ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 4 AND ISSUE 2 OF 2025

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

"SAFEGUARDING PRIVACY IN THE DIGITAL ERA: A CYBER CRIME PERSPECTIVE"

AUTHORS - MR. YOGESH CHAUHAN* & MR. HARINDER SINGH**

* LL.M RESEARCH SCHOLAR AT SANT BABA BHAG SINGH UNIVERSITY, JALANDHAR

EMAIL ID- ARYANCHAUHAN49040@GMAIL.COM

** ASSISTANT PROFESSOR IN LAW AT SANT BABA BHAG SINGH UNIVERSITY, JALANDHAR

EMAIL ID- HARRYSINGH213@GMAIL.COM

BEST CITATION - MR. YOGESH CHAUHAN & MR. HARINDER SINGH, "SAFEGUARDING PRIVACY IN THE DIGITAL ERA: A CYBER CRIME PERSPECTIVE", ILE MULTIDISCIPLINARY JOURNAL, 4 (2) OF 2025, PG. 44-54, APIS – 3920-0007 | ISSN - 2583-7230.

ABSTRACT

In the digital age, the rapid evolution of technology has brought about significant advancements, but also unprecedented challenges. One of the most pressing concerns is the protection of personal data and privacy in the face of increasing cybercrime. This research explores the complex relationship between privacy, data protection, and cybercrime, with a focus on the legal and regulatory frameworks governing data protection in India. The primary objectives of this research are to examine the existing legal framework for data protection in India, analyze the impact of cybercrime on individual privacy, and identify gaps and weaknesses in the current regulatory framework. This research employs a doctrinal analysis of laws and regulations related to data protection and cybercrime in India, including the Information Technology Act, 2000, and the proposed Personal Data Protection Bill, 2019. The study also draws on existing literature and case law to illustrate the challenges and complexities of data protection in the digital age. The research reveals that while India has made significant progress in developing a legal framework for data protection, there are still significant gaps and weaknesses that need to be addressed. The study highlights the need for a more comprehensive and robust data protection law that takes into account the complexities of the digital age and the evolving nature of cybercrime. The research concludes that effective data protection and privacy require a multi-faceted approach that involves not only legal and regulatory frameworks but also technological solutions and individual awareness. The study recommends that policymakers and regulators prioritize the development of a robust data protection law that balances individual rights with the needs of businesses and organizations. The findings of this research have significant implications for policymakers, regulators, and individuals. The study highlights the need for a more nuanced understanding of the complex relationship between privacy, data protection, and cybercrime, and the importance of developing effective solutions to protect individual rights in the digital age.

Keywords: Data privacy, Digital privacy, Cyber crime, Privacy laws in India, IT Act 2000, Data Protection, Right to Privacy.

1. OVERVIEW OF PRIVACY LAWS IN INDIA

Privacy laws in India have greatly changed over time, particularly because of the growth in digitization of society as well as a growing need for the security and confidentiality of an individual's personal information. Privacy is embodied in Article 21 of the Indian Constitution, under which there is a right to life and personal liberty. This right to privacy was also upheld in 2017 by the Supreme Court of India in its

landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, which established the right to privacy as a fundamental right under the Constitution. This judgment was critical in defining India's privacy law, as it recognized privacy as a vital part of an individual's dignity, autonomy, and personal freedom.[22]

Post-Puttaswamy judgment, the Indian government initiated efforts to further bolster protection of privacy via legislation and regulation. One important step in this direction was the proposed introduction of the Personal Data Protection Bill, 2019. The Bill is patterned after the European Union's General Data Protection Regulation (GDPR), and its objective is to regulate processing of personal data by both private and public parties operating in India. It creates a strong structure for the processing, storing, and collection of personal data such that data subjects have great control over their information and utilization.[23]

The Personal Data Protection Bill enacts a number of significant provisions. It requires organizations collecting personal data to get active consent from individuals prior to processing data. This conforms to international practices in data protection, whereby the consent of persons is taken to be the linchpin of privacy legislations. The Bill also sets the stage for creating a Data Protection Authority (DPA) whose responsibility will be ensuring that organisations comply with the law and apply data protection rules. The DPA can also impose penalties against organisations in cases of non-compliance, and hence secure responsibility in the processes of handling data.[24]

Additionally, the Bill focuses on the rights of individuals with regard to their personal data. Such rights are the right to access, right to correction, and the right to erasure (also referred to as the right to be forgotten). According to the Bill, individuals have the right to withdraw consent at any time, and businesses are required to stop processing data once consent is withdrawn. The Bill also puts obligations on data fiduciaries (organizations that collect and process personal data) to adopt measures that secure data, including technical and organizational measures to safeguard personal information from unauthorized access or breaches.[25]

Nevertheless, even with the increasing acknowledgement of privacy as a basic right and the legislative efforts to control personal data processing, there are powerful challenges in India's privacy arena. A key issue is the absence of robust data protection legislation prior to the promulgation of the Personal Data Protection Bill. The lack of a clear, codified law created loopholes in the regulation of privacy and protection of data, and organizations tended to operate without proper precautions for personal data. Additionally, India has not yet passed a dedicated Privacy Act, which would deal with issues like biometric data protection, data localization, and crossborder data flow in a holistic manner. The Personal Data Protection Bill's introduction is an important step towards filling these gaps and bringing India's privacy legislation at par with global standards.

Lacking robust data protection legislation, some provisions under other legislations have tried to deal with privacy issues. For instance, the Information Technology Act, 2000 (IT Act), namely Section 43A, requires companies dealing with sensitive personal data to take reasonable steps to secure it. Further, Section 72A of the IT Act penalizes the unauthorized disclosure of personal information. These provisions, although helpful in the context of cybercrime, are not as comprehensive as the protections provided under the Personal Data Protection Bill.

[22] Astha Srivastava, —The Evolution Of Data Privacy Laws In India: A Comparative Analysis With Global Standards » Lawful Legall Lawful Legal, 2024 *available at*: https://lawfullegal.in/theevolution-of-data-privacy-laws-in-india-a-comparative-analysis-with-global-standards/ (last visited April 1, 2025).

[23] {"@type": Person, —Understanding India‘s New Data Protection Lawl Carnegie Endowment for International Peace.

[24] *available at*: https://prsindia.org/billtrack/prs-products/prs-legislative-brief-3399 (last visited April 1, 2025).

[25] —Art. 17 GDPR – Right to erasure (‗right to be forgotten‘),‖ General Data Protection Regulation (GDPR), 2016 *available at*: https://gdpr-info.eu/art-17-gdpr/ (last visited April 1, 2025).

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]
VOLUME 4 AND ISSUE 2 OF 2025
APIS – 3920 – 0007 | ISSN - 2583-7230
Published by
Institute of Legal Education
https://iledu.in

In addition, India's telecommunication policies, such as The Telecom Regulatory Authority of India (TRAI) regulations on data privacy, place some responsibilities upon telecommunication service providers to safeguard subscriber information. The policies are intended to protect privacy in the telecommunication industry, though they remain inadequate for ensuring holistic privacy protection in the age of technology.[26]

Although Indian privacy law has come far, issues like breaches of data, unauthorized monitoring, and ignorance of rights to privacy among the public continue. The emergence of digital media, social media, and e-commerce has generated an explosion of data concerning individuals that is being accumulated and processed by the public and private sectors. These organizations tend to be opaque in their use of consumer information, and there is an urgent need for enhanced privacy protections and effective enforcement mechanisms. As India still struggles with these issues, the enactment of the Personal Data Protection Bill will play a critical role in ensuring privacy rights are well protected in the digital space.

2. DATA PROTECTION UNDER THE IT ACT

The Information Technology Act, 2000 (IT Act) is the major law that governs cybercrimes and electronic commerce in India. Although it is mainly meant to regulate electronic transactions, digital signatures, and cybercrimes, it also has provisions addressing data protection. Nevertheless, the IT Act in its current form is not a complete law with regard to data protection. The sections of the IT Act that relate to data protection and privacy are fairly narrow in scope, and it is increasingly acknowledged that India needs stronger and more comprehensive data protection legislation, like the Personal Data Protection Bill, 2019.

The IT Act comprises a few major sections dealing with data protection and privacy. Section 43A of the IT Act is perhaps the most significant provision regarding data protection. According to this section, any body corporate or individual who is in charge of processing sensitive personal data must adopt and ensure reasonable security practices and procedures. The section particularly addresses sensitive personal data or information (SPDI), which comprises financial data, passwords, health data, and other personally identifiable data. If a party does not follow reasonable security practices, it can be held liable for compensation under the Act. This section does not have precise guidelines on what kind of security practices and procedures need to be followed, and it is based on self-regulation by the organizations.[27]

In addition, Section 72A of the IT Act deals with the unauthorized disclosure of personal information. This section makes it a criminal offense to disclose personal information by an individual who has gained access to it in the name of his employment or official work. An individual convicted of an offense under this section can be imprisoned for a period of three years or fined up to Rs. 5 lakh. This section is designed to preserve the privacy of individuals by preventing unauthorized use or disclosure of their personal information, but its application is restricted because it only addresses cases of disclosure without consent.

Apart from these provisions, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 were brought in to supplement the IT Act and give a regulatory framework for the protection of sensitive personal data. The rules also establish the definition of sensitive personal data and set out guidelines for data controllers (i.e., businesses) regarding how to deal with and secure such data. The regulations stress the requirement of clear consent from individuals prior to gathering

[26] —Privacy Policy,‖ Telecom Regulatory Authority of India *available at*: http://trai.gov.in/portalsapps/privacy-policy (last visited April 1, 2025).

[27] Nirma University, —Institute of Law Nirma University‖ Institute of Law, 2019 *available at*: https://law.nirmauni.ac.in/data-privacy-protection-in-india-technology-vis-a-vis-law/ (last visited April 1, 2025).

sensitive personal information and require companies to ensure data security and avoid data breaches. They also necessitate organizations to designate a grievance officer to handle data protection issues raised by data subjects.

In spite of these provisions, the IT Act is confronted with a number of challenges in offering complete protection for personal data. The absence of definitive provisions on data breach notifications, data processing, and data subject rights creates major holes in the whole scheme. As compared to global standards such as the GDPR, which contains provisions on the right to erasure (right to be forgotten), data portability, and the need for data protection impact assessments, the data protection provisions of the IT Act are quite rudimentary and inadequate for addressing the increasing complexity of data processing in the digital era.

In addition, the IT Act does not well address cross-border data flow issues, which are becoming increasingly relevant in the scenario of global digital trade and cloud computing. The Personal Data Protection Bill, 2019, attempts to remedy some of these issues by prescribing data localization mandates, requiring some categories of sensitive data to be stored and processed in India. This section mirrors the increasing concern regarding the susceptibility of Indian citizens' personal information being processed by foreign bodies, which could be beyond the purview of Indian law and regulations.[28]

Though the IT Act has attempted to control data protection in India, the necessity for a more complete and contemporary data protection law is evident. The Personal Data Protection Bill, which is currently under consideration, seeks to address this gap by establishing more stringent data protection measures, broadening the scope of personal data rights, and giving a more transparent and accountable mechanism for data processing activities. As India continues with these legislative changes, the IT Act's contribution to data protection will itself change in concert with the wider legal framework designed to protect individuals' privacy and personal data.

3. RIGHT TO PRIVACY IN THE DIGITAL ERA

In the digital era, privacy has become an issue of paramount importance, as increasing utilization of digital technologies, web-based applications, and interlinked systems have thrown up questions about data collection, processing, and abuse of personal information. The right to privacy as guaranteed under Article 21 of the Indian Constitution has developed over the years, particularly with the emergence of digital technologies. Whereas Article 21 protects the right to life and personal liberty, the Supreme Court of India's 2017 ruling in Justice K.S. Puttaswamy v. Union of India recognized that the right to privacy is an integral component of this general right. The Court ruled that privacy is a constitutional right, affirming the need to protect personal data in the digital era.

The internet's accelerated development, mobile technology, social networks, and online services have given rise to the explosive growth of personal information that is created, stored, and processed by private and public sectors. Ranging from smartphones and cloud computing to social networks, digital technologies have simplified interactions, communications, and data exchange. But these developments have also introduced new challenges to the protection of individuals' privacy rights. With personal data frequently crossing borders and being processed by multinational companies, data protection and privacy breaches have become more of an issue.[29]

In India, the digital privacy right is controlled by a matrix of legal provisions, such as those under the Information Technology Act, 2000 (IT Act),

[28] Akriti Gaur, ―Cross-Border Data Flows and India's Digital Sovereignty‖ Verfassungsblog (2025).

[29] ―Introduction to Cloud Computing Computing,‖ Springer Nature Singapore, 2023 *available at*: https://link.springer.com/chapter/10.1007/978-981-19-3026-3_1 (last visited April 1, 2025).

the Personal Data Protection Bill, 2019, and the overall constitutional framework. The IT Act has certain provisions regarding the protection of sensitive personal data, as provided in Section 43A and Section 72A, which put obligations on entities to implement reasonable security practices for protecting personal data and penalize the unauthorized disclosure of personal information. But these provisions are not complete, and it is increasingly felt that a stronger and more inclusive framework is required to deal with privacy issues in the digital age.

The Personal Data Protection Bill, 2019, which aims to provide for the regulation of processing of personal data in India, includes a number of provisions to improve privacy protection. The Bill aims to enhance the right to privacy by providing individuals with more control over their personal data. Some of the most important provisions of the Bill are the right to access personal data, the right to correction, the right to erasure (right to be forgotten), and the right to data portability. Consent to data processing must be informed, explicit, and revocable under the Bill. In addition, the Bill proposes data fiduciaries, or business entities that hold and process people's personal information, and places their obligations relating to data handling and protection. Organizations must make strong security procedures to avoid breaking into data to ensure that rights of privacy on the part of data subjects are maintained.

Right of privacy is affected by new and emerging technologies as well, such as artificial intelligence (AI), big data analysis, biometric identification systems, and Internet of Things (IoT) products. Although the technologies have vast advantages, for example, the improvement of health, security increase, and reduction of business procedures, they, however, carry serious privacy-related issues. For instance, biometric data collection through Aadhaar (India's biometric identification system) has sparked debates about the potential for mass surveillance and the risk of personal data being misused or accessed without consent.[30]

The challenge of protecting privacy in the digital era also involves ensuring that individuals' personal information is not subject to unauthorized surveillance or data mining. With the advent of data-driven business models, organizations increasingly depend on gathering and analyzing massive amounts of user data for personalized services and targeted advertising. Such activities are reported to be invasive in terms of raising issues of data profiling, data exploitation, and a lack of transparency regarding the use of personal information. Moreover, the deployment of surveillance technologies, including facial recognition and tracking of locations, has raised alarms regarding the erosion of public space individual privacy.

To address these challenges, privacy activists demand more robust legal protections and enhanced transparency in collecting and processing personal information. The Personal Data Protection Bill is a step in this direction, but it has to be enacted in its entirety to ensure that the right to privacy is respected in the context of emerging digital threats. With digital technologies becoming increasingly advanced, it will be important for legal frameworks to evolve with new developments and ensure that people's privacy is safeguarded while balancing the legitimate interests of businesses and government agencies.

4. DATA BREACHES AND SECURITY VIOLATIONS

Security breaches and data breaches are one of the biggest privacy and data protection threats in the modern digital era. A data breach happens when a person's information or sensitive information is accessed, disclosed, or used without permission from the data subject, typically because of cyberattacks, unauthorized access, or carelessness. Such violations can be

[30] —Internet of Things and Privacy – Issues and Challenges – Office of the Victorian Information Commissioner,‖ *available at*: https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-ofthings-and-privacy-issues-and-challenges/ (last visited April 1, 2025).

very costly for individuals, organizations, and society as a whole, as they can lead to financial loss, identity theft, damage to reputation, and liability under the law. In India, the Information Technology Act, 2000 (IT Act) deals with data breaches from the perspective of cybersecurity and protection of data. Section 43A of the IT Act specifically states that companies that deal with sensitive personal data or information (SPDI) have to put in place reasonable security practices and procedures to secure the data from breaches. In case a company does not adhere to these security protocols and a breach happens, the company can be held liable for damages. Section 72A of the IT Act also criminalizes unauthorized disclosure of personal information, including disclosure of data by an employee/third party without permission.[31]

Apart from the IT Act, the Personal Data Protection Bill, 2019 offers a more comprehensive framework for dealing with data breaches. The Bill proposes the mandate for data fiduciaries to inform both the Data Protection Authority (DPA) and concerned persons upon a breach of personal data. Such notification must be made without unreasonable delay and within a specific time limit. The Bill also fines organizations that are not taking enough precautions to keep personal data safe, and data fiduciaries are mandated to use robust technical and organizational security measures to protect against breaches.

In spite of these legal provisions, data breaches remain a common phenomenon in India, primarily because of the rising level of sophistication in cyberattacks and the expanding amount of personal data being gathered. High-profile data breaches, such as those involving large-scale customer data breaches by e-commerce, banking, and telecom companies, have raised questions regarding the sufficiency of current legal frameworks and the extent of cybersecurity readiness in India.

One of the greatest challenges to data breach responses is that industries have no common standard for security procedures. While some industries, like banking and telecom, fall under regulatory authorities and have to comply with strict data security protocols laid down by bodies like the Reserve Bank of India (RBI) and the Telecom Regulatory Authority of India (TRAI), others may not be held to the same level of regulatory scrutiny or have security measures in place. Consequently, data breaches in such industries can remain undetected or unreported for extended periods, causing extensive damage to individuals and organizations. Apart from cybersecurity issues, data breaches can also result from human error or negligence. For example, employees can accidentally expose sensitive information by not adhering to proper security protocols or by mishandling data storage devices. Insider threats, in which people from within an organization abuse their access rights to pilfer or leak information, are another major concern. In order to deal with these, the Personal Data Protection Bill requires organizations to have a Data Protection Officer (DPO) on board who will be in charge of data protection procedures and monitoring compliance with data security norms.[32]

India also has problems regarding cross-border data flows. Most Indian companies keep and process data in foreign jurisdictions, where various data protection laws and regulations might be applicable. In case of a data breach, the issue of jurisdiction and legal remedies for affected individuals becomes more complicated. The Personal Data Protection Bill attempts to cover this gap through data localization mandates, which would require some types of personal data to be processed and stored locally within India. Data localization has the potential to protect personal data from

[31] Sneha Mahawar, —Is Section 43A out of the scope of the Information Technology Act, 2000‖ iPleaders, 2023 *available at*: https://blog.ipleaders.in/is-section-43a-out-of-the-scope-of-informationtechnology-act-2000/ (last visited April 1, 2025).

[32] —What is an insider threat,‖ Fortinet *available at*: https://www.fortinet.com/resources/cyberglossary/insider-threats (last visited April 1, 2025).

extraneous threats, yet at the same time could give rise to concerns related to the transfer of data across borders as well as to international cooperation against global cybersecurity risks. The growing pace and complexity of data breaches also point to a greater need for robust data protection legislation and enforcement capabilities. As good as the IT Act and the Personal Data Protection Bill are, it will be necessary for Indian law enforcers and regulatory agencies to enhance their capability to deal with data breaches and cyber attacks. This involves ensuring that businesses are made accountable for not keeping personal information secure and that those who are affected are given reasonable compensation for any damages resulting from data breaches.

5. IMPACT OF GDPR ON INDIAN CYBER CRIME LAWS

The General Data Protection Regulation (GDPR), which was rolled out by the European Union (EU) in May 2018, is a landmark legislation that was designed to enhance data protection for people in the EU. The GDPR has profoundly changed the ways of data protection across the world, even in India. With organizations and companies worldwide, including those in India, transacting with data subjects within the EU, the extent and impact of GDPR cannot be disputed, especially concerning cybercrime and the legal protection of personal information.[33]

Although the Information Technology Act, 2000 (IT Act) and the Personal Data Protection Bill, 2019 (PDP Bill) focus on data protection in India, the GDPR has created a new benchmark in international data protection standards. The focus on accountability and transparency in data processing operations is one of the major effects of the GDPR on Indian cybercrime laws. The GDPR's obligation for data controllers and processors to have transparent and detailed records of their data processing activities has had an impact on the evolution of data protection practices in India. This accountability aligns with the provisions contained in the PDP Bill, which also stresses the significance of transparency, consent, and control of personal data.

In addition, the GDPR's strong data subject consent requirements have impacted Indian cybercrime legislation significantly. The Personal Data Protection Bill, modeled after the GDPR, requires organizations to receive express consent from individuals prior to processing their personal data, in order to make sure that the individuals are still in control of their personal information. This demand is reminiscent of the GDPR emphasis on the doctrine of informed consent, which guards against unauthorized gathering, processing, and sharing of data. In addition, the PDP Bill provisions for the right to be forgotten and the right to data portability mirror the GDPR's sweeping scope of rights of the individual, enabling the individual to ask for erasure of their data and transfer of their personal data across service providers, strengthening protection of the individual's privacy right.

The GDPR focus on notification of data breach has also shaped India's regulation. Organisations under the GDPR are obligated to inform data subjects within 72 hours of breach that has leaked personal data. Although the IT Act makes data breaches provisions possible under Section 43A for entities to incorporate reasonable security measures, the PDP Bill exceeds this by putting in place breach notification provisions based on obligation like the GDPR. This places India closer to international standards for transparency and accountability, with a focus on the timely reporting of violations that might impact individuals' personal data.

Moreover, cross-border data transfer in the GDPR affects Indian law in that Indian organizations processing European data subjects are required to keep in line with the GDPR limits on cross-border transferring of personal data to non-compliant countries. This has left Indian regulators looking into the

[33] —What is GDPR, the EU's new data protection law?,‖ GDPR.eu, 2018 *available at*: https://gdpr.eu/what-is-gdpr/ (last visited April 1, 2025).

possibility of imposing tougher data localization rules, as evidenced in the PDP Bill. The Bill also provides for data localization, mandating the storage and processing of sensitive personal data within India, a step that is consistent with the GDPR's stringent data transfer requirements.[34]

Though the GDPR has shaped the formation of India's cybercrime and data protection environment, its extraterritorial nature has generated controversy in India, particularly for corporations and institutions dealing in cross-border data processing. Indian firms trading within the EU or handling the data of EU residents need to be in conformation with the GDPR, increasing the compliance expenditure and demands on profound adjustments to data processing culture.

6. DATA PROTECTION REGIMES: COMPARATIVE STUDY

Data protection regimes are critical to protecting individuals' privacy and ensuring personal data is processed lawfully, transparently, and securely. Many nations have established data protection legislation to regulate the collection, storage, and processing of personal data, each having its own means of privacy protection. A comparative analysis of the data protection regimes in different jurisdictions, such as India, the European Union (EU), and the United States (US), assists in understanding the merits and demerits of various approaches, along with their implications for addressing cybercrime.

The European Union's General Data Protection Regulation (GDPR) is widely regarded as one of the strongest and most comprehensive data protection regimes. The GDPR covers all EU member states and governs processing of personal data in the EU, as well as by organizations outside the EU that provide goods or services to EU citizens. Perhaps the most significant aspect of the GDPR is the focus on data subject rights, such as the right of access, the right to rectify, and the right to delete personal data, and the right to data portability. Moreover, the GDPR also places substantial responsibilities on data controllers and processors, such as obtaining the explicit consent of data subjects, performing data protection impact assessments (DPIAs), and the implementation of adequate security to avoid breaches. The extraterritorial application of the GDPR has established an international benchmark for the protection of data, and its regulations have inspired other countries across the world to revise their respective data protection legislation.[35]

In comparison, India's data protection framework is evolving, with the Information Technology Act, 2000 (IT Act) and the Personal Data Protection Bill, 2019 (PDP Bill) serving as the primary legal instruments governing cybercrime and data protection. While the IT Act includes provisions for the protection of sensitive personal data and criminalizes unauthorized data disclosure, it lacks the comprehensive framework provided by the GDPR. The PDP Bill, modeled after the GDPR, seeks to create a stronger regime of data protection in India by adding data subject consent, right of access, right of erasure, and breach notification obligations. The Bill also incorporates the notion of data fiduciaries or data protection entities that are responsible for protecting data and lays down certain obligations on them for the processing of personal data. But the PDP Bill has still not been fully enacted and put into effect, meaning that the data protection regime in India remains in the transition phase.

On the other hand, the United States has a sectoral approach towards data protection with legislation varying with the nature of the data or the industry concerned. For instance, the Health Insurance Portability and Accountability Act

[34] Asaad Ahmad Qureshy, ―Cross-Border Data Transfer Requirements Under India DPDPA‖ Securiti, 2024 *available at*: https://securiti.ai/cross-border-data-transfer-requirements-under-india-dpdpa/ (last visited April 1, 2025).

[35] ―What is GDPR, the EU's new data protection law?,‖ GDPR.eu, 2018 *available at*: https://gdpr.eu/what-is-gdpr/ (last visited April 1, 2025).

(HIPAA) shields health-related information, whereas the Gramm-Leach-Bliley Act (GLBA) regulates financial institutions' treatment of personal information. The California Consumer Privacy Act (CCPA) is among the most widely known state-level data protection acts, providing California residents with specific rights over personal data, such as the right to access and erase data. Still, there is no single federal data protection law in the US similar to the GDPR or India's PDP Bill. This patchwork framework has been criticized for its failure to develop a unified framework for safeguarding personal data and maintaining data privacy across various industries.

The most significant difference between the US and the EU is the framework for data subject consent. The GDPR mandates explicit, informed consent to process data, while under the US regime, consent tends to be implicit, and users may be less in control of what happens to their personal data. Moreover, the EU has robust enforcement powers under the GDPR, including high fines for non-compliance, while enforcement in the US tends to be more restricted and divided by sector.[36]

The contrast between the EU, the US, and India brings into focus the necessity of a unified and holistic global system to deal with data protection issues and cybercrime. India's Personal Data Protection Bill subscribes to the GDPR's focus on users' rights and data processors' responsibilities. India, however, needs to address concerns such as data localization, cross-border flows of data, and the establishment of a specific regulatory agency for effective enforcement. The PDP Bill's international standards of data breach notifications and data subject rights are acceptable, but the real test is to see how India will incorporate future technological advancements and the increased risks of cybercrime.

7. ROLE OF THE DATA PROTECTION AUTHORITY IN INDIA

The position of the Data Protection Authority (DPA) in India is very important in ensuring the implementation, enforcement, and compliance with data protection legislation. The Personal Data Protection Bill, 2019 (PDP Bill), pending consideration, sets the stage for the establishment of a Data Protection Authority of India (DPA) responsible for regulating and overseeing data protection activities in India. The DPA will be tasked with ensuring compliance of organizations with the provisions of the PDP Bill, handling complaints from data subjects, investigating offenses, and levying penalties for non-compliance.

The Data Protection Authority will be at the forefront of regulating data protection practices and cybersecurity practices in India. Its core duties will be to monitor and enforce data protection law compliance, investigate allegations of data breaches and infringements, and advise the government on legislative and policy issues pertaining to data protection and privacy. The DPA will also carry out audits and investigations to ascertain that organizations treat personal data in a secure and legal way.

One of the most important roles of the DPA will be the registration and regulation of data fiduciaries, which are entities that process personal data. Data fiduciaries will be obligated to keep detailed records of their data processing operations, which the DPA will be able to audit. If there is a data breach, the DPA will be able to investigate and impose penalties depending on the gravity of the offense.[37]

The Data Protection Authority will also be empowered to issue codes of practice and guidelines to assist organizations in complying with the provisions of the PDP Bill. It will be responsible for resolving issues of data breaches, processing of data without authorization, and misuse of data, and for

[36] Cristina Pop, ―EU vs US: What Are the Differences Between Their Data Privacy Laws?‖ Endpoint Protector Blog, 2023 *available at*: https://www.endpointprotector.com/blog/eu-vs-us-what-are-thedifferences-between-their-data-privacy-laws/ (last visited April 1, 2025).

[37] ―The Digital Personal Data Protection Bill, 2023,‖ PRS Legislative Research *available at*: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023 (last visited April 1, 2025).

ensuring the protection of rights of data subjects. The DPA will operate in conjunction with other enforcement agencies and regulators, such as the Information Technology (Reasonable Security Practices and Procedures) Rules, 2011, that regulate data protection under the IT Act.

The establishment of an independent DPA is critical to enhancing data protection in India, offering an institutional framework to ensure compliance with data protection legislation, investigate grievances, and provide advice to individuals and organizations. The PDP Bill proposes a multi-member board for the DPA comprising law, technology, and data protection experts. This autonomous body will be provided with the required powers to deal with the fast-changing arena of cybercrime and data protection so that India's data protection framework continues to remain effective and agile in the face of emerging threats in the digital world.

Finally, the Data Protection Authority will be an important institution to protect privacy and data security in India. Its function of making sure the PDP Bill is complied with will assist in making a transparent and accountable framework for data processing that is crucial for the protection of individuals' right to privacy in the digital age.

8. CONCLUSION

The development of cybercrime in India raises tremendous challenges to policymakers, law enforcement, and the justice system. The violent boom in technology, the internet, and the growing digitalization of society exposed the country to a variety of cybercrimes, ranging from financial fraud to identity theft, cyber terrorism, cyberbullying, and online harassment. As the virtual world keeps changing, it is obvious that the problem of combating and preventing cybercrime is by no means easy and needs constant readjustment of laws and an efficient, multi-pronged strategy.

The Information Technology Act, 2000 (IT Act) was India's initial serious effort to regulate cyberspace and deal with cybercrime. It set legal grounds for the prosecution of cybercriminals and laid the framework for protecting electronic records, digital signatures, and secure electronic transactions. In spite of the very first steps towards regulation, the Act came under criticism in some key aspects as the digital world dramatically grew. The necessity for frequent amendments to the IT Act was realized, especially as cybercrimes evolved, necessitating more technical legal provisions to tackle them. The IT Act amendments like the addition of Section 66A and the subsequent deletion of this provision by the Supreme Court indicated the intricacies involved in governing cyberspace and ensuring that provisions of law hit a balance between safeguarding people's rights and discouraging criminal activity.

Cybercrime has unique characteristics that make it distinctly different from traditional crimes, which has caused significant challenges for legal systems around the world, including India. One of the foremost challenges is the cross-border nature of cybercrime. Unlike traditional crimes that are typically confined within specific geographical jurisdictions, cybercrimes can be committed from any location with internet access. This generates jurisdictional problems that make both investigation and prosecution of cybercrimes difficult. Though India has strengthened cybercrime law enforcement, e.g., with the creation of specialized cybercrime cells and standalone cyber forensics units, these initiatives tend to be impeded by the absence of resources, skills, and coordination among national and global enforcement agencies.

In addition, the changing environment of frontier technologies like artificial intelligence (AI), blockchain, cryptocurrency, cloud computing, and the Internet of Things (IoT) has brought more complexities to combating cybercrime. These technologies, as much as they bring with them great efficiency and innovation, also afford new space for

cybercriminals to take advantage of vulnerabilities. For example, AI can be employed in launching more competent and autonomous cyberattacks, and blockchain can afford a space for making anonymous financial transactions, which makes it difficult to track criminal activity. The absence of an explicit legal framework to deal with these new threats creates numerous gaps in prosecuting cybercriminals. Additionally, the absence of global consistency in tackling cybercrime means that there are enforcement issues because cybercriminals can be located in various jurisdictions, frequently beyond the jurisdiction of national laws.

Another pertinent area of concern is the protection of individuals' data and privacy. With more personal information being archived and processed online, there is an increased threat of data breaches and invasion of privacy. India's current data protection legislation, including the Aadhaar Act and the Personal Data Protection Bill, 2019, are moves in the right direction, but more needs to be done to protect people's rights in the digital era. The increasing use of biometric data and big data offer opportunities as well as risks, with misuse of these data having the potential to cause privacy breaches, identity theft, and even cyber terrorism. Legal frameworks for the protection of personal data, together with robust enforcement measures, must be in place to safeguard the privacy and integrity of individuals.

As India seeks to develop a stronger and better system for combating cybercrime, a number of important areas need to be focused on. Education and training of police officers and judiciary personnel in handling cybercrime cases and comprehending the intricacies of digital evidence are imperative. Law enforcement bodies must be supplied with the equipment and technology they need to probe and prosecute cybercrimes successfully. For this purpose, partnership among the government, law enforcement agencies, business entities, and international bodies is vital. The capacity development of law enforcement bodies has to be accompanied by robust national and international cybercrime cooperation mechanisms that allow nations to collaborate to counter transnational cybercriminal syndicates.