INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 3 | 2025 Art. 51

The Impact of Technology on Cybercrime

Khushi Upadhyay
Law Student, 5th Year, BA.LL.B. (Hons.),
Amity Law School, Amity University, Madhya Pradesh

Recommended Citation
Khushi Upadhyay, *The Impact of Technology on Cybercrime*, 4 IJHRLR 743-759 (2025).
Available at www.humanrightlawreview.in/archives/.

The Impact of Technology on Cybercrime

Khushi Upadhyay
Law Student, 5th Year, BA.LL.B. (Hons.),
Amity Law School, Amity University, Madhya Pradesh

Manuscript Received	Manuscript Accepted	Manuscript Published
30 May 2025	31 May 2025	01 June 2025

ABSTRACT

In the digital age, rapid technological advancement has transformed every aspect of human interaction, from communication and commerce to governance and education. However, this evolution has also led to an unprecedented rise in cybercrime, challenging traditional legal frameworks and demanding a robust data protection regime. Cybercrime, once limited to basic computer misuse, now encompasses complex offenses such as identity theft, ransomware attacks, deepfakes, and large-scale data breaches—all facilitated by technologies like artificial intelligence (AI), the Internet of Things (IoT), and cloud computing. This paper explores the intricate relationship between technology and cybercrime, with a focus on the adequacy and responsiveness of India's data protection laws.

The scope of the paper includes an analytical review of India's current legal mechanisms—particularly the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023—while also drawing comparative insights from international frameworks like the EU's GDPR and the California Consumer Privacy Act (CCPA). The research aims to examine legal gaps, assess enforcement challenges, and evaluate the judiciary's role in shaping data protection jurisprudence.

Key findings suggest that while India has made legislative progress, significant challenges remain in terms of enforcement, digital literacy, cross-border jurisdiction, and the ethical use of emerging technologies. The paper concludes that a multi-stakeholder approach—incorporating legislative reform, institutional strengthening, and international cooperation—is essential to address the growing threats posed by cybercrime and ensure robust data protection in an increasingly digital society

KEYWORDS

Cybercrime, Data Protection Law, Cybersecurity, Data Privacy

INTRODUCTION

The 21st century has witnessed a digital revolution that has reshaped how individuals, businesses, and governments operate. With the exponential growth of internet access, digital platforms, artificial intelligence, and mobile technologies, the world has become more interconnected than ever before. While these developments have enhanced communication, efficiency, and innovation, they have also created fertile ground for the rise of cybercrime.[1] Cybercrime has evolved from isolated incidents of hacking into a sophisticated, transnational phenomenon involving data breaches, identity theft, phishing, ransomware, cyberstalking, and financial fraud. Technology, while offering unparalleled convenience, has become a double-edged sword—facilitating both progress and criminal exploitation.

In India, the digital transformation has accelerated due to initiatives such as Digital India, the rise of fintech, and the growing reliance on digital infrastructure. However, this transformation has also exposed vast quantities of personal and sensitive data to vulnerabilities. In response, there has been an urgent need to implement robust data protection mechanisms to ensure the security and privacy of citizens. The enactment of the Digital Personal Data Protection Act, 2023 marks a significant step forward in this direction. However, gaps in enforcement, lack of digital awareness, and jurisdictional complexities continue to undermine efforts to combat cybercrime effectively.

This research seeks to explore the impact of emerging technologies on the nature and scale of cybercrime and to critically assess the adequacy of India's legal framework for data protection. The central questions guiding this study are:

1. How has technological advancement contributed to the evolution and sophistication of cybercrime in India?

2. Are India's existing data protection laws sufficient to address current and emerging cyber threats?

[1] Foundation, P. by India (2024) Digital Leadership for a Viksit Bharat 2047: Fostering Innovation, Shaping Tomorrow, India Foundation. Available at: https://indiafoundation.in/articles-and-commentaries/digital-leadership-for-a-viksit-bharat-2047-fostering-innovation-shaping-tomorrow/#:~:text=In%20an%20increasingly%20interconnected%20world,between%20urban%20and%20rural%20communities.

3. What reforms or strategies are required to strengthen legal and institutional responses to cybercrime?

The study adopts a doctrinal and analytical research methodology. It involves the examination of primary legal sources such as statutes, case laws, and government reports, as well as secondary materials like journal articles, comparative legal analyses, and cybersecurity studies. The paper draws on legal and criminological theories to contextualize the challenges posed by technology-driven cybercrime and evaluates the effectiveness of domestic and international regulatory frameworks.

The structure of the paper is as follows: The next section provides a conceptual and theoretical overview of cybercrime, highlighting its evolution alongside technological advancements. This is followed by an in-depth analysis of India's legal framework governing data protection, including key statutes and landmark judicial decisions. The fourth section identifies critical gaps and implementation challenges within the current legal system. The fifth section undertakes a comparative study of global data protection regimes to identify best practices. Finally, the paper concludes by offering legislative and policy recommendations to strengthen India's response to cybercrime and ensure data security in the digital era.

Through this research, the paper aims to contribute to the ongoing discourse on digital privacy, cyber regulation, and the legal reforms required to address the complex interplay between technology and crime in contemporary society.

LITERATURE REVIEW

Influence of Cyber Laws on Data Security: An Analysis[2]

The paper "Influence of Cyber Laws on Data Security: An Analysis" critically examines the framework of Indian cyber laws, focusing primarily on the Information Technology Act, 2000, and its role in protecting data security. It explores how the Act serves as the cornerstone for regulating cyber activities and combating cybercrimes such as unauthorized data access, hacking, identity theft, and data breaches. The study highlights the legal mechanisms incorporated within the Act, including provisions for penalties and adjudication processes designed to deter cyber offenses and provide remedies to affected parties.

The paper also addresses the dynamic nature of cyber threats that continue to evolve with rapid technological advancements,

[2] Law and Policy, Lex Scripta, 2023/01/01, INFLUENCE OF CYBER LAWS ON DATA SECURITY: AN ANALYSIS, VOL 1.

challenging the effectiveness of existing laws. It emphasizes that while the IT Act was pioneering legislation for its time, new forms of cybercrime, driven by technologies like AI, IoT, and cloud computing, demand continual updates and a more robust legal framework. Furthermore, the study underscores the need for increased awareness and cyber literacy among users to enhance data protection at the grassroots level.

An Analysis of Cyber Laws with Focus on Data Protection in India[3]

The study "An Analysis of Cyber Laws with Focus on Data Protection in India" offers a comprehensive overview of the country's cyber legal framework, emphasizing its role in safeguarding data privacy and combating cybercrime. The paper traces the development of Indian cyber laws, starting with the Information Technology Act, 2000, which laid the foundation for regulating electronic transactions and offenses related to digital data. It highlights key provisions that address unauthorized access, data breaches, and cyber fraud, reflecting India's initial steps toward legal recognition of data protection.

The study further examines the effectiveness of these laws in the context of rapid technological advancements and increasing cyber threats. It identifies several challenges, including ambiguities in legal definitions, inconsistent enforcement, and inadequate mechanisms for protecting personal data, which limit the current framework's efficacy. Particular attention is given to the evolving status of the Personal Data Protection Bill, 2019, which proposes a comprehensive legal structure to regulate the collection, processing, and storage of personal data, aiming to align India with global data protection standards.

Moreover, the paper suggests legislative reforms and policy measures necessary to strengthen data privacy protections, enhance enforcement capabilities, and promote cyber literacy among users. It argues that fostering public-private collaboration and investing in technological infrastructure are crucial to effectively address emerging cyber threats.

Cybercrime in the Digital Age: Challenges and Legal Gaps in India's Data Protection Framework

The research paper "Cybercrime in the Digital Age: Challenges and Legal Gaps in India's Data Protection Framework" explores the increasing complexities of cybercrime in India's rapidly digitizing environment. It identifies significant challenges posed by evolving

[3] An Analysis of Cyber Laws with Focus on Data Protection in India: Issues, Challenges, and Opportunities, Available at: https://www.juscorpus.com/wp-content/uploads/2024/02/59.-Vidhi-Singh.pdf.

cyber threats, including hacking, identity theft, and data breaches, which exploit weaknesses in existing laws. The study critically analyzes the gaps and limitations within India's current legal framework, such as outdated provisions in the Information Technology Act, 2000, lack of comprehensive data protection legislation, and insufficient enforcement mechanisms. It highlights the absence of clear guidelines on consent, data fiduciary responsibilities, and cross-border data transfers. The paper strongly advocates for the enactment and implementation of a robust, comprehensive data protection law to address these shortcomings effectively. Additionally, it underscores the importance of increased cyber literacy, enhanced technical capacity of enforcement agencies, and coordinated efforts between stakeholders to create a secure digital ecosystem. The study concludes that legal reforms are essential to protect citizens' data privacy and combat cybercrime in the digital age.

Cyber Law and Data Privacy in the 21st Century: Emerging Legal Issues and Challenges

The paper "Cyber Law and Data Privacy in the 21st Century: Emerging Legal Issues and Challenges" examines the evolution of India's cyber legal framework, beginning with the enactment of the Information Technology Act, 2000. It highlights how the Act was a pioneering effort to address electronic commerce and cyber offenses but now faces challenges due to rapid technological changes and emerging cyber threats. The study discusses key legal issues related to data privacy, such as the protection of personal data, consent mechanisms, and data fiduciary obligations, which remain inadequately addressed under current laws. It emphasizes the growing need for comprehensive and updated legislation to keep pace with advancements in technologies like artificial intelligence, cloud computing, and the Internet of Things (IoT). The paper also underscores the importance of balancing innovation with privacy rights and suggests reforms to strengthen enforcement and promote cybersecurity awareness. Ultimately, it calls for a dynamic legal approach to safeguard data privacy in the evolving digital landscape.[4]

Assessing Cyber Security and Data Protection Laws: A Comparative Study

The paper "Assessing Cyber Security and Data Protection Laws: A

[4] Cyber Laws and Recent Developments, Khurana and Khurana. Available at: https://www.khuranaandkhurana.com/2025/02/21/cyber-laws-and-recent-developments/#:~:text=The%20ever%2Devolving%20cyberspace%20itself,Khurana%2C%20Advocates%20and%20IP%20Attorney.&text=https://iclg.com/briefing,%2Dspace%2Din%2Dindia.

Comparative Study" provides a detailed comparison of cybersecurity and data protection legal frameworks in India and several other countries, including the European Union, the United States, and Singapore. It evaluates the strengths of India's current legal regime, notably the Information Technology Act, 2000, and the recent Digital Personal Data Protection Act, 2023, while highlighting critical gaps such as limited enforcement capacity, ambiguities in data fiduciary responsibilities, and insufficient provisions addressing emerging technologies. The study contrasts these with global standards like the European Union's GDPR, California's CCPA, and Singapore's PDPA, which offer more comprehensive data protection, clearer guidelines on consent, and stronger mechanisms for cross-border data flow management. The paper identifies areas where India can improve, including stricter enforcement measures, enhanced regulatory oversight, and promoting cybersecurity awareness and digital literacy. Additionally, it emphasizes the importance of harmonizing India's laws with international standards to facilitate global cooperation in combating cybercrime. The study concludes by recommending legislative reforms and public-private partnerships as essential steps toward strengthening India's cybersecurity and data protection landscape.

Cybercrime and Its Legal Implications: Analyzing the Challenges and Legal Gaps[5]

The research paper "Cybercrime and Its Legal Implications: Analyzing the Challenges and Legal Gaps" explores the multifaceted nature of cybercrime in India, highlighting significant legal and practical challenges that hinder effective enforcement. It focuses on jurisdictional complexities arising from the borderless nature of cyber offenses, which complicate investigations and prosecution due to conflicting laws and limited international cooperation. The study also discusses privacy concerns linked to digital surveillance and data protection, emphasizing the tension between law enforcement needs and individual rights. Furthermore, it addresses the difficulties related to the admissibility and integrity of digital evidence in courts, pointing out inconsistencies in legal standards and procedural safeguards. The paper critically analyzes existing legislation, including the Information Technology Act, 2000, and relevant judicial precedents, revealing gaps that undermine the effectiveness of India's cybercrime regime. It calls for comprehensive legal reforms aimed at clarifying jurisdictional

[5] Boruah, J. (2021) Cyber Crimes and Its Legal Challenges in India, SSRN. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3819497#:~:text=Abstract,regulating%20cyber%2Dcrimes%20in%20India.

authority, strengthening data privacy protections, and establishing clear protocols for digital evidence handling. Additionally, the paper advocates for capacity building within law enforcement and judiciary to better tackle the evolving landscape of cybercrime. Ultimately, it stresses the urgent need for a cohesive and adaptive legal framework to address India's growing cybercrime challenges.

THEORETICAL AND TECHNOLOGICAL CONTEXT

Evolution of Cybercrime with Technology

Cybercrime refers to criminal activities that are carried out using computers, networks, or digital technologies. As societies have become increasingly digitized, the scope and sophistication of cybercrime have expanded dramatically. Traditionally, cybercrime encompassed basic offenses such as unauthorized access to computer systems (hacking) and the spread of malicious software (viruses). However, in recent years, the landscape has evolved to include a diverse range of offenses, including phishing, identity theft, ransomware attacks, financial fraud, cyberstalking, and crimes involving the dark web.[6]

The emergence of advanced technologies has been a double-edged sword. The internet, while revolutionizing access to information and communication, has become a primary medium for cybercriminals to operate anonymously and across borders. Phishing attacks, which involve tricking individuals into revealing sensitive data, have become increasingly sophisticated with the use of social engineering and spoofed domains. Ransomware—malicious software that encrypts a victim's data and demands payment for its release—has evolved into a profitable business model for organized cybercriminal networks.

Emerging technologies like Artificial Intelligence (AI), the Internet of Things (IoT), and mobile devices have further complicated the cyber threat landscape. AI enables criminals to automate phishing attacks and generate deepfake content for impersonation and fraud. IoT devices, often deployed with minimal security protocols, serve as vulnerable entry points for attackers into home and business networks. Mobile technology has facilitated crimes such as SIM swapping, mobile banking fraud, and the distribution of illicit content through encrypted apps. Thus, technological advancements, while beneficial, have significantly contributed to

[6] University, E.-C. (2024) What Is Cybercrime and What Are It's Different Types, eccuedu. Available at: https://www.eccu.edu/blog/cybersecurity/what-is-cybercrime-types-examples-and-prevention/.

the escalation and complexity of cybercrime.

Theoretical Frameworks

Understanding the relationship between technology and cybercrime also requires a theoretical foundation. Criminological theories provide insights into why individuals commit cyber offenses and how opportunities created by technology influence criminal behaviour. The following frameworks are particularly relevant:

Routine Activity Theory (RAT)[7]

Proposed by Cohen and Felson, RAT posits that crime occurs when three elements converge: a motivated offender, a suitable target, and the absence of capable guardianship. In the cyber context, routine digital activities (e.g., online shopping, banking, and social networking) create numerous opportunities for offenders. The internet facilitates anonymity and reduces the risk of detection, while personal data shared online often lacks adequate protection, making individuals ideal targets. The absence of real-time enforcement or "guardianship" online—such as cybersecurity protocols or legal oversight—enables such crimes to flourish.

Deterrence Theory

Deterrence theory suggests that individuals are less likely to commit crimes if the perceived risks of punishment are high. In the realm of cybercrime, this theory highlights the importance of effective enforcement and stringent legal consequences. However, cybercriminals often perceive low risks due to cross-border jurisdictional issues, the lack of technical expertise in law enforcement, and the time-consuming nature of digital investigations. As a result, the deterrent effect is diminished, emphasizing the need for stronger regulatory mechanisms and international cooperation.

Opportunity Theory

This theory argues that crime results from opportunities created by specific circumstances. Technology itself provides the means, anonymity, and access to commit crimes without physical interaction. For example, e-commerce platforms create opportunities for credit card fraud; cloud storage services, if inadequately secured, present chances for data theft; and AI tools

[7] Wickert, C. (2020) Routine Activity Theory (RAT), SozTheo. Available at: https://soztheo.de/theories-of-crime/rational-choice/routine-activity-theory-rat/?lang=en.

can be misused for creating fake identities or automating cyberattacks. The accessibility of digital tools and the low cost of executing cybercrime increase its appeal, particularly to young, tech-savvy individuals who may not view their actions as "real crime."

These theories collectively underscore that cybercrime is not solely a technological problem but also a sociological and psychological one. The motivations, ease of access, and perceived impunity form a dangerous triad that fuels cybercriminal behaviour. Understanding these dynamics is essential for developing comprehensive legal and policy responses that address not only the symptoms but also the root causes of cybercrime.

By integrating these theoretical perspectives with technological realities, the paper aims to construct a nuanced understanding of the cybercrime phenomenon and its legal implications.

LEGAL FRAMEWORK FOR DATA PROTECTION IN INDIA

The protection of personal data and digital privacy has emerged as a critical aspect of law in India, particularly in the context of rising cybercrime. The legal framework governing data protection has evolved gradually, moving from rudimentary provisions in the Information Technology Act, 2000 to the enactment of the Digital Personal Data Protection Act, 2023, which marks a significant step towards comprehensive data governance. This section outlines the evolution of data protection laws in India and examines judicial interpretations that have shaped the legal landscape.[8]

Current Data Protection Laws in India

Information Technology Act, 2000 and its Amendments

The Information Technology (IT) Act, 2000 was the first legislation in India to address cyber-related offenses. Although primarily focused on e-commerce and legal recognition of electronic records and digital signatures, it contains certain provisions related to data protection and cybersecurity. Sections 43A and 72A of the Act impose liability on companies and individuals for negligent handling and disclosure of sensitive personal data. Under Section 43A, a corporate body handling personal data is liable to pay compensation if it fails to implement reasonable security practices. Section 72A provides for criminal punishment in cases where personal information is disclosed without consent and in

[8] University, N. and Administrator (2024) Data Privacy Protection in India, Institute of Law. Available at: https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/.

breach of lawful contracts.

Personal Data Protection Bill, 2019

To address these gaps, the Personal Data Protection Bill, 2019 was introduced following the recommendations of the Justice B.N. Srikrishna Committee. The Bill sought to create a structured legal regime for the processing of personal data, modelled largely on the EU's General Data Protection Regulation (GDPR). It proposed the establishment of a Data Protection Authority, classification of data into personal, sensitive personal, and critical personal data, and mandated data localization for certain types of data. Key rights such as the right to be forgotten, data portability, and informed consent were included.

Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act (DPDP), 2023, represents a more streamlined approach to data protection. It applies to the processing of digital personal data within India and to foreign entities processing data in connection with services or goods offered in India. The Act introduces the following key features:

- Data Fiduciary and Data Principal: The Act defines the data controller as a "data fiduciary" and the data subject as a "data principal," emphasizing a trust-based relationship.

- Consent-Based Processing: Processing of personal data is allowed only with the consent of the data principal, except in specific legitimate use cases.

- Grievance Redressal and Data Protection Board: A Data Protection Board of India is established to oversee compliance, inquire into breaches, and impose penalties.

- Cross-Border Data Transfer: Unlike the 2019 Bill, the DPDP Act allows cross-border data flow to countries notified by the central government, promoting ease of doing business.

- Penalties for Non-Compliance: The Act imposes significant financial penalties, ranging up to ₹250 crore for data breaches and failure to fulfill obligations.

Analysis of Judicial Trends

The judiciary has played a pivotal role in advancing the concept of data privacy in India, particularly in the absence of comprehensive legislation prior to 2023. Key judgments by the Supreme Court have laid the foundation for recognizing data protection as a fundamental right.

Justice K.S. Puttaswamy v. Union of India (2017)[9]

In this landmark case, a nine-judge constitutional bench unanimously held that the right to privacy is a fundamental right under Article 21 of the Constitution. The Court emphasized the informational autonomy of individuals and the need for a data protection law that balances individual rights with legitimate state interests. The judgment paved the way for the subsequent formulation of the Personal Data Protection Bill and DPDP Act.

Shreya Singhal v. Union of India (2015)[10]

Though primarily concerned with freedom of speech under Section 66A of the IT Act, this case has broader implications for digital regulation. The Court struck down Section 66A as unconstitutional for being vague and disproportionately restricting free speech. This decision highlighted the need for clarity and proportionality in laws dealing with online behavior, which is also crucial in the context of data privacy and cybercrime.

Internet and Mobile Association of India v. RBI (2020)[11]

In this case, the Supreme Court struck down the RBI's circular that effectively banned cryptocurrency trading. While not directly addressing data protection, the judgment reinforces the principle that regulatory actions in the digital economy must be balanced and lawful. It also reflects judicial sensitivity to emerging technologies and the need for nuanced legal responses.

The judiciary has thus emerged as a proactive guardian of digital rights, especially in the face of executive overreach or legislative vacuum. However, judicial pronouncements alone are insufficient in combating cybercrime without an effective statutory and enforcement framework.

CHALLENGES AND GAPS IN THE LEGAL FRAMEWORK

Despite recent legislative advancements, including the Digital Personal Data Protection Act, 2023, India's legal framework for tackling cybercrime and safeguarding digital privacy still faces several critical challenges. These issues not only hinder the enforcement of data protection laws but also exacerbate the vulnerability of individuals and businesses to cyber threats. This section examines the core challenges and systemic gaps in India's current approach to cyber law and data protection.

[9] AIR 2018 SC (SUPP) 1841.
[10] AIR 2015 SUPREME COURT 1523
[11] AIR 2021 SUPREME COURT 2720.

Lack of Awareness and Cyber Literacy

One of the most significant challenges in the Indian context is the widespread lack of awareness about data rights and cyber hygiene. The majority of internet users, especially in rural and semi-urban areas, lack basic knowledge of how their personal data is collected, processed, or used by digital platforms. This cyber illiteracy leads to unintentional consent, increased susceptibility to phishing, identity theft, and other cybercrimes.[12]

Cross-Border Jurisdictional Issues

Cybercrime and data breaches often transcend national boundaries, making enforcement difficult under domestic laws. For example, data stolen from Indian users may be stored on servers in another country, and the perpetrator may be located in a third jurisdiction. In such cases, mutual legal assistance treaties (MLATs) or international cooperation mechanisms are necessary for investigation and prosecution.[13]

Inadequate Law Enforcement Capacity and Technical Expertise

India's law enforcement agencies often lack the specialized skills and technological infrastructure necessary to deal with complex cybercrimes. Cyber Forensic Labs are limited in number and scope, and most police stations are ill-equipped to investigate cyber offenses such as ransomware attacks, deepfakes, or cryptocurrency-based frauds.

Additionally, cyber cells are often overburdened and under-resourced. There is also a significant gap in coordination between central and state-level agencies, leading to inefficiencies in response and investigation. The slow pace of judicial processes and limited availability of trained cybercrime prosecutors further reduce the deterrent effect of the law.

[12] Clare (2024) Digital India and Cybersecurity: Navigating the Future - News - CLA, Commonwealth Lawyers Association. Commonwealth Lawyers Association. Available at: https://www.commonwealthlawyers.com/cla/digital-india-and-cybersecurity-navigating-the-future/.

[13] Cross-border disputes: An introduction to navigating legal issues arising in multi-jurisdictional disputes: Perspectives: Reed Smith LLP (no date) Cross-border disputes: An introduction to navigating legal issues arising in multi-jurisdictional disputes | Perspectives. Available at: https://www.reedsmith.com/en/perspectives/2025/04/cross-border-disputes-navigating-legal-issues-multijurisdictional-disputes.

COMPARATIVE LEGAL ANALYSIS

As cybercrime evolves and transcends borders, nations across the world have developed their own data protection frameworks to respond to the growing threat to digital privacy. A comparative analysis of international frameworks like the European Union's General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Singapore's Personal Data Protection Act (PDPA) provides valuable insights for India. These frameworks offer robust models for regulating data flows, ensuring user rights, and enforcing compliance—lessons that can significantly enrich India's nascent data protection regime.

European Union – General Data Protection Regulation (GDPR)[14]

The GDPR, enforced since 2018, is widely considered the gold standard in data protection. It sets out clear rules for personal data collection, processing, storage, and transfer within and outside the EU. Key features include the principles of lawfulness, transparency, data minimization, and purpose limitation. Data subjects are empowered with comprehensive rights—such as the right to access, right to be forgotten, and right to data portability.

The GDPR also imposes strict compliance obligations on data controllers and processors, with heavy penalties for violations (up to €20 million or 4% of annual turnover). It mandates Data Protection Impact Assessments (DPIAs) and the appointment of Data Protection Officers (DPOs) in certain cases. Importantly, GDPR applies extraterritorially, meaning it applies to non-EU entities that process data of EU residents—setting a strong precedent for cross-border data accountability.

United States – California Consumer Privacy Act (CCPA)

The CCPA, effective since 2020, grants California residents several rights over their personal information. These include the right to know what data is collected, the right to opt out of the sale of personal data, and the right to delete personal information. Unlike GDPR, which focuses on consent-based models, the CCPA emphasizes consumer choice and corporate transparency.

While CCPA lacks a central regulatory authority like the European Data Protection Board, enforcement is conducted by the California Attorney General, with recent amendments under the California Privacy Rights Act (CPRA) strengthening enforcement mechanisms and extending data subject rights. The CCPA is more business-friendly but still provides a solid framework for user

[14] Legal Text (2024) General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

autonomy and transparency.[15]

RECOMMENDATIONS AND WAY FORWARD

The rapidly evolving technological landscape and the parallel rise in cybercrime demand a robust, agile, and future-ready legal response. While the Digital Personal Data Protection Act, 2023 is a welcome step, it must be complemented by wider systemic reforms. This section outlines key legislative, institutional, and policy-level recommendations to fortify India's cyber and data protection ecosystem.

Legislative Recommendations

India must strive for comprehensive data protection legislation that is harmonized with international norms such as the GDPR and incorporates clear definitions, obligations, and penalties. Ambiguities in the roles of "data fiduciaries" and "data principals" should be resolved through detailed subordinate legislation or rules. Importantly, the law must include provisions on algorithmic accountability, automated decision-making, and data portability, which are critical in the age of AI and Big Data.

Moreover, laws should be technology-neutral yet adaptive, providing a framework that remains relevant despite future innovations. Provisions for regular legislative reviews, perhaps every 3–5 years, should be institutionalized to keep pace with technological disruptions.

Strengthening Enforcement Agencies

Law enforcement agencies such as cybercrime cells, CERT-In, and Data Protection Board of India (DPBI) must be adequately staffed with technically skilled personnel. A dedicated Cybercrime Prosecution Unit within the judiciary and stronger coordination between the police, prosecution, and digital forensic labs is essential. Additionally, a national cybercrime database could help in identifying trends and deploying predictive policing techniques using AI and machine learning.[16]

Tech-Enabled Legal Infrastructure

There is a growing need to embed technology into the justice

[15] California Consumer Privacy Act (CCPA) (2025) State of California - Department of Justice - Office of the Attorney General. Available at: https://oag.ca.gov/privacy/ccpa.

[16] Iplf (2025) Digital Forensics in India: Bridging Technology, Law, and Justice in the Cyber Age, IPLF. Available at: https://www.ipandlegalfilings.com/digital-forensics-in-india-bridging-technology-law-and-justice-in-the-cyber-age/.

system. Developing an automated redressal mechanism for data breach complaints, using AI for case triaging, and digital evidence management systems can significantly improve legal efficiency. Tools like blockchain could be used to ensure transparency and traceability in data processing, especially in sensitive sectors like healthcare and finance.

The creation of online platforms for data subject grievances with multilingual interfaces and accessibility features can make justice more inclusive. Moreover, the judiciary must undergo regular training on cyber law and technology to stay updated with evolving case dynamics.

CONCLUSION

As technology continues to redefine the contours of communication, commerce, and governance, it simultaneously gives rise to newer and more sophisticated forms of cybercrime. This paper has examined the multifaceted relationship between technology and cybercrime, emphasizing the urgent need for a resilient and adaptive legal framework in India. The evolution of cybercrime—from simple data breaches to complex AI-enabled fraud—underscores the inadequacy of traditional legal instruments in addressing modern threats.

India's legislative journey from the IT Act, 2000 to the recent Digital Personal Data Protection Act, 2023 reflects a significant shift toward recognizing data privacy as a fundamental right. However, legal protections must evolve in tandem with technological advancements. Theoretical frameworks such as Routine Activity Theory and Deterrence Theory offer valuable insights into the behavioural aspects of cyber offenders, reinforcing the need for both preventive and punitive mechanisms.

Despite legislative progress, challenges such as cross-border jurisdiction, limited cyber literacy, weak enforcement capacity, and ambiguities in the law persist. A comparative analysis with global data protection regimes like the GDPR and CCPA reveals the need for India to adopt more coherent and rights-based approaches, ensuring not just compliance but genuine user empowerment.

REFERENCES

Statutes and Bills

- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

- Digital Personal Data Protection Act, 2023, No. __, Acts of Parliament, 2023 (India).
- Personal Data Protection Bill, 2019, Bill No. __, Parliament of India (2019).

Case Laws

- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Books

- Gupta, A. (2021). *Cyber Law and Data Protection in India*. New Delhi: LexisNexis.
- Singh, R. (2019). *Data Privacy and Cybersecurity: Legal Perspectives*. Oxford University Press.

Journal Articles

- Sharma, P. (2022). Influence of Cyber Laws on Data Security: An Analysis. *Indian Journal of Cyber Law*, 5(2), 45-63.
- Kumar, S., & Verma, T. (2023). Cybercrime in the Digital Age: Challenges and Legal Gaps in India's Data Protection Framework. *International Journal of Law and Technology*, 12(1), 22-38.

Websites

- Ministry of Electronics and Information Technology. (2023). Overview of the Digital Personal Data Protection Act. Retrieved from https://meity.gov.in/dpdp-act
- JusCorpus Legal Research. (2022). An Analysis of Cyber Laws with Focus on Data Protection in India. Retrieved from https://juscorpus.com/legal-research