International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Outlining Principle of Data Protection through various Indian Legislations with comparison to The Digital Personal Data Protection Act, 2023

Ravi Prakash Rahul

Ph.D. Scholar, Dr. Ram Manohar Lohiya National Law University, Lucknow

Abstract

This article is exploring a variety of legislations in different sectors, such as, financial, health, information technology, etc. to discover how the principle of personal data protection and privacy was dealt with under Indian legal regime before the enactment of the Digital Personal Data Protection Act, 2023. It attempts to compare between them and examine how the new law is an improvement over previous laws and finally suggest what changes or modifications it may require, learning from provisions under the other laws from the different sectors.

Keywords: Data Protection, Data Principals, Data Fiduciaries, Sensitive Personal Data, Cross-border data flow, UIDAI, DPDP Act.

Introduction

Data is present in an infinite amount, and is broadly classified as personal data and public data. They are moving all around the whole world through all kinds of platforms, whether they are digital or non-digital. In its basic nature, any data is simply scattered information. However, it can become one of the most influential tools in one's hands, only when it is processed and analysed, to convert and produce a more usable data, for instance: professional data, financial data, health data, geolocation data, and even browsing data. Currently, data is considered be among the most rewarding commodities as the most high-profile companies like Apple, Google, Meta, Microsoft, Amazon, etc. operate in data sector and every nation's power is based on it.[1]

A number of sectors deal in the processing of data, such as financial, health, information technology and telecommunication, security and others. These sector store and process individual's personal information like their images, signatures, locations, financial details, medical information, browsing information and so on. Additionally, the attachment of sensitive personal data, like biometrics, with Aadhaar identification, has created a state where such sectors, whether government or non- government, may obtain immeasurable authority over the data principals. The Digital Personal Data Protection (DPDP) Act, 2023 has passed only recently, following the landmark Supreme Court judgment of '**Justice K.S. Puttaswamy v. Union of India**'[2] and so the question that comes up with this is whether any safeguards were already present to the

[1] Mohan D., "Personal Data Protection Laws in India". https://www.lexology.com/library/detail.aspx?g=08197ebe-aeb4-41d6-a855-ce57a313ea6d

[2] Writ Petition (Civil) No. 494 of 2012, (2017) 10 SCC 1.

data principals to protect them from unlawful storage and processing of their data by any sectors or otherwise.

Let's examine various legal provisions already present to protect data principal's data and whether they are adequate for data protection over the new Act of 2023. The provisions already present in India that are dealing with data processing are as follows, categorised according to their concerned sector:

1) Financial Sector:

- Banking Regulation Act, 1949
- Insolvency and Bankruptcy Code, 2016
- Payment and Settlement Systems Act, 2007
- Reserve Bank of India Act, 1934
- The Security and Exchange Board of India (SEBI) Act, 1992, and allied regulations
- Insurance Act, 1938 and The Insurance Regulatory and Development Authority of India Act, 1999 (the IRDAI Act)
- The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983
- The Credit Information Companies (Regulation) Act, 2005
- The Prevention of Money Laundering Act, 2002
- The Income Tax Act, 1961

2) Health Sector:

- The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002
- Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994
- The Mental Health Act, 1987
- Digital Information Security in Healthcare Act, 2018 (DISHA Act)

3) Information Technology and Telecommunications Sector:

- The Indian Telegraph Act, 1885
- Information Technology Act, 2000, and SPDI Rules, 2011
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

4) Other relevant sectors:

- The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016
- The Right to Information Act, 2005

Financial Sector

Before the new Data protection law of 2023, the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the SPDI Rules) mainly dealt with protection of personal data in financial sector, to lay the obligations on corporate bodies, where the SPDI rules regulated data collections and processing. As per these Rules, personal data includes passwords, financial information such as account details or payment instrument details, mental, physical, or physiological health condition, medical records, sexual orientation, and/or biometric information. The principle of data privacy is critical in the financial sector, as it mainly deals with data related to any individuals' finances, along with their other personal details.

The laws and regulations directing to preserve the privacy principle among the data collectors in this sector are as given below: -

1. **Banking Regulation Act, 1949** and the norms and regulations related to it creates a structure for operational aspect of Indian banks and provides the RBI with the authority to control, authorize and oversee the banks. The Act mentions confidentiality of information and regulation of data gathering, storage and protection. The Tribunal or any other authority do not have to power to compel the Central Government or Reserve Bank to produce any account or document which is considered as confidential.[3]
2. **Insolvency and Bankruptcy Code (IBC), 2016** came to promote the quick resolve to the bankruptcies and making insolvency laws consistent with international standards. Under the code. The Liquidator has power to access any data for the proof and admission of claims and determining liquidation assets of the corporate debtor. He may be asked to provide the creditors with any financial data of such debtor.[4] The Code further provides the Insolvency and Bankruptcy Board of India with the power to call for any data relating to insolvency from insolvency professional agencies, and to form the method of collection, storage, and access of the data records.[5]
3. **Payment and Settlement Systems Act, 2007** was passed to supervise and regulate payment methods and designate Reserve Bank as an authority on payment systems in India. The Act has defined "*trade repository*" as a person who collects, organize, store, maintain, process or distribute electronic records and data relating to financial transactions;[6] and the obligations mentioned in the Act are also applicable on such trade repository.[7] RBI can access any data related to any system provider's payment system[8] and further can authorise any officer of RBI to inspect any equipment, documents and call any employee working in the premises where such payment system is operated and to provide any document or other information required.[9] However, RBI is mandated to keep such collected data confidential, except where disclosure is necessary for protecting the integrity and effectiveness of the payment system.[10] The Act further obligates the system providers to keep the system participants' data confidential, unless the disclosure is required by law, or with their consent, express or implied, or under the obedience of an order passed by any court.[11]
4. **Reserve Bank of India Act, 1934** was brought to establish RBI as an authority to regulate the issuing of Bank notes as well as securing monetary stability in the country. Under Chapter III-A of the RBI Act, i.e., the "**Collection and Furnishing of Credit Information**", RBI is authorized to collect and furnish the credit information to and from banking companies.[12] However, such Credit information collected or furnished as mentioned under Sections 45C and 45D of the RBI Act is prohibited to be revealed as it shall be considered confidential, unless under certain circumstances like public interest, and with prior permission of RBI. However, RBI or other banking companies cannot be compelled by Court, Tribunal or any authority to disclose the information obtained.[13]

[3] Sections 34A, 36AI, The Banking Regulation Act, 1949.
[4] Section 37, Insolvency and Bankruptcy Code, 2016.
[5] Section 196, Insolvency and Bankruptcy Code, 2016.
[6] Section 2(1)(a), Payment and Settlement Systems Act, 2007.
[7] Section 34A, Payment and Settlement Systems Act, 2007.
[8] Section 13, Payment and Settlement Systems Act, 2007.
[9] Section 14, Payment and Settlement Systems Act, 2007.
[10] Section 15, Payment and Settlement Systems Act, 2007.
[11] Section 22, Payment and Settlement Systems Act, 2007.
[12] Section 45B, Reserve Bank of India Act, 1934.
[13] Section 45E, Reserve Bank of India Act, 1934.

5. **The Security and Exchange Board of India (SEBI) Act, 1992** was enforced to establish SEBI as an authority to call for information regarding stock exchange, mutual funds or other person associated with securities market, including any Bank, authority or Board or corporation related to any investigation of the SEBI. The data can be called from within or outside India. However, when providing any information to any authority outside India, it may have to be done through an agreement with such authority with a prior approval of the Central Government.[14] The Act imposes penalties of up to 1 lakh to 1 crore per day, on persons failing to furnish the information required or furnishing incomplete or incorrect data.[15]
6. **Insurance Act, 1938** along with the **Insurance Regulatory and Development Authority Act, 1999 (IRDA Act)** deals in the insurance area which has forever stood as a data focused sector due to working through substantial amount of data collection and processing of clients and employees, including their health data. The insurance work chain includes third-party administrators, third-party broking houses, human brokers and contractual agents, who handle customers and their data on insurer's behalf, therefore, creating additional circulation of the consumers' personal data. In any inspection by an investigating officer, the Act requires the insurers, including the service provider, insurance intermediary, etc. to produce all the relevant documents and other information.[16] The IRDA Chairperson has similar power to call for any information, by a written notice, from any insurer regarding his business and the insurer will be obligated to comply.[17] The IRDA Act obligates insurers to keep the customers' information confidential by having sufficient protection measures, that also applies to the third-party service providers.
7. **The Income Tax Act, 1961** largely deals in data privacy related to book-keeping and maintaining information in relation with transactions, whether made locally or outside India.[18] The income tax authorities have the authority to ask for providing them with certain personal information, which is subject to the provisions and regulations of Information Technology Act and SPDI rules.

Health Sector

The Healthcare system fundamentally functions through the trust of their clients or patients. So, the principle of data privacy is also essential under the healthcare system, as the organizations store various kinds of personal data of their clients, including name, address, medical records, psychological profile, and in current times, their Aadhaar details. These types of information are known as **Protected Health Information** or **PHI**.

Therefore, the protection of their data needs to be ensured too, for easy access to healthcare, without the breach of trust and privacy of the patients. The Indian laws related with healthcare, that are also dealing with the data protection principle, are discussed as follows: -

1. **The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002** was enforced to give the Medical Council of India (MCI) power to regulate professional conduct, ethics and etiquettes related to medical professionals, such as, the physicians' duty to keep medical records and maintain the secrecy of their patients, as given under first chapter of the Regulations, dealing with

[14] Section 1, The Security and Exchange Board of India (SEBI) Act, 1992.
[15] Section 15A, The Security and Exchange Board of India (SEBI) Act, 1992.
[16] Section 33, The Insurance Act, 1938.
[17] Section 110C, The Insurance Act, 1938, and Section 14(2)(h), IRDA Act.
[18] Section 9, The Income Tax Act, 1961.

Code of Medical Ethics. It also mandates every physician to issue such records within 72 hours, if requested by the patient, their authorised attendant or any legal authorities concerned.[19] In case of failure, it would constitute a professional misconduct.[20] The seventh chapter, dealing with **Professional Misconducts**, obligates the registered medical practitioners to not disclose any secrets of their patients, including their identity, unless it is required by the court, or where such non-disclosure may be leading to a high risk to another specific person or community, for instance, in case of communicable disease.[21]

2. **Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994** was enforced as a necessary action against pre-conception sex determination or selection done by any individual, association, Genetic Counselling Centre, Labs or Clinics, etc. Under this Act, it is prohibited, in all manners, to communicate, publish, or distribute any information regarding the pre-natal determination of sex or sex selection pre-conception. The punishment for violation of this prohibition is up to 3 years imprisonment and fine which is not more than 10,000 rupees.[22] The Appropriate Authority has the power to enter such centres, search and examine any records and relevant documents, and seize and seal them in case any violation and the genetic clinic, etc. has to maintain records, reports, consent letters and other relevant documents, to furnish them to the authority or any authorised person.[23]
3. **The Mental Health Act, 1987** regulates the treatment and care of the mentally ill person. So, in relation with the data privacy principle, any patients' personal records found during inspection must be kept confidential unless the inspecting officer believes with reason that the psychiatric hospital is not providing a proper treatment and care to their patients. The officer, in this case, will report the matter to the licensing authority, which, consequentially, will issue instructions to the hospitals for them to comply with.[24]
4. **Digital Information Security in Healthcare Act, 2018 (DISHA Act)** was drafted by the Ministry of Health and Family Welfare (MoHFW) to promote and ensure the data security, privacy, reliability, and confidentiality related to digital health. An individual is provided with several rights under the Act, for instance, right to have access to their digital health records, correct or change it, right to confidentiality, right to seek damages at the events of data breach, and the right to consent for each usage of their data along with the right to refuse consent for access, collection, storage, or disclosure, etc.[25]

Information Technology and Telecommunications Sector

The information technology sector is the key sector that deals with the normal, personal and sensitive data of all citizens of India. Data and Technology are so interconnected that whenever the access, collection, storage, processing or transmission of data are being discussed, the information technology systems will always be the most responsible for data privacy mechanism. Hence, it is crucial to understand the way this

[19] Regulation 1.3, The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
[20] Regulation 7.2, The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
[21] Regulations 7.14, 7.17, The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002.
[22] Section 22, Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994.
[23] Sections 29, 30, Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994.
[24] Section 13, The Mental Health Act, 1987.
[25] Section 28, Digital Information Security in Healthcare Act, 2018.

sector deal with the personal data, the security measures it adopts and legal remedies it provides to the data owners when there is breach. A few laws under this sector are discussed below: -

1. **The Indian Telegraph Act, 1885** was passed during the British India to govern and regulate the telegraph services. While the prime intention behind it was to control telegraphy, its provisions contain inferences for data privacy, mainly within the framework of communication interception. The Act was framed way before the arrival of the digital age and the modern technologies, and the law is not clearly addressing current data privacy issues per se. The Act gives the government the authority to monitor as well as intercept telegraphic communications for the sovereign interest and national integrity, security, foreign relations, etc.[26] Though it is subject to certain procedures and safeguards; it anyway permits the interception without obtaining an individual's explicit consent.
2. **Information Technology Act, 2000, and SPDI Rules, 2011** were the main legislation related to e-commerce and data protection before the passing of new DPDP Act, 2013. Section 43A of IT Act read with Rule 4 of the SPDI Rules, specifically mentions safeguarding Sensitive Personal Data that is under possession of a body corporate, by way of employing measures to maintain secured procedures, and in failure of compliance, liability for compensation. The IT Act, 2000 has defined "Sensitive Personal Data" as such information as it may be proposed by Government, while the SPDI Rules defines it under Rule 3 as any data in relation with passwords, mental, physical, and physiological health conditions, sexual orientation, medical records, financial information, and biometric information. Punishment in case of breach has been given under the IT Act, if a person, access any data and download without permission of the owner of data, or damage, delete, alter or steal such data.[27] Authority to access any computer system, data, etc. for investigation has been given to the Controller if he has reason to believe that a violation has been done.[28] Section 44 of IT Act mentions punishment where there is failure to furnish such information to the Controller. SPDI Rules obligates the body corporate to obtain prior consent from the data owners before disclosing their data to a third party, unless a contract permitting such disclosure exists or it is for identification, investigation, detection, or prevention of cyber-crimes by the Government agencies. However, the data obtained must not be disclosed to any other person.[29] The Rules also puts body corporate under obligation to implement appropriate security practices and measures, and in case of any breach of data, they have to prove that they implemented such measures.[30]
3. **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** was brought to regulate social media platforms and their conduct. It primarily sets parameter to regulate contents, online safety, and hold the social media intermediaries accountable. the intermediaries must follow due diligence, such as, informing their users about privacy policies, etc., instructing not publish, or store, etc. any derogatory content, invasive of another person's privacy, and the outcome of violation of their policies, such as service termination, etc.[31] The Rules obligates the Significant intermediaries to allow recognition of first originator of an information for detection,

[26] Section 5, The Indian Telegraph Act, 1885, s. 5.
[27] Section 43, The Information Technology Act, 2000, s. 43.
[28] Section 29, The Information Technology Act, 2000, s. 29.
[29] Rule 6, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[30] Rule 8, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[31] Rule 3, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

prevention, or punishment, etc. of any crime harmful to national security, foreign relation or public order, whenever required by a judicial order. However, the disclosure is limited the identification and no other information of the first originator.[32]

Other Relevant Sector

Other sectors dealing in data processing, collection and protection that are there, either providing services to the Indian citizen or working as a backing of the government. They are briefly discussed below.

1. **Aadhaar Act, 2016** was enacted to govern and protect Aadhaar Data. Initially, the Planning Commission considered the project called 'Unique Identification for Below Poverty Line (BPL) Families' as an initiative towards providing credentials to each citizen of India in order to provide them with efficient welfare schemes.[33] On September 29th, 2010, it was the first time a UID number was allotted to a resident of Maharashtra. Later, on July 12th, 2016, the government, under the Ministry of Electronics and Information Technology (MeitY), established a statutory body, namely, The Unique Identification Authority of India (UIDAI). UIDAI was created in accordance with the Aadhaar Act which was passed on March 11th, 2016 to provide legal backing to the UID number. The statutory body's main function was to create UID, also known as, Aadhaar, issuing it to all the Indian citizens, as well as, making policies, procedures for managing the stages of Aadhaar.[34]
   The Act puts a requirement to obtain informed consent from the UID holder, before using it for authentication[35], and in case of a minor, the parents' or guardian's consent is required.[36] The use and disclosure of UID data is limited only for the informed purpose given in writing at the time of its submission. However, sharing the core biometric information is not permissible under any situation whatsoever, except for generating UID and its authentication, as such data is considered as '**sensitive personal data**' as mentioned under Section 30 of the Act.[37] UIDAI is obligated to assure the confidentiality of the identity information and incorporate essential measures to prevent unauthorised access, use, or disclosure of the information stored.[38] Any such violation, i.e., unlawful access, stealing, damaging, deleting, etc. is met with punishment of imprisonment, and fine.
2. **The Right to Information Act, 2005** was passed with intent to promote government's accountability and transparency for theirs conducts by inspiring the Indian people to pursue information from authorities. This is an opposite right to the data privacy principle that promotes privacy, and therefore, a conflict between these two rights exists. Unless the Central Public Information Officer or the State Public Information Officer or the appellate authority is satisfied with the data disclosure, the Act excuses any such data disclosure through RTI which is not related to the interest of public at large in any way and which needlessly invades an individual's privacy.[39] Moreover, when such data is partially exempted, then the disclosure of the part of non-exempted data will be permitted.[40]

[32] Rule 4, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[33] UIDAI. https://upite.gov.in/UPDESCO/StaticPages/UIDAI.aspx
[34] Unique Identification Authority of India. https://uidai.gov.in/en/about-uidai/unique-identification-authority-of-india.html
[35] Section 4, The Aadhaar Act, 2016.
[36] Section 3A, The Aadhaar Act, 2016.
[37] Section 29, The Aadhaar Act, 2016.
[38] Section 28, The Aadhaar Act, 2016.
[39] Section 8(1)(j), The Right to Information Act, 2005.
[40] Section 10, The Right to Information Act, 2005.

Complexities of above laws with Digital Personal Data Protection Act, 2023

Bits of the data privacy principle can be discovered within these legislations that function in their own specific areas and capacity. It is observable that these laws have a particular way of dealing with data collection, usage or protection according to their framework. They act either as a protection and support for the Indian citizens or as an advancement to the government role and authority. Since the Digital Personal Data Protection Act, 2023 has been enacted, these sectoral laws may occasionally function as a support to this Act wherever the digital personal data protection of an individual will be concerned.

However, with its own limitation the Act is not applicable to data present in non-digital form. The DPDP Act does not define Sensitive Personal Data or has any specific law for its protection. The IT Act and the SPDI Rules may still have the ability to provide better protection here, as they have covered it. If the DPDP Act is compared with previous present laws of the above-mentioned sectors, some similarities may be found too. Legislations like the Credit Information Companies (Regulation) Act, 2005, The Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983 and the Prevention of Money Laundering Act, 2002 have similar provisions related to calling for data and the confidentiality of it, along with regulating measures related to collection, processing, storage or usage, and even prevention unauthorized access and disclosure. The DPDP Act has provisions under Chapter II, such as sections 4, 5, 8, 9, etc., similarly obligating the data fiduciaries to take measure for lawful, collection, storage or processing of data. In 2018, RBI brought the data localisation norms by a written guideline on storage of payment system data, which requires all the data regarding local transaction to be stored within the servers located in India. Similarly, the Digital Personal Data Protection Act, 2023 mentions cross border data flow under section 16. Such common principles can be found all over the place, if these laws are compared.

Conclusion and Suggestions

So, it is apparent that a number of similar provisions regarding data privacy principles are present in both, the new DPDP Act and the other sectoral legislations, however the key difference is either regarding the intensity of the protection and punishment, or its implementation. For instance, earlier, it was discussed how the restriction on cross-border data flow has been mentioned by RBI, in its guideline, and under the Digital Personal Data Protection Act, 2023. However, under the DPDP Act, the power has been given to central government to restrict the data transfer outside India by notification and no other harsher scrutiny mechanism has been specified, regardless of how crucial it is to aim for a strict mechanism here. Another difference that is found is that the DPDP Act gives out a much stricter punishment in the event of a breach. For instance, punishments under the Payment and Settlement Systems Act, 2007, for violations in few cases, is a fine of rupees up to 10 lakh or imprisonment for not more than 6 months or with fine not exceeding 5 lakh or an amount equal or twice the damages suffered. However, under the DPDP Act, the punishment ranges from 10,000 to up to 250 crores, which is clearly way higher than any punishment provided.

The Act has brought some great changes, from greater obligations on Data Fiduciaries to establishment of Data Protection Authority. There is undoubtedly a need to wait and perceive its practical implementation with respect of these sectors or otherwise, and know what improvements or loopholes have been brought into existence. However, a few suggestions are there that may solve some of the issues with the new Act, which are as follows:

1. There must be a specific provision under the DPDP Act dealing with Sensitive Personal Data, to ensure the safety and security in the usage, processing, storage and transfer of such crucial data.

2. A more serious scrutiny mechanism for cross-border data flow is needed rather than a vague authority of central government to notify any data as restricted.
3. The data fiduciaries can utilize Artificial Intelligence and machine learning processes to determine, and prevent any breach in their system in order to avoid violations and harm to the data owners. However, it can be said without a doubt that this practice may not be foolproof and may contain errors.
4. Data literacy must be encouraged at the education level in order to teach people the skill to understand the type of data they share, identify potential harm and furthermore, critically evaluate online distribution of their data.