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

CYBER LAW IN INDIA: OVERVIEW AND RECENT TRENDS

SHIVYA SETHI

ABSTRACT

This paper offers an in-depth analysis of the digital legal system in India, with a special focus on the actions taken on the ground through the Information Technology (IT) Act, 2000. It looks into both the advantages and threats of the digital media by illustrating how internet networks can serve the global trade and education while still being the source of the cybercrimes like financial fraud, identity theft, and violation of personal data privacy. The study describes the working of the major criminal aspects of the law under the Act like Sections 65 66 66C, 66E 67 67A, 67B, and 72. Also, it identifies and discusses the five major challenges that are having a significant impact on the direction of internet law namely data privacy adherence to the DPDP Act, cybersecurity rules by CERT-In, the regulation of cryptocurrencies, hardware security problems of the Internet of Things (IoT), and issues of legal liability related to developments in artificial intelligence. Based on discussion of main landmarks court decisions like K.S. Puttaswamy v. Union of India, CBS Online Services, NASSCOM v. Ajay Sood, and Anuradha Bhasin v. Union of India, the article concludes that Indian judiciary is gradually recognizing data protection and digital access as essential rights guaranteed under the constitution.

INTRODUCTION

Not limited by the physical factors, The world is becoming more and more driven by the digital infrastructure these days. Thus the need for upgrading the legal framework which cyber laws have risen to govern the digital reality. Similar to the rules and regulations that have existed, this digital legal framework against cyber crimes attempts to shield the individuals and organizations, maintaining the standards that are as robust as the physical world. These clear sets of rules help

to regulate online behaviour and enforce agencies that can combat malicious activities like fraud, identity theft, and hacking. This modern legal structure attempts to replicate the safety and accountability of the digital landscape.

OVERVIEW OF CYBER LAWS IN INDIA

In India the foundational architecture of the digital legal framework is rooted within the Information Technology (IT) Act, 2000[1]. The Act was first legislated to validate and govern the electronic and digital commerce and has been since expanding its tentacles to reach above and beyond the ever-expanding virtual landscape. The act has served as the bedrock for the nation's cyber jurisprudence. It has explicitly defined boundaries and listed the online conduct within the righteous limits. It deters and corrects the behavior of miscreants through strict penalties and punishments for digital offenses. With a digital landscape ever expanding and growing complex by the day, the laws have been amended to penalize modern offenses including privacy breaches, identity theft, financial fraud, hacking, publication of obscene material, cyber terrorism and others.

With the rapid evolution of the digital landscape, the transformation has certainly been a sharp double-edged sword for Indian society. The digital ecosystem, on one hand, has unprecedented benefits enabling online payments, online transactions, and remote businesses. It has given way to vulnerable digital networks that streamlined the virtual scams, including automated deepfakes, corporate insecurity, and other cybercrimes.

NEGATIVE IMPACT OF CYBERSPACE

Conversely, the expansion of cyberspace has its social, legal, psychological, and physiological extremities. The pervasive nature of social networking platforms has virtually erased individual privacy, creating an environment where personal data is vulnerable to leaks and exposure. From the criminal aspect, the structural anonymity and transborder nature of the Internet open up the opportunity for cybercriminals to conduct multiple cyber offences, including financial fraud,

[1] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

identity theft, hacking, and phishing campaigns, among others. The psychological impact of going through these digital crimes can result in public vulnerability, social anxiety, depressive disorders, and low self-esteem, among others, leaving behind a lasting impact.

POSITIVE IMPACTS OF CYBERSPACE

The democratized cyberspace has certainly brought unprecedented global benefits in commerce. From overcoming the geographical barriers to enjoying collaborating over the continents, the digital realm has offered instantaneous borderless connectivity, blurring the lines of time and place. This massive paradigm shift has given way to multiple digital platforms that have stopped the gatekeeping for expanding entrepreneurship and have fostered robust e-commerce ecosystems that last beyond borders. It has opened up the economy of accessing information across the globe, from highly qualifying educational resources to specialized skill training. Cyberspace has opened the flood gates to learning without having to travel or deviate from your time zone.

INFORMATION TECHNOLOGY ACT 2000

With the increase in the digital economy and networked technology, there is definitely a need for a fundamental shift in traditional jurisprudence, a shift culminating in the enactment of the Information Technology Act 2000. It has been heavily influenced by the United Nations Commission on International Trade Law's Modern Law on Electronic Commerce 1996[2], which marked the entrance of India into the regulated digital era.

To begin with, the functional aspect of the ITR 2000 was to dissolve the historical disparity between tangible and virtual transactions. It offers trade-facilitating architecture and a core structural objective and establishes an info-sourced code of digital conduct. There are several offences that have been laid down in this act, leading to the imposition of penalties for misuse of electronic communication or technology.

[2] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, U.N. Doc. A/CN.9/SER.C/GUIDE/1 (1996).

Section 65[3]: If a person is found to be tampering with the documents that are being stored in the computer, it leads to an offence under this Act. Thus, the person is liable to the punishment of imprisonment of three years and a fine of two lakh rupees, or both.

Section 66[4]: This section lays down the offence that if any person commits any other offence that is associated with the computer system, it is punishable by three years of imprisonment and a fine of ₹5 lakh, which can be imposed.

Section 66C[5]: If a person represents himself or herself on the Internet by deceiving his or her identity or presenting himself or herself with a false identity, it leads to the crime of identity theft. The person accused of this offence will be charged with three years of imprisonment and a one-lakh-rupee fine, or both.

Section 66E[6]: This act leads to the offence of invading privacy if a person in the digital era tries to invade the privacy of the victim without consent, leading to either a three-year punishment of three years or a fine of ₹2 lakhs or both.

Section 67[7]: If the offender is sending obscene or explicit material through the electronic medium to the child or any person, it leads to the penalty of 5 years of imprisonment and a fine of ₹10 lakhs.

Section 67A[8]: If a person sends any of the material or a photo/video that contains sexually explicit acts through the electronic medium, it leads to the imposition of the punishment of 7 years' imprisonment and 10 lakhs as a fine.

Section 67B[9]: If the offender depicts a child in a sexually explicit form and shares the sexually explicit material with the child through digital media, it leads to imprisonment of 7 years and a fine of ₹10 lakh.

---

[3] Information Technology Act, 2000, § 65, No. 21, Acts of Parliament, 2000 (India).
[4] Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India).
[5] Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).
[6] Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India).
[7] Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).
[8] Information Technology Act, 2000, § 67A, No. 21, Acts of Parliament, 2000 (India).
[9] Information Technology Act, 2000, § 67B, No. 21, Acts of Parliament, 2000 (India).

Section 72[10]: If the offender breaches or intentionally breaches the privacy or confidentiality of the victim, including a child, woman or any other person, it can lead to the penalty of ₹500,000.

RECENT TRENDS

The digital frontier is undoubtedly expanding at an exponential rate, changing how society communicates, transacts, and operates. However with this hyper-connectivity in place, the traditional legal systems are falling short behind. This calls for the necessity of a dynamic overhaul of the IT laws worldwide. Following the ever-changing cyberspace, the jurisprudence is shifting away from the reactive measures and addressing five critical vectors:

Data privacy and protection: With the advent of cyberspace, the need for the value of personal data has become higher than ever. It is actively being used by the criminals as a leverage for coercing the innocent. This rapid transition to online spaces has left behind vulnerable spots and digital footprints that are easier to track by experts. This systematic exposure has fundamentally reshaped our expectation of privacy. To combat this vulnerability, the legislative frameworks have moved towards strictly protecting the sovereignty of the individual data. The paradigm shift came with the digital personal data protection act. The framework shifts accountability to organizations termed as Data fiduciaries, enforcing strict principles and consent purposes to prevent data breaches. This updated regime has focused on circling and protecting the personal data, making it a legal mandated civic right. If an organization fails to comply with this code, severe financial penalties mandate the civic right.

Cybersecurity: As the cyber attack surface widens, the need for tackling cyber threats has increased as well. From basic isolated incidents to highly sophisticated cyber warfare, digital crime has come a long way and needs a critical legal framework to counter it. These attackers heavily rely on data misinterpretation, system penetration, and structural spoofing to disrupt the infrastructure, causing corporate espionage and cyber warfare.

The modern cybersecurity laws are designed to offer a proactive zero-trust approach to protect the network. The regulatory bodies, such as India's Computer Emergency Response Team, have come

[10] Information Technology Act, 2000, § 72, No. 21, Acts of Parliament, 2000 (India).

forward with rigorous incident reporting rules and mandatory security audits that are an attempt to safeguard the organizations against such attacks. The legal framework attempts to act as a firewall protection against cyber threats.

Cryptocurrency: The global platforms have seen a meteoric rise in blockchain-based cryptocurrencies and decentralized finance, rewriting the rules of digital commerce, opening the doors to financial freedom and transactional autonomy. The blockchain has also opened the gate for cybercriminals to penetrate into the vulnerable digital assets. This is why the need for regulatory guardrails has increased as well. These digital currencies can easily be the vehicles of laundering international money, ransomware payouts, and other illicit activities. To ensure that these vulnerabilities are sealed tight shut, cyber law is intervening in the web3 space, embracing anti-money laundering and know-your-customer frameworks to ensure that every asset and transaction is tracked and disclosed to the enablers. Cyber laws are aimed to preserve blockchain innovation without opening the avenues for financial cybercrime.

Internet of things: With a wide range of smart Home appliances available in the market. Automation comes with the Internet of Things or IoT. These consumer-centric devices are designed for offering hard-coded security configurations and have weaker firewalls that are soft targets for hackers. This smart device acts as a backdoor to an individual's entire private network, enabling them to penetrate into the more serious and vulnerable points to bridge the gap. The Cyber Law mandates manufacturing of the hardware with strong compliance standards, strict essential requirements of connected devices, and clear documentation of microtrip origins. This is needed from the ground up to prevent consumers from legally welcoming digital malware.

Artificial intelligence: With the advent of cyberspace, artificial intelligence and algorithm-based searches are taking over our daily lives with AI tools streamlining the workflows. The exposure to databases has been quite simple. These pose severe risks to data privacy and human dignity. This is why the malicious use of AI has been used for digital fraud, for automated phishing scams, model poisoning, or highly realistic deepfakes that lead to identity theft or disinformation. Transcription by CastingWords.

CASE LAWS

K.S. PUTTASWAMY VS. UNION OF INDIA[11]

Facts of the Case: This case originated in 2012 when Justice Puttaswamy, the retired judge of the Karnataka High Court, filed a writ petition against the validity of the government's Aadhaar scheme. The petitioner argued that the mandatory collection of fingerprints and personal geographic data without a robust legislative framework could violate citizens' bodily autonomy and expose them to surveillance. This, in the long run, infringes upon their right to privacy. The government then countered that the Indian Constitution did not explicitly guarantee privacy as a fundamental right.

Legal Judgement: The matter led to a historic nine-judge bench of the Supreme Court that unanimously overruled the past precedents mentioned by the government. It declared the right to privacy as a fundamental right, intrinsic to life and personal liberty under Article 21 of the Constitution.[12] The judgement established that privacy is not an elitist concept but a core human right. This ruling directly laid the legal foundation for striking down the Aadhaar Act, parts of the Aadhaar Act, decriminalising section 377[13], and mandating the creation of India's Digital Personal Data Protection (DPDP) Act.[14]

CBS ONLINE SERVICES LTD. V. STATE OF MP (2020)[15]

Facts of the Case: The CBS Online Services Limited discovered that its internal corporate database, proprietary algorithms, and sensitive commercial client records were systematically copied, leaked, and transferred to an external server. This stolen corporate data was then used by the ex-employees to launch a competing business venture, causing financial losses to the original form.

---

[11] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[12] India Const. art. 21.
[13] India Penal Code, § 377
[14] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[15] CBS Online Servs. Ltd. v. State of M.P., 2020 M.P.L.J. Online 42 (India).

Legal Judgement: In the matter, the Madhya Pradesh High Court addressed the issue of accessing the unauthorized data, theft of network data. The court sustained criminal charges under Section 43 of the IT Act[16] and Section 66 of the IT Act.[17] The court firmly established that the unauthorized extraction, downloading or deprecation of corporate data without explicit permission of the owner is punishable by cyber offense.

NATIONAL ASSOCIATION OF SOFTWARE AND SERVICE COMPANIES (NASSCOM) V. AJAY SOOD & OTHERS (2005)[18]

Facts of the Case: The National Association of Software and Services Companies recognized a ring of fraudsters operating a deceptive phishing racket with its name. The defendants had created a similar identity with fraudulent email accounts and have spoofed corporate messages to job seekers. They claimed to be official recruiters for the alleged company and had requested personal and bank credentials alongside processing fees. This deception severely damaged NASSCOM's corporate credibility.

Legal Judgement: The plaintiff filed a civil suit for trademark infringement on unfair trade competition. In the matter, the Delhi High Court addressed the issue of domain name masking. The punitive damages awarded were Rs 5 lakhs against the defendants. It was established that the commercial brand impersonation and spoofing in virtual places is punishable under the trademark law, making a strong precedent against online identity theft.

ANURADHA BHASIN V. UNION OF INDIA (2020)[19]

Facts of the Case: After the revocation of the special constitutional status of the Government of Kashmir under Article 370[20] in 2019, the government imposed a total indefinite internet suspension, internet, mobile, and broadband service suspension across the region. Anuradha Bhasin, Executive Editor of the Times of Kashmir daily newspaper, filed a writ petition with the Supreme Court arguing that an open-ended, indefinite internet blackout could paralyse print

[16] Information Technology Act, 2000, § 43, No. 21, Acts of Parliament, 2000 (India).
[17] Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India).
[18] Nat'l Ass'n of Software & Serv. Cos. v. Ajay Sood, (2005) 119 D.L.T. 596 (India).
[19] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India)
[20] India Const. art. 370.

journalism and violate the fundamental right to practice a profession and receive information over the web.

Legal judgement: In this matter the Supreme Court delivered a historic verdict that recognized the need for digital access as an extension of fundamental rights. The Court upheld the freedom of speech and expression and the right of carrying on any trade or business over the internet as constitutionally protected under Article 19(1)(a)[21] and 19(1)(g)[22]. Indefinite suspension of internet services did not uphold the test of proportionality and was a violation of law.

[21]India Const. art. 19, cl. 1(a).
[22] India Const. art. 19, cl. 1(g).