VOLUME 4 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

A CRITICAL ASSESSMENT OF THE DIGITAL PERSONAL DATA PROTECTION ACT IN LIGHT OF THE GDPR FRAMEWORK

- Sunidhi Tyagi[1]

ABSTRACT

In an increasingly digital world where personal data fuels modern economies and technologies, the protection of individuals' data privacy rights has emerged as a matter of paramount concern. In the Indian techno-legal context, one of the most prominent regulations in the realm of data privacy is the Digital Personal Data Protection Act (DPDPA), which aligns partly with the General Data Protection Regulation (GDPR) of the European Union (EU). While the shared legal principles serve as the bedrock for data protection, subtle nuances distinguish the DPDPA from the GDPR. The GDPR boasts of an extraterritorial scope, applying globally to organisations processing data of EU residents. In contrast, the DPDPA primarily focuses on entities within India, although it can have extraterritorial effects under specific circumstances. While the GDPR and the DPDPA share fundamental principles that reflect a global commitment to data privacy, their nuanced differences stem from regional legal, cultural, and economic contexts. Emphasising on how protection of personal data of the citizens is critical, the paper tries to dissect the provisions of the DPDPA considering the provisions of the GDPR. The main argument that resonates across the length and width of this paper is that the DPDPA is sectoral in nature. The inferences drawn in this paper are *apriori* in nature and are based on normative findings.

INTRODUCTION

With a new stage of industrial revolution in the offing, data security and data privacy have become matters of primary concern for all, and data has become the defining paradigm for nations across the globe. In fact, 'data is the new oil'[2] and many nations continue to rely on data to promote good governance and public administration.

In the Indian techno-legal context, the relevance of data protection has been gaining relevance for more than a decade now. As per the findings of the National Economic Survey, India will be a five

[1] Final Year Student, LLB (Hons.), Amity Law School, Noida

[2] Lok Sabha Secretariat, "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, last accessed March 28, 2024.

©2024 International Journal of Advanced Legal Research

Trillion Economy and ⅕ of it will be through the digital sector, by means of selling public data.[3] The findings are a testament to the increasing relevance of data, including digital data. The rising significance of data calls for a classified data protection approach, focusing on data security and privacy. Courts and legislators alike have been trying to create a new genre of data protection rights, highlighting data privacy in particular. With reference to the issue of privacy and its significance in developing economies such as India, one of the erstwhile judgements of the Supreme Court of India in *Gobind v. State of Madhya Pradesh* deserves special mention.[4] In *Govind's case*, the Apex Court not only provided a watershed area to the right to privacy but also observed that right to privacy is enshrined under Article 21 of the Constitution of India. The Court had critically distinguished the judgements in the earlier precedents set in *M P Sharma v. Satish Chandra*[5] and *Kharak Singh v. State of Uttar Pradesh*.[6] Finally in *Justice KS Puttaswamy and Another v. Union of India*,[7] Apex Court confirmed the right to privacy as a fundamental right, constituting a vital part of Article 21. However, of late, the focus of both the courts and legislators has been shifted from physical and bodily privacy to data and intellectual privacy.

Before DPDPA, there was no specific data protection law in India although a few provisions of the IT Act, 2000 read with the Rules attempted to augment data protection and to punish body corporates if found negligent in maintaining and implementing reasonable security procedures and practices to ensure protection of sensitive personal data. In addition, till the enactment of the DPDPA, there was hardly any institution (established by law) that administered the relationship between the government, intermediaries and the individuals with reference to data protection. From 2011 to 2014, there were talks on curating a data protection law and in 2011, the Justice AP Shah Committee was formulated to (a) conduct a vivid comparative analysis of the laws relating to data privacy (b) conduct a comprehensive analysis of the various policies and programmes of the Government of India assessing the impact of such policies and programmes on data privacy (c) suggest for the incorporation of the findings in a prospective draft Bill concerning privacy.[8] The Justice AP Shah Committee Report, which was submitted in 2012 stressed on nine principles concerning data privacy. The nine principles were (a) principle of collection limitation (b) principle of access and correction (c) principle of purpose limitation (d) principle of openness (e) principle of accountability (f) principle of security (g) principle of information disclosure (h) principle of consent and choice (i) principle of

[3] Ministry of Electronics and Information Technology, Government of India, "India's Trillion-dollar Digital Opportunity," https://www.meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf, last accessed March 28, 2024.
[4] AIR 1975 SC 1378.
[5] AIR 1954 SC 300.
[6] AIR 1963 SC 1295.
[7] AIR 2017 SC 4161.
[8] Press Information Bureau, "Group of Experts on Privacy Submit Report," https://pib.gov.in/newsite/PrintRelease.aspx?relid=88503, last accessed March 28, 2024.

notice.[9]

The AP Shah Committee was followed by the Justice B N Srikrishna Committee, which was formulated in July 2017 to revisit the data protection framework in India. One of the key observations made by the Committee was a comprehensive data protection law in India. In its Report that was submitted in July 2018, the Committee highlighted the importance of a legislation that would help in safeguarding the privacy and personal data of Indian citizens, especially in a digital age where data would be increasingly being collected, processed, and shared by various entities.[10] The Committee proposed a set of principles which would form the basis of the data protection law in India. These principles included transparency, accountability, data minimization, purpose limitation, storage limitation, data quality, security, and user consent. The Committee recommended the implementation of data localization measures, which would require companies operating in India to store and process data locally. This was seen as a means to ensure better control and protection of data of the Indian citizens. The Committee stressed that people should knowingly agree (informed consent) before their personal information is collected and used. They also suggested giving individuals more control over their data, including the ability to see it (right to access), move it elsewhere (right to data portability), and have it erased (right to be forgotten). To ensure these rights are protected, the Committee recommended creating a new agency, the Data Protection Authority of India (DPAI), to manage and enforce a data protection law.

The DPAI would be responsible for regulating data fiduciaries, handling complaints, conducting inquiries, and imposing penalties for non-compliance. Overall, the Committee's recommendations laid the groundwork for the drafting of the Personal Data Protection Bill, which was introduced in the Indian Parliament in 2019. The 2019 Bill aimed to provide a framework for the protection of personal data and to regulate its processing in India.

Interestingly, a few provisions of the Bill sparked controversy and many amendments were suggested to the same. Resultantly, the 2019 Bill was withdrawn and an all-new bill was tabled in the Parliament in 2022.[11] The 2022 Bill was further modified in 2023, and the 2023 Bill finally got approved by both the houses of the Parliament. The Bill got the assent of the President and came into force on 11th August 2023 as the DPDPA, which comprised new arrangements that would ensure transparency, efficiency and to help in data usage by lawful means. The main principles which are

[9] Ananya Chakraborty, "Right to Privacy: Nine Principles of Data Privacy in AP Shah Report," https://www.news18.com/news/india/right-to-privacy-a-fundamental-right-nine-principles-of-data-privacy-in-ap-shah-report-1500003.html, last accessed March 28, 2024.

[10] 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, last accessed March 28, 2024.

[11] PRS, "The Digital Personal Data Protection Bill, 2023," https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023, last accessed March 28, 2024.

embodied in the DPDPA include (a) usage of data in a lawful manner (b) usage of personal data solely for the purpose it is collected (c) data minimisation (d) data accuracy (e) non-perpetual storage of personal data, by default (f) reasonable safeguards (g) accountability of the authority, which decides the means of processing personal data.

Apart from embodying the aforementioned principles, a few provisions of the DPDPA are in harmony with international standards, to facilitate cross-border data flows, to promote interoperability with global business practices, and to enhance competitiveness in the digital economy. By embracing a forward-looking approach to data protection, grounded in the principles of the GDPR, the DPDPA signaled India's commitment to upholding the rights and freedoms of individuals in an increasingly digitally interconnected world.

DISSECTING THE PROVISIONS OF THE DPDPA

Preamble of the Act outlines its purpose to regulate the handling of online personal data in a way that respects both personal rights to defend their individual information and the requirement to process such data for legal reasons, along with related matters. In Section 2(x), processing personal data is defined as a fully or partially automated set of actions performed on digital personal data. This includes operations such as gathering, arranging, recording, organizing, storing, modifying, retrieving, aligning, utilizing, combining, sharing, categorizing, disclosing through transmission, spreading, or making accessible, restricting, deleting, or annihilating digital personal data. According to Section 2(n) of the DPDPA, digital personal data refers to personal data in a digital form and personal data according to Section 2(t) of the Act denotes any data about persons who are identifiable by or in relation to these data. Data as per Sec. 2(h) of the Act denotes representation of information, fact, concept, opinion or instructions in a way appropriate for communications, interpretations or processing by people. 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 of the Act. However, the exact import of what constitutes a "lawful purpose" will become clearer once the courts review and interpret the expression "certain legitimate uses."

Section 2(j) of the Act defines data principals. As per the provisions of the DPDPA, data principals are entitled to the following rights:[12]

(a) Right to Consent for the usage of data (of data principals) by the data fiduciaries:[13] the data principals have the right to know for what purpose and in what manner the data will be used.

(b) Right to withdraw consent: the data principals must also be informed about this right with the notice and such notice shall be made accessible in all the languages specified in the 8th Schedule of the Constitution of India.

[12] Sections 11 to 14, Chapter 3, Digital Personal Data Protection Act, 2023.

[13] As per Section 2(i) of the DPDPA, 2023, data fiduciary refers to any person who determines the means and purpose of processing personal data.

(c) Right to deletion/right to erasure/the right to be forgotten: it is also a part of right to life and personal liberty under Article 21 of the Constitution of India 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 suit their personal interests.

(d) Right to request summary of the data that belongs to the user: this includes the right to be informed about where the data is being used, the right to collect the data from the fiduciaries, the right to Nominate another trustworthy in case of death of the user whose data is in question, the right to access the data, the right to rectification/addition/omission of data.

The aforementioned rights of the data principals come with duties. As per Section 15 of the DPDPA, data principals have the duty to (a) conform with the provisions of all the laws while exercising their rights (b) make sure to not impersonate any other person while furnishing personal data (c) make sure to not suppress any information while furnishing personal data (d) make sure to not register (with a Board/data fiduciary) any frivolous/false complaint/grievance (e) provide only the information that is authentic. Any breach in compliance with the above-mentioned duties under Section 15 would render a data principal liable to a monetary penalty, which may extend to Rupees 10,000.[14]

Another important feature of the Act is that it requires parental consent for the collection of personal data of children, and for this the individual who is below the age of 18 will be considered as a child.[15] This has been done with a view to keep the children away from malicious content, which gets circulated online and tends to affect the mental and physical well-being of children in their budding stages.

In DPDPA, there is also a mandatory requirement of Government of India's permission in case of cross border transfers of data.[16] The Act also provides for the creation of a list of countries with whom the personal data cannot be shared or transferred. This negative list of countries has been created keeping in mind the data protection laws of other nations and how secure the data of Indian citizens in other countries is. Further, the Act also provides for data processors for processing the data of data principals and data fiduciaries. Furthermore, the Act contemplates the appointment (by the data fiduciary) of a data protection officer,[17] who will be responsible for deleting and modifying the collected data. Apart from the above, the Act stipulates regular data audits, data protection impact assessments, consent managers, data minimisation, data accuracy, data localisation and data protection authorities to ensure reasonable safeguards that will help in protecting the data of the Indian citizens. This means that the data will only be collected for intended purposes, and no unnecessary processing of data will take place; stringent security measures will be imposed in case of

[14] Section 33(1), DPDPA, 2023 read with the Schedule to the Act.
[15] Section 9, DPDPA, 2023.
[16] Section 16, DPDPA, 2023.
[17] Section 10(2)(a), DPDPA, 2023.

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,[18] security and public order.

It is an obligation of the data fiduciaries to make use of reasonable security measures in order to prevent 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 the responsibility of the data fiduciary to inform the data principal along with the Data Protection Board (DPB) about the same. However, the state, especially the Government of India, in the interest of sovereignty, integrity and security of India may ask for disclosing the personal data of individuals. This may also be extended in case of medical emergencies, epidemics, disasters, etc. In fact, Section 7 of the DPDPA allows the data fiduciaries, especially the state and its instrumentalities,[19] to process personal data, including sensitive personal data, to fulfil any obligation under a law that is in force. Such a plenary power of the state to process personal data extends to taking measures in the event of a threat to public health or collapse of public order.

Relief to the data principals through grievance redressal platforms is supposed to be provided by the data fiduciaries, as per the provisions of the DPDPA.[20] Such an obligation on the data fiduciaries is further augmented by the right of the data principals of grievance redressal.[21] A further grievance redressal and dispute resolution mechanism that is operable is the DPB, which is an adjudicatory and not a regulatory authority. The DPB, which is for two years tenure,[22] is vested with the powers of a civil court and may, therefore (a) summon and enforce attendance of any person (b) receive evidence on affidavit (c) inspect records (d) discharge any other functions that are valid in law. Any person resentful of the decision of the DPB may appeal to the Telecom Disputes Settlement and Appellate Tribunal within 60 days from the date the order/direction of the DPB is received.[23] The grievance redressal obligation of the data fiduciaries must be read in conjunction with Section 33(1) of the Act that obligates data fiduciaries to pay monetary penalty extending to Rupees 250 Crores if the data fiduciaries fail to undertake reasonable security safeguards so as to prevent breach of personal data.[24]

The DPDPA amends other enactments to ensure compliance with other laws. For example, Section 8(1)(j) of the Right to Information Act, 2005 has been amended by which information can be withheld by calling it personal data or information of public officers and ministers. The DPDPA has also amended Section 14 of the Telecom Regulatory Authority of India Act, 1997. Further, it has amended Section 81 of the IT Act and has omitted Sections 43A and 87(2)(ob) of the IT Act. With reference to the amendment of the IT Act, the DPDPA will help in replacing yet diluting the

[18] Section 17(2)(b), DPDPA, 2023.
[19] The expression "state" under Section 2(zb) of the Act means the state as has been defined under Article 12 read with Article 36 of the Constitution of India.
[20] Section 8(10), DPDPA, 2023.
[21] Section 13(1), DPDPA, 2023.
[22] Section 20(2), DPDPA, 2023.
[23] Section 29 read with Section 2(a), DPDPA, 2023.
[24] Section 33(1), DPDPA, 2023.

provisions of the IT (Reasonable Security Practices, Procedures and Sensitive Personal Data or Information) Rules, 2011. The IT Rules, 2011 applies on body corporates and persons located in India only, it also involves sensitive personal data such as passwords, credit card and debit card information, biometric information, which are required for authentication and other physical physiological and mental health data. Since the DPDPA omits Section 43A of the IT Act, no compensation will be provided by the data fiduciaries to the data principals in case of failure to protect data.

THE GDPR REGIME AND ITS BEARING ON DPDPA: A COMPARATIVE ANALYSIS

Jurisdiction is closely linked to sovereign equality and territorial sovereignty of states.[25] The General Data Protection Regulation (GDPR) marks a significant departure by extending its reach beyond national boundaries. Traditional international law, which usually confines a state's authority to its own territory based on the Westphalian concept of exclusive state sovereignty, typically allows for the extraterritorial application of human rights only in rare cases. However, the GDPR introduces the concept of the domestic-market principle, notably outlined in Article 3(2). This principle imposes obligations on data processors or controllers located outside the EU if they provide goods or services to individuals within the EU or monitor the behavior 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 commons, it is important to note that cyberspace possesses a distinctive nature and is not 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 within the EU must comply with the GDPR, even if it lacks any other substantial connection with the EU. As a result, the passive personality principle leads to outcomes that have effects beyond national borders.

The DPDPA is modelled on the GDPR, the data subjects and data controllers[26] of the GDPR are data principals and data fiduciaries of DPDPA, respectively. The DPDPA tries to enforce stricter requirements for notifying data breaches. Under the Act, data fiduciaries are obligated to inform both the DPB 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 DPDPA does not embody these rights. Instead, it offers two other rights – the right to grievance redressal and the right to appoint a nominee.

The GDPR imposes obligations such as maintaining records of processing activities and practising data minimization, which are not addressed in the DPDPA. In addition, the GDPR defines a

[25] Article 2(1), Charter of the United Nations, 1945.
[26] Article 4, GDPR, 2016.

child as someone below 16 years of age, whereas the DPDPA defines a child as someone below 18 years of age. The GDPR allows data processing to the extent of consent provided by the parents or guardians, while the DPDPA permits processing of all types of data. It is important to note that the GDPR doesn't regulate non-personal or anonymous data, whereas the DPDPA may allow access to such data.

Under the DPDPA, data fiduciaries must ensure that any transfer of personal data outside India adheres to adequate safeguards, as approved by the Government of India. It also requires explicit consent from data principals before transferring their sensitive personal data. Conversely, the GDPR prohibits the transfer of personal data outside the EU or European Economic Area (EEA) unless the recipient nation guarantees sufficient levels of protection, or appropriate safeguards.

Both the DPDPA 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.

In terms of enforcement, the DPDPA establishes a DPB[27] to undertake various measures in response to personal data breach. The GDPR establishes the European Data Protection Board to ensure consistent application of the GDPR across the EU.[28]

Penalties for non-compliance differ; under the provisions of the DPDPA, monetary penalties range from Rupees 10,000 to Rupees 250 Crores while under the provisions of the GDPR, monetary penalties (fines) may go up to 20 million Euros 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.

In addition to the above, the GDPR does not categorise data controllers and does not recognize the concept of consent managers. In contrast, the DPDPA introduces a classification of data fiduciaries, distinguishing significant data fiduciaries based on factors such as the volume and nature of data they collect. This classification entails additional obligations for the identified significant data fiduciaries[29]. Moreover, the DPDPA establishes the role of a consent manager, who is registered with the DPB, serving as a central contact point for data principals to manage their consents through accessible platforms.

The GDPR and the DPDPA both regulate the cross-border transfer of personal data, but with some distinctions. While the GDPR prohibits such transfers outside the EU or EEA unless certain conditions are met, like ensuring adequate data protection levels or using approved mechanisms by the European Commission, the DPDPA in India requires data fiduciaries to follow government-

[27] Chapter 5, Sections 18-26, DPDPA, 2023.
[28] Section 3, Article 68, GDPR, 2016.
[29] Section 10, DPDPA, 2023.

determined safeguards for such transfers. Moreover, the DPDPA mandates explicit consent from individuals before transferring their sensitive personal data abroad.

Although the DPDPA is similar to the GDPR in structure, it has unique aspects. These include more stringent criteria for processing data, exemptions for government bodies, government authority to specify and exempt fiduciaries, absence of predefined protection for special data categories, and the government's ability to request and restrict access to information.

IMPORTANCE AND NEED FOR A ROBUST DATA PROTECTION FRAMEWORK

Although, the DPDPA is an important enactment taking cue from the EU's GDPR 2016, and to an extent from other international data protection laws such as Thailand's Personal Data Protection Act, Swiss Revised Federal Act on Data Protection, Bahrain's Personal Data Protection Law, Singapore's Personal Data Protection Act, Irish Data Protection Act, Qatar's Data Protection Law, Saudi Arabia's Personal Data Protection Law, etc.,[30] it still falls short of creating a robust data protection framework. Also, the DPDPA, which aligns closely with the data protection law in China that was implemented in November 2021,[31] falls short of replicating the Chinese law. In China, the Personal Information Protection Law and the Data Security Law provides the highest level of data security measures. Arguably, compared to the global counterparts, India's data protection law has a sectoral focus, which fails to involve a combination of policies and measures to enhance and advance the level of protection in key domains.

It must also be noted that since almost 65% of the online population is below 35 years of age,[32] verifiable parental consent along with strict cyber security regulations is the need of the hour. For this, a comprehensive approach and not a mere sectoral approach must be adopted by the nations such as India. In addition, there is also a robust need to incorporate the principles of data empowerment and to holistically promote the principles of protection architecture, data sovereignty, and data localisation within the broader confines of the DPDPA.

The sectoral approach of the DPDPA is also reflected because it has loose ends to protect breach of sensitive personal data and data concerning public health. 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

[30] Debatably, approximately 71% countries across the globe have data protection and privacy legislation in place, and about 9% have draft legislation governing data protection.

[31] China Briefing, "The PRC Personal Information Protection Law (Final): A Full Translation," https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/, last accessed March 28, 2024.

[32] Statista, "Distribution of internet users worldwide as of 2021, by age group," https://www.statista.com/statistics/272365/age-distribution-of-internet-users-worldwide/, last accessed March 28, 2024.

expose the need to make DPDPA more nuanced so that critical data of the citizens of this country is robustly protected.

With the growing influence of technology, and artificial intelligence (AI) being in an advanced evolutionary stage, platforms such as ChatGPT also pose significant challenges to cyber security. In fact, with the emergence of AI,[33] there is an urgent need for a holistic framework for data governance and privacy regulations to administer cross border data flows and to strengthen *global cybersecurity defenses.* Such a local yet differentiated approach by the DPDPA will seemingly reverse growing cyber security threats posed by offences such as identity theft, cyber obscenity, cyber terrorism, etc. There is no gainsaying the fact that AI applications are widely used in diverse sectors such as the healthcare sector for disease mapping and prediction, the agricultural sector, the industrial sector, etc., as there are apparently many benefits such as automation, accuracy, durability, efficiency, precision, etc. However, certain uses of AI involve high cost which may further lead to inequality in society. There is also a possibility of bias and discrimination attached to AI applications.

Apart from the unregulated use of AI, there are rising cases of deep fakes being circulated on the internet that leads to misapprehension;[34] this may also result in a divide in the society and a feeling of animosity which may in turn give rise to the menace of cyber terrorism. Although guidelines such as multi-factor authentication, cloud storage and security through cloud computing, Microsoft's video authenticator technology and watermarks have been introduced to curb the menace of deep fakes, the situation relating to the regulation of deep fakes seems to be far from satisfactory. 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 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 *KS Puttaswamy case*[35] relating to the privacy of an individual must be followed.

[33] "Invention of AI is more revolutionary than the invention of fire" - This was the statement by the Chief Executive Officer of one of the most powerful companies in the world, Google.

[34] 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 within 16 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. For further details see: European Parliament, "The Ethics of Artificial Intelligence: Issues and Initiatives,"https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf, last accessed March 28, 2024.

[35] AIR 2017 SC 4161.

With the rising clout of AI, which is also called the Black Box due to its ability to self-learn algorithms,[36] and Cyberspace being the 5th dimension of warfare,[37] the cases of inter-governmental information technology warfare have proliferated over time. Chinese hacking group Volt Typhoon attacking the Space Force of the US military is one such example. For this, the US passed the AI Bill of Rights and India's national strategy towards harnessing the potential of AI reasonably of NITI AAYOG has been modelled based on the same. The G7 nations have also initiated the Hiroshima AI Process,[38] focused on making rules and regulations for a trustworthy AI.

Apart from the concerns pertaining to the use of AI, the cases of copyright infringement have also been rising constantly; the producers must bear the actual brunt of this facade as their intellectual property is being used by Large Language Models such as ChatGPT, thereby reducing their credibility. India has also been vigilant and vigorous regarding this and, therefore, launched the Cyber Surakshit Bharat Yojana, Cyber Swachhata Kendra (A botnet cleaning and a malware analysis center) 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 of the software so that tracing them back becomes impossible, for this, the Government of India has included the provision for cryptocurrencies and non-fungible tokens in the Prevention of Money Laundering Act 2002 and draft Cryptocurrency Bill by taking inspiration from Markets in Crypto-Assets Regulation - the crypto law of the EU.[39] The Linux-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. Despite efforts, the digital personal data protection regime in India is still in a nascent stage.

CONCLUDING REMARKS

The DPDPA grants authority to the union government to exclude processing carried out by government entities from certain or every provision. This is done in view of holistic statal objectives such as safeguarding the state's security and upholding public order. In specific instances, such as processing for the prevention, investigations, and prosecution of offences, rights of data subjects and responsibilities of data handlers will not be applicable. With these exemptions, based on national

[36] European Commission, "Opening the 'black box' of artificial intelligence," https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine/opening-black-box-artificial-intelligence, last accessed March 28, 2024.
[37] R S Panwar, "Cyberspace: The Fifth Dimension of Warfare – Part 1," https://futurewars.rspanwar.net/cyberspace-the-fifth-dimension-of-warfare-part-i/, last accessed March 28, 2024.
[38] Organisation for Economic Co-operation and Development, "G7 Hiroshima Process on Generative Artificial Intelligence (AI)," https://www.oecd.org/publications/g7-hiroshima-process-on-generative-artificial-intelligence-ai-bf3c0c60-en.htm, last accessed March 28, 2024.
[39] *Ibid.*

security grounds, a government entity could gather information on citizens to construct a comprehensive profile for surveillance purposes. This raises the question of whether these exceptions align with the principle of proportionality. Additionally, it is worth noting that India currently lacks a legal framework addressing limitations on data storage and specifying the purposes for which data can be used. This can eventually lead to the violation of human rights of the Indian citizens.

Autonomy as opposed to heteronomy explained in Immanuel Kant's Critique of Practical Reason[40] clarifies that the only way to act autonomously is to follow the moral law; personal autonomy does not mean unconstrained choice. 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 does not fortify the personal data of its citizens to protect their privacy, in case of excessive control by the state where will the citizens go seeking for their personal autonomy.

The non-personal data of individuals has been excluded from the ambit of the DPDPA, which raises tremendous concerns because of the risk of theft and privacy being created 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 or where he/she regularly visits through the data that is being fed by them on the app and can be used against them.

Arguably, the DPDPA suffers from another significant infirmity; the DPB does not have the authority to take *suo moto* cognizance of the matters since it is not independent or autonomous in discharging its functions. Along with this, the Board is also digital in design. Moreover, the integral functions of the Board, appointments of the members and other overreaching powers are in the hands of the executive authorities, leading to chances of red tapism and other administrative excess.

By diluting the Right to Information Act, 2005 amending Section 8(1)(j) of the Act, the DPDPA has led to losing consonance between the right to information and the right to privacy, a statutory and a fundamental right of an individual. The dilution 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. In addition to the above, the Registration of Births and Deaths (Amendment) Act, 2023, provides for linking it to the Aadhaar. The current report of the Moody's[41] suggested a more decentralised digital identity system, away from the already existing centralised Aadhaar identity verification.

---

[40] Immanuel Kant, "Critique of Practical Reason," https://www.bard.edu/library/arendt/pdfs/bc_Arendt_Kant_CritiquePracticalReason.pdf, last accessed March 28, 2024.

[41] Moody, "Digital Finance," https://www.moodys.com/newsandevents/topics/Digital-Finance-007060, last accessed March 28, 2024.

One of the issues in DPDPA circumscribes around 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 main question is: if the consent is the actual consent, which means it should be freely given, it should be specific, informed, unconditional and unambiguous and not just some form of implied consent through the persistent use of the application.

Another purported shortcoming of the DPDPA is that the Act does not include any non-digitised/analog or meta data though Section 3 of the Act applies to processing of digital personal data in India where the personal data is gathered in non-digital form and digitised subsequently, which means that the 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 to digitise data through endeavours such as Ayushman Bharat Digital Mission, preserving the Manuscripts through the National Mission of Manuscripts or the SWAYAM Portal is an increasingly uphill task.

As we embark on this journey towards a more privacy-conscious and data-responsible future, the DPDPA, despite its sectoral approach, stands as a testament to our commitment to safeguarding personal data, promoting innovation, and fostering trust in a digital age. Through collaborative efforts and stakeholder engagement, India endeavors to realize the full potential of this legislation, making sure that it serves as a cornerstone for building a resilient, inclusive, and ethically driven digital society. In conjunction with the mandates of the DPDPA, India must focus on creating a supportive environment for startups, joint research conferences, technology transfer programs, and must facilitate knowledge exchange between the key stakeholders, keeping in mind the scrupulous use of digital data.