The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

LEGAL ASPECTS OF CYBER SECURITY IN INDIA

George N. Taylor

ABSTRACT

Cyber security has emerged as one of the most critical public policy and legal issues in India.

As digital technologies permeate every aspect of governance, business, and social interaction, the Indian legal system has evolved to address cyber threats, data protection, privacy, and cybercrimes. This paper examines the legal architecture governing cyber security in India, including the *Information Technology Act, 2000*[1] (with its amendments), the Digital Personal Data Protection Act, 2023, subordinate rules, ancillary statutes, enforcement mechanisms, jurisdictional challenges, judicial interpretations, regulatory complexities, and areas for future reform. The analysis highlights strengths, gaps, and the dynamic interplay between security needs and fundamental rights. The rapid expansion of digital technologies and internet-based services in India has significantly transformed governance, commerce, communication and social interaction. Alongside these developments, the country has witnessed a sharp rise in cyber threats such as data breaches, on online fraud, identity theft, cyber stalking and cyber terrorism. This evolving threat landscape highlights the growing importance of a robust legal framework to ensure cyber security and protect digital rights. This research paper examines the legal aspects of cyber security in India by analysing the existing statutory framework, regulatory mechanisms and institutional responses aimed at preventing and addressing cybercrimes. The study primarily focuses on the *Information Technology Act, 2000* and its subsequent amendments along with allied rules and regulations governing data protection, intermediary liability and cyber incident reporting. It also discusses the relevance of the *Digital Personal Data Protection Act, 2023*[2] in strengthening privacy rights and accountability in the digital ecosystem. The paper further evaluates the role of enforcement

[1] Information Technology Act, 2000 (Act No. 21 of 2000)

[2] Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)

agencies such as CERT-In, cybercrime cells and the judiciary in implementing cyber law and ensuring compliance. Key judicial pronouncements are reviewed to understand the interpretation and application of cyber laws in India. Additionally, the research highlights emerging challenges including jurisdictional issues, technological advancements, lack of awareness and enforcement gaps. The paper adopts a doctrinal and analytical research methodology based on statutory provisions, case laws, reports and secondary sources. It concludes by emphasizing the need for continuous legal reforms, capacity building and public awareness to develop an effective cyber security regime. Strengthening India's legal framework is essential to balance technological growth with the protection of individual rights, national security and digital trust.

KEYWORDS

Cyber Security, Cyber Crime, Information Security, Digital India, Cyber Law in India.

INTRODUCTION

Cyber security refers to the protection of information systems, networks, electronic data, and digital processes from unauthorized access, misuse, damage, or disruption. In India's rapidly digitizing economy, with widespread use of e-governance, digital payments, and internet services, cyber security is imperative not only for economic development but also for national security, individual privacy, and societal stability. The evolution of cyber law in India has attempted to balance technological innovation with legal safeguards against misuse such as cybercrimes, data breaches, identity theft, and cyber terrorism.

This research paper explores *legal aspects* of cyber security in India, examining legislation, subordinate rules, institutional frameworks, enforcement mechanisms, key case law, and contemporary challenges.

HISTORICAL OVERVIEW OF CYBER LAW IN INDIA

Prior to the 2000s, Indian legal frameworks lacked specific provisions for digital or cyber activities. Traditional statutes like the *Indian Penal Code (IPC) 1860*[3] and the *Indian Evidence Act 1872*[4] were applied by analogy to cases involving computers and electronic evidence; a practice fraught with ambiguity and inconsistent outcomes.

Enactment of the Information Technology Act, 2000

[3] Indian Penal Code, 1860 (Act No. 45 of 1860)
[4] Indian Evidence Act, 1872 (Act No. 1 of 1872)

The *Information Technology Act, 2000* (*IT Act*) was India's first comprehensive cyber law, enacted to give legal recognition to electronic records, digital signatures, and to criminalize cyber offences. It was influenced by the *United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce*[5] and aimed to bridge the regulatory gap created by digital transformation.

Subsequent amendments, notably in 2008 through the *Information Technology (Amendment) Act, 2008*, modernized the law by expanding offense categories and reinforcing regulatory controls on digital authentication.

RESEARCH METHODOLOGY

This research adopts a doctrinal and analytical methodology to examine the legal framework governing cyber security in India. The aim is to critically evaluate existing laws, regulations, judicial interpretations and institutional mechanism that address cyber security concerns, identify gaps and propose recommendations for strengthening legal responses. This methodology comprises several stages described as followed:

RESEARCH DESIGN

This study follows a qualitative, descriptive and analytical research design. It focuses on understanding the legal principles, provision and judicial decisions related to cyber security, rather than quantities measurement or empirical data collection from surveys or experiments.

SOURCES OF DATA

The research relies on secondary legal sources, which include:

Statutory provisions like the *Information Technology Act, 2000 (IT Act)* and its amendments, the *Digital Personal Data Protection Act, 2023* as well as Rules, notifications and subordinate legislation under cyber laws

These statutory sources are analysed to determine the scope, definitions, penalties, powers of authorities and procedural frameworks relevant to cyber security and cybercrime.

JUDICIAL PRONOUNCEMENTS

[5] UNCITRAL Model Law on Electronic Commerce, 1996 (36 I.L.M 197 (1997)

Selected case laws from Supreme Court and High Courts addressing cybercrime, data protection, policy violations interception powers, jurisdictional issues and constitutional rights in digital context.

REPORTS AND POLICY DOCUMENTS:

Reporting cybercrimes often happens through platforms like; the National Cyber Security Policy (2013), Reports by Indian Computer Emergency Response Team (ERT-In)

COMPARATIVE LEGAL STUDY

A comparative perspective is integrated by briefly referencing cyber security and data protection laws in other jurisdictions (such as the EU GDPR framework) to highlight comparative strengths and weaknesses.

LIMITATIONS

a. The study does not involve primary interviews or empirical surveys, since it focuses on doctrinal legal analysis.

b. Rapid technological changes may out pace legal developments, making some interpretations provisional.

OUTCOME

The methodology enables a comprehensive understanding of legal structures, enforcement mechanisms, judicial interpretations and practical challenges in implementing cyber security law in India, thereby laying the foundation for informed recommendations and future legal reforms.

LITERATURE REVIEW

Information Technology Act, (IT Act) 2000, The foundational statute governing cyberspace in India, providing legal recognition to electronic records, digital signatures, and defining cyber offences such as hacking, data theft, and publishing obscene content online.

SUPPLEMENTARY RULES AND POLICIES

IT Rules (e.g., 2021 Intermediary Guidelines) provide procedures for intermediaries and content moderation, though they raise privacy and free speech concerns. CERT-In Rules & Policies, Indian Computer Emergency Response Team guidelines shape incident reporting

and response expectations. National Cyber Security Policy, 2013, outlines strategic objectives for national cyber resilience.

EMERGING DATA PROTECTION LAW

Digital Personal Data Protection Act, 2023 (DPDP Act), influences cyber security by setting data processing and protection norms, although its interaction with cyber incident obligations is still an active scholarly focus. The cyber security legal framework in India is described as *complex and evolving*, driven by rapid digital adoption but facing fragmentation across statutes and rules. Scholars highlight that although multiple instruments exist, their coherence and enforcement alignment remain issues.

CRITICAL EVALUATIONS OF THE IT ACT & CHALLENGES

Several studies argue that the IT Act, last substantively amended in 2008, is out dated—struggling to address *emerging technologies* like AI, IoT, and advanced cyber threats, which were not anticipated when the Act was drafted.

GAPS IN ADDRESSING NEW CHALLENGES

The literature points out that current definitions and offence categories inadequately capture *AI-related cyber incidents* and evolving threat vectors, suggesting a need for expanded legal definitions and reporting frameworks.

FRAGMENTATION AND OVERLAPS

Hussainara Khatoon & Ors vs. Home Secretary, State of Bihar[6]

The presence of multiple regulations and *overlapping rules* across sectors (IT, telecom, finance) complicates compliance and enforcement for both public and private sector entities.

Judicial Interpretation and Case Law

Balancing Rights and Regulations

Judicial decisions have played a crucial role in shaping the cyber legal regime. A notable example is the *Shreya Singhal v. Union of India*[7] verdict, where the Supreme Court struck down Section 66A of the IT Act for violating free speech, significantly influencing how digital expression and cyber security enforcement coexist.

[6] Hussainara Khatoon and Ors. vs. Home Secretary, State of Bihar, 1979 AIR 3169
[7] Shreya Singhal v. Union of India (on 24 March, 2015

Cybercrime Jurisdiction and Enforcement

High courts have clarified procedural aspects—such as local police having authority to investigate cyber offences, strengthening law enforcement reach within the existing statutory framework.

Socio-Legal Perspectives on Cybercrime and Security

Studies taking a socio-legal lens emphasize the *social consequences* of cybercrime (e.g., privacy violations, identity theft) and critique how legal provisions affect individual rights and societal trust in digital services.

PROTECTION OF PRIVACY AND DATA

The intersection between cyber security and privacy law is a frequent theme, especially in light of the *right to privacy* becoming a constitutional right in India. Literature critiques whether existing statutes sufficiently protect privacy without stifling cyber security enforcement.

POLICY AND COMPLIANCE PERSPECTIVES

Articles on implementing cyber security policies underscore that effective legal compliance involves not just understanding legislation, but also practical integration of cybersecurity standards and incident reporting obligations.

NEED FOR CLEAR REGULATORY STANDARDS

Research calls for standardized guidelines to help organizations navigate overlapping rules (e.g., IT Act provisions, RBI cyber security directions for financial firms) and to clarify responsibilities for breach reporting and data protection.

FUTURE DIRECTIONS IN LEGAL AND ACADEMIC RESEARCH

A common recommendation in the literature is *modernizing the IT Act* and introducing more targeted laws covering areas such as AI-driven threats, cyber insurance, and cross-border data flows.

INCIDENT REPORTING & ENFORCEMENT MECHANISMS

There’s academic advocacy for robust incident reporting frameworks that balance transparency with legal safeguards for cyber security researchers and ethical hackers. This

includes calls for safe harbour provisions to encourage vulnerability disclosure without penalizing good-faith actors.

LEGAL FRAMEWORK GOVERNING CYBER SECURITY IN INDIA AND RECOGNITION OF ELECTRONIC RECORDS AND SIGNATURES

The IT Act remains the primary statutory framework defining cyber security and cybercrime offences in India. It establishes legal recognition for electronic transactions, authentication mechanisms, and punitive sanctions for unauthorized or malicious activities. Section 4 of the IT Act ensures that electronic records have legal validity and enforceability equivalent to paper documents. Section 5 grants legal status to digital signatures, facilitating secure electronic transactions. These provisions are foundational to the legality of e-commerce, digital governance, and contractual obligations carried out online.

INTERMEDIARY LIABILITY (SAFE HARBOUR)

Section 79 of the IT Act provides conditional immunity to intermediaries, such as ISPs, hosting platforms and social media networks, if they: did not initiate the transmission, do not modify content, exercise due diligence, and remove unlawful content upon receiving actual knowledge. This framework seeks to balance freedom of expression and corporate responsibility for content moderation.

INSTITUTIONAL PROVISIONS: CERT-IN AND CCA

Sections 70, 70A, and 70B empower the government to protect critical information infrastructure and designate agencies like Indian Computer Emergency Response Team (CERT-In) to respond to cyber incidents. The CERT-IN Cyber Incident Reporting Guidelines were introduced to ensure that organizations report cybersecurity incidents in a timely and structured manner. These guidelines are part of a broader regulatory framework aimed at improving the overall cybersecurity posture of the country. The guidelines mandate that certain types of incidents must be reported to CERT-IN within a specified timeframe, enabling the agency to take appropriate action and mitigate the impact of the incident CERT-In's role includes incident monitoring, warning dissemination, and coordination among stakeholders[8]. The Act also created the Controller of Certifying Authorities (CCA) to regulate digital signature providers.

[8] CERT-IN Cyber Incident Reporting Guidelines: A Complete Guide, November 8, 2024 https://www.securityium.com/cert-in-cyber-incident-reporting-guidelines-a-complete-guide/

DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The *Digital Personal Data Protection Act, 2023 (DPDP Act)* represents India's first standalone *data protection law*. It provides a statutory regime for processing personal data with emphasis on consent, purpose limitation, data minimization, breach notifications, and statutory remedies for violations.

The DPDP Act also led to the notification of *Digital Personal Data Protection Rules, 2025*[9], detailing operational requirements for compliance by data fiduciaries and data principals.

ANCILLARY LEGISLATION

Other laws interact with cyber security, such as: Indian Penal Code (IPC), 1860 – complements the IT Act for offences like criminal breach of trust, fraud, and cheating involving digital contexts. Indian Evidence Act, 1872 – governs admissibility of electronic evidence. Additionally, sectorial frameworks (e.g., banking cyber security norms by RBI, telecom regulations) align with the IT Act to ensure layered protection across industries.

ENFORCEMENT MECHANISMS AND INSTITUTIONAL ARCHITECTURE

Cybercrime enforcement in India involves: Cyber Crime Police Units at state and national levels, Specialized Cyber Cells within city police jurisdictions, Dedicated Prosecutors trained in cyber law. Recent policy changes have abolished monetary thresholds for registering cybercrime FIRs, making investigative access more uniform and efficient.

CERT-IN INCIDENT REPORTING

CERT-In plays a central role in cyber security operational response. It maintains guidelines for incident reporting by intermediaries and private entities, providing technical coordination during breaches.

ADJUDICATION AND APPEALS

Cases under the IT Act are adjudicated by Tribunals and regular courts, with the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) being the appellate forum for certain disputes. In the case of *Suhas Katti v. State of Tamil Nadu (2004)*[10] which is one of the earliest cybercrime convictions in India, involving an online abuse and defamatory messages

[9] Digital Personal Data Protection Rules, 2025 (G.S.R. I November 14, 2025)
[10] Suhas Katti vs. State of Tamil Nadu (CC No. 4608 of 2004)

sent through digital platforms. The court convicted the accused under the IT Act for publishing obscene content online.

PRIVACY JURISPRUDENCE AND CYBER LAW

The Supreme Court's recognition of the *right to privacy* as a fundamental right in *KS Puttaswamy v. Union of India (2017)*[11] underpins the interpretation of data protection and cyber security laws. The Supreme Court ruled that the Right to Privacy is "intrinsic to life and personal liberty" and is inherently protected under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution. In this way, the Court overruled its own eight-judge bench and six-judge bench judgements for the M.P. Sharma and Kharak Singh cases, respectively[12].

CONTEMPORARY CHALLENGES AND CRITIQUES

The IT Act was last comprehensively amended in 2008. Rapid developments like AI-driven threats, deep fakes, and complex ransom ware attacks strain the applicability of older legal definitions and sanctions. Scholars argue that existing provisions do not adequately address *AI-enabled cyber threats* and lack clear definitions for modern attack vectors, complicating prosecution and risk mitigation.

BALANCING SECURITY AND FUNDAMENTAL RIGHTS

Cyber security measures sometimes intersect with free speech, privacy, and transparency. For instance, exemptions for CERT-In under the Right to Information Act have raised concerns about institutional accountability and transparency.

Effective cyber law enforcement is constrained by limited forensic resources, skills deficits in law enforcement, and low public awareness about safe digital practices.

INFORMATION TECHNOLOGY ACT, 2000 (IT ACT); COMPARATIVE PERSPECTIVES

Comparative studies between India and jurisdictions like the EU's GDPR highlight the need for stronger data protection regimes, explicit breach notification obligations, and stronger enforcement mechanisms. India's DPDP Act draws elements from global standards but also features context-specific compliance frameworks suitable for Indian enterprises. 1.

[11] Justice K.S Puttaswamy v. Union of India (2017) AIR 2017 SC 4161
[12] Right to Privacy, Evolution, Significance, Challenges; Vajiram, December 23, 2025 https://vajiramandravi.com/upsc-exam/right-to-privacy/

Foundation of India's Cybersecurity Legal Framework. The *Information Technology Act, 2000* is the primary statute governing cybercrime and cybersecurity in India. It was amended in *2008* to address emerging cyber issues.

KEY FEATURES

Definition of Cyber Offences: *Hacking* and unauthorized access (Section 66), *Data theft* and damage (Section 43), *Identity theft & fraud* (Sections 66C/D), *Cyberterrorism* (Section 66F) punishable with imprisonment up to 7 years or more. Digital signatures & e-governance: Legitimize electronic records and transactions. Intermediary Liability: Online platforms have a duty to follow due diligence to avoid liability for user content. Extraterritorial Application: If cyber-activities affect Indian systems, the Act applies even to foreign actors.

LIMITATIONS

The Act predates modern threats like AI-driven attacks, ransom ware, and deepfakes. Penalty levels and definitions are sometimes viewed as *out-dated* compared with global standards. Certain offences (e.g., ethical hacking) lack clear legal protection *unless explicitly authorized*.

A more recent statute aimed at personal data protection, consent norms, and breach penalties. The *DPDP Rules, 2025* further detail breach reporting, cross-border transfer safeguards and operational requirements.

COMPARISON WITH IT ACT

IT Act focuses on *offences and penalties* for cybercrimes whereas, the DPDP Act focuses on *privacy, data lifecycle, and fiduciary obligations*. India's law is *not as comprehensive* as the EU's GDPR. For example, independent oversight and stronger enforcement mechanisms are debated among experts.

REGULATORY AND INSTITUTIONAL FRAMEWORK

Indian Computer Emergency Response Team (CERT-In), CERT-In is the nodal agency for cyber incident response and directives (e.g., mandatory breach reporting within six hours, data retention mandates). Regulatory actions include: Cyber incident reporting timelines, guidelines for data storage and log retention and Incident response duties.

CERT-In has been exempted from the RTI Act, raising concerns about accountability and public scrutiny.

SECTORIAL AND SUPPLEMENTARY LAWS

Indian Penal Code / Bhartiya Nyaya Sanhita, complements cyber-offence definitions (e.g., theft). Telecommunications Act, 2023 – consolidates telecom law and affects cybersecurity governance for networks. Sectorial mandates like finance and health also impose cybersecurity obligations under industry-specific regulations.

CONTEMPORARY LEGAL DEBATES IN INDIA

Policy moves like mandatory domain e-KYC to reduce fraud show judicial and regulatory emphasis on accountability — but raise privacy questions.

POLICY REVERSALS AND TRUST

Recent reversal of a mandate to preload a government cybersecurity app highlighted the tension between *state security ambitions* and *privacy concerns*.

Enforcement agencies often face resource and forensic challenges. Cybercrime conviction rates remain low relative to crime volume a common concern in many jurisdictions.

KEY GAPS & FUTURE DIRECTIONS

A dedicated, comprehensive cybersecurity law beyond sector-specific mandates. Clear legal protections for security researchers and responsible disclosure. Stronger privacy safeguards and independent oversight of data and incident reporting authorities. Alignment with global frameworks (e.g., OECD, GDPR, NIST standards) for international interoperability.

CONCLUSION

India's legal framework for cybersecurity is anchored in the IT Act and evolving with laws like the DPDP Act and CERT-In regulations. It offers a *multi-layered legal ecosystem* that balances *cybercrime deterrence* with *data protection*. However, gaps remain particularly regarding *comprehensiveness*, *privacy safeguards*, *AI-era threats*, and *global harmonization* making on-going reform and judicial interpretation critical.

RECOMMENDATIONS FOR REFORM

Comprehensive Cyber security Legislation: India may benefit from an integrated Cyber security Act that consolidates cybercrime, infrastructure protection, data security standards, and incident response protocols into a cohesive statute. AI and Emerging Technologies as well as legal definitions should incorporate contemporary technologies, specifying liability

and forensic standards for AI-related cybercrime. Ethical Hacker Protections wherein legal safeguards for *good-faith vulnerability disclosures* can encourage responsible security research without fear of penal liability. Capacity Building wherein enhanced training for police, prosecutors, and judiciary in technical aspects of cyber law will improve outcomes.

COMPREHENSIVE REVISION OF THE INFORMATION TECHNOLOGY ACT, 2000

The IT Act, 2000, though foundational, has become out dated in addressing modern cyber threats such as artificial intelligence–based attacks, deep fakes, ransom ware, Internet of Things (IoT) vulnerabilities, and block chain misuse. A comprehensive legislative overhaul is required rather than piecemeal amendments. The revised law should: Clearly define emerging cyber offences, introduce technology-neutral and future-proof provisions, strengthen penal consequences for sophisticated cybercrimes, and remove ambiguities in overlapping sections.

HARMONISATION BETWEEN CYBER SECURITY AND DATA PROTECTION LAWS

The coexistence of the IT Act and the Digital Personal Data Protection Act, 2023 has created overlapping compliance obligations. Legal reforms should ensure: Clear demarcation between *data protection violations* and *cyber security offences*, harmonised breach notification timelines and reporting authorities, unified compliance standards to reduce regulatory confusion for organisations, and coordination between the Data Protection Board and cyber security authorities.

STRENGTHENING INSTITUTIONAL FRAMEWORK AND COORDINATION

Multiple agencies such as CERT-In, sectorial regulators, law enforcement agencies, and ministries operate simultaneously, often leading to jurisdictional overlap. Reforms should: Establish a centralized national cyber security coordination authority, clearly define roles of central, state, and sectorial bodies, enable real-time inter-agency information sharing, and introduce statutory backing for coordination mechanisms

ENHANCED CYBERCRIME INVESTIGATION AND CAPACITY BUILDING

Effective enforcement requires skilled investigators and infrastructure. Legal reforms should mandate: Specialized cybercrime courts or dedicated cyber benches, continuous training programs for police, prosecutors, and judiciary, legal recognition of advanced digital forensic

methods, uniform investigation procedures across states, and increased funding for cyber forensic laboratories[13].

CLEAR JURISDICTION AND CROSS-BORDER COOPERATION FRAMEWORK

Cybercrimes often involve cross-border elements, creating enforcement challenges. Reforms should: Clarify territorial jurisdiction for online offences, strengthen mutual legal assistance mechanisms (MLATs), encourage bilateral and multilateral cybercrime treaties, and align Indian law with international standards such as the Budapest Convention principles, while preserving sovereignty.

STRONGER PROTECTION FOR CRITICAL INFORMATION INFRASTRUCTURE (CII)

Critical sectors such as banking, healthcare, energy, telecom, and transport require special legal safeguards. Recommendations include: Sector-specific cyber security obligations backed by penalties, mandatory periodic security audits, legal recognition of cyber resilience standards, and incident response obligations for CII entities with accountability mechanisms.

LEGAL FRAMEWORK FOR ETHICAL HACKING AND VULNERABILITY DISCLOSURE

India lacks a clear statutory safe-harbour mechanism for ethical hackers. Reforms should: Introduce responsible disclosure laws, protect good-faith security researchers from criminal liability, encourage bug bounty programs through legal recognition, and promote collaboration between government and cyber security researchers.

PROTECTION OF FUNDAMENTAL RIGHTS IN CYBER SECURITY ENFORCEMENT

Cyber security measures must respect constitutional values. Legal reform should: Ensure proportionality and necessity in surveillance and interception, provide judicial oversight for data access and monitoring, protect freedom of speech and expression online, and prevent misuse of cyber laws for censorship or harassment.

STRENGTHENING CYBER SECURITY COMPLIANCE AND ACCOUNTABILITY

[13] India's Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations, Kaushik https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations

To ensure effective implementation, the law should: Mandate cyber security audits for organizations handling sensitive data, introduce graded penalties based on severity and negligence, impose liability for failure to implement reasonable security practices, and encourage adoption of international cyber security standards (ISO/IEC).

PUBLIC AWARENESS AND LEGAL LITERACY PROGRAMS

Legal reform must be supported by awareness initiatives. The government should: Promote nationwide cyber law literacy campaigns, educate citizens on cyber rights, duties, and remedies, integrate cyber security law education into academic curricula, support research and innovation in cyber law and digital governance.

INCORPORATING TECHNOLOGY-SPECIFIC REGULATIONS

Future reforms should include specific legal frameworks for: Artificial Intelligence–enabled cyber threats, deepfake regulation and misinformation control, cloud security governance, cloud security governance, block chain and digital asset security, and quantum computing-related risks. This approach would ensure proactive rather than reactive legislation.

REFERENCES

Information Technology Act, 2000 (Act No. 21 of 2000)

Right to Privacy, Evolution, Significance, Challenges; Vajiram, December 23, 2025 https://vajiramandravi.com/upsc-exam/right-to-privacy/

Justice K.S Puttaswamy v. Union of India (2017) AIR 2017 SC 4161

CERT-IN Cyber Incident Reporting Guidelines: A Complete Guide, November 8, 2024 https://www.securityium.com/cert-in-cyber-incident-reporting-guidelines-a-complete-guide/

Digital Personal Data Protection Rules, 2025 (G.S.R. I November 14, 2025)

India’s Cyber Forensics Push Since 2020: Building National Capacity for Digital Investigations, Kaushik https://www.orfonline.org/expert-speak/india-s-cyber-forensics-push-since-2020-building-national-capacity-for-digital-investigations