INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 3 | 2026 Art. 1

Cyber Law and Data Protection with the Emerging Technology in India

Princy Yurembam
Research Scholar,
Department of Law, Dhanamanjuri University, Manipur

Dr. Yumkham Sarojbala
Assistant Professor,
Department of Law, Dhanamanjuri University, Manipur

Brahmacharimayum Debajit Sharma
Research Scholar,
Department of Law, Dhanamanjuri University, Manipur

Recommended Citation
Princy Yurembam, Dr. Yumkham Sarojbala and Brahmacharimayum Debajit Sharma, *Cyber Law and Data Protection with the Emerging Technology in India*, 5 IJHRLR 1-16 (2026).
Available at www.humanrightlawreview.in/current-issues/.

Cyber Law and Data Protection with the Emerging Technology in India

ABSTRACT

Cybercrime has evolved rapidly with significant rises in AI-driven exploitation and sophisticated social engineering. These crimes are causing reputational damage, financial loss, or psychological trauma to the victims. This often target vulnerable groups of the society such as women and children who fall into this trap as a victim such as deepfakes, cyberstalking, sextortion, defamation etc. Cyber law is fundamental component of data protection which provides the legal framework for how personal data is collected, stored and processed online to ensure privacy and security while prescribing penalties for data breaches. In India, IT Act, 2000 amended in 2008 is the legal framework governing cybersecurity and minimize cybercrime. Other provisions such as the Digital Personal Data Protection Act 2023 Act are used for proper prosecution and safeguards against cybercrimes in the country. This Act governed digital personal data processing, ensuring lawful use and user consent. It establishes the Data Protection Board of India to handle inquiries into data breaches and enforces accountability. Under the IT Act, 2000 also provides specific penalties for digital harassment, privacy violations such as Section 66E mention on violation of privacy, Section 67 mention on obscene material, and Section 67B mention on child abuse material. Under the BNS, 2023 which replaces the IPC also covers different forms of crimes such as cyber stalking (Section 78), Voyeurism (Section 77), etc. The topic will examine the evolving patterns of cybercrimes in society. It will aim to evaluate the legal framework in curbing rates of cybercrime and safeguard personal data to ensure digital education and awareness among individuals.

KEYWORDS

Cyber Crime, Penalties, BNS, Cyberstalking, Voyeurism.

INTRODUCTION

Internet usage has increased to a certain height with the rise of modern technology, and so cyber crimes and legal accountability. India is rapidly becoming a digitally driven society with online banking, e-commerce, remote work, cloud storage and digital communication now integral to everyday life. While these advancements have enhanced efficiency and connectivity, they have also significantly challenges concerning data privacy has also increased as well. In today's world where most of the

activities are done using internet from online shopping, online transactions, connecting people worldwide through social media, etc. Sometimes, using these without limitations and proper regulations lead to illegal activities affecting the individuals known as cyber crime. Due to the dynamic and emerging technological advancements, Indian cyber law is constantly evolving to a great height. The Council of Europe's Convention on Cybercrime (Budapest Convention) is one of the first treaty on Cybercrimes to improve cybercrime investigation and international coorperation. In India, we have the IT Act, 2000 amended in 2008 is one of the most important law on cyber crimes and electronic commerce. It is formulated with the Model Law on Electronic Commerce adopted by the the United Nation Commission on International Trade Law on 30th January, 1997.[1] Apart from this, the recent legislation law on data protection known as the Digital Personal Data Protection (DPDP) Act, 2023 represents India's first comprehensive framework for data privacy which balance an individual's right to protect the personal data with processing such data for lawful purposes. Thus, the cyber law and data protection law in India are not only for preventing cyber crimes but also for building trust, resilience and proper safeguards in the digital ecosystem.

OBJECTIVE

The objective of this paper is to give awareness and share knowledge on how to tackle against cyber crime affecting the individuals such as online harassment, child pornography, cryptojacking, stalking, email spoofing, etc. It will also try to study the gaps regarding enforcement, jurisdiction and cross boarder coordination for curbing cyber crimes in the country and to provide better understanding. On the present legislation such as IT Act, 2000, Digital Personal Data Protection Act of 2023, it is important in bringing innovative and inductive thinking to promote the development of security consciousness against cyber crime.

EVOLUTION OF CYBER LAW IN INDIA

With the spread of internet and other digital technologies, cyber law has developed globally. Before 2000, India didn't have any laws specifically for cyberspace. Instead, crimes were added to the Indian Penal Code (1860). India passed the Information Technology (IT) Act, 2000 which is based on the UNCITRAL Model Law on Electronic Commerce (1996). The main goal is to make electronic transactions legal and make e-governance easier. It also listed early cybercrimes, such as hacking and changing computer source code. The 2008 amendment

[1] *Convention on Global Cybercrime*, DRISHTI IAS (Nov. 23, 2019), https://www.drishtiias.com/daily-news-analysis/convention-on-global-cybercrime (Accessed on February 5th , 2026).

strengthened the act to a great extent by launching an arbitration for digital platforms and expanding its scope to include crimes such as cyber terrorism and identity theft.

India has also recently passed the Digital Personal Data Protection Act, 2023 for ensuring lawful transparent data collection and usage and safeguarding privacy rights. The idea of data privacy is an evolving fundamental rights guaranteed to every citizen of this country. In late 1984, privacy was legally acknowledged through the Universal Declaration of Human Rights (UDHR) under Article 12(4). Subsequently, in 1980, the Organisation for Economic Cooperation and Development (OECD) issued guidelines regarding privacy protection and the transborder movement of personal data. Nations began establishing their data privacy regulations as early as 1970 in Germany. The significant General Data Protection Regulation (GDPR) was implemented on May 25, 2018, transforming the laws surrounding data privacy and protection.[2] In India, privacy has been a contentious issue in the courts, with some considering it a fundamental right while others do not recognize it as a right under Article 21 of the Constitution. Ultimately, in 2017, the renowned case of K.S. Puttaswamy v. Union of India[3] declared the right to privacy as a fundamental right protected by Article 21. After seven years of efforts and three attempts to enact privacy legislation, India enacted a comprehensive data protection and privacy law on August 9, 2023.

UNDERSTANDING CYBER LAW AND DATA PROTECTION LAW

Cybercrime across India means illegal actions carried out using computers, networks, or digital devices. In India, there is no single statutory definition for "cybercrime" which expressely mentioned. Instead, it is defined conceptually through a combination of various legislation such as Information Technology (IT) Act, 2000, the Bharatiya Nyaya Sanhita (BNS), 2023, Digital Personal Data Protection Act, 2023.

In simple term, cybercrime is any unlawful activities committed where a computer, network, or communication device is used as:

1. A tool used to commit crimes such as phishing, financial fraud).
2. A target as the object of the crime such as hacking, spreading viruses).

[2] Sneha Mahawar, *Data Protection and Data Privacy Laws in India*, iPleaders (Feb. 2, 2024), https://blog.ipleaders.in/data-protection-laws-in-india-2/(Accessed on February 5th, 2026)
[3] Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) 10 SCC 1

3. A repository which is used to store illegal information such as child pornography, stolen data).

So, Cyber law in India is about the rules that apply to the internet and digital communication. It is a set of laws that cover things like shopping protecting peoples personal information and stopping cybercrime. Cyber law deals with things like signatures, privacy and intellectual property rights on the internet. The main law that governs cyber law in India is the Information Technology Act, 2000 which is prominent in the entire Indian legal framework, as it directs the whole investigation process for governing cyber crimes[4]. This Act says that electronic transactions are legally valid and it sets punishments for people who commit cyber crimes.[5] The Information Technology Act helps to keep the internet and digital communication safe and secure. Cyber law in India is very important because it helps to regulate the use of electronic records and digital data. It plays an major role in keeping the internet safe for people in India against cyber crimes. On the other hand, data protection law creates the standard on how information must be guarded which act as a shield and mandates the organizations (Data Fiduciaries) to implement reasonable security safeguards to prevent unauthorized access. Digital Personal Data Protection Act, 2023 focuses on accountability of the data holder while cyber law focuses on the criminality of the data thief and provide criminal penalties including imprisonment and fines while Digital Personal Data Protection Act, 2023 provide civil penalties upto Rs 250 crore for failing to prevent a breach).[6]

- ***The Statutory Framework***

  With the new digital advancement in technology has reached to an extreme height, the need for an hour to regulate this legislations is necessary to mitigate cyber crime. Some of the legislations relevant with cyber laws are:

  a. **Information Technology Act, 2000 (Amended 2008):** The primary law dealing with cyber-offenses. It provides legal recognition for electronic transactions and prescribes penalties for digital offences.

[4] Nikunj Arora, *Cyber Crime Laws in India*, iPleaders: Blog (Apr. 28, 2022), https://blog.ipleaders.in/cyber-crime-laws-in-india/ (Accessed on February 7th 2026)

[5] Pramod Agrawal, Information Technology Act – 2000 (ITA-2K), C. & Auditor Gen. India, https://cag.gov.in/uploads/media/ (Accessed on February 10th, 2026).

[6] Ajay Gautam, *Data Protection Laws in India*, VIKASPEDIA (Jan. 30, 2026), https://en.vikaspedia.in/viewcontent/e-governance/digital-india/data-protection-and-privacy/data-protection-laws-in-india (Accessed on February 12th, 2026)

b. **Bharatiya Nyaya Sanhita (BNS), 2023:** This replaces the Indian Penal Code, 1860 and includes modern provisions for cyber-enabled crimes like digital forgery, online defamation and organized cybercrime.[7] The BNS modernises terminology and punishment while recognising cybercrime as a serious threat to national security, the economy, and individual rights

c. **Digital Personal Data Protection Act (DPDPA), 2023**: Focuses on the privacy and protection of data of every individuals imposing heavy penalties for data breaches. It aimed at ensuring protecting and securing personal and non-personal information of the citizens.

REASON BEHIND THE RISE OF CYBER CRIME IN INDIA

1. Increase of rapid digital transformation

India's digital growth has been a sprint, not a marathon. Millions of people got smartphones, computers and high-speed data before they were taught how to spot a scam. Because the "digital doors" opened so fast, many people forgot to put "locks" on them. India has witnessed a remarkable rise in internet penetration of rapid digital transformation in various sectors such as banking, e commerce, government services. Adopting digital platforms and rise of internet usage has created new opportunities for criminals to exploit and commit cyber crimes targeting vulnerable group of the society specially women and children.

2. The Convenience of Digital Cash

Apps like UPI (PhonePe, Google Pay) have made life incredibly easy for payment and online transaction of money, but they've also made stealing "frictionless." Scammers no longer need to physically rob someone; they just need to trick them into clicking a link or entering a PIN. Since the money moves instantly, it's often gone before the victim realizes it. Digital money is a virtual form of money without the need of physical money which are easy to transfer and faster way of transaction.

3. Using of AI

AI is the use of human like intelligence and mental process in an artificial device through the use of computational process. It is used

[7] Megha Rodrigues, *Offences Against Cybercrime under the Bharatiya Nyaya Sanhita, 2023 (BNS)*, Your Law Article (Feb. 20, 2026), https://www.yourlawarticle.com/post/offences-against-cybercrime-under-the-bharatiya-nyaya-sanhita-2023-bns (Accessed on February 20th, 2026)

to solve many difficult tasks at the short period of time. AI was first term by John McCarthy in 1956. AI algorithms have attracted in this fast changing world of technology in various sectors in the field of business, engineering, medicine, education, crime investigation, information retrieval, etc. Even though AI has provided a lot of benefits to people, sometimes misusing them may lead to many illegal activities. These days online scammers are using Artificial Intelligence to:

- **Clone Voices:** It is a technique used with the help of artificial intelligence to replicate a person's voice which enables criminals to create convincing, emotional and fabricated audio in order to manipulate the victims. It may lead to the risk of cyber frauds such as family emergency where scammers will clone a love one's voice to in order to create panic, calling family members to demand financial help such as car accidents, medical help, kidnapping, etc.

- **Deepfake Videos:** They are artificial image or videos that replaced a person's voice or images, videos which create highly realistic videos but fake ones. Sometimes using deepfake videos may lead to severe risks of scams, financial fraud, defamation, blackmail, identity theft etc. For example pretending to be police officers or bank managers on video calls. When technology makes a lie look like the truth, even smart people get fooled.

4. The "Ghost" Network

In cybercrime, the term ghost refers to several malicious or illegal activities platforms to deceived the person. They are coordinated clusters of fake or hijacked accounts used to distribute malware on trusted platforms. Criminals have built a massive "underground" system to stay invisible. They use:

- **Mule Accounts:** It is the used of bank accounts of unsuspecting people to funnel stolen money. They are bank or payment account used by criminals to move stolen money and hide its original source. It is essentially a middleman bank account. Instead of sending the stolen money directly into their bank account, they send it first to a mule account. So, the owner of the mule account then transfers the fund to another account or withdraws the cash to give to the criminals. For example, students, job seekers are targeted through online advertisements or fake job posting which promise them easy income with high paying jobs.

- **Remote Hubs:** Illegal call centers operations typically bypass Indian telecom regulations which facilitates various

cybercrimes in the country ranging from financial fraud, identity theft, spoofing to impersonate banks, government agencies or technical support entities.

5. Lack of "Cyber Knowledge"

With lack of digital awareness, it affect the vulnerable groups in the society such as women, children, etc who fall into the victim of cyber crime easily. Providing digital and cyber awareness is a must which can save the individuals from cyber criminals from committing online phishing, email spoofing, stalking, cyberstalking, defamation. And giving legal awareness on existing laws on cyber law and data protection law are important in combating cybercrime in the country.

INDIAN REGULATORY FRAMEWORK

1. Under the Indian Constitution

The Indian Constitution does not mentioned a clear definition on cyber law. However, it indirectly mentioned the right to privacy under Article 14 that is right to equality, Article 19 (1)(a) that is freedom of speech and Article 21 that is right to privacy recognized as a fundamental right and protecting personal data. In the case of *Justice K.S Puttaswamy v. Union of India*[8], the Court determined that privacy is a facet of human dignity. The right to privacy protects an individual to make personal decisions and manage important elements of their life.[9] Furthermore, it highlighted those personal relationships (marriage, reproduction, and family), along with sexual orientation, are fundamental to a person's dignity.

Additionally, the Court characterized discrimination based on sexual orientation as "profoundly disrespectful to dignity and self-esteem". It highlighted that the right to privacy lies at the crossroads of Articles 15 and 21 of the constitution, referencing its ruling in NALSA, which upholds the right to self-identification of gender. It expressed that the right to privacy represented personal autonomy, dignity, and identity.

Under Article 248 of the Constitution, mentioned about residuary power**.** The Union Government uses its residuary powers (under Entry 97 of the Union List) to legislate on IT and cybercrimes which is why the IT Act, 2000 is a central law. Under the Seventh Schedule, "Police"

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

[9] Oishika Banerji, *Right to Privacy*, iPleaders (Feb. 5, 2024), https://blog.ipleaders.in/different-aspects-of-right-to-privacy-under-article-21/ (Accesssed on March 5th, 2026)

and "Public Order" are State subjects. Therefore, the investigation and prosecution of cybercrimes are handled by state police departments.

2. Under Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 has replaced the Indian Penal Code, 1860 with effect from 1st July, 2023. It also mentioned the different forms of offences related to cyber crimes provisions. Here are some of the provisions highlighted with relevant to cyber crimes :

Sexual Harassment under Section 75

Sexual harassment are the unwanted, explicit sexual advances, physical contact, requests for sexual favors, showing pornography against a woman's will, or making sexually colored remarks. This criminal provision applies broadly to any setting, punishable by up to three years of rigorous imprisonment for physical advances/demands, or up to one year for sexual remarks.[10]

There are other relevant provisions such as:

- Voyeurism under Section 77
- Stalking under Section 78
- Organized crime under Section 111(1)
- Petty organized crime under Section 112(1)
- Defamation under Section 356
- Act endangering sovereignty, unity and integrity of India under Section 152
- Public servant framing an incorrect document with the intent to cause injury under Section 201

3. IT Act, 2000

To align with international developments, particularly the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996), India formulated the IT Act.[11] IT

[10] *Section 75 BNS: Sexual Harassment Law Meaning, Punishment & Complete Analysis*, TESTBOOK, https://testbook.com/judiciary-notes/section-75-bns (Accessed on March 16th, 2026).

[11] *Information Technology Act, 2000*, Lawctopus (Apr. 16, 2020), https://lawctopus.com/clatalogue/clat-ug/information-technology-act-2000/. (Accessed on April 2th, 2026).

Act, 2000 amended in the year 2008 is one of the most important legislation related to cybercrimes and electronic commerce. The Act primarily governs cyber activities such as legal recognition of electronic records, digital signatures and define various types of cyber offences and their relevant penalties.

The provisions of this Act oversee electronic commerce and punish cybercriminals from committing various cyber offences such as online harassment, stalking, email spoofing, defamation, child pornography, etc. The Act outlines the duties and obligations of intermediaries, along with the circumstances in which they can be relieved of liability. The Indian Computer Emergency Response Team (CERT-In) is India's national agency for cyber incident response, function and mandated by the IT Act, 2000. The Act grants legitimacy to electronic records and signatures used in commerce. The regulations of this Act ensure the protection of personal and sensitive data. It acknowledges and determines the validity of digital signatures.

With the advancement of technology, there is a need to acknowledge the necessity to update the Act to better fit societal requirements, leading to its amendment. The 2008 amendment introduced changes to Section 66A of the IT Act, 2000. This part specified consequences for distributing inappropriate messages online. This was the first significant shift . It changed the emphasis from "Electronic Commerce" to data privacy and cybersecurity. "Electronic Signatures" were substituted for "Digital Signatures" to accommodate with new emerging technologies. Section 66A was introduced which penalized sending "offensive" communications. The Supreme Court overruled this in 2015 (Shreya Singhal v. Union of India)[12] because it was too ambiguous and violated free speech. Section 43A was also added on data protection. It says to established corporate liability for neglecting to safeguard private information of an individual. The amendment additionally mentioned that if a company handles sensitive personal data negligently leading to wrongful loss for any individual, that company is held liable to compensate the affected person.

Some important sections of IT Act, 2000 are

- ***Section 66 of the IT Act 2000***

  When a person partake in any act specified in Section 43 with deceitful or fraudulent intent, he will face penalties. According to Section 66 of the IT Act 2000, this penalty can involve

[12] *Shreya Singhal v. Union of India* AIR 2015 SC (CRIMINAL) 834

incarceration for a duration of up to 3 years and a maximum fine of Rs. 5 lakhs, or either.

- ***Section 66B of the IT Act 2000***

  Section 66B details the penalties for unlawfully obtaining stolen computer resources or communication equipment. According to this section, any individual who intentionally obtains or keeps any stolen computer resource or communication device shall face imprisonment for a maximum of 3 years, or a penalty of up to Rs. 1 lakh, or either.

- ***Section 67A***

  It addresses the penalties for disseminating or sharing electronic content that includes sexually explicit activities. Upon first conviction, those who disseminate such content may be sentenced to prison for as long as 3 years and fined up to Rs. Five hundred thousand. For a 2nd or further conviction, the penalty could include imprisonment for as long as 5 years and a fine reaching up to Rs. 1000000.

- ***Section 67B of IT Act, 2000***

  It deals with the publication or transmission of electronic content that shows young children engaging in sexually explicit behavior. It states that anyone who electronically transmits or publishes any information concerning sexually explicit acts involving children will face maximum penalty of five years in prison and a fine of up to ten lakh on their first conviction.

- ***Section 66(A) of IT Act, 2000***

  It mention for the punishable offence of any person to send offensive information using a computer or any other electronic device. The Court struck down the provisions as unconstitutional and violation of free speech guaranteed under Article 19 (1) (a) of the Indian Constitution. The situation started after multiple people were detained under Section 66A of the IT Act, which punished anyone sending offensive messages through a computer or communication device. The clause faced criticism due to its ambiguous wording, especially the undefined phrases "offensive" and "menacing." This resulted in extensive abuse, with even benign content, like political commentary or jokes, being targeted.

Important Progress in the Context:

Section 66A: This regulation enabled authorities to penalize individuals for transmitting messages considered to be extremely offensive, threatening, or meant to provoke annoyance or insult.

Detentions and Disputes: Multiple arrests, notably of two women for sharing a Facebook post regarding a political figure's death, ignited public anger concerning the abuse of Section 66A.

Legal Challenge: These events led numerous individuals, civil society groups to contest the constitutionality of Section 66A. They contended that the clause was excessively ambiguous and unconstitutional limitation on free expression.

In *Shreya Singhal v. Union of India*[13], the petitioners contended that Section 66A infringed upon the fundamental rights assured by Articles 19(1)(a) (freedom of speech and expression) and Article 21 (right to life and personal liberty). They argued that the law was both ambiguous and had a chilling effect on free speech which allow for arbitrary arrests and the stifling of legitimate expression.

4. Digital Personal Data Protection (DPDP) Act, 2023

- ***Significance of DPDP Act, 2023***

The Digital Personal Data Protection (DPDP) Act, 2023 signifies a significant change in India's legal framework, transitioning from antiquated regulations to a strong system tailored for the current internet era. At its essence, the Act is founded on the principle of "Consent," that any organization gathering the data operates more as a trustee than as an owner. It encompasses all personal information gathered digitally or converted from offline records and it also extends beyond India's borders to make international companies responsible when they handle data of Indian citizens.[14]

It establishes particular roles: the Data Principal (the person whose data is being referred to) and the Data Fiduciary (the entity that determines the purpose and manner of data utilization). The Act also strongly focuses on Responsibility and Safety. Organizations must ensure the data they possess is accurate, safeguard it with adequate security measures to avert breaches and dispose of it once the

[13] *Shreya Singhal v. Union of India* AIR 2015 SC (CRIMINAL) 834.

[14] Ernst & Young, *Decoding the Digital Personal Data Protection Act, 2023*, EY (Aug. 2023), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023 (Accessed on April 25th, 2026).

particular purpose for its collection has been fulfilled.[15] In the event of a data breach, the company must legally inform both the impacted individuals and the newly established Data Protection Board of India (DPBI), which acts as the authority for resolving these issues. Specific safeguards are established for at-risk populations especially minors. The Act considers that children below 18 years requires parental consent prior to processing their data.

- ***Need for data protection law***

There is a need of data protection law in India which can be summarized as under:

a. Enforcement of fundamental right to privacy which also mentioned under Article 21 of the Indian Constitution.
b. Providing national security and cyber resilience in the era of increasing cyber warfare and data theft to mandate better security practice.
c. Providing economic growth and global alignment to build trust among countries where there is a need of multilateral treaties and cooperation to fight against cyber crimes. Outsourcing its legal standard must align with international frameworks like the EU's GDPR.
d. Maintain the children's privacy as children have become more active to digital platforms due to which there is demand for special laws and provisions in order to provide protection of their data.
e. It provides data ethics which means data collection are processed in ethical standards in fair, transparent data processing which should be non arbitrary and non discriminatory.

MEASURES TO REDUCE CYBER CRIME RATES WITH THE EMERGING TECHNOLOGY

- Awareness programs and educating women, children, elderly people on digital literacy.

- Organizing public campaigns, workshops on cyber security and data protection.

- Publish papers and organizing conferences, seminars on cyber laws and cyber security.

[15] *Data Protection Laws in India*, DLA Piper: Data Prot. Laws of the World, (February 13th, 2026) https://www.dlapiperdataprotection.com/?t=law&c=IN (Accessed on April 12th, 2026).

- Analyzing data on cybercrime reporting patterns and conducting surveys.

- Studying the impact on cybercrime specially in business sectors and government offices.

- Strengthening domestic laws such as IT Act, 2000 and DPDP Act, 2023 while fostering cross boarder judicial cooperation is essential to combat cyber crime and data protection.

CONCLUSION

With the rise and advancement in digital technology, many elements are appearing in the internet affecting children, women and other vulnerable groups in the society.. Internet and communicating device has become a tool of evil deeds that are exploited in various ways from child pornography, online stalking, email spoofing, web jacking, etc. With all these factors there is a need of an hour for proper regulation and monitoring the culprits who commit cyber crimes. The best way is to provide education and awareness on cyber crime, cybersecurity and data protection by providing digital literacy to every individuals. On the other hand public campains such as organizing workshops, online courses to educate people on phishing, scams and data protection is necessary in tackling against cyber crime.[16] To bridge this gap, future data protection strategies must move toward adaptive regulation and international harmonization of cyber laws. By strengthening the laws such as IT Act, 2000, DPDP Act, 2023 it will tackle against cyber crime to protect individual privacy against the encroaching risks of the digital frontier. Hence, proper law implementation and providing legal awareness on cyber laws can protect people from cyber criminals. Proper strategy on this existing laws is required to promote creativity, accountability and trust within the digital economy. India can strengthen its position as a digital leader worldwide, while protecting the rights and safety of its citizens in rapidly developed cyberspace due to institutional, technical and legal obstacles.[17]

REFERENCES

1. Abhishek Aggarwal et al., *A Legal Analysis of Emerging Threats of Cyber Crimes in India*, 14 Int'l J. Early Childhood Special Educ. 1186 (2022)

[16] Kaspersky, *What is Cybercrime? How to Protect Yourself*, Kaspersky (Mar. 23, 2026), https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (Accessed on April 16th, 2026)

[17] Pratik Yadav & Jully Garg, *The Emerging Information Technology and Cyber Laws: Issues and Challenges in India*, 2 Motherhood Int'l J. Rsch. & Innovation 89, 89–92 (2025)

2. Ajit Kumar et al., *Cyber Law and Digital Governance in India: Challenges and Emerging Trends*, 1 Int'l J. Advanced Dig. Sys. & Multidisciplinary Stud. 53 (2026)
3. Ananya Garg & Priyanka Jain, *UNCITRAL Model Law on Electronic Commerce*, iPleaders (2024), https://blog.ipleaders.in/model-law-on-electronic-commerce/.
4. Anoushka Soni, *Gimmicking the Gillick Test: Evaluating the Age of Consent Under India's DPDPA 2023*, IJLT Blog (2024), https://forum.nls.ac.in/ijlt-blog-post/gimmicking-the-gillick-test-evaluating-the-age-of-consent-under-indias-dpdpa-2023/
5. *Cyber Crime: How It Works and Its Types*, LEGAL SERV. INDIA, https://www.legalserviceindia.com/legal/article-17477-cyber-crime-how-it-works-and-its-types.html
6. *Data Protection Laws in India*, DLA Piper: Data Prot. Laws of the World, (February 13th, 2026) https://www.dlapiperdataprotection.com/?t=law&c=IN
7. Divya Singh & Rahul Kumar, *A Legal Analysis of Emerging Threats of Cybercrimes in India* (2023), Divya Singh & Rahul Kumar, *A Legal Analysis of Emerging Threats of Cybercrimes in India* (2023)
8. *Indian Computer Emergency Response Team (CERT-In)*, Drishti *IAS* (2026), https://www.drishtiias.com/daily-updates/daily-news-analysis/indian-computer-emergency-response-team-cert-in.
9. *Jurisdiction in Combating Cyber Crimes: Issues and Challenges Pornography and Indian Jurisdiction*, LEGAL SERVICES INDIA, https://www.legalservicesindia.com/article/1386/Issue-of-Jurisdiction-in-Combating-Cyber-Crimes:-Issues-and-Challenges-Pornography-and-Indian-Jurisdiction.html (last visited , 2023).
10. Lakshya Malhotra, *Digital Crimes and Modern Solutions: Addressing Cybercrime Under the Bharatiya Nyaya Sanhita*, 7 Indian J.L. & Legal R. (2025).
11. Mona Acharya, *IT Act 2000: Objectives, Features, Amendments, Sections, Offences and Penalties*, Cleartax (Apr. 17, 2024), https://cleartax.in/s/it-act-2000.
12. Naeem Allahrakha, *Balancing Cyber-security and Privacy: Legal and Ethical Considerations in the Digital Age*, 2023 Legal Issues in the Digital Age, no. 2, 78, 78–121, https://ouci.dntb.gov.ua/en/works/4VYBw2W7/.
13. Prashant Mali, *Important Cyber Law Case Laws in India*, CYBER LAW BLOG INDIA (May 16, 2017), https://www.prashantmali.com/cyber-law-blog-india/important-cyber-law-case-laws-in-india.
14. Press Release, Ministry of Home Affairs, Cyber-Crime Targeting Children (July 29, 2025), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2149788

15. Pratik Yadav & Jully Garg, *The Emerging Information Technology and Cyber Laws: Issues and Challenges in India*, 2 Motherhood Int'l J. Rsch. & Innovation 89, 89–92 (2025)

16. Rajbangshi et al., *Cyber Technology in the Postmodern Era and the Growing Significance of Its Accountability*, 3 CYBER L. REP. 4, Issue 4 (2024)
17. RBL Bank, *How to Report Cybercrime in India: National Portal Guide*, RBL Bank: Blog (Feb. 5, 2025), https://www.rbl.bank.in/blog/banking/safe-banking/report-cybercrime-india-national-portal
18. Santosh Kumar & Gagandeep Kaur, *Cyber Crimes and Laws* (Whitesmann, 2024)
19. Saraswat Pathak & Vir Vikram Bahadur Singh, *A Critical Study on Legal Framework of Cyber Law in India*, 7 IJFMR, no. 2, 2025, 1-8
20. Saroj Mehta & Vikram Singh, *A Study of Awareness About Cyberlaws in the Indian Society*, 4 Int'l J. Computing & Bus. Res. 1 (2013)
21. Satish Kumar, *Cyber Crimes Against Women In India: Types, Impact, And Legal Challenges*, 13 Int'l J. Creative Res. Thoughts m623 (2025)
22. Sneha Mahawar, *Data Protection and Data Privacy Laws in India*, ipleaders (Jan. 26, 2024), https://blog.ipleaders.in/data-protection-laws-in-india-2
23. Taxmann, *Overview of Digital Personal Data Protection Act (DPDP Act) 2023*, TAXMANN BLOG (May 4, 2025), https://www.taxmann.com/post/blog/overview-of-digital-personal-data-protection-act-dpdp-act
24. Lalit Kalra, *Decoding the Digital Personal Data Protection Act, 2023*, EY India (Nov. 21, 2025), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023
25. PMF IAS CA Team, *Cybercrimes in India: Current Status & Challenges*, PMF IAS (Jan. 20, 2026), https://www.pmfias.com/cybercrimes-in-india/.