INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 4 AND ISSUE 4 OF 2024

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Free and Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 4 and Issue 4 of 2024 (Access Full Issue on - https://ijlr.iledu.in/volume-4-and-issue-4-of-2024/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

AI IN COMBATING PHISHING AND SOCIAL ENGINEERING: A LEGAL PERSPECTIVE

AUTHOR – PREETI & DR. MOHIT KANWAR, LL.M. (MASTER OF LAWS)* & ASSISTANT PROFESSOR**, UNIVERSITY INSTITUTE of Legal Studies, Chandigarh University, Mohali, Punjab, India.

BEST CITATION - PREETI & DR. MOHIT KANWAR, AI IN COMBATING PHISHING AND SOCIAL ENGINEERING: A LEGAL PERSPECTIVE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 4 (4) OF 2024, PG. 455-465, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Cyber threats like phishing and social engineering are very popular in India, where weak technical vulnerabilities are taking advantage of psychological vulnerabilities and thus causing financial and privacy losses. Conventional legal measures under the Information Technology Act, of 2000, struggle to catch up with the intelligent nature of these attacks, and AI has become a tool of paramount importance in cybersecurity. Machine learning, natural language processing, behavioural analytics, and other AI technologies can recognize phishing and manipulation in real-time—powerful solutions. But building AI systems to achieve these goals requires complicated legal and ethical questions, particularly around data privacy, accountability, and visiting regulatory compliance. Some of these concerns are addressed in India's "Digital Personal Data Protection Act, 2023" (DPDPA), but they also need some AI-specific guidance. In this paper, I investigate how AI and the law intertwine in Indian cybersecurity, evident in the present legal terrain and global norms, and suggest reforms. We provide key suggestions for how a liability framework for using AI against cyberterrorism, transparent sharing of data within organizations, and formation of public-private partnerships for proactive, balanced AI in cybersecurity could be achieved. By taking these steps, India can harness the power of AI to fight cybercrime without compromising ethics and the law.

Keywords - Phishing, Social Engineering, Artificial Intelligence, Cybersecurity, Data Privacy, Information Technology Act, Digital Personal Data Protection Act, Machine Learning

INTRODUCTION

In the digital age of rapid rise in usage of the internet and digital transactions in India, phishing and social engineering attacks have grown to be prominent threats. Fellows alerted the world to the risks that phishing, an attempt by someone who is not who they claim to be to extract sensitive information, and social engineering, where a user is manipulated to give away private information, placed millions of digital users at risk. In a developing society, technologically, these forms of cybercrime have been harsh to financial security, privacy, and data protection in different fields. The rapidly evolving cyber threats in India faced the challenges of a legal and regulatory framework to cope with those that traditionally dealt with conventional forms of crime. The 'Information Technology Act, 2000' (hereafter, IT Act) does have legal provisions against illegal access and data breaches; however, it still falls short in curbing illegal cyber acts targeting users, which herein necessitates rapid development of robust and adaptive technological solutions such as that of artificial intelligence to effectively combat such threats, as explained in the subsequent sections.

Phishing and social engineering attacks mostly fall out of the equation of human psychology rather than technical vulnerabilities, which means they are hard to control and manage with the usual security measures.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Cybercriminals frequently trick people into giving them their sensitive information via emails, using fake websites, or social media interactions. Criminalizing phishing and related crimes have been made possible on a legal basis under the IT Act, more specifically under "section 66D" of that Act, which criminalizes cheating by personation by using computer resources. Still, the attacks are sufficiently dynamic for an equally adaptive solution to be required. [722]

By integrating artificial intelligence (AI) into cybersecurity, we have seen a paradigm change in the current fights against phishing and social engineering. AI (using algorithms such as machine learning, natural language processing, and behavioural analysis) can distinguish and pre-empt a phishing attack with more precision and velocity than old processes. Using machine learning, the models can learn and adjust to the changing patterns of an attack, and thus they can detect the phishing website, email, or message in advance before it reaches the user. Natural language processing identifies suspicious language and phrasing patterns used in phishing attempts. Yet, as of now, Indian legal frameworks do not provide specified regulations concerning the use of AI in defeating social engineering attacks in cybersecurity. This absence demands that existing cybersecurity legislation be modified to specify the legal obligations of AI systems and system operators and requires new legislation to enable the deployment of AI in cybersecurity with a clear structure.

The objective of this paper is to examine the legal implications and challenges involved with the use of AI to fight phishing and social engineering, in particular within the context of India. The paper will scrutinize current legal frameworks, case law, and statutory provisions and examine if AI deployment is an effective and risk-free approach to countering these forms of cybercrime. The discussion includes a discussion of the legal responsibilities and liabilities of AI system operators, the privacy concerns of AI from its capability to process data, and the need for legislative reforms. In addition, the paper evaluates international legal approaches, such as those in the European Union and the United States, which might provide valuable lessons for India's regulatory regime.

UNDERSTANDING PHISHING AND SOCIAL ENGINEERING

Phishing and social engineering have become mature forms of cybercrime, exploiting masses of vulnerabilities in the structures of human psychology to harm both individuals and organizations. These cyber-attacks, starting as mere general email scams, have evolved into more advanced trickery aimed at users sharing important information. Phishing is usually a deceptive communication (such as an email) to fool victims into releasing personal information, such as passwords, credit card numbers, or identifiers. In contrast, social engineering revolves around the exploitation of human trust and emotion without even trying to break into the technical defense. As Indian law struggles to define liability and to determine preventive measures, these crimes have taken on a legal significance. [723]

Phishing and social engineering are now classed under broader cybercrime legislation; the law has responded. The Information Technology Act (IT Act) of 2000 in India is central. There are specific provisions, such as 'Section 66D', of the IT Act that penalize cheating by personation impersonating using a computing resource, such as deception techniques used in phishing and social engineering. We also see "Section 43" dealing with unauthorized access and damage to computer systems and "Section 66C", addressing identity theft, which is often a result of phishing schemes. This brings us to *National Association of Software and Service Companies*

[722] Dipesh Juneja, *Artificial Intelligence, Law and Evidence with Cyber Crimes* 125 (Kamal Law House, Kolkata, 1st edn., 2024).

[723] M. H. Zaidi, *Artificial Intelligence: AI Law and Evidence with Cyber Crimes* 210 (Aliya Law Agency, Delhi, 1st edn., 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

v. Ajay Sood[724], a court of law ruled that as a legally actionable offense, phishing is treated under misrepresentation and fraud under Indian law. The decision emphasized the necessity of legal instruments preventing consumers and organizations from being exposed to such emerging threats.

Types and Techniques of Phishing

Phishing has taken more than one form and instead become many forms, each with its methods to fool and trick users. There are some common types, for example, email phishing, spear phishing, and whaling. Classic email phishing happens through mass emails masquerading as communications from respected organizations. It is intended to trick the recipients into clicking on the malicious links or downloading the infected attachments that give the cybercriminals access to important data. More targeted is spear phishing—narrowing the messages based on the information of the recipient and creating it through various personal information about the recipient, such as social media info or whatever they have posted online. Spearphishing attacks can bypass general security awareness and trick even careful users by impersonating trusted individuals, such as a company colleague or executive. Phishing of this sort can also be dangerous for organizations, where it can lead to sensitive data being leaked. [725]

Finally, whaling is yet another sophisticated technique that is targeted at high-level executives or individuals being able to access highly sensitive data organizations have access to. Attackers impersonating senior executives or high-ranking officials feed off corporate structures where orders seldom have to be questioned and often have access to proprietary information or financial resources. These variants of phishing prove how sophisticated cybercriminals are getting and how difficult it is to put legal liability. Offenses such as these can be treated under the IT Act provisions like "Section 66C", which deals with identity theft, or Section 66D, dealing with impersonation. Yet, because phishing tactics become more complex, the legal system has to keep up, facing new types of risks that emerge from carefully targeted phishing schemes.

Social Engineering Tactics in Cybercrime

Social engineering is a general term for any tactics based on psychological manipulation. Attackers take advantage of our trust in things, fear, urgency, and even our empathy to trick us into disclosing confidential information. Pretexting, baiting, and quid pro quo are common social engineering tactics. The term pretexting refers to having created an entire scenario pretending to be someone else to obtain information. For example, attackers can represent themselves as customer service representatives who need to verify your information and earn your trust by showing a valid pretext. The victim is tricked into downloading the malware hidden in gifts (such as free software presented in gift cards). Quid pro quo schemes play on the same weakness, this time in the opposite direction: attackers promise services or help in return for information.

In this regard, the incident 'Cognizant Technology Solutions Phishing Attack [2020] shows how attackers infiltrate corporate networks while taking advantage of employee behavior; it is noteworthy that the same tactics that are used to target individuals are also being used to compromise corporate networks. Social engineering is not specifically laid down in the IT Act, but provisions such as 'Section 66D' dealing with personation give a scaffold to do away with these tactics. Besides, the BNSS (formerly "Code of Criminal Procedure") and Bharatiya Sakshya Adhiniyam describe the investigative process to deal with these types of cybercrimes, therefore indicating that more elaborate definitions and domains by India's cyber law are necessary to address social

[724] [2005] DLT 363 DLT 363.
[725] Talat Fatima, *Cyber Crimes* 200 (Eastern Book Company, New Delhi, 3rd edn., 2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

engineering in generalized ways. [726]

Impact on Data Privacy and Security

Phishing and social engineering threaten data privacy and security, and access to unauthorized data, identity theft, and financial loss are typical consequences. These attacks degrade the integrity of personal and commercial information, resulting in major legal and financial consequences. It is an offense under 'Section 72' of the IT Act to disclose such information without the permission of the concerned person — or authority but there is a problem with its enforcement. While they violate privacy rights, phishing, and social engineering breaches also significantly burden regulatory frameworks and make the evolving legal response necessary to secure data integrity in India.

AI TECHNOLOGIES IN COMBATTING PHISHING AND SOCIAL ENGINEERING

One of the biggest allies against phishing and social engineering attacks is artificial intelligence (AI), which empowers security systems to detect and act upon threats at much higher speeds and much higher accuracy than traditional methods. When it comes to phishing, AI is capable of sifting through massive databases to search for patterns and instances of irregular behavior, and signs of a scamming pattern, and can be an incredibly useful weapon in the prevention of cyber-attacks. Psychological manipulation is just another challenge, and AI attempts to help us out with it. Because AI allows you to constantly analyze and learn from user behaviours and communication patterns, it can help warn security teams of signs that someone is potentially being manipulated ahead of a breach happening. Regardless, the 'Information Technology Act, of 2000' in India covers phishing cybercrime types like phishing under sections like 'Section 66D' (personation of to cheat), and other social engineering attacks are evolving and growing in sophistication; one has to fall back on technology intervention up and onwards. Seemingly, AI, essentially through machine learning (ML), natural language processing (NLP), behavioural analytics, and predictive analytics, has given organizations new perspectives and means to tackle cybersecurity, laying the groundwork that will solidify the new or more robust legal frameworks in place. [727]

Machine Learning and Pattern Recognition

Phishing detection is a subset of AI called machine learning, as it uses algorithms to spot patterns of suspicious activities across multiple channels. In this, AI can also analyze email metadata like URLs, IP addresses, and sender behavior and morph these algorithms to recognize any subtle indicator of spam activity. For example, phishing attacks can be identified when ML models trained on past phishing attacks recognize common traits in phishing attacks—odd syntax, unusual sender addresses, embedded malicious links—before they are exposed to the recipient. The training of models using massive data sets means that AI systems can become better and better, adapting in the face of new phishing techniques as they emerge. ML is invaluable in spear phishing and whaling attacks on high-profile individuals since it is these types of attacks that are manually created to get around existing security defense.

From the legal perspective, using ML to detect phishing buys privacy and data protection since ML requires masses of data for effective pattern recognition. The legal basis for incorporating AI into the protection of user data is the mandate on corporate entities to maintain reasonable security practices concerning sensitive personal data as specified in "Section 43A" of the "Information Technology Act, 2000." Nonetheless, data privacy is a major obstacle in ensuring that there are adequate datasets on which AI can rest, thus curtailing its

[726] Avtar Singh, *Principles of The Law of Evidence* 125 (Central Law Publication, 24th edn., 2023).

[727] Ratanlal and Dhirajlal, *The Law of Evidence* 175 (Lexis Nexis, 27th edn., 2019).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

creation, respectively. In *"K.S. Puttaswamy v. Union of India"*[728], the Supreme Court declared that privacy is a fundamental right, making things even messier when it comes to how ML initiatives work within the bounds of India's legal framework.

Natural Language Processing (NLP) in Phishing Detection

Another AI-driven technology useful in counter phishing and social engineering is natural language processing (NLP). NLP algorithms can analyze the text of an email, a message, or other means of communication for which the patterns of language used are characteristic of phishing attempts. NLP can flag communications as looking deceptive or coercive by analysing sentence construction, word choice, and semantic meaning. It's particularly useful for detecting spear phishing attacks in which attackers craft convincing messages. NLP can catch differences—formal language in an informal setting or a request for an urgent balance transfer of money with sensitive information. Organizations can use NLP to feed cybersecurity systems so that organizations can filter out potentially harmful communications before they reach users.

Legally speaking, the inclusion of NLP in detecting phishing attacks is supported by "Section 66C" of the IT Act, which criminalizes identity theft, a frequent result of well-executed phishing attacks. As an enabler of proactive NLP to identify (and alert on) potentially malicious content, this aligns with the legal requirement to protect user identities. As advanced as phishing techniques become, legal reforms may need to explicitly embrace and reflect the role language-based (namely, AI-powered) algorithms play in cybersecurity, including whether and how tools such as NLP need to be held accountable. [729]

Behavioural Analytics for Identifying Phishing Attempts

Behavioural analytics is used by AI to recognize and respond to phishing and social engineering attacks. With AI, you can monitor and understand user behavior, on the lookout for anomalies that may hint at a phishing attempt. Through behavioural analytic security systems, they can identify deviations in how users behave, like unusual login locations, abnormal file access patterns, over-the-top requests for sensitive information, etc. In the case of such deviations, AI will call for extra verification steps, security personnel will be alerted, or access will be temporarily suspended. This technique offers dynamic, real-time protection against phishing and only in corporate environments where users unknowingly compromise sensitive data. The effectiveness of behavioural analytics has been proven most effective in detecting social engineering when attackers exploit users through means other than established security protocols.

Behavior analytics in cybersecurity is however legally operational under Section 43 of the IT Act, which deals with unauthorized access to data and data protection. However, the use of the network brings in issues around privacy. Organizations, having to monitor user behavior to ensure compliance with privacy-related regulations, especially with 'Section 72A' about wrongful disclosure of personal information, will have to come up with much more efficient ways of reducing the occurrence of such breaches while ensuring minimal intrusion into the user's world. Therefore, behavioural analytics exemplifies the delicate weighing of user protection versus privacy, an important revelation for those formulating rules for policymakers tasked with determining the part that AI should play in cybersecurity. [730]

[728] [2017] 10 SCC 1.

[729] Irshaad Jada and Thembekile O. Mayayise, "The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome of a Systematic Literature Review," 8 *Data and Information Management* 163 (2024).

[730] Aaron Jarrett and Kim-Kwang Raymond Choo, "The Impact of Automation and Artificial Intelligence on Digital Forensics," 3 *Wiley Interdisciplinary Reviews: Forensic Science* 1418 (2021).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Role of Predictive Analytics and Automation

AI-driven cybersecurity frameworks have made predictive analytics and automation essential components for organizations to get ahead of phishing attacks before they occur. These predictive models observe historical data and anticipate if phishing attacks are likely (by identifying patterns that would demonstrate a very high probability of malicious activity). Thanks to this capability, organizations can automatically respond to these detections by blocking suspicious emails, restricting access to sensitive files, or notifying users about potential threats. In addition to improving response times, automation lightens the load for human operators and supports a fast and uniform defense against phishing.

In the context of India, predictive analytics in the prevention of phishing faces legal implications in terms of compliance with data protection laws specifically relating to the acceptance and use of data. Access to personal and behavioural data is often needed for predictive analytics, and it is a good question whether they are legal under India's Digital Personal Data Protection Act, 2023 (DPDPA). How organizations carry out predictive analytics is immediately affected by sections on purpose limitation and data minimization. In addition to the consent provisions, the Act also emphasizes transparency: Cybersecurity organizations must tell their users what types of data are used to drive AI. With predictive analytics becoming central to fighting the maturing menace of phishing, India's legal infrastructure must keep pace to address these privacy and transparency issues.

LEGAL CHALLENGES IN AI-DRIVEN ANTI-PHISHING SOLUTIONS

With the rise of AI in combating phishing and social engineering, there has been an immense challenge regarding AI integration, which needs to be addressed to have both efficacy and compliance in alignment with the Indian legal framework. To identify and mitigate phishing threats, AI flourishes by collecting and analysing an avalanche of data and sometimes by capturing user behavior and network activities. Although these practices increase security considerations, they lead to some important questions on privacy, liability, and regulatory compliance. In India, the 'Digital Personal Data Protection Act, 2023' (hereafter, DPDPA) has certain provisions about handling data, and it focuses on making the data processing process transparent and on the consent of the user, etc. However, with the growing use of AI-based cybersecurity solutions, legal and ethical concerns related to privacy, accountability, and regulatory compliance need to be carefully navigated to reconcile the needs of security with the rights of individuals. This complex set of interactions between technology and law shows how important it is to clarify on a legal basis the use of AI in cybersecurity, notably for data privacy, liability, and the requirements of regulation and ethics. [731]

Data Privacy Concerns in AI-Driven Cybersecurity

Data privacy is one of the most pressing legal challenges with AI-driven anti-phishing solutions. Many AI technologies that can detect and prevent phishing attacks require large datasets to work well, and that requires collecting large amounts of user information—including personal and behavioural information. Unauthorized access or misuse of this data collection may violate individuals' privacy rights, which conflict with this data collection. The DPDPA, which lawfully safeguards personal data, mandates that data must be collected in a lawful, fair, and transparent manner. Under "Section 4 of the Data Protection and Privacy Act (DPDPA), organizations need to notify users regarding a specific purpose for data collection and have to obtain users' consent specifically." But about AI-driven cybersecurity, that's not an easy thing because who knows if they are giving their informed consent?"

[731] Rohit Tahsildar Yadav, "AI-Driven Digital Forensics," *10 International Journal of Scientific Research & Engineering Trends* 75 (2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 4 AND ISSUE 4 OF 2024

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

Moreover, when continuously using AI for monitoring in cybersecurity, there is a possibility of breaching privacy. In *"K.S. Puttaswamy v. Union of India*[732]", established the right to privacy as a fundamental right and confirmed that any breach of privacy must be necessary and proportionate. Monitoring AI user activity every second may be too much, especially if it implies private data processing with no proper, compelling use. When AI is used in cybersecurity, working in compliance with privacy regulations such as the DPDPA and General Data Protection Regulation (GDPR) in the EU is essential for organizations. Failure to comply could result in significant penalties and reputational damage, and if companies intend to use privacy-preserving AI, limited data collection is needed for effective threat detection—only what is truly necessary.

Accountability and Liability Issues

Accountability in AI-driven cybersecurity is complicated, especially when AI systems miss phishing threats or do unintended harm. Due to increasingly complex AI systems being developed and deployed by multiple stakeholders, including technology providers, organizations, and third-party vendors, determining liability can be difficult. If an AI solution misses a phishing attempt, leading to a data breach, questions surface regarding who, in the hierarchy, should be held responsible. Depending on specific case circumstances and contractual terms, both the organization using the AI and the tech provider, or either of them, could be liable.

Under DPDPA, entities that process personal data are held accountable for data breaches that occur, which means organizations that use AI solutions may well be responsible for damages that result from security lapses. However, in India, liability issues are complicated by the lack of clear legal precedents. In some cases, strict liability may apply, meaning companies will be liable for harm caused by AI regardless of control over an outcome. [733]

Ethical Concerns: Surveillance vs. Privacy

In cybersecurity, AI-driven surveillance has large ethical implications, as it is necessary for organizations to perfectly balance user rights to privacy and security. However, AI's ability to monitor and analyze user activity in real time can serve a valuable purpose, thwarting many phishing and social engineering attacks while also opening up the possibility of pervasive surveillance. Monitoring continually can result in users suffering the feeling that they are being watched (eventually) creating the impression that they are being spied upon. Under the "Puttaswamy" judgment, a proportional approach to privacy violations is involve; this has become especially relevant.

Whether AI surveillance in cybersecurity can be justified based on its ability to prevent massive harm poses an ethical dilemma. For example, monitoring user behavior can disclose phishing attack patterns while inadvertently also disclosing private information not related to the security threats. The collection of only the minimum data needed to achieve the desired security goals is also an ethical principle, although it might not always be achieved. Yet the balance between maintaining user privacy and security while ensuring the success of AI is hard to achieve because organizations need to program AI systems so they respect user privacy but do not compromise security. To tackle ethical concerns, a set of transparent policies about how the data is used and give users the ability to see how their data is collected and control its collection can be added.

Regulatory Compliance and Challenges

The big challenge is the speed of technological evolution compared to the ability to align new AI cybersecurity platforms with existing

[732] [2017] 10 SCC 1.

[733] Artificial Intelligence and Cyber Crime: Facing New Threats and Embracing New Potential, *available at:* https://sdi.ai/blog/artificial-intelligence-and-cyber-crime/ (last visited on October 12, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

regulatory frameworks. As per India's DPDPA, personal data must be processed with transparency, fairness, and user consent. Yet, AI's need to work with huge datasets in order to work properly can come into conflict with these regulations. Enforcing DPDPA principles, including purpose limitation, data minimization, and storage limitation, is challenging in AI-driven systems, which constantly learn and evolve with user data.

Indian organizations too, who deal with data of EU citizens, have to comply with these international regulations like GDPR, creating yet more complexity in compliance efforts. The GDPR's stringent requirements for user consent, the right to be forgotten, and data portability might not always fit easily with AI-driven cybersecurity. Moreover, cyber threats tend to be cross-border and remain challenging in terms of jurisdictional matters due to the cross-border nature of AI-based solutions. [734]

LEGAL FRAMEWORK AND REGULATORY MEASURES FOR AI IN CYBERSECURITY

With multiple national and international frameworks on its head, AI in cybersecurity is a complex legal landscape. The role of artificial intelligence in detecting and mitigating phishing and social engineering attacks has led regulatory bodies across the world to institute standards that regulate data handling, privacy, and accountability around cybersecurity. All of these frameworks are built around the tension between innovation in security technologies and the protection of individual privacy and civil rights. Over recent years, however, the growing popularity of AI-based cybersecurity solutions has created a high demand for laws to ensure their correct functioning. The problem, however, is that existing legal frameworks often fall behind the pace of progress of fast-developing technologies leaving a critical need for reforming the law in line with the technological changes, especially when it comes to AI, ensuring that the latter complies with privacy and data protection laws as well as keeping abreast of modern events. The research addresses global standards, India's unique regulatory regime, outlined reforms towards improved oversight, and case studies to demonstrate legal responses to AI-induced cyber threats. [735]

Global Regulatory Perspectives

The most prominent regulation of AI in cybersecurity at the global level is represented by the General Data Protection Regulation (GDPR) within the framework of the European Union (EU). One of the most stringent data protection laws in the world, GDPR lays down tight standards for how companies can process data, how to get consent from users, and how to protect user privacy. In the case of utilizing AI for cybersecurity, new regulations under GDPR obligate companies to justify their data processing activities, more so if sensitive data is processed. Particular provisions—for example, "Article 22"—already restrict the use of automated decision-making, affecting, therefore, the deployment of AI technologies that may profile or monitor user behavior without prior consent. GDPR also includes the right to be informed and the right to object to data processing, an obstacle for AI systems that gather data continually to adapt and make their threat detection more effective. The legal emphasis on transparency and the autonomy of users has led AI cybersecurity solutions in the EU to take a more privacy-focused approach, and these regulations are influencing regulations globally.

Unlike the United States, however, there is no centralized federal data protection law, like GDPR. Herein, the U.S. segments its data protection rules, imposing sectoral laws dealing with data protection in this or that sphere (the Health Insurance Portability and Accountability

[734] Jaime Gaona, "The Role of AI in Forensics," *available at:* https://marymount.edu/blog/the-role-of-ai-in-forensics/ (last visited on October 13, 2024).

[735] Harsh Behl, "From Sci-Fi to Crime-Solving: How AI is Transforming Digital Forensics for Law Enforcement," *available at:* https://www.exterro.com/resources/blog/from-sci-fi-to-crime-solving-how-ai-is-transforming-digital-forensics-for-law-enforcement (last visited on October 15, 2024).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 4 AND ISSUE 4 OF 2024
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Act (HIPAA) may serve as an example, which covers data protection in a healthcare context). State-level initiatives like the California Consumer Privacy Act (CCPA) have recently come about and are changing the rules of the game to offer greater consumer privacy protections in the AI space and cybersecurity. Although U.S. regulations like the Federal Trade Commission (FTC) have offered ethical use guidelines for AI, they are a sum of the parts rather than a single cohesive federal AI framework. A decentralized approach poses challenges for companies operating internationally, which have to contrapose different regulatory standards. Unlike the EU's GDPR, the U.S. lacks a federal AI regulation model, which demonstrates an enormous gap between global cybersecurity regulatory models toward AI.

India's Legal Framework on AI and Cybersecurity

India's approach to using AI in cybersecurity is currently unfolding as India endeavours to enhance its legal framework for AI in cybersecurity via the recently passed "Digital Personal Data Protection Act, 2023" (DPDPA), seeking to ensure data privacy, transparency, and accountability. The DPDPA requires that personal data processing including AI-driven monitoring is lawful, fair, and transparent. Provisions such as 'Section 4' demand that individuals be freely consented to before data processing by AI cybersecurity tools, namely they must receive express authorization to gain access to personal information. Apart from that, India's cybersecurity regulation relies on several backbones, together with the IT Act, of 2000, also known as the 'Information and Technology Act of 2000'. Crimes under "Section 43", unlawful access, and "Section 66D", cyber fraud, which includes phishing or social engineering, have been specified to be punishable offenses. While the current regulatory focus on cybersecurity is almost exclusively oriented toward addressing cyber threats from a technical angle, the unique implications of AI in cybersecurity are not being addressed.[736]

Also, there are various policies and initiatives launched by India to promote responsible AI deployment. NITI Aayog's "National Strategy for Artificial Intelligence" emphasizes the ethical use of AI and [recommends] transparency, privacy, and accountability principles for development and implementation practices. However there have been no related specific AI laws prohibiting applying AI to the area of cybersecurity, so there is a regulatory gap for the implementation of AI standards in cyber defense. As pressure mounts on AI to help defend sensitive data and critical infrastructure, this makes for an excellent case for India to take a targeted approach toward AI regulation, with specific clauses to cover steps AI can take to fight the growing cyber threat. This requires guidelines for the permissible use of AI in cybersecurity and compliance requirements consistent with international best practices. Cases like *Shreya Singhal v. Union of India*'[737], speak for the balance of privacy rights and the demands of cybersecurity that have prompted the continuing AI discourse in India's legal terrain.

Case Study: Legal Responses to AI-Driven Cyber Threats

The EU's handling of the *"Google Spain SL v. Agencia Española de Protección de Datos"* [738] case is an illustrative example of legal developments to address cyber threats posed by AI. This landmark decision applied data protection laws to digital platforms that use automated data processing, establishing a precedent for AI applications related to data protection, specifically the "right to be forgotten" under the GDPR. Although not directly focused on phishing, the case set critical boundaries for AI-driven data analysis in the EU, reinforcing user control over personal data in the context of AI. This legal response shapes

[736] AI Policies in India: A Status Paper, *available at:* https://www.tec.gov.in/pdf/Studypaper/AI%20Policies%20in%20India%20A%20status%20Paper%20final.pdf (last visited on October 15, 2024).
[737] [2015] 5 SCC 1.
[738] (2014) C-131/12.

how AI is permitted to handle data within the EU, demonstrating a framework that could inspire similar protections in India. By implementing robust data protection mechanisms for AI tools, India can reinforce the right to privacy, ensuring AI's responsible use in cybersecurity.

CONCLUSION

The incorporation of the use of AI against phishing and social engineering is a vital step in the evolution of cybersecurity and supplies a new resource to be used against continuously more complex cyber threats. Phishing and social engineering attack human weaknesses rather than technical weaknesses and therefore do not fit well with traditional defense and instead show the need for adaptive, intelligent systems. Machine learning, natural language processing, behavioural analytics, and predictive analytics are just some of the AI technologies that offer strong methods for spotting and preventing phishing attempts and bolstering cybersecurity defense. However, as this paper has demonstrated, the introduction of AI in cybersecurity faces some complicated legal and regulatory challenges, especially in India. Current legislation—such as the "Digital Personal Data Protection Act, 2023" and the "Information Technology Act, 2000"—provides some basic guidance, but it isn't an all-encompassing solution for the specific issues presented by AI, such as privacy ramifications, accountability, and ethical responsibilities.

At present, India's legal framework will need to evolve to make the most of the benefits that AI can bring while protecting individual rights. New reforms are needed to precisely define the responsibilities and liabilities of AI operators, establish the standard of data privacy, and lay ethical guidelines for AI-driven surveillance. India can learn from international standards like the GDPR and adopt best practices to not only ensure that our compliance is airtight but also protect our users. Furthermore, if the public sector doesn't grow into the digital landscape, it will be left behind, but if public sector actors work together with the private sector, they can help shape policy, promote transparency, and adapt over time to newly developing cyber threats. By proactive cybersecurity legislative reform and working together, AI can be used to bolster cybersecurity by finding the right balance between security and privacy to responsibly and appropriately realize the benefits of AI in cybersecurity.

SUGGESTIONS

As AI takes a more central role in fighting phishing and social engineering in India, there are a few suggestions that can improve its effectiveness while preserving privacy and filling regulatory holes. To create a balanced and effective framework, India should consider the following approaches:

- Some of the preexisting cybersecurity laws are the 'Information Technology Act of 2000' and the 'Digital Personal Data Protection Act of 2023 (DPDPA), although these laws provide fundamental protection for data but do not offer procedures for artificial I intelligence. Bearing in mind those features of AI when developing regulations concerning cybersecurity can help to reduce legal uncertainty and assign proper liability to the operators and developers of AI tools.
- As data collection and storage are the key aspects when it comes to the DPDPA and the focus on specific user consent, all organizations that use AI for the detection of phishing incidents should keep the users of the services informed about data collection practices. This should come in the form of the type of data being collected, the purpose for the analysis, and how the data is secured from misuse. To ensure compliance with the principles of general protectiveness and respect for individual autonomy, there is recommended transparent communication that is respectful for the recipients and allows them to obtain their informed consent.
- CCTV for cybersecurity cannot

compromise the privacy of users. Substantial privacy issues can be addressed by methods of ethics that define limitations to monitor, store, and analyze data. Conducting privacy by design provisions and guaranteeing compliance with proportionality principles respects simultaneously security and individual rights, according to the "Puttaswamy" judgment on privacy.

- The built-in bias check can occur through regular audit checks of the AI algorithms used for phishing detection to detect bias issues, system and data security considerations, and regulatory compliance, meaning that the AI system is ethical and sufficient. Third-party evaluations should also be promoted to offer external confirmation that enhances the general credibility and compatibility with the standards of regulatory authorities.
- Since there are several players when it comes to the deployment of AI technologies: the developers, the technology providers, and the respective organizations, there is a need to have defined structures of liability. He suggested a structure of attributing liability about control and supervision while echoing intermediary liability principles in *"Shreya Singhal v. Union of India"*[739], which may also assist in identifying when the use of AI solutions is unsuccessful.
- Since one of the biggest needs of AI is data, coming back to data protection standards is necessary. Implementing high levels of data minimization, purpose limitation, and storage limitation policies guarantees that only the data required is processed when deploying AI, making its use compliant with privacy principles to protect end users' data.
- It is agreed that industry, academia, and the government can collectively foster both the technical and the supportive functions of AI. Such partnerships can enhance the timely and accurate exchange of information concerning the strategies used in phishing, enhance the demystification of cyber security, and develop enhanced and flexible policies.
- Incorporating the lessons from global standards like the EU's GDPR or the advice it receives from the international AI ethic bodies, India can boil down the best practice that propels the country towards the right values of privacy, transparency, and data protection. Implementing principles following the right to information and limiting the use of automated decisions increases users' control as well as legal protection.
- Aiding RND for AI-based anti-phishing products can help India develop certain sophisticated certifications for protecting against phishing. To meet these challenges, India should invest in research on emerging areas of analytics like prediction, quantum computing, and multi-modal AI for cybersecurity.

They can all collectively constitute a comprehensive, legally viable strategy that will enable AI to fortify cybersecurity in India. Thus, through these measures, India can successfully protect the legal rights and provide the incentive for more development of artificial intelligence.

[739] AIR 2015 SC 1523.