INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

CRITICALLY ANALYSING THE DIGITAL PERSONAL DATA PROTECTION ACT IN LIGHT OF THE GDPR FRAMEWORK

AUTHORED BY - SUNIDHI TYAGI,
Final Year Student, LLB (Hons.), Amity Law School, Noida
CO-AUTHOR - SHAILJA KHOSLA,
Assistant Professor, Amity Law School, Noida

"Data is the new Oil"[1],the Digital Personal Data Protection Bill got the approval of both the houses of the parliament and has come into force with the new arrangements which will ensure transparency, efficiency and will help in data usage by lawful means. With the 4th Stage of Industrial Revolution, national security and privacy have become the primary concerns for all and data is becoming the defining paradigm for nations across the globe. As per the National Economic Survey, India will be a 5 Trillion Economy and ⅕ of it will be through the digital sector, by means of selling public data.[2]

Prior to this, there was no specific data protection law in India and hence there was no body governing the relationship between the Government, Intermediaries and the Individuals.From 2011 - 2014, there were talks on making a data protection law and even the Justice AP Shah Committee[3] was formulated to look into the same. The issue of privacy and its significance in the developing economies came into light with the Judgement of Gobind vs State of Madhya Pradesh (1975)[4] which provided a watershed area to Right to Privacy and observed that it is enshrined under Article 21 of the Indian Constitution[5] after the opposing judgements in the earlier precedents set in M P Sharma vs Satish Chandra in 1954[6] and

1 .REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019 https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf

2 'India's Trillion-Dollar Digital economy', report by the Government of India's Ministry for Electronics and Information Technology (MEITY)

3 Committee of Experts under the Chairmanship of Justice B N Srikrishna, "Report of the Committee of Experts under the Chairmanship of Justice B N Srikrishna," Committee Report (India: Ministry of Electronics & Information Technology, Government of India, July 27, 2018), https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf. See Office Memorandum constituting the Committee provided in Annexure A of the report

4 1975 AIR 1378, 1975 SCR (3) 946

5 "Justice KS Puttaswamy and Another Vs. Union of India and Ors," 10 SCC 1, Supreme Court of India, 2017, https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017. pdf.

6 1954 AIR 300, 1954 SCR 1077

 ISSN: 2582-6433

Kharak Singh vs State of Uttar Pradesh in 1963[7]. Justice KS Puttaswamy Judgement of 2017[8], confirmed the Right to Privacy as a Fundamental right, making it an intrinsic part of Article 21 of the Constitution. Even the Ministry of Electronics and Information Technology, through the B N Srikrishna Committee in 2017 reiterated the same. The focus has now been shifted from Physical and Bodily Privacy to Data and Intellectual Privacy.

The Committee of Experts on a Data Protection Framework for India submitted its report called - A Free and Fair Digital Economy Protecting Privacy, Empowering Indians Committee of Experts under the Chairmanship of Justice B.N. Srikrishna in 2018.[9]

The Committee observed[10] that the relationship between the individual and the service provider must be viewed as a fiduciary relationship. It also suggested that to prevent abuse of power by service providers, the law should establish their basic obligations. Defined personal data to include data from which an individual may be identified or identifiable, either directly or indirectly. The Committee sought to distinguish personal data protection from the protection of sensitive personal data, since its processing could result in greater harm to the individual.

In order to protect individuals' data privacy, the Committee proposed a two-pronged approach. First, they stressed that consent should generally be required before using someone's personal data. However, they acknowledged there might be situations whereprocessing data is necessary without consent. These exceptions include circumstances where the government needs information to deliver social welfare programs, when a court order mandates data access within India, when urgent action is necessary, or under specific conditions within employment contracts. Additionally, the Committee recommendedestablishing three key data subject rights: the right to access and correct one's own data, the right to object to data processing, and the "right to be forgotten" which allows individuals to request data deletion in certain situations. To ensure these rights are upheld, the Committee emphasized the importance of creating a regulatory body specifically for data protection.They also recognized that existing laws related to data collection and processing might still

[7] 1963 AIR 1295, 1964 SCR (1) 332
[8] (2017) 10 SCC 1, AIR 2017 SC 4161
[9] WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA
https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf
[10] Report Summary on A Free and Fair Digital Economy https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy

 ISSN: 2582-6433

be relevant and should be considered within the overall data protection framework.

As a consequence of this, the Personal Data Protection Bill was put forward in the house of parliament in 2019[11], but the provisions of the bill sparked controversy and many amendments were suggested to the same. Which is why the bill was completely withdrawn and an all new fresh bill was tabled in the parliament in 2023[12], which finally got an approvalof both the houses and the assent of the President. The 7 Principles which were laid down when this bill was passed included Usage of data by Organisations in a lawful manner, Personal data, solely being used for the purpose for which it is collected, Data Minimisation, Data Accuracy, Personal Data, not be be stored perpetually, by default, Reasonable Safeguards and a Person Authority who decides the means of processing personal data - accountable for the same.

The preamble of the Act[13] outlines its purpose to regulate the handling of digital personal datain a way that respects both individuals' right to safeguard their personal information and the necessity to process such data for legal reasons, along with related matters. In Section 2(x), processing concerning personal data is defined as a fully or partially automated set of actions performed on digital personal data. This includes operations like gathering, recording, arranging, organising, storing, modifying, retrieving, utilising, aligning, combining, categorising, sharing, disclosing through transmission, spreading, or making accessible, restricting, deleting, or annihilating.

According to Section 2(n) digital personal data means personal data in digital form and personal data according to Section 2(t) means any data about an individual who is identifiableby or in relation to such data wherein data as per Section 2(h) means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication,interpretation or processing by human beings or by automated means. The ambit of lawful purposes can be understood by looking at Section 2(d) of the act which defines certain legitimate uses as the uses referred to in Section 7. However, the exact extent of what

11 THE PERSONAL DATA PROTECTION BILL, 2019 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf 12 The Digital Personal Data Protection Bill, 2023 https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
13 THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

 ISSN: 2582-6433

constitutes a "lawful purpose" will become clearer as the legislation is put into practice by the state to process personal data as it deems appropriate.

The terms Data Principals[14] and Data Fiduciaries[15] are defined under the Act, Data Principals being the users of the internet services, individual to whom the personal data relates and where such individual is a child, includes the parents or lawful guardian of such a child or a person with disability, includes her lawful guardian, acting on her behalf whereas the Data Fiduciaries being the intermediaries, may be private or government entities - means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

The Data Principals are entitled to the following rights[16] -

Right to Consent for the usage of data of data principals by the fiduciaries have beenprovided under the act, for this the data principals also have the right to know for what purpose and in what manner the data is being used.

Right to withdraw consent, the data principals must also be informed about this right of theirs with the notice and such notice shall be made accessible in all the languages specified in 8th Schedule of the constitution.

Right to Deletion/ Right to Erasure, the right to be forgotten is also a part of right to life and personal liberty under Article 21 of the Constitution and hence the user at any time can request for deletion or erasure of their personal data that is present online, in order to best suittheir personal interests.

Right to request Summary of the data that belongs to the users, Right to be Informed about where the data is being used, Right to collect the data from the fiduciaries, Right to Nominateanother trustworthy in case of death of the user whose data is in question, Right to Access thedata, Right to Rectification/Addition/Omission of data are many such privileges given to the data principals with the aim to empower them. Duties of Data Principals have also been defined - Penalty for false or frivolous Grievance or Complaint amounting to Rs. 10,000.

A very progressive step taken by this act, the parental consent will be required for Collection of data of personal data of children[17] and for this the individual who is below the age of 18

14 Section 2(j) of the Digital Personal Data Protection Act, 2023 15 Section 2(i) of the Digital Personal Data Protection Act, 2023 16 Chapter 3, Digital Personal Data Protection Act, 2023
17 Section 9, Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

will be considered as a child.[18] This has been done with a view to keep the children away from the malicious content which circulates online and affect their mental well being in their budding stages.

There is also a mandatory requirement of GOI's permission in case of Cross Border Transfersof Data,[19] that is if the data processing is in connection with the goods and services being offered in India. The act also provides for creation of a list of countries with whom the personal data cannot be shared or transferred. This negative list of countries has been created by keeping in mind the data protection laws of other nations and how secure the data of Indian citizens in other countries is.

Jurisdiction is closely linked to the sovereign equality and territorial sovereignty of states[20]. The General Data Protection Regulation (GDPR)[21] breaks new ground with its application beyond national borders. While international law, rooted in the idea of exclusive state sovereignty according to the Westphalian concept, typically limits a state's jurisdiction to its own territory and permits extraterritorial application of human rights only in exceptional circumstances, GDPR introduces the domestic-market principle, notably in Article 3(2) GDPR. This principle places obligations on data processors or controllers located outside the European Union (EU) if they offer goods or services to individuals within the EU or monitor the behaviour of EU residents.

The general principle in international law is that a state is typically unable to assert jurisdiction with effects beyond its own territory unless there is a specific rule allowing for it. Despite numerous attempts to classify cyberspace as a global common, it is important to note that cyberspace possesses a distinctive nature and is not completely separate from a state's exercise of jurisdiction. The passive personality principle adds a layer of complexity. In the context of the GDPR, this means that any company providing services to an individual withinthe EU must comply with the GDPR, even if it lacks any other substantial connection to the

18 Children and Consent under the Data Protection Act: A Study in Evolution https://corporate.cyrilamarchandblogs.com/2023/08/children-and-consent-under-the-data-protection-act-a-study-in-evolution/
19 Section 16, Digital Personal Data Protection Act, 2023
20 Art. 2 (1) Charter of the United Nations
21 European Commission, "2018 Reform of EU Data Protection Rules," Text, European Commission, accessed March 7, 2019, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

 ISSN: 2582-6433

EU. As a result, the passive personality principle leads to outcomes that have effects beyond national borders. The principle of passive personality allows a country to exercise jurisdiction over an act committed by an individual outside its territory because the victim is one of that country's nationals. This happens when personal data is collected, disclosed, shared or processed in India - irrespective of where the data fiduciary is incorporated or where any subsequent processing takes place. This is based on the principle of territoriality and passive personality.

The act also provides for Data Processors for processing the data of Data Principals and Data Fiduciaries, a provision of a Data Protection Officer[22], who will be responsible for deleting and modifying the collected data. Regular Data Audits, Data Protection Impact Assessments and post of consent managers.

Data Minimisation, Data Accuracy, Data Localisation and Data Protection Authorities are many such reasonable safeguards which will help in protecting the data of citizens of the country. This basically means that the data will only be collected for specific intended purposes and no unnecessary processing of data will take place, along with this stringent security measures will be imposed in case of any unauthorised use or breach of data.

Exemptions are also provided to Data Fiduciaries for collecting data on the grounds of Research, Archiving, Statistical Purposes[23], Security and Public Order.

It is an obligation of the data fiduciaries to make use of reasonable security measures in orderto prevent the data breach of the data that belongs to the data Principals so that no third party can access the data and use it for their own benefit. And in case any such breach occurs it is a responsibility of the data fiduciary to inform the data principal along with the Data Protection Board about the same.

The Government of India, in the interest of Sovereignty, Integrity and Security of India - mayask for disclosing the personal data of individuals. This may also be extended in case of Medical Emergencies, Epidemics Disasters - provide data and even the intermediaries are involved in the process.

A Grievance Redressal and a Dispute Resolution Mechanism will be operable through the Data Protection Board which will be an adjudicatory and not a regulatory authority. The

22 Section 10(2)(a), Digital Personal Data Protection Act, 2023
23 Section 17(2)(b), Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

tenure of the DPB will be 2 years. The appeal for the decision of the board will go to the Telecom Disputes Settlement and Appellate Tribunal. Penalty for breach, starts from 5 Croresand may extend to 250 Crores[24].

Amendments are suggested to other acts in order to comply with the provisions of the Digital Personal Data Protection Act -
Section 8(1)(j) of the Right to Information Act[25] has been amended by which, informationcan be withheld by calling it Personal data or information of public officers and ministers.But according to the provisions of the Right to Information Act, 2005, if there is a clash between the two laws, the public interest will prevail.

This act will help in replacing yet diluting the provisions of the IT (Reasonable Security Practices, Procedures and Sensitive Personal Data or Information) Rules, 2011. Information Technology (Reasonable Security Practices & Procedures and Sensitive Personal Data or Information) Rules, 2011 - Applies on body corporates and persons located in India only, it also involves sensitive personal data like passwords, credit card and debit card information, biometric information which is required for authentication and other physical physiological and mental health data.

Section 43A of the Information Technology Act[26] will be amended in a way that no compensation will be provided by the data fiduciaries to the data principals in case of failure to protect data and the data principals will only be entitled to the Judicial Compensation, which will be decided by the competent court on the basis of the merits of the case.

24 Section 33(1), Digital Personal Data Protection Act, 2023
25 Section 8(1)(j) in The Right To Information Act, 2005 - information which relates to personal information the disclosure of which has not 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.
26 Section 43A Compensation for failure to protect data - Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

 ISSN: 2582-6433

Many amendments have been made to the Information Technology Act, 2000[27] provisions as to regulating intermediaries, digital media and OTT platforms, appointment of Chief Compliance Officer, Nodal contact person and Grievance Officer, the embodiment of CERT-in (Computer Emergency Response Team - India) for dealing with cyber security threat incidents have been included. Alongside this, The IT (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021 were also introduced in order to minimise the usage ofthe Safe Harbour Clause by big tech. Giants. Now, the government is even planning to replace this with the Digital India Bill which will be based on the UNCITRAL Model which will be better equipped to tackle cyber-crimes and digital landscape.

The DPDP Act is modelled on the GDPR, the Data Subjects and Data Controllers[28] of the GDPR are Data Principals and Data Fiduciaries of DPDP Act respectively.

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law[29]. Whereas the DPDP Act apply to the processing of digital personal data within the territory of India where the personal data is collected— (i) in digital form; or (ii) in non-digital form and digitised subsequently; also apply to processing of digitalpersonal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India[30].

27 "The Information Technology Act, 2000," Government of India, June 9, 2000, https://meity.gov.in/writereaddata/files/The%20Information%20Technology%20 Act%2C%202000%283%29.pdf.
28 Article 4 of General Data Protection Regulation
29 Article 3 Territorial scope, General Data Protection Regulation
30 Section 3 Application of Act, Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

Under GDPR processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent, processing is necessary for the performance of a contract, processing is necessary for compliance with a legal obligation, processing is necessary in order to protect the vital interests of the data subject, processing is necessary for the performance of a task carried out in the public interest, processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party[31]. Whereas under DPDP Act a Data Fiduciary may process personal data of a Data Principal for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, for the State and any of its instrumentalities to provide orissue to the Data Principal such subsidy, benefit, service, certificate, licence or permit, in the interest of sovereignty and integrity of India or security of the State, for fulfilling anyobligation under any law for the time being in force in India on any person to disclose any information to the State, for compliance with any judgement or decree or order issued under any law, for responding to a medical emergency, for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health, for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order[32].

The Digital Personal Data Protection Act, 2023 does not distinguish between personal and sensitive personal data/critical personal data. Sensitive personal data includes passwords, financial data, biometric data, genetic data, caste, religious or political beliefs, or any other category of data specified by the Authority. Additionally, fiduciaries are required to institute appropriate mechanisms for age verification and parental consent when processing sensitive personal data of children. Whereas, all personal data including racial, political, religious, trade union membership, genetic, biometric, sexual orientation, and health details of individuals from the EU falls under the GDPR's sensitive data list.

According to GDPR, organisations can rely on six different legal bases to justify the collection and processing of personal data. The GDPR imposes six data protection principles on controllers and processors - lawfulness, fairness and transparency, purpose limitation, dataminimization, accuracy, storage limitation and integrity and confidentiality. In addition,

31 Article 6 Lawfulness of processing, General Data Protection Regulation
32 Section 7 Certain legitimate uses, Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

controllers and processors must also comply with the principle of accountability[33]. However, India's DPDP Act only lists two legal bases: Consent and Legitimate Use[34].

India's Data Protection and Privacy (DPDP) Act enforces stricter requirements for notifying data breaches. Under this act, data fiduciaries are obligated to inform both the Data ProtectionBoard and the Data Principals about any breaches. In contrast, the GDPR mandates breach notification only if there is a potential risk to the rights and freedoms of data subjects.

While the GDPR introduces the right to data portability and the right to object to personal data processing, the DPDP Act does not encompass these rights. Instead, it offers two other rights – the right to grievance redressal and the right to appoint a nominee.

The GDPR imposes obligations like maintaining records of processing activities and practising data minimization, which are not addressed in India's DPDP Act. Additionally, the GDPR defines a child as someone below 16 years of age (or even 13 in some countries), whereas the DPDP Act defines a child as someone below 18 years of age. The GDPR allows data processing to the extent of consent provided by parents or guardians, while the DPDP Act permits processing of all types of data.
It's important to note that the GDPR doesn't regulate non-personal or anonymous data,whereas the DPDP Act may allow access to such data.

Under the DPDP Act, data fiduciaries must ensure that any transfer of personal data outside India adheres to adequate safeguards, as approved by the Government of India. It alsorequires explicit consent from data principals before transferring their sensitive personal data.Conversely, the GDPR prohibits the transfer of personal data outside the EU or EEA unless the recipient country ensures an adequate level of protection, or appropriate safeguards are in place.

Both the DPDP Act and the GDPR mandate obtaining consent from data principals before processing their personal data. They also require providing notice about the purpose, nature, and categories of personal data being collected, as well as other related information.

33 Article 5 Principles relating to processing of personal data, General Data Protection Regulation
34 Section 4 Grounds for processing personal data, Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

In terms of enforcement, the DPDP Act establishes a Data Protection Board[35] with the authority to take various measures in response to a personal data breach. The GDPR establishes the European Data Protection Board (EDPB)[36] to ensure consistent application of the GDPR across the EU.

Penalties for non-compliance differ, with the DPDP Act ranging from INR 10,000 to INR 250 Crores, and the GDPR prescribing fines up to EUR 20 million or 4% of global annual turnover. Both laws have exemptions, such as for national security, legal proceedings, research, and archiving. The GDPR also exempts purely personal or household activities from its provisions.

The General Data Protection Regulation (GDPR) does not categorise data controllers anddoes not recognize the concept of consent managers. In contrast, the Data Protection and Privacy Act (DPDP) of 2023 in India introduces a classification of data fiduciaries, distinguishing significant data fiduciaries[37] based on factors like the volume and nature of data they collect. This classification entails additional obligations for the identified significant data fiduciaries[38]. Moreover, the DPDP Act establishes the role of a consent manager[39] who isregistered with the Data Protection Board, serving as a central contact point for data principals to manage their consents through accessible platforms.

In terms of cross-border transfer of personal data, the GDPR prohibits such transfers outside the EU or EEA unless the recipient country ensures an adequate level of data protection, or appropriate safeguards like standard contractual clauses, binding corporate rules, or other mechanisms approved by the European Commission are in place. Data subjects also have the right to obtain a copy of their personal data being transferred. On the other hand, the DPDP Act mandates data fiduciaries in India to ensure that any transfer of personal data outside the country[40] adheres to adequate safeguards, as determined by the Government of India. Additionally, explicit consent from data principals is required before transferring their sensitive personal data outside India.

35 Chapter 5, Digital Personal Data Protection Act, 2023
36 Section 3, Article 68 General Data Protection Regulation
37 Section 2(z), Digital Personal Data Protection Act, 2023
38 Section 10, Digital Personal Data Protection Act, 2023
39 Section 6(8), Digital Personal Data Protection Act, 2023
40 Chapter 4, Digital Personal Data Protection Act, 2023

 ISSN: 2582-6433

Although the DPDP Act shares a basic structure with global laws like the GDPR, it has unique features, including more restricted grounds of processing, broad exemptions for government entities, regulatory powers for the government to specify and exempt fiduciaries, no predefined protection for special data categories, and the unusual inclusion of government powers to request and block access to information.

This is an important act as it includes many provisions that did not exist before and had no regulatory mechanism regarding the same. The Act has taken inspiration from the EU's - General Data Protection Regulation of 2016, USA's - Open Banking Data Sharing Framework, EU on one hand follows a Comprehensive Data Protection Regime whereas the USA follows a Sectoral Approach.[41] China on the other hand has the Personal Information Protection Law and the Data Security Law, which provides the highest level of security measures attached to it. The data protection laws abroad focus on a more comprehensive approach towards protecting the data whereas India's law has a sectoral focus wherein it involves combination of policies and measures being developed in order to enhance and advance the level of protection in key domains. There are 71% countries across the globe with a Data Protection and Privacy Legislation[42] - Thailand's Personal Data Protection Act, Swiss Revised Federal Act on Data Protection, Bahrain's Personal Data Protection Law, Australian Privacy Act, Hong Kong Personal Data (Privacy) Ordinance, Singapore's Personal Data Protection Act, Irish Data Protection Act, Qatar's Data Protection Law, Saudi Arabia's Personal Data Protection Law to name a few, and 9% with a draft legislation on the same.

Almost 65% of the population online is below 35 years of age[43] and hence verifiable parental consent along with strict cyber security regulations is the need of the hour. For this, a comprehensive approach in lieu of a mere sectoral approach must be adopted by the nations across the globe before it becomes a global threat. Since technology is an enabler and not an inhibitor, the decision to enhance the world with technological advancements without causing harm to society lies in the hands of mankind. There is a need for Data Empowerment and

41 https://dig.watch/topics/privacy-and-data-protection
42 UNCTAD Data Protection and Privacy Legislation Worldwide https://unctad.org/page/data-protection-and-privacy-legislation-worldwide
43 https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/

 ISSN: 2582-6433

Protection Architecture, Data sovereignty and Data localisation for which India already has a India Data Management Office[44].

Lately, cases of data breach and leak such as the AIIMS medical records being hacked for accessing the medical history and records of the patients, and the data of patients registered on the CoWIN portal being stolen through Telegram were dealt with with the help ofCERTin, this can all be rectified with a stringent data protection law such as this one since this is the data of the public, the citizens of the country and thus it has to be protected for safeguarding their interests. This act will not only strengthen the goodwill and help in risk assessment of organisations but also assist in building a transparent and a sustainable organisation.

With the growing influence of technology and AI being the 4th stage of revolution platforms such as Chat GPT, cyber security and identity theft is one of the major challenges that this century has to face. With the emergence of AI, there is an urgent need for an international framework for data governance and privacy regulations for cross border data flows as it will aid in strengthening *global cybersecurity defenses.*

"Invention of AI is more revolutionary than the invention of fire"[45] - This is the statement by the CEO of one of the most powerful companies in the world, Google.
AI applications are widely used in the healthcare sector for disease mapping and prediction, agriculture industry, gaming sites, social media platforms, E-commerce industry as there are many benefits arising out of it such as automation, precision, durability, accuracy, efficiency, making life easy etc. AI involves a very high cost which will lead to inequality in the society and will give rise to a capitalist society where the rich will become richer and the poor, poorer. There is a possibility of bias and discrimination attached to AI applications due to the mindset and perspective of its maker or creator which will amplify with time. Lack of regulation and supervision will lead to accelerated hacking which was lately witnessed when

44 India Data Management Office | Non-personal data regulator after consultations: MoS IT https://indianexpress.com/article/business/india-data-management-office-non-personal-data-regulator-after-consultations-mos-it-8176909/

45 I definitely think there will be a competitive aspect to it. There'll be national security aspects to it. And those are all important questions. But where I draw the parallel to climate changes is profound enough that you're not going to reach safety on a unilateral basis because the world is connected. And so for you to truly solve for, you know, peaceful coexistence with AI, you would again need over time global frameworks and constructs. And everyone will get affected the same way, just like the climate. And I think that's what will draw people together" - Sundar Pichai

 ISSN: 2582-6433

the AIIMS server was hacked, these activities are possibly done to extract the health and medical records of an individual and then use it against them. There are rising cases of deep fakes being circulated on the internet which leads to misapprehension, this results in a divide in the society and a feeling of animosity and this will in turn give rise to the menace of terrorism which will no longer be in the hands of humans to stop, it will result in unintended or unforeseen consequences which will finally lead to Intelligence explosion. In 2016, Microsoft's AI generated TAY when started operating Twitter, learnt from the tweets of the fellow users and started posting offensive and inflammatory tweets, it had to be closed within16 hours, and hence AI can be compared to the pet animal who lives with us and learns from us and therefore it cannot be set out in the open and needs to be tied with a leash[46].

Therefore, it must be guided by the principles of moral behaviour. There is a need for transparency in the system, the method of designing the algorithm must not be concentrated only in the hands of a few, rather this information must be available to the supervisory and executive authorities in order to mitigate the possibility of bias and accelerate justice and fairness. The principle of non-maleficence i.e.; to do no harm to others must be followed while creating such applications, the creators and designers of such applications must be held accountable and responsible in case of any mishap or adversity. The concerns regarding personal space, integrity and dignity of an individual shall be duly addressed and the principles laid down in the K S Puttaswamy case relating to the privacy of an individual mustbe followed.

With the rising clout of AI which is also called the Black Box[47] due to its ability to self-learn algorithms and Cyberspace being the 5th dimension of warfare[48], the cases of inter-governmental information technology warfare have risen. Chinese hacking group Volt Typhoon attacking the Space Force of the US military is one such example. For this the US has passed the AI Bill of Rights and India's - National Strategy towards harnessing the potential of AI reasonably of NITI AAYOG[49] have been modelled on the basis of the same.

---

46 The ethics of artificial intelligence: Issues and initiativeshttps://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.p df
47 Opening the 'black box' of artificial intelligence https://ec.europa.eu/research-and-innovation/en/horizon-magazine/opening-black-box-artificial-intelligence
48 CYBERSPACE: THE FIFTH DIMENSION OF WARFARE https://futurewars.rspanwar.net/cyberspace-the-fifth-dimension-of-warfare-part-i/ 49 Discussion Paper National Strategy for Artificial Intelligence https://indiaai.gov.in/documents/pdf/NationalStrategy-for-AI-Discussion-Paper.pdf

 ISSN: 2582-6433

Mandatory guidelines such as Multi Factor Authentication, Cloud Storage and Securitythrough Cloud Computing, Microsoft's Video Authenticator technology and Watermarks have been introduced in order to curb the menace of deep fakes.

The cases of copyright infringement have also been rising constantly, the producers have to bear the actual brunt of this facade as their intellectual property is being used ferociously by these Large Language Models such as Chat GPT, thereby reducing their credibility. The G7 nations have initiated the Hiroshima AI Process[50] in this regard as its focus is on making rulesand regulations for a trustworthy AI. India has also been vigilant and vigorous regarding this and therefore launched the Cyber Surakshit Bharat Yojana, Cyber Swachhata Kendra whichis a botnet cleaning and a malware analysis centre and the India Cyber Crime Coordination Centre in 2018, under the Ministry of Home Affairs. The cases of Malware and Ransomware such as Akira are taking a hike and the hackers too demand for cryptocurrency in return ofthe software so that tracing them back becomes impossible, for this, the GOI has included theprovision for Cryptocurrencies and NFTs in the Prevention of Money Laundering Act 2002 and Draft Cryptocurrency Bill by taking inspiration from MiCA - the crypto law of EU[51]. TheLinux based Maya Operating System has now replaced the Microsoft Windows in the Defence Ministry and is also backed by a protection system called Chakravyuh which will help defence forces in eliminating the risks of cyber-attacks. India is already a part of the UN's Internet Governance Forum, UNGA'S Open Ended Working Group and the Group of Governmental Experts. We must also take inspiration and become a part of other conventionssuch as the Budapest Convention[52] (2004) on Cybercrime.

The Bill grants authority to the central government to exclude processing carried out by government entities from certain or all provisions. This is done in the interest of objectives like safeguarding the state's security and upholding public order. In specific instances, such as processing for the prevention, investigation, and prosecution of offences, the rights of data subjects and the responsibilities of data handlers will not be applicable. The Bill does not

50 G7 Hiroshima Process on Generative Artificial Intelligence (AI)
https://www.oecd.org/publications/g7-hiroshima-process-on-generative-artificial-intelligence-ai-bf3c0c60-en.ht m
51 Markets in Crypto-Assets Regulation (MiCA)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R1114&pk_campaign=todays_OJ&pk_source=EURLEX&pk_medium=TW&pk_keyword=Crypto%20assets&pk_content=Regulation&pk_cid=EURLEX_todaysOJ
52 https://www.coe.int/en/web/cybercrime/the-budapest-convention

 ISSN: 2582-6433

mandate government agencies to erase personal data once the processing objective has been fulfilled. With these exemptions, based on national security grounds, a government entity could gather information on citizens to construct a comprehensive profile for surveillance purposes. They may utilise data preserved by various government bodies for this endeavour. This raises the question of whether these exceptions align with the principle ofproportionality. Additionally, it's worth noting that India currently lacks a legal framework addressing limitations on data storage and specifying the purposes for which data can beused. This can eventually lead to the violation of Human Rights of the citizens of one of the leading democracies across the globe.

Autonomy as opposed to Heteronomy explained in Immanuel Kant's Critique of Practical Reason[53] explains that the only way to act autonomously is to follow the moral law - Personal Autonomy does not mean unconstrained choice. Personal Autonomy means the capacity to decide for oneself and pursue a course of action in one's life regardless of any moral contents whereas Kant explains Moral Autonomy as the capacity to deliberate and give oneself to the moral law rather than heeding injunctions of others. The consonance between Privacy and Personal Autonomy can only be achieved when the rights of an individual are kept above the rights of the state, which means that privacy is at its zenith only when personal autonomy is valued. If a state fortifies the personal data of its citizens in order to protect their privacy, in case of excessive control by the state where will the citizen go seeking for their personal autonomy by means of a remedy. We are fully autonomous when we are self determined agents and act in conformity with the formal principle that constitutes an exercise of practicalreason.

The non-personal data of individuals has been excluded from the ambit of the act, which raises tremendous concerns because of risk of theft and privacy being invoked through apps such as Uber, Google, Maps, Zomato etc. For example- The data being inserted on apps such as Uber is not included or is not a part of personal data but it becomes easy to ascertain and find out the house of the individual, the workplace of the individual or where the individual regularly visits through the data that is being feeded by him on the app and can be used against him.

53 https://www.bard.edu/library/arendt/pdfs/bc_Arendt_Kant_CritiquePracticalReason.pdf

 ISSN: 2582-6433

The DPB - Data Protection Board does not have 'suo moto' cognizance over the matters since it is not independent or autonomous in discharging its functions since discretionary executive powers are given to the central government[54]. Along with this the board is also digital by design. This is primarily because the integral functions of the board, appointments of the members and other overreaching powers will be in the hands of the executive authorities.

Diluting the RTI Act, The amendment of Section 8(1)(j) of the Right to Information Act[55] leads to losing consonance between the Right to Information and Right to Privacy, a statutoryand a fundamental right of an individual respectively. It exempts "Personal Information" which is not a part of any public activity from being revealed, this information can be misused by the authorities and gives them the Right to Deny the same. This may give rise to corruption and administrative inefficiency.

The National Automated Facial Recognition System, in the name of National Security - hinders the privacy of the citizens of the nation[56]. The Registration of Births and Deaths (Amendment) Act 2023, provides for linking it to the Aadhaar. The current report of the Moody's[57] suggested a more decentralised digital identity system, away from the already existing centralised Aadhaar Identity Verification.

One of the issues is regarding the Consent for the use of personal data - that is, even when the users (Data Principals) continue to use the website or the application that they are browsing, without explicitly consenting to the terms and conditions - the continued and unhindered use is often considered as an implied consent of the users which will come into force when the Express Terms will not be consented to within the time frame provided for the same. The realquestion is if the consent is actually the real consent, which means it should be freely given, itshould be specific, informed, unconditional and unambiguous and not just some implied consent through the persistent use of the application. The Bill overrides consent of an

54 Understanding India's New Data Protection Law https://carnegieindia.org/2023/10/03/understanding-india-s-new-data-protection-law-pub-90624
55 The London School of Economics and Political Science The Right to Information Act in India: The Turbid World of Transparency Reforms https://etheses.lse.ac.uk/579/1/Sharma_Right_Information_India_2012.pdf 56 Facial recognition technology: fundamental rights considerations in the context of law enforcement https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf
57 Decentralised Finance and Digital Assets, 2023

 ISSN: 2582-6433

individual where the State processes personal data for provision of benefit, service, licence, permit, or certificate.

The Act does not include any non - digitised/analog or meta data though Section 3[58] of the act applies to the processing of digital personal data within the territory of India where the personal data is collected in non-digital form and digitised subsequently, which means thatthe data that still lies in the physical form is under the fear of being misused and manipulated.Though, there are many measures being taken by the government in order to digitise the medical data through Ayushman Bharat Digital Mission[59], preserving the Manuscripts through the National Mission of Manuscripts[60] or the SWAYAM Portal[61] for facilitating education, the most fundamental and foremost motive should be a credible Data protection regime.

One of the drawbacks is that the act does not define or regulate any harm for wrongful processing of data even though the Personal Data Protection Bill, 2019[62] had defined harm to include mental injury, identity theft, financial loss, reputational loss, discriminatory treatment and observation or surveillance not reasonably expected by the data principal. Nothing of this nature has been included in the present legislation.

India must focus on creating a supportive environment for startups, joint research conferences, technology transfer programs and facilitate knowledge exchange between the key stakeholders in order to come out with cutting edge technology. This will be possible with successful implementation of laws such as this one, which will definitely be proved to be a boon for India in its race with other developing nations.

58 Section 3 - Application of Act, Digital Personal Data Protection Act, 2023
59 The Ayushman Bharat Digital Mission (ABDM): making of India's Digital Health Story https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10064942/
60 National Mission for Manuscripts http://indianculture.gov.in/MoCorganization/national-mission-manuscripts
61https://pmevidya.education.gov.in/swayam-portal.html#:~:text=Status,of%20cost%20to%20any%20learner.
62 http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf