, it may result in people being unwarrantedly monitored or punished. Finding a balance, regulators should provide that AI-driven cybercrimes interventions are balanced with the constitutional protections and international human rights norms.

Altogether, the AI-driven hacking, phishing, and identity theft regulation are actively impeded by several intersecting problems. Jurisdiction, attribution, and evidentiary ambiguities, obsolete law, privacy-security conflicts, and corporate liability gaps and human rights issues all demonstrate the inefficiency of existing models. The above problems point to the fact that AI cybercrimes are not a continuation of existing forms of digital crime but a qualitatively new phenomenon that requires a reconsideration of legal principles. The problem of enforcing autonomy, adaptability, and generative nature of AI systems will be reactive and fragmented and will only be effectively enforced by legislation that is specific to such systems.[11]

5. Comparative Perspectives

The governance of AI-fueled cybercrimes is influenced by the technological evolution, but also by the wider legal, cultural, and political philosophies that inform governance in various jurisdictions. When comparing the European Union (EU), the United States (US) and India, it is clear that the three countries have vastly different strategies concerning the balancing of innovation, security and protection of rights. Whereas the EU has been rather rights-based and precautionary, the US is market-based and innovation-oriented, and India has been security-first historically, yet it is also experimenting with hybrid approaches. Considering these strategies, one can learn many important lessons regarding best practice, as well as the constraints of exporting foreign regulatory framework to India.[12]

EU is the most active of the jurisdictions in formulating comprehensive laws on AI to regulate its use and misuse. The General Data Protection Regulation (GDPR) established a global standard by integrating robust individual rights on personal information in such a way that AI-driven phishing and identity theft that depend on unlawful data gathering will be rectified by high compliance requirements. This is accompanied by the Network and Information Security (NIS) Directive that requires cybersecurity standards among critical infrastructure and digital service providers. The latest and most recent initiative is the proposed EU AI Act that suggests a risk-based approach to the regulation of AI systems, where minimal, high, and unacceptable risks can be distinguished. With the focus on AI-related cybercrimes, the aspects of transparency, accountability, and human control in the AI Act also seem especially applicable. An example is that high-risk AI systems when used in biometric identification or law enforcement have strict requirements, which indirectly discourage the production of tools to facilitate identity theft or surveillance misuse. The philosophy of the EU is based on human rights and precaution, and it aims at regulating AI before as many people are harmed as possible. This rights-based model is however, usually

[11] Amlan Mohanty &Shatakratu Sahu, India's Advance on AI Regulation, Carnegie Endowment for Int'l Peace (Nov. 21, 2024).

[12] Marco Almada, The EU AI Act in a Global Perspective (June 17, 2025) (SSRN working paper, available at SSRN).

accused of placing excessive compliance load which might suppress the emergence of small startups and innovation in tools against cybersecurity.[13]

The United States is, by contrast, more fragmented and sector-specific. At the federal level, the computer fraud and abuse act (CFAA) is the most important law that covers hacking, but it was passed in 1986 and cannot easily suit AI-powered attacks that act autonomously across boundaries. The Federal Trade Commission (FTC) has been on the go in applying its consumer protection mandate in penalizing companies that do not safeguard users against AI-assisted phishing and data breaches but this is more of a reactive than anticipatory measure. A number of states, including California with its Consumer Privacy Act (CCPA), have taken stricter measures in terms of data protection, however, there is no overarching federal privacy law on a comparable scale as the GDPR. On the governance level, the US has introduced such initiatives as AI Bill of Rights Blueprint and the National Institute of Standards and Technology (NIST) AI Risk Management Framework, which emphasize on ethical application of AI, equity, and responsibility. They are mostly voluntary and can be said to be built on the market driven philosophy of the US whereby its main focus is to create innovation and competitiveness in AI development. This has not only resulted in the US becoming a center of AI research and application, but has also created regulatory loopholes especially in dealing with malicious applications of AI to commit phishing and identity theft. There is still no uniformity in enforcing this and due to a lack of harmonized national laws, coordinating against cross-border AI cybercrimes is complicated.[14]

In India, there is the other type of regulatory philosophy which is less about rights or markets, more to do with national security and state control. The Indian Penal Code and CERT-In guidelines are backed by the Information Technology Act, 2000 that offers the foundation of the Indian law on cybercrime. These laws, though, did not consider AI and thus, only indirectly deal with AI-powered crimes. More recently, the Digital Personal Data Protection Act, 2023 has brought key requirements on data processing, but remains immature in addressing AI-generated synthetic identities or phishing made possible by deepfakes. The regulatory strategy of India is often focused on the state enforcement power instead of legal rights of individuals, as observed in the provision of regulations that enable CERT-In to impose data storage on entities or give orders to service providers. Although such a security-first approach offers agility in addressing the demands of the threats, it also brings up the concern of possible excesses in surveillance and lack of checks to governmental power. India has not created an inclusive AI law, similar to EU AI Act or even voluntary standards, such as those in US, which leaves a big gap in its ability to efficiently control AI-driven cybercrimes.[15]

The rights-based framework by the EU helps identify the importance of incorporating accountability and risk classification into the regulation of AI in comparison with the best practices. Mandatory transparency and documentation to ensure that it is easier to assign responsibility to AI-powered phishing or identity theft cases. It is also evident that the US model demonstrates the benefits of a more flexible, innovation-focused system, in the framework of which voluntary standards such as the NIST AI Risk Management Framework can adapt fast to reflect the technological shifts. India, however, exemplifies how a centralized enforcement model proves useful in those areas where the cyber threat is also

[13] Marco Almada, The EU AI Act in a Global Perspective (June 17, 2025) (SSRN working paper, available at SSRN).

[14] EU pushes ahead with AI code of practice, Financial Times (July 2025).

[15] EU pushes ahead with AI code of practice, Financial Times (July 2025).

related to national security, yet also demonstrates the dangers of underdeveloped rights protection and overdependence on the obsolete legislation.[16]

But it is neither possible nor desirable to directly transplant foreign models into India. Examples include the EU model which can prove to be too resource-heavy to Indian startups and businesses which are already high compliance cost. The US pattern of fragmented, voluntary regulation would tend to deteriorate the enforcement problem, since India already has a strained institutional capacity that has been overstretched. Rather, a mix of strategies borrowed by the respective jurisdictions can be used to good effect in India: with the risk-based system of AI classification developed in the EU, the US with its innovation-focused approaches to creating safe AI tools, and India with its robust enforcement systems to address threats to national security. More importantly, India also needs to create its own standards that meet the socio-economic realities of the country, such as capacity building to combat law enforcement, public-privacy alliances, and digital literacy campaigns to ensure that vulnerable populations will not become targets of AI-driven perils.

To sum up, the comparative analysis highlights that there is no ideal framework to govern AI-driven cybercrimes within a particular jurisdiction. The EU offers rigor and right protection, the US offers flexibility that encourages innovation, and India focuses on the interests of security with enforcement. The best way forward in the case of India is to leverage the positive aspects of these strategies and to overcome its own challenges of scale, capacity and digital vulnerability. In this way, India can create a strong but flexible regulation framework to guarantee the security and credibility in the era of AI-based cyber threats.[17]

6. Policy Gaps and Reform Proposals

Although there is an increasing awareness of AI-driven cybercrimes, the majority of legal frameworks still use the old fashioned cybercrime and data security statutes that were never constructed to deal with autonomous, adaptive, and scaled AI threats. Such a loophole requires AI-specific laws to outline clearly the extent of AI-enabled hacking, phishing, and identity theft, and the liability structures of those who commit them, party facilitators, and AI service providers. This specific legislation must bring in the civil and criminal aspects, which must deter by ensuring penalties and at the same time offer the victims avenues of compensation.

As AI cybercrimes are cross-border in nature, harmonization of laws on the international level is urgent. Similarly, to global cooperation in cybercrime enforcement, a new treaty or an addition to an earlier agreement would offer a framework on jurisdiction, attribution, and information exchange on AI-driven threats. In parallel to this, domestic reforms have to enhance data protection systems, and it should be required that organizations disclose AI-related breaches in a timely and open way.

The other important reform is liability frameworks. Scholarly guidelines of when AI creators, businesses or web site administrators can be responsible in cases of abuse would stop regulatory arbitrage and motivate accountable design. Governments might implement regulatory sandboxes to strike a balance between innovation and regulation, that is, under controlled legal circumstances, AI technologies may be tried before they are implemented.

Last, sustainable enforcement needs good partnerships between the public and the private. Cybersecurity companies, technology firms and governments should join together and develop threat intelligence networks. Similarly, law enforcement and the court system must be invested in through training and capacity building to be competent in investigating,

[16] Olivia J. Erdélyi & Judy Goldsmith, Regulating Artificial Intelligence: Proposal for a Global Solution, arXiv (May 22, 2020)

[17] Olivia J. Erdélyi & Judy Goldsmith, Regulating Artificial Intelligence: Proposal for a Global Solution, arXiv (May 22, 2020)

prosecuting and adjudicating AI-driven crimes due to technical skill. Taken together, these reforms would establish a dynamic and proactive regulatory space that could prevent AI-enabled cyber threats to society without suppressing innovation.

7. Future Outlook: Technology and Regulation

Generative AI is likely to become the most significant factor in the future of cybersecurity because it will allow cybercriminals to automatedly attack with precision like never before. AI is already being used to create and improve phishing, deepfake impersonations, and malware creation through the capability of AI to simulate human behavior and create credible digital artifacts. With the development of these capabilities, attacks will become larger in scale, adaptive and difficult to detect posing systemic risks throughout financial systems, critical infrastructure, and democratic processes.

Nevertheless, AI is also turning out as a potent defense mechanism. Machine learning models can identify abnormalities as they happen, learn suspicious network behaviors and forecast vulnerabilities prior to attack. Such an AI vs. AI dynamic, with defensive algorithms evolving to meet counter malicious ones, will characterize the coming age of cybersecurity. The successful implementation of AI-based defenses, in turn, presupposes powerful data-sharing systems and collaboration among states, industries, and international organizations.

On the regulatory front, the existence of formal legal frameworks will soon be challenged by the fast-moving AI technologies. Rather, there is a need to have change based and principles based regulations that enable lawmakers to react to new threats without inhibiting innovation. The integration of moral protections, or transparency, responsibility, and human control, will make certain that the security provisions do not undermine the basic rights.

International collaboration will be the ultimate factor of success. Cybercrimes that artificial intelligence is driving do not recognize international bounds and disjointed national strategies will only increase the vulnerabilities. An integrated global system the combination of legal, technical, and ethical guidelines proves to be the most promising step in order to deploy the potential of AI and address its dangers.

8. Conclusion

The analysis makes it clear that artificial intelligence has far surpassed the ability of the current legal systems to cope with the issues of AI-related cybercrimes. Although India has made significant steps with the help of the Information Technology Act, 2000, the Indian Penal Code, CERT-In guidelines, and, most recently, the Digital Personal Data Protection Act, 2023, such tools are still primarily reactive and fragmented against the constantly changing threats. Even in developed jurisdictions like the GDPR of the EU, NIS Directive, or the developing AI Act, and the sectoral regulations and enforcement efforts of the United States, are limited, in the face of cross-border crime driven by generative AI. Global conventions such as the Budapest Convention offer the background but are not enough to address the complexity of autonomous, adaptive cyberattacks.

One of the main themes that arise in this analysis is that the traditional statutes, which are designed to deal with human-focused offenses, cannot be effective in dealing with the problem of jurisdiction, attribution, and reliability of evidence in cases where the AI has free will. These issues are complicated by the fact that the responsibility especially the corporate and platform liability is not clear. More to the point, there is a growing concern about the need to balance cybersecurity imperatives and privacy and human rights safeguards.

Immediate reform is thus in order. India, as is the case in other jurisdictions, needs to embrace AI-related cybercrime schemes, which are aided by liability framework, regulatory sandboxes, as well as, increased capacity building among enforcement bodies. It is also vital that international standards be harmonized with cooperative agreements and public/private collaborations so as to have coordinated actions against cross-border offenses.

Moving ahead, the future course is to find a delicate balance between allowing AI to be innovative and at the same time building in security, accountability, and rights respect. Principle-based regulation, which uses adaptive regulation, and cooperation on a global level can change AI into a threat vector to a cornerstone of enhanced cybersecurity. Such a development of law and technology cannot but go hand in hand to guarantee the digital age.