International Journal of Arts, Commerce, Science and Technology

(International Open Access, Peer-reviewed & Refereed Journal)
(Multidisciplinary, Monthly, Multilanguage)

Volume: 1 ** Issue: 1** **November 2025**

www.ijacst.com

ISSN (Online): Applied

Impact of Cyber Laws on Data Privacy and Protection in India

Dr. Manoj Kumar Gupta

Principal, Model Public Law College, Chandausi, Uttar Pradesh
E-mail ID- manojgupta12@gmail.com

Abstract

The rapid expansion of digital technologies in India has significantly increased concerns over data privacy and protection, prompting the evolution of cyber laws to address emerging cyber risks. The Information Technology Act, 2000, along with its 2008 amendment and subsequent rules, forms the foundational legal framework for regulating data governance, preventing unauthorized access, and ensuring accountability for data breaches. Despite these developments, existing cyber laws remain fragmented and insufficient to cope with advanced cybercrime, large-scale data processing, and cross-border data transfers. The emergence of the Digital Personal Data Protection Bill, 2022, marks a progressive step toward establishing comprehensive safeguards aligned with global standards such as the EU GDPR. However, challenges persist in areas including enforcement, breach notification, and data localization. This study examines the historical evolution, statutory provisions, and enforcement mechanisms of Indian cyber laws while assessing their impact on personal data protection. It highlights the necessity for strengthened regulatory frameworks to balance technological advancement, national security, and individual privacy rights in the digital era.

Keywords: Cyber Law, Data Privacy, Information Technology Act, Data Protection Bill, GDPR Alignment

Introduction

The rapid evolution of digital technologies has transformed personal privacy and data protection, giving rise to cyber laws aimed at regulating the Information and Communication Technology sector and mitigating cybercrime risks. The core objective of cyber laws is to promote safe internet usage while effectively combating data breaches within the country. These legal regulations encompass a range of federal statues, supporting laws, rules, notifications, guidelines, and bye-laws, constituting the framework of India's cyber laws. The analysis focuses on the factors contributing to the urgent necessity for Indian cyber laws, particularly concerning the protection of individual data privacy rights (harma, A., 2022).

The concept of privacy is intrinsically linked to data, with shared knowledge derived from collected data directly reflecting an individual's privacy. The protection of personal data is imperative to safeguard personal and organizational data breaches, prevent fraud, maintain confidentiality, and secure information exchanged during electronic transactions. Although numerous Indian statutes address data protection, significant improvement remains to be achieved. The human right to personal privacy is expressly enshrined in Articles 12, 17, and

21 of the Constitution of India. Empirical studies conducted in India indicate a growing public concern about privacy, amplifying the need for dedicated data privacy legislation (Sood, 2015).

Evolution of Cyber Law in India

The framework for data protection in India, which is still evolving, is primarily governed by the doctrine of privacy that permeates across these judicial pronouncements. Although privacy and data protection are not treated as fundamental rights in the Constitution, the development of such rights regarding personal data is derived mainly from the clauses enshrined in Article 19, which states that the right to express free speech, right to privacy, and right to data protection form an important pre-condition in the fulfilment of such objective; hence, a multiplicity of restrictions on data protection cannot be imposed, as directed by an array of judicial pronouncements of the apex court.

The Information Technology Act was enacted in 2000 as a broad legal basis for electronic communications and storage. It aims to provide a functional legal framework to facilitate electronic commerce, promote e-governance, and enhance cyber security through regulatory structures designed to prevent the widespread misuse of the internet and the associated technologies. The Act has undergone a large number of amendments, and with the rapidly changing technological landscape, several provisions of the legislation have become redundant and need to be repealed (Misra & Chacko, 2021).

(i) Historical milestones: Laws governing technology, specifically information technology (IT) and data protection, have significantly evolved to address shifting paradigms of commerce and technology. Acknowledged as an enabler of business transactions, IT, and e-commerce continue to burgeon both in India and globally. Financial transactions of varying moduli are now conducted online, routinely resulting in the asset transfer of customers. Revolutionary changes in telecommunications, such as convergence of data, telephony, and broadcasting, coupled with resounding social acceptance of IT, necessitated regulatory reforms aligning aged standards with current requirements. Many anticipate a similar berthing of the predominant sector; however, e-commerce regulations range widely in concept and execution (Mohanty, A., 2011).

India has one of the largest populations of software professionals, yet cyber security incidents continue to plague Indian Society. Information security breaches range from hacking into government agencies, banks, and telecommunication networks, to stealing the identity of digital citizens, siphoning their financial resources, or threatening physical harm to their families or finances. Transparency and accountability of state-run initiatives, from the Aadhaar identity project to the Covid-19 pandemic response applications, remain questionable. These quality and standard issues arise from inadequate regulatory frameworks and leaves commerce vulnerable to illegal enterprise. Even with the recent protection of information and technology Act, 2000, a comprehensive data protection and privacy statute remains elusive. Current regulations, implemented through the Indian contracts Act of 1872, the Indian penal code of 1860, the India information technology Act of 2000, and the information technology (Amendment) Act, 2008, trail cybercrime legislation elsewhere. Business facilities and services, coupled with stimulus packages to boost e-commerce, further intensify the sector's unresolved legal predicament (Misra & Chacko, 2021).

Even as computer, internet, mobile, and communications technologies expand guilelessly, social attitudes are becoming progressive rather than censorious. Privacy, however, remains centre-stage, albeit approached diametrically opposed to most developed democracies. Indian society tilts judiciary/legislature dedicated to security rather than privacy (Sood, 2015).

(ii) Key statutes and amendments: By 2000, Internet access had grown exponentially, yet Indian laws remained inadequate to tackle specific cybercrimes like hacking, data forgery, and information theft. These gaps highlighted the need for a holistic framework to govern

cyberspace. The Information Technology (IT) Act, enacted in 2000, addressed these issues. Following the enactment of the IT Act, the government formed the National Task Force for Cyber Security in 2003 to probe the increasing threat of cyber terrorism. The Task Force submitted its report in 2004, noting the lack of data privacy laws and recommending the formation of a Data Protection Authority for India to oversee the protection of personal data. Subsequently, the need for an overarching privacy law became evident due to growing concerns about government-enforced surveillance, biometric Aadhaar-based digital payments, controversy over the ownership of personal data shared on social media, and several data breaches by public and private entities. The IT Act, 2000, and its consequential amendments remain the key regulatory framework governing data privacy in India (Iqbal, J., & Beigh, B. M., 2017).

The IT Act, passed in 2000, provided legal recognition to electronic records and electronic signatures, coping with issues arising from the increasing reliance on information and communication technology in business, trade, and commerce by the general population. Subsequently, the 2008 amendment underscored the need for a specific law to safeguard sensitive personal data and address growing data protection concerns. The legislative framework predominantly covers legal recognition of electronic documents, electronic signatures, secure electronic records, data and message integrity, electronic governance, data protection and information security, breach of confidentiality, hacking of information systems, and cyber terrorism (Sood, 2015).

Data Privacy Framework in India

One of the most significant developments in Indian cyber security in the last few decades has been the emergence of a data privacy framework (Kethareswaran, 2017). Privacy concerns have escalated in all parts of the world, especially since the advent of the internet and the proliferation of digital devices. Privacy means the state of being free from intrusion, interference, or disturbance by others and the regulation of access to information about oneself. Compliance with personal data protection regimes has been imperative to participate in the global economy and international trade. In India, issues relating to confidentiality and privacy had not been adequately addressed until the enactment of the Information Technology (IT) Act, 2000, which was later amended into the Information Technology Act, 2008.

In the Indian context, the regulatory compliance and legal position are particularly challenging due to the sheer variety and proliferation of electronic data processing. Sensitive personal data covers specific categories of data, which if released are likely to cause substantial discomfort, and include but are not limited to, financial data, passwords, health-related data, sexual orientation, and political preference. Even though sensitive personal data has been recognized as an important category, no specific regulations or guidelines have been issued for large parts of electronic data processing. The only general requirement specified is the need for "reasonable security practices" under section 43A of the Indian IT Act, but no standard or scheme has been specified for determining the reasonableness of security associated with sensitive personal data. The legislative intent to bring in a data protection framework in India has been mooted since the earlier drafts of the IT Bill, 1999 and its amendments in 2008, further analysis of personal data protection and issuance of recommendations were made on data protection, security and privacy (Brahmam, & Muppavaram, 2023).

(i) Personal Data Protection considerations: The focus is on the elements of personal data under the proposed legislation and how they differ from other data types within the generality of privacy protection. The assessment further explicates the nature of rights available to individuals concerning personal data, what constitutes consent concerning these data, and whether that consent can be made subject to a general terms of service banner. The section then seeks to articulate the provisions of the Information Technology Act, as they pertain to an individual's right to privacy. The analysis centres on the provisions of the IT Act that the Indian

judiciary has interpreted as complementary to the right to privacy and various security obligations that indubitably provide some protection for personal data. Consent, still a central concept, implicitly features through terms used in the Act, the Rules, and the jurisprudential discussions that stem from those legal sources.

The earlier sections indicate that the consideration of personal data protection must evaluate two propositions. First, a proposed right must include other broader rights under consideration, whether freedom, dignity, or privacy. Second, the proposed right must not conflict with another fundamental right like freedom of speech or expression (Kethareswaran, 2017).

(ii) Information Technology Act provisions relevant to privacy: The Indian legislature has adopted various measures pertaining to privacy under the Information Technology (IT) Act, 2000, primarily through provisions governing the collection, storage, transmission, and disclosure of personal information. The main thrust of these provisions is that intermediaries must obtain the requisite consent of users before storing or processing their personal information. Section 43A of the IT Act also makes intermediaries liable for damages to the affected persons in case of wrongful loss or wrongful gain from the disclosure of personal information in breach of an implied or express agreement (Sood, 2015). The outlets of access to communication, whether it pertains to telephones, email systems, online chats, or any other medium, fall within the scope provided for by the IT Act. The provisions of the IT Act, including the amendments incorporated through the IT (Amendment) Act, 2008, and the judicial pronouncements interpreting the provisions of the Act, nevertheless receive consideration.

The legislative history of the IT Act illustrates the rapid transition occurring since the onset of the Information Age. The preamble of the IT Act identifies the underlying objective of the Act as the promotion of e-commerce and e-governance through the financial availability of a framework for the legal recognition of electronic records. The relevance of legislation containing provisions dedicated to privacy and related media access establishing surveillance machinery nevertheless becomes apparent from the deliberations that preceded the enactment of the IT Act in the year 2000. The first draft of the privacy provisions was adopted during the Second Roundtable India, shortly after the General Agreement on Tariff and Trade (GATT) negotiations had concluded and shortly before the conclusion of the Internet Governance Forum 2010 at Hyderabad. The framework of the IT Act remains enshrined within India's universal declaration of the right to privacy, reflected in the Preamble of the Constitution of India and various Enforcement Guidelines (Chatterjee, A. (2021).

The coverage of the IT Act, and various orders passed under the provisions establishing a security framework, have been subject to scrutiny. The information and communication technology ecosystem continues to grow without parallel since the enactment of cyber law legislation, with innovative technological approaches addressing national challenges. A multitude of private and public sector entities, such as mobile networks, and digital ports are now accessing user-related hardware and personal citizen information at every functional point, from transactions to validated delivery stamps.

(iii) Rules and guidelines on data protection and breach notification: The rules and guidelines under the Information Technology Rules, 2011, for both data protection and breach notification, lay down procedural requirements applicable to specified personal information that is collected, stored, and processed by cloud service providers, service and application providers, and outsourced service providers (Sood, 2015). The guidelines specify the time frameworks for all the actions required in case of data breach notification. Data protection arrangements operating under the IT Act are supervised by the Ministry of Electronics and Information Technology (MEITY) and the Cyber Security Wing of the Ministry of Home Affairs, both of which, being government ministries, are responsible for law enforcement and jurisdictional inquiries.

Interplay with Global Data Protection Standards

The World Wide Web and mobile applications have severely altered the nature and degree of privacy intrusion into an individual's life. Almost every activity is now recorded, collated, and analysed for diverse purposes; for example, individuals are tracked from their mobile phones, which have reached extreme levels in some cases like China. These days, privacy is often understood only when consent is granted for data collection is at stake, while processing, retention, and transfer of data have overlooked.

The GDPR came in force by streamlining and harmonising data protection legislation across EU member states and imposing strict obligations on data processors. As observed by Palmieri, 2019), it is impossible to synchronise promptly either with the OECD Guidelines or the GDPR, since these frameworks are legion and extensive, it aims to find convergence between General Data Protection Regulation or whereas the former involves same regulation of personal data online or transcending borders.

The Indian legal regime does not have substantial global information arrangement. In the past few decades numerous International Instruments are passed like Undertaking, Agreement or Convention for encouraging and nurturing cross border information, however, globe privacy remains unexplored. The OECD's recommendations are followed by few countries; thus OECD became the medium for various countries to settle their own legislation. The Recommendation concerning Guidelines for the Protection of Privacy published in September 1980 is non-binding in nature but recognition came on a universal scenario. So, those nations taking the OECD gaining membership with Information Technology provisioning like Law, Act, Bill passed by the Government of India, it can be enhanced better leveraging of those Guidelines.

International conventions and cross-border data flow: To safeguard the cross-border flow of data, international agreements are crucial. The legal framework concerning cross-border data flow has been elaborated with conventions, treaties, and guidelines formulated by both international organizations and regional economic communities. Copy-book models with regard to cross-border transfer of data have also been adopted by certain countries, such as the APEC model and EU data protection directives. Non-legally binding instruments on the rights of individuals regarding the security of personal data and privacy protection are recognised for effective regional cooperation on cross-border issues (Sood, 2015).

The Global Data Protection Regulation (GDPR) has set up international competition among jurisdictions struggling for the compliance stamp of the European commission. The first stage of compliance is the determination to provide an adequate level of data protection to European citizens, in line with Article 45 of the new regulation (Corley, 2016).

Alignment with GDPR principles: While the IT Act assists businesses in many ways, further data protection measures are imperative for readiness of Indian enterprises to comply with GDPR norms. Legislative measures in compliance differentiate between those in relation to the data principles themselves and those in relation to the rights afforded to the data principal in respect of their personal data. As regards principles, GDPR incorporates additional principles of data protection by design and data protection by default. Degree of applicability of the enumerated principles also needs to be assessed in the light of their definition (Kethareswaran, 2017).

Mechanisms for Data Protection in Cyber Law

As a result of increased digitization, the amount of personal data being generated and stored has increased enormously over the past few years. Organizations routinely carry out near-constant processing of personal data, often for purposes they may not explicitly identify such as machine-learning applications, pattern recognition, intellectual property enrichment via behavioral analysis, and social network graph exploitation. Data security violations remain a significant concern, underscoring the importance of data protection measures. India's Cyber

Law Framework lays down several specific provisions for securing data and addresses these issues.

Organizations must implement appropriate security measures and standards for operating within the Indian regime. These include organizational, procedural, and information-security measures. Organizations can take a risk-based approach to information security which may, in turn, bring a balance between various competing risks, approve the minimal set of counters to key risks, adhere to acceptable and affordable levels of loss, budget for security efficiently, and be agile enough to seize new opportunities on a rapidly evolving technological front. The DPIAs describe the overall business, identify risks of wide-ranging significance such as long-term lock-in, critical functionality affectation, or multi-party exposure, and recommend additional prospective security measures that could mitigate them. Compliance with standards and frameworks ensures that organizations deploy best-practice controls that meet globally-accepted operational templates addressing diverse security risks. Organizations must comply with the principle of data minimization, by collecting or generating only the minimum amount of information absolutely necessary to achieve each specific proposed business purpose. The positioning further extends to retaining data sets for much shorter periods and drawing separate conclusions on data adequacy and security measures during data-transfer activity. Data localization requirements continue to be hotly debated, with the Government of India ensuring that all personal data of Indian citizens are ultimately stored within Indian Territory and remain under Indian jurisdiction and control. Proposals for transferring raw data out while subject matter of subsequent processing remaining within India are also being considered (Kathuria, Y., Ruhani, V., Tyagi, M., & Jain, V., 2024).

No guidelines exist for data-incident reporting within the Indian regime. Organizations therefore remain free to define their own incident-response procedures subject only to broad legislative and regulatory requirements. Properly-documented incident-response procedures which remain durable across personnel or operating-team changes and preclude an overwhelming focus on the external network boundary are recommended. A Data Breach Notification Policy and associated template, clarifying the pre-determined definitions of such incidents, is also advisable. Most guidelines either define the incidents exhaustively or remain vague and uncertain such as alleging any unauthorized or abnormal access; adopting a mixture of both approaches may confer maximum prudence. Organizations are typically mandated to declare only the most serious and essential violations when unrepresented data are inaccessible or deemed sufficient; significant corrective measures are nevertheless also usually taken. Specific guidance can assist in defining the key expected elements of high-level security that organizations should take into consideration to protect their information and their operations. Compliance with security-recognition standards such as ISO27001, SOC2, NIST, and PCI-DSS demonstrates adherence to what have emerged as globally-accepted baseline security-implementation vectors and frameworks across geographical and service-implementation concerns. Although indispensable, a formal security or security-and-privacy-posture designation can deliver additional clarity and confidence to both the enterprise and third parties on the standing that has already been achieved (Sood, 2015) ; (Misra & Chacko, 2021).

(i) Data security measures and due diligence: Information is still the most essential element in the entire legal regime, a proposition not discriminated against by the IT Act and, hence, treated equally across various masks. According to Section 70B of the IT Act, "the Indian Computer Emergency Response Team or its successor authority designated by the Central Government" defines guidelines for the protection of 'information', including the establishment of the "Indian Cyber Crime Coordination Centre". All the guidelines framed by these two authorities are applicable to the data protection regime (Sood, 2015).

The term 'data security' is dissimilar from 'information security' and 'data protection'; also, all the regulations cannot be accommodated in elaborating a single terminology. A variety of

data, including Personal Data, Administrative Data, Statistical Data, and Aggregated Data, gives preeminence to the identification of 'de-identified data'. The separation of 'data', as used in the legal apparatus, identifies distinct data types, and administrative data also cannot be neglected. Beginning from the regulatory phase, a personal data or information, is a data where an individual is enshrined in any computable form (Misra & Chacko, 2021).

(ii) Processing, storage, and transfer of information: Data minimization and retention play integral roles in personal data protection, with the latter attracting widespread interest and debate in the Indian context. In the draft 2019 Personal Data Protection Bill, storage limitations on personal data were mandated, with retention restricted to the specified purposes. Detailed data localization and transfer rules similarly captured attention and public discourse. Globally, the academic community widely reiterates the data minimization principle. To comply with the principle, organizations must limit data collection, processing, and access to only the personal information necessary to meet the objectives specified to the data subject (Misra & Chacko, 2021). Moreover, organizations should establish retention timelines for document and record-keeping deadlines appropriate to business needs and applicable provisions.

Privacy Rights and Remedies under Indian Law

The draft of the previous section provides an overview of the privacy rights arising from the status of data principal under the data protection bill introduced in the Parliament of India. The definition of the term "data principal" has become significant in recent years as it provides the rights of a data principal. The rights entitled to data principal that have been elaborated in the draft include the right to access, correction, erasure, and restriction. The accompanying remedies have also been described, along with the enforcement and redress mechanisms available in India.

The data protection bill defines data principal as "the natural person to whom the personal data relates." A data principal has certain rights under the bill that can be exercised against the data fiduciary. The data protection bill entitles a data principal to the following rights:

The Data Protection Bill, 2021 creates multiple rights for data principals. A succinct overview is portrayed in the Table below. Principals can exercise rights of access, correction, erasure, and objection to continued processing of personal data (Sood, 2015).

According to the Bill, the Principal is empowered to obtain information as to whether or not data is being processed, obtain confirmation in respect of such processing, request, under certain exemptions, rectification of inaccurate or incomplete personal data, seek erasure of personal data, or exercise a right to data portability. The right to withdraw consent may be exercised either at the commencement of processing, or thereafter. Further, a Principal may restrict or oppose the processing of personal data, or specify unauthorised categories of data, designation and means of processing the data, or revoke previously given consent. Such safeguards intend to enhance the control of the Principal over the collection of personal data.

The Government of India is also in the process of establishing compliance of an in-depth monitoring mechanism in order to ensure adherence of the data privacy protection rights provided in the Information Technology Act, 2000 (Sood, 2015). Various measures have been introduced for the protection of consumers against unscrupulous businesses by the Consumer Protection Act, 1986. The rise of the Internet has lead to a paradigm shift in the transactions and therefore the reach of the act. These sections impose reasonable restrictions on the right to free trade and business, as provided under the Constitution of India. The various labour laws like the Industrial Employment Act, 1946, Contract Labour Act, 1970, Information Technology Act, 2000 etc. also naturally impose restrictions on the right to privacy in order to prevent unfair labour practices.

Challenges and Critiques of the Current Framework

Cyber law in India faces criticism from different quarters regarding its coverage,

enforcement, and balance with national interests. The existing framework, while valuable, has some gaps. Certain masses, such as small-scale traders and micro, small and medium enterprises (MSME), have not been included within its scope. In addition, some categories of information remain unprotected. Even though rules concerning reasonable security practices and procedures have been articulated, enforcement efficiency is lacking in terms of both resources and capacity. The budgetary outlay for data protection in the fiscal year 2022–2023 and the organization of additional courts to lessen the backlog of judicial cases remain debatable. The cybersecurity ecosystem still struggles because of compliance costs generated by notifications to the Data Security Council of India which constitute a burden on start-ups (Sood, 2015).

The right to privacy has been incorporated into various policy documents, yet within the cyber law framework the need to strike a fair balance between security interests and privacy-related concerns has gone unaddressed. The United Nations (UN) Security Council deliberates on activities that threaten international peace and security, while surveillance and monitoring are two techniques which have emerged. Surveillance of public spaces appears to enjoy greater acceptance, although following the Paris attacks in 2015 the possibility of global surveillance through electronic devices nevertheless induced fear and apprehension. In India, government agencies and the Ministry of Information Technology have strongly advocated for a technological solution that enables encrypted data to be processed at traffic nodes as a way to counter terrorist acts. Hence, the current draft aims to facilitate greater access to user data in order to assist such activities, which presents an indirect implication for privacy (Kethareswaran, 2017).

On the surface, the right to privacy can be viewed as a sub-set of the right to life. It is prescribed in various national laws and India professes the right to privacy through mobile intercepts, e-mail monitoring, and the use of software deployed in the name of cyber prevention. Various rates of suicides and deaths owing to harassment and inhuman behavior have appeared in newspapers, which have served instructions for preventive actions, leading to a consequent increase in interception and privacy involvement activities by the cyber laws. The Constitution of India recognises the right to life through Article 21 and various economic policies, yet governmental measures by the IT Act have indirectly strained the protection of privacy and data under consideration whereas debates on deciphering the mass intercept prevention/ facilitating disposal of genuine grievance requests occupy a keen agenda (Basu, 2012).

Comparative Perspective: Indian Cyber Law vs Global Jurisprudence

Registered in 2001 with a sole member, an organization celebrating personal privacy can hardly claim to serve the interests of citizens or construct a robust legislative framework to protect privacy in India. Instead, harmful doctrines such as the "post-knowledge doctrine" persist from the colonial era when Indian freedom fighters were hounded by the military police under laws that later became the Indian Penal Code and the Criminal Procedure Code. Indeed, the establishment of a full Data Protection Authority should await constitutional amendments, the construction of a modernized Board for India or a similar agency, the implementation of a systematic Privacy Impact Assessment for each personal information category, and a thorough review of the laws surrounding other categories of personal information—ideally through comprehensive public consultations. Without safeguards enabling citizens to question executive control or bureaucratic abuse, and without widespread transparency enforcement—backed by timely and severe punishments—citizens will remain second-class users of the law. A future government intent on disabling democratic institutions might exploit overlapping authorities for information control similar to the fireside chat facility established by Franklin D. Roosevelt for deeper societal penetration (Basu, 2012).

Conclusion

The analysis highlights the significance of data privacy and protection in the context of

cyberspace in India and evaluates the impact of cyber laws on these aspects. Safety, reliability, and confidentiality of data are of utmost concern. The World Wide Web and other online activities create cyberspace and garner Data Privacy and Protection into the focus (with the increase in World Wide Web Service). The Cyber Law has become a pivotal tool for assuring data privacy and protection. The major aim of Cyber Law is to prevent cyber crimes and secure Internet Services. Cyberspace is a much-favoured term to define the whole online platform. Cyber Law has its impact on five major aspects of life, primarily on Privacy Protection Policies. The modern age may either be termed the age of computers or the Internet Age. The Internet, the most Marvellous invention of the computer, allows exchange of information in any form at phenomenal speeds. It has become an integral part of human life. Through the Internet, a person can connect with another person across country/world. E-commerce, e-banking, mobile banking, digital payments and a lot more activity can be conducted through Internet. The facilities of e-commerce and e-banking have simplifed life. Cyber Law helps building trust over e-transactions. Ninety-seven percent of data privacy is yet to be protected from misuse or cyber crime in India.

References:

1. harma, A. (2022, April 29). Cyber security, cyber laws and preventive actions. Times of India.
2. Mohanty, A. (2011). New crimes under the Information Technology (Amendment) Act. Indian Journal of Law and Technology, 7, 103
3. Iqbal, J., & Beigh, B. M. (2017). Cybercrime in India: Trends and challenges. International Journal of Innovations & Advancement in Computer Science, 6(12), 187–196.
4. Brahmam, K. V., & Muppavaram, A. O. K. (2023). Data privacy and cyber security in India: A critical examination of current legal frameworks. In Cyber Crime & Cyber Securities in India (pp. 86–94).
5. Chatterjee, A. (2021). Cybersecurity in India: Challenges and Prospects. Indian Journal of Criminology and Cyber Law, 8(3), 109–127.
6. Kathuria, Y., Ruhani, V., Tyagi, M., & Jain, V. (2024). Protecting data privacy in the age of AI: A comparative analysis of legal approaches across different jurisdictions. AIP Conference Proceedings, 040007. https://doi.org/10.1063/5.0234669
7. Sood, G. (2015). Comparative analysis of cyber privacy law in India and in the United States of America. International Journal of Advanced Research, 3(12), 1-15. https://www.academia.edu/64403928/Comparative_Analysis_of_Cyber_Privacy_Law_in_India_and_in_the_United_States_of_America
8. Misra, A., & Chacko, M. (2021). Square pegs, round holes, and Indian cybersecurity laws. International Cybersecurity Law Review, 2(1), 57–64. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8023505/
9. Kethareswaran, V. (2017). An Indian perspective on the adverse impact of Internet of Things (IoT). ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal, 6(4), 35–40. https://gredos.usal.es/bitstream/handle/10366/137945/An_Indian_Perspective_on_the_adverse_imp.pdf
10. Palmieri, N. F., III. (2019). Data protection in an increasingly globalized world. Indiana Law Journal, 94(1), 297–352. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=11319&context=ilj
11. Corley, M. (2016). The need for an international convention on data privacy: Taking a cue from the CISG. Brooklyn Journal of International Law, 41(2), 721–774. https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1425&context=bjil