INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

FROM PRIVACY TO PROTECTION: EVALUATING INDIA'S EVOLVING DATA PROTECTION REGIME

AUTHORED BY - NAVYA YADAV[1]
CO AUTHOR - AXITA SRIVASTAVA[2]

ABSTARCT

With the advancement of technology around the word and easy access to internet at cheaper price every human being has fallen in trap to use technology in their day-to-day life making the issues of data protection and right to privacy a debatable topic and a topic to be focused upon. Data privacy basically refers to the protection of personal information ensuring that individual have control over how their data is collected, processed and stored both data protection and privacy are interrelated issues regarding internet governance. We all must have come across the expression, "Data is the new oil" which simply says that data is a valuable asset that is being explored in order to gain profit. Service providers who are responsible to manage the websites, applications and social media platforms often collected and store user's personal data with objective of providing adequate service as required by users, usually they have the responsibility of protecting the personal data of the users form unauthorised access however these platforms fail to protect the data collected which results to data breach and exposure of users sensitive data to unauthorised parties who can use the personal data to defraud and harass the users or send unwanted adverts without the users consent infringing users fundamental rights. Simultaneously, numerous accusations concerning breaches of privacy rights have arisen over time involving both the Government and Private Commercial Entities in India. Such accusations were also presented in the Courts of Law, where the Courts issued landmark Judgments that included guidelines and rulings. It is therefore crucial to examine all these legal advancements concerning the Right to Privacy and Data Protection to comprehend the level of security provided by the Indian legal system to citizens regarding their Right to Privacy. Nonetheless, it has been established that the Indian Legal System has sufficiently acknowledged the Right to Privacy, and significant measures have been implemented to curb data theft and misuse of sensitive information. However, considerable advancement is still required to broaden the scope of data protection today to safeguard the

[1] Author is Student of Amity University Lucknow.
[2] Co Author is Assistant Professor of law Amity Law School Amity University Lucknow.

ISSN: 2582-6433

Right to Privacy of Indian citizens. The right to privacy has been recognised as a basic human right in India through numerous judicial rulings and as a legal right via statutes. It has been also acknowledged in global agreements like the Universal Declaration of Human Rights, 1948, and the International Covenant on Civil and Political Rights, 1976, along with numerous other international and regional human rights treaties. Up until 2023, India lacked a separate law or system to regulate data protection. The Information Technology Act, 2000 (IT Act) and the rules issued under it established the foundation on which the data protection structure was cantered. This paper will be covering all legislations and regulations covering data protection and privacy laws, while stating issues surrounding data privacy and data protection also the challenges faced in ensuring safety of users.

Keywords: Data Protection, Privacy, Sensitive Information, Confidentiality, Personal Information, Information Technology, Legal Right.

INTRODUCTION

Individuals, both as members of society and as consumers, must have the ability to assert their right to privacy and safeguard themselves and their information from exploitation. This is especially true regarding our personal data. Data protection is fundamentally about preserving our inherent right to privacy, a right recognized in international and regional laws and agreements. Data protection is typically understood as legislation that is crafted to safeguard your personal information, which is gathered, processed, and stored using automated methods or is intended to be included in a filing system. In contemporary societies, to enable us to manage our precious information and defend ourselves against misuse, it is crucial that data protection laws regulate and influence the actions of various businesses and governments. As many institutions have shown repeatedly that unless there are rules restricting their actions, they will misuse our information.

Data privacy and data security hold great significance for both users and companies. The idea of privacy is regarded as a basic human right in numerous legal systems since privacy is vital for a free society. Data privacy is recognized as the entitlement of individuals to decide who may access their personal data, what personal data is disclosed, and the safeguarding of this information from unauthorized entities that should not have access. On the other hand, data protection is viewed as the duty of companies to safeguard their user's personal information from unauthorized access. It encompasses implementing policies to prevent the misuse or

ISSN: 2582-6433

unauthorized access of user's personal data and applying protective measures against all weaknesses in their data collection and storage systems. Businesses are also required to provide users with an explanation of the measures implemented to safeguard data from breaches, sales, and any forms of intrusion in their privacy policies. All privacy policies should be available on the company's websites detailing with every type of personal information gathered, its usage, the parties with whom it is shared, and what is the methods of its protection. This level of transparency regarding the collection of user data, its sharing practices, and management demonstrates to users that the company can be trusted to handle their personal information responsibly.

Before the enactment of the Digital Personal Data Protection Act, 2023 by the Indian Parliament, safeguarding data in India encountered numerous challenges and frustrations because of a lack of adequate legislative structures. India, as the largest hub for outsourced data, can easily attract cyber criminals primarily because of inadequate legal protections. Before the formation of the Digital Personal Data Protection Act, 2023, the framework for data protection was located in specific sections of the Information Technology Act, 2000, also in its rules called Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and also, personal data is safeguarded under Article 21 of the Constitution of India.

Supreme Court of India has recognized the right to privacy as a part of the right to life and personal liberty under Article 21. In 2017, the Supreme Court of India viewed the right to privacy as a constitutionally safeguarded right in the Puttaswamy ruling, which is often referred to as the Right to Privacy judgment. The court highlighted India's absence of a thorough privacy law and the constraints of the current Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, or SPDI Rules, established in 2011. In response to the Right to Privacy ruling, the Indian government prepared draft legislation aimed at safeguarding the privacy of its citizens. Previous iterations of the Personal Data Protection Bill underwent extensive examination and ultimately failed, such as the Data Protection Bill 2021, which bore certain resemblances to the European Union's General Data Protection Regulation (GDPR). It got revoked in August 2022.

PRIVACY AND DATA PROTECTION IN INDIA UNDER

ISSN: 2582-6433

CONSTITUTIONAL AND STATUTORY PROTECTION[3]

At present, India does not have a single, comprehensive legislation that specifically addresses data privacy and protection in a definitive manner. However, this does not mean that the right to privacy or protection of personal data is completely unregulated. In the absence of a standalone law, there exists a combination of constitutional guarante**es** and statutory provisions that indirectly but effectively address issues concerning privacy and data protection.

Broadly, privacy in India is safeguarded through two major legal avenues:

1. Constitutional Protection
2. Statutory Protection

Constitutional protection of Privacy

Although the Constitution of India does not explicitly mention the "Right to Privacy" as a Fundamental Right, the Supreme Court has interpreted it as an essential part of the Right to Life and Personal Liberty under Article 21, and as implicit in various other rights under Part III of the Constitution. The landmark judgment in the case of *Justice K.S. Puttaswamy (Retd.) vs. Union of India* (2017) affirmed that the Right to Privacy is a Fundamental Right, forming an inalienable part of human dignity and liberty. A nine-judge constitutional bench unanimously held that privacy is inherent in Article 21. However, like most fundamental rights, it is not absolute. It is subject to reasonable restrictions under Article 19(2) in the interest of sovereignty, national security, public order, and similar considerations. Interestingly, even before the Puttaswamy verdict, several dissenting opinions from earlier cases had voiced that privacy must be recognized under Article 21. These opinions laid the foundation for a broader understanding of civil liberties in a digitally evolving society. Article 21 continues to evolve, absorbing new rights and interpretations to keep pace with the changing demands of the modern world, and privacy is now firmly part of its expanding scope.

Statutory Protection

While constitutional protection lays the foundational right to privacy, several statutory laws provide more specific and operational protections relating to data and information handling. These laws may not directly address privacy, but they include important safeguards that protect individuals against unauthorized use or disclosure of personal data. Some of the key statutes

[3] Bandita Das and Jayanta Boruah. (2020). Right To Privacy and Data Protection under Indian Legal Regime. DME Journal of Law, Volume 1, pp. 63-70.

ISSN: 2582-6433

include:

1. **Information Technology Act, 2000**

The Information Technology (IT) Act, 2000 was India's first legislation addressing electronic commerce, governance, and cybercrime. It contains provisions relevant to data security and unauthorized access. Some important sections include:

- **Section 43**: Imposes penalties for unauthorized access to computer systems and data, including destruction, alteration, or misuse of data.
- **Section 65**: Criminalizes intentional tampering with source code or information stored in a computer.
- **Section 66**: Deals with data theft and prescribes penalties for hacking and data breaches.

Penalties under these provisions may include imprisonment up to three years, fines up to ₹5 lakhs, or both. Moreover, companies involved in breaches can also be held liable, and their managers or directors may be held personally accountable. The IT (Amendment) Act, 2008 strengthened the original Act by introducing Section 69A, which allows the government to intercept, monitor, or decrypt data in the interest of national security. Although controversial, the Supreme Court upheld its constitutional validity in 2015, citing the presence of adequate procedural safeguards.

2. **Indian Penal Code, 1860**

The IPC does not have direct provisions for data privacy violations. However, it does criminalize certain related acts. **Section 408**: Penalizes criminal breach of trust by a clerk or servant, which can include unauthorized use or disclosure of data. Although not tailored for data privacy, these provisions can be invoked in cases involving misuse of personal or confidential information.

3. **Intellectual Property Law**

In India, Copyright Act, 1957 deals with matters of copyrighted piracy (theft) and for such piracy impose compulsory punishment which is in proportion to the seriousness of offence. Section 65 of the Act provides that whoever makes use of a computer or an infringing copy of computer program shall be punishable with imprisonment which may extent to 3 years or with fine. Moreover, wherein an author produces a books, records or broadcast program by collecting information from different source by devoting time, money, labour and skill amounting to literally work within the meaning of Copyright Act are protected as being

ISSN: 2582-6433

copyright of that person. Thus, the outsourcing parent entity may have recourse under the Copyright Act for any violation occurring to that data bases.

4. **Credit Information Companies (Regulation) Act, 2005 (CICRA)**

CICRA regulates how credit information of individuals and companies is collected, stored, and shared. It mandates strict privacy norms for credit information companies. Any unauthorized modification or disclosure of data can result in liability. The Act enforces accountability by making entities that handle credit-related information responsible for data protection, and these principles are also overseen by the Reserve Bank of India (RBI).

5. **Indian Contract Act, 1872**

Contracts between parties often contain confidentiality clauses that serve as a form of privacy protection. When parties agree not to disclose any personal information without consent, breach of such clauses mentioned in contract can result in legal liability. For instance, in insurance contracts, insurers collect sensitive personal information from customers. Unauthorized disclosure of such information by insurers may result in an action for damages based on breach of a contract. This is particularly significant in commercial settings where data-sharing agreements are increasingly common and prevalent.

RECOGNITION OF RIGHT TO PRIVACY BY JUDICIARY (A CRONOLOGICAL ANALYSIS)

The Indian Constitution does not explicitly define or mention the term "privacy." Yet, the essence of privacy, the right of an individual to live with dignity, free from unwarranted interference is a fundamental aspect of human existence. It includes the freedom to make personal choices, the right to be left alone, and the ability to control one's personal information. However, in the absence of awareness and clear codification, many people are deprived of this right or remain ignorant of its existence. Recognising this gap, international human rights instruments and domestic courts have played a significant role in affirming privacy as a human right. In India, it is through judicial pronouncements that the right to privacy evolved from a vague, implicit idea into a well-recognised and enforceable Fundamental Right under Article 21 of the Constitution.

1. **MP Sharma v. Satish Chandra (1954)[4]**

[4] MP Sharma v. Satish Chandra (1954) SCR 1077 (SC).

ISSN: 2582-6433

In this early case, the petitioners challenged search and seizure powers on the ground of privacy violation. However, the Supreme Court held that the Constitution does not recognise the Right to Privacy as a Fundamental Right, and such state action could not be declared unconstitutional solely on the ground of privacy infringement. The judgment reflected a limited understanding of individual liberty at the time.

2. **Kharak Singh v. State of Uttar Pradesh (1963)**[5]

This case questioned the legality of police surveillance under Regulation 236(b) of the UP Police Regulations. While the majority upheld most parts of the regulation and denied that privacy was a fundamental right, it struck down night-time domiciliary visits as violative of "ordered liberty." Significantly, Justice Subba Rao dissented, asserting that the Right to Privacy is implicit in Article 21, even though not explicitly mentioned. His opinion laid early groundwork for future recognition of privacy.

3. **Gobind v. State of Madhya Pradesh (1975)**[6]

In this case, police regulations permitting surveillance of habitual offenders were challenged. The Supreme Court recognised a limited Right to Privacy, stating it was not absolute and could be curtailed in the interest of compelling public interest. The Court accepted that privacy could evolve with societal needs and could be derived from Articles 19(1)(a), 19(1)(d), and 21.

4. **R.M. Malkani v. State of Maharashtra (1973)**[7]

Even though this judgment preceded Gobind, it holds relevance. The Court held that phone tapping without legal procedure violated the Right to Privacy, hinting at the necessity of procedural safeguards. The case laid the foundation for future judgments on surveillance and privacy in telecommunication.

5. **R. Rajagopal v. State of Tamil Nadu (1994)**[8]

Popularly known as the "Auto Shankar case", this judgment was a major leap in privacy jurisprudence. The Court held that an individual's right to publish or not publish their life story without state interference was protected under Article 21. It clearly distinguished between private and public life and upheld the citizen's right to protect personal data and reputation.

[5] Kharak Singh v. State of Uttar Pradesh (1963) AIR 1295 (SC).
[6] Gobind v. State of Madhya Pradesh (1975) 2 SCC 148.
[7] R.M. Malkani v. State of Maharashtra (1973) AIR 157 (SC).
[8] R. Rajagopal v. State of Tamil Nadu (1994) 6 SCC 632.

ISSN: 2582-6433

This case significantly expanded the contours of privacy in relation to freedom of expression and media.

6. People's Union for Civil Liberties (PUCL) v. Union of India (1997)[9]

This case dealt specifically with telephone tapping and its legal validity. The Supreme Court declared that telephone conversations are part of an individual's private life, and any surveillance or interception must follow legal procedure. The Court held that privacy includes communication privacy, and any tapping without statutory backing violates Article 21.

7. Malak Singh v. State of Punjab & Haryana (1981)[10]

In this case, the Court upheld that State surveillance, if done within legal limits and without infringing personal liberty, does not violate privacy rights. However, it emphasized that any abuse or overreach would be unconstitutional, indicating the Court's cautious approach in balancing individual rights with state interest.

8. Selvi v. State of Karnataka (2010)[11]

This judgment was critical in establishing mental and bodily privacy. The Court held that narco-analysis, polygraph tests, and brain mapping, when conducted without consent, violated the individual's personal autonomy, mental integrity, and Article 20(3) rights against self-incrimination, as well as Article 21. This ruling strengthened the idea of bodily privacy and informed consent.

9. Shreya Singhal v. Union of India (2015)[12]

In this landmark judgment, the Supreme Court struck down Section 66A of the IT Act, which criminalised online speech deemed "offensive" or "menacing." The Court held that the provision was vague and arbitrary, leading to censorship and surveillance, and thereby infringing on freedom of speech and privacy. This case reaffirmed that surveillance laws must be clear, proportionate, and justified.

10. Justice K.S. Puttaswamy v. Union of India (2017)[13]

This historic judgment by a nine-judge bench conclusively held that the Right to Privacy is a

[9] People's Union for Civil Liberties v. Union of India (1997) 1 SCC 301.
[10] Malak Singh v. State of Punjab & Haryana (1981) 1 SCC 420.
[11] Selvi v. State of Karnataka (2010) 7 SCC 263.
[12] Shreya Singhal v. Union of India (2015) 5 SCC 1.
[13] Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

ISSN: 2582-6433

Fundamental Right, intrinsic to life and liberty under Article 21. The Court overruled the earlier judgments in MP Sharma and Kharak Singh to the extent they denied privacy as a fundamental right. This case laid the foundation for all subsequent discussions on data protection, digital rights, and informational privacy.

11. K.S. Puttaswamy (Aadhaar Judgment) v. Union of India (2018)[14]

Following the 2017 ruling, this five-judge bench examined the Aadhaar Act's constitutionality. While the Court upheld mandatory Aadhaar for welfare schemes, it struck down Section 57, which allowed private companies to demand Aadhaar data. The Court emphasized the principles of data minimization, informed consent, and the necessity of a robust data protection regime. It reiterated the need to protect individuals' privacy in the digital space.

12. Anuradha Bhasin v. Union of India (2020)[15]

This case arose in the context of internet shutdowns in Jammu and Kashmir. The Supreme Court ruled that freedom of speech and trade via the internet is constitutionally protected, and any restriction must meet the test of proportionality. Although not exclusively a privacy case, it reinforced that digital access is essential to exercise privacy and expression rights in a modern democracy.

13. Supreme Court on WhatsApp Privacy Policy (Ongoing since 2021)[16]

Concerns have been raised regarding WhatsApp's sharing of user data with Facebook, raising issues of corporate surveillance and user consent. The Supreme Court has taken cognizance of the matter, seeking explanations from both the company and the government regarding privacy safeguards. The case is significant for developing norms around data sharing by private companies and will likely influence future data protection legislation.

RECOGNITION OF RIGHT TO PRIVACY UNDER INDIAN CONSTITUTION

[14] K.S. Puttaswamy v. Union of India (Aadhaar) (2018) 1 SCC 809.
[15] Anuradha Bhasin v. Union of India (2020) 3 SCC 637.
[16] Supreme Court of India (2021–Present), In re: WhatsApp Privacy Policy Case, W.P. (C) No. 313 of 2021. [Pending].

ISSN: 2582-6433

[17]The Constitution of India stands as the supreme law of land providing a foundational framework for governance and safeguarding the rights and freedoms of individuals. One of its most remarkable attributes is its dynamic nature, the ability to adapt to the changing needs of society. Over time, this adaptability has enabled the judiciary to expand the scope of constitutional rights, including the recognition of the right to privacy as a fundamental right. While the Constitution does not explicitly mention the term "privacy," the right to life and personal liberty enshrined under Article 21 has been interpreted to include it. Article 21 states "No person shall be deprived of his life or personal liberty except according to procedure established by law" This provision has been the bedrock for a broad range of rights, and the right to privacy is now understood as a natural extension of life and liberty. It safeguards an individual's autonomy, dignity, and freedom from unwarranted intrusion.

Over the years, the Supreme Court of India has played a crucial role in shaping right to privacy through a series of landmark judgments R. Rajagopal v. State of Tamil Nadu (1994) which is also popularly known as the Auto Shankar case, this was the first time when Supreme Court explicitly acknowledged that the right to privacy in Article 21. The Court held that a person has the right to safeguard the privacy of their personal life, including matters such as family, education, motherhood, marriage, procreation, and other aspects of intimate life. It also established that no one, including the State or any form of media, can publish personal details without consent of a person, unless the matter is of public record or public interest. State of Maharashtra v. Madhukar Narayan Mardikar (1991) This case reaffirmed that the right to privacy is universal right and it does not depend on a person's character or his background. The Court ruled that even a woman of "easy virtue" has the right to privacy, and no one has the authority to intrude upon her personal life without her consent. This judgment emphasized that dignity and privacy are essential to all individuals, regardless of their social standing or status in society.

People's Union for Civil Liberties v. Union of India (1997). In this well-known "Phone Tapping Case", the Supreme Court held that any form of telephone conversations is part of an individual's personal and private life, and any unauthorized interception constitutes a serious breach of privacy. While acknowledging that surveillance may be permitted in specific situations to be conducted by the appropriate authorities involving public safety or national

[17] Nivedita Baraily (2021). An Analysis of Data Protection and Privacy Law in India. International Journal of Law Management and Humanities, Volume 4(1), pp. 1232-1234.

ISSN: 2582-6433

interest, the Court insisted that such measures must be as per law and follow proper procedure. The Court further clarified that surveillance must adhere to all standards laid out in the Indian Telegraph Act, 1885, and later, the Information Technology Act, 2000. These laws permit state surveillance only under clearly defined circumstances such as threats to sovereignty, integrity, public order, or national security, aligning with the reasonable restrictions permitted under the Constitution. Landmark decision in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India a nine-judge bench of the Supreme Court clearly held that the right to privacy is a fundamental right, protected under Articles 14, 19, and 21 of the Indian Constitution. This judgment overruled previous decisions that had denied privacy its rightful constitutional status and clarified that privacy is intrinsic to human dignity and liberty.

The Court also recognized that in the age of digital technology, privacy violations are not limited to state actions alone. Private entities such as corporations and digital platforms can also pose significant threats to individual privacy. Therefore, the protection of privacy must extend both vertically (against the State) and horizontally (against non-State actors). However, the Court acknowledged that, like other fundamental rights, the right to privacy is not absolute. Any limitation imposed on this right must pass the "triple test" laid down by the Court stating Legality (There must be a law in existence that justifies the encroachment), Legitimate Aim (The action must serve a legitimate state interest), Proportionality (The restriction must be necessary and proportionate to the aim pursued). This ruling cemented privacy as a core constitutional value also setting the foundation for the future of data protection laws in India.

LEGISLATIVE FRAMEWORK IN INDIA ON RIGHT TO PRIVACY SO FAR

1. Digital Personal Data Protection Act, 2023 (DPDP Act)

The Digital Personal Data Protection Act, 2023, serves as a comprehensive law governing the handling of personal data it is also recognized as India's central legislation on personal data protection. The Act introduces vital principles such as data minimization, user consent, and the recognition of individual rights, all aimed at safeguarding personal privacy. It lays down clear provisions concerning the collection, retention, and processing of such data. It applies to any entity domestic or foreign that processes the personal data of individuals residing in India. Non-compliance with its provisions can result in huge penalties, thereby underlining the importance of strictly following all its regulatory requirements.

ISSN: 2582-6433

2. Information Technology (IT) Act, 2000

The Information Technology Act, 2000 forms the foundational legal framework for governing cyber activities in India. Specific sections included in this act address issues related to data protection. Notably, Section 43A obliges companies to compensate individuals who suffer data breaches due to the company's negligence. Meanwhile, Section 72A penalizes any form of unauthorized disclosure of personal information acquired in the course of providing services. These sections ensure accountability and establish legal consequences for mishandling personal data.

3. Information Technology (Reasonable Security Practices and Procedures) Rules, 2011

Enacted under the IT Act, the 2011 Rules mandate that companies adopt adequate security protocols to safeguard sensitive personal data. This includes implementing strong password protections, encrypting data, and conducting regular security audits. Additionally, organizations are required to develop and disclose privacy policies that clearly explain how personal data is gathered, managed, and utilized. These rules are especially critical when handling highly sensitive information such as passwords, health records, and financial data.

4. Consumer Protection Act, 2019

The Consumer Protection Act, 2019 not only safeguards buyers from unfair trade practices but also extends its protection to the misuse of consumers' personal data. This Act provides individuals with the authority to challenge businesses that fail to comply with established data protection standards, particularly in contexts involving e-commerce or digital services. It offers legal avenues for consumers to file complaints and seek redressal when their personal information is misused or when their rights are violated.

5. Reserve Bank of India (RBI) Regulations on Payment Data

The Reserve Bank of India has implemented stringent data localization rules specifically for the financial sector. One such mandate is the 2018 Circular on Payment Data Localization, which requires all entities operating payment systems including banks, financial technology firms, and payment gateway providers to store all data related to payments exclusively in India. These regulations are designed to ensure that crucial financial data remains within India's jurisdiction and is readily accessible to Indian regulators and enforcement agencies, without dependence on foreign systems. This includes transaction information, customer details, and

ISSN: 2582-6433

account data. While certain types of foreign processing are permitted, such as those required for fraud prevention, a complete and current copy of the data must still be stored within Indian territory.

6. Telecom Regulatory Authority of India (TRAI) Regulations

TRAI has released significant recommendations concerning the privacy, ownership, and security of personal data in the telecom sector. Additionally, TRAI's framework emphasizes data minimization, requiring providers to collect only as much data as is necessary for delivering telecom services, and to store it securely. According to these guidelines, the ownership of personal data rests with the consumers, while telecom service providers (TSPs) act merely as custodians. It is mandatory for TSPs to obtain informed and explicit consent from users before collecting, processing, or sharing their data. The recommendations also uphold the Right to Be Forgotten, giving users the power to request the deletion of their data from telecom databases.

Key aspects of the TRAI's stance include:

- Telecom Data Localization: TRAI supports local storage of telecom-related data to prevent unauthorized access by foreign entities and ensure conformity with Indian legal standards. This aligns closely with the objectives of the DPDP Act, 2023, and the RBI's data localization directives.
- Oversight of Over-The-Top (OTT) Platforms: TRAI is contemplating bringing OTT platforms like WhatsApp and Zoom under regulatory scrutiny. TRAI seeks to ensure that they comply with data protection and localization norms akin to traditional telecom providers. These platforms handle massive volumes of communication data.
- Consumer Data Security: The authority mandates robust cybersecurity measures by telecom operators to guard consumer data from breaches. It is essential for all telecom providers to store and manage personal data exclusively within Indian jurisdiction, ensuring greater data sovereignty and legal accountability.

NEED OF SPECIFIC PRIVACY LAW

ISSN: 2582-6433

[18]Despite the presence of an existing legal framework and the initiatives undertaken by the government, the current statutes have not proven to be fully effective in safeguarding the right to personal privacy and ensuring robust data protection. Several gaps and shortcomings are evident in laws such as the Information Technology Act and the 2011 Rules. These deficiencies underscore the necessity for a specialized and comprehensive privacy law. The need for such legislation arises from the following key limitations in the current legal system:

a. Proposed amendments to the IT Act, specifically the insertion of Sections 48A and 72A, have not brought about any meaningful changes to the original legislation. The suggestions provided by the Standing Committee to the Ministry of Parliamentary Affairs have been received, but there has been no follow-through in terms of implementation or application.
b. Furthermore, the amendments fail to address vital aspects of data protection, such as the management of sensitive personal data, the adoption of safeguards during data collection, and the procedures for processing personal information.
c. The Ministry of Communications and Information Technology (MCIT) introduced the "2011 Rules" under Section 87(2) read with Section 43A of the IT Act. These rules primarily deal with sensitive personal data and information. However, their applicability is restricted only to corporate bodies or individuals situated within India.
d. Government authorities and state institutions are one which are excluded from the ambit of these rules. which provides for liability and compensation in cases of negligence. However, the statute does not define the exact quantum or limit of such compensation, leading to ambiguity.
e. Rule 4 of the 2011 Rules mandates that private sector service providers, such as Bharti Airtel Limited and Vodafone India Limited, must publish their privacy policies on their websites. In contrast, several state-run service providers have been reported to have failed in doing so. The absence of published privacy policies reflects a lack of commitment to data protection principles and raises serious concerns regarding enforcement.
f. The 2011 Rules are focused solely on the regulation of Sensitive Personal Data or Information (SPDI), which includes details such as passwords, biometric data, and medical records. However, there is limited oversight over non-sensitive personal information in the Indian legal framework. Moreover, the jurisdictional reach of Indian

[18] Bandita Das and Jayanta Boruah. (2020). Right To Privacy and Data Protection under Indian Legal Regime. DME Journal of Law, Volume 1, pp. 69-71.

ISSN: 2582-6433

laws remains constrained. Their applicability in certain cross-border scenarios is uncertain. For instance, it is unclear whether the IT Act or the privacy rules would apply to a company based in the United States that collects the SPDI of Indian nationals while those individuals are traveling in the US.

g. In addition to the aforementioned loopholes, there are several broader structural weaknesses in the Indian data protection regime including the Absence of a comprehensive law safeguarding the right to privacy in the private domain, Lack of clear classification distinguishing private, public, and sensitive information, No well-defined procedures governing the generation, processing, transmission, and dissemination of personal information, No established guidelines defining essential data protection principles such as data quality, proportionality, and transparency.

SOME STEPS TAKEN BY GOVERNMENT FOR PROTECTION OF DATA[19]

To address rising concerns over data protection and cybersecurity, and in response to growing international expectations, the Government of India has initiated several key measures. These efforts aim to enhance the country's cyber infrastructure, establish international credibility, and secure critical data assets. Two significant initiatives in this direction are the establishment of the Standardization Testing and Quality Certification (STQC) Directorate and the Computer Emergency Response Team- India (CERT-In).

Recognizing the global demand for Indian companies to meet international security standards, the Indian government, under the aegis of the Department of Information Technology (DIT), has established the STQC Directorate. This body plays a vital role in setting benchmarks for quality and security compliance in the IT sector. One of the major accomplishments of the STQC Directorate has been the development of an independent, third-party certification system for Information Security Management Systems (ISMS). This certification is based on BS 7799 Part 2, which is a widely accepted global standard for information security. Importantly, this system has received international accreditation from the Raad voor Accreditatie (RvA) of the Netherlands, reinforcing its credibility on a global platform. The scope of services offered by the STQC Directorate includes Testing of hardware and software products to ensure their

[19] Indian Law Officer LLP. 2024. Data Protection Laws In India. Available at: https://www.indialawoffices.com/legal-articles/data-protection-laws-in-india [Accessed 15 June 2025].

ISSN: 2582-6433

reliability and security, Certifying IT products and systems based on established security and performance standards, Training personnel in best practices concerning quality assurance and information security protocols. By providing such services, the STQC Directorate not only enhances the trustworthiness of Indian IT products but also helps build a workforce that is skilled in managing data securely.

To strengthen India's cyber resilience and actively participate in the global cybersecurity network, the Department of Information Technology (DIT) established the Computer Emergency Response Team – India (CERT-In). This national-level body functions as India's frontline defines against cyber threats and IT-related vulnerabilities. CERT-In plays a multifaceted role in safeguarding India's digital infrastructure and performs the following key functions like Acts as a central coordinating body for responding to cybersecurity incidents. It serves as a reliable and trusted point of contact available 24/7, particularly in emergency situations involving data breaches or attacks. Disseminates best practices in cybersecurity among system administrators, internet service providers, and other stakeholders. This helps organizations enhance their internal security frameworks. Enhances public awareness and knowledge about information security and related threats. CERT-In undertakes various initiatives to educate the Indian cyber user community about potential risks and preventive measures. Issues timely alerts and advisories about emerging cybersecurity threats. These include publishing vulnerability notes, incident bulletins, and security advisories to help organizations take proactive steps in securing their systems. Facilitates inter-organizational coordination by acting as a liaison between various sectors government bodies, private organizations, and academic institutions to collectively address cybersecurity challenges. Establishes international linkages by collaborating with similar institutions across the world. These partnerships allow for the exchange of threat intelligence, policy frameworks, and effective strategies to counter global cyber risks. Engages in research and development activities in collaboration with premier educational and research institutions. These efforts focus on improving the security of current systems and exploring solutions for emerging cybersecurity issues.

Through these roles, CERT-In not only responds to immediate cyber threats but also contributes to building a long-term security ecosystem in the country. the establishment of STQC and CERT-In reflects the Indian government's proactive and structured approach to data protection and cybersecurity. These institutions form the backbone of national efforts to secure

ISSN: 2582-6433

digital information, comply with international standards, and promote a safe digital environment for individuals, businesses, and government entities alike.

DATA PROTECTION, PRIVACY AND THE INFORMATION TECHNOLOGY ACT, 2000[20]

The Information Technology Act, 2000, which draws its foundation from the United Nations Model Law on Electronic Commerce, lays down several important provisions related to data protection and individual privacy. Over the years, it has become one of the key legislations addressing the use and misuse of electronic data in India. Section 43A of the Act provides that any organization or entity that fails to adopt reasonable security practices and procedures (RSPP) to protect Sensitive Personal Data or Information (SPDI), and as a result causes a wrongful gain to someone or a wrongful loss to another, will be liable to pay compensation to the affected individual. The term "reasonable security practices and procedures" refers to security protocols intended to safeguard sensitive information from unauthorized access, misuse, alteration, damage, disclosure, or destruction. These protocols can be mutually agreed upon by the involved parties (such as an employer and an employee), Prescribed under existing laws, or Specified by the Central Government, in cases where no such agreement or specific legal provision exists. This implies that if both parties decide in advance on a particular standard of data security through a contract or agreement, then the default government-prescribed rules would not be applicable.

Under Section 2(o) of the IT Act, “data” is broadly defined as any representation of facts, knowledge, instructions, or concepts that is prepared or stored in a formalized manner to be processed using a computer system or network. This includes all forms of data storage whether it's a computer printout, magnetic tape, optical disk, punched cards, or even internal computer memory. Meanwhile, Section 2(v) defines “information” in an even wider sense, covering not only data but also text, sound, images, voice, codes, computer programs, software, databases, microfilms, or even computer-generated microfiches. Section 72A establishes that if a service provider, while delivering services under a lawful contract, discloses personal information without consent, and does so intentionally or with knowledge that such an act may cause wrongful gain or loss, then the provider can face criminal punishment. This provision ensures

[20] Nivedita Baraily (2021). An Analysis of Data Protection and Privacy Law in India. International Journal of Law Management and Humanities, Volume 4(1), pp. 1232-1234.

ISSN: 2582-6433

that even private entities are held accountable if they misuse personal information in the course of executing their service obligations. While Section 72A covers private actors, Section 72 deals with government officials or authorities. It makes it a criminal offense for a public servant to reveal personal records or information accessed during the course of their official duties, without the consent of the concerned individual, unless the disclosure is permitted under another existing law.

Introduced under Section 43A, these Rules lay down what qualifies as Sensitive Personal Data or Information (SPDI). According to the Rules, SPDI includes any Passwords, Financial details such as bank account or card information, Health-related data, including physical, physiological, or mental conditions and medical history, Sexual orientation, Biometric data. In addition, the Rules also define "personal information" as any piece of information related to a natural person that can identify them either directly or indirectly. These definitions help in setting clear boundaries and responsibilities for organizations handling personal data, especially in sectors such as healthcare, finance, telecom, and e-commerce.

PERSONAL DATA PROTECTION BILL, 2019 was introduced with the objective of regulating the processing of personal data by both government entities and private companies, whether domestic or international, that handle the personal information of individuals located in India. Personal data, as defined in the Bill, includes characteristics, traits, and attributes that can identify an individual. The Bill further classifies certain categories of personal data as sensitive, such as financial details, biometric information, religious beliefs, and other types as may be notified by the government. To empower individuals, the Bill lays down a set of rights regarding their personal data. These include the right to be informed about whether their data has been processed, the right to correct or update inaccurate, incomplete, or outdated data, and under certain conditions, the right to transfer their data from one data fiduciary to another. The Bill also permits individuals to withdraw their consent, in which case the fiduciary is restricted from further disclosing the data if it is no longer necessary for the stated purpose.

A data fiduciary, according to the Bill, refers to any individual or organization that determines the purpose and means of processing personal data. Such processing is bound by limitations concerning purpose, collection, and storage, meaning data can only be processed for purposes that are clear, specific, and lawful. To ensure that individuals' rights are respected, data fiduciaries are required to adopt transparency and accountability measures. These include the

ISSN: 2582-6433

implementation of security safeguards to prevent misuse of data, setting up a grievance redressal mechanism, and taking additional precautions while handling the sensitive personal data of children, such as verifying age and obtaining parental consent.

While certain sensitive personal data may be transferred outside India with the explicit consent of the individual and subject to specific conditions, it must still be stored within the country. However, some categories of data, identified as critical, are mandated to be processed solely within India. To oversee the implementation and compliance of the provisions of the Bill, the establishment of a Data Protection Authority has been proposed. This Authority will be composed of a Chairperson and six members, each with a minimum of ten years' expertise in fields related to data protection and information technology. The Authority will be tasked with ensuring that personal data is protected, preventing its misuse, and upholding the responsibilities laid out in the Bill. Its decisions can be challenged before an Appellate Tribunal, and any appeals against the Tribunal's decisions can be made to the Supreme Court. Furthermore, the Bill provides the Central Government with the power to exempt any of its agencies from certain provisions of the Act, if such exemptions are deemed necessary for safeguarding national sovereignty, security, public order, or to maintain cordial international relations, or to prevent incitement to commit cognizable offences relating to these concerns. Strict penalties are proposed in the event of violations. For instance, if a data fiduciary processes or transfers personal data in contravention of the law, it can face a penalty of up to ₹15 crores or 4% of its annual global turnover, whichever is higher. If a fiduciary fails to carry out mandatory data audits, it may be penalized up to ₹5 crores or 2% of its turnover. Moreover, re-identifying anonymized personal data without obtaining consent is considered a serious offence, punishable with imprisonment of up to three years, a fine, or both. The Bill also proposes amending relevant sections of the Information Technology Act, 2000, particularly those related to compensation for failure to safeguard personal data, in order to harmonize existing laws with the new data protection regime.

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

The Digital Personal Data Protection Act, 2023 officially became law after it was passed by both Houses of Parliament and received the President's assent on 11th August 2023. This legislation has been designed with the key objective of regulating how digital personal data is processed while ensuring that the privacy rights of individuals are respected, balanced with the legitimate need to use such data for legal purposes. The Act applies to personal data processed

ISSN: 2582-6433

within India, and also extends its scope to cover data processed outside India, but only when such processing is tied to activities like offering goods or services to individuals located in India. However, it excludes data that an individual may use for personal or household purposes, and also data that the individual has made publicly available themselves.

Understanding the concept of data "processing" is vital in the context of this Act. It broadly refers to any action taken on digital personal data whether collecting, recording, storing, retrieving, using, sharing, or even erasing such data. The law defines the person whose data is being processed as the Data Principal, while the Data Fiduciary is the entity or person who determines why and how that data is to be processed. One of the foundational principles of the Act is that data can only be processed if it is done in accordance with the provisions of the law and for a lawful purpose meaning a purpose that is not specifically prohibited by law. Importantly, data must only be processed with the consent of the individual, or in specific situations deemed as legitimate use. The consent provided by the Data Principal must be free, specific, clear, informed, and unambiguous. The Data Fiduciary must present a clear notice when requesting consent, outlining what data will be processed and why. This notice must also explain how an individual can raise a grievance with the Board if they believe their data rights have been violated. Consent requests must be drafted in plain language and should be made available in English or any of the official Indian languages listed in the Eighth Schedule of the Constitution.

Data Principals are granted the right to withdraw their consent at any time, and this process should be as easy as the process through which consent was originally given. If the data in question pertains to a child (defined as someone under 18 years of age) or a person with a disability, then the consent of a parent or legal guardian is required. The Act also places a number of duties on Data Fiduciaries. These include making sure that personal data used for decision-making is accurate, complete, and consistent; adopting technical and organisational safeguards to comply with the Act; protecting data from breaches by implementing adequate security measures; notifying both the individual and the Board in case of a data breach; deleting data once the purpose of processing is fulfilled or if consent is withdrawn unless retention is legally necessary and providing mechanisms to handle grievances.

Entities that meet specific criteria based on the volume or sensitivity of data handled, or based on potential implications for national interests like sovereignty or public order, may be

ISSN: 2582-6433

classified by the Central Government as Significant Data Fiduciaries (SDFs). These fiduciaries carry additional responsibilities, such as appointing a Data Protection Officer based in India to handle grievances, hiring an independent data auditor, and conducting regular Data Protection Impact Assessments and audits. The Act also ensures several rights for Data Principals. They have the right to request a summary of the data that has been processed by a fiduciary and details of any other fiduciaries with whom the data has been shared. This right, however, is restricted when data is shared for law enforcement or legal purposes. Data Principals can also request correction, completion, updating, or erasure of their personal data, although erasure may not always be possible if the data needs to be retained for specific legal obligations. Moreover, individuals are entitled to effective redressal mechanisms for any breach or mishandling of their data, and grievances must be addressed within a reasonable timeframe.

At the same time, Data Principals are expected to fulfil certain responsibilities. They are required not to impersonate others while sharing data, must refrain from hiding material information, and should avoid lodging false or malicious complaints. To monitor and enforce the law, the Data Protection Board of India, established under Section 18 of the Act, has been vested with various powers. The Board can issue directions to mitigate or remedy breaches of personal data, investigate such breaches, and impose penalties on violators.

Despite the many positive and protective elements of the Act, certain concerns remain. Notably, the legislation does not contain any provision for compensating individuals in the event of a data breach. While penalties are imposed on violators, these fines are credited to the Consolidated Fund of India, not to the affected individuals. Furthermore, the Central Government is entrusted with the authority to appoint members of the Data Protection Board, with short tenures and the possibility of reappointment, which could potentially affect the independent functioning of the Board. The Act also provides broad exemptions for State agencies, allowing them to process data without being subject to its provisions if it is in the interest of India's sovereignty, national security, public order, or relations with foreign states. This wide latitude could lead to excessive collection and retention of data, potentially infringing upon the fundamental right to privacy.

Additionally, some situations are exempt from the requirement of notice and consent such as when personal data is processed to enforce legal claims or in criminal investigations, which may raise transparency concerns. Also, the erasure of data is not absolute and may be

ISSN: 2582-6433

disallowed if the data is needed for specific reasons. The law allows cross-border data transfers unless restricted by a list of prohibited countries notified by the Central Government. Moreover, the Central Government has the authority to request any information from the Data Fiduciary or the Data Protection Board, but the Act does not clearly define what kind of information can be demanded, leaving room for possible misuse. Although the Act has become law, it has not yet been brought into force. The government is expected to issue a set of detailed rules that will outline the practical aspects of implementing the law. These upcoming rules are expected to clarify procedures related to consent, handling of children's data, breach notifications, grievance redress, exemptions, and other important operational matters. Until the Digital Personal Data Protection Act officially comes into effect, the existing framework under the Information Technology Act, 2000 and the IT Rules of 2011 will continue to govern data protection in India.

The Act emphasizes consent-based processing, requiring that any data collection be accompanied by free, specific, informed, and unambiguous consent. It also mandates transparency obligations on data fiduciaries, including clear notices and accessible grievance mechanisms. By introducing the role of a Data Protection Board of India, the Act establishes a regulatory body with powers to investigate breaches and impose penalties, signalling a shift toward accountability and governance in the data ecosystem. Moreover, the categorization of certain entities as Significant Data Fiduciaries (SDFs) adds another layer of regulatory depth. These entities are required to appoint Data Protection Officers, conduct regular data audits, and perform Data Protection Impact Assessments, thus introducing stronger oversight mechanisms for large-scale or sensitive data processing operations. The Act's inclusion of children's data protection and restrictions on international data transfers except to nations restricted by the government—also highlights its attention to critical aspects of global data governance.

Despite these strengths, the DPDP Act is not without notable weaknesses. One of the main criticisms is the lack of provision for compensation to individuals whose data privacy is violated, which limits direct relief to affected persons. Another major concern is the extensive exemptions granted to State agencies on broad grounds such as national security, public order, and friendly international relations. Such open-ended exemptions could potentially undermine the fundamental right to privacy, as they permit data collection and processing without adequate oversight or limitations. Some weaknesses that invite scrutiny include:

ISSN: 2582-6433

- Appointments to the Data Protection Board: The Central Government retains control over the selection and tenure of members, raising concerns about the Board's independence and autonomy.
- Consent exemptions: The Act waives consent requirements in several contexts, including law enforcement and legal claims, which may dilute individual control over personal data.
- Ambiguity in enforcement mechanisms: Although the Act outlines penalties, these fines are paid to the Consolidated Fund of India, offering no compensation to the data principal, and it remains unclear how enforcement will be uniformly applied across sectors.

In addition to these weaknesses, the challenges in enforcement are considerable. First, the Act's successful implementation hinges on the timely and effective notification of subordinate rules and procedures by the Central Government. Many key aspects including the framework for grievance redress, the technical standards for data protection, and the operational details of the Board—remain undefined as of now. Furthermore, there is a lack of widespread awareness and digital literacy among the population, especially in rural and semi-urban areas, which may hinder the ability of individuals to understand and exercise their rights effectively.

Another practical challenge lies in compliance costs, particularly for small and medium enterprises (SMEs) that may lack the infrastructure to implement stringent data protection measures. The Act also demands technological readiness, such as strong data governance frameworks, privacy-enhancing technologies, and trained personnel, which are still in short supply across many sectors. Additionally, cross-border enforcement remains a grey area although the Act applies to entities outside India if they process data in connection with offering goods or services to Indians, enforcing such obligations across jurisdictions will be complex without reciprocal arrangements or international cooperation.

In conclusion, while the DPDP Act, 2023, represents a progressive leap in India's digital governance landscape, its enforcement will demand not just legal compliance but also institutional independence, public awareness, and technological capacity-building. Addressing the current gaps and ambiguities will be essential for the Act to truly protect personal privacy and ensure accountability in the expanding digital economy. Only with a careful balance between state interests, individual rights, and practical enforceability can the law fulfil its

ISSN: 2582-6433

intended promise of a privacy-respecting digital India.

LEGAL FRAMEWORKS ON DATA PRIVACY AND DATA PROTECTION IN NOTABLE JURISDICTIONS[21]

The General Data Protection Regulation (GDPR) – European Union

The General Data Protection Regulation (EU) 2016/679, widely referred to as GDPR, is globally recognized as one of the most far-reaching and detailed data protection laws. Adopted by the European Parliament and Council in April 2016, it came into force on May 25, 2018, replacing the previous Data Protection Directive 95/46/EC. Its main goal is to regulate how organizations, both within and outside the EU, handle the personal data of EU residents, ensuring the free flow of such data while maintaining a high level of privacy protection. The regulation applies uniformly across EU member states and extends its jurisdiction to non-EU entities that process data of EU citizens in connection with goods or services offered to them. The GDPR reinforces the fundamental right to data protection enshrined in Article 8 of the EU Charter of Fundamental Rights.

Comprised of 11 chapters, 99 articles, and 173 recitals, the GDPR sets out core principles of data protection, the rights of individuals (data subjects), the obligations of data controllers and processors, and provisions on international data transfers, enforcement, and penalties. However, it does not apply to data processed solely for law enforcement, national security, or personal household purposes. Key features of the GDPR include the data subject's right to withdraw consent at any time, access their data, request corrections, or demand erasure ("right to be forgotten"). It also mandates clear and transparent communication about how data is collected and used, and the legal basis for its processing. Data subjects can also request portability of their data and object to its use for marketing purposes.

Organizations are expected to implement strong technical and organizational measures, such as data protection by design and by default. They must notify data breaches to regulators and, when necessary, to the individuals affected. Certain organizations are required to appoint Data

[21] Alafaa Princess Uche-Awaji, DATA PRIVACY AND DATA PROTECTION: THE RIGHT OF USER'S AND THE RESPONSIBILITY OF COMPANIES IN THE DIGITAL WORLD.https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChsSEwivzdeioYKOAxWPo2YCHQJsD_sYACICCAEQABoCc20&co=1&gclid=Cj0KCQjwsNnCBhDRARIsAEzia4AcKO14WyaNUJXZcGTvxbgarSOMRYauD2_wwPzFKOXfboOdigHZR1gaAscUEALw_wcB&ohost=www.google.com&cid=CAESV-D2pormT7MkuayHr-oqKbj3UTycn3nebWF0OOkUziCtMD_VJYsnG6t7OMOsOzrM_shygj97NqUgKz-VEub0Mz8sAvxl20KDiDPSbv-

ISSN: 2582-6433

Protection Officers (DPOs) to oversee compliance. In cases of non-compliance, the GDPR imposes hefty penalties up to 4% of a company's global annual turnover or €20 million, whichever is higher. A unique aspect of the GDPR is its endorsement of pseudonymisation transforming personal data so that it cannot be attributed to a specific individual without additional information kept separately. Techniques such as encryption and tokenization are commonly used for this purpose to reduce risks associated with unauthorized access.

Despite its comprehensiveness, the GDPR presents challenges. Many companies, especially small businesses, struggle with the cost and complexity of compliance such as conducting data audits, managing cross-border transfers, and responding to data subject requests. Some companies outside the EU have even restricted access to their websites for EU users to avoid GDPR obligations. Yet, the GDPR has had a notable global impact, encouraging greater awareness about data rights and privacy among users and motivating businesses to improve their privacy practices.

The California Consumer Privacy Act (CCPA) – United States

Enacted on June 28, 2018, and amended in 2019, the California Consumer Privacy Act (CCPA) became effective on January 1, 2020. The law was further strengthened by the California Privacy Rights Act (CPRA), passed in November 2020. Together, these acts provide one of the strongest state-level data privacy frameworks in the United States. The CCPA applies to businesses that collect, process, or sell the personal information of California residents, regardless of the company's physical location. It grants consumers various rights, including the right to know what data is being collected, the purpose of collection, and with whom it is shared. Consumers can opt-out of the sale of their personal data and have the right to request its deletion.

The law is grounded in three key principles: transparency, control, and accountability. Businesses are required to include a clearly visible "Do Not Sell My Personal Information" link on their websites and provide privacy notices outlining their data practices. They must also disclose the types of personal information collected, such as geolocation, identifiers, browsing history, and inferences made from data to build user profiles. The CCPA also prohibits businesses from discriminating against users who choose to exercise their privacy rights. It requires that privacy policies be written in plain language and updated regularly to reflect actual data practices. Enforcement is strict, with the California Attorney General having the power to

ISSN: 2582-6433

impose penalties, and consumers having the right to sue businesses for data breaches even in the absence of concrete financial loss. Overall, the CCPA marked a significant step in the U.S. toward recognizing and protecting consumer privacy rights, signalling a move toward stronger data privacy frameworks akin to those in the EU.

The Nigerian Data Protection Regulation (NDPR) – Nigeria

In light of increasing concerns over digital privacy, Nigeria took a significant step forward in 2019 by enacting the Nigerian Data Protection Regulation (NDPR). Developed by the National Information Technology Development Agency (NITDA), the NDPR marks the country's most detailed and structured effort to regulate the handling of personal information. Prior to this regulation, Nigeria lacked a dedicated legal framework specifically addressing data protection. The legal foundation of the NDPR lies in Section 37 of the Nigerian Constitution, which affirms the right to privacy concerning personal correspondence and information. Nigerian courts have reinforced this right in key cases such as Digital Rights Lawyers Initiative v. National Identity Management Commission and Incorporated Trustees of Digital Rights Lawyers Initiative v. L.T. Solutions, where data privacy was affirmed as a constitutional entitlement, enforceable under the Fundamental Rights (Enforcement Procedure) Rules. The scope of the NDPR covers both public and private sector entities that handle or process the personal information of Nigerian citizens. One of its central pillars is the requirement for lawful and transparent data processing, obligating organisations to secure informed and voluntary consent from individuals before collecting or using their data. This consent must be given without deceit, pressure, or manipulation.

Under the regulation, data controllers the entities managing personal data must implement stringent security practices. These include restricting data access to authorised personnel, adopting cybersecurity measures to protect against data breaches, and ensuring overall data integrity. The NDPR also confers rights upon individuals, such as the ability to request corrections, deletions, and portability of their data, as well as the right to object to certain forms of data processing. A key requirement of the regulation is that privacy policies on any data-collecting platforms must be written in clear and understandable language, ensuring that users are well informed about how their data will be used. If organisations violate the regulation, they can be subjected to penalties, and an administrative panel has been established to address such grievances and enforce compliance.

The NDPR represents Nigeria's alignment with broader global movements toward responsible

ISSN: 2582-6433

digital governance. Its dual emphasis on individual autonomy through consent and robust data security protocols has positioned it as a landmark development in Africa's data protection landscape. It not only safeguards the rights of Nigerian citizens but also lays the groundwork for a culture of privacy and data stewardship an essential prerequisite for Nigeria's deeper participation in the international digital economy. Globally, nations are updating and refining their data protection laws to respond to rapid technological change. Although varying in legal design, the GDPR (EU), CCPA (California, USA), and NDPR (Nigeria) all aim to reinforce individual control over personal data and compel organisations to adopt responsible data management practices. These frameworks have emerged as influential models for countries looking to establish or enhance their own data privacy regulations, underscoring a growing global consensus on the urgency and importance of protecting digital rights in the 21st century.

COMPARATIVE STUDY OF LEGAL FRAMEWORKS ON DATA PRIVACY AND DATA PROTECTION IN INDIA AND OTHER NOTABLE JURISDICTIONS

In today's highly digitised and globally interconnected environment, safeguarding personal information and upholding informational privacy have emerged as key pillars in both national laws and international human rights frameworks. India, acknowledging this global trend, has taken steps to establish a dedicated legislative regime for data protection. Yet, its approach, scope, and execution differ substantially from established frameworks such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) in the United States, and Nigeria's Data Protection Regulation (NDPR). This comparative overview analyses these four frameworks in terms of their foundational approaches, legal scope, user rights, regulatory mechanisms, and real-world challenges.

1. Legal Scope and Structural Approach

India's Digital Personal Data Protection Act, 2023 (DPDP Act) marks the country's first comprehensive legislation devoted solely to the protection of personal digital data. The Act introduces fundamental concepts such as data fiduciaries, data principals, and explicit consent, along with the establishment of the Data Protection Board of India. However, the law is confined to digitally processed personal data, leaving out physical records unless converted into digital format. In contrast, the GDPR has a broader purview, covering both automated data and structured non-digital records. Its extraterritorial application brings any entity handling EU

ISSN: 2582-6433

residents' data under its ambit, irrespective of geographic location. The CCPA, while applicable only to certain for-profit entities based on revenue and data processing thresholds, extends its reach to businesses handling the data of California residents, even if those companies are based outside the state. Nigeria's NDPR is similarly expansive, applying to both the private and public sectors and extending its jurisdiction to entities abroad processing the data of Nigerian citizens.

2. Understanding Personal and Sensitive Data

The DPDP Act defines personal data but omits the concept of sensitive personal data, which had been part of earlier drafts and is recognised by many global frameworks. This omission raises concerns about adequate protection for particularly vulnerable data types. In contrast, GDPR distinguishes clearly between ordinary personal data and sensitive categories, such as ethnic background, political affiliations, genetic information, and sexual orientation, with stricter controls on processing. The CCPA takes a broader view of personal data, encompassing even inferred data such as behavioural profiles and geolocation. Nigeria's NDPR also recognises sensitive data types, including religious beliefs, health status, and biometric identifiers.

3. Consent and Legal Basis for Processing

All four jurisdictions regard consent as a key element in legitimising data collection and processing. The Indian DPDP Act mandates that consent must be clear, voluntary, informed, and specific, closely resembling GDPR's consent requirements. The GDPR further requires explicit consent for handling sensitive data and allows individuals to withdraw their consent as easily as it was given. In the CCPA, the consent model is less about pre-approval and more about consumer control especially the right to opt out of the sale of personal data via mechanisms like the "Do Not Sell My Information" option. The NDPR also places emphasis on informed and voluntary consent, specifically mandating that such consent not be procured through deception or coercion.

4. Rights of Individuals Over Their Data

The DPDP Act grants limited rights to data principals, including the right to access, correction, and erasure of personal data, along with access to a grievance redressal process. However, it does not offer several important rights protected under the GDPR, such as data portability, right to object, or restriction of processing. GDPR stands out for its comprehensive rights

ISSN: 2582-6433

framework, including the right to be forgotten, data portability, and protections against automated decision-making. Meanwhile, the CCPA gives users the ability to access, delete, and opt out of data sales, as well as protection from discriminatory treatment for exercising these rights. Nigeria's NDPR extends similar rights to citizens, including the right to object to processing and the right to data portability, although practical enforcement remains limited due to resource constraints.

5. Role and Accountability of Data Handlers

The DPDP Act introduces Data Fiduciaries, and Significant Data Fiduciaries (SDFs) entities that have additional responsibilities based on the scale or sensitivity of data handled. This is similar to GDPR's distinction between Data Controllers and Processors, who are subject to contractual and operational obligations such as Data Protection Impact Assessments (DPIAs) and appointment of Data Protection Officers (DPOs). Under GDPR, both controllers and processors may be held liable for violations, and privacy must be embedded by design. The CCPA categorises actors as businesses, service providers, and third parties, each with distinct roles. Nigeria's NDPR primarily uses the Data Controller concept and requires data protection protocols but lacks detailed obligations and industry-specific standards.

6. Enforcement Mechanisms and Remedies

The Indian DPDP Act empowers the Data Protection Board of India to oversee compliance and impose penalties. However, it does not provide a direct remedy or compensation mechanism for individuals whose data rights are violated, which limits its effectiveness. In contrast, GDPR provides for substantial fines up to €20 million or 4% of a company's annual global turnover and allows individuals to pursue damages through the courts. The CCPA also allows enforcement through the California Attorney General and grants individuals the right to sue for breaches, even in the absence of proven financial harm. Nigeria's NDPR includes administrative penalties and consumer complaint avenues but continues to struggle with weak enforcement due to limited institutional capacity.

7. Government Powers and Exemptions

One of the DPDP Act's most controversial features is its broad exemptions for the state, which allow public agencies to process personal data for reasons including national security, law and order, or public interest without strict oversight or judicial review. This has raised fears of excessive surveillance. Conversely, the GDPR restricts even state authorities from bypassing

ISSN: 2582-6433

data protection standards, requiring any exemptions to be compatible with the EU Charter of Fundamental Rights. The CCPA provides some carve-outs for legal compliance and law enforcement, but still maintains corporate accountability. The NDPR, while drawing from constitutional privacy protections, lacks detailed procedures to control state access to citizen data.

8. Data Transfer Across Borders

The DPDP Act allows data transfer to other countries except those restricted via government notification. This blacklist-based model lacks clear criteria and has created uncertainty for companies operating across jurisdictions. By contrast, GDPR offers a structured mechanism, permitting cross-border data transfers only when adequate protection is guaranteed through adequacy decisions, Standard Contractual Clauses (SCCs), or Binding Corporate Rules (BCRs). The CCPA does not directly restrict such transfers but enforces accountability regardless of where data is sent. Nigeria's NDPR permits international data flow but requires that the data subject be informed and that strong safeguards are in place.

9. Implementation and Practical Challenges

While the DPDP Act marks a significant step for India, it faces numerous implementation roadblocks, including vague sectoral guidelines, potential delays in framing rules, and limited public understanding of the law. Concerns have also been raised regarding the independence and autonomy of the Data Protection Board, given its short tenure and government-appointed members. Even the GDPR, widely considered the gold standard, is not without issues. It poses high compliance costs for smaller businesses and suffers from uneven enforcement across member countries. The CCPA has led to confusion among businesses about compliance responsibilities, particularly the definitions of service providers and third parties. Nigeria's NDPR suffers from weak regulatory capacity, a limited culture of compliance, and minimal public outreach.

For India to fully realise its data governance ambitions, it must strike a balance between state interests and individual freedoms, build public awareness, ensure the true autonomy of its regulatory body, and develop detailed rules across sectors. Only then can the DPDP Act mature into a globally respected data protection regime rooted in transparency, accountability, and democratic values.

CASE STUDY

ISSN: 2582-6433

1. Aadhaar and The Safeguarding of Biometric Data Information

The rollout and mass adoption of Aadhaar—India's nationwide biometric identity initiative has triggered intense discussions regarding the security and proper management of biometric information. As the system required individuals to submit sensitive identifiers like fingerprints and iris scans, it raised valid apprehensions about how well Indian legal provisions, especially the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules of 2011, could protect this information. These worries have only grown due to repeated reports of data leaks and unauthorized data exposure. When one compares India's legal safeguards to international regimes such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA), the differences become stark.

The GDPR expressly classifies biometric identifiers as a "special category" of personal data, requiring heightened levels of protection and processing only under clearly defined, lawful grounds. Meanwhile, the CCPA although less detailed grants users the authority to opt out of the sale or sharing of their biometric data, reinforcing the principles of consent and control over personal information. In India's context, the IT Rules, 2011 lack this level of clarity and enforcement. They do not categorically define biometric data as distinct from other sensitive information, nor do they provide stringent enforcement structures. This creates a legislative void, particularly in the context of Aadhaar, leaving such critical data exposed to possible misuse. These shortcomings highlight the urgent necessity for India to reform and strengthen its legal architecture to safeguard biometric privacy and align with international best practices.

2. Cross-Border Data Transfer in the E-commerce

An international e-commerce corporation conducting business in India finds itself facing multiple legal hurdles concerning the transfer of customer data to overseas servers. These issues emerge in a context where cross-border data flows are integral to delivering seamless digital services and enhancing user experience. Despite the essential nature of such data sharing, businesses must navigate a fragmented legal landscape under India's Information Technology Act and prepare for impending obligations set out in the Digital Personal Data Protection Act (DPDPA) of 2023. Internationally, the GDPR sets strict conditions for transferring personal data outside the European Union. It mandates either explicit consent from the individual or the use of legal instruments such as Standard Contractual Clauses or adequacy decisions. These mechanisms ensure that data exported beyond EU borders retains the same standard of protection. In contrast, the CCPA does not prohibit cross-border transfers per se,

ISSN: 2582-6433

but it mandates transparency. Companies must inform users when personal data is being "sold" or shared and give them a clear choice to opt out thus indirectly controlling how such data is handled overseas.

This scenario underscores the complex compliance environment that global firms must navigate when operating in multiple jurisdictions. For companies active in India, it is vital to establish data governance models that satisfy both domestic requirements and international legal standards. As India moves toward implementing stricter data protection norms, including possible data localisation obligations, businesses must be proactive in adapting their data management strategies. Adhering to such evolving norms is essential not only for regulatory compliance but also for maintaining consumer trust and long-term business integrity.

3. Consent Mechanisms in Social Media Platforms

A popular social media company with a large user base in India comes under scrutiny for how it manages and collects user consent for data processing. With personal data being a major asset in the digital advertising economy, the transparency and clarity with which platforms inform users and obtain their consent have come into the spotlight. This scenario explores how Indian law particularly through the lens of the proposed Personal Data Protection Bill, 2019, and the later DPDP Act, 2023 deals with this issue. GDPR requires companies to provide users with clear and accessible notices explaining what data will be collected, for what purpose, and with whom it will be shared. A comparison with the GDPR shows that both frameworks emphasize informed, specific, and freely given consent. Consent must be affirmative pre-ticked boxes or implied consent are not acceptable. On the other hand, the CCPA adopts a different approach by giving users the right to opt out of data sales, especially for marketing purposes. While it may not focus as much on prior consent, it grants users control over how their data is used, especially regarding monetisation.

This case underscores the urgent need for Indian platforms to update their consent mechanisms in line with global norms. Vague or buried consent notices, bundled consents, or non-user-friendly interfaces no longer meet acceptable standards. As user awareness grows, platforms must ensure that consent is not just a checkbox, but a genuine expression of user understanding and autonomy. In this regard, India must continue refining its legal framework to encourage explicit, purpose-specific, and revocable consent.

4. Healthcare Data Protection in Telemedicine

ISSN: 2582-6433

With the rapid expansion of telemedicine services in India, particularly post-pandemic, significant volumes of sensitive health information are being collected, stored, and processed digitally. These include personal medical histories, prescriptions, diagnostic reports, and mental health records. This case examines whether India's current and proposed data protection laws sufficiently safeguard such highly sensitive medical data, especially as more healthcare services shift online. Under the GDPR, health-related data falls under the umbrella of special category data, which requires explicit consent and may only be processed for limited purposes such as treatment, public interest, or with proper safeguards. Entities processing such data must adhere to privacy by design principles and conduct data protection impact assessments. In the CCPA, although there isn't a separate category for health data, it still qualifies as personal information. This means companies must inform users about how their health data is collected, used, or shared and must allow them to opt-out of its sale.

This case points to a critical gap in India's regulatory ecosystem, where there are limited specific protections for healthcare-related data. The existing laws lack industry-specific guidelines for telemedicine, which can leave patient data exposed to misuse. As healthcare becomes increasingly digital, there is a growing need for tailored rules within India's data protection legislation that address the unique sensitivity and confidentiality needs of medical data. Ensuring that patients' health information is protected is not just a legal requirement but a matter of public trust in digital healthcare systems.

CONCLUSION AND SUGGESTIONS

In India, the recognition of the right to privacy has evolved significantly over time, mainly due to progressive interpretations by the judiciary. Despite this legal advancement, the practical application of privacy in everyday life remains a pressing concern in an era marked by rapid technological growth and global interconnectedness. Privacy is not just a legal concept it is central to individual dignity, allowing people the freedom to make personal choices without unwarranted interference. However, the very technologies that enhance our lives also pose serious risks, as they facilitate cyber offences, identity fraud, unauthorized surveillance, and data misuse.

In today's digital environment, individuals are routinely required to provide personal data whether to private corporations or government agencies for accessing even the most basic services. This obligatory sharing of sensitive information has raised substantial concerns, particularly given India's still-developing data protection landscape. While some legal

ISSN: 2582-6433

instruments like the Information Technology Act, certain criminal law provisions, and aspects of intellectual property law touch on privacy issues, the country still lacks a consolidated legal framework that comprehensively governs personal data protection.

This legislative gap has tangible consequences. When personal data is compromised or misused especially by third-party service providers or digital intermediaries' victims often find themselves with limited legal recourse. Many data handlers distance themselves from accountability, claiming no knowledge of the breach, and the current legal setup does little to compel responsibility. Therefore, there is an urgent requirement for an effective, enforceable legal regime that can address data privacy violations head-on.

Although the Supreme Court's affirmation of privacy as a part of Article 21 of the Constitution marks a legal milestone, such judicial recognition alone cannot guarantee practical protection. Public understanding and active awareness of privacy rights are equally vital. Citizens must be educated not only about the existence of their rights but also about the processes available for addressing violations. Without such knowledge, infringements may go unreported and unchallenged, undermining the very essence of democratic accountability.

Traditionally, privacy in India was perceived in terms of physical space and personal boundaries. However, in this digital age, the scope of privacy must expand to cover informational and data-related concerns. The state must adopt advanced technological tools capable of identifying and neutralising threats such as data leaks or unauthorised usage in real time. Alongside this, lawmakers should pass robust legislation that ensures the safety of collected information. This includes using strong encryption, limiting access to only authorised entities, and ensuring that the use of data strictly aligns with declared and lawful purposes. Entities entrusted with personal data be they public institutions or private firms must bear full responsibility for the information they handle. The legal system should establish harsh consequences for data mishandling, including significant financial penalties and criminal liability, to discourage future violations. Such deterrents are essential to instil a culture of accountability.

Concerns have also been raised over the collection of biometric data under programmes like Aadhaar. In response, experts have recommended alternatives such as smart card-based systems. These require active consent and participation from users, often through PIN

ISSN: 2582-6433

authentication, making them inherently more secure than biometric systems, which can identify individuals even without their knowledge. Smart cards offer the added benefit of being easily deactivated or discarded, thereby limiting the risk of misuse if lost or stolen. Implementing such alternatives could help protect citizens from threats posed by the exploitation of biometric databases by hostile entities or criminal groups.

In summary, while India has made notable legal strides in recognising privacy as a constitutional guarantee, the practical realisation of that right remains incomplete. To safeguard the privacy of individuals in the digital age, India needs a holistic and enforceable data protection law, strengthened by modern technological safeguards, widespread public education, institutional accountability, and strict legal penalties. Only through such a multidimensional approach can the country hope to uphold the digital rights and personal dignity of its people in an increasingly interconnected world.

REFERENCES

The Constitution of India, 1950

The Indian Contract Act, 1872

The Indian Copyright Act, 1957

The Indian Evidence Act, Act, 1872

The Information Technology (Amendment) Act, 2008

The Information Technology (Reasonable Security Practices and procedures and sensitive personal data or information), Rules, 2011

The Information Technology Act, 2000

Indian Penal Code, 1980

Apar Gupta, "Balancing online privacy in India", 6 IJLT, (2010).

Asok Kini, "Aadhaar the summary of majority (4:1) judgement", pdf.

Dr Payal Jain &Ms Kanika Arora, "Invasion of Aadhaar on right to privacy: huge concern ofissues and challenges", 45 (2) ILR (2018).

The Personal Data Protection Bill, PRS LEGISLATIVE RESEARCH, (Visited on June 16, 2025) https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.

"An Extensive Article on Data Privacy and Data Protection Law in Nigeria" by Uche Val Obi SAN, 9th September, 2020. Available at https://inplp.com/latest-news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/ accessed 16th June, 2025.

"Data Privacy and Protection under the Nigerian Law" by Francis Oloho (S.P.A. Ajibade and

ISSN: 2582-6433

co.), 19th February,2020. Available https://www.mondaq.com/nigeria/privacy-protection/895320/data-privacy-and-protection-under-the-nigerian-law/ accessed 16th June, 2025.

9 NDPR- A regulation made by the NITDA by virtue of s. 6 of the National Information and Technology Development Agency, Act (2007). Available at https://nitda-gov.ng/wp-content/uploads/2019/01/NigeriaDataProtectionRegulation.pdf/ accessed 17th June, 2025.

"What is the GDPR? Understanding and complying with GDPR requirements in 2019" by Juliana De Groot, 30th September, 2020. Available at https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection/ accessed 17th June, 2025.

"Data Protection", available at https://edps.europa.eu/data-protection_en/ accessed 17th June, 2025.