https://doi.org/10.48047/AFJBS.6.Si2.2024.5334-5350

The Contours of Data Protection: Study of Indian Jurisdiction in View of Global Perspective

Alina Ali[1]
student, Department of Law, Manipal University Jaipur.

Dr. Sony Kulshrestha[2*]
Associate Professor, Department of Law, Manipal University Jaipur

Article history
Volume 6 issue si2 2024
Received:18Apr2024
Accepted:20Jun2024
doi:10.48047/AFJBS.6.Si2.2024.5334-5350

Abstract:
In the modern era, with the ubiquity of online services, it has become necessary for individuals to share personal information with websites, which can pose a significant risk to their privacy. This is because it can lead to identity theft and other security breaches. The need to accentuate privacy requirements with a robust system, and to halt the constant misery of an individual to compromise his/her personally identifiable and user-sensitive information, was thus immediately felt, especially when Non-Personal Data loosely fits in the definition of 'data' and does no good in identifying individuals and pose a complex matter when it comes to the security of Non-Personal Data. Therefore, it is paramount to establish a robust system that efficiently safeguards sensitive data and prevents any unauthorized use. It is essential to note that even non-personal information can still pose a risk to individuals. This research paper is a thorough analysis of India's data protection framework using the doctrinal research methodology. The critical examination will cover relevant technology and data protection laws. A comparison with other jurisdictions to identify potential gaps in the Indian context has also been looked into. Finally, based on the findings of the paper, necessary measures are recommended to address any shortcomings so discovered.
Keywords: Online services; Personal information; Risk to privacy; Identity theft; Security Breaches; Robust system; User-sensitive information; Non-Personal Data; Sensitive data; India's Data protection framework; Data protection laws; Personal identity

1. Introduction

1.1. Purpose

This paper analyses the aspects of data protection in India through the lens of a comparative study of foreign jurisdictions and puts forth the inferences followed by suggestions to combat situations that pose a threat to data protection and data privacy.

1.2. Methodology

The analysis of all the aforesaid literature has been done Doctrinal based on analysis of relevant reports, cases, and statutes followed by a comparative and inferential study.

1.3. Findings

- Whether the current and prospective Indian legislation meet the global data protection standards?
- Whether the laws are adequate to cover the aspects of non-personal data?
- Are there any progressive efforts for data protection given the Personal Data Protection Bill, of 2019, and Digital Data Protection Bill, of 2022, and the Personal Data Protection Act, of 2023?

1.4. Originality/Value

The research conducted for the paper has been purely undertaken by the Author(s) and is purely original.

2. Overview Of the Paper

Table I: ***Overview of the Paper***

S.No.	Number and Name	Brief Overview
A.	**1. Nature and Types of Data**	The foremost topic deals with a brief introduction about what is data and what are the different types of data by mentioning the definitions as defined under various statutes regarding Data in India.
B.	**2. Personal V. Non-Personal Data: A Perusal Through the Lens of Anonymization**	Part 2 throws light on the process of anonymization and defines non-personal data to be more anonymized in comparison to personal data.
C.	**3. Personal and Non-Personal Data: Roles and Importance**	Part 3 highlights the roles and the importance of personal and non-personal data by emphasizing the legal framework and insisting on its implementation in India.

D.	**4. Privacy Concerns and Risks Associated with Data –** **4.1.Personal Data** **4.2.Non-Personal Data**	Part 4 briefs about the two broad types of Data- Personal and Non-Personal Data, along with the associated risks and privacy concerns while handling them.
E.	**5. Legal Framework for Data Protection in India**	Part 5 deals with the mentioning of the existing legal frameworks in India under the ambit of which the concept of Data Protection falls, such as the Information Technology Act.
F.	**6. National Data Governance Framework Policy (NDGFP)**	Part 6 briefly describes the constitution of NDGFP by the Ministry of Electronics and Information Technology (MEITY) which comprehends the ways of processing Digital Government Data in various efficient ways.
G.	**7. Juxtaposing The Digital Data Protection Bill, 2022, And the Personal Data Protection Bill, 2019: Will the New Act Suffice?**	Part 7 draws a stark comparison in a tabular format, between two different types of bills introduced in the Indian legislature, the Digital Data Protection Bill, 2022, and Personal Data Protection Bill, 2019, as compared to the Digital Personal Data Protection Act, 2023.
H.	**8. Global Perspective of Personal Data: in**	Part 8 curates a comparative study between the legislature of the various global countries and that of India. The major focus of the study is the comparison between the European Union's

	relevance of Indian Scenario	framework and the Indian framework for dealing with Personal and Non-Personal Data.
I.	**8.1.European Union's: General Data Protection Regulation (GDPR)** ***8.2.****Unique Features of GDPR* ***8.3.****Application of GDPR* **8.4.***Impact of GDPR on various spectrums of technological advancements*	The sub-section under Part 8 deals with the specific Data Protection and Regulation legislature of the European Union, involving its unique features, its application, and its impact on technology under 9.2., 9.3., and 9.4., respectively.
J.	**9. Inferences and Loopholes** **9.1.Indian Perspective** **9.2.European Union's Perspective** **10. Recommendations**	Part 9 compares the stance of both, the Indian Non-Personal Data Framework and the European Union's General Data Protection Regulation (GDPR) followed by country-specific recommendations under sub-section 10.3.1. and 10.3.2.
K.	**11. Conclusion**	The conclusion gives a glance over the existing loopholes that the Indian framework on Personal as well as Non-Personal Data and the need for appropriate and robust laws for a secured position of the data of the citizens of the country. The conclusion also addresses the Research proposition aforementioned.

2.1 The Nature and Types of Data

Indian legislature does not deal with data protection yet with a robust and bolstered mechanism. Nevertheless, in 2006, the Indian Parliament introduced the Personal Data Protection Bill, the law of which was successfully passed in the year 2023. The Bill has been framed on the generic principles stated in the European Union's Data Privacy Directive, 1996. It aims to follow a comprehensive model that sets forth its objectives, including collecting, processing, and distributing personal and private data (1). Various revised versions of the PDP Bill, 2006 were passed in the subsequent years of 2019 and 2021.

The Personal Data Protection Act, of 2023 defines "data" under Section 2(h) as a representation of information of the facts, opinions, or instructions in a manner suitable for purposes of communication, interpretation, or processing either by humans or through an automated mechanism.

According to the reports of the Kris-Gopalakrishnan Committee on Non-Personal Data Governance Framework, data may be categorized in many ways as follows (2)

i. Arising from the subject of data
ii. About its purpose
iii. The source of data
iv. Level of processing
v. Collector of the data
vi. The extent of involvement of stakeholders in the creation of data

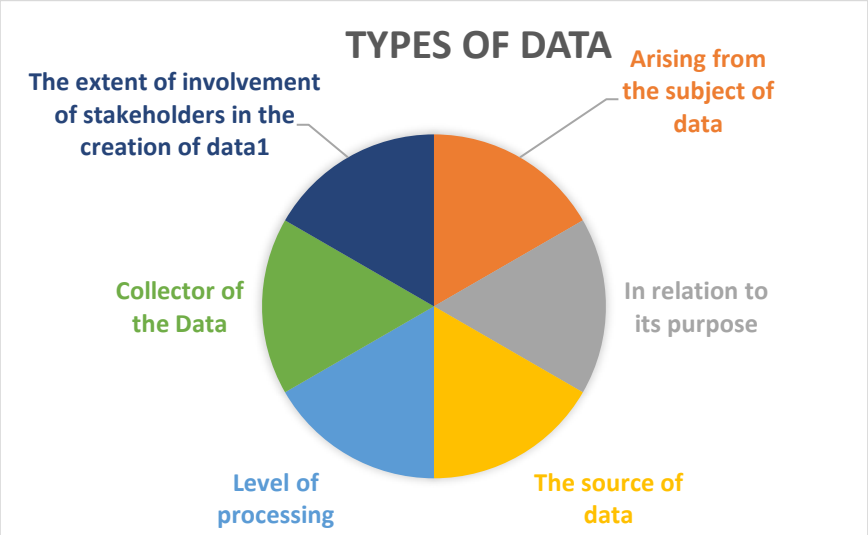

Figure 1: ***Visual Representation of the Types of Data***

For this research, the aforementioned basis of the 'collector of the data', is useful which divides the data into 'Public or Government Data' and 'Private Data'. The Personal Data Protection Act, of 2023 defines "personal data" under Section 2(t) as the data about an individual who is identifiable by or in relation to such data. (3)

On the other hand, the Non-Personal Data revolves around any set of data that does not contain personally identifiable information. This means that no individual or living person can be identified by looking at such data. The principal characteristics of such type of data are that it pertains to traits, attributes of identity, and individual characteristics of an individual which does not include any personal details. Non-personal data is never related to natural persons – or else, the nature of personalized data can be changed through a process known as anonymization. Data Anonymization is a data processing technique to protect private or sensitive information by removing or modifying personally identifiable

information through erasing or encrypting identifiers (measures to identify an individual, like name, age, contact number, etc.). Identifiers, also known as Personally Identifiable Information (PII) help detect an individual and get connected to him/her from the data stored on the internet. Various anonymization techniques involved are- K-anonymity, L-diversity, T-closeness, Diffix, ARX, Amnesia, etc. (4)

When the data is not 'Personal Data' (as defined under the PDP Act), or the data is without any Personally Identifiable Information (PII), it is considered Non-Personal Data (5)

A general definition of Non-Personal Data according to the data's origins can be: -

- Firstly, the type of data which not related to any identifiable natural person, for example, data on weather conditions, data from sensors installed in machines, etc.
- Secondly, data that were personal when derived but were later turned into anonymous data through data transformation techniques.

Non-personal data can also be classified on a different basis, broadly speaking of which are Public Non-Personal Data (the data which is cumulated by the government), Community Non-Personal Data (comprehensive data identifiers that involve information about a set of people who hail from the same demography), and Private Non-Personal Data (It includes data collected by most of the private companies or entities through privately owned processes).

3. Personal V. Non-Personal Data: A Perusal Through the Lens of Anonymization

Non-personal data is suspected to be in a more anonymized manner as compared to personal data and the true nature of anonymized non-personal data lies within the essence of personal data. If the latter is in the sensitive mode, the former would also result in being of sensitive character. Albeit the anonymization procedure could discard the chances of Non-Personal Data being used for some illegal or unethical usages, data related to a certain nature or category, such as that of national security or maybe of strategic significance, even the anonymized disposition could prove to be harmful. Simultaneous involvement of both, computer science technology and human interference will inevitably lead to some degree of mutability or reversibility of "completely anonymized" data.

4. Personal And Non-Personal Data: Roles and Importance

The legal framework relating to data had a well-planned intent of setting rules for processing the personal data of officials hailing from companies situated in India and other foreign countries that deal with the personal data of individuals and residents in/of India. The role of personal data is to instill accountability in the companies for the usage of data which requires them to foster security safeguards such as data encryption, along with necessary institution of grievance redressing mechanisms for addressing complaints of the individuals. One of the key importance of the provision of Personal Data is that it sets the rights of individuals in place, such as the right to obtain information, seek transfer of data, etc. (6)

Looking on the other side of the coin, the primary role or importance of Non- Personal Data is suspected to be aiding any data fiduciary or a data processor in the provision of any anonymized non-personal data for directly targeting the deliverance of services or implementation and formulation of any authentication- based policies by the Government of India. The NPD Committee states through its report that the collection of Non-Personal Data by both, the government as well as any independent organization, involving citizens and laymen would ultimately lead to an increase in transparency, exceptional services and innovation, and overall improved efficiencies – protecting and regulating the nature of which will help bolster overall economy of the country.

5. Privacy Concerns and Risks Associated with Data

5.1. Personal Data

Privacy as a concept is as old as human civilization but it is difficult to entertain at the same time. For a government to contemplate matters of 'privacy', it is important to search for the correct meaning of the term "Privacy". There are a variety of Privacy types that have evolved with time and have developed as an important Right that needs to be safeguarded looking at the speed of developments in the digital age we live in today. Privacy concerns and associated risks are part and parcel of every shared information online and mishandling, misusing of private information to gain unfair advantages over the owner of the information, location tracking and disclosure, cyberstalking, etc. are all part of it.

Along very similar lines, Personal Data in the forms of writing, speeches, or any other electronic format has failed to be protected by one wholesome legislation in India. There are a wide variety of safeguards, although indirectly related to each other, such as the IT (Amendment Act of 2008) and IT (Sensitive Personal Data or Information) Rules of 2011 which cover the significant and most relevant as well as repetitive crimes in the sector of Data Breach of Personal Data. The risks of a non-legislated matter like that of Data Protection in fields of consumerism and data localization in applications, to name a few, can come at a cost for the individuals.

The Supreme Court upheld the "Right to Privacy" in K.S. Puttaswamy c. UOI in August 2017 (7) after which a Committee of Experts by the Indian government was established, headed by Justice B.N. Srikrishna, which was instilled with the responsibility to dig deeper and investigate the Data Privacy problems pertaining in India during the case. (8)

The legislation as recommended by the committee is still not enacted in the form of a statute as it is pending before the parliament for future deliberations.

However, it must be taken into account that risk related to non-personal data is equally alarming, therefore the Digital Data Protection Act, 2022 aims to cover both types of data. The crucial aspects and intricacies of risk related to non-personal data are covered under the heading below.

5.2. Non-Personal Data

There are a lot of rising cases regarding concerns revolving around the re-identification of Non-Personal Data since it is anonymized, and the same problem is not identified by the Report given by the committee since it assumes that as soon as Personal data converts its nature to non-personal, the frameworks tend to treat it with less sensitivity and less prone to risk, which is a false assumption. NPD is just as prone to risk as personal data, if not more. (9) The risk factor for Non-Personal Data also revolves around the required consent of the data principal (the owner of the data) for its collection and processing. Since procedures like re-identification and de-anonymization of the anonymized data are easier to carry out, the NPD committee has advocated the mandatory consensual framework by data principals for data usage. Since the major risk involved concerns data re-identification, the committee suggests that anonymization of data should follow appropriate standards

The three different types of Non-Personal Data based on Sensitivity Levels, as defined by the Report given by the committee of Experts set up by The Ministry of Electronics and Information Technology (MeitY), Office Memorandum No. 24(4)/2019-CLES dated 13.09.2019 was issued to create the 8-member committee to deliberate on a Data Governance Framework (10) suggests that the information can become vulnerable and thus can be classified- namely, the General NPD, the Critical NPD, and the Sensitive NPD. Where the former 2 are yet to be defined by the committee, the latter includes non-personal data related to national security or strategic interests, and all other confidential information that bears the potential of becoming prone to re-identification. As the risk and threat to data both personal and non-personal are highlighted it is now, relevant to analyze the available legal framework in India for data protection.

6. Legal Framework for Data Protection in India

The articulation of privacy in every sphere of life is done in every plausible manner – through messages, social media, advertisements, and whatnot. The intensity and frequency of such awareness messages stress enough the matter of privacy and why privacy matters. For an economy like India which is data-driven, data privacy and protection should be made a foundational stone. Statistics reveal that around 21% of online users are victims of account hacking. The right to privacy is so important that Article 21 of the Indian constitution reserves the privacy matters of individuals, under the Right to Life which comprises the Right to privacy as well as the right to protect life and personal freedom. Privacy matters because of reasons like power limitation, individual respect, management of reputation, giving away of one's life to another's hands, and conservation of rights like freedom of thought (11) and speech under article 19(1)(a) of the Indian Constitution.

The real question revolves around whether there could be a healthy co-habitation of advanced capabilities of technology and intelligence companies and agencies to have access to any individual's private information, with bolstered privacy rights of the same individuals. (12)

With increasing access to social media all over the world, Indians make up a huge part of the available data for data hackers to use. For the avoidance of such mishaps, robust legal procedures are required, and some of the following procedures for the protection of the privacy of individuals, in India, are: -

- Article 43(A) of the Information Technology Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011- A corporate body entrusted with possessing, handling, and dealing with data must maintain reasonable security practices to safeguard the data of individuals. (13)
  No upper limit has been prescribed for compensating the victim or the affected party in varying circumstances.
- Section 72A of the Information Technology Act, 2000, Punishment for disclosure of information in breach of lawful contract. – Any person who secures access to any personal data containing sensitive and personal information with intent to cause or knows that it can cause wrongful gain or loss to the concerned person shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both. (14)
- Section 66C of the Information Technology Act, 2008 says- If any person fraudulently or dishonestly uses electronic signature, or password or any other unique identification
- feature shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to a fine which may extend to rupees one lakh. (15)
- Section 8(1)(j) of the Right to Information Act – deals with information related to personal with no public interest or such information if declared in public will cause an invasion of the right to privacy shall not be generally disclosed unless Central Public Information Officer or State Information Public Officer or concerned appellate authority deems fit in the larger public interest. (16)

The aforementioned and many other provisions in the Indian context for the protection of privacy of individuals and their personal information have been in force in India for a long time but merely providing for such provisions and lacking in their proper implementation does not resolve the issues of privacy matters and concerns of individuals revolving around the data of Personal nature and completely ignores the existence and use of non-personal data.

Indian legal framework only specifically targets Personal Data and has worked in the direction of safeguarding the measures of Personal Data and any mishap. The non-personal data, on the other hand, remains uncovered, thus posing a serious threat to the individual owners of it along with being indicative

of major lacunae in the legislative processes with regards to Data Protection – which only aims at protecting one its kind; Personal Data, and leaves the other, totally untampered.

7. National Data Governance Framework Policy (NDGFP)

Continuing the trend of protection of personal and non-personal data, the Ministry of Electronics and Information Technology (MEITY) published the draft plan of the National Data Governance Framework Policy (NDGFP) aiming at the transformation of government data collection strategies and managerial procedures (17). The Government of India realized the barriers that prevented an innovative ecosystem of data science, analytics, and AI from emerging to its full potential and the subsiding efficacy of data-driven governance which must be curbed through a systematic authority. It comprehended the differing and inconsistent ways of managing, storing, and assessing the Digital Government Data currently and hence felt the need for a National Data Governance Framework Policy (NDGFP) for a better-abled effective Digital Government, public good, and innovation. (18) NDGFP is anticipated to become a catalyzer of Data and AI start-ups that will in turn spur research, innovations, and growth of the Indian Data by creating and accessing anonymized and non-personal data sets.

NDGFP has focused on the creation of the following: -

- India Data Management Office (IDMO) creation which is responsible for framework, management, reviewing, and revising the policy along with the development of rules, standards, and guidelines. It will also serve as a developer of a standard mechanism for inter-government data access, and a provider of a comprehensive and flexible set of rules and standards.
- India Datasets Platform is responsible for designing and managing of Indian datasets platform that would process dataset requests and will be responsible for the provision to the researchers and start-ups, access to non-personal data and anonymized data.
- Dataset Requests, according to NDGFP would be accessible and available to Indian entities only on a priority basis or exclusively.
- Data Principal Rights are specified by NDGFP that it is the responsibility of IDMO that the 'data usage rights in addition to the permission purposes' should be with the data principal (the owner of the data). With the ambiguity of the nature of the data usage rights of the data principal and the absence of any existing legislation on the protection of non-personal data, in India, there is unclarity.

8. Juxtaposing The Digital Data Protection Bill, 2022, And the Personal Data Protection Bill, 2019: Will the New Act Suffice?

The lack of enough comprehensive legislation regarding Data Protection in the country has led the Center's Ministry of Electronics and Information Technology (MeitY) to pen down yet another interesting aspect of the Data Protection series, another version of the Data Protection Bill, called the Digital Data Protection Bill, 2022. Both, the Digital Data Protection Bill and the Personal Data Protection Bill have finally found their intersection which led to legislation of the Digital Personal Data Protection Act, 2023. The fundamental right of Right to Privacy which is enshrined under Article 21 of the Indian Constitution, is upheld in this draft bill, as expected.

Through the lens of the development of Privacy protection rights and bills in the country, it is safe to conclude that India has struggled to table a perfect, flawless, and non-controversial law on privacy and its domains. However, the government of India legislated the Digital Personal Data Protection Act of 2023 as the result of the modifications done to the Personal Data Protection Bill of 2019, undertaken by a committee report under the Chairmanship of Justice B.N. Srikrishna.

A juxtaposing view on the Digital Data Protection Bill, 2022, the Personal Data Protection Bill, 2019, and The Digital Personal Data Protection Act, 2023, is as follows: -

Table II: Juxtaposing view on the DDPB, PDPB, and the DPDP

BASIS	(DRAFT) DIGITAL PERSONAL DATA PROTECTION BILL, 2022 (DDP)	(DRAFT) PERSONAL DATA PROTECTION BILL, 2019 (PDP)	DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (DPDP)
Target sector(s)	The Digital Data Protection Bill, 2022 is more industry-targeted as compared to previous versions of itself.	The Personal Protection Bill, 2019 targets the Data Fiduciaries which includes an individual, State, Companies, any juristic entity, real estate, hospitals, and pharmaceutical companies. (19)	Considering the inefficiency of various sectoral Acts such as the Indian Penal Code, 1860; and the Protection of Children from Sexual Offences Act, 2012; the data of Indian citizens was never prioritized. Hence, comprehensive legislation dedicated specifically to the privacy of the citizens was the dire need of the country.
Regulation	The bill maintains a narrower approach since it only regulates the data protection practices of digital data which qualifies itself as personal data.	The PDP, on the other hand, has a wider approach as it covers under its ambit all the cross-border data flows, along with aspects that wouldn't necessarily qualify under the realm of personal data protection.	This act represented a major milestone in safeguarding personal data, in both, digital or non-digital form. It shall also impact the e-vendors who look after the personal and non-personal data of the citizens of the country (20).

Precise Balance	The bill follows a more nuanced approach since it takes into account both, the digital ecosystem of the country in its most nascent stage, along with the majority of new digital tech heads of the country while taking care of the international standards.	The PDP bill was drawn back by the Government board due to the realization of non-indulgence of the non-personal data in the draft bill, thus creating an imbalance for the legislations curated by the Committee.	The DPDP ACT perfectly summarizes the protection of patron's privacy while being influenced by the European Union's General Data Protection Right (GDPR). It constructively specifies eleven principles laid down as privacy guidelines.
Scope and Application	The bill does not extend to bring under its ambit the offline personal data and non-automated processing. It also removes reference to business carried on in India.	It has expanded the scope of The Draft Personal Data Protection Bill, 2018 which included the processing of personal data within and outside India for businesses offering goods and services, in India and now includes anonymized personal data.	The DPDP ACT extends its ambit to the citizens of the country along with a special focus on the library vendors and the e-vendors.
In matters of transference of personal data outside Indian territory	The classification of sensitive and critical personal data is removed under this bill. It also provides for the transference of personal data to countries as notified by the central government, according to the prescribed terms and conditions.	Transference of specific sensitive personal data may only be possible on explicit consent so provided, and no restrictions are placed on other personal data. A copy of sensitive personal data should remain in India.	The government imposes restrictions on e-vendors and libraries, prohibiting the transfer of any stored personal user data to vendors located outside the country. However, there are exceptions to this regulation, allowing the sharing of personal data for sovereign, research, and statistical purposes.

9. Global Perspective of Personal Data: In Relevance of Indian Scenario

It is contemplated that our future will be driven by data and 'Personal data is the new oil of the internet and the new currency of the digital world'. This leads to the conclusion that development taking place in every sphere of Machine Learning and Artificial Intelligence is charged and pumped by data. Everything in the world has been data-driven from calibrating and concentrating network-based, to complex mechanisms and models.

If we turn the coin the other way around, we see a new insight. The aforementioned statements indicate that privacy has been rising as an issue and newly emerging awareness regarding the privacy of data and the urgent need to curate a robust regulation mechanism revolving around the same is a quintessential pre-requisite. In the same direction, regulations curated by several countries like the General Data Protection Regulation of the European Union and the Personal Data Protection Act of 2023 of India impose new hindrances in obtaining data in required quantities.

To eradicate such hindrances, many innovation-friendly countries must introduce regulatory provisions to corroborate that personal data is duly protected and the extraction of non-personal data from personal data is practiced.

Several countries and regions are still in the mode of regulating the use of NPD while on the other hand, several countries like the European Union have already operationalized the regulation of the free flow of Non-Personal Data. India also took a step further in the same direction by introducing a 9-member expert committee to contemplate the regulation of NPD in 2019. Countries like the United Kingdom (UK) and Singapore are also in the same queue.

9.1. European Union's: General Data Protection Regulation (GDPR)

There is a preconceived notion that the EU's GDPR holds – which suggests that personal data are important, as much as all aspects of interacting with data require careful planning. GDPR has been considered the most crucial regulatory progression in information policy in a generation. It brings personal data into the enlightenment of a complex and protective regulatory regime.
The ideas consisting in the Regulation Framework do not revolve totally around the European taste, and are not something so innovative as such – but the way it has been put out is commendable. It has been more or less, albeit in weaker forms – inspired by the U.S. laws for the privacy of personal data and in Federal Trade Commission settlements with companies. (21)
The sole theme for the formulation of such a law in the European Union is that they consider the Right to Personal Data Protection a promise or a fundamental right of their citizens. Such a concept has seen an intensification of itself even when it germinated long back because, in Europe, data protection has always been seen as a separate concept from that of the 'right to privacy'.

9.2. Unique Features OF GDPR

- All privacy laws usually revolve around covered data. GDPR, on the other hand, defines 'personal data' as 'any information relating to an identified or identifiable natural person (who is also known as the data subject) as an identifiable natural person can be identified, directly or indirectly. Thus, it sums up that GDPR's concept of personal data covers much more than just personally identifiable information such as names or addresses. The role of GDPR comes into play when 'personal data is processed.
- GDPR also suggests that any organization requiring to collect any personal data should consent to the user first for the collection of data and provides for the implementation of apt technical and organizational measures to protect the personal data of EU residents.
- Larger technological companies like Google, Facebook, and Amazon have complied with the regulations and privacy laws of the GDPR and have earned a greater advantageous position in the market as compared to the competitors who haven't complied with the GPDR laws yet.
- GDPR is quite a large legislative piece with around 99 Articles in it but it can be narrowed down to 3 basic objectives–
    - To provide rules for the protection and processing of the personal data of natural persons.
    - To protect the fundamental rights of natural persons about their data.
    - To ensure that personal data can move freely within the European Union.

9.3. APPLICATION OF GDPR

9.3.1. Personal data and its processing (22)

The concept of GDPR is applied when personal data is processed. The activities inclusive of 'processing' according to GDPR are – collecting, storing, divulging, and erasure of the data. In a way, all the procedures that personal data would undergo can come under the ambit of 'processing'.
Thus, whenever an organization touches the data of an individual – irrespective of the nature of such data, be it sensitive or non-sensitive, able to directly or indirectly identify an individual, public or private, etc., it will be considered as an organizational process to undertake 'personal data within the horizon of the GDPR.

9.3.2. Actors accountable for upholding GDPR requirements (23)

The most important actors in the GDPR are

- 'Data subjects' – who are natural persons (or individuals) whose personal data is taken for processing.

- 'Controllers' – those persons who determine the processes and the means of the processing of personal data.
- 'Processors' – bodies that perform with personal data in a way on behalf of controllers.
- 'Data Protection Authorities' – entities are given the authority to protect the data of natural persons.

9.3.3. Exceptions from the application of the GDPR

- GDPR exempts data activities for 'purely personal or household activity' – but this is subject to variation in different circumstances as spying outside the house through recording cameras installed outside the house, will not count as a 'purely personal or household activity.
- No regulation of National security – the prevention of any criminal offenses or activities falls outside the scope of GDPR.

9.4. Impact Of GDPR on Various Spectrums of Technological Advancements

9.4.1. On Technological Platforms

GDPR is prognosticated to affect most technology platforms and data architectures that are solely responsible for the collection, storage, and management of the personal data of natural persons. (24) Due to the requirements of GDPR for data controllers and processors to look after personal data which would include data protection, the record of all processing activities, along with the requirements to offer the residents of the EU, vigorous privacy rights to be enjoyed. For example, the right to be forgotten, the right to access data, the right to data portability, etc. The individual has the right to ask or question or investigate the purpose and the nature of the information collected about him/her by a particular company or organization and the latter is accountable to such individuals.

Noticeable manpower and resources are required to be invested by companies to meet and comply with the requirements of GDPR. The impact of the introduction of the GDPR has had a great visible and significant impact on American and Chinese companies since a lot of companies hailing from these 2 origins practiced businesses with the EU and some companies like Huawei, a Chinese company, have also tried complying with GDPR as it appointed data protection officers. (25)

9.4.2. On Cybersecurity

Inevitable implications of GDPR on organizations' cybersecurity policies can be foreseen since it requires companies to introduce and implement reasonable and called-for data protection measures for the utmost benefit of the consumer's data and privacy against loss of data.

According to the Journal of Global Information Technology Management, 2019- GDPR has now inculcated in its requirements, a mandatory provision that requires the data controller to "notify the personal data breach to the supervisory authority without undue delay and where feasible, become aware of it, not later than 72 hours" (26). Privacy and security issues are interspersed with user trust which ultimately brings new opportunities for companies along with compliance benefits with GDPR.

9.4.3. On Emerging Technologies

Emerging technologies including artificial intelligence, blockchains, robotics, etc. have effectively resulted in boosting performance and overall productivity. Their development has now become the key to ultimately developing the economic status of a country. Stricter rules and regulations centering on such emerging technologies will lead to an unsolicited increment in the cost of developing other new technologies.

10. Inferences And Loopholes

Comparing the stance of both, the Indian rules and regulations on Non-Personal Data and the European Union's General Data Protection Regulation (GDPR) it seems that they are fit for the conditions they are applied to except for certain loopholes.

10.1. Indian Perspective

The Indian framework for the governance of NPD is still lacking behind since it has not covered the larger spectrums and the objectives of the competition of various companies/organizations working in India, trade, national security, and privacy of individuals. It is only concerned with the aspects of privacy and the protection of data risks of individuals through the Non-Personal Data framework. (27)

- It lacks the interaction of the newly formed framework with the existing laws and regulators – on the interaction of which, the nature of NPD would be transformed into more holistic.
- Promotion of cross-border data transference
- Data-anonymization and re-identification criminalization- Even when non-personal data means personal data without personally identifiable information in it, the chances of re-identification of an individual are reduced, not removed. Only 1 provision for criminalizing the re-identification of an individual is given in the existing law of the Digital Personal Data Protection Act, of 2023. Thus, it is advised to not introduce the concept of non-personal data into the same existing legislation, but instead, the provision of re-identification is used as a deterrent against it.
- Having two regulatory authorities for the same subject – data.

The principles of personal data need not be applied to non-personal data as it obstructs the economic growth of the country. The nature of personal data doesn't take up much time to get converted into intellectual property but non-personal data is also obtained through various algorithms and analytical tools used by businesses. When the flow of such data is restricted, the company's intellectual property will be questioned about the true owner of such data.

10.2. EUROPEAN UNION'S PERSPECTIVE

- The lack of assessment on controllers outside the EU is something bugging the perspective of GDPR. Since it is aimed at protecting people residing in the European Union, when their data is controlled or monitored by organizations or companies outside the EU, it becomes weak to protect the data of its natural persons. Once an outside company or organization obtains the personal data of the residents of the EU, the entity after following GDPR norms, may use the same personal information of the individuals for purposes other than for offering goods and services.
- No stricter policies or rules are made for companies not abiding by the rules of GDPR. It is optional and convenient for companies and organizations to comply with the laws of GDPR and practice their normal course with the data of people (be it private or public).
- The anonymization of the Data so collected under GDPR can be easily transferred to others and easily escape from falling under the ambit of the protection of the law.

10.3. Recommendations

10.3.1. Indian Perspective

For the Non-Personal Data Act to be a success in a country like India, the sole focus should be redirected toward a robust governance of NPD which should include the following: -

- Issues about competition – introduction of the Competition Commission of India (CCI) which is already in charge of looking at issues such as anti-competitive practices, dominance,

monopoly, market distortion, and barriers for trade which are composed of various entities, should be involved in the regulation procedures for NPD. (28)

- Localization of the data and its cross-border flow– if any intra-group scheme or any contract involving the transference of data across borders along with the consent of the data principal, is against the public policy, it should not be approved, nor implemented.
- Looking out for jurisdiction challenges to be resolved – when two separate frameworks are implemented simultaneously or moreover, incorporated into each other (that of NPD and PDP), problems regarding jurisdiction may pop up which have to be resolved through proper mechanisms and the formation of appropriate expert committees under the Digital Personal Data Protection Act of 2023.

10.3.2. European Union's Perspective

- To revert to the Court of Justice of the European Union – in matters of dispute, an authoritative and authentic source of resolution is required for which CJEU is appropriate since the law ignores the authority who would intervene in the matters of dispute on the violation of the laws inclusive of GDPR.
- Making robust mechanism to ensure personal data so collected during original activities continues to enjoy the protection of law – An ad-hoc mechanism is required to be curated to ensure that the personal data and the anonymized version of it (non-personal data) is in the safe hands even when it is used for purposes other than the one, they were collected for.
- Supervisory authorities to keep a check on the chains of data in operation – Supervision is a requirement faced by every domain of innovation to ensure its smooth functioning and prove the true nature of the problem that it was made to dissolve. Supervisory authorities will lead to a better protracted motive which will help reduce the problems of illegitimate sharing of data.

Conclusion

Both, personal and non-personal data being new concepts in India, they need to be tackled with due diligence with proper and appropriate laws in the country which remain intact and effective at the same time, as mentioned in one of the Research propositions above. Regulation of both types of data shouldn't be the sole purpose to be served as ultimately the same would go in vain since the essential and intricate purpose of protection of the data is to advocate the protection of privacy of the individuals. Just like the adoption and formation of the Constitution of the country has been inspired by various other countries and their experiences and faults, a similar spirit should be adopted for the introduction of new and innovative laws and their inception in the country along with a proficient application and implementation of the same. There are various loopholes in the Indian laws for Non-Personal Data, and thus, it should be inspired by some foreign countries and what has worked the best for them which could be taken as an inspiration to make it work for the best for India as well. Non-personal data is a good and valuable resource for innovation and developmental purposes and to restrict its outflow in the economy would ultimately hamper its true purpose as it would nevertheless lead to cost increment for the businesses and many outside/foreign businesses will have to bring changes in their procedural structures as this approach revolving around the non-personal data, is comparatively new and does not have direct repercussions.

References

1. Digital Personal Data Protection Act, 2023, S.2(h), NO. 22, Acts of Parliament, 2023 (India).

2. Hoofnagle, et al., (2019), "The European Union general data protection regulation: what it is and what it means", available at: https://www.tandfonline.com/doi/full/10.1080/13600834.2019.1573501 (accessed 16 May 2022)
3. MeiTY, (2020), "Report by the Committee of Experts on Non-Personal Data Governance Framework", available at: https://ourgovdotin.files.wordpress.com/2020/07/kris-gopalakrishnan-committee-report-on-non-personal-data-governance-framework.pdf (accessed 16 May 2022)
4. Supra Note 3.
5. Supra Note 3.
6. Supra Note 3.
7. Punj, S. (2022), "Why India needs to strengthen data protection laws without stymieing industry", available at: https://www.indiatoday.in/india-today-insight/story/why-india-needs-to-strengthen-data-protection-laws-without-stymieing-industry-2000587-2022-09-15 (accessed 20 May 2022)
8. Supreme Court of India, (2017), "Justice K.S. Puttaswamy (Retd.) & Anr. Vs. Union of India & Ors." available at: https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors#:~:text=Case%20Brief&text=The%20nine%20Judge%20Bench%20in,of%20dignity%2C%20autonomy%20and%20liberty (accessed 11 June 2022).
9. Id.
10. Heda S. and Upadhyay S. (2021), "Future of Non-Personal Data Governance in India: A Consumer Perspective", available at: https://cuts-ccier.org/pdf/policy-brief-future-of-npd-governance-in-india.pdf (accessed 11 June 2022).
11. Supra Note 3.
12. Solove D. (2014), "10 Reasons Why Privacy Matters", available at: https://teachprivacy.com/10%20reasons%20privacy%20matters (accessed 11 June 2022).
13. Verma A., "Right to Privacy", available at: https://www.studocu.com/in/document/aryabhatta-knowledge-university/btechit-btechcse/right-to-privacy-and-rti-by-aditya-verma-1/25532532# (accessed 15 June 2022).
14. Ministry of Law, Justice, and Company Affairs (2000), "The Information Technology Act, 2000", available at: https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY= (accessed 21 June 2022).
15. Id.
16. Ministry of Law, Justice, and Company Affairs (2008), "The Information Technology Act, 2008", available at: https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf (accessed 21 June 2022).
17. Supra Note 14.
18. Ministry of Electronics and Information Technology, GOI "National Data Governance Framework Policy" available at: https://www.meity.gov.in/writereaddata/files/National-Data-Governance-Framework-Policy.pdf (accessed 25 June 2022).
19. Tunggal A., (2023), "What is the Personal Data Protection Bill, 2019?", available at: https://www.upguard.com/blog/personal-data-protection-bill (accessed 25 June 2022).
20. Bareh K. C., (2023), "Reviewing the Privacy Implications of India's Digital Personal Data Protection Act, 2023", available at: https://www.researchgate.net/profile/Chanlang-Ki-Bareh/publication/ (accessed June 24 2024).
21. Id.

22. Supra Note 2.
23. Supra Note 2.
24. Supra Note 2.
25. He Li et al., (2019), "The Impact of GDPR on Global Technology Development", available at: DOI: 10.1080/1097198X.2019.1569186 (accessed 28 June 2022).
26. Id.
27. Supra Note 23.
28. Singh A. et al., (2019), "The Contours of Public Policy for Non-Personal Data Flows in India", available at: https://www.dvara.com/research/blog/2019/09/24/the-contours-of-public-policy-for-non-personal-data-flows-in-india/ (accessed 7 September 2023).