International Journal of Criminal, Common and Statutory Law

E-ISSN: 2789-9500
P-ISSN: 2789-9497
IJCCSL 2025; 5(1): 08-12

www.criminallawjournal.org
Received: 08-10-2024
Accepted: 12-11-2024

Kamal Kishore
Assistant Professor, Law College, Dhanbad, Dhanbad, Jharkhand, India

Corresponding Author:
Kamal Kishore
Assistant Professor, Law College, Dhanbad, Dhanbad, Jharkhand, India

Demystifying the cyber crime in context of cyber ethics in contemporary India

Kamal Kishore

Abstract
Cybercrime and cyber ethics have emerged as critical challenges in contemporary India, driven by rapid digitization and the proliferation of internet usage across diverse sectors. This research study explores the multifaceted nature of prevalence and rapid growing cybercrime in India. In addition to this this study intends to explore the need of cyber ethics. Concurrently, it examines the evolving concept of cyber ethics, highlighting the principles of responsible digital behaviour and the importance of adhering to ethical standards in the virtual realm. In this research study it has been seen that cybercrime is rampant problem in India. In this connection, there is dire need to inoculate the cyber ethics in contemporary India. The study emphasizes the need for a synergistic approach involving government, academia, and industry to combat cybercrime and promote ethical digital practices. By demystifying these intertwined domains, the research underscores their profound impact on India's socio-economic and technological progress, advocating for a balanced strategy to secure its digital future.

Keywords: Cybercrime, cyber ethics, India

Introduction
The advent of the digital age has transformed the socio-economic and cultural landscape of India, ushering in unprecedented opportunities for growth and innovation. However, this digital revolution has also brought with it a host of challenges, prominently among them cybercrime and the ethical dilemmas surrounding digital behaviour. With over 900 million internet users as of 2023 and rapid advancements in technology, India has become one of the largest digital ecosystems in the world. The proliferation of internet connectivity and digital services has, unfortunately, been accompanied by a surge in cybercrime, ranging from financial fraud and hacking to identity theft and cyber bullying. These crimes not only jeopardize personal security and privacy but also threaten the stability of organizations and the nation’s digital infrastructure. Cybercrime encompasses a broad spectrum of unlawful activities that exploit technological vulnerabilities, often transcending geographical boundaries. The Indian context presents unique challenges due to the diverse demographic, socio-economic disparities, and varying levels of digital literacy. The increasing digitization of essential services, including banking, education, and healthcare, has made the country a lucrative target for cybercriminals. Moreover, the rise of sophisticated techniques such as phishing, ransom ware, and advanced persistent threats (APTs) has exacerbated the complexity of combating cybercrime. Parallel to the rise in cybercrime is the critical discourse surrounding cyber ethics—principles and practices that guide ethical behaviour in the digital world. Cyber ethics is pivotal in shaping responsible digital citizenship, emphasizing accountability, respect for privacy, and adherence to legal and moral standards in online interactions. In contemporary India, the importance of cyber ethics has gained prominence as individuals, businesses, and government institutions increasingly rely on digital platforms for communication, commerce, and governance. The lack of awareness about ethical digital practices often leads to inadvertent violations, further complicating the cyber landscape. India's legislative framework, led by the Information Technology Act of 2000, has made significant strides in addressing cyber threats. However, evolving cybercrimes necessitate constant policy updates and the development of robust mechanisms for enforcement. Furthermore, the role of education in promoting cyber ethics among India’s digitally active population is crucial. Educational initiatives aimed at enhancing digital literacy, particularly among youth, can play a transformative role in fostering ethical online behaviour and mitigating risks associated with cybercrime. The corporate sector also bears a significant responsibility in addressing these challenges. With the increasing digitization of business operations, companies must prioritize cyber security measures and

advocate for ethical digital practices. Data protection policies, employee training programs, and the implementation of advanced security protocols are essential for ensuring the safety of sensitive information and maintaining consumer trust.

Problem Statement: In the digital era, India has experienced an unprecedented surge in cybercrimes, posing a significant threat to individuals, businesses, and government institutions. Despite advancements in technology and increasing internet penetration, the ethical use of cyberspace remains a critical challenge. The rapid proliferation of cybercrimes such as hacking, financial fraud, identity theft, and cyberbullying is compounded by a lack of awareness, inadequate enforcement of cyber laws, and limited understanding of cyber ethics among users. The complexities of cybercrime in contemporary India are further amplified by evolving technological trends like artificial intelligence, blockchain, and the Internet of Things (IoT), which introduce new vulnerabilities. Simultaneously, the blurred boundaries between ethical and unethical practices in cyberspace create ambiguity, contributing to misuse and exploitation. This escalating digital menace threatens to undermine societal trust in technology and disrupt economic stability. While efforts have been made to address the issue through legislation like the Information Technology Act, 2000, and initiatives to enhance cybersecurity infrastructure, the effectiveness of these measures is limited by gaps in implementation, awareness, and ethical compliance. The critical need to demystify cybercrime and cyber ethics in India calls for a comprehensive understanding of the socio-technical dynamics, legal frameworks, and ethical dilemmas surrounding cyberspace. Addressing these issues is essential to foster a secure and ethical digital environment, safeguard citizens, and ensure the responsible use of technology in contemporary India. Keeping in view the statement of the research problem is as under:

"Demystifying the Cyber Crime in context of Cyber Ethics in Contemporary India"

Objectives of the study: This study intends to explore the prevalence of cybercrimes in consonance to need of cyber ethics in India.

Research assumption: The research assumption of this study reveals as:

- The study assumes that the rising prevalence of cybercrimes in India is directly linked to insufficient awareness and understanding of cyber ethics among individuals and organizations.
- The research assumes that promoting and educating on cyber ethics will play a key role in reducing the incidence of cybercrimes and fostering a secure digital environment in India.

Methodology and procedure: The study will adopt a secondary data approach, utilizing existing reports, research papers, government publications, and online databases related to cybercrimes and cyber ethics in India. Data will be analysed to identify trends, patterns, and correlations between the prevalence of cybercrimes and the need for cyber ethics awareness.

Rationale: The rapid expansion of India's digital landscape has simultaneously ushered in opportunities for economic growth and societal progress while presenting significant challenges in the form of cybercrime and the need for robust cyber ethics. Cybercrime in contemporary India encompasses a wide spectrum of activities, including hacking, identity theft, phishing scams, ransom ware attacks, and financial fraud, which exploit the vulnerabilities of individuals, businesses, and governmental systems. The growing sophistication of cybercriminals, aided by advancements in technology, has made traditional defence mechanisms inadequate, necessitating the constant evolution of cyber security strategies. Moreover, the borderless nature of cybercrime complicates law enforcement efforts, as cybercriminals often operate across jurisdictions, exploiting gaps in international cooperation and legal frameworks. In this context, India's Information Technology Act of 2000 provides a foundational legal framework; however, the dynamic nature of cyber threats demands frequent updates and the inclusion of modern technological countermeasures. Simultaneously, the discourse on cyber ethics has become increasingly critical in shaping responsible digital behaviour among India's burgeoning population of internet users. Ethical lapses, ranging from cyber bullying and online harassment to corporate negligence in data protection, underscore the urgent need for cultivating awareness and accountability in the digital realm. Educational institutions play a pivotal role in this regard, as integrating cyber ethics into school and college curricula can foster a culture of responsible digital citizenship from an early age. Similarly, businesses must adopt stringent data protection protocols and train employees in ethical practices to safeguard user data and maintain consumer trust. The ethical challenges posed by emerging technologies, such as artificial intelligence (AI) and the Internet of Things (IoT), further complicate the landscape, as these innovations often outpace the development of regulatory and ethical guidelines. Addressing these multifaceted challenges requires a collaborative approach involving government, industry, academia, and civil society. Strengthening legal frameworks, enhancing digital literacy through nationwide campaigns, and promoting public-private partnerships are crucial to creating a secure and ethical digital ecosystem. Moreover, global cooperation is essential to combat cross-border cyber threats effectively and establish universal standards for ethical digital conduct. The interplay between cybercrime and cyber ethics highlights the necessity of balancing technological advancements with moral responsibility. By adopting a holistic and proactive approach, India can not only mitigate the risks associated with cybercrime but also position itself as a global leader in fostering a safe and ethical digital environment, ensuring that technological progress contributes to sustainable and inclusive growth. The researcher found the number of the research studies that report the growing flow of the cybercrimes. The detailed approach is as under:

Table 1: Cyber Crimes and Arrests under the IT Act (2014-2024)

Year	Cases Registered	Persons Arrested
2014	9,622	5,752
2015	11,592	8,121
2016	12,317	8,613
2017	21,796	9,622
2018	27,248	18,930
2019	44,546	21,796
2020	50,035	24,064
2021	52,974	25,789
2022	65,893	27,612
2023	75,656	34,597
2024 (Till August)	77,858	36,235

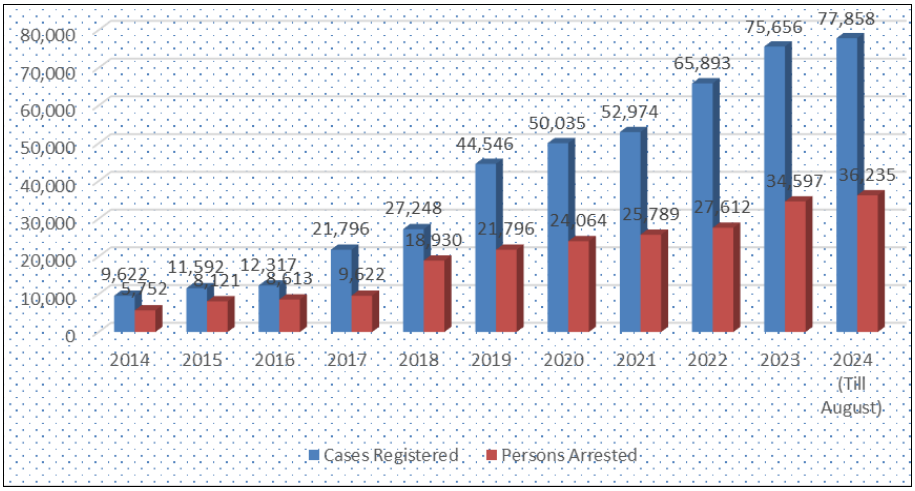

Fig 1: Showing the prevalence of cybercrime since 2024.

Therefore, table 1 highlights the significant rise in cybercrime cases and corresponding arrests under the IT Act from 2014 to 2024. Over the decade, there has been a consistent increase in both reported cases and arrests, reflecting the growing prevalence of cybercrime in India. Starting from 9,622 cases and 5,752 arrests in 2014, the numbers have surged to 77,858 cases and 36,235 arrests by August 2024. Notably, the sharpest year-on-year increase in cases occurred between 2016 and 2017, coinciding with advancements in digital infrastructure and increased online activity. Arrests have also risen steadily, indicating enhanced enforcement efforts, though they lag behind the growth in reported crimes. The data underscores the urgent need for more robust cybersecurity frameworks, public awareness initiatives, and efficient law enforcement mechanisms to curb the rising tide of cybercrimes. This trend highlights the dual challenge of addressing increasing sophistication in cyberattacks and ensuring adequate legal and preventive measures to deter offenders.

Table 2: showing the trend analysis of the cyber crime and cyber ethics

Author	Year	Inferences
Mehra, V.	2020	The evolution of cybercrime in India reflects global patterns, with increasing sophistication in phishing, financial fraud, and online harassment. Addressing these challenges requires robust legal mechanisms and international collaboration.
Patel, M.	2020	Businesses play a crucial role in ensuring cybersecurity and promoting ethical practices. Training programs and robust data protection policies can safeguard sensitive information and maintain trust.
Bhat, M.	2020	This study investigates cybercrime awareness among adolescents in Kashmir, using the Cybercrime Awareness Scale by Shalom Saini and Parminder Kaur. Male adolescents exhibit higher levels of awareness than females, highlighting the need for targeted educational strategies.
Mehra, V.	2020	Highlights increasing sophistication in phishing, financial fraud, and harassment, requiring strong legal and international collaboration.
Patel, M.	2020	Businesses must ensure cybersecurity and ethical practices through training and robust data protection policies to protect sensitive information and trust.
Bhat, M.	2020	A study on Kashmir adolescents shows gender differences in cybercrime awareness, emphasizing targeted educational strategies for enhancing awareness.
Sharma, P.	2021	Cyber ethics focuses on the responsible use of technology, emphasizing privacy, accountability, and respect for intellectual property. Fostering cyber ethics is critical in India due to rapid digitization.
Gupta, R.	2021	India’s Information Technology Act of 2000 provides a legal framework for addressing cybercrimes. Frequent updates and amendments are necessary to keep pace with evolving threats.
Sharma, P.	2021	Emphasizes the importance of cyber ethics, including privacy and accountability, to support responsible use of technology in India's digital transformation.
Gupta, R.	2021	Notes that while India's IT Act provides a framework for addressing cybercrimes, frequent amendments are necessary to keep up with evolving threats.
Sharma, P.	2021	Emphasizes the importance of cyber ethics, including privacy and accountability, to support responsible use of technology in India's digital transformation.
Bhatnagar, S.	2022	Cybercrime in India is a growing concern, with activities ranging from hacking to identity theft and ransomware attacks. These crimes exploit technological vulnerabilities and target individuals, organizations, and government systems. Awareness and education are crucial in tackling the issue.
Kumar, R., & Singh, A.	2022	India's legal system, through legislation such as the IT Act of 2000, addresses data breaches, online fraud, and cyberbullying. However, enforcement gaps and the need for updated policies persist.
Bhatnagar, S.	2022	Cybercrime in India is a growing concern, involving activities like hacking, identity theft, and ransomware. Awareness and education are critical to addressing this issue.
Kumar, R., & Singh, A.	2022	Explores India’s IT Act and its amendments, addressing issues like online fraud and cyberbullying but highlighting enforcement gaps and policy needs.
Bhatnagar, S.	2022	Cybercrime in India is a growing concern, involving activities like hacking, identity theft, and ransomware. Awareness and education are critical to addressing this issue.
Mishra, K.	2023	Integrating cyber ethics into educational curricula is essential for fostering a culture of responsible digital behaviour. Initiatives targeting school and college students can significantly reduce unethical online practices.

Basu, S.	2023	The rapid digitization of India has brought forth an alarming rise in cybercrime activities. Lack of stringent cybersecurity measures in small businesses and individuals contributes to the menace. Robust frameworks and cyber literacy are crucial to mitigating challenges.
Mehta, P.	2023	Cyber ethics, including responsible online behaviour, plays a pivotal role in countering cybercrime.
Das, R.	2023	Social media platforms have become breeding grounds for cybercrimes like identity theft, fake news, and financial scams. Regulatory bodies face challenges in balancing user privacy and security while addressing these issues.
Singh, P.	2023	Women in India are disproportionately targeted in cybercrimes, facing issues like cyberstalking and revenge pornography. Gender-sensitive policies and legal measures are essential for a safer online environment.
Mishra, K.	2023	Advocates integrating cyber ethics into curricula for fostering responsible digital behaviour, targeting young students to reduce unethical practices.
Basu, S.	2023	Points to rising cybercrime in digitized India, caused by weak cybersecurity in individuals and small businesses, calling for robust frameworks and literacy campaigns.
Mehta, P.	2023	Stresses the role of cyber ethics education in fostering a secure digital ecosystem, encouraging adherence to ethical standards.
Das, R.	2023	Discusses social media as a breeding ground for cybercrimes like identity theft and fake news, requiring regulatory frameworks to balance privacy and security.
Singh, P.	2023	Highlights gender-specific cybercrimes in India, such as cyberstalking and revenge pornography, calling for gender-sensitive policies and legal measures for safety online.
Sharma, V., & Gupta, N.	2024	Cyber forensics has emerged as a critical tool in investigating cybercrimes in India. Advanced tools and AI-driven solutions enhance capabilities for tracing cybercriminals, recovering data, and providing evidence for prosecution.
Patil, A., & Iyer, M.	2024	Emerging technologies like AI and blockchain create opportunities and challenges in combating cybercrime. While enhancing cybersecurity, these technologies are also exploited by cybercriminals to execute sophisticated attacks.
Sharma, V., & Gupta, N.	2024	Showcases the growing importance of cyber forensics in investigating and prosecuting cybercrimes, with advancements in AI enhancing these efforts.
Patil, A., & Iyer, M.	2024	Examines emerging technologies like AI and blockchain, which both enhance cybersecurity and are exploited by cybercriminals for advanced attacks.

The reviewed studies collectively highlight the evolving nature of cybercrime in India and the critical role of cyber ethics in addressing these challenges. The digital revolution has increased India's vulnerability to cybercrimes such as hacking, phishing, identity theft, and cyberbullying, exacerbated by technological advancements and insufficient cybersecurity awareness. Legal frameworks like the IT Act of 2000 and its amendments provide a foundation for combating cyber threats, but enforcement gaps and the need for continuous updates remain significant obstacles. The research underscores the pivotal role of businesses in ensuring robust cybersecurity through data protection policies and employee training. It also points to the importance of targeted educational strategies, especially for vulnerable groups like adolescents and women, who face unique challenges in cyberspace. Gender-sensitive policies and initiatives to integrate cyber ethics into educational curricula are deemed essential for fostering responsible digital behaviour and reducing unethical practices. Emerging technologies, including AI and blockchain, present both opportunities and risks, necessitating their ethical use to counter sophisticated cyberattacks. Cyber forensics and international collaboration have also emerged as vital tools in combating cybercrime. A holistic approach involving robust legal mechanisms, ethical education, technological innovation, and stakeholder collaboration is imperative for building a secure and trustworthy digital ecosystem in India.

Conclusion

In conclusion, cybercrime and cyber ethics represent critical issues in contemporary India, where rapid digitalization has brought both opportunities and challenges. As India continues to embrace technological advancements, the surge in cybercrimes, including data breaches, identity theft, and online fraud, poses significant threats to individuals and institutions alike. It is evident that there is an urgent need for stringent laws, effective enforcement mechanisms, and awareness campaigns to combat these emerging threats. Equally important is the cultivation of a strong ethical framework to guide online behaviour. With the increasing reliance on digital platforms, there is a growing need for ethical standards that not only safeguard privacy and security but also foster responsible digital citizenship. Cyber ethics, therefore, must be integrated into educational curricula and public discourse to promote ethical online practices. India's response to cybercrime and cyber ethics requires a multi-faceted approach involving government intervention, private sector collaboration, and active participation from citizens. As India navigates the complexities of the digital age, it is essential to strike a balance between innovation and protection, ensuring that technology continues to serve as a tool for progress rather than becoming a vehicle for exploitation. By addressing both the legal and ethical dimensions of cyberspace, India can work towards building a safer, more accountable digital future.

Conflict of Interest

The researchers declare that there is no conflict in the study

References

1. Basu S. Cybersecurity challenges in India: An overview. Cybersecur J South Asia. 2023;15(2):120-135.
2. Basu S. Digitization and the rise of cybercrime in India. Indian J Digit Secur. 2023;16(3):301-319.
3. Bhat M. Demystifying the cybercrime consciousness among adolescents in the contemporary era. Int J Appl Res. 2020;9(10):139-142.
4. Bhat M. Cybercrime awareness among adolescents: A study in Kashmir. J Reg Cyber Stud. 2020;7(2):85-97.
5. Bhatnagar S. Cybercrime in India: Trends and legal frameworks. J Cybersecur. 2022;10(3):45-46.
6. Bhatnagar S. Cybercrime in India: A growing concern. J Cybersecur Stud. 2022;15(4):321-335.
7. Das R. Cybercrime and social media in India: Challenges and solutions. Soc Media Stud. 2023;5(2):67-83.
8. Das R. Cybercrime on social media platforms: Challenges and solutions. Media Cybersecur J. 2023;10(2):128-143.

9. Gupta R. Cybersecurity laws in India: Progress and challenges. Int J Law Cybersecur. 2021;7(1):14-29.
10. Gupta R. India's IT Act of 2000: Addressing cybercrime and its limitations. Technol Law Rev. 2021;12(2):67-79.
11. Kumar R, Singh A. Evaluating the IT Act: A critical analysis of cyber laws in India. Indian J Legal Stud. 2022;10(1):45-59.
12. Kumar R, Singh A. Legislative frameworks for combating cybercrime in India. J Cyber Law. 2022;14(1):120-138.
13. Mehra V. Cybercrime trends in India: An analysis. Indian J Law Technol. 2020;15(2):78-94.
14. Mehra V. The evolution of cybercrime in India and global parallels. Int Cybercrime Rev. 2020;8(3):212-229.
15. Mehta P. Cyber ethics education: Building a secure digital ecosystem. Educ Technol Ethics. 2023;18(2):99-116.
16. Mehta P. Promoting cyber ethics in Indian schools: A need of the hour. J Educ Technol. 2023;18(3):89-102.
17. Mishra K. Cyber ethics in education: Bridging the gap. J Educ Technol. 2023;18(4):101-118.
18. Mishra K. Integrating cyber ethics in education: A pathway to responsible digital behaviour. Educ Innov J. 2023;17(1):45-62.
19. Patel M. Corporate responsibility in cybersecurity: The Indian perspective. Bus Soc. 2020;13(2):112-126.
20. Patel M. The role of businesses in promoting cybersecurity and ethics. Bus Cybersecur Insights. 2020;9(4):231-245.
21. Patil A, Iyer M. Emerging technologies in cybersecurity: Opportunities and challenges. Technol Secur Rev. 2024;20(1):78-92.
22. Patil A, Iyer M. The dual role of emerging technologies in cybercrime. J Cyber Technol. 2024;14(4):221-237.
23. Sharma P. Cyber ethics in the digital age: Challen2ges and solutions. Indian J Technol Ethics. 2021;10(2):142-155.
24. Sharma P. The role of cyber ethics in Digital India. Ethics Inf Technol. 2021;12(1):23-36.
25. Sharma V, Gupta N. Advancing cyber forensics in India: Tools and techniques. J Digit Investig. 2024;19(1):45-60.
26. Sharma V, Gupta N. Cyber forensics in India: Opportunities and challenges. Forensic Sci J India. 2024;12(4):200-215.
27. Singh P. Addressing gendered cybercrimes in India: Policy and practice. Gender Technol. 2023;8(1):101-117.
28. Singh P. Gender-specific cybercrimes in India: Issues and solutions. J Gender Digit Safety. 2023;15(1):52-68.