Safeguarding Personal Data in the Digital Age: Evolving Scope of Data Protection Regulations

[*]V.V.Badarinath, [**]P.Nihanth, ***V.Dakshayani
**B.A.LL.B Graduate, Dr. B. R. Ambedkar College of Law, Andhra University.*
*** B.A.LL.B Student, Dr. B.R Ambedkar College of Law, Andhra University.*
**** LLM Scholar, Dr. B.R Ambedkar College of Law, Andhra University.*

Abstract: In the digital age data privacy and data protection has been a focal point of contention all around the world irrespective of national borders while many industrialized nations have taken strides in enforcing data protection regulations the developing countries are still lagging behind in this aspect it is important for the developing to catch up and prioritize enforcing the data protection regulations at the earliest time frame possible, it is a well acknowledged fact is that relevance and importance of data is growing with each and every passing day and data is often dubbed as new oil. Till now the human race has witnessed three industrial revolutions and it is gearing up for the fourth industrial revolution based on A.I, machine learning and internet of things. During the last industrial revolution oil has been the primary source for driving growth and change in the society but this time around data is going to take up the role of oil. It is also worth noticing some striking similarities between oil and data, both oil and data are available in crude form and requires processing prior usage. Oil is controlled by few countries where as data is controlled by few organizations whose revenue is greater than GDP of many countries. More importantly data has the ability to control behavioral patterns of individuals and affect their choices. Hence, it is of utmost importance to regulate data as to how it is obtained, processed, stored, used and erased. Here's where Digital Personal Data Protection Act, 2023 herein called as DPDP Act, 2023 comes into picture. It regulates data and provides users with better control over their data. This paper critically analyses the background, provisions and challenges in regards to DPDP Act, 2023 and suggests solutions for some of its shortcomings.

Key words: Data privacy, data protection, industrialized nations, data protection regulations, oil, 4th industrial revolution, behavioral patterns, Digital Personal Data Protection Act, 2023.

I. INTRODUCTION

It is estimated that there are over 700 million internet users in India till December, 2022[1] and an obvious fact is that many users avail long list of services like internet banking, online shopping etc from the internet which also makes it imperative for the companies that provide such products and render such services to the users to collect the data of their users which will include personal data of the users in order to deliver their goods and services efficiently and effectively. The issue surfaces when the organizations that collect data does not seek the consent of the users as to what data they are collecting from the users and how they are processing, maintaining, storing, handling and disposing the same. The real problem arises when such personal data is used for exploitative purposes in an illegal manner by the companies or when there is a breach of such personal data due to security lapses in the data storage systems of the companies.

Personal data is nothing but intimate data of a living individual that can be used to identify such individual and the breach of which will lead to violation of his/her privacy. In the year 2017 the honorable Supreme Court of India has come up with a landmark judgment in K.S.Puttaswamy vs. Union of India (Aadhar case) declaring Right to privacy as a fundamental right under Article 21 of the Constitution of India. Therefore, it can be understood that unauthorized usage of one's personal data amounts to violation of right to privacy under Article 21 of the Indian Constitution. In general with the ever increasing number of internet users and the shady techniques employed by many companies for collection and exploitation of personal data there has been a demand from users, legal experts and cyber security specialists to enforce strict data protection laws. There is also a

[1] Ministry of External Affairs, Govt of India, https://indbiz.gov.in/india-had-over-700-mn-active-internet-users-by-dec-22-report/#:~:text=India%20had%20over%20700%20million,areas%2C%20with%20295%20million%20users. Visited on 22-01-2024

responsibility on the government to safeguard the rights and interests of its citizens in the cyber space.

The Supreme Court's declaration of right to privacy as a fundamental right under Article 21 of the Indian Constitution further amplified the demand from the public and responsibility of the government to enforce data protection regulations all across the country. When we consider IT Act, 2000 the law does not have specific provisions to protect the personal data of the users it was mainly brought into force to legalize, validate and enable online transactions, digital signatures, submission of documents to various government agencies and to ease electronic data storage regulations in India.[2] Considering all these issues surrounding privacy of the individuals in online space and ineffectiveness of the existing laws to deal with the same, the government thought that it would be appropriate to bring in and enforce a new law protecting personal data of the individuals in accordance with the same parliament has recently passed Digital Personal Data Protection bill of 2023 which came into force on 12th of August, 2023 but before we go into history and provisions of the new Digital Personal Data Protection Act of 2023 it is very important to have a fair idea on GDPR in order to understand the new data protection law that is being enforced in India as the law which is being enforced in India also owes its genesis to GDPR of Europe.

The European Union started to enforce a law called GDPR (General Data Protection Regulation) from 2018 in order to safeguard the rights of its citizens. GDPR is considered as the most stringent data protection regulation enforced all across the world. GDPR is the toughest privacy law and security law all over the world. It imposes many obligations on the organizations so long as they collect data from the citizens of Europe. It all started in 1950 when right to privacy was declared as a basic right in European convention of Human rights, With the technological progress that included the introduction of internet consensus was built among the members of EU in relation to data privacy and protection hence, it has passed the European data protection directive in the year 1995 establishing minimum data privacy and security standards upon which each member can frame their own laws for implementation.

In 2011, a Google user sued Google for scanning her emails without her consent in that case the European data protection authority opined that Europe needed a comprehensive approach for protecting personal data of individuals whereby work began to update 1995 directive. After many discussions and deliberations the European parliament has passed GDPR and it entered into force on 2016 while it became applicable from 2018.[3] The overview of GDPR includes and provides for data protection and privacy rights to its citizens which includes[4]

i. Right to be informed
ii. Right to access
iii. Right to rectification
iv. Right to erasure
v. Right to restrict processing
vi. Right to data profitability
vii. Right to object
viii. Rights in relation to automatic decision making and profiling.

If an organization is processing data they have to follow accountability and protection principles as outlined in Article 5.1 of Chapter 2 of GDPR which includes[5]

i. Lawfulness, fairness and transparency: Processing must be lawful, fair and transparent to the data subject
ii. Purpose limitation: Processing of data must be for legitimate purposes specified explicitly to be data subject
iii. Data minimization: Organizations that process the data must collect minimum and quintessential data that is required for the organizations from the data subject
iv. Storage limitation: Once the data requirement is fulfilled such data must be deleted immediately
v. Integrity and confidentiality: Reasonable security measures like encryption etc must be taken while processing and storing data to avoid data breaches

[2] Data protection and data privacy laws in India, https://blog.ipleaders.in/data-protection-laws-in-india-2/#Objectives_of_the_Act, visited on 26-01-2024.
[3] What is GDPR, the EU's new data protection law?, GDPR.EU, https://gdpr.eu/what-is-gdpr/ visited on 26-01-2024.
[4] What is GDPR, the EU's new data protection law?, GDPR.EU, https://gdpr.eu/what-is-gdpr/ visited on 26-01-2024.
[5] What is GDPR, the EU's new data protection law?, GDPR.EU, https://gdpr.eu/what-is-gdpr/ visited on 26-01-2024.

vi. Accountability: The data controller is responsible for compliance of GDPR

Also, an individual/organization can be allowed to process data if[6]

i. Data subject gave unambiguous, unequivocal and specific consent
ii. When processing is necessary to execute or prepare to enter into a contract where data subject is a party
iii. Data processing is essential to comply with a legal obligation (court orders for instance)
iv. When processing of data is required to save someone's life
v. Data processing is necessary to perform a task in public interest
vi. Data processing in view of a legitimate interest however it is to be noted that fundamental rights and freedom of the data subject can override any such interest especially in case of child data

In this context, the terms "data subject," "data controller," and "data processor" refer to the individuals whose data is processed, the latter of whom processes the data on the controller's behalf. It is worth noting that GDPR is applicable to organizations whether or not based in EU when the processed data belongs to EU citizen also, GDPR is only applicable to professional and commercial activity and not otherwise.[7] In order to comply with the provisions of GDPR Data protection officers are appointed they are required to understand how GDPR applies for a specific organization, advising people in the organization regarding their responsibilities, conducting data protection training, audits and monitoring compliance, not to mention serving as a liasionary officers with regulators.[8]

Coming back to the Indian context the need for a data protection law truly emerged after the judgment of the Supreme Court in the case of KS Puttaswamy vs. UOI where Right to privacy has been declared as a fundamental right under Article 21 of the Indian Constitution. Soon after the judgment of Apex court a committee was formed under retired justice BN Sri Krishna by central government to draft a new data protection law accordingly 1st draft was prepared by July, 2018 after taking feedback from various stakeholders it was sent to joint parliamentary committee in 2019 that later suggested atleast 80 changes. The bill was re-introduced in the parliament after complying with many recommendations of joint parliamentary committee to be again withdrawn by the government on August, 2022. Later in November, 2022 a new draft was prepared which was approved by the union cabinet on 5th July, 2023 and passed by both houses of the parliament, it came into force on 11th August, 2023 after obtaining the assent of the President.

The Digital Data Protection Act of 2023 is based on basic principles that include,

i. Collection and usage of data must be done in compliance with DPDP Act, 2023
ii. Nobody shall collect data without consent of the data principal
iii. Data which is collected can only be used for the purpose for which it is collected
iv. No platform can store data beyond the duration than needed to deliver the product or service
v. One can only collect minimum amount of data that is quintessential for the delivery of goods and services
vi. Data fiduciaries are obliged to store data with necessary security measures in order to avoid breach.
vii. Data fiduciaries are mandated to report in case of a breach.

Here data principal is the one who generates data while data fiduciary is an individual or entity who stores and process the data. DPDP Act, 2023 classifies data into 4 categories including,

i. Digital data
ii. Personal data
iii. Non-Personal data
iv. Critical data

The information or statistics kept in electronic devices are referred to in this context as digital data. Information about a specific person who may be recognized from or via such information is referred to

[6]What is GDPR, the EU's new data protection law?, GDPR.EU, https://gdpr.eu/what-is-gdpr/ visited on 26-01-2024.

[7] Does the GDPR apply to companies outside of the EU?, GDPR.EU, https://gdpr.eu/companies-outside-of-europe/ visited on 26-01-2024.

[8]What is GDPR, the EU's new data protection law?, GDPR.EU, https://gdpr.eu/what-is-gdpr/ visited on 26-01-2024.

as personal data. Non-Personal data means information generated by an individual which does not come under personal data for instance traffic data shown by GPS while information related to critical infrastructure of our country is referred to as Critical data. Some of noteworthy facts about DPDP Act, 2023 is that DPDP Act, 2023 does not cover non digitized and nonpersonal data. DPDP Act also mandates that the data which is generated in India must be stored in India and should be dealt with appropriate laws of India.

II. FEATURES OF DPDP ACT, 2023

DPDP Act, 2023 covers the handling of digital personal data in India that is either digitally collected offline or digitally gathered online. If personal data is processed outside of India in order to provide products or services in India, this will also be covered. Data fiduciary must take consent from data principal to process personal data such consent can be revoked by data principal subsequently if in case the data principal is a minor consent in such cases has to be given by his/her parents.[9] The Data Principal possesses several rights regarding their personal data. They can request information about how their personal data is being processed by the data fiduciary. Additionally, they have the right to demand corrections or erasure of their data when necessary. The Data Principal can also appoint a nominee for their personal data. Furthermore, provisions have been made for a Grievance Redressal Officer to address any complaints or issues related to data processing.

The Data Principal has certain duties to uphold. They must not provide false data when giving consent, and they can be fined up to 10,000 rupees for filing a false complaint. Meanwhile, Data Fiduciaries have specific obligations, including taking necessary security measures to prevent data breaches and ensuring the accuracy of the data collected. In the event of a data breach, the data fiduciary must notify the Data Principal and the Data Protection Board of India. Additionally, any organization that receives data from a data fiduciary must erase the data after its use. However, an exemption exists for the Government of India, which means an individual cannot request the erasure of data in this context.

The act permits the transfer of personal data to countries outside India, except those specifically restricted by the Central Government through notification. However, there are certain exceptions. During an investigation by the Government of India, neither the Data Principal nor the Data Fiduciary can claim protection under the act. Additionally, the Government of India can exempt any provisions of the act in the interests of state security, public order, as well as for archival, research, and statistical purposes. It is mandated under the act that appeals should go to Telecom Dispute settlement and appellate tribunal. Fines up to 250 crore rupees can be levied on data fiduciaries in case of breach while fine up to 200 crore rupees can be levied in child related matters. Data Protection Board of India has to be established by Government of India under this act to oversee the implementation of the act, levy penalties on data principal and data fiduciary in case of violations of various provisions of the act. It also helps data fiduciaries to take curative steps in case of breach.

III. CHALLENGES OF DIGITAL DATA PROTECTION ACT

The first issue is with the appointment of chairperson and members of the Data Protection Board, the power to appoint the chairperson and members of Data Protection Board completely vests with the Central Government this raises the question of independence and integrity of the board. The fact that the central government exercises too much control over the board and short tenure of the chairperson and members combined with provision of re-appointment casts serious questions on the independence of the board especially in adjudicating the disputes that may arise especially those against the government. The next issue is regarding wide sweeping exemptions provided to Government of India and different government agencies the fact that government of India can be exempted from the provisions of DPDP Act, 2023 especially on the grounds of security of the state and public order may defeat the purpose of the law which has been enacted to protect the privacy of data principals but the wide scope of public order and security of the state confers ample powers upon the government to intrude the privacy of an individual

[9]The Digital Personal Data Protection Bill, 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023, visited on 26-01-2024.

violating right to privacy under Article 21 of the Indian Constitution.

Some other challenges include no right of erasure in case of data collected by the government. Also, there is no right to be forgotten for data principal which has also been recommended by the joint parliamentary committee previously. It should be noted that there is no restriction on data transfer outside India except to those countries notified by the central government this may not ensure adequate evaluation of data protection standards in the countries where such personal data has been transferred. There is also an issue where with the introduction of DPDP Act, 2023 the IT Act, 2000 has been amended and section 43(a) of the said act has been omitted it is problematic because section 43(a) of IT Act, 2000 which runs as "If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, - (a) accesses or secures access to such computer, computer system or computer network; he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected"[10]. Basically, the above section provides for compensation up to 1 crore rupees to the data principal in case of negligence on part of the company to protect data. As the above section has been completely omitted an individual cannot seek compensation from the company in case of data breach caused due to negligence in the handling of data by the company.

Lastly, one more important challenge is the compatibility with the RTI Act, 2005. When we look at Section 8(1) (j) that runs as "information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information: Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person"[11] It basically says that personal information cannot be disclosed unless the authorities are satisfied that there is significant public interest which justifies such disclosure.

Meanwhile, when we take a look at Section 44(3) of DPDP Act, 2023 which runs as "In section 8 of the Right to Information Act, 2005, in sub-section (1), for clause (j), the following clause shall be substituted, namely:- (j) information which relates to personal information"[12] it can be understood that DPDP Act, 2023 further narrows down the scope of section 8(1) (j) because of which RTI authorities will get a new ground to deny the information to public essentially undermining RTI Act. For instance, when a person file an RTI application seeking details of properties owned by public officer sensing corruption considering the public interest the RTI authorities might have disclosed information if they are satisfied but now RTI authorities can say that information the applicant is seeking is personal information which is protected under DPDP Act, 2023 and deny the same. DPDP Act, 2023 in this case is prioritizing privacy over significant public interest.

IV. CONCLUSION

With the consistent raise in the instances of data breaches every year, illegal exploitation of personal data by many organizations and inability of existing laws to deal with data protection the Digital Personal Data Protection Act, 2023 is a step forward in the right direction. In recent years, the landscape of digital privacy in India has undergone significant transformation, culminating in the enactment of the Digital Personal Data Protection Act (DPDP Act) of 2023. This development is particularly noteworthy given the surge in internet usage, which has surpassed 700 million users as of December 2022. Consequently, an increasing number of individuals are engaging in various online services, such as internet banking and e-commerce, which necessitate the collection and processing of personal data by companies. However, this practice raises profound ethical and legal concerns, especially when organizations fail to obtain informed consent from users regarding the nature and

[10]THE INFORMATION TECHNOLOGY ACT, 2000 , https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY, visited on 26-01-2024.

[11] THE RIGHT TO INFORMATION ACT, 2005, https://rti.gov.in/rti-act.pdf visited on 26-01-2024.

[12] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf visited on 26-01-2024.

extent of data collection, as well as the methods employed in its processing and storage.

The critical concern is not just the collection of personal data but its potential misuse, which can severely violate privacy rights. The Supreme Court's 2017 ruling in K.S. Puttaswamy vs. Union of India affirmed the right to privacy as fundamental under Article 21, escalating public demands for robust data protection laws and urging the government to protect citizens' rights in the digital realm. Historically, the existing legal framework in India, primarily encapsulated within the Information Technology Act of 2000, was insufficient for addressing the nuances of personal data protection. Although the IT Act laid the groundwork for legalizing online transactions and digital signatures, it lacked explicit provisions for the protection of personal data. Consequently, following the Supreme Court's declaration of privacy as a fundamental right, the government-initiated efforts to draft a new data protection law. This led to the establishment of a committee under retired Justice B.N. Srikrishna, which proposed the first draft of the Personal Data Protection Bill in 2018. However, this draft underwent multiple revisions and extensive discussions in Parliament, reflecting the complexity and urgency surrounding the issue.

The DPDP Act of 2023, which came into force on August 11, 2023, introduces several key principles aimed at enhancing data protection in India. Among these is the requirement for explicit consent from individuals termed "data principals" before any collection or processing of their personal data can occur. Furthermore, the Act mandates that data fiduciaries (entities that handle personal data) can only collect data for specific, legitimate purposes and must refrain from retaining it longer than necessary for those purposes. Such provisions are designed to promote transparency, accountability, and ethical data practices. In this context, the DPDP Act is influenced by the General Data Protection Regulation (GDPR) implemented by the European Union in 2018. The GDPR is widely regarded as one of the most stringent data protection frameworks globally, providing comprehensive rights to individuals concerning their personal data. These rights include the right to be informed, the right to access, the right to rectification, and the right to erasure, among others. The introduction of similar rights within the DPDP Act reflects India's commitment to aligning its data protection standards with international norms.

Nevertheless, the DPDP Act is not without its challenges and criticisms. A significant concern is the degree of control that the central government holds over the Data Protection Board, which is responsible for overseeing the implementation of the Act. The government’s power to appoint members of the Board raises questions about its independence, particularly in adjudicating disputes involving government agencies. The potential for governmental overreach in matters of data privacy is particularly alarming given the sweeping exemptions provided to the government under the Act. These exemptions allow the government to bypass certain provisions in the name of public order or national security, potentially undermining the very purpose of the law. Another critical issue pertains to the lack of certain rights for data principals, particularly concerning government-collected data. The absence of a right to erasure data held by government entities poses significant challenges to individual privacy. Furthermore, the Act does not explicitly grant a "right to be forgotten," which has become a vital aspect of data protection in various jurisdictions worldwide. These limitations could hinder the Act’s effectiveness and its ability to genuinely protect the privacy of individuals.

Moreover, the interplay between the DPDP Act and other existing laws, such as the Right to Information (RTI) Act, requires careful consideration. The amendments introduced by the DPDP Act may inadvertently narrow the scope of the RTI Act, thereby limiting public access to information that serves the public interest. This tension underscores the necessity of striking a balance between privacy rights and the imperative of transparency in governance. As India continues to advance in the digital era, the implementation of the DPDP Act will be crucial in shaping the relationship between individuals and organizations that handle personal data. While the Act presents an essential framework for protecting digital privacy, its success will depend on the government's commitment to ensuring its effective enforcement and addressing the challenges that arise in practice. Policymakers must engage with various stakeholders including legal experts, civil society, and the tech industry to foster a comprehensive understanding of data protection that upholds individual rights while enabling innovation and growth.