



## CYBER LAW AND PRIVACY IN INDIA: CHALLENGES AND THE PATH FORWARD

**Yashwant Shailendra Soni\***

### ABSTRACT

*Rapid technological development in the digital age has changed all facets of human interaction, including governance, business, communication, and instruction. But this change has also brought about an unparalleled increase in cybercrime, which calls into question established legal frameworks and necessitates a strong data protection policy. A thorough legal framework is urgently required to address the new problems brought on by the rise in data breaches, cyberattacks, and surveillance concerns. Although groundbreaking when it was first passed, the Information Technology (IT) Act of 2000 has come under fire for failing to adequately address modern problems, including sophisticated cybercrimes, the difficulties presented by artificial intelligence, and the management of cross-border data. These shortcomings are intended to be addressed by the planned Digital Personal Data Protection Act, 2023 (DPDPA), which will replace the previously proposed Personal Data Protection Bill. The new law prioritises responsibility, data minimisation, and individual consent to balance innovation, privacy, and national security. The required cybersecurity reporting guidelines set in place by the Indian Computer Emergency Response Team (CERT-In) and a greater emphasis on data localisation restrictions are two of the current trends covered in the article. It evaluates how the rules will affect all parties involved, such as businesses that are having trouble complying, individuals fighting for their right to privacy, and the government pursuing digital sovereignty. The report also takes into account India's participation in international cybersecurity frameworks and initiatives, which reflects the country's attempts to protect its sovereignty while bringing its laws into compliance with international norms.*

---

\*LLM, SECOND YEAR, MAHATMA GANDHI KASHI VIDYAPEETH.

**Keywords:** Cybersecurity Legislation, Privacy Protection, Digital Personal Data Protection Act 2023, IT Act 2000.

## INTRODUCTION

The digital revolution of the twenty-first century has changed how people, organisations, and governments function. The globe is now more connected than ever thanks to the rapid expansion of digital platforms, artificial intelligence, mobile technology, and internet access. Although these advancements have improved efficiency, creativity, and communication, they have also made it easier for cybercrime to flourish. From isolated hacking instances, cybercrime has developed into a complex, international phenomenon that includes financial fraud, ransomware, phishing, identity theft, data breaches, and cyberstalking. Despite providing unrivalled ease, technology has turned into a double-edged weapon that can be used for both advancement and illegal exploitation.

Initiatives like Digital India, the emergence of fin-tech, and the country's increasing reliance on digital infrastructure have all contributed to India's digital transformation. But this change has also made a significant amount of sensitive and personal data vulnerable. As a result, strong data protection measures ought to be put in place immediately to guarantee citizens' security and privacy.<sup>1</sup>

India's rise as a major global digital force has been marked by the rapid advancement of technology and an unparalleled rise in internet availability. Due to the country's increased susceptibility to cybercrime and privacy violations as a result of its digital transition, comprehensive legal frameworks are now required to address the intricacies of cybersecurity and data protection. The increasing reliance on digital platforms for communication, business, and government emphasises how important it is to maintain individual privacy rights while guaranteeing cybersecurity.

The primary component of legislation governing online transactions and cybercrimes in India is the Information Technology Act, 2000 (IT Act).<sup>2</sup> A comprehensive legal change has been sparked by its shortcomings in responding to sophisticated cyberattacks and changing data privacy concerns. The Digital Personal Data Protection Act, 2023 (DPDPA), which emphasises

---

<sup>1</sup> **India's Digital Infrastructure**, *Insights on India* (Dec. 9, 2024), <https://www.insightsonindia.com/2024/12/09/indias-digital-infrastructure/>.

<sup>2</sup> The Information Technology Act, No. 21 of 2000, India Code (2000)

user permission, data minimisation, and duty attribution, represents a paradigm shift in Indian law.

Recent court decisions highlight how crucial the judiciary is in developing India's privacy and cybersecurity laws. For example, the Supreme Court supported the constitutional right to privacy under Article 21 of the Indian Constitution in Justice K.S. Puttaswamy (Retd.) v Union of India,<sup>3</sup> which made it easier to create more extensive data protection laws. Additionally, the Court supported the need for strict cybersecurity standards in Anvar P.V. v P.K. Basheer.<sup>4</sup> by highlighting the importance of electronic evidence.

Additionally, to further emphasise the government's proactive participation, organisations like the Indian Computer Emergency Response Team (CERT-In) have required businesses to report cybersecurity vulnerabilities within specified time frames. These actions show India's dedication to bringing its digital infrastructure into compliance with global standards, including the General Data Protection Regulation (GDPR) of the European Union. In order to fully evaluate the opportunities and challenges in this area, as cyberattacks progress and public debate over privacy heats up, this paper examines India's legal framework on cybersecurity and privacy, concentrating on case law and recent legislative changes.

## **UNDERSTANDING CYBERSECURITY AND PRIVACY IN THE INDIAN CONTEXT**

Cybersecurity is used to guard against malicious activity, cyberattacks, and unauthorised access to networks, systems, and data. Because of the rapid growth of digital infrastructure, cybersecurity has become more important in India. Sensitive and personal data must be managed securely and ethically due to data privacy concerns. Both are necessary to protect the security and confidence of India's rapidly growing digital economy, especially given the country's efforts to balance user rights, global regulatory norms, and technological innovation.

India's digital progress has coincided with a rise in cyber threats and privacy concerns. A landmark step in codifying the rights and obligations surrounding the processing of personal data is the Digital Personal Data Protection Act (DPDPA), 2023, which builds on the Supreme Court's recognition of the right to privacy as an essential right in Justice K.S. Puttaswamy

---

<sup>3</sup> (2017) 10 SCC 1.

<sup>4</sup> (2014) 10 S.C.C. 473

(Retd.) v. Union of India. However, enforcement and adaptability to evolving threats, such as ransomware, phishing, and cross-border data governance, continue to be lacking.

## CYBERSECURITY IN INDIA'S GROWING DIGITAL ECONOMY

India's economy is becoming more technologically sophisticated in tandem with the support of programs like Digital India and the growth of services like e-commerce, Aadhaar-based governance, and the Unified Payments Interface (UPI). Over 18 million attacks and threats occurred in the first quarter of 2023, highlighting the need for cybersecurity in maintaining consumer confidence, protecting vital infrastructure, and maintaining national security. The 2022 AIIMS ransomware attack revealed weaknesses in public sector networks, highlighted the need for strong cybersecurity policies, and caused weeks-long disruptions to vital health services.<sup>5</sup>

Cybercrimes, including identity theft, have increased in India, according to reports. financial fraud, computer espionage, and theft. The 2018 Cosmos Bank cyberattack revealed weaknesses in financial systems following the deployment of a malware assault to embezzle almost 94 crores. Additionally, phishing attempts continue to be prevalent; one recent example involves impersonating the Income Tax Department in order to gain the private financial information of taxpayers. Critical infrastructure has been seriously harmed by ransomware attacks, such as the one that struck Oil India Limited in 2022. To restore operations, the terrorists have demanded ransom payments of millions of dollars.

## LEGAL LANDSCAPE

The primary framework for cybersecurity and privacy in India is the Information Technology Act of 2000 and its subsequent amendments, as well as sector-specific laws. One new law that mandates user rights, accountability, and data minimisation is the Digital Personal Data Protection Act (DPDPA), 2023. Implementation challenges are still present, as seen by the judiciary's involvement in privacy-related cases like *Anuradha Bhasin v. Union of India*,<sup>6</sup> which looked at the connection between cybersecurity and freedom of expression during internet shutdowns.

---

<sup>5</sup> **Prasid Banerjee**, *India's Cybersecurity Framework Still Evolving*, *Livemint* (Oct. 12, 2021), <https://www.livemint.com/technology/tech-news/indias-cybersecurity-framework-still-evolving-11634112345678.html>.

<sup>6</sup> (2020) 3 SCC 637,

India's cybersecurity regulatory structure has to be significantly revised in order to meet the demands of the digital age. The Information Technology Act of 2000 is a crucial piece of law in this field that, among other things, established the foundation for electronic commerce and attempted to stop cybercrimes like identity theft and hacking. The law was significantly revised in 2008, adding additional clauses to address intermediary liability, cyberterrorism, and data breaches. The National Cyber Security Policy was unveiled in 2013 as a long-term strategy for protecting cyberspace in response to the growing significance of protecting critical infrastructure. The Digital Personal Data Protection Act of 2023 replaced the Personal Data Protection Bill of 2019 to address privacy issues.

The Strict rules were introduced under the previous measure to protect people's data rights and ensure that digital information was processed legally. With these legal changes, India is taking the initiative to establish a strong cybersecurity framework in response to changing technology threats.

The first act of legislation in India to regulate internet activity was the Information Technology (IT) Act, which was passed in 2000. The law's formal recognition of digital signatures and electronic records, which protected online financial transactions, was its distinctive feature.

The Act's list of cybercrimes included the distribution of pornographic material, data breaches, theft of personal information, and unauthorised computer access. The Act provided procedures for adjudication and fines, including the imposition of monetary penalties for damages and the appointment of adjudicating officers. In addition, the law permitted authorities to monitor individuals' internet chats if they believed it was essential to do so in order to safeguard the nation. The Act expanded its purview to cover acts committed outside of India in order to overcome jurisdictional issues, so long as they involved a computer, network, or device with an Indian base.<sup>7</sup>

**Examining Cybersecurity Legislation from Different Countries:** Despite being founded on its fundamental relevance, India's IT Act and its amendments differ from global cybersecurity approaches in both scope and intent. For instance, in order to safeguard consumers' privacy, the General Data Protection Regulation (GDPR) of the EU imposes stringent guidelines on how businesses collect, store, and distribute personal data. The IT Act, which focuses mostly

---

<sup>7</sup>A Brief Overview of Information and Technology Act, 2000, *Legal Vidhiya* (Feb. 27, 2023), <https://legalvidhiya.com/a-brief-overview-of-information-and-technology-act2000/>.

on cybercrime and the defence of vital infrastructure, does, however, provide a minimum remedy for data privacy.<sup>8</sup> The Indian law only requires that intermediaries report events without encouraging collaboration, in contrast to the US Cybersecurity Information Sharing Act (CISA), which promotes increased voluntary information sharing between government and private sector organisations to combat cyber threats. Furthermore, India has not yet completely embraced Singapore's 2018 Cybersecurity Act. Through the regulation and registration of cybersecurity service providers, this law seeks to safeguard vital information infrastructure. These trends suggest that India will need to implement some of the best practices from other nations in order to handle both domestic and international issues.

**The Evolution of Privacy as a Constitutional Right in India:** The landmark ruling in Justice K.S. Puttaswamy (Retd.) v. Union of India<sup>9</sup> confirmed the recognition of privacy as a constitutional right under Article 21 of the Indian Constitution. By expanding its purview to include issues of data protection, human autonomy, and informational privacy, the Supreme Court reaffirmed that privacy is covered by the rights to life and personal liberty. The decision allowed for privacy-related legislation, particularly in the current digital age where many organisations regularly collect and profit from personal data. The decision also had an impact on other cases, like *Anuradha Bhasin v. Union of India*.<sup>10</sup> (2020), where the Court assessed how proportionate internet shutdowns were in light of the rights to privacy and free speech. The Puttaswamy decision provides a constitutional foundation for continuing debates about the need to balance privacy rights, surveillance needs, and state security.

The Digital Personal Data Protection Act 2023 is India's most recent and extensive law for protecting personal information in the digital era. The Act establishes the parameters of acceptable data processing, including data reduction, consent-based processing, and restricting data use to specified objectives. Included in the Act are the ideas of "data fiduciaries" and "data principals," which require businesses to handle personal data sensibly while giving people the ability to access, edit, and remove their data. A Data Protection Board is established under the DPDPA to handle complaints and uphold the law. The Act allows government agencies to make exceptions in specific situations because of changing concerns.

---

<sup>8</sup> EU General Data Protection Regulation (GDPR), *Trend Micro* (n.d.), <https://www.trendmicro.com/vinfo/us/security/definition/eu-general-data-protection-regulation-gdpr>.

<sup>9</sup> Ibid.

<sup>10</sup> Ibid.

## CHALLENGES & GAPS IN LEGAL FRAMEWORK

India's legal system for combating cybercrime and protecting digital privacy still confronts a number of significant obstacles, notwithstanding recent legislative developments such as the Digital Personal Data Protection Act, 2023. These problems increase people's and companies' susceptibility to cyberattacks in addition to impeding the application of data protection regulations. The main issues and structural flaws in India's existing approach to data protection and cyber law are examined in this section.

**Lack of Cyber-literacy and Awareness:** The general lack of knowledge regarding data rights and cyber hygiene is one of the biggest issues facing India. Most internet users, particularly those in rural and semi-urban regions, are not familiar with the fundamentals of how digital platforms gather, process, and use their personal data. Unintentional consent and heightened vulnerability to phishing, identity theft, and other cybercrimes are caused by this cyber illiteracy.

## ISSUES OF CROSS-BORDER JURISDICTION

Data breaches and cybercrime frequently cross national borders, making it challenging for domestic laws to enforce them. For instance, information that has been taken from Indian consumers might be kept on servers in a different nation, and the criminal might be based in a third state. International collaboration mechanisms or mutual legal assistance treaties (MLATs) are required in these situations in order to conduct an investigation and bring charges.<sup>11</sup>

**Insufficient Technical Expertise and Law Enforcement Capability:** The technology infrastructure and specialised expertise required to handle sophisticated cybercrimes are frequently lacking in India's law enforcement organisations. The majority of police stations lack the necessary tools to look into cybercrimes like ransomware attacks, deep-fakes, or cryptocurrency-based scams, and there are few and poorly equipped Cyber Forensic Labs.

Cyber cells are also frequently underfunded and overworked. Additionally, there is a large coordination gap between federal and state entities, which results in ineffective response and

---

<sup>11</sup> **Clare**, *Digital India and Cybersecurity: Navigating the Future – News – CLA, Commonwealth Lawyers Association, Commonwealth Lawyers Association* (2024), <https://www.commonwealthlawyers.com/cla/digital-india-and-cybersecurity-navigating-the-future/>.

investigation. The deterrent power of the law is further diminished by the sluggishness of legal proceedings and the scarcity of qualified cybercrime prosecutors.<sup>12</sup>

Recent law modifications show India's commitment to improving cybersecurity. In November 2024, the Competition Commission of India penalised WhatsApp \$25.4 million for antitrust violations pertaining to its 2021 privacy policy, which prohibited the sharing of user data with other Meta companies for a period of five years. (Commission on Indian Competition, 2014). When a judge in New Delhi lifted an earlier order in October 2024, allowing Reuters to reprint its investigative article on the hack-for-hire activities of the Indian company Appin, it further demonstrated the judiciary's role in fighting cybercrime.<sup>13</sup>

## COMPARATIVE ANALYSIS WITH INTERNATIONAL JURISDICTIONS

Countries all around the world have created their own data protection policies in response to the growing danger to digital privacy posed by cybercrime, which is constantly evolving and beyond national boundaries. India can gain important insights from a comparison of overseas frameworks such as Singapore's Personal Data Protection Act (PDPA), the California Consumer Privacy Act (CCPA), and the European Union's General Data Protection Regulation (GDPR). The lessons learnt from these frameworks can greatly improve India's fledgling data protection system. They provide strong models for controlling data flows, protecting user rights, and enforcing compliance.

**European Union – General Data Protection Regulation (GDPR):** Most people agree that the GDPR, which has been in effect since 2018, is the gold standard for data protection. It lays out precise guidelines for the gathering, handling, storing, and transferring of personal data both inside and outside the EU. The concepts of lawfulness, transparency, data minimisation, and purpose limitation are important components. Comprehensive rights, including the right to data portability, the right of access, and the right to be forgotten, are granted to data subjects.

Additionally, data controllers and processors are subject to stringent compliance requirements under the GDPR, with severe penalties for noncompliance (up to €20 million or 4% of yearly turnover). In some circumstances, it requires the appointment of Data Protection Officers

---

<sup>12</sup> **Cross-Border Disputes: Navigating Legal Issues in Multijurisdictional Disputes**, *Reed Smith* (Apr. 8, 2025), <https://www.reedsmith.com/en/perspectives/2025/04/cross-border-disputes-navigating-legal-issues-multijurisdictional-disputes>.

<sup>13</sup> **India's New Cybersecurity Laws 2024: Balancing Innovation and Regulation**, *Legal Onus* (2024), <https://legalonus.com/indias-new-cybersecurity-laws-2024-balancing-innovation-and-regulation/>.

(DPOs) and Data Protection Impact Assessments (DPIAs). Crucially, the GDPR is extraterritorially applicable, which means it covers non-EU organisations that handle the data of EU citizens. This establishes a high standard for cross-border data accountability.

### **United States – California Consumer Privacy Act (CCPA):**

Residents of California have many rights regarding their personal information under the CCPA, which went into force in 2020. These include the rights to erase personal information, to opt out of the sale of personal data, and to know what data is gathered. The CCPA places more emphasis on consumer choice and corporate openness than the GDPR, which is more concerned with consent-based approaches. Although the California Attorney General is in charge of enforcing the CCPA, it does not have a central regulatory body like the European Data Protection Board. However, recent changes made under the California Privacy Rights Act (CPRA) have strengthened enforcement procedures and expanded the rights of data subjects. Although the CCPA is more business-friendly, it nonetheless offers a strong foundation for user autonomy and openness.<sup>14</sup>

## **RECOMMENDATIONS & WAY FORWARD**

A strong, flexible, and forward-thinking legislative response is required due to the quickly changing technology world and the concurrent increase in cybercrime. The Digital Personal Data Protection Act of 2023 is a positive move, but it needs to be supported by more extensive systemic changes. The main legislative, institutional, and policy-level suggestions to strengthen India's cyber and data protection ecosystem are outlined in this section.

**Legislative Recommendations:** India has to work towards comprehensive data protection laws with precise definitions, responsibilities, and sanctions that are in line with international standards like the GDPR.

The roles of "data fiduciaries" and "data principals" should be clarified by specific subordinate laws or regulations. Crucially, the rule must have clauses pertaining to data portability, automated decision-making, and algorithmic accountability—all of which are essential in the era of artificial intelligence and big data.

---

<sup>14</sup> **California Consumer Privacy Act (CCPA)**, *State of Cal. Dep't of Just., Off. of the Att'y Gen.* (2025), <https://oag.ca.gov/privacy/ccpa>.

Laws should also be flexible but technology-neutral, offering a framework that will continue to be applicable even in the face of future advancements. In order to keep up with technological advancements, provisions for frequent legislative reviews—possibly every three to five years—should be established.

**Increasing the Power of Enforcement Organisations:** Law enforcement organisations like the Data Protection Board of India (DPBI), CERT-In, and cybercrime cells need to have a sufficient number of technically qualified employees. Stronger coordination between the police, prosecution, and digital forensic labs is crucial, as is the establishment of a specific Cybercrime Prosecution Unit inside the judiciary. A national database of cybercrimes may also be useful for seeing patterns and implementing AI and machine learning-based predictive policing strategies.<sup>15</sup>

**Technology-Assisted Legal Framework:** Technology integration into the legal system is becoming more and more necessary. Legal efficiency can be greatly increased by creating digital evidence management systems, an automated redress procedure for data breach complaints, and AI-powered case triage. Particularly in delicate industries like healthcare and finance, tools like blockchain might be utilised to guarantee traceability and transparency in data processing.

Justice can be made more inclusive through the development of online grievance platforms for data subjects that have accessibility features and multilingual interfaces. In order to keep up with changing case dynamics, the judiciary must also receive frequent training on cyber law and technology.

Newer and more complex types of cybercrime are emerging at the same time that technology continues to reshape communication, business, and governance. The complex relationship between technology and cybercrime has been explored in this essay, highlighting the pressing need for India to have a robust and flexible legal system. The progression of cybercrime from straightforward data breaches to intricate frauds enabled by artificial intelligence highlights how inadequate existing legal tools are to combat contemporary dangers.

---

<sup>15</sup> **Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age**, *IPLF* (2025), <https://www.ipandlegalfilings.com/digital-forensics-in-india-bridging-technology-law-and-justice-in-the-cyber-age/>.

From the IT Act of 2000 to the most recent Digital Personal Data Protection Act of 2023, India's legislative path shows a substantial shift in favour of acknowledging data privacy as a fundamental right. However, as technology advances, legal protections must also change.

By taking part in international agreements like the Budapest Convention on Cybercrime and bringing its domestic laws into line with international norms, India may strengthen its linkages with nations and organisations battling cyber threats.

Furthermore, information-sharing agreements and cooperative structures would improve India's ability to handle significant cyber crises. It is essential to support institutional capacity, advance cyber forensics, and encourage ethical hacking in order to meet India's long-term cybersecurity objectives. While ethical hackers are essential for locating and addressing system vulnerabilities, cyber forensics assists in the investigation and prosecution of cybercrimes.

Government programs like the "Cyber Surakshit Bharat" project and collaborations with groups like the Data Security Council of India (DSCI) have emphasised the value of skilled cybersecurity experts. The current shortage of cybersecurity experts in India is a serious problem since reports show a large gap between supply and demand. It is crucial to strengthen training programs, scholarships, and cooperative capacity-building activities in order to close this gap. The deployment of cutting-edge technologies like blockchain, machine learning, and artificial intelligence (AI) for proactive defences is essential to India's cybersecurity future.