IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Navigating The Legal Landscape: Data Protection Laws In India

[1]Jyoti Devi, [2]Dr. Anil Balhera

[1]Ph.D Scholar, Department of Laws, BPSMV, Khanpur Kalan, [2]Assitant Professor, Department of Laws, BPSMV, Khanpur Kalan

Abstract

In both national and international contexts, rights that are inherent to human society have been codified into enforceable documents. While these documents explicitly mention certain rights, they are interconnected, often requiring interpretation to understand their full implications. The right to privacy is particularly important, allowing individuals a level of confidentiality in their personal lives. Key international agreements, such as the Convention on the Rights of the Child and the International Covenants on Civil and Political Rights, reference this right. In India, the right to privacy is recognized as essential to life and liberty, ensuring that each individual has a personal space free from unwarranted scrutiny by the state or others. Despite the widespread acknowledgment of the importance of privacy, there is a lack of clear international guidelines defining this right, contributing to difficulties in its enforcement. This right is seen as a qualified one, posing challenges in determining public interest and managing the private sector's role. Communication confidentiality allows individuals to share thoughts and information away from societal, commercial, and governmental interference, emphasizing the significance of privacy in communication systems. Since the mid-20th century, the notion of a right to non-interference in personal life has gained attention, particularly with the rise of technology. The integration of technology in daily life has led to concerns about personal data collection and monitoring, prompting demands for clearer regulations. Data protection, a part of privacy, has recently gained global attention, as the right to privacy extends to the protection of one's data.

India's growth in sectors like education, health, and communication has been significantly influenced by the Internet and outsourcing, providing employment opportunities. However, India's approach to data protection varies from Western norms, reflecting its unique cultural context. This cultural variance creates a divide in privacy rights discussions, as different social philosophies shape the principles governing data protection. This paper will discuss current Indian legislation related to data privacy safeguarding.

(*Keywords*: data protection, privacy, legislation, judiciary, Digital Personal Data Protection (DPDP) Act, 2023)

A. Introduction

The rapid growth of digital technology and the internet has made it easy for anyone to collect, process, share, and store information globally. However, this fast development has created many new legal and ethical issues, and the law has not kept up, leaving significant gaps to address these problems. Technology is often viewed as a double-edged sword, providing great benefits in efficiency and productivity but also raising concerns about privacy, particularly data privacy. Tools like surveillance cameras, mobile phones, GPS, smart tags, biometrics, and RFID are not originally intended to invade privacy, but they can be misused for that purpose. The large-scale collection, processing, and storage of personal data has become a concern for individuals who worry about the harmful effects of misuse.

Personal data can be easily accessed from various sources, including government agencies. Governments collect and process large amounts of personal data for various reasons throughout an individual's life. The right to privacy was first defined as the "right to be left alone" by US Judge Thomas M. Cooley in 1888, and it was further explored by Warren and Brandeis, who highlighted the need for legal protection of privacy as new technologies emerged.

Privacy varies by country and lacks a universal definition. It involves individuals' interest in maintaining personal space without interference and their ability to control how their personal information is shared. Privacy law can be divided into four areas: data privacy, physical privacy, communications and surveillance privacy, and territorial privacy. This text focuses on data privacy, which is treated as a fundamental human right in Europe, while the US views it more as consumer protection. Over the past two decades, nations have struggled to regulate the protection of sensitive personal information effectively.

At the international level, several important legal instruments address data protection and privacy law. These include the Council of Europe's Convention[1], OECD Guidelines[2], the EU Data Protection Directive[3], the APEC Privacy Framework[4], the European Convention on Human Rights (ECHR), the European Union Charter, and the Personal Data Protection Act in various countries. India recognizes the right to privacy as a universal human right through its commitment to the Universal Declaration of Human Rights (UDHR) and the International Covenant for Civil and Political Rights (ICCPR), specifically under Article 12 of the UDHR and Article 17 of the ICCPR.

However, at the national level, India lacks a comprehensive law regarding privacy and data protection. The issue of data protection is mainly addressed in the Information Technology Act of 2000,

[1] Council of Europe's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 1981
[2] Organisation for Economic Corporation and Development Guideline Governing the Protection of Privacy and Tran-Border Flows of Personal Data 1980
[3] European Community Directive on the Protection on the Individuals with Regards to the Processing of Personal Data and Free Movement of Such Data
[4] Asia Pacific Economic Corporation Privacy framework 2004

while privacy concerns are tied to Article 21 of the Indian Constitution. This Article acknowledges an individual's right to privacy, emphasizing the importance of personal space and the modern necessity of privacy.

Initially, the right to privacy was not listed as a fundamental right in the Constitution. It has been viewed as implicit in the fundamental right to life and liberty guaranteed by Article 21, which includes the right to be let alone. Advocates have argued for the right to privacy under two fundamental rights: the right to freedom under Article 19 and the right to life and personal liberty under Article 21.

Article 19(1)(a) grants citizens the right to freedom of speech and expression, but this is limited by Article 19(2), which allows for reasonable restrictions to protect national sovereignty, security, public order, and other interests. Thus, freedom of expression is not an absolute right and can be limited under certain conditions. Article 21 ensures that no person can be deprived of life or personal liberty without due legal process.

A significant case, **Justice K. S. Puttaswamy (Ret.) and Others v. Union of India**[5], ruled that the right to privacy is a fundamental right, shielding individuals from both state and non-state interference. Before this, earlier cases like **M P Sharma v. Satish Chandra**[6] and **Kharak Singh v. State of Uttar Pradesh**[7] found that the right to privacy was not constitutionally protected.

The path towards recognizing the right to privacy gained momentum with the Kharak Singh case, where police surveillance was deemed a violation of personal rights. The Supreme Court acknowledged unauthorized intrusions harm the essence of ordered liberty. Justice Subba Rao noted that personal liberty included a right to privacy. Subsequent cases, including **R. M. Malkani v. State of Maharashtra**[8], highlighted privacy rights in the context of wiretapping, while the **Govind v. State of Madhya Pradesh**[9] case marked a setback, as the court upheld police surveillance of suspected criminals under certain regulations.

In the case of **R. Rajagopal v. State of Tamil Nadu**[10], the court examined the balance between citizens' right to privacy and the press's right to criticize public officials. The case involved the alleged autobiography of Auto Shankar, a convicted murderer, which discussed his relationships with police officials. The Supreme Court declared that the right to privacy is part of the right to life and liberty under Article 21 of the Constitution. This includes a citizen's control over personal matters such as family and education, prohibiting publication without consent, regardless of the content's truthfulness.

In **PUCL v. Union of India**[11], the court reviewed whether wiretapping violated citizens' privacy rights. The Supreme Court reinforced that privacy includes telephone conversations in private spaces and

[5] 2017(10) SCALE 1
[6] 1954 AIR 300
[7] AIR 1963 SC 1295
[8] AIR 1973 SC 157
[9] (1975)2 SCC 148
[10] (1994)6 SCC 632
[11] AIR 1997 SC 568

ruled that unauthorized phone tapping breaches Article 21 unless conducted per legal procedures. Furthermore, in the case of **Justice K. S. Puttaswamy**, the court overruled earlier decisions, affirming that privacy is a fundamental right linked to personal liberty under Article 21, protecting individuals from intrusion.

While Article 21 grants the right to privacy, there is no specific law on data protection in India. Personal data collection has increased through various applications and websites, exposing people's information to risks from non-state actors who might misuse this data for cyberattacks or profiling. Although individuals often face pressure to share personal data, many are unaware of the privacy implications. The judiciary struggles with data privacy due to the lack of targeted legislation, relying instead on existing laws, which are insufficient. Therefore, there is a need for comprehensive data protection legislation for present and future generations.

B. India's Current Legal Framework for Data Protection

i. Contract Law

The legal framework in India for data protection in offshoring mainly relies on contract law. The Indian Contract Act of 1872 allows a firm to enter a contract that requires another company to protect its data. This is based on the definition of "consideration," which means that one firm can legally require another to keep data confidential[12]. Contracts must clearly detail the responsibilities of all parties, including the Indian company's obligations for data privacy and its use. Currently, all offshoring activities in India follow these contracts. Foreign data exporters negotiate with Indian businesses to balance corporate benefits and the protection of personal data.

ii. The Financial Institutions Act of 1993

This legislation outlines India's long-standing commitment to protecting privacy in banking transactions. Bankers must keep bank account information confidential, as customer records accurately reflect their financial activities. Allowing third parties unrestricted access to these records could lead to negative consequences. Bankers must exercise extreme caution to maintain this confidentiality and cannot share customer account details with outsiders. A legal case highlighted the banker's duty of absolute confidentiality, which is based on trust. However, this obligation is not always absolute, as the law allows for certain disclosures under specific circumstances.[13]

iii. The Indian Telegraph Act, 1885

The regulation of wiretapping in India is based on the Telegraph Act of 1885. The Supreme Court has recognized wiretapping as a serious violation of privacy. Article 5 of this Act allows authorities to intercept communications for surveillance. The government can take control of licensed telegraphs during a public emergency or for public safety. In such cases, the Central Government, State Government, or an

[12] Indian Contract Act, 1872 s-2.
[13] Kattabomman Transport Corporation Ltd. v. State Bank of Travancore and others AIR 1992 Ker.351.

authorized officer can intercept specific messages that relate to important issues, aiming to protect India's sovereignty, public order, or prevent crimes. All decisions to intercept messages must be documented, and the contents can be disclosed to the government. However, accredited press messages are typically exempt from interception unless explicitly prohibited.

Section 7(2)(b) gives the government power to set rules to prevent unauthorized message interception or publication, but no solid regulations were in place as noted in the **PUCL v. Union of India**[14] case. The Supreme Court has outlined who can authorize wiretaps and under what conditions. Only the Union Home Secretary or a state equivalent can order a tap, which must be backed by evidence, and a high-level committee is authorized to assess the legality of wiretaps.

iv. Credit Information Companies (Regulation) Act, 2005

The Credit Information Companies (Regulation) Act was enacted in May 2005 and published in the Gazette on June 23, 2005. This law aims to regulate credit information firms and set guidelines for information privacy and the sharing of credit information. Its main goal is to create a system for effectively distributing credit information. A credit information company must obtain a registration certificate as specified in the Act. Credit information pertains to data related to loans, credit cards, and credit facilities provided by financial institutions, along with the measures of protection required from borrowers.

Under the Act, a credit institution is mainly defined as a banking company, which includes various types of banks and non-banking financial companies. It also involves organizations offering credit-related services. The term “information of an identifiable individual” does not include general details like a name or phone number, aligning closely with European personal data definitions. The Act mandates credit information firms to ensure proper recording, compiling, and processing of the obtained information.

The Act contains fundamental clauses concerning the accuracy and security of credit information. Companies collecting this information must implement measures to maintain accurate and secure data and ensure protection against unauthorized access or loss. As the data directly impacts individuals, it must always be accurate. Section 20(b) requires credit information firms to provide an adequate explanation for data collection and its intended use, limiting disclosures to necessary occasions. Institutions must verify the accuracy of information before sharing it, following guidelines in Section 20(c).

Section 20(d) establishes proper storage protocols for the data maintained by credit information firms and credit institutions, including preservation and deletion guidelines[15]. Regulations from the Reserve Bank may include additional practices regarding credit information. Every credit reporting agency must accurately collect, compile, and handle data while protecting it from loss or unauthorized use. Credit institutions must update records regularly to ensure that data remains current and accurate.

[14] (1997) 1 SCC 301.
[15] Section 20, Credit Information Companies (Regulation) Act, 2005

Additionally, credit reporting agencies and financial organizations must develop protocols that allow individuals to access their records, requiring them to provide identity proof for access. They have the right to request modifications, which must be processed within specific timeframes. Data collection must adhere to the principle of proportionality, ensuring information is relevant and accurate for its intended purpose.

The data use limitations specify acceptable scenarios for obtaining credit reports, such as fulfilling court directives and responding to individual requests for their information. Credit Information Companies are obligated to ensure data accuracy, and credit institutions are responsible for maintaining and updating data regularly. Data must be archived for a minimum of seven years, with separate rules for information on financial defaults and criminal records. Non-individual information must be kept indefinitely.

The person requesting the credit facility will have access rights, and the lending company will handle their requests. Only credit information can be accessed, and clients can request updates to their information. Security measures must comply with Act regulations, and all employees must pledge confidentiality. Data must be collected and transmitted securely. If a credit information company violates the Act, complaints can be filed with the RBI, which can impose penalties.

v. Specific Relief Act, 1963

The Specific Relief Act aims to give people a remedy when their rights are violated. It allows plaintiffs to seek both interim and permanent injunctions to prevent further violations. If a service provider does not fulfill their agreement, the affected person can sue for an injunction. Additionally, they may seek damages along with or instead of the injunction, as the court decides may be appropriate[16].

vi. The Information Technology Act 2000

The Act established in 2000 based on the United Nations Model Law on Electronic Commerce went into effect on October 17, 2000. In 2008, changes were proposed to address issues related to cybercrime, data protection, and electronic signatures, with these updates effective from February 2019. The Act contains limited provisions for data protection. Data is defined in Section 2(o) as the formal representation of information processed in computer systems, while information includes various forms such as messages and software as per Section 2 (Subsection 1 Clause V). There is no clear distinction in the Act between sensitive and personal data.

Section 43 addresses illegal access to computers or networks without permission, with potential damages up to one crore rupees for violations. The 2009 amendment, Section 43A, focuses on data protection responsibilities for companies handling sensitive personal data, leaving the definition of such data to the central government.

[16] Sections 37 and 38, Specific Relief Act, 1963

Section 66 C penalizes individuals committing identity theft using someone else's electronic signature or unique identification, with penalties including jail time up to three years and fines up to one lakh rupees. Section 66 E imposes a maximum of three years in prison and fines up to two lakh rupees for unauthorized capture or transmission of intimate images. Section 72 deals with unauthorized access to electronic records, allowing for fines or up to two years in prison. Finally, Section 72A provides for criminal penalties for intermediaries who disclose personal information without consent, with punishments including up to three years in prison and fines up to five lakh rupees.

vii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

On April 13, 2011, the IT Rules, 2011 (SPDI Rules) were published under Section 87(2)30 and Section 43-A of the IT Act. These rules apply to companies and individuals in India and focus on handling sensitive personal data or information (SPDI). They govern how SPDI is collected, stored, used, and shared. Data subjects have the right to review, update, and revoke their consent for SPDI. Personal information is defined as any data that can identify an individual. SPDI includes specific categories like passwords, financial data, and health information. However, the rules do not impose criminal penalties for violations or establish security measures for data protection.

viii. Information Technology (Intermediaries Guidelines) Rules, 2011

The Indian government established the Information Technology (Intermediaries Guidelines) Rules, 2011, to regulate online intermediaries. The guidelines aim to balance the needs of free speech and the protection against harmful online content. Intermediaries are required to show due diligence and must publicly share their rules, user agreements, and privacy policies, ensuring transparency in their services.

Under these guidelines, intermediaries must remove or block harmful content within 36 hours of receiving a complaint from a government authority. They are not permitted to host any content that violates Indian laws. By requiring this adherence, intermediaries are made aware of their legal responsibilities in controlling illegal material.

While the guidelines have improved data privacy and accountability among online intermediaries, they have also faced criticism. Some experts believe the rules may limit legitimate online speech, while others argue they don’t do enough to protect user privacy. Despite these concerns, the guidelines remain a key framework for managing internet intermediaries in India, emphasizing the need for ongoing updates to address the evolving internet landscape.

ix. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The Ministry of Electronics and Information Technology of the Government of India announced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on February 25, 2021. These new rules replace the 2011 guidelines and apply to both digital media content

creators and publishers. Each intermediary must set up a Grievance Office and publish its name on their website or app.

Rule 3 outlines obligations for data protection in India for intermediaries, including the need to post information for users about accessing their computer resources. Users must be informed about the intermediary's resources within the terms of service or privacy statements. Intermediaries must warn users at least once a year about the consequences of breaking access rules. They are not liable if they receive proper legal notice about content issues. Intermediaries must keep users updated on any changes to terms or policies at least once a year.

They need to preserve deleted information during investigations, and any third party holding user information must keep it for 180 days after the user cancels registration. Intermediaries have 72 hours to provide information to authorized government agencies for investigations. They must not alter the operation of their computer resources unlawfully. When handling cyber security incidents, intermediaries must follow established procedures.

The name and contact details of the grievance officer must be clearly displayed. Intermediaries have 24 hours to notify the officer after receiving a complaint and should allow complainants to provide further information about the issue. However, the rules do not specify additional steps intermediaries must take beyond current due diligence to ensure compliance.

x. Data Empower and Protection Architecture (DEPA)

DEPA is a framework designed to give people control over their personal data while ensuring its security. It aims to make data sharing between individuals and organizations easier and safer. The key principles of DEPA include user consent, data minimization, and purpose limitation. A consent dashboard allows users to manage how their data is used and shared across different services. Users can review and adjust their data permissions through this dashboard. DEPA also introduces a data fiduciary model, where individuals can designate a trusted organization to manage their data. This fiduciary ensures that data is used only for approved purposes and follows legal requirements. Additionally, DEPA includes a data empowerment API to enable secure sharing of data with third-party services. The framework aligns with principles from GDPR and CCPA and was outlined in a blueprint by NITI Aayog in 2020, as part of India's digital infrastructure initiative.

xi. Formation of the B.N. Srikrishan Committee and Its Recommendations

In August 2017, the Supreme Court of India recognized the Right to Privacy as a Fundamental Right under Article 21 of the Indian Constitution in the case of **K. S. Puttaswamy v. Union of India**[17]. This case led to the formation of the BN Srikrishna Committee, established by the Ministry of Electronics and Information Technology to study data protection issues and suggest recommendations for India's data

[17] (2017) 10 SCC 1.

protection framework. On July 27, 2018, the Committee released its final report along with a draft of the Personal Data Protection Bill, which formed the basis for subsequent legislation.

The committee made several observations regarding privacy and data protection, emphasizing the definition of personal data, the necessity for a fiduciary relationship between service providers and individuals, and the need for clear obligations for service providers to ensure fair data processing and user notifications. It stressed that consent must be obtained before collecting data, particularly sensitive information.

The committee outlined people's rights related to data, including the right to object to data processing, access, and correction, and the right to be forgotten. It also recommended establishing a regulatory body to oversee implementation and suggested changes to existing laws about data privacy. The proposed Personal Data Protection Bill includes provisions for a Data Protection Authority, covers 112 sections, and highlights protecting personal information while fostering a secure digital economy and ensuring accountability for data handlers.[18]

❖ **Important Elements of the 2018 Personal Data Protection Bill**

The Bill Application covers Indian companies, citizens, corporations, and companies outside India that handle personal data. It defines key terms like "consent," "data fiduciary," "data principal," and “sensitive personal data”. The Bill specifies data protection requirements, including restrictions on data collection, processing, storage, and accountability. It recognizes rights for data principals such as rectification, access, and being forgotten. A Data Protection Authority was established to monitor compliance and enforce penalties. It also regulates cross-border data storage and allows for certain exemptions.[19] The parliament asked for revisions to create a new data protection law, leading to the personal data protection bill of 2019.

- **Key Elements of the Data Protection Bill, 2019**

The Joint Parliamentary Committee began reviewing the Privacy Bill in 2019, following the Puttaswamy judgement from August 2017, which recognized the "Right to Privacy" as a basic right. This Bill aims to protect individual rights by regulating how personal information is collected, used, and shared, marking a significant change in personal data protection in India.

The structure of the Bill facilitates clear relationships between states, businesses, and individuals regarding data handling, ensuring privacy agreements. It sets out principles for data security and requires accountability from organizations. The measure emphasizes citizens' rights to know what personal data organizations hold and how it's used. Additionally, the Bill proposes the creation of the Data Protection

[18] A Free and Fair Digital Economy, available at: https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy (last visited on January 5, 2025).
[19] Personal Data Protection Bill, 2018.

Authority (DPA) as an independent body to oversee data processing and handle user complaints against organizations that fail to meet obligations.[20]

- **Issues related to the Data Protection Bill, 2019**

The bill's efficiency is questioned due to certain clauses that may favor government agencies and weaken user data protections. Article 35 may allow the Centre to exempt government agencies from the bill's safety standards, leading users to feel their data isn't fully protected. Consent could be weakened, making it difficult for users to enforce their rights, as withdrawing consent could lead to legal issues.

Recommendations of A Joint Parliamentary Committee

The Personal Data Protection Bill of 2019 was introduced in the Lok Sabha on December 11, 2019, but was not passed. Instead, a committee was set up to review the bill, which presented its findings on December 16, 2021. The report, led by Chairman P. P. Chaudhary and 30 other members, focuses on recent improvements in the bill and general observations. The Data Protection Bill 2021 aims to maintain high safety standards and build public trust but has faced criticism for prioritizing state interests over data protection.

The Committee made several important recommendations regarding the Personal Data Bill, which aims to safeguard personal data processing by various entities, including the State. The key recommendations include a 24-month implementation window after the Bill is enacted, applying the Bill to Non-Personal Data, special handling guidelines for children's data, removing certain information from the sensitive data definition, creating a Data Protection Authority (DPA) for oversight, emphasizing Data Localization, using the term "social media platform," and providing protections for the rights of deceased individuals concerning their personal data.[21]

xii. Digital Personal Data Protection Bill 2022

In the Fifth Instance of Data Protection Law, MEITY introduced a draft of the revised Digital Personal Data Protection Law, 2022. This draft consists of 6 chapters and 30 sections, which is fewer than the previous Personal Data Protection Bill 2021. The draft is currently pending and has not yet been introduced in Parliament. The Ministry of Electronics and Information Technology released the draft for public comment in November 2022.

The key elements of the Bill include its application to digital personal data processed in India, whether acquired online or converted from offline data. It will also apply to processing done outside India if it involves creating profiles of individuals in India for the purpose of selling products or services. Personal data is defined as any information that can identify a person, while processing refers to actions performed on this data, such as collection and dissemination.

[20] Personal Data Protection Bill, 2019.

[21] Joint Parliamentary Committee Report, available at: https://prsindia.org/billtrack/prs-products/joint-parliamentary-committee-report-summary (last visited on January 10, 2025).

Regarding consent, the Bill states that personal data can only be processed if an individual has given valid consent after receiving proper notification about the data being collected and its intended purpose. Consent can be revoked at any time. Valid reasons for obtaining consent include fulfilling legal obligations, providing state benefits, responding to medical emergencies, pursuing employment, and public interest purposes like security or fraud prevention. For individuals under 18, consent must come from a legal guardian.

The Bill outlines the rights and responsibilities of data principals, allowing them to request information about how their data is processed, correct or erase personal data, designate a substitute in case of death, and file grievances. However, data principals are prohibited from filing false claims, withholding information, or impersonating others. Violators may be penalized with fines up to Rs 10,000.

Organizations, termed data fiduciaries, are responsible for ensuring data accuracy, implementing security measures to prevent breaches, and deleting personal data once its purpose has been fulfilled. This retention condition does not apply to government organizations. The central government will also manage the transfer of data outside India, setting terms and restrictions.

Some exemptions are included for government agencies, allowing them to bypass certain rights and duties under specific conditions, such as the prevention and investigation of crimes. Similarly, processing for state security and public order may also be exempt. The Bill mandates the creation of the Data Protection Board of India, which will impose sanctions for noncompliance, take necessary actions during data breaches, and handle complaints.

Penalties can reach up to Rs 250 crore for not implementing adequate data security measures and up to Rs 150 crore for not fulfilling obligations towards children. The Board will impose these penalties following inquiries.

The analysis section highlights potential issues with the Bill, particularly regarding privacy rights. The Supreme Court ruled that any invasion of privacy must be justified. The Bill allows government processing of data with vague conditions, which may infringe personal privacy. Exemptions granting the government authority to process data without oversight could lead to excessive data collection for surveillance, raising concerns about proportionality. The absence of defined limits for data retention after processing is alarming. Similar exemptions in other countries, like the UK, involve strict regulations and judicial oversight, which are lacking in this Bill.[22]

- ✓ **Processing without authorization to stop the spread of erroneous information**

One goal of "preventing dissemination of false statements of fact" is included in the Bill as a reason for assumed consent benefiting the public. This raises questions about its necessity since existing

[22] Draft Digital Personal Data Protection Bill, 2022, available at: https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022 (last visited on January 15, 2025).

regulations protect against harm. The Supreme Court said speech can be regulated if it incites, but harmful or unpopular communication is still protected by the Constitution.

✓ **Bill may not ensure independence of the Data Protection Board of India**

The Bill requires the national government to establish the Data Protection Board of India, which should operate independently. The central government will decide the membership, appointment terms, and expulsion procedures. There is a question about whether details ensuring the Board's independence should be included in the main statute. The Board's main duties include detecting violations of the Bill, imposing penalties, and ensuring data fiduciaries take appropriate action in case of a data breach. Government agencies, which manage large amounts of personal data, are often scrutinized, raising concerns about the Board's independence in such cases.

The Personal Data Protection Bill of 2019 aims to create an independent Data Protection Authority, including details on appointments and processes, similar to other regulatory agencies. These laws specify employment duration and limited termination grounds. The RTI Act of 2005 allows the federal government to set the Central Information Commission's term while also outlining membership and removal requirements.

✓ **Right to data portability and the right to be forgotten not provided**

The Bill does not include the right to be forgotten or the right to data portability. Previous drafts, such as the 2018 Draft Bill and the 2019 Bill, attempted to address these rights, with recommendations from the Joint Parliamentary Committee to keep them intact. The European Union's GDPR recognizes these rights too. The Srikrishna Committee (2018) stated that data protection laws should ensure data principal rights, focusing on responsibility, transparency, and autonomy.

The right to data portability allows individuals to obtain and transfer their data in a recognized format for personal use, enhancing their control over information. Concerns arise regarding possible trade secret disclosures, but the Srikrishna Committee suggested ensuring data release without compromising these secrets. The Joint Parliamentary Committee stated technological feasibility is the only valid reason for denying data portability.

The right to be forgotten grants individuals control over their personal information online, aiming to limit online memory. However, it may conflict with others' freedom of expression and information access. Its effectiveness can depend on the sensitivity of data, its public importance, and the individual's public profile.

✓ **Additional provisions for children**

Age verification on digital sites is important to get confirmed parental consent before handling a child's personal information. Data fiduciaries must verify the age of each user and ensure they are not minors to comply with this requirement. This could harm internet anonymity, as currently, many fiduciaries

only require users to confirm they meet the legal age for consent. Minors can access services by providing false information, so enforcing age verification would eliminate this issue but compromise anonymity.

Different countries define a child differently when it comes to giving consent for data processing. Generally, more protection for children's data is recommended. The Bill defines a child as anyone under 18, while in the US and UK, those aged 13 and older can give consent. The EU's GDPR states the age is 16, but it can be lowered to 13 by member countries. The Srikrishna Committee suggests a single age threshold for consent, ideally between 13 and 18, but keeping the legal age at 18 for consistency.

The Bill defines harm to a data principal as physical harm, identity theft, harassment, loss of legal benefits, or significant loss. It lists various forms of harm, including psychological harm and unfair treatment, which are not included in the 2022 Draft Bill. The Joint Parliamentary Committee proposed including psychological manipulation in the 2019 Bill's compensatory damages, which is absent in the 2022 Draft Bill. The government does not have the authority to enforce damages according to the Bill.

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

A major decision by the Indian Supreme Court in the case of Justice **K. S. Puttaswamy and Anr. v. Union of India**[23] recognized the right to informational privacy as part of the fundamental right to life in India, including privacy. However, the ruling did not define the specifics of this right or how it should be upheld. Since 2018, the Indian government has been drafting a central law to replace the SPDI Rules and act as a standalone data protection law. The Digital Personal Data Protection Bill, or DPDP Bill, is the latest version of this law and was passed by the Lok Sabha on August 3, 2023, and by the Rajya Sabha on August 9, 2023. The DPDP Act was officially published on August 11, 2023, after the President's approval.

The DPDP Act regulates the handling of digital personal data in two situations: when data is obtained in digital format and when it is collected in non-digital format and then converted to digital. It does not cover data processing in non-digital form, making it more limited compared to previous drafts. The Act's jurisdiction has been broadened, covering digital personal data processing outside India for services to individuals in India. It is unclear if the DPDP Act applies to personal data of individuals outside India. Unlike the GDPR, which only applies within the EU, the DPDP Act could create uncertainty regarding its authority, which will depend on future interpretations by the Central Government.

The DPDP Act also addresses the unique challenges of startups and includes provisions for their exemption, alongside exemptions for state and research purposes. It defines "digital personal data" as personal data in digital form and narrows its scope to include only identifiable information about individuals, eliminating previous distinctions between sensitive and critical personal data. Data fiduciaries must protect personal data with reasonable security measures and inform relevant parties in the event of a data breach, although the exact notification process is yet to be decided. The criteria for "appropriate

[23] (2017) 10 SCC 1.

security measures" are not specifically defined in the DPDP Act, but non-compliance with data protection regulations results in serious consequences.

The DPDP Act defines 'processing' as any automated procedure or sequence of procedures performed on digital personal data. This includes activities like collecting, storing, modifying, using, merging, and deleting data. When it comes to children's personal data, the Act requires that parental consent must be verified, though it doesn't specify what 'verifiable' means. The Central Government can exempt certain data fiduciaries from this rule but only if the data processing is secure. Additionally, data fiduciaries cannot process data that might harm a child.

The DPDP Act allows personal data to be shared with countries outside India unless the Central Government prohibits it.[24] While the definition of 'processing' in the DPDP Act is similar to that in the GDPR, it only includes automated processes, while the GDPR includes both automated and some non-automated processes.

The Act removes many exclusions that were present in the 2022 Bill, except for data processed by individuals for personal purposes. It adds a new exemption for personal data that individuals have made public or that must be made public by law.

The term 'data principal' has been expanded to include not only individuals but also parents or guardians of minors and legal guardians of those with disabilities. While the Act doesn't define 'person with disability,' it references the Rights of Persons with Disabilities Act, 2016, which describes it as someone with long-lasting impairments that hinder their participation in society. [25]

Data principals have rights, including the right to access their personal information, correct it, file complaints, and nominate someone to act on their behalf. They should be informed about their processed data, the companies that have it, and what data has been shared. Data fiduciaries must make necessary changes and may refuse erasure if legally required to keep data.

Data fiduciaries are defined as individuals or entities that determine how personal data is handled. The Act specifies legitimate purposes for data processing without explicit consent. They must stop storing data when it is no longer needed and are prohibited from tracking minors or targeting them with advertisements, ensuring children's privacy protection.

The DPDP Act allows the Central Government to identify certain data fiduciaries or groups as "important data fiduciaries" based on various criteria such as data volume, sensitivity, potential harm to individuals, the status of democratic elections, and state security.[26] The previous Bill's provision to consider "other variables" has been removed. Important data fiduciaries must take on additional responsibilities, which include appointing a data protection officer in India, hiring an independent data auditor for

[24] Section 16(1), Digital Personal Data Protection Act, 2023.
[25] Section 2(s), The Rights of Persons with Disabilities Act, 2016
[26] Section 10(1), Digital Personal Data Protection Act, 2023.

compliance checks, conducting data protection impact assessments, and undergoing regular compliance audits.[27] Non-compliance may result in penalties of up to INR 250 crore.

Data fiduciaries can only manage personal data for allowed purposes if they obtain the individual's consent, which must be voluntary, specific, informed, unequivocal, and clear. The individual must explicitly agree to the processing of their data for the specified purposes. The consent request must be understandable and available in English or any of the 22 languages recognized in the Indian Constitution, along with contact information for the data protection officer. Additionally, data fiduciaries must provide a detailed notice to the data principal before or while obtaining consent, explaining the data to be collected, the reasons for processing, the rights of the individual, and how to lodge complaints. If consent was obtained prior to the DPDP Act's implementation, the notice must be given as soon as possible in a clear manner.

Data principals can manage their consent through a "consent manager," which is a registered entity that facilitates consent handling.[28] There is still some ambiguity regarding consent managers' specific roles and whether all data fiduciaries must interact with them to get consent. Data principals can revoke consent at any time, which does not affect the legality of past processing. Upon withdrawal, the data manager must delete the personal data unless legally required to keep it. The Act also includes a provision for "parental permission," allowing for consent from a legal guardian when necessary.

A new adjudicatory body called the Data Protection Board of India is to be established under the DPDP Act, with the Central Government responsible for its creation and operational details. The Board will mainly function digitally for handling complaints and making decisions. While referred to as an "autonomous body," the Central Government controls the Board's composition, appointment processes, and employment terms, leading to questions about its independence. The Act outlines that members should possess integrity and expertise, with at least one legal expert, but does not provide detailed qualification criteria. Members could be disqualified for having conflicts of interest that might impair their duties.

The Board has the authority to initiate investigations based on complaints or notifications, with the power to examine individuals and call witnesses. They can issue interim and final orders, dictate corrective actions in case of data breaches, and can recommend alternative dispute resolutions or voluntary undertakings. Appeals against Board decisions must be made to the Telecom Disputes Settlement and Appellate Tribunal (TDSAT) within 60 days. TDSAT has the power to confirm, alter, or overturn Board orders, with a mandate to resolve appeals within 6 months. The TDSAT operates digitally and its orders are enforceable as civil court decrees. Penalties of up to INR 250 crore can be imposed for certain offences under the DPDP Act, with fines for data principals up to INR 10,000. The DPDP Act, 2023 safeguards privacy by mandating consent for data processing, giving individuals control over their data, enhancing

[27] Section 2(l), Digital Personal Data Protection Act, 2023
[28] Section 6(7), Digital Personal Data Protection Act, 2023

security for children's data, requiring notice and restriction of data use by organizations, and providing mechanisms for addressing complaints and imposing penalties.

The implementation and enforcement of the law by the government will be crucial for setting industry standards. Concerns remain about the potential weaknesses in certain parts of the legislation and whether the focus of enforcement will be on data-dependent enterprises or the entire industry.

Initially, the exemptions for permission give the government significant power and prioritize its regulations over those of private entities. While this may be justified during emergencies, the Act expands the situations where this applies. Section 7(b) allows the government to bypass consent if a recipient of services has previously consented. This could lead to government databases merging, allowing access to personal information of beneficiaries without a clear endpoint for data use, which raises concerns about privacy.

The law also provides exemptions for criminal prosecution, investigation, and national security. Section 17(1)(c) states that notice and consent are not required for activities aimed at preventing or investigating crimes. While this seems reasonable, Section 17(2)(a) offers a broad exemption from the law for any government body chosen by the government to maintain public order and security. This indicates that Parliament intended for certain agencies to be exempt from privacy laws, which raises concerns about the state's exemption from regulations that apply to private organizations, especially in unnecessary cases.

Additionally, the government's ability to create rules may undermine legal protections. For five years after the law's enactment, the government can declare that no company must comply with certain provisions. There is no specific timeline for this exemption, nor guidelines on its use, which could weaken the law's intent. Certain exemptions for startups and industries may also lead to further weakening of the legislation.

The government can also exempt firms from rules regarding children's data management, but the criteria for such exemptions are unclear, raising potential for misuse. While the law allows the government to set conditions and regulations, unclear guidelines can lead to excessive power over implementation, which may violate constitutional principles.

Moreover, there are issues with the design of the Data Protection Board (DPB). Procedures for appointing members are left to the government, and there are few qualifications outlined, such as a requirement for legal expertise. The lack of transparency in appointing members and assigning investigation tasks could affect the board's fairness and independence. Therefore, while the Data Protection Act aims to protect data privacy, its effectiveness may be compromised if the government does not enforce its regulations properly.

C. Comparison between GDPR and DPDPA

The EU GDPR applies to organizations in the European Union and those outside that process personal data tied to the EU. It also concerns digital personal data handled within India’s borders and by

non-Indian entities offering products or services in India. The GDPR is a rule-based framework focused on safeguarding personal data, while India's DPDPA aims to regulate personal data processing within the country.

The GDPR distinguishes between data controllers and processors, imposing different requirements. In contrast, the DPDPA refers to organizations that hold data as "data fiduciaries," who are liable for actions by their data processors. The GDPR has stricter rules for sensitive personal data, whereas DPDPA treats all personally identifiable data equally.

For international data transfers, the GDPR requires additional security measures, unlike the DPDPA, which lacks similar precautions. GDPR outlines various lawful bases for data processing, while DPDPA allows processing primarily with the data principal's consent or for legitimate use.

Both GDPR and DPDPA require consent to be informed and specific, but GDPR includes more detailed conditions around consent. DPDPA mandates comprehensibility and accessibility of consent across languages.

GDPR establishes seven data principal rights, focusing on fairness and responsibility, whereas DPDPA emphasizes justice and confidentiality. Enforcement under GDPR involves national supervisory agencies, while DPDPA allows the Indian government to create a Data Protection Board for complaint resolution. GDPR penalties, while significant, are less severe than those under DPDPA, which can reach INR 250 crores. Lastly, GDPR is rigorously supervised, while DPDPA aims for simplicity and business-friendliness, based on a fundamental right to privacy declared by the Supreme Court of India.

D. Conclusion

This paper discusses India's current data protection laws, which focus on rising fraud and data theft in the information technology sector. The laws are weak because the Information Technology Act, 2000 was mainly created to fight cyber fraud, not to protect data. The Information Technology Act, 2000 and the Information Technology Rules 2011 provide some level of privacy protection. The researcher has evaluated these laws to see how effective they are. The DPDP Act marks the start of formal personal data protection law after years of discussion. The effectiveness of personal data privacy will depend on future regulations. While the current law is practical, it may still harm privacy interests due to government control over rights.