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 CRIMES AND LEGAL REMEDIES

-Pracheeta Beck

The fast growth of the internet has changed the way people talk, study, work, buy things, make payments and use services. However, the same digital world has also created chances for activities. Cyber Crimes are actions where computers, phones, networks, digital platforms or electronic data may be used as a way of target or both. Unlike crimes, Cyber Crimes can be done from far away without being known and across different places making it hard to find and punish the people behind them.

Cyber Crimes in India include things like breaking into systems, stealing data, stealing identities, cheating, fake messages, following people online, spreading bad content, ransomware attacks and attacks on computer systems. Financial fraud has become very important because online payments and banking are part of life. The legal way to deal with this cannot depend on one law. It needs a mix of cyber laws, regular criminal laws rules for evidence and ways to protect data.

The main law in India for crimes is the *Information Technology Act, 2000*[1](IT Act). The situation has changed a lot since then. The *Bharatiya Nyaya Sanhita*, *2023*[2] took the place of the *Indian Penal Code* (IPC) from July 1 2024. It also deals with some crimes done using tools. So, the system for crimes in India uses both specific laws for technology and general criminal laws.

Cyber Crime does not mean one type of crime. It includes different illegal activities that use digital tools. Some crimes directly attack computer systems or data while others use tools to help with regular crimes. Breaking into computer systems changing data or destroying systems is covered by the *Information Technology Act*[3]. *Section 43*[4] deals with paying for damage when someone does these things without permission like breaking in, copying data,

[1] Information Technology Act, 2000, No. 21 of 2000, § 43 (India).
[2] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, India Code (2023), enforced July 1, 2024.
[3] Information Technology Act, 2000, No. 21 of 2000, § 43 (India).
[4] Id. § 43.

putting things in or breaking systems. If these acts are done with dishonesty or fraud then *Section 66* may cause problems.

Identity theft is another area. *Section 66C of the Information Technology Act*[5] makes it illegal to use someone's electronic signature, password or other login details for dishonest reasons. *Section 66D*[6] deals with pretending to be someone using a computer or phone. These rules are very important for profiles, fake accounts and online payment scams. The IT Act also deals with privacy and bad online content. *Section 66E*[7] is about breaking privacy by showing someone's parts without permission. *Sections 67, 67A* and *67B*[8] deal with sharing explicit or child abuse material online.

Cyber attacks can also target systems. *Section 70*[9] of the IT Act protects systems and *Section 70B*[10] creates the Indian Computer Emergency Response Team to handle cyber security issues.

Legal System That Deals with Cyber Crimes in India

The IT Act is the law for Cyber Crimes. It gives both criminal solutions. *Sections 43* and *43A*[11] are important for paying for damage and protecting computer systems and personal data. *Sections 66 to 67B*[12] create types of crimes.

The law has rules for government powers and what online companies must do. *Section 69* [13]allows checking, watching or decoding information in cases. *Section 69A*[14] gives a way to stop people from seeing information. These powers have to be used within the law and rules. *Section 79*[15] gives ways for online companies. It says that online platforms may host user content and get protection from being blamed for third-party content. The 2021 rules on companies add more duties.

At the time not every crime online is only covered by the IT Act. The *Bharatiya Nyaya Sanhita, 2023* (BNS) has parts that may apply when digital tools are used for crimes like cheating pretending to be someone forging or threatening. For example- *Section 318 of the*

---

[5] Information Technology Act, 2000, No. 21 of 2000, § 66C, Acts of Parliament, 2000 (India).
[6] Id. § 66D.
[7] Id. § 66E.
[8] Id. §§ 67, 67A–67B.
[9] Id. §§ 70.
[10] Id. §§ 70B.
[11] Id. §§ 43, 43A.
[12] Id. §§ 66–67B.
[13] Id. §§ 69.
[14] Id. §§ 69A.
[15] Id. § 79.

BNS[16] deals with cheating and *Section 319*[17] deals with pretending to be someone. So, an online money scam may involve both the IT Act and the BNS depending on the situation.

Cyber Fraud and Online Money Crimes

Online money fraud is one of the common types of Cyber Crime. Scammers may use messages, fake websites, pretending to be someone else, fake support teams or other ways to get banking details or trick people into sending money. The law to deal with this might use *Section 66D* of the IT Act when someone pretends to be another person using a computer or phone. The *Bharatiya Nyaya Sanhita* [18](BNS) parts about cheating may also apply when the rules of cheating are met. How fast the person who was hurt reports the crime matters a lot. Digital transactions leave records like details of the money, messages, account info and other online proof. Reporting quickly may help the people in charge find the money and keep the proof. Victims should keep the proof instead of deleting messages or records. Screenshots, transaction details, emails, web addresses and other info can help the people who look into the problem. The real proof and whether it can be used in court must follow the rules of proof.

Electronic Proof and Looking into the Crime

One problem with handling Cyber Crimes is finding, keeping and using electronic proof. Digital proof can be changed, deleted or moved quickly. So, the people who check need tech skills to find, keep and look at that proof.

The *Bharatiya Sakshya Adhiniyam, 2023*[19] (BSA) now deals with the rules of proof in India. It says that digital records count. The old rules about proof from the *Indian Evidence Act, 1872* (IEA) are still important for understanding how to use proof. In *Anvar P.V v P.K*[20] case, the Supreme Court said that electronic proof needs to follow the rules for it to be used. For *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*[21] case made it clear that some rules about proof must be followed when needed. The *Bharatiya Sakshya Adhiniyam* (BSA) has changed the rules for proof but the main idea is still important that is the digital proof must meet the rules for being real and allowed in court. This shows that winning a Cyber Crime case needs more than finding the person who did it. The people in charge must also show that the digital proof connecting the person to the crime is real and allowed by law.

---

[16] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318–319, Acts of Parliament, 2023 (India).
[17] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318–319, Acts of Parliament, 2023 (India).
[18] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, §§ 318–319, Acts of Parliament, 2023 (India).
[19] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, §§ 61–63, Acts of Parliament, 2023 (India).
[20] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[21] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Constitutional Rights and Cyber Crimes

Cyber rules must also match rights. The Constitution says people can speak and share ideas but only with some limits[22]. At the time, the Supreme Court says that privacy is a right under the Constitution. In a case the Supreme Court said that a part of the *Information Technology Act* (IT Act) was not allowed because it was not good for speech. This shows that fighting online behaviour cannot justify rules that are too vague or too strict. Another court decision said that privacy is a right. The ruling said that privacy is important because the Constitution gives people freedom. This becomes very important in the world, where a lot of personal info is collected, used and shared.

Data Protection and Cyber Security

Cyber Crimes are closely linked with keeping personal data safe. A data breach can show names, contact details, money info, passwords and other important details which could lead to identity theft or money fraud. The *Digital Personal Data Protection Act 2023* (DPDP Act or DPDPA) gives a way to handle data. The rules make sure that companies handling data have duties and people have rights about their data. The 2025 rules make the rules clearer. Data protection and Cyber Crime laws have related goals. Data protection laws make sure that personal data is used properly while criminal laws punish actions. Good cyber rules need both ways to stop problems and punish people.

A person who is hurt by a Cyber Crime may have options depending on what happened. First, the person can tell the police or the right Cyber Crime groups. A website lets people report crimes, including money scams. Reporting quickly is very important in money cases because helping early may help find and stop actions. Second, criminal cases may start under the IT Act, BNS or other laws. The exact crime depends on what the person did and what proof is available. Third, the person may get money back if the rules are met. The IT Act has rules that let people get money for actions that break into systems or data. Fourth, if there is online content the person can ask for it to be removed or blocked. This must follow the rules and what the online companies can do. Finally, civil help may be available if the online actions caused damage, hurt reputation, broke rights or other problems. The right solution depends on the facts and the rights that were broken.

[22] INDIA CONST. art. 19(1)(a), art. 19(2).

With many laws, fighting Cyber Crime is very hard. The first problem is where the crime happened. A crime may involve someone in one country, a person hurt in another and servers or companies in places. Old rules about who's, in charge can be hard to use. The second problem is keeping hidden. Criminals may use names, hacked accounts and smart tricks to stay hidden. The people who look into it may need help from internet companies, online platforms, banks and other countries. The third challenge is change. New ways of committing crimes appear faster than the laws can keep up. Artificial intelligence, deepfakes, automated scams and advanced phishing methods create new problems for the people who try to stop crime. Another challenge is literacy. Many Cyber Crimes work because people are tricked into giving away information or approving transactions. Legal enforcement needs to be supported by people knowing how to stay safe online, better security practices in organizations and better habits when using the internet.

CONCLUSION

India’s Cyber Crime plan needs to balance three goals: keeping people and organizations safe from threats, making sure that investigations and court cases work well, and protecting the rights that are in the constitution. Special teams that handle Cyber Crime need technology and people who know what they are doing. Police officers, people who bring cases to court and judges also need training about digital evidence and new types of Cyber Crime. More working together between the people who enforce the law, banks, tech companies and security groups can make things better.

Working with countries is just as important because crimes online often happen in more than one place. Ways to keep evidence safe and share it properly can help investigations go faster. Most important of all changes to the law should not favour any technology and should respect people’s rights. Laws need to be wide enough to deal with types of Cyber Crime but also clear enough to stop unfair use of the law.

Cyber Crime is one of the legal problems created by the way society has changed with technology. India’s laws have grown a lot through the IT Act, BNS, BSA, BNSS rules for service providers and laws to protect data. These laws offer ways to punish wrongdoers, give compensation, investigate and protect online rights.

Laws alone can't stop Cyber Crime. Getting help, keeping digital evidence safe, having experts who can look into these crimes, judges who understand technology and working together between different groups is needed. At the time, rules about the internet must respect

the rights in the constitution especially freedom to speak and privacy. The future of law is not just about making more rules or punishing people more. It is about building a system that works with technology and the law to protect people while keeping the internet open and free. As technology keeps changing India's cyber law must also change so that new ideas and more people using the internet come with responsibility, safety and good ways to fix problems.