



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

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CYBER LAW IN INDIA: EMERGING ISSUES AND CHALLENGES

~ *Vanshika Sharma*

ABSTRACT

Digital tech keeps changing how people live - touching money matters, schools, government work, health care, buying things, talking online. Even though new tools help economies grow and make services easier to reach, they also open doors to smarter digital dangers for people, firms, offices. Crimes like stolen identities, fake emails asking for details, locked-up files for cash, scams with money, internet terror acts, false videos that look real, abuse on platforms, illegal crypto deals, leaks of private records now pop up more often across India.¹ Because of this, laws around online spaces matter a lot - not just to block harm but also to protect basic freedoms: who gets to know what about you, what you can say, where you find knowledge.

Though laws like the IT Act, 2000, updated in 2008² - form the base, newer rules such as the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023 now shape India's online legal scene.³ Alongside these sit supporting regulations covering e-governance, platform responsibilities, and how digital proof is handled in court.⁴ Even with fresh updates rolling in over time, problems remain tangled across many areas. One hurdle hides where authority begins and ends when crimes jump between regions.⁵ Others grow from weak tools for probing digital offences effectively. Fast-moving tech shifts outpace rulebooks before they settle. Smart machines get twisted into harmful uses faster than guards go up. Criminal actions crossing borders slip through gaps no single force can close alone. Courts built just for cyber

¹ National Crime Records Bureau, Crime in India (latest ed.).

² Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Information Technology (Amendment) Act, No. 10 of 2009, INDIA CODE (2009).

³ Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023); Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).

⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

⁵ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

issues? They are few, sometimes absent where most needed. Awareness among people about their duties and rights online stays thin, barely reaching daily life.

Looking back at how cyber law grew in India forms a core part of this work, while also taking stock of current laws that handle online crimes. Shifting into newer areas, attention turns toward problems sparked by artificial intelligence, threats to personal data, virtual money, fake videos made by software, internet-based terror acts, along with cross-border hacking incidents. Instead of inventing new paths, the approach sticks close to written laws, court decisions, scholarly texts, official documents, plus recent shifts in public guidelines. Near the end, suggestions emerge - not loud or forceful - for updating both legal rules and governing bodies so they flex well within a fast-moving tech world without losing sight of human rights.

Keywords: Cyber Crime, Information Technology Act, Digital Personal Protection Act, Cyber Security, Bharatiya Nyaya Sanhita.

INTRODUCTION

Out here, life keeps shifting because machines now shape how nations run. Not just offices but schools too depend on digital tools more than ever before. What started small now powers entire economies. Across India, new pathways opened - payments without cash, IDs linked to data, government help online.⁶ Systems talk to each other faster, settling arguments through screens instead of courts sometimes. Buying and selling happens in clicks, guided by smart algorithms watching every move.⁷ One thing stands clear: staying offline feels like stepping backward.

Online access spreading fast opens new paths for fresh ideas and growth in society and economy. Banking, shopping, work chats, learning, medical advice, government tasks - people handle them all online today. Even though tech progress makes things quicker and easier to reach, it brings sharper digital dangers too.

Crime on the internet now spreads faster than almost any other kind.⁸ Not like old-style crime, it ignores borders, letting attackers hide while striking from anywhere.⁹ Money scams show up often, along with stolen identities, fake emails that trick people, locked files held for payment, harassment online, digital sabotage, leaked private records, realistic fakes made by machines,

⁶ Ministry of Electronics & Information Technology, Digital India Programme (Gov't of India).

⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁸ National Crime Records Bureau, Crime in India (latest ed.).

⁹ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

and illegal deals using digital cash¹⁰ - each a headache for authorities everywhere. As more daily life leans on connected systems, weak spots grow - and so do chances for those who know how to twist tech against itself.

After India passed the Information Technology Act in 2000,¹¹ rules around online activity began taking shape - this law gave weight to digital documents and e-signatures, along with setting penalties for cybercrimes. Though originally limited, the 2008¹² update pushed boundaries wider; suddenly issues like stolen identities, attacks on digital systems, safeguarding information, responsibilities of internet platforms, personal privacy, and how government services go electronic were part of it. Now, fresh changes have arrived - the 2023¹³ Digital Personal Data Protection Act plus the new criminal code-named Bharatiya Nyaya Sanhita, 2023 - are shifting ground again, deepening privacy safeguards and updating laws tied to digital evidence and tech-facilitated wrongdoing.

Still, even after many law updates, India's digital rules face tough ongoing issues. New tech like artificial intelligence, machine learning, and blockchain moves faster than laws can keep up.¹⁴ Laws already in place often fail when dealing with fresh threats - deepfakes, scams made by AI, stolen fingerprints, fake news waves, tricks using algorithms. What works today might lag tomorrow. Rules shaped yesterday rarely fit what happens online now.¹⁵

Most times, online crimes stretch across national borders.¹⁶ That brings tangled legal authority issues, needing countries to work together closely just to follow basic leads. Getting things moving often stalls because law enforcement might not have deep tech skills on hand. Labs that handle digital clues are too few, which drags out how long it takes to gather proof. Cases sometimes go nowhere since there aren't enough lawyers trained for these types of charges. A lot of people still do not grasp how they fit into broader security patterns. Laws must keep shifting - step by step - all while systems slowly grow stronger behind the scenes.

Looking at today's context, this study takes a close look at how India's cyber laws are changing. It questions new tech issues that keep coming up. Old rules get tested here for what they can

¹⁰ Indian Computer Emergency Response Team (CERT – In), Annual Report (latest ed.)

¹¹ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

¹² Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

¹³ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

¹⁴ United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).

¹⁵ Shreya Singhal V. Union of India, (2015) 5 SCC 1.

¹⁶ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

actually handle. Some updates seem needed if the system is to work well. Tech changes fast - laws should keep pace without breaking core freedoms. Security matters, yet so does guarding basic rights. A balance must be found somehow.

RESEARCH OBJECTIVE

The present study attempts to achieve the following objectives:

- 1) To study the role of Information Technology Act, 2000 and its subsequent legislative developments.¹⁷
- 2) To study the effect of Digital Personal Data Protection Act, 2023 and Bharatiya Nyaya Sanhita, 2023 on cyber regulation.¹⁸
- 3) To identify emerging technological challenges such as artificial intelligence, deepfake technology, cryptocurrency, ransomware and cyber terrorism.¹⁹
- 4) To study significant judicial decisions that have shaped cyber jurisprudence in India.
- 5) To recommend legal and policy reforms for strengthening India's cyber security and digital governance architecture.

RESEARCH QUESTIONS

The following questions guide the research:

- Are the current cyber laws in India adequate to address the contemporary cyber threats?
- The effectiveness of the Information Technology Act, 2000 in regulating emerging technologies.
- Legal issues concerning artificial intelligence, cryptocurrency and cross-border cybercrime.
- How have Indian courts understood rights in the digital age?
- What kind of reforms are needed for better cyber governance in India?

¹⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

¹⁸ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

¹⁹ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

RESEARCH METHODOLOGY

The present study uses doctrinal research methodology. The research is based mainly on qualitative analysis of statutory provisions, judicial precedents, government reports, books, journal articles, policy papers and scholarly publications on cyber law and cyber security.

The primary sources are the Constitution of India, Information Technology Act, 2000, Information Technology (Amendment) Act, 2008, Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023 and significant judgments of the Supreme Court and various High Courts.²⁰

The secondary sources included books, peer reviewed journal articles, reports of the National Crime Records Bureau, publications of the Ministry of Electronics and Information Technology, reports of CERT-In, academic commentaries and relevant study.

The study is analytical and descriptive in nature. It is aimed at evaluating the strengths and limitations of the existing legal regime and make proposals for reforms for future legislative development.

EVOLUTION OF CYBER LAW IN INDIA

Starting in the 1990s, India saw tech transform how people communicated, traded, governed, banked, managed business. Paper trails began fading when digital links spread across daily operations. Because old legal rules could not handle computer crimes, fresh approaches became unavoidable. Instead of ignoring online threats, lawmakers focused on crafting specific tools for digital wrongdoing. As connectivity grew, so did risks beyond what earlier statutes ever covered. So, legislation evolved - not by choice but by demand - to meet challenges of E - transactions and virtual misconduct.²¹

Back then, global talks led to new rules. The U.N.'s trade law group put forward a blueprint in 1996²² for handling online deals - making digital papers and E -signatures count legally. Because of that shift, India moved fast. New laws arrived by 2000,²³ setting clear terms for

²⁰ INDIA CONST.; Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India); Digital Personal Data Protection Act, 2023, No. 22, Act of Parliament, 2023 (India); Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

²¹ United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).

²² United Nations Commission on International Trade Law, UNCITRAL Model Law on Electronic Commerce (1996).

²³ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

internet activity. Among Asian nations, it stood out early, building one of the region's first full sets of cyber rules.

Starting off, the Information Technology Act of 2000 aimed to give legal status to digital records along with electronic signatures.²⁴ Instead of just focusing on paper trails, it opened doors for online governance systems across government functions. Because of this law, doing business electronically became more supported under national rules.²⁵ At the same time, actions like hacking or data theft started carrying defined punishments.²⁶ While making these changes, older laws saw updates too - adjustments touched criminal code provisions, evidence handling methods, banking record usage, and central bank operations.²⁷ Since then, paperwork done through screens gained equal weight in courtrooms.²⁸ One key shift came when an oversight body emerged to supervise who could issue digital certificates.²⁹ Overall, progress in India's move toward digital processes got a strong push because of how documents without ink began counting as valid.

Technology moved forward, bringing fresh threats like stolen identities, fake emails, digital attacks, breaking into systems, money scams online, along with breaches of personal space - showing clear gaps in earlier laws. Because of this shift, lawmakers passed the updated Information Technology Act in 2008,³⁰ reshaping how India handles internet-related crimes. New rules came into picture, pretending to be someone else got defined as illegal, safeguards around private details improved, duties were set for companies storing data, middlemen faced clearer responsibilities, authority to spy on messages grew stronger, alongside tougher measures against digital terror acts.³¹

Later on, India put in place various supporting laws - like the 2011 rules setting out security standards for handling personal data, along with guidelines for managing sensitive information. These were followed by new regulations in 2021 focused on intermediary responsibilities and ethical norms for digital media platforms. Together, they increased the requirements for tech firms and online service providers to follow legal procedures more closely.

²⁴ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁵ Id.

²⁶ Information Technology Act, 2000, No. 21, §§ 43, 65, - 67F, Acts of Parliament, 2000 (India).

²⁷ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁸ Indian Evidence Act, 1872, § 65B, Acts of Parliament, 1872 (India).

²⁹ Information Technology Act, 2000, No. 21, §§ 17 – 34 Acts of Parliament, 2000 (India).

³⁰ Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2009 (India).

³¹ Information Technology Act, 2000, No. 21, §§ 43A, 66C, 66D, 66F, 72A, 79, Acts of Parliament, 2000 (India).

Now more than ever, people see why keeping info private matters. That is how the Digital Personal Data Protection Act came into being in 2023. A new law shaped by Parliament took form because old rules could not keep up. Instead of leaving things unmanaged, clear steps were set on handling digital details. Gathering data follows structure now, just like using it or holding onto it. Moving such information across borders also has boundaries drawn. People gain stronger say about what happens to their own records. Their control becomes real through specific legal backing. Rules apply differently depending on context but fairness stays central. Oversight exists so promises made in law actually take root.

At the same time, changes to criminal laws under the Bharatiya Nyaya Sanhita, 2023 brought in rules about electronic documents, crimes using the internet, harassment online, fake digital records, group-based hacking activities, and proof stored digitally. With these steps, India keeps adjusting its legal system because technology keeps changing fast.

EXISTING LEGAL FRAMEWORK GOVERNING CYBER LAW IN INDIA

CONSTITUTIONAL FRAMEWORK: The Indian Constitution does not explicitly mention cyberspace, but constitutional provisions have been interpreted to apply to the digital environment.³² Article 19(1)(a) guarantees the freedom of speech and expression including on the internet subject to reasonable restrictions in Article 19(2).³³ The right to life and personal liberty under Article 21 has also been interpreted by the courts to include the right to privacy and personal data as part of the constitutional protection of the right to privacy³⁴ and personal data.

INFORMATION TECHNOLOGY ACT, 2000: Even today, the Information Technology Act of 2000 holds central ground in India's cyber laws.³⁵ Built at first to support online trade, it gave legal weight to digital documents along with e-signatures.³⁶ As years passed, its role grew - now it shapes how cybercrimes are handled across the country. The major objectives of the Act include:

Electronic records get official acceptance under law³⁷

³² Justice K.S. Puttaswamy (Retd.) V. Union of India, (2017) 10 SCC 1.

³³ INDIA CONST. art. 19(1)(a).

³⁴ INDIA CONST. art. 21; Justice K.S. Puttaswamy (Retd.) V. Union of India, (2017) 10 SCC 1.

³⁵ Information Technology Act, 2000, No. 21, § 1 (India).

³⁶ Information Technology Act, 2000, § 4 – 5 (India).

³⁷ Information Technology Act, 2000, § 4 (India).

Legal recognition of digital signatures;³⁸

Promotion of electronic governance;³⁹

Regulation of Certifying Authorities;⁴⁰

Prevention and punishment of cyber offences;⁴¹

Protection of electronic data and computer systems.⁴²

Starting with broad strokes, the law treats all tech forms equally. It covers legal consequences when computers get used the wrong way. Wrongdoing might lead to court cases, whether public or private. Penalties depend on how systems are misapplied. Rules apply regardless of the tool involved. Consequences follow misuse, not the machine. Liability shows up in different shapes under this framework.

IMPORTANT PROVISIONS OF THE INFORMATION TECHNOLOGY ACT:

SECTION 43 DAMAGE TO COMPUTER EQUIPMENT: Anyone caught using a computer system without permission might face legal consequences under Section 43.⁴³ Getting into systems they should not be in, pulling files out, slipping in harmful software - those acts count too.

SECTION 43A FAILURE TO PROTECT DATA RESULTS IN COMPENSATION: Now companies must answer for how they handle sensitive and private data.⁴⁴

SECTION 65 ALTERING COMPUTER SOURCE CODE: Whoever hides, wipes out, or tampers with software code after being told to keep it safe breaks Section 65.⁴⁵ That rule treats deliberate changes - or making it vanish - as a crime when keeping the original was mandatory. Messing with digital records on purpose crosses the line if law demands their storage. Altered files count too, just like erased ones, so long as backup duties existed. Keeping quiet about missing data also triggers penalties under this clause.

³⁸ Information Technology Act, 2000, § 5 (India).

³⁹ Information Technology Act, 2000, § § 6 – 10A (India).

⁴⁰ Information Technology Act, 2000, § § 17 – 34 (India).

⁴¹ Information Technology Act, 2000, § § 43 – 74 (India).

⁴² Information Technology Act, 2000, § § 43 & 43A (India).

⁴³ Information Technology Act, 2000, § 43, No. 21, Acts of Parliament, 2000 (India).

⁴⁴ Information Technology Act, 2000, § 43A, No. 21, Acts of Parliament, 2000 (India).

⁴⁵ Information Technology Act, 2000, § 65, No. 21, Acts of Parliament, 2000 (India).

SECTION 66 COMPUTER RELATED CRIMES: When actions turn sneaky or deceitful, what was once just a private legal issue becomes a crime under Section 66.⁴⁶ Behaving with intent to deceive reshapes outcomes defined earlier in Section 43. Wrongdoing gains new weight if driven by lies or trickery. The law shifts its stance the moment honesty falls away. Hidden motives change how acts are judged. Deception marks the point where civil turns criminal.

SECTION 66C IDENTITY THEFT: Criminals stealing personal details now rank among the most common online crimes.⁴⁷ Using someone else's details without honesty becomes a crime under Section 66C when done with deceitful intent password, digital signature, electronic signature, unique identification credentials.

SECTION 66D THROUGH IMPERSONATION: Section 66D punishes online impersonation committed through communication devices or computer resources.⁴⁸

SECTION 66E BREACH OF PERSONAL PRIVACY: Hidden cameras or secret photos of someone's body? That's what Section 66E makes illegal.⁴⁹ Taking such pictures without permission crosses a legal line. Sharing them, even online, counts as breaking this rule too. Sending these images through messages is treated just as harshly. The law sees no difference between snapping, spreading, or streaming them. Consent matters - its absence turns acts into offences. No approval means it's against the law.

SECTION 66F CYBER TERRORISM: Out there among digital crimes, cyber terrorism stands as perhaps the most severe offence acknowledged by India's legal system.⁵⁰ Acts intended to threaten the, sovereignty, integrity, security of India, critical infrastructure, breaking into computers without permission can be called cyber terrorism, Time behind bars could last a lifetime.

SECTION 67: Criminalises publication or transmission of obscene electronic material.⁵¹

⁴⁶ Information Technology Act, 2000, § 66, No. 21, Acts of Parliament, 2000 (India).

⁴⁷ Information Technology Act, 2000, § 66C, No. 21, Acts of Parliament, 2000 (India).

⁴⁸ Information Technology Act, 2000, § 66D, No. 21, Acts of Parliament, 2000 (India).

⁴⁹ Information Technology Act, 2000, § 66E, No. 21, Acts of Parliament, 2000 (India).

⁵⁰ Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).

⁵¹ Information Technology Act, 2000, § 67, No. 21, Acts of Parliament, 2000 (India).

SECTION 69: Empowers the Central Government to intercept, monitor, or decrypt electronic information under specified circumstances involving: sovereignty, national security, defence, public order, prevention of offences.⁵²

SECTION 72: Anyone sharing digital data without permission faces penalties under Section 72.⁵³ This rule applies when info is gathered using legal authority. Keeping sensitive details, private matters just as much as following proper process. Leaking such material breaks the law outright.

SECTION 79 INTERMEDIARY LIABILITY: Provides conditional safe harbour protection to intermediaries including: social media platforms, internet service providers, e-commerce platforms, search engines.⁵⁴ Still, protection kicks in just if platforms follow proper care rules plus act on official warnings about illegal material.

DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A shift unfolds in how India manages online information with the new 2023 law on personal data.⁵⁵ Though quiet in tone, its arrival reshapes rules that guide digital trust across the nation.

Fresh rules aim to guard private info while still making space for new tech ideas.⁵⁶ How they handle data matters just as much as what gets built next. With care, progress does not have to risk exposure. Rules shape how details move, who sees them, why. Privacy stays intact when systems respect limits from the start. Major features include: consent-based processing; notice obligations; rights of Data Principals; responsibilities of Data Fiduciaries; children's data protection; grievance redressal mechanisms; establishment of the Data Protection Board of India; Fines apply when rules aren't followed.⁵⁷

Nowhere near the patchwork rules before it, this law sets up its own system for handling digital data - working inside government agencies just as much as in big companies. One clear structure replaces scattered attempts.

BHARATIYA NYAYA SANHITA, 2023: Electronic messages can now face legal consequences under a fresh law from 2023.⁵⁸ This new code walks alongside the older IT Act,

⁵² Information Technology Act, 2000, § 69, No. 21, Acts of Parliament, 2000 (India).

⁵³ Information Technology Act, 2000, § 72, No. 21, Acts of Parliament, 2000 (India).

⁵⁴ Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).

⁵⁵ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁵⁶ Digital Personal Data Protection Act, 2023, No. 22, §§ 4 – 15, Acts of Parliament, 2023 (India).

⁵⁷ Digital Personal Data Protection Act, 2023, No. 22, §§ 4 – 33, Acts of Parliament, 2023 (India).

⁵⁸ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

covering digital wrongs once left unclear.⁵⁹ Where tech meets crime, rules have sharpened without fanfare. A message sent online might hold weight in court, just like paper did before. Laws adapt, even if quietly, matching how people connect today. Among the key rules are those covering acts such as: online stalking; voyeurism; Spreading lewd content online; sending explicit digital files; forgery of electronic records; fabrication of electronic evidence; organised cybercrime; cyber-enabled financial offences.⁶⁰

Nowhere is change clearer than in how digital files are treated under the updated legal framework. Because online crimes often mirror traditional ones, authorities must work across two laws at once - one focused on tech, the other on general conduct.

EMERGING ISSUES AND CHALLENGES IN CYBER LAW

The fast-changing face of digital technology has also greatly changed what is considered cybercrime. Crimes previously defined as hacking or email fraud have now turned into very sophisticated attacks that involve artificial intelligence (AI), ransomware, cryptocurrency, deepfakes, cloud computing (CC), and transnational (cross-border) crime.⁶¹ The result is that countries will increasingly have difficulties regulating cyberspace, balancing individual rights with technological innovation. In India, although improvements are being made in cyber law and legislation, there are still many practical and legislative limitations to the existing legal framework.⁶²

1. **ARTIFICIAL INTELLIGENCE AND DEEPFAKE TECHNOLOGY:** Something strange is happening in tech - machines now handle tasks once thought impossible. From hospitals to courtrooms, hidden programs help make decisions faster than before. Yet trouble follows where progress goes unchecked. Fake messages written by computers trick people more easily these days. Malware evolves on its own without human input sometimes. Faces get swapped or misidentified through altered software patterns. Old defences struggle because attacks adapt too quickly. Laws scramble to catch up with what machines can do now.⁶³

⁵⁹ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India); Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

⁶⁰ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

⁶¹ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

⁶² Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁶³ Shreya Singhal V. Union of India, 2015 5 SCC 1.

Deepfake tech has shown up lately, raising serious concerns.⁶⁴ Using artificial intelligence, it builds fake photos, videos, or sound clips that look real. Because of this, hackers can copy leaders, twist public conversation, push lies, steal money, or invade someone's private life instead of just guessing. Fake clips of famous people have already appeared online - proof of how easily trust in facts and government can crack under pressure. What once felt like sci-fi now shapes what we see and believe every day.

Right now, India does not have a specific law made just for content created by artificial intelligence.⁶⁵ Some parts of existing rules - like those in the Information Technology Act or the new Bharatiya Nyaya Sanhita - can step in under particular circumstances.⁶⁶ Copyright policies along with legal views on privacy might also play a role sometimes. Yet overall, there is still a need for full-fledged laws that clearly cover how AI should be handled.

2. **DATA PRIVACY AND PERSONAL DATA PROTECTION:** Out in the open, digital services gather vast stacks of private details - bank histories, fingerprints, health reports, websites visited, habits tracked.⁶⁷ Because of this shift, info now ranks among the top assets driving online markets. All at once, massive leaks have left countless people facing stolen identities, money scams, spying risks, damaged names.⁶⁸

A landmark ruling by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India placed privacy firmly within the realm of fundamental rights, reshaping how personal data is viewed under Indian law.⁶⁹ Following that shift, lawmakers passed the Digital Personal Data Protection Act in 2023, setting up a system where handling personal information requires clear permission, while those managing data must answer for their actions, individuals gain control over their own details, and breaking rules brings heavy financial consequences.⁷⁰

Even now, problems stick around when it comes to moving data across borders because rules differ wildly from one place to another. Government watching doesn't stop just

⁶⁴ Ministry of Electronics & Information Technology, Advisory on Deepfakes and AI – generated Content (Gov't of India, 2024).

⁶⁵ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁶⁶ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).

⁶⁷ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁶⁸ Indian Computer Emergency Response Team (CERT – In), Annual Report (latest ed.).

⁶⁹ Justice K.S. Puttaswamy (Retd.) V. Union of India, (2017) 10 SCC 1.

⁷⁰ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

because laws change elsewhere. Decisions made by hidden algorithms often shape lives without clear explanation behind them. Storing data in specific countries creates headaches for global systems trying to function smoothly. Enforcement of privacy rights? That part still limps along, slow and uneven.⁷¹

3. **CRYPTOCURRENCY AND FINANCIAL CYBERCRIME:** Out of nowhere, cryptocurrencies changed how digital money works - cutting out middlemen entirely.⁷² Yet hidden behind that freedom is a flip secret dealing now move easier than ever before, slipping through cracks in oversight. Illicit cash finds new paths here, feeding crime networks, hackers demanding payoffs, fake investment traps, undeclared income escapes, terror groups getting funds - all tucked into corners of the internet⁷³ most never see.

Payments demanded by hackers often go to digital currencies because tracking money on blockchains gets messy fast. Scam investments that promise big returns - pyramid setups, phony trading sites, rigged tokens - have wiped out serious cash from people putting faith in them.

For now, India handles virtual digital assets by taxing them and applying rules against money laundering. Still, there is no full law yet covering cryptocurrencies, which leaves questions about how investors are protected and who exactly watches over these markets.⁷⁴

4. **RANSOMWARE ATTACKS:** Out of nowhere, ransomware became a top threat in digital crime.⁷⁵ Locked files show up without warning - pay up or stay shut out. Hospitals often find themselves hit hard, along with schools playing host to chaos too. Money movers in finance get caught in the crossfire just as fast. Even power grids and air travel hubs aren't safe when hackers strike. Officials running government offices brace for impact nearly every day.

Out here, money troubles ripple outward - schools feel it, hospitals slow down, roads lag behind, trust slips away. Because hackers keep levelling up, defences must too:

⁷¹ Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁷² Reserve Bank of India V. Internet & Mobile Association of India, 2020 10 SCC 274.

⁷³ Prevention of Money – Laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

⁷⁴ Finance Act, 2022, No. 6, Acts of Parliament, 2002 (India); Prevention of Money – laundering Act, 2002, No. 15, Acts of Parliament, 2003 (India).

⁷⁵ Indian Computer Emergency Response Team (CERT – In), Annual Report (latest ed.).

sharper response plans, clearer warnings sent across borders, teams working closer despite distance.⁷⁶

5. **CYBER TERRORISM AND NATIONAL SECURITY:** Out here, digital sabotage ranks among the most serious dangers to a country's safety.⁷⁷ Not like traditional terror methods, online strikes can break vital services without anyone stepping inside. Power supplies might fail when hackers interfere. Money handling systems could freeze under pressure from remote intruders. Military communications face risks too, since data routes aren't always safe. Phone lines and messaging hubs sometimes buckle during intense breaches. Trains, traffic lights, even hospital gear - these things often depend on links that bend easily. Few layers stand between chaos and control.

Most times, tracking who launched a digital attack feels like chasing smoke. That is because tools exist that hide identities, reroute traffic through distant computers, scramble messages beyond reading. Section 66F under India's IT law labels such acts as cyber terrorism.⁷⁸ Governments back some of these actions, making detection even harder. So, dealing well means countries must exchange hidden details. Strong digital shields also become necessary.⁷⁹

Dark Web and Organised Cybercrime: Hidden corners of the internet rely on scrambled signals to hide who is talking.⁸⁰ Though some people use these spaces to speak freely without being watched, others sell dangerous things there instead. Secret marketplaces exchange narcotics alongside guns, fake IDs, hacked bank details, harmful software, images of child exploitation, and even people.⁸¹ These networks protect identities, which helps both whistleblowers and criminals alike. Out of sight, these crime groups now trade through hidden online hubs shielded by encryption. When law enforcement steps in, old tactics tend to fall short - especially when suspects scatter across borders without a central base.⁸²

6. **JURISDICTIONAL CHALLENGES:** Across borders, cybercrime often moves without limits.⁸³ From a single nation, an attack might launch, yet rely on machines hosted far away. People in many countries can feel its impact at once. Because of this

⁷⁶ National Cyber Security Policy, 2013, Ministry of Electronics & Information Technology, Government of India.

⁷⁷ Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).

⁷⁸ Information Technology Act, 2000, § 66F, No. 21, Acts of Parliament, 2000 (India).

⁷⁹ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

⁸⁰ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

⁸¹ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

⁸² United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

⁸³ United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime (2013).

spread, legal authority gets tangled. Sorting out who investigates becomes messy. Gathering proof crosses lines governments do not always agree on. Getting suspects to court involves negotiations between states. Punishing offenders grows harder when laws clash.

One country's laws might clash with another's when chasing online crimes. Electronic proof collected in one place may not meet the rules somewhere else.⁸⁴ Agreements meant to help courts work together tend to fall short these days. Old-style treaties struggle to keep pace with how fast digital cases move.

7. **DIGITAL EVIDENCE AND FORENSIC CHALLENGES:** These days, cops often solve crimes by looking at digital clues - think email trails or footage from security cameras. Sometimes it's timestamps buried in server files that tell the real story.⁸⁵ Footage isn't always clear, yet what shows up later in logs can shift everything. Information hiding inside a phone might link pieces others miss. Even transactions on blockchains leave traces nobody planned. Data tucked away in online storage accounts tends to surface when least expected.

Start with truth - digital proof often slips through cracks. Files vanish, change shape, or lock behind codes without warning. Because of this mess, those digging into data need sharp skills and solid tools. Keeping records valid for court means walking a tightrope few know how to tread.

LANDMARK JUDICIAL DECISIONS

Shreya Singhal V. Union of India (2015) 5 SCC 1⁸⁶

A ruling struck down part of India's tech law, saying it clashed with free expression rights. Words like "annoyance" gave too much power to officials - open-ended terms invited misuse. That kind of uncertainty made people hold back online speech. Unclear phrasing, the judges said, led to fear instead of fairness.

Still today, few rulings have shaped online expression in India like this one did. Though years have passed, its weight lingers across courtrooms and screens alike. A single case - unexpectedly pivotal - now echoes through debates on rights and reach.

⁸⁴ Budapest Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.

⁸⁵ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Indian Evidence Act, 1872, § 65B.

⁸⁶ Shreya Singhal V. Union of India, (2015) 5 SCC 1.

Justice K.S. Puttaswamy (Retd.) V. Union of India (2017) 10 SCC 1⁸⁷

Surprisingly, nine judges stood together in saying privacy belongs as a basic right within Article 21. This ruling laid down constitutional roots for how personal data should be protected - later shaping the law known as the Digital Personal Data Protection Act, 2023.

Anvar P.V. V. P.K. Basheer (2014) 10 SCC 473⁸⁸

Out of nowhere, the Supreme Court made it clear: electronic proof counts in court just if Section 65B of the Indian Evidence Act is followed. Only after meeting that rule does such data stand a chance - raising the bar quietly but firmly.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1⁸⁹

Electronic evidence now stands on firmer ground thanks to a recent court ruling. Not just confirming but insisting - Section 65B demands strict compliance when certifying digital records. Confusion among past rulings melted away under this decision's clarity. Legal outcomes in online-related disputes gain more predictability because of it. Rules around digital proof feels less shaky after this moment.

Avnish Bajaj v. State (NCT of Delhi)⁹⁰

Born from what many call the Bazeem.com Case, this ruling took a close look at how web platforms handle questionable material online. It shaped changes later woven into law, carving out shelter for intermediaries through Section 79 of the IT Act. Not every outcome was planned - some shifts emerged quietly, over time. What started as one legal challenge rippled outward, redefining responsibility without rewriting everything.

COMPARATIVE ANALYSIS

Still, India's rules on digital matters have grown a lot - yet looking at how others do it shows room to go farther.

Out of Brussels came a firm hand on personal data, shaped by the GDPR.⁹¹ Clear permission now gates how info moves across borders. Being open about what happens to details sits at its

⁸⁷ Justice K.S. Puttaswamy (Retd.) V. Union of India (2017) 10 SCC 1.

⁸⁸ Anvar P.V. V. P.K. Basheer, (2014) 10 SCC 473.

⁸⁹ Arjun Panditrao Khotkar V. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

⁹⁰ Avnish Bajaj V. State (NCT of Delhi), 150 (2008) DLT 769 (Del.).

⁹¹ Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 Apr. 2016 (General Data Protection Regulation).

core. Responsibility? That belongs squarely on companies using the data. Rules stretch far beyond Europe's edge.

Federal rules in America target distinct areas - banks, medical records, kids' online safety, and buyer rights - each under its own law. Yet strong digital shield systems exist alongside them.

Heavy fines hit those who break computer rules in the UK, thanks to laws like the Computer Misuse Act. Tough safeguards guard personal details under the Data Protection Act. Expert teams tackle online threats full time across dedicated security units.⁹²

India's laws have moved faster than many others, yet gaps remain in handling tech-heavy cases through dedicated courts. While rules on artificial intelligence slowly take shape, chasing online crimes across borders stays tricky. Building stronger digital evidence skills is still a work in progress. Getting agencies to sync up also proves difficult, even with new frameworks in place.

SUGGESTIONS AND RECOMMENDATIONS

To strengthen India's cyber legal framework, the following reforms are recommended:

- Enact a comprehensive Artificial Intelligence Regulation Act.
- Strengthen implementation of the Digital Personal Data Protection Act, 2023.
- Establish specialised cyber courts across all States.
- Increase investment in digital forensic laboratories.
- Working together across borders grows stronger when nations sign agreements on fighting online crime.
- Develop specialised training programmes for police officers, prosecutors, and judges.
- Promote nationwide cyber awareness and digital literacy campaigns.
- Strengthen CERT-In and institutional cyber incident response mechanisms.
- Introduce stronger regulatory oversight of cryptocurrency transactions.

Working together across government and business helps strengthen defences for essential services. When agencies team up with companies, systems stay safer during digital threats. Shared efforts mean stronger shields around power grids, hospitals, transport networks. Joint planning builds tougher responses to hacking risks. Cooperation spreads knowledge where it's needed most.

⁹² Computer Misuse Act 1990, c. 18 (UK); Data Protection Act 2018, c. 12 (UK).

CONCLUSION

The digital revolution has had a profound impact on the economic, social, and administrative landscape of India such that cyberspace has become a critical aspect of modern governance and business transactions. Nonetheless, growing reliance on digital technologies has also created a platform where cybercriminals can operate, hence, necessitating continuous legislative adaptations and preparedness.

While the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023 have provided a considerable legal framework for controlling cyber activities, technological developments have continued to evolve faster than existing legislations. Issues related to artificial intelligence, deepfake technologies, ransomware, cryptocurrency, cloud computing, and cross-border cybercrimes are some emerging legal issues which cannot be tackled solely by means of traditional regulation strategies.

For future cyber governance in India, technology neutral, rights-centric and internationally collaborative approach must be adopted. While legislative measures are necessary, special cyber courts, improved investigatory measures, digital literacy campaigns, privacy protection measures, and international collaboration are needed. For the development of a legal framework that is able to promote innovation while guaranteeing constitutional rights, national security, and digital rights at once, India requires this balanced approach.