JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Cyber Law in 2025: Challenges and Legal Responses in the Age of AI, Data Breaches, and Digital Governance

Annesha Nag

Student (Pursuing LLM.)

Haldia Law College (Vidyasagar University)

Abstract:

In today's digital ecosystem, cyber law plays a crucial role in regulating cyberspace, protecting data, preventing cybercrimes, and upholding constitutional rights. With India's technological transformation, the rise of AI, and the exponential increase in digital dependency, cyber threats have also grown multifold. This paper examines the scope of cyber law in India in 2025, analyzes the effectiveness of existing legal frameworks like the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, and discusses challenges in enforcement, jurisdiction, and technological adaptation. The paper also highlights key case laws, global comparisons, and recommends legal reforms to make India's cyber legal infrastructure more robust, rights-protective, and future-ready.

Keywords: Cyber law, internet, AI, technologies, privacy, cybercrimes.

I. INTRODUCTION

The digital revolution has radically transformed the way individuals, governments, and corporations interact, reshaping every aspect of modern life—from commerce and communication to governance and education. In this interconnected environment, digital platforms have become essential tools for social interaction, economic transactions, and public service delivery. However, this technological advancement has also brought with it a complex set of challenges. The proliferation of cybercrimes, including financial fraud, ransomware attacks, identity theft, and data breaches, poses serious threats to individual privacy, organizational integrity, and national security. The emergence of deepfakes, AI-generated content misuse, and cyberbullying has blurred the line between virtual and real-world harm, undermining trust in online content and increasing vulnerabilities for users, especially women and marginalized communities. These evolving threats highlight the urgent need for a comprehensive, dynamic,

and adaptive legal framework to regulate cyberspace. In this context, cyber law has emerged as an indispensable pillar for ensuring safety, accountability, and justice in the digital age.

India, which is now one of the world's largest digital economies, has witnessed unprecedented growth in internet usage, digital payments, and e-governance initiatives. Programs like Digital India, Aadhaar-based welfare delivery, and Unified Payments Interface (UPI) have revolutionized public access to digital services. Yet, this increasing digital dependency also exposes millions to cyber vulnerabilities, making robust legal safeguards not just necessary but urgent. Despite progressive steps such as the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023, significant gaps remain in India's cyber legal framework. These include insufficient protection against AI-based threats, weak enforcement of privacy rights, jurisdictional challenges in cross-border crimes, and lack of specialized training for cybercrime investigation. Therefore, this paper seeks to explore the current landscape of cyber law in India, critically analyze its strengths and limitations, and suggest reforms to make it responsive to the fast-evolving digital ecosystem of 2025 and beyond.

Brief History and Evolution of Cyber Law

Cyber law, or digital law, has evolved globally alongside the rise of the internet and digital technologies. Initially, in the 1980s and 1990s, legal attention was limited to regulating unauthorized access and computer misuse. As the internet became commercialized in the late 1990s, countries began recognizing the need for legal mechanisms to address cyber fraud, hacking, cyberstalking, and online data theft. In India, the turning point came with the enactment of the Information Technology Act, 2000, which provided legal recognition to electronic records and digital signatures while defining cyber offences. The Act was further strengthened by the 2008 Amendment, which expanded its ambit to include offences like cyber terrorism, identity theft, and introduced intermediary liability for digital platforms. The dynamic nature of the digital world, especially with advancements in AI, blockchain, and big data, has since pushed India to continue updating its legal regime, most notably with the Digital Personal Data Protection Act, 2023.

Importance of Cyber Law in a Digital Society

Cyber law plays a foundational role in safeguarding the rights and interests of individuals and institutions in an increasingly connected digital society. It ensures the protection of personal data, prevents cyberbullying, addresses cybercrime, and maintains national cybersecurity. Additionally, it supports the legal validity of digital contracts, facilitates secure e-commerce, and upholds freedom of expression while regulating hate speech, fake news, and harmful content online. In an era where most services—banking, healthcare, education, and governance—are digitized, cyber law provides the regulatory framework to protect users, promote responsible digital behaviour, and enable technological innovation within lawful boundaries.

India's Increasing Digital Dependency

India's rapid digitization has been driven by visionary initiatives like Digital India, launched in 2015 to enhance digital infrastructure, deliver services electronically, and increase digital literacy. This has led to the widespread adoption of e-governance platforms such as DigiLocker, UMANG, and eCourts. The growth of Unified Payments Interface (UPI) has revolutionized the financial sector, making India a global leader in digital transactions. Programs like Aadhaar have enabled large-scale biometric identity integration, streamlining public welfare schemes and services[1]. The country's rising dependence on artificial intelligence, big data analytics, and cloud computing across sectors has made it imperative to have strong cyber laws that protect users from cyber threats, ensure data privacy, and regulate the ethical use of emerging technologies. As India continues to embrace digital transformation, cyber law stands as a critical pillar ensuring digital trust, security, and accountability.

II. CURRENT SCENARIO AND KEY CONCERNS

Cybercrime Surge in 2024–2025: Phishing, Ransomware, Identity Theft

The years 2024[2] and 2025 have witnessed a steep rise in cybercrime incidents across India and the globe, highlighting serious gaps in digital safety and enforcement. Phishing attacks—where attackers deceive users into revealing sensitive information—have become more sophisticated with the use of cloned websites, fake payment portals, and deceptive emails mimicking government schemes or banking services. Ransomware has emerged as a particularly damaging threat, where cybercriminals encrypt victims' data and demand payment in cryptocurrency to restore access. Even major hospitals, universities, and municipal corporations have reported being crippled by such attacks. Additionally, identity theft has surged, with fraudsters using stolen Aadhaar numbers, mobile SIMs, or leaked personal data to commit financial fraud or impersonate users. The common citizen, small businesses, and even senior citizens are increasingly becoming vulnerable targets in this growing digital crime wave.

AI-Driven Threats: Deepfakes, Voice Cloning, and Algorithmic Manipulation

The misuse of artificial intelligence (AI) has introduced an entirely new dimension to cyber threats in 2025. One of the most dangerous developments is the spread of deepfakes—hyper-realistic AI-generated videos and images that can falsely portray individuals in compromising or misleading situations. These have been weaponized for character assassination, political propaganda, and cyber extortion. Similarly, AI-based voice cloning has enabled fraudsters to impersonate relatives, government officials, or corporate managers to trick people into transferring money or sharing confidential information. Moreover, algorithmic manipulation on social media platforms has raised concerns about targeted misinformation, emotional manipulation, and electoral interference, especially when bots

[1] Ministry of Electronics and Information Technology, *Digital India Programme*, available at https://www.digitalindia.gov.in/ (last visited June 24, 2025).
[2] Unique Identification Authority of India (UIDAI), *Aadhaar Dashboard*, available at https://uidai.gov.in/ (last visited June 24, 2025).

and AI are used to sway public opinion or suppress dissent. These AI-driven threats are largely unregulated under existing cyber law, making enforcement extremely challenging.

Data Breaches and Institutional Failures: Case Studies from 2025

Large-scale data breaches continue to plague both public and private institutions in India. A recent 2025 case involved an alleged breach of the Aadhaar database, exposing the personal data of millions, including biometric information and financial details. This has not only raised concerns about the effectiveness of government data protection mechanisms but has also undermined public trust in digital governance.[3] Similarly, global tech giants like Meta (Facebook) and Google reported significant data leaks involving users' browsing history, location data, and ad interactions, which were allegedly sold to third-party advertisers or leaked on the dark web[4]. These breaches underline the vulnerability of centralized databases and the urgent need for stronger encryption, audit trails, and accountability frameworks. Despite the enactment of the Digital Personal Data Protection Act, 2023, enforcement mechanisms and public awareness remain weak, contributing to the scale and frequency of such incidents.

Dark Web and Cryptocurrency Frauds

The dark web, an encrypted part of the internet inaccessible to standard browsers, has become a thriving marketplace for illegal goods, stolen data, and malicious software. It is also central to many cryptocurrency-related frauds, where users are lured into fake investment schemes or scammed through pump-and-dump crypto tokens. The anonymity offered by cryptocurrencies like Bitcoin and Monero makes it difficult for law enforcement agencies to trace financial transactions, especially in extortion or drug trafficking cases. While India has taken a cautious approach by taxing crypto assets and requiring KYC compliance for exchanges, there is no comprehensive regulatory framework to monitor the misuse of blockchain technology for illegal purposes. This grey zone continues to allow cybercriminals to exploit legal loopholes and evade prosecution.

Cybersecurity in National Defense: CERT-In and Digital Warfare Risks

The increasing digitization of defense, infrastructure, and intelligence systems has made India vulnerable to cyber warfare and state-sponsored attacks. The Indian Computer Emergency Response Team (CERT-In) plays a crucial role in monitoring cybersecurity incidents, issuing advisories, and coordinating incident responses[5]. However, the growing sophistication of cyber-attacks targeting power grids, financial institutions, and even satellite systems suggests that current capabilities are not always sufficient. Recent cyber intrusions suspected to be backed by foreign states have underscored the need for a more integrated national cybersecurity strategy, better coordination among military and civilian agencies, and the establishment of a dedicated Cyber Command within the armed

[3] "Aadhaar Data Breach Exposes Biometric and Financial Information of Millions," *The Hindu* (May 2025), available at https://www.thehindu.com/news/national/aadhaar-breach-2025 (last visited June 24, 2025).
[4] Rahul Matthan, "Data Protection in India: Institutional Gaps and Legal Challenges," *The Indian Journal of Law and Technology*, Vol. 21, 2025, p. 45.
[5] Indian Computer Emergency Response Team (CERT-In), *Functions and Responsibilities*, Ministry of Electronics and Information Technology, available at https://www.cert-in.org.in/ (last visited June 24, 2025).

forces. The threat landscape has shifted from individual hackers to well-funded digital warfare units, and India's legal and technical infrastructure must evolve accordingly to ensure national security in cyberspace.

III. LEGAL FRAMEWORK IN INDIA

A. Information Technology Act, 2000[6] (with amendments)

The Information Technology Act, 2000 (commonly known as the IT Act) is the cornerstone of cyber law in India. Enacted to provide legal recognition to electronic commerce and digital communications, the Act was a timely legislative response to the increasing use of information technology in governance, business, and personal transactions. It marked India's first attempt to formally recognize digital documents, digital signatures, and online contracts, giving them the same legal status as their physical counterparts. This move was critical for the growth of e-commerce and digital business models in India, especially in the early 2000s. The IT Act also provided a basic legal framework to regulate cybercrimes and offenses committed in cyberspace, laying down penalties for hacking, data theft, and tampering with computer systems.

Recognition of Digital Evidence and Offenses

One of the major achievements of the IT Act was the formal recognition of electronic records and digital signatures under Sections 3[7] and 4[8]. This allowed digital contracts and communications to be admissible as evidence in courts, streamlining e-governance and business operations. However, with the expansion of the internet and growing concerns over cybercrime, it became evident that the original legislation lacked sufficient provisions to deal with emerging threats such as identity theft, cyberstalking, online fraud, and digital obscenity. This led to the amendment of the IT Act in 2008, which significantly broadened the scope of the law.

Key Penal Provisions under the IT Act

The 2008 amendment introduced several new sections to deal with specific cyber offenses. Section 66C deals with identity theft, punishing anyone who fraudulently or dishonestly uses another person's electronic signature, password, or other unique identification features. Section 66D criminalizes cheating by personation using a computer resource, which is particularly relevant in cases involving online financial scams, phishing, and fake profiles. These provisions have become increasingly important in the wake of rising online fraud incidents in India.

Section 67 addresses the publishing or transmission of obscene material in electronic form, including child pornography and sexually explicit content. This section plays a crucial role in regulating adult content and protecting minors online, although its implementation has faced criticism for sometimes infringing upon artistic freedom and privacy rights. Meanwhile, Section 69A empowers the government to block public access to any

[6] The Information Technology Act, 2000, Act No. 21 of 2000, Gazette of India, Extraordinary, Part II, sec. 1 (9 June 2000), available at https://legislative.gov.in/sites/default/files/A2000-21.pdf (last visited June 24, 2025).
[7] The Information Technology Act, 2000, s. 3, Act No. 21 of 2000, available at https://legislative.gov.in/sites/default/files/A2000-21.pdf (last visited June 24, 2025).
[8] *Ibid*, sec.4

information through any computer resource in the interest of sovereignty, public order, or national security. This section has gained prominence in recent years, especially with the banning of certain mobile applications and websites deemed harmful to national interests.

Criticism and Contemporary Relevance

While the IT Act has undoubtedly laid the groundwork for cyber regulation in India, it has also attracted criticism for being outdated in addressing modern technological threats, such as AI-generated deepfakes, sophisticated cyber espionage, and mass surveillance. The Act lacks clarity on issues like data portability, algorithmic accountability, and the legal status of emerging technologies like blockchain. Moreover, the broad powers given under Section 69A have raised concerns about censorship and the lack of transparency, as website blocking orders are not always made public. Despite these shortcomings, the IT Act remains a vital piece of legislation and continues to be the primary legal tool for handling cybercrimes, even as India considers new laws on cybersecurity and digital governance.

B. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023, marks a significant milestone in India's journey toward building a comprehensive legal framework for data privacy and protection. Passed in response to the Supreme Court's landmark judgment in *Justice K.S. Puttaswamy* v. *Union of India*[9] (2017), which affirmed the right to privacy as a fundamental right, the DPDP Act was introduced to regulate the collection, storage, and processing of personal data by both private entities and government institutions. It aims to empower individuals (referred to as "data principals") with control over their personal information while obligating entities (referred to as "data fiduciaries") to follow principles of transparency, accountability, purpose limitation, and data minimization. The Act applies to data collected within the territory of India and to processing outside India if it involves offering goods or services to Indian residents.

Key Features and Regulatory Mechanism

One of the central features of the DPDP Act is the creation of an independent regulatory body known as the Data Protection Board of India. This quasi-judicial authority is responsible for receiving complaints, conducting inquiries, imposing penalties for non-compliance, and guiding the implementation of data protection norms. The Act provides individuals with several rights, including the right to access their personal data, the right to correction and erasure, and the right to grievance redressal. At the same time, it obliges data fiduciaries to obtain informed consent before processing personal data and to implement reasonable security safeguards to prevent data breaches[10].

[9] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

[10] The Digital Personal Data Protection Act, 2023, s. 6–7, Act No. 22 of 2023, available at https://egazette.nic.in/ (last visited June 24, 2025).

Criticism and Limitations

Despite its positive intent, the DPDP Act, 2023, has attracted significant criticism for its limited scope and sweeping exemptions, especially under Section 17, which grants the central government powers to exempt any of its agencies from the provisions of the Act in the interest of national security, public order, or friendly relations with foreign states. Critics argue that such a clause may lead to unchecked state surveillance, thereby undermining the very privacy rights the Act seeks to protect. Furthermore, the Act does not provide sufficient clarity on data localization, algorithmic accountability, or the processing of non-personal or anonymized data, leaving substantial gaps in India's data governance ecosystem. The absence of a strong provision for independent oversight and limited parliamentary scrutiny over executive actions have also raised concerns among civil society and legal experts.

IV. COMPARATIVE PERSPECTIVE

Comparative Perspective: United States and European Union

The United States follows a sector-specific approach to data protection, where different laws apply to different industries rather than having a single comprehensive federal privacy law.[11] For example, the Health Insurance Portability and Accountability Act (HIPAA) governs the privacy of medical records, while the Children's Online Privacy Protection Act (COPPA) protects the online data of children.[12] More recently, the California Consumer Privacy Act (CCPA) has emerged as one of the most influential state-level legislations, granting consumers rights to know, access, delete, and opt out of the sale of their personal data. Several other states, such as Virginia and Colorado, have also enacted their own privacy laws.[13] While the U.S. legal system provides strong civil remedies for data breaches and misuse, it currently lacks a unified federal data protection law, which has led to inconsistencies in enforcement and protection across states. This fragmented approach poses challenges, especially when dealing with cross-border data flows and international compliance.

In contrast, the European Union has adopted a more cohesive and rights-based approach with the implementation of the General Data Protection Regulation[14] (GDPR) in 2018. The GDPR is widely regarded as the global benchmark for data protection, offering comprehensive rights to individuals—such as the right to access, correct, delete, and port personal data—while imposing strict obligations on data controllers and processors. It emphasizes privacy by design, requires clear consent for data processing, and mandates timely breach notifications. The regulation has extraterritorial application, meaning that companies handling EU citizens' data must comply regardless of where they are based. Building on the GDPR, the European Union is now in the process of enacting the Artificial Intelligence Act, which is set to become the world's first legal framework regulating AI systems. This

[11] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (USA).
[12] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.
[13] California Privacy Rights Act (CPRA), Ballot Initiative Proposition 24 (2020), amending the CCPA.
[14] European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88.

proposed legislation takes a risk-based approach, classifying AI applications into categories such as prohibited, high-risk, and low-risk, with strict compliance obligations for high-risk systems. Together, the GDPR and the upcoming AI Act reflect the EU's commitment to safeguarding digital rights and regulating emerging technologies with a strong ethical and legal foundation.

V. Key Case Laws

1. *Justice K.S. Puttaswamy* v. *Union of India*[15] (2017)

In this landmark judgment, the Supreme Court unanimously declared the right to privacy as a fundamental right under Article 21 of the Constitution. The case arose from challenges to the Aadhaar scheme, with concerns over data collection and surveillance. The Court held that privacy is intrinsic to life and liberty, including informational autonomy. This decision laid the foundation for privacy rights in India's digital age and influenced later data protection laws and Aadhaar-related rulings.

2. *Shreya Singhal* v. *Union of India* (2015)

In *Shreya Singhal* v. *Union of India*[16], (, the Supreme Court struck down Section 66A of the Information Technology Act, 2000, declaring it unconstitutional for violating Article 19(1)(a) — the right to freedom of speech and expression. The Court held that the provision was vague and overbroad, creating a chilling effect on free speech due to fear of arbitrary arrest for online content. This landmark ruling emphasized the need for legal clarity and proportionality in regulating digital expression, setting a vital precedent for internet freedom in India.

3. *Anivar Aravind* v. *Union of India* (2021)

In *Anivar Aravind* v. *Union of India*[17], the petitioner challenged the CERT-In directions mandating mandatory breach reporting, extended data retention by service providers, and time synchronization requirements. The case raised concerns over privacy, due process, and lack of transparency in cybersecurity enforcement. The petitioner argued that the directives were issued without adequate consultation or legal safeguards, potentially infringing upon user rights. The case brought attention to the urgent need for procedural fairness, accountability, and oversight mechanisms in India's cybersecurity regime.

4. *Google India Pvt. Ltd*. v. *Visaka Industries* (2020)

In *Google India Pvt. Ltd*. v. *Visaka Industries Ltd*.[18], the Supreme Court addressed the scope of intermediary liability under the Information Technology Act, 2000, specifically interpreting Section 79, which grants conditional immunity to intermediaries like Google. The case arose when defamatory content was posted on a blogging platform, and the company was sued for not removing it. The Court held that while intermediaries are not primarily

[15] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[16] (2015) 5 SCC 1
[17] WP(C) No. 12223/2021 (Kerala High Court)
[18] (2020) SCC OnLine SC 1046

liable for third-party content, they are obliged to act with due diligence and must remove unlawful material upon receiving actual knowledge or being notified by a competent authority. This ruling reinforced the responsibilities of digital platforms to balance freedom of expression with accountability, and affirmed that immunity under Section 79 is not absolute, but contingent on prompt compliance and responsible conduct.

VI. RECOMMENDATIONS

1. Enact a Comprehensive Cybersecurity Law

Explanation:
India currently lacks a single, unified law that comprehensively governs cybersecurity. A robust cybersecurity law should:

- Address emerging technologies like Artificial Intelligence (AI), machine learning, and blockchain.
- Lay out frameworks for handling digital evidence and cyberforensics, crucial for investigating and prosecuting cybercrimes.
- Provide a legal mechanism to respond to ransomware attacks, data breaches, and malware threats.
- Outline a national cybersecurity strategy, detailing roles of government, private sector, and individuals in preventing cyber threats.
- Ensure data protection, incident response procedures, and cyber audit requirements for critical sectors like banking, defense, and healthcare.

A comprehensive law would not only consolidate existing fragmented rules (like the IT Act, 2000 and its amendments) but also respond to evolving cyber risks in a dynamic digital environment.

2. Judicial and Police Training

Cybercrimes are technical in nature and often involve digital evidence, encryption, anonymity tools (like VPNs), and cross-border complexities. Many law enforcement and judicial officers lack adequate training to handle such cases effectively.

Recommendations include:

- Establishing specialized cybercrime courts for speedy and informed adjudication.
- Providing technical and legal training to police officers, prosecutors, and judges in cyber law, digital forensics, and handling electronic evidence.
- Setting up cyber police stations and forensic labs at the district level.

Such training will ensure informed investigations and reduce wrongful prosecutions, improving public trust in cybercrime enforcement.

3. Strengthen Intermediary Guidelines (2021 Rules)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 were introduced to regulate digital intermediaries like social media platforms, messaging services, and online publishers.

However, the guidelines must:

- Strike a balance between platform accountability and freedom of speech.
- Ensure clearer responsibilities for content takedown, grievance redressal, and due diligence by intermediaries.
- Avoid over-regulation that could hinder innovation, especially for startups and Indian tech companies.

Strengthening and clarifying these rules—while respecting constitutional rights—will foster a safer digital space without compromising democratic values.

4. Public Awareness Campaigns

Explanation:
Cybersecurity is not just a technical or legal issue; it requires mass awareness. Citizens often fall prey to online fraud, phishing, cyberbullying, and misinformation due to lack of knowledge.

Public campaigns should focus on:

- Digital literacy: Educating people about safe internet practices, password hygiene, and reporting mechanisms.
- Rights-based education: Making citizens aware of their legal rights and remedies under cyber law, such as filing cyber complaints, protecting online privacy, and understanding terms of service.
- Special focus should be on vulnerable groups like children, women, and the elderly who are more susceptible to online threats.

5. International Treaty Participation

Explanation:
Cybercrime is a global challenge. Hackers and cybercriminals operate across borders, making international cooperation essential.

India must:

- Join and actively participate in international agreements like the Budapest Convention on Cybercrime or ongoing UN treaty negotiations.
- Form bilateral and multilateral alliances for sharing cyber threat intelligence, mutual legal assistance, and harmonizing cyber laws.
- Engage in global policy discussions to shape norms around cyber warfare, espionage, data protection, and cross-border digital trade.

Active participation in international treaties helps India enhance its cyber diplomacy, improve global cooperation, and protect its citizens and digital infrastructure from transnational cyber threats.

VII. CONCLUSION

As we move through 2025, cyber law stands at a critical crossroads, confronting challenges that are more complex and multifaceted than ever before. The rapid evolution of technologies like artificial intelligence (AI), machine learning, blockchain, and quantum computing, coupled with the unchecked spread of data monetization and cross-border digital transactions, has created an intricate legal landscape. Cybercrimes are no longer limited to traditional forms like hacking or phishing but now include AI-generated misinformation, algorithmic bias, surveillance capitalism, and deepfake-based extortion. In this dynamic environment, the protection of digital rights, individual privacy, and national cybersecurity requires much more than piecemeal legislation.

India has made commendable progress with instruments like the Information Technology Act, 2000 (as amended) and the Digital Personal Data Protection Act, 2023. However, enforcement remains uneven, and gaps persist in areas like state surveillance oversight, AI regulation, and dark web crimes. As the global digital economy continues to expand, cyber law must evolve beyond reactive regulation to a forward-looking, rights-based, and tech-informed framework. This demands not only robust policymaking and legislative clarity but also investment in technical expertise, judicial training, and cybercrime infrastructure.

In today's borderless digital ecosystem, where cyber threats transcend national boundaries and digital economies are globally interdependent, international cooperation is no longer a matter of choice—it is an imperative. The complex and evolving nature of cybercrimes, from ransomware and data breaches to misinformation and state-sponsored attacks, demands collaborative legal and technological responses. Harmonizing cybersecurity standards, sharing threat intelligence, enabling cross-jurisdictional investigations, and aligning privacy norms are essential components of a global cyber governance strategy.

India, as a rapidly digitizing economy and an emerging digital power, must take a leadership role in shaping this international dialogue. This includes actively participating in global treaties, forging bilateral and multilateral agreements, and fostering partnerships between governments, technology companies, and civil society organizations. Domestically, laws like the Information Technology Act, 2000, and the Digital Personal Data

Protection Act, 2023, must be continually updated to reflect global best practices while safeguarding national interests.

Ultimately, India's digital sovereignty, economic resilience, and the protection of constitutional freedoms—including the right to privacy, freedom of expression, and access to information—can only be secured through the development of a holistic, inclusive, and globally-aware legal ecosystem. The future of cyber governance lies not in isolation, but in collaborative innovation, legal harmonization, and shared responsibility across borders.

REFERENCES

- "Aadhaar Data Breach Exposes Biometric and Financial Information of Millions," *The Hindu* (May 2025), available at https://www.thehindu.com/news/national/aadhaar-breach-2025 (last visited June 24, 2025).
- Anivar Aravind v. Union of India, WP(C) 12223/2021 (Kerala HC).
- California Privacy Rights Act (CPRA), Ballot Initiative Proposition 24 (2020), amending the CCPA.
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.
- Digital Personal Data Protection Act, 2023 (India).
- European Commission. (2024). Artificial Intelligence Act.
- European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88.
- Google India Pvt. Ltd. v. Visaka Industries, (2020) SCC Online Del 2532.
- Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (USA).
- Indian Computer Emergency Response Team (CERT-In), *Functions and Responsibilities*, Ministry of Electronics and Information Technology, available at https://www.cert-in.org.in/ (last visited June 24, 2025).
- Information Technology Act, 2000 (India).
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Ministry of Electronics & IT, Government of India. (2023). CERT-In Guidelines.
- Ministry of Electronics and Information Technology, *Digital India Programme*, available at https://www.digitalindia.gov.in/ (last visited June 24, 2025).
- Puttaswamy v. Union of India, (2017) 10 SCC 1.
- Rahul Matthan, "Data Protection in India: Institutional Gaps and Legal Challenges," *The Indian Journal of Law and Technology*, Vol. 21, 2025, p. 45.
- Shreya Singhal v. Union of India, AIR 2015 SC 1523.
- Singh, A. (2024). *Cybersecurity Laws and AI Risks: An Indian Perspective*. Indian Law Review, 12(2), 89–103.

- The Digital Personal Data Protection Act, 2023, s. 6–7, Act No. 22 of 2023, available at https://egazette.nic.in/ (last visited June 24, 2025).
- The Information Technology Act, 2000, Act No. 21 of 2000, Gazette of India, Extraordinary, Part II, sec. 1 (9 June 2000), available at https://legislative.gov.in/sites/default/files/A2000-21.pdf (last visited June 24, 2025).
- The Information Technology Act, 2000, s. 3, Act No. 21 of 2000, available at https://legislative.gov.in/sites/default/files/A2000-21.pdf (last visited June 24, 2025).
- Unique Identification Authority of India (UIDAI), *Aadhaar Dashboard*, available at https://uidai.gov.in/ (last visited June 24, 2025).
- WP(C) No. 12223/2021 (Kerala High Court)