InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-1 / January - 2026

Original Article

A Study on Cyber Laws and Cyber Security: A Review

Bharati V. Anantapur [1], Vrushali G. Borkar [2]
[1, 2] CES's Dr. Arvind B. Telang Senior College of Arts, Science and Commerce Pradhikaran, Nigdi Pune

Manuscript ID:
IBMIIRJ -2026-030103

Submitted: 06 Dec. 2025

Revised: 10 Dec. 2025

Accepted: 05 Jan. 2026

Published: 31 Jan. 2026

ISSN: 3065-7857

Volume-3

Issue-1

Pp. 10-14

January 2026

Correspondence Address:
Bharati V.Anantapur
CES's Dr. Arvind B. Telang Senior College of Arts, Science and Commerce Pradhikaran Nigdi Pune
Email: bharati.antp@gmail.com

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.18918066

DOI Link:
https://doi.org/10.5281/zenodo.18918066

Creative Commons

Abstract

Cyber law refers to legal concerns and regulations related to the internet and cyberspace. Cyber law governs computer technology, the internet, and communication. It covers the areas of intellectual property rights, data privacy, data protection, online transactions, e-contacts, cyber security and the prevention of cybercrime. Computers, smartphones, and the internet play a major role in our everyday lives these days. They facilitate rapid information retrieval, research, business, and interpersonal communication. People can easily share information, interact with anyone in the world, through an internet. But there are risks in addition to these advantages. Cyber threats such as hacking, identity theft, online fraud, and scams are becoming more dominant. These may be harmful to people, companies, and society. To protect people from these dangers, strong cyber laws and good cybersecurity systems are needed. The Information Technology Act, 2000 in India establishes guidelines for the safe use of computers, the internet, and digital services. It assists to prevent cybercrime and secure intellectual property and personal information. IT professionals are not the only ones who need to be careful when using digital devices. People should use secure software and passwords, understand about online safety, and follow regulations. The digital world is safer when safety precautions are taken, people are informed, and regulations are confidently imposed. Together, we can safely use technology for business, education, and communication. The paper aims to understanding of cyber laws and security in the digital age.

Keywords: *Internet, Cyber Laws, Cyber security, Unauthorized Access, Punishments.*

Introduction

The legal framework that governs actions in cyberspace is referred to as "Cyber Law." It can be easily defined as the laws controlling the digital world, despite the fact that it lacks a definitive definition. Cybercrimes, digital and electronic signatures, data security, privacy, and the responsible use of digital technologies are only a few of the many topics covered by cyber laws [1]. "Cyber" refers to anything that has to do with computers, information technology, or the internet, whereas "law" refers to the laws and regulations that govern social behaviour. Cybercrimes, online transactions, privacy difficulties, and intellectual property are just a few of the issues that are addressed by cyberlaw. Cybercrimes, which are illegal activities carried out over the internet or digital methods, are a crucial subject of cyber law [2]. Cyberlaw also deals with online harassment and cyberbullying, shielding people from dangerous online behaviours like defamation or threatening messages. For example, under cyber law, it would be deemed identity theft if someone stole personal information and used it for fraudulent reasons, such applying for loans in your name. In that case, you may file a lawsuit against the offender. In this way, cyber law provides a framework to maintain fairness, security, and privacy in the digital world, addressing the legal challenges posed by technology and the internet. The term "cyber security" refers to a collection of technological innovations, techniques, and procedures designed to protect computers, networks, programs, and related data against damage, destruction, or unauthorized access. Cyber security is crucial because it safeguards internet-connected devices that support a variety of activities used in progress, including trade, the availability of education for remote learning, social media, and global connections that allow people to exchange ideas and find opportunities in a variety of fields that are advantageous for development. This illustrates how the expansion of industries and job opportunities worldwide is facilitated by cybersecurity. There are many different types of cybercrimes, and cyber security becomes crucial in order to combat them.

How to cite this article:
Anantapur, B. V., & Borkar, V. G. (2026). A Study on Cyber Laws and Cyber Security: A Review. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(1), 10–14. https://doi.org/10.5281/zenodo.18918066

Cyberstalking, hacking, phishing, cybersquatting, ransomware and trojan assaults, malware, denial of service attacks, identity and data theft, password attacks, and many more are examples of these cybercrimes [3]. Cyber law establishes the legal structure for activities in cyberspace, while cybersecurity focuses on protecting computer systems, networks, and data from digital threats. The Information Technology Act, 2000 (IT Act), which grants legal status to digital signatures, electronic documents, and e-governance projects, forms the basis of cyber law in India. It supports the growth of e-commerce and online transactions by ensuring their legal validity. The Act also establishes sanctions for a number of cybercrimes, including identity theft, data theft, and hacking. The IT Act helps to build a safer and more reliable digital environment in India by bridging the gap between traditional laws and contemporary digital behaviours by addressing both legal recognition and cyber offenses [4].

Literature Review

Mohanty A: Cyber laws in India and around the world need to change as a result of the growth of digital services and resulting increase in cyber-related risks. Cyber law, which covers a broad range of legal issues related to information technology, cyber security, data protection, electronic commerce, and digital rights, is an essential area of legal study. Our understanding of how public law systems, like India's, have attempted to solve the difficulties brought up by cybercrime and internet governance has been aided by numerous researches. Dr. Gupta and Agrawal (2008) provide a comprehensive analysis of the Indian cyber law system in their essential work, Cyber Laws. They specifically focus on the Information Technology Act, 2000 (IT Act) and highlight how it was the nation's first legislative response to cyber concerns. They assess its scope, limitations on enforcement, and the role played by the government in promoting cyber hygiene. In a similar vein, K.M. Muralidharan and R. Singaravalan focus on how Indian courts have proven cybercrimes while analysing specific IT Act provisions in Law of Cybercrimes in India. They point out legal loopholes and recommend changes to make the law more understandable and useful in modern circumstances [5]. Roshmi Sarmah, Animesh Sarmah, etc.In this study work, the authors claimed that cybercrime is a set of behaviours that revolve around the illegal manipulation of computer data or systems and cannot be adequately described. Digital bias or information systems may be used as instruments, targets, or both in these activities. Electronic crimes, computer-related crimes, e-crime, high-tech crime, and information age crime are other names for cybercrime. Colourful conditioning, including online transactions, is carried out at the era of widespread internet use. Because of the internet's worldwide accessibility, anybody can access its resources from any location. Regrettably, some individuals use the internet for illicit activities, such as fraud and illegal network access. These illegal actions connected to the internet are collectively referred to as cybercrime. The idea of "Cyber Law" was presented in order to deal with and punish cybercriminals. The area of law that addresses legal matters related to the internet, cyberspace, and online conditioning is known as cyber law. Freedom of expression, internet access, application, online security, and privacy are just a few of the many themes it covers. In general, it refers to the regulations that control the internet. Cybercrimes have increased recently as a result of the emergence and widespread use of newly technology technologies. Protection against comparable crimes is crucial for any nation since cybercrime poses serious risks to society, culture, and security. The Act also modifies other existing laws, such as the Reserve Bank of India Act of 1934, the Indian Penal Code of 1860, the Indian Evidence Act of 1872, and the Banker's Books Evidence Act of 1891. Cybercrimes can originate from anywhere in the globe and pass public boundaries through the internet, making it difficult to investigate and carry out these crimes legally. To effectively tackle cybercrimes, international measures to harmonise legislation, coordinate conduct, and promote collaboration among governments are required [6]. M.P. Gupta and Jaijit Bhattacharya Cyber security is required to protect the expanding ICT. For crucial ICT systems that support the nation's governance framework, the expert commission should identify and provide an appropriate combination of outcomes [7].

Objective

The aim of this paper is to make the laws introduced by the government more accessible and understandable, especially those that deal with crimes and the punishments attached to them. By presenting the full scope of these legal measures, the study hopes to show how justice is enforced in practice. Alongside this, attention is given to the growing field of cyber security, highlighting the importance of protecting individuals and institutions in an increasingly digital world. Together, these discussions provide a clearer picture of how traditional law and modern security concerns intersect in shaping a safer society.

History of Cyber Law

Globally, cyber law, sometimes known as digital law, has developed in conjunction with the growth of digital technologies and the internet. The first focus of legal attention in the 1980s and 1990s was on controlling computer abuse and illegal access. With the commercialization of the internet in the late 1990s, nations realized they needed legal frameworks to deal with online data theft, hacking, cyberstalking, and cyber fraud. The Information Technology Act, 2000, which defined cybercrimes and gave legal status to electronic records and digital signatures, was a turning point in Indian history.

Cyber Laws and Cyber Security

1. **Cyber Law**

Cyber law encompasses the laws governing digital communications, the internet, and computer technology. It covers a wide range of topics, including online transactions, cybersecurity, cybercrime, intellectual property rights, data privacy, and data protection.

2. **Cyber laws cover following areas:**

Cybercrime – Cybercrime, encompassing illegal activities such as hacking, identity theft, online fraud, phishing, virus assaults, and ransom ware, is one of the topics covered by cyber laws.

Data Protection and Privacy: Data protection and privacy regulations, which protect sensitive and confidential information that is shared or stored digitally. Electronic and Digital Signatures – legal recognition of digital documents and authentication methods.

Intellectual Property Rights – Intellectual property rights, which safeguard digital assets such as multimedia, software, and pictures.

E-commerce Regulations: guidelines for conducting business and conducting transactions online.

3. **The Significance of Cyber Law**

Cyber law is crucial in this modern technological era. It is essential because it affects nearly every facet of transactions and activities that occur on the internet and other communication devices. Every action and reply in cyberspace has certain legal and cyber legal perspectives, whether we are conscious of it or not [8].

4. **Some significance of cyber laws:**

- **Protection against Cybercrime**: Cyber laws aid in the prevention and punishment of illicit actions such as virus attacks, identity theft, hacking, and online fraud.
- **Data Security and Privacy:** They ensure privacy by protecting sensitive and private information that is exchanged or stored digitally.
- **Legal Acceptance of Digital Transactions:** Online business transactions, electronic contracts, and signatures are all recognized under cyber laws.
- **Intellectual Property Protection:** They guard against illegal usage and piracy of software, digital content, and artistic creations.

Cyber Laws in India

The Information Technology Act of 2000 was enacted to address the growing problems in cyberspace and to establish a legal foundation for electronic business. The IT Act was required to control digital transactions and protect data security due to the growing reliance on computers, the internet, and other digital technologies [9].

1. **Important aspects of Indian cyber laws:**

- **Cyber-crime Prevention:** Cyber stalking, phishing, online fraud, hacking, identity theft, and malware distribution are all covered by laws.
- **Protection of Data and Privacy:** This safeguards private and sensitive data that is shared or stored digitally.
- **Electronic Signing and Digital Contracts:** Verifies online agreements and acknowledges e-signatures.
- **Intellectual Property Rights:** Prevents unauthorized use and privacy of software, digital content, and multimedia.
- **Cyber Security Measures:** Promotes knowledge of cyber threats and the safe use of information technology.
- **Violations and Penalties:** Describes penalties, such as fines and jail time, for cyber violations.

1. **Other related laws:**

- Indian Penal Code (IPC) provisions related to cybercrime
- Companies Act, 2013 (for corporate data security)
- Rules under IT Act, like the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

2. **Important Sections under the Information Technology Act, 2000 and Their Punishments**

- **Section 65:** Temporary use of computer-generated documents anyone who knowingly or purposefully destroys, hides, or modifies the source code of a computer, computer program, computer system, or computer network. Penalties: Anyone found guilty of such offenses faces a maximum penalty of three years in prison, a fine of two lakh rupees, or both.
- **Section 66:** Hacking with computer system, data alteration etc Anyone who intends to destroy, erase, or modify any information stored on a public or private computer, or who intends to cause any harm or damage. reduces its usefulness, values, or negatively impacts it in any way, including by hacking.

Penalties: Anyone found guilty of such offenses faces a maximum penalty of three years in prison, a fine of two lakh rupees, or both.

3. **Section 66A:** Harmful communications sent via any medium

- Unsettling or intrusive letters or information provided by a communication provider.
- Inaccurate or false information supplied with the goal of causing difficulties, discomfort, abuse, barriers, wounds, illegal intent, animosity, disgust, or malice.
- Posts or emails sent with the intention of deceiving the receiver or misleading them about where the messages came from Penalty: Violations of this provision may result in a fine and/or a maximum sentence of three years in jail.

4. **Section 66B:** obtaining or retaining any stolen processors, communication plans, or CPU resources with the intention of thinking they are identical.

Penalty: Those found guilty of such activities may face a fine of one lakh rupees, three years in prison, or both.

5. **Section 66C:** This section should be used to classify theft. It is illegal to steal a digital signature, PIN, or other distinctive identify from someone else.

Penalty: A conviction for such crimes may result in a fine of up to one lakh rupees and a three-year prison sentence.

6. **Section 66D – Personation-based fraud**
   - **Offense:** Fraudulently deceiving someone using a computer resource or network.
   - **Punishment:** Imprisonment up to 3 years and fine up to ₹1 lakh.
7. **Section 66E – Privacy Violation**
   - **Offense:** Capturing, publishing, or transmitting someone's private images without consent.
   - **Punishment:** Imprisonment up to 3 years and fine up to ₹2 lakh.
8. **Section 67 – Publication or Transmission of Obscene Content**
   - **Offense:** Publishing or sharing obscene content electronically.
   - **Punishment:** Imprisonment up to 3 years for first offense and fine up to ₹5 lakh;for repeated offenses, imprisonment up to 5 years and fine up to ₹10 lakh.
9. **Section 69 – Powers to Intercept Information**
   - **Offense:** Unauthorized interception or monitoring of digital information.
   - **Punishment:** As prescribed under the IT Act; strict legal action depending on the offense.

Cyber Security

Cyber security is defined as the process of preventing unauthorized access, abuse, and damage to manipulative networks, structures, dossiers, and certainties. It encompasses a wide variety of schemes, forms, and procedures designed to safeguard the uniqueness, probability, and completeness of mathematical properties. Cybersecurity necessitates stopping, identifying, and combating a variety of online threats, including as malware infections, taxicab attempts, dossier breaches, and other cybercrimes [10].

The significance of cyber security

- **Preserves Sensitive Data:** Cybersecurity prevents loss, theft, and illegal access to private, financial, and corporate data.
- **Prevents Cybercrime:** Assists in protecting against ransomware, malware, phishing, hacking, and other online assaults.
- **Guarantees Safe Online Transactions:** Prevents fraud in online payment systems, banking, and e-commerce.
- **Preserves Privacy:** Prevents misuse or leaks of organizational and personal data.
- **Promotes Business Continuity:** Prevents cyberattacks from interfering with digital operations.
- **Fosters Trust:** Guarantees that people and companies can utilize digital services and technology in a safe manner.
- **Preserves National Security:** Prevents cyberattacks on vital infrastructure, government networks, and private data.

Cyber security Techniques:

- **Password security and access control:** The idea of a user name and password has been a key component of data security. One of the initial steps in cyber security might be this.
- **Data authentication:** Before downloading any document we get, it must always be verified that it originated from a reliable source and hasn't been altered. These documents are often authenticated using anti-virus software that is installed on the devices. Therefore, a strong antivirus program is also necessary to keep the gadgets safe from malware.
- **Malware scanners:** This type of software typically checks all of the files and documents on the device for harmful viruses or malicious code. Malicious software programs, commonly referred to as malware, include Trojan horses, worms, and viruses. [11]
- **Firewalls:** A firewall is a piece of hardware or software that helps prevent viruses, worms, and hackers from using the Internet to access your computer. Every message that enters or exits the internet must go through the firewall in place, where it is reviewed and those that don't meet the security requirements are banned. Firewalls are therefore essential for identifying malware.
- **Anti-virus software:** An antivirus program is a computer program that finds, stops, and gets rid of dangerous software programs like viruses and worms. The majority of antivirus programs offer an auto-update feature that enables them to download fresh virus profiles so they may be scanned for as soon as they are found. Every computer system needs anti-virus software.

Conclusion

Cybercrimes have grown dramatically in recent years because to the quick development of technology. A nation's security, safety, and social well-being all depend on preventing these crimes. International cooperation and coordination are crucial since cybercriminals can commit crimes from anywhere in the world, transcending physical borders. To address these challenges, many nations have enacted stringent cyber laws with harsh penalties. This paper's primary goal was to educate readers about India's cyber laws and the significance of cybersecurity. People can defend themselves from digital risks and cybercrimes by being aware of these regulations and protective measures. In order for people, companies, and organizations to use technology responsibly and safely, it is essential to increase understanding of cyber laws and security measures.

Acknowledgment
The author sincerely expresses gratitude to the faculty members of CES's Dr. Arvind B. Telang Senior College of Arts, Science and Commerce, Pradhikaran, Nigdi, Pune, for their valuable guidance, encouragement, and continuous support during the completion of this research work.

Financial support and sponsorship
Nil.

Conflicts of interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Vivek Kumar and Guru Nanak Dev International Journal of Novel Research and Development¯ 2024 IJNRD | Volume 9, Issue 4 April 2024| ISSN: 2456-4184 | IJNRD.ORG
2. Bhavya, R. (2025). Introduction to Cyber Law and Understanding the evolution, scope, and significance of cyber law.Int J Criminol Criminal Law, 3(3), 01-05.
3. Abhijeet Deb, Cyber Crime and Judicial Response in India, 3 INDIAN J.L. & Just. 106 – 117, 107 (2012).
4. An Introduction to Cyber Law - I.T. Act 2000 (India) (slideshare.net)
5. Mohanty, A. (2011). New crimes under the Information Technology (Amendment) Act. Indian Journal of Law and Technology, 7, 103
6. Animesh Sarmah, Roshmi Sarmah, et.al., "A Brief Study on Cyber Crime and Cyber Laws of India" 4 International Research Journal of Engineering and Technology 1633-1640 (2017). 7. M.M. Chaturvedi, M.P.Gupta and Jaijit Bhattacharya "Cyber Security Infrastructure in India: A Study"pp.115
7. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 - 0056 Volume: 04 Issue: 06 | June - 2017 www.irjet.net p-ISSN: 2395-0072
8. Halder, D. (2011). Information Technology Act and cyber terrorism: A critical review. Cyber-crime and digital disorder, 75-90.
9. Atul Arun Patil: International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) ISSN (Online) 2581-9429 Volume 4, Issue 1, January 2024
10. Ansh Singh and Gulshan Kumar, : A Research Paper on Cyber Security: International Journal of Research Publication and Reviews journal homepage: www.ijrpr.com ISSN 2582-7421
11. Kuzior, A., Tiutiunyk, I., Zielińska, A.,& Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies, 17(2), 220- 239. doi:10.14254/2071-8330.2024/17-2/12
12. Singh, M., Husain, J. A., & Vishwas, N. K.(2014). A Comprehensive Study of Cyber Law and Cyber Crimes. International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), 3(2), 20-24.
13. Prateek Singh, Cyber Law in India: IT Act 2000, Legal Service India E-Law Journal
14. Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. International Journal of Enterprise Computing and Business Systems, January, Vol 2, Issue 1.
15. Mishra, A. et al. (2011, September). A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. In 2011 European Intelligence and Security Informatics Conference (pp. 286-289). IEEE.