LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National & International Scholars"

EDITORIAL TEAM

LEX SCRIPTA MAGAZINE OF LAW AND POLICY (VOL-4, ISSUE-1)

ISSN-2583-8725
Vol - IV, Issue - I
Published by INTEGRITY EDUCATION INDIA

New Delhi
First Floor, 4598/12-B, 1st Floor,
Padam Chand Marg, Daryaganj,
New Delhi, Delhi 110002
Phone: +91 98 11 66 62 16 (M)
Phone: +91 70 11 60 56 18 (M)

Bengaluru
Jallahalli East
Bengaluru, Karnataka. India.
Phone: +91 98 11 66 62 16 (M)
Email: publisher.integrity@gmail.com

USA
New Jersey
14 Grandview Ave, Upper Saddle River,
NJ-07458, USA
Phone: +14805226504 (M)

London
37 Degree Media
64, Hodder Drive, Perivale, London UB68LL.
United Kingdom.
Phone: +44 7950 78 18 17 (M)
Website: integrityeducation.co.in

For any Query / Feedback
Phone: +91 98 11 66 62 16 (Vineet Sharma)

Printed in India @ New Delhi

ISSN: 2583-8725

Lex Scripta Journal

Quarterly Online and Print Edition

Law & Policy

"Join the League of National and International Scholars"

LEX SCRIPTA MAGAZINE
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

LexScriptaMagazine.com ISSN: 2583-8725 Vol. 04 - Q1 Jan - Mar, 2026

Lex Scripta Journal

Cybercrime in India (2024–2026): Emerging Threats, Landmark Cases, and the Evolving Legal Response

Author
Rajat Jharwal
Alpika Shrivastava

Cybercrime in India (2024–2026): Emerging Threats, Landmark Cases, and the Evolving Legal Response

Rajat Jharwal1
LL.M., Faculty of Law,
Jagannath University, Jaipur

Alpika Shrivastava2
Assistant Professor, Faculty of Law,
Jagannath University, Jaipur

Abstract

India has completely changed the nature of cybercrime in the years 2024 and 2025.It only increased by 206 percent in 2024 alone to an approximate of Rs 22,845 crore in losses due to cyber fraud, and cybercrime cases were registered in the country more than once a category of crime had reached the history of a nation. This monumental rise has not only been enabled by the rising digital access but by a qualitative shift in crime techniques: AI created deepfake impersonation, the so-called phenomenon of digital arrest fraud, massive stealing of cryptocurrency and systematic data breaches impacting tens of millions of citizens. It has also given rise to a wave of historic judicial interventions such as the Madras High Court declaring cryptocurrency legally recognized as a protected property and the first major litigation based on the Digital Personal Data Protection Act, 2023 that occurred as a result of corporate data breaches. Herein the paper looks at the major forms of cybercrime that have developed or increased in this timeframe, considers the major cases that have led to a developing legal knowledge base and how well the legal and enforcement framework in India has kept up with a more complex threat landscape. It claims that the next three years, 2024-2026, is a decisive inflexion point where an incremental response in legislation should be displaced with an actual and sustainable integrated governance base, which can keep up with the speed and human resourcefulness of the latest cyber criminality.[124]

1. LL.M., Faculty of Law, Jagannath University, Jaipur
2. Assistant Professor, Faculty of Law, Jagannath University, Jaipur
3. Hatakambari v. Zanmai Labs Pvt. Ltd., Madras High Court (2025).

Keywords: *Cybercrime; digital arrest; deepfake fraud; WazirX; Star Health data breach; DPDP Act 2023; cryptocurrency; AI-enabled fraud; India.*[78]

Introduction

Aqutely vulnerable to 2024 to 2026 India entered a phase of vulnerability in its digital economy.The two drivers of blistering digital growth and professionalization of cyber-crime came together to create a situation where any and every sector of the economy, including healthcare insurance and cryptocurrency exchange, government welfare portals and individual mobile banking consumers, could not be targeted by a large-scale cyber-attack.What is not just significant in terms of this period in the history of Indian cybercrime but also qualitative is the level of criminal activity: hackers have used artificial intelligence to create convincing fake profiles of law enforcement agents, have broken through multi- signature cryptocurrency wallets, designed with cutting-edge security measures, and have employed rogue insiders to sell sensitive health information of tens of millions of citizens.This has forced the legal system to react to it and occasionally in manners that have yielded truly new jurisprudence.The acceptance of cryptocurrency by the Madras High Court as a form of property, which has a potential to enjoy legal protection, the regulatory measures that arose following the Star Health Insurance breach under thethe recently passed Digital Personal Data Protection Act, 2023 as well as the focus on electronic arrest laid on by the very Prime Minister is indicators of an era where cyber crime came to dominate the fringes of the Indian law and governance discourse. However, enforcement still remains behind the development of threats, and the legislative infrastructure, which is not designed but is repurposed, demonstrates signs of structural incompetence against AI-powered and global-scale criminal activities.

As argued in this paper, 2024-2026 should be interpreted as an intermediate phase in Indian cybercrime law, characterized by three overlapping tendencies: in the field of fraud and impersonation, there is a weaponization of artificial intelligence; in the field of critical digital infrastructure, institutional targets of high value are being targeted; and the Digital Personal Data Protection Act framework is being first seriously tested with real enforcement controversies. Both of these trends involve queries that surpass the technicalities of any particular statute and assail underpinning inquiries of the governance structure, institutional capability, and the security of constitutional rights and freedoms in the digital realm.

The Scale of the Problem: Data and Dimensions

The pandemic of cybercrime in India 2024-2026 is a scenario of a growth that almost doubles every year. National Crime Records Bureau reported that in India, officially registered cases of cybercrimes increased by about 18 percent in 2024, first time passing one lakh cases, and registered 1,01,928 cases as compared to 86,420 cases in 2023.[2] Among these 73,987 incidents were associated with fraud, financial cheating and scams on the internet, by far the most prevalent. Women were victims in over 18,600 cybercrime incidents and minors in 1,753 reported cases, indicating a wide demographic impact of victimization online. Even more difficult is when there is a loss of money. According to information collected by the Indian Cyber Crime Coordination Centre, cyber fraud losses are estimated to be about Rs 22,845 crore in 2024, 206 percent higher than the lost sum of Rs 7,496 crore in 2023.[3i] The majority of this number which was estimated to be as high as Rs 17,400 crore could be said to have been due to investment-related frauds, where the victims would be lured into the fraudulent schemes on social media and messaging applications, on the promise of getting unrealistic returns on their financial instruments and cryptocurrency. It was estimated that by early 2025 India would finally surpass 25 lakh cybercrime complaints via the National Cyber Crime Reporting Portal indicating not only increasing crime but also a higher level of knowledge of reporting systems among the population.[3]

The institutional reaction has been a large-scale but not necessarily effective one.The budget 202526 of the Union Budget has designated funding to cybersecurity projects to the tune of Rs 782 crore, and the I4C has reported that it has stopped more than 9.42 lakh SIM cards and 2,63,348 IMEI numbers associated with operating cyber frauds.The immediate assistance through calling the national helpline 1930 on cybercrime significantly increased the number of calls compared to the time before[13] , and 109 cybersecurity mock drills involving 1,438 organizations of all sectors were achieved by March 2025 with the support of CERT-In.But these measures have failed to halt the increases in losses and that it can only be inferred that the responses of operations, no matter how scaled, cannot replace the structural legal and institutional changes that the situation requires.[53]

4. Cybercrime Cases Up 18%, Fraud Emerges Biggest Motive, Times of India (2026).
5. 1930 Indian Cybercrime Helpline, Government of India.

The Rise of AI-Enabled Cybercrime: Deepfakes and Digital Arrest Fraud

The most notable aspect of the 20242026 India cybercrime environment has been the careful application of the artificial intelligence to make the criminal activities more impactful and believable. Two types of AI-powered fraud have received special legal and policy concern: the impersonation through deep faking and the so-called digital arrest fraud. These categories overlap in terms of technical processes, however, they differ in terms of psychological processes and legal characterisation.Deepfake scams, which are the creation of fake audio or video recordings, are what make it believable that the image or face of a actual person familiar to the victim is being duplicated, say a family member, workplace supervisor, or government official, and they are being influenced to send or reveal details about sensitive data. The State of AI-Powered Cybercrime Report 2025 declared that in 2024, 82.6 percent of phishing content detected in India was created with the help of machine-learning tools.[9] In India, law Deepfake fraud is already a legal issue: the Information Technology Act itself does not directly deal with AI-generated synthetic media, and a prosecution would have to invoke the cheating by impersonation provisions of the Bharatiya Nyaya Sanhita, 2023 and the cyber fraud provisions of the IT Act, which were not written regarding synthetic media. Digital arrest fraud is probably the most psychologically advanced type of cybercrime that has been introduced during this time. The fraud is usually in the typical form a victim is called or a video message is sent by a law enforcement agent, customs official or narcotics authority that the victim or a relative is somehow involved in a major criminal case. The victim has to spend large amounts of money to get their home or specially selected room clearance or a relative imprisoned to be released, and they are to keep their phone or laptop camera running at all times, staying awake to make the payments. The scammers engage AI generated overlay videos, contrived identity documentation and involved theatrical multi participant setups to maintain the scam sometimes several days. The extent of online fraud involved in arrests in India has been astonishing. The number of reported cases almost tripled in 2022-24, as it reached approximately 40,000 in 2022 and almost 1,24,000 in 2024.In February 2025, the amount of losses due to the digital forms of arrest had strolled up to Rs 2,600 crore.[12] It came under the personal notice of Prime Minister Narendra Modi, who discussed the phenomenon in his October 2024 Mann Ki Baat speech, clearly stating that there was no system of mass surveillance and regulation of the digital world in the Indian laws at all - something which would not have been clarified without the popular credibility that the scam had some degree of achieving

even among well-educated and professionally successful victims such as doctors, former bureaucrats, and former police officers. The human cost has been extremely high: few victims, who cannot endure the long-term psychological stress caused by the fraud, have committed suicide. From a legal standpoint, digital arrest fraud engages provisions of the Bharatiya Nyaya Sanhita relating to cheating, impersonation of a public servant, and criminal intimidation, as well as sections 66C and 66D of the IT Act covering identity theft and cheating by impersonation using computer resources. The organised, cross-border nature of many such operations — a significant proportion originating from fraud factories in Southeast Asia, particularly Myanmar, Cambodia, and Laos — creates attribution and jurisdictional challenges that domestic enforcement mechanisms are poorly[64]

The WazirX Hack (2024): Cryptocurrency, Jurisdiction, and Property Rights. July 18, 2024, WazirX - the largest domestic cryptocurrency exchange in India at the time - experienced what was later to be one of the biggest cyber-theft incidents in Indian history.Attacks, which were later alleged by worldwide cybersecurity experts to have been led by the North Korea-related Lazarus Group, exploited loopholes in multi-signature wallet infrastructure on WazirX which is controlled by Singapore-based custodian Liminal Custody, looting about USD 234.9 million (approximately Rs 1,900 crore) of digital assets.It was a well-planned attack, with the pre-insurance of funds with Tornado Cash taking place seven days previous to the breach, and the typical hacking of a smart contract that puts the wallet in charge.The exchange had to halt all withdrawals and trading and 4.2 million users were unable to get their assets back.In November 2024, one suspect, Masud Alam of West Bengal was arrested by Delhi Police.Investigations further established that in addition to a Telegram account, Alam had opened up a WazirX account under an alternate identity and sold an access to the WazirX account via Telegram, which was later utilized in the breach.Nevertheless, the essential attribution issue of conclusively attributing the technical execution of the attack to the Lazarus Group and any other form of legal responsibility of state-linked foreign actors is still out of realistic capabilities of Indian domestic law enforcement.The non-cooperation of Liminal Custody in providing Indian police dissatisfaction with its investigations or even the data requested has also complicated the investigation process, raising concerns about the inadequacy of current frameworks when it comes to forcing cross-border evidence disclosure in

6. Singh & Dhiman, Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India (2025).

cases of cyber-theft.The most legal event that happened due to the WazirX incident was that in October 2025, a landmark decision was taken in the case of Hatakambari v. Zanmai Labs Pvt. Ltd and Ors. by the Madras High Court.The case was brought on after Wazir in its Singapore court-monitored restructuring suggested a model, known as socialization of losses, in which all of the users, even those not in possession of the impacted ERC-20 tokens, would incur a proportional portion of the losses incurred on the hack.JusticeThe Indian High Court N. Anand Venkatesh blocked WazirX from transferring the 3532 holdings of XRP belonging to a user and ordered the Indian arm of the business, Zanmai Labs, to satisfy the value of the frozen assets that was awaiting an arbiter with a bank guarantee.This way, the Court formally acknowledged cryptocurrency as property, which could be held under the trust and could be legally protected under the terms of Indian law, the first court ruling of this kind in the entire legal history of the country.The consequences of the Hatakambari case go way beyond the circumstances of the Wazir case.Defining cryptocurrency as property, the Court has provided a doctrinal framework to enable victims of cybercrime involving cryptocurrencies to seek civil damages such as injunctions, recovery actions, and trust actions.It further casts doubt on whether the stealing of digital assets meet the definition of theft under the current criminal legislation of cryptocurrency theft - specifically, whether the act of stealing digital assets qualifies as a case of theft in the Bharatiya Nyaya Sanhita, 2023 or must be characterized akin to unauthorized access and dishonesty the acts under the IT Act. misappropriation of computer resources.[1]

The Star Health Insurance Data Breach: DPDP Act and Intermediary Accountability

The 2024 Star Health Insurance data breach is the most legally notable instance of corporate data security breach in the recent Indian history, not only because of the proportion of its effects, but also because of the new legal issues it brought out such as the intermediary liability, regulatory jurisdiction, and the early application of the Digital Personal Data Protection Act, 2023.The largest stand-alone health insurer in India, Chennai-based Star Health and Allied Insurance Company was a victim of a security breach, where personal medical and medical records, PAN card numbers, policy details, and personal medical photos of approximately 31 million customers were stolen. The data was then auctioned on the dark web at up to USD 150,000 and worse still, they were searchable in real-time due to chatbots that the hacker ran on the Telegram messaging platform. The law suits due to violation were complex. Star Health brought a civil proceeding against

Telegram and Cloudflare, the content delivery network by which some of the data leaked was available and obtained interim injunctive relief requiring the sites to block and remove the objectionable material. On October 25, 2024, the Madras High Court ordered Telegram to block and delete any posts or chatbots flagged by Star Health and order the distribution of customer data, with Justice K. Kumaresh Babu ordering Star Health to provide unique URLs and account information to allow the takedown. The arguments that Telegram was not afforded the ability under the IT Act to search actively and delete offensive content without identifying factors and that it was not given the power to drop accounts in their entirety without a reasonable cause were intriguing regarding the scope of intermediary liability in the Indian law. Another writ petition made by a cybersecurity researcher Himanshu Pathak of CyberX9, to seek a court-ordered investigation into the breach by the Ministry of Home Affairs, was rejected by the Madras High Court, on the allegation that Star Health had already instituted parallel civil proceedings and an interim order was in force. On October 18, 2024, the Insurance Regulatory and Development Authority of India confirmed reports of data leaks by two insurers without naming the companies as it issued a press statement acknowledging the breach and stated that there were mandatory cybersecurity guidelines that applied to insurance companies.

The regulative reaction received criticism due to its muted tone considering the magnitude of the breach and the Internet Freedom Foundation sent an email to the Ministry of Electronics and Information Technology requesting CERT-In to take charge of the investigation. The Star Health incident is of special interest to the early implementation of the DPDP Act. The structure of the Act in relation to the notification of breaches, liability of data fiduciaries, and civil penalties which may include up to Rs 250 crore in the most severe instances was the first to be used in a high-profile context in regulatory debates into this breach. Legal practitioner commentary noted that there was a conflict between the section 43A of the IT Act, which had established a more sophisticated compensatory mechanism on data security negligence, with the more recent, but more comprehensive, framework of the DPDP Act. Other issues raised pertaining to insider were also brought to the table. Threats: it was reported that a senior official at the company had sold data to the hacker, raising issues of corporate governance and the individual criminal responsibility of the company officials in case of data breaches effected through internal misconduct.[5]

7. 1930 Indian Cybercrime Helpline, Government of India.

Institutional Breaches and Critical Infrastructure: Hathway and Sector-Wide Vulnerabilities

The breach at Star Health was not the only one in the 2024 cyber world. Using a weakness in the Larval framework software applied by Hathway cable and datacom ltd a leading internet service provider in India, a cybercriminal who goes under the name downfield topped the personal data of about 41 million customers including Aadhaar numbers, email address, and home addresses. This breach exposed 12 gigabytes of sensitive data publicly with another 214 gigabytes of production data that was said to have been compromised - a breach of colossal magnitude since Aadhaar biometric-linked identifiers were included in the breach data. The incident brought to sharp focus the security procedures of the internet service providers, who access sensitive data of subscribers yet might not be subject to the same regulatory scrutiny as financial institutions. Both HDFC Life Insurance and Niva Bupa Health Insurance claimed that they experienced possible data security events in 2024 related to the allegedly exfiltrated customer data by unidentified individuals.

In Bengaluru, digital identity verification company Signzy, which operates as part of the network of more than 600 financial institutions around the world, was breached, impacting a large portion of its institutional and end-user clientele of its clients — an event that has demonstrated the systemic risks posed by aggregation of sensitive financial data to third-party technology service providers. The target of the McLeod Russel ransomware attack, which targeted India and the biggest tea plantation company in the world, put the financial and healthcare sectors on a par with traditional industry demonstrating that no type of commercial establishment may consider cyber risk as something that only digitally native businesses have. The unlawful nature of such institutional violations can be seen as cumulatively legally significant as it demonstrates how discrepant the official regulatory standards and the real security practices are.[6] Mandatory reporting guidelines by CERT-In, the RBI-regulated cybersecurity systems of regulated participants and the sector-specific guidelines of IRDAI all carry implications that were evidently not met in some of such incidents. Such an enforcement gap can be viewed both as a symptom of resource limitations that regulatory authorities endure, and as a result of the inherent impossibility to pre-empt standards-based regulation through the pursue of threats in an area where the threats are changing more rapidly than the regulatory processes. The penalty framework

[6] Cybercrime Cases Up 18%, Fraud Emerges Biggest Motive." The Times of India, 2026

provided by the DPDP Act, of a penalty based on provable harm and failure to meet certain obligations, has the potential to provide a more effective enforcement tool than the prescriptive-standards method however its practical implementation will require the creation of an effective Data Protection Board of India.[7]

Legal Framework: The DPDP Act 2023, BNS 2023, and Emerging Regulatory Architecture

The period under review has been characterized by architecture change in its legislative structures which are defining and prosecuting cybercrime.The Bharatiya Nyaya Sanhita, 2023, to supersede the Indian Penal Code, July 1, 2024, had transferred and continued and in certain aspects.cases enhanced laws applicable in cyber-enabled crimes such as cheating, impersonation, criminal intimidation, and extortion.The shift, although much the same in its approach to substantive cyber offences, brought procedural reform, and caused some modification by researching agencies used to the framework of the century-old predecessor law.The Digital Personal Data Protection Act, 2023, which was assented to by the president in August 2023, and began implementing in phases until 2024, is the most structurally significant change in the Indian digital law environment since the IT Amendment Act of 2008.

The Act provides a framework of consent-based personal data processing, a duty to disclose breaches to the Data Protection Board and individuals harmed as a result and a regime of civil penalties up to Rs 250 crore in the case of the most egregious offenses.The initial practical test of its provisions with reference to the operations of the Star Health breach and other 2024 breaches revealed that the Data Protection Board of India, upon which the Act is to be mostly depended, was not yet in full force by the time of the great breaches of 2024, which made its active application constrained.The regulatory framework was also augmented by the Promotion and Regulation of Online Gaming Act, 2025 which was signed on August 21, 2025 and put a complete prohibition on online money gaming along with its promotion, advertisement and financial transactions.Although it is mainly a consumer and financial regulation, the Act has some consequences of cybercrime governance insofar as some of the most popular tools of high scale financial cyber fraud throughout the period have been fraudulent online gaming and websites of investment.

[7] 1930 Indian Cybercrime Helpline, Government of India.

In 2024, the action of SEBI concerning algorithmic manipulators who trade with AI-driven bots and spread fake news to fix the price of securities further expanded the boundaries of regulatory control of cybercrime responsibility to securities markets.[5] [8]

Enforcement Architecture: Progress and Persistent Gaps

India's enforcement response to the cybercrime surge of 2024–2026 has been marked by genuine institutional change and structural constraint over time.Expanding the I4C, scaling the National Cyber Crime Reporting Portal, enrolling more than 1,05,796 police officers in the CyTrain digital forensics training portal, and introducing coordinated efforts like the CyHawk in Delhi Police - which has so far seen the arrest of more than 1,000 cyber fraudsters - reflect a significant increase in enforcement capability.Although the probability of frozen funds being returned is low (in absolute terms), it increased, to an average of 24 percent in 2025, which was a boost of about 10 percent by 2025 as a result of having better coordination between police, banks, fintech companies and telecom providers.[8]

These profits should be tempered when it is found that they work in a system that is highly strained.By early 2024, there were almost 75,000 cybercrime cases pending trial in Indian courts alone and more cases referred throughout the year.The courts themselves, as they build up more intricate jurisprudence about digital evidence and the property rights on cryptocurrency, even have a volume problem that endangers to demand specialised focus that cybercrime cases need.There is an increased use of Cyber Crime reporting portal.dramatically however the complaint-investigation-prosecution ratio is quite low and also the time between reporting and action has been an emotive point of huge frustration among the populace.The most unyielding aspect of the issue remains to be the cross-border enforcement.Another large percentage of financial internet fraud committed by victims in India has its roots in organised crimes in the South East Asian nations.The presence of Indian nationals in these offshore fraud factories, not only as organizers, but also as victims of trafficking forced to take part in the fraudulent activities, provides the problem of human rights with a nuanced facet to the problem that might be otherwise perceived as an issue of a strictly law enforcement issue.The mutual legal assistance treaty system of India has been not established in such a manner that it can deal with this form of digitally

[8] 1930 Indian Cybercrime Helpline, Government of India.

enabled, mobile and transnational organised crime and that the repatriation of suspects as well as evidence relies on bilateral trade documents that may not work as fast as digital investigations need to proceed. [9] The developments of 2024 to 2026 make a compelling case for a comprehensive reconsideration of The governance structure in cybercrime in India.The most urgent is that AI-enabled crimes such as deepfakes, voice cloning, and AI-generated impersonation are explicitly treated within the legislations.The current section of the IT Act and the Bharatiya Nyaya Sanhita concern downstream harms - cheating, impersonation, fraud -but not directly regulate the means of their perpetration in a manner that may impose a duty of care on AI-writing software creators, those running the platform, or the distributor of the output.An offence-specific clause that deals with the production, trading and use of synthetic media on fraudulent activities would help seal this gaps and vice as an indication of the gravity with which the legal system treats this group of harm.The second key reform agendah is the regulation of cryptocurrency.

The acknowledgement that the Madras High [10] Court has given crypto property in a WazirX case is a positive legal move, but it still can never replace a legislative framework that spells out regulatory treatment of the digital asset, the exchange accountability requirements, and the provision of clear mechanisms of the freezing, seizing and reclaiming of stolen crypto.The taxation presently adopted in India where cryptocurrency is treated as a financial asset, but the legal status of the cryptocurrency is not clearly established as property, presents the enforcement gap that the Lazarus Group and others have seized.The development of a specific virtual digital assets law, in which the civil facet and the criminal enforcement facet of offences related to cryptocurrencies are considered, has become a practical and urgent issue.Implementation of the framework of DPDP Act with the timely constitution and proper resources of Data Protection Board of India is crucial to effective functioning of the regulatory response to the data breach of the corporation.The Star Health incident revealed that the lack of an operational enforcement body within the Act places victims in the reliance of patchwork of sectoral regulators and civil court proceedings which the Act is meant to complement.

[9] Singh & Dhiman, Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India (2025).

[10] Cybercrime Cases Up 18%, Fraud Emerges Biggest Motive." The Times of India, 2026

Moreover, the intermediary liability system of the recently popular platform like Telegram, which was the key element in promoting the spread of stolen Star Health information.— needs stricter specifications on the proactive surveillance requirements of important platforms and of the repercussions of failing to comply with court orders and law enforcement requests.

Conclusion

The years 2024-2026 have been watershed years in terms of dealing with cybercrime in India. Professionalization of criminal activities, the application of the full power of artificial intelligence and vulnerability to critical infrastructure of an institution has led to losses and social harms of scale that no longer fit into the framework of change based on gradual revisions of laws drafted in a different technological landscape. The law has reacted by demonstrating bona fide inventiveness particularly via acknowledging cryptocurrency as legally safeguarded property and in injunctive jurisdiction to instill status-of-real-time liability on internationally connecting communications infrastructures. However impressive and impressive it may be, judicial creativity still is no substitute to legislative clarity. The Star Health Insurance breach, WazirX attack, the digital arrest epidemic and the Hathway data breach are symptomatic manifestations of inherent weaknesses of a system - in corporate cybersecurity governance, in the regulatory framework of data protection, in the legal framework of cryptocurrency, and in how well the enforcement agencies can keep pace with the sophistication of transnational organised cybercrime.

Combating these transgressions would necessitate that the legislative, judicial and executive arms of government consider addressing cybersecurity an issue of constitutional concern- one propagating out of the right to privacy as established in Justice K.S Puttaswamy [11]v. Union of India and the larger duty of the state to safeguard citizens against grave economic and personal damages in cyberspace. Cyberspace Justice The legal, technical, institutional and international aspects of a problem as cannot be addressed by a single tool alone are integrated: the direction of Indian cybercrime law.The events of 20242026 have rendered the price of fragmentation and defined it in hard financial and human numbers. The answer that such events require is a political system so solemn, and united, as befits the seriousness of the task.[4]9

References:

- Afzal, A., & Singh, A. (2026). Cyber Crimes in India: Challenges and Legal Reform. International Journal of Social Science Research (IJSSR), 3(1), 243–253.
- "Cybercrime Cases Up 18%, Fraud Emerges Biggest Motive." The Times of India, 2026.
- "India Says Cyber Fraud Cases Jumped Over Four-Fold in FY2024." Reuters, 2025.
- Cyber Crimes in India: Challenges and Legal Reform. ResearchGate publication, 2026.
- Cybercrimes and the Legal Framework of India. International Journal of Science and Research Archive (IJSRA), 2025.
- Cyber Crime Cases: Issues, Challenges & Solutions. Judicial Academy Jharkhand, 2025.
- Legal Challenges of Cybersecurity in Indian Context. TIJER Research Journal, 2026.
- Tripathy, S. S. (2025). A Comprehensive Survey of Cybercrimes in India Over the Last Decade. arXiv preprint.
- Singh, S., & Dhiman, S. (2025). Cybercrime and Computer Forensics in Epoch of Artificial Intelligence in India. arXiv preprint.
- Sarkar, G. (2024). A Framework for Distinguishing Cybercrime, Cyberattacks, and Cyberterrorism. ScienceDirect.
- "First Gangsters Act Case Slapped on Cyber Fraudsters in UP." The Times of India, 2026.
- "Rs 11.6 Crore Lost to Digital Arrest Fraud Since 2023." The Times of India, 2026.
- 1930 Indian Cybercrime Helpline. Government cybercrime reporting and response framework overview.
- Sanchar Saathi Initiative and India's Cyber Safety Measures. Government-backed cyber fraud prevention initiative.
- Kunal Kamra v. Union of India (2024) – Bombay High Court case on IT Rules and online speech regulation.

ABOUT LEX SCRIPTA JOURNAL

Lex Scripta Magazine is a premier peer-reviewed online and print journal dedicated to advancing scholarly research in law, policy, and social sciences. With the vision of promoting academic excellence and fostering a culture of intellectual exchange, the magazine provides a distinguished platform for academicians, researchers, legal professionals, and students to publish their original work and contribute to contemporary legal discourse.

Each submission undergoes a rigorous double-blind review process conducted by a panel of eminent national and international professors, ensuring the highest standards of quality and academic integrity. Lex Scripta not only encourages original and innovative research but also strives to bridge the gap between theoretical insights and real-world applications in the legal domain.

Contributors and editorial members receive global recognition through certificates and publication opportunities, while readers gain access to insightful, authoritative, and thought-provoking content across diverse areas of law and policy.

Now managed by Integrity Education India, Lex Scripta Magazine is committed to expanding its academic footprint through enhanced digital presence, global collaborations, and university partnerships. Upholding its ISSN identity, Lex Scripta continues to evolve as one of India's most trusted and respected journals in the field of legal research and education.

KEY FEATURES

- **Scholarly Insights** – Access in-depth, peer-reviewed research articles written by distinguished academicians and legal experts.
- **Global Perspectives** – Explore diverse viewpoints on law, policy, and governance from national and international scholars.
- **Authentic Content** – Read verified and academically sound articles that uphold the highest standards of research quality.
- **Knowledge Enhancement** – Stay updated with emerging trends, case studies, and policy developments across multiple legal domains.
- **Easy Accessibility** – Enjoy seamless access to online editions and exclusive hardcover issues for academic and professional use.

LEX SCRIPTA JOURNAL
JOURNAL MAGAZINE BY INTEGRITY EDUCATION INDIA

CONNECT WITH US 9811 666 216
7011 605 618