NIILM University Shodh Manjusha: An International Multidisciplinary Journal

ISSN: 3049-2785 Vol.02, Issue 02, July- Dec 2025

Cybercrime and the Law: Emerging Challenges in the Digital Era

Kumar, Surender

Research Scholar, Department of Law, NIILM University, Kaithal

CITATION

Kumar, S., (2025). Cybercrime and the Law: Emerging Challenges in the Digital Era

Shodh Manjusha: An International Multidisciplinary Journal, *02*(02), 519–524.
https://doi.org/10.70388/sm250177

Article Info
Received: May 21, 2025
Accepted: July 23, 2025
Published: Nov 10, 2025

https://doi.org/10.70388/sm250177

Abstract

In today's rapidly digitizing society, cybercrime has emerged as one of the most pressing challenges for legal systems worldwide. Unlike conventional crimes, cyber offenses transcend geographical boundaries, exploit technological loopholes, and often outpace legislative responses. India, as one of the fastest-growing digital economies, faces unique legal and policy dilemmas in this sphere. The Information Technology Act, 2000, along with subsequent amendments, provides the primary framework for addressing cyber offenses in India. However, issues such as cross-border jurisdiction, weak enforcement mechanisms, and gaps in data protection legislation reveal significant limitations. Judicial interventions, including the Supreme Court's landmark judgment in Shreya Singhal v. Union of India (2015), highlight the tension between ensuring cybersecurity and safeguarding fundamental rights like freedom of expression and privacy. At the global level, conventions such as the Budapest Convention on Cybercrime and UN initiatives encourage harmonization, but India's cautious approach toward international treaties reflects concerns about sovereignty and adaptability to domestic needs. The interplay between domestic law and international cooperation therefore remains crucial. This paper seeks to explore these emerging challenges by analyzing the adequacy of existing Indian cyber laws, identifying shortcomings in enforcement, and evaluating the scope for legal reform. By situating the discussion in both national and international contexts, the research aims to highlight pathways for strengthening India's legal framework against the evolving threats of cybercrime while balancing constitutional rights and state security interests.

Keywords: Cybercrime, Cyber Law, India, Information Technology Act, Privacy, Jurisdiction, International Cooperation, Digital Era

Introduction

The digital revolution has transformed the way individuals, businesses, and governments operate, but it has also created unprecedented opportunities for criminal activity. Cybercrime today ranges from online fraud, identity theft, and ransomware attacks to sophisticated state-sponsored cyber espionage. Unlike traditional crimes, cyber offenses often transcend national boundaries, making investigation and prosecution a complex legal challenge.

In India, the rapid expansion of internet usage fueled by affordable smartphones and government-led initiatives like Digital India has significantly increased the country's exposure to cyber threats. The Information Technology Act, 2000, supplemented by various amendments, remains the principal legal framework governing cybercrimes. Yet, concerns persist about its adequacy in addressing modern threats such as data breaches, phishing scams, and misuse of artificial intelligence in cyberspace. Judicial pronouncements, particularly the Supreme Court's decision in Shreya Singhal v. Union of India (2015), reflect the tension between protecting national security and upholding constitutional guarantees like free speech and privacy.

Globally, efforts such as the Budapest Convention on Cybercrime seek to establish common legal standards and foster international cooperation. However, India's reluctance to accede to this convention demonstrates the ongoing struggle between global harmonization and the preservation of national sovereignty. As cybercrime continues to evolve, the pressing question for lawmakers and jurists is whether current legal systems both domestic and international are capable of providing effective protection without compromising fundamental rights.

This paper aims to explore these issues by situating cybercrime within the broader legal framework, analyzing India's domestic responses, and evaluating the need for stronger international collaboration.

Legal Dimensions of Cybercrime in the Digital Era

Cybercrime is a multifaceted challenge that tests the adaptability of both national and international legal systems. Unlike conventional offenses, cybercrimes are not confined by geography and can be committed with anonymity, making detection and enforcement particularly difficult. They encompass a wide spectrum from financial fraud, hacking, and identity theft to online harassment, cyberterrorism, and large-scale data breaches. Each of

these offenses raises questions about jurisdiction, evidence collection, privacy, and enforcement mechanisms.

In India, the Information Technology Act, 2000 forms the backbone of cyber law. It criminalizes unauthorized access to computer systems, identity theft, cyber fraud, and the publication of obscene material online. Amendments introduced after 2008 attempted to address issues such as cyber terrorism and data protection. However, rapid technological innovation, including the growth of artificial intelligence and the dark web, has exposed loopholes in the Act. For instance, while the law provides punishment for online offenses, it is less effective in tackling transnational crimes where offenders operate from jurisdictions outside India.

Internationally, the Budapest Convention on Cybercrime (2001) represents the first treaty aimed at harmonizing cyber laws and promoting cross-border cooperation. India has not signed the convention, citing concerns over sovereignty and the adequacy of its provisions to meet domestic realities. This reflects a broader dilemma: while cybercrime is global, legal responses remain largely national, creating enforcement gaps.

The judiciary in India has also played a key role in shaping cyber law. In Shreya Singhal v. Union of India (2015), the Supreme Court struck down Section 66A of the IT Act, emphasizing the need to balance cybersecurity with freedom of expression. More recently, debates on the proposed Digital Personal Data Protection Act, 2023 highlight how India is moving towards a more structured legal regime for data security and individual rights.

Thus, the legal dimensions of cybercrime lie at the intersection of criminal law, constitutional rights, and international cooperation. The pressing challenge is to evolve a framework that is not only effective in combating cyber threats but also consistent with democratic values and human rights protections.

Challenges in Regulating Cybercrime

Despite steady progress in legislation and enforcement, cybercrime continues to expose critical gaps in the legal and institutional framework. The challenges are both domestic and international, and they cut across issues of jurisdiction, privacy, enforcement, and technological adaptation.

1. **Jurisdictional Complexities-** Cybercrime often originates in one country, is executed through servers in another, and targets victims located elsewhere. This borderless

nature of digital offenses complicates prosecution. Indian authorities, for instance, frequently face hurdles in obtaining digital evidence stored on servers located in the United States or Europe. The absence of a comprehensive international treaty that includes India leaves law enforcement agencies dependent on slow and unpredictable channels such as Mutual Legal Assistance Treaties (MLATs).

2. **Outdated and Fragmented Laws-** The Information Technology Act, 2000, though a landmark in its time, has not kept pace with evolving cyber threats. While amendments in 2008 addressed cyber terrorism and data breaches, they did not anticipate crimes involving artificial intelligence, cryptocurrency, or the dark web. This creates a situation where criminals exploit grey areas while law enforcement struggles to find legal backing for prosecution.
3. **Privacy vs. Security Dilemm-** Balancing the right to privacy with the need for surveillance is another pressing challenge. Following the Supreme Court's ruling in Justice K.S. Puttaswamy v. Union of India (2017), which recognized privacy as a fundamental right, state surveillance practices have come under greater scrutiny. The push for stronger cyber laws must therefore reconcile security imperatives with constitutional freedoms.
4. **Weak Enforcement and Capacity Constraints-** Even where laws exist, enforcement remains weak. Many police forces in India lack specialized cybercrime units or trained digital forensic experts. Victims often report difficulties in filing cybercrime complaints, and delays in investigation reduce the chances of conviction. This undermines public confidence in the justice system's ability to address cybercrime effectively.
5. **International Cooperation and Sovereignty Issues-** Global cooperation is vital for combating cybercrime, but it remains limited by sovereignty concerns. India has refrained from signing the Budapest Convention on Cybercrime, citing the need for a treaty drafted under the United Nations framework rather than a regional initiative led by Europe. While this reflects legitimate sovereignty concerns, it also restricts India's ability to engage in real-time cross-border data sharing and investigation.
6. **Rapidly Evolving Technology-** The pace of technological advancement often leaves laws outdated. New threats such as ransomware-as-a-service, crypto-jacking, and AI-enabled deepfake crimes illustrate how cybercriminals adapt more quickly than

legislatures. This "cat-and-mouse game" makes it difficult for lawmakers to craft durable solutions.

Conclusion

The rise of cybercrime in the digital era highlights the growing tension between technological innovation and the law's ability to regulate it effectively. While India has taken important steps through the Information Technology Act, 2000 and recent initiatives such as the Digital Personal Data Protection Act, 2023, these measures remain limited in scope when compared with the complex and transnational nature of cyber threats. Courts, too, have played a vital role in balancing fundamental rights with security imperatives, but enforcement challenges, jurisdictional conflicts, and technological advancements continue to undermine the effectiveness of legal responses.

Internationally, efforts like the Budapest Convention on Cybercrime underscore the need for greater cooperation, yet India's cautious approach reflects an unresolved dilemma between global integration and national sovereignty. This reality underscores the urgent necessity for India to both strengthen its domestic legal framework and actively engage in shaping inclusive global norms on cybercrime.

Ultimately, the fight against cybercrime cannot be won through legislation alone. It requires a holistic strategy that combines robust laws, specialized enforcement agencies, international collaboration, and digital literacy among citizens. The law must evolve in step with technology, but in doing so, it must remain anchored in the principles of justice, human rights, and democratic accountability. Only then can states ensure that the digital revolution becomes a tool of empowerment rather than a weapon in the hands of criminals.

References:

1. Council of Europe. (2001), Budapest Convention on Cybercrime. https://www.coe.int/en/web/cybercrime/the-budapest-convention
2. *Digital personal data protection act*. (2023).
3. *Shreya Singhal versus Union of India*, (2015) Case text available at: https://indiankanoon.org/doc/110813550/.
4. *Justice K.S. Puttaswamy versus Union of India*, (2017). Case text available at: https://indiankanoon.org/doc/127517806/.
5. *Information technology act*. (2000).

Kumar, S.

6. Ministry of Electronics and Information Technology. India's digital initiatives and cybersecurity measures. *(MeitY)*. https://www.meity.gov.in/
7. Ministry of Electronics and Information Technology. *MeitY*. Digital India Programme.
8. Ministry of Home Affairs. National Cybercrime Reporting Portal. https://cybercrime.gov.in/
9. United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive study on cybercrime*.
10. Vishwanathan, A. (2021). *Cyber law: Indian and international perspectives*. LexisNexis.
11. Jha, D., & Khadelwal, J. (2025). Save life with AI. *Shodh Sari-An International Multidisciplinary Journal*, *04*(02), 282–290. https://doi.org/10.59231/sari7824