



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.

NEED OF CYBER LAWS IN INDIA TODAY'S IN DIGITAL WORLD

- **SIDRA MALIK**

ABSTRACT

The rapid digitisation of modern society has made the internet an indispensable component of daily life, transforming fundamental sectors such as education, commercial transactions, banking, and entertainment. However, this extensive reliance on digital networks has brought significant security vulnerabilities, giving rise to a rapid surge in cybercrimes, including unauthorised system breaches, financial fraud, identity theft, and severe invasions of personal privacy. In response to these emerging digital threats, the establishment of a robust cyber jurisprudence becomes essential to maintain order, safeguard user rights, and regulate the virtual ecosystem.

of cyber laws in India, providing a structured analysis of the key statutory provisions under the IT Act, 2000—including Sections 66C (Identity Theft), 66D (Cheating by Impersonation), 66E (Privacy Violation), 69 (Government Interception), and Section 79 (Intermediary Liability). Furthermore, it examines key structural evolutions, such as the IT Amendment Act of 2008.

KEYWORDS: Cyber Law, IT Act 2000, Cybercrime, Digital Governance, Intermediary Liability, Data Privacy, UNCITRAL Model Law.

INTRODUCTION

Today, we can see that our day-to-day life is becoming increasingly dependent on the

internet. If we talk about education, it has become entirely internet-based. Shopping, too, has shifted online. Even if we look at digital payments, the traditional cash transactions have evolved, and almost all of our banking facilities are now internet-based. Consider entertainment: where there used to be massive movie theaters, we can now access all forms of entertainment right from the comfort of our homes through the internet. Therefore, the internet has become absolutely indispensable in modern times. All of these examples illustrate just how vital the internet has become, and looking further, countless other aspects of our lives are now completely dependent on it. Today, thinking about surviving or functioning without the internet is nearly impossible.

However, as our reliance on the internet grows, we observe that whenever something expands to this scale, it brings both advantages and disadvantages. While the internet is highly beneficial for us, it is simultaneously becoming a breeding ground for various negative consequences. Consequently, cyber offenses have begun to rise rapidly, such as cyber fraud and cyber stalking. Moreover, hacking has become rampant, where our phones and bank accounts are being compromised, and our privacy is constantly being breached. As these digital offenses continue to escalate, it has become imperative to find a way to curb them. To prevent and regulate such crimes, the absolute necessity for Cyber Laws emerged.

WHAT IS CYBER LAW

Cyber Law is a specialized branch of law that regulates and governs all essential activities, transactions, and aspects related to the internet and the digital world.

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.¹

NEED OF CYBER LAW

To curb offenses in today's digital world, the intervention of cyber law is absolutely indispensable. We are witnessing a massive surge in internet-based crimes, such as rampant cyber fraud and online cheating where perpetrators exploit victims remotely. Furthermore, obscenity and inappropriate content are spreading rapidly across platforms, necessitating cyber law to regulate and restrain them.

¹[Cyber Laws \(IT Law\) in India - GeeksforGeeks](#)

Our privacy is also under constant attack; today, nothing remains truly private, as we never know when our personal data might be extracted from our devices and gone viral across the internet. These are just a few illustrations among countless other digital crimes that desperately require legal regulation. As our dependency on the internet grows and we become increasingly habituated to it, cyber law becomes essential to ensure the technology is not misused. To steer society in the right direction, maximize the advantages of the internet, and place a strict check on its dark side, a robust legal framework like cyber law is the need of the hour.

THE IT ACT, 2000: INDIA'S CYBER LAW FRAMEWORK

To address the massive surge in various offences associated with cyber law, the Government of India drafted a new legislation in the year 2000, which we know as the Information Technology Act, 2000 (IT Act). Furthermore, keeping in view the evolving digital needs and contemporary challenges, significant amendments were also introduced to this Act in 2008.

The Information Technology (IT) Act, 2000 is the cornerstone of India's cyber jurisprudence. Enacted to provide legal recognition to e-commerce and govern the digital ecosystem, it outlines the rules, regulations, and penalties for the virtual world. Information technology Act, 2000 is based on UNCITRAL Model. The main purpose of this model is to make uniformity in E-commerce law of all country. On the basis of this model Indian government draft E-commerce bill in 1998 after amending this bill in 1999 this bill was presented in Parliament as Information Technology Bill 1999. On 9th June 2000 president of India gave its assent on this bill finally on 17th October 2000 it was enforceable in the whole of India.

Basically Information Technology Act, 2000 has 94 sections, 13 chapter and 4 schedules.

Here is a crisp breakdown of everything you need to know about the IT Act.

CORE OBJECTIVES

The main objectives of IT Act, 2000 is to provide legal recognition to all works which is based digital such as: Digital signature, Electronic signature E-contract And E-transaction etc.

Digital Authentication: Recognises digital and electronic signatures as legally binding.

Enables E-Governance: Allows government agencies to accept online filing, storage, and processing of official documents.

Combats Cybercrime: Defines and penalises virtual offences to protect internet users.

KEY PROVISIONS

1. LEGAL RECOGNITION FOR DIGITAL ACTIVITIES

Electronic Records & Signatures (Sections 3 & 5): Gives legal validity to digital contracts and electronic signatures, treating them at par with physical paperwork.

E-Governance Support (Section 4): Enables government departments to accept, file, and store official documents digitally.

2. PROTECTION AGAINST CYBERCRIMES

Unlawful System Access (Section 43): Requires offenders to pay financial compensation if they damage or access a computer system without authorization.

Hacking & System Interference (Section 66): Intentionally corrupting or altering someone else's system can result in up to 3 years in prison or a ₹5 lakh fine.

Identity Theft (Section 66C): Misusing another person's digital signature, password, or unique identification features carries a penalty of up to 3 years in jail.

Impersonation Scams (Section 66D): Cheating someone online by pretending to be someone else can lead to 3 years of imprisonment.

Violation of Personal Privacy (Section 66E): Capturing or sharing intimate images of a person without their explicit consent is punishable by up to 3 years in prison.

Publishing Obscene Content (Section 67): Circulating sexually explicit or offensive material online carries a 3 to 5-year prison sentence.

3. PROTECTION FOR ONLINE PLATFORMS (SECTION 79)

Safe Harbor Principle: Grants immunity to intermediaries (such as social media networks, ISPs, and search engines) for user-generated content, provided they comply with legal take-down requests promptly.

4. GOVERNMENT SUPERVISION & CONTENT BLOCKING

Data Interception (Section 69): Empowers authorities to monitor, decrypt, or intercept digital data to safeguard national security and public order.

Blocking Web Content (Section 69A): Allows the government to restrict public access to specific apps, websites, or online links in the interest of national sovereignty (e.g., app bans).

The EVOLUTION: IT AMENDMENT ACT, 2008

To keep up with changing technology, a major amendment was introduced in 2008.

It introduced Section 66A to 66F to address new-age cybercrimes.

It redefined "Digital Signatures" to "Electronic Signatures" to make the law technology-neutral.

It added specific provisions regarding corporate data protection and liability for data leaks.

CONCLUSION

In short we can say that According to increasingly use of internet the Indian government enacted the Information Technology Act,2000. This law prevent cyber crimes and punish those person who commit cyber crime. This law regulate the Cyber world.

References:

- Information Technology Act,2000
- [Cyber Laws \(IT Law\) in India - GeeksforGeeks](#)