CRITICAL ANALYSIS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Anurag Sourot, Asian Law College, Noida

Deepali Kushwaha, Asian Law College, Noida

ABSTRACT

The article critically analyses the Digital Personal Data Protection Act, 2023, tracing its inception from pivotal historical cases like MP Sharma v. Satish Chandra (1954) to landmark decisions such as K.S. Puttaswamy v. UoI and subsequent developments. It examines the legislative trajectory of the act, commencing from the setup of Justice B. N. Shrikishna Committee to the passing of DPDP Bill 2023 by both the houses of Parliament. The Article explores rights and principles, compliance obligations, regulatory enforcement under The DPDP Act and shedding light on its profound implications for data processing and privacy practices. Additionally, delves into cross-border data transfer, including the contentious issue of data localization and their reverberations on global data flows and national sovereignty. By drawing comparisons between GDPR and DPDP Act, the article discerns the strength and weaknesses. It consequently culminates in a critical assessment of the Act, with regards to the suggestion put forth by Joint Parliamentary Committee (JPC) in its report, following to which a set of prospective recommendations has been proffered, which could be deliberated upon to facilitate efficacious attainment of rights and uphold democratic governance.

I. Introduction: -

In the digital age, the rapid advancement of technology has revolutionized the way information is generated, collected, and utilized. The exponential growth in data generation has led to unprecedented challenges in safeguarding individuals' privacy rights. To address these concerns, governments around the world have enacted comprehensive legislation aimed at protecting personal data in digital ecosystems. India the country that has the second highest internet-using population has also enacted one such significant legislation to protect individual privacy rights. That is the Digital Personal Data Protection Act, of 2023 ('the Act'). This Act, is a crucial milestone in the realm of data protection, and it sets a legal framework to govern the processing, storage, and transfer of personal data by both public and private data fiduciaries. This Act, aims to incorporate principles that are enumerated under Article 12 of the *Universal Deceleration of Human Rights ('UDHR')*, *1948* and Article 17 of the *International Covenant on Civil & Political Rights ('ICCPR'), 1966* to achieve global standards in privacy laws. As technology is continuously evolving, it becomes imperative for us to critically analyse the provisions of this Act through the lens of constitutional principles and the fundamental right to privacy which will in turn make this Act achieve global standards. This research paper endeavours to undertake a comprehensive examination of the Act. Through a critical and comparative analysis of its provisions with the *General Data Protection Regulation* ('GDPR') which is globally acknowledged as an effective data privacy law and the recommendations of the parliamentary committee. This paper seeks to assess the Act's effectiveness in upholding constitutional mandates while ensuring the protection of individual privacy rights in the digital sphere. By delving into key aspects of the Act and its implications, this study aims to contribute to the ongoing discourse on data protection and privacy in the digital era. Through this holistic analysis, we aim to shed light on the complexities and challenges inherent in balancing technological innovation with the protection of fundamental rights.

II. Historical Development: -

The Right to Privacy has not been defined and envisaged by the Constitution makers

in the original draft of the constitution of India[1] and as such is not mentioned in Part III of any such Fundamental Rights. However, it was the first time in 1954, just four years after the Constitution came into force, the Supreme Court dealt with the question of privacy in the case of *MP Sharma vs Satish Chandra case*[2], in this case, the Supreme Court decided that power of the police to search and seizure in Criminal Procedure Code[3] is not subjected to Right to privacy as there is no mention of any such right in part III of the constitution which is analogous to the fourth amendment made in the constitution of United States[4] which prohibits the arbitrary search and seizure.

In 1962, the Supreme Court decided the case of *Kharak Singh vs State of UP.*[5], examined the power of police surveillance under section 236 of UP Police Regulations[6] concerning habitual criminals. In this judgment Court partially allowed the right to privacy in the name of the liberty and dignity of the individual under article 21 of the constitution which is being violated because of the nightly domiciliary visits by the police but had rejected the contention that the police surveillance over the habitual offender is the violation of the privacy of that individual on the ground that there is no concept of right to privacy in the constitution and it ruled in the favour of the police.

It was 1975 that became a turning point for the right to privacy in India. The Supreme Court while hearing the *Govind vs State of MP. & ors*.[7] Case introduced the compelling state interest test from the case of *Griswold vs Connecticut*[8] and *Roe vs Wade*[9] which were decided by the Supreme Court of the US. The Court stated that the right to privacy is a right under Article 21[10] of the constitution and it can only be interfered with when there is a larger state interest.

[1] INDIA CONST.
[2] MP Sharma v. Satish Chandra case, (1954) 1 S.C.R. 1077
[3] Code of Criminal Procedure, No. 2, Act of Parliament, 1974, §165
[4] US CONST.
[5] Kharak Singh v. State of UP, A.I.R. 1963 S.C. 1295
[6] UP Police Regulations, 1948, Gazette Extraordinary Part. II Rule 236
[7] Govind v. State of MP, 1975 S.C.C. (2) 148
[8] Griswold v. Connecticut, 381 U.S. 479 (1965).
[9] Roe v. Wade, 410 U.S. 113 (1973).
[10] *Supra* note 1 at 1.

In 1997, in the case of *PUCL vs Union of India*[11], which is commonly known as the telephone tapping case, the Supreme Court while considering the relation between Indian and International jurisprudence affirmed the right to privacy and said that individuals have a privacy interest in the content of their telephonic communications and same can only be interfered by procedure established by law. The Court further gave some guidelines as to the procedure to proceed with the surveillance and put a check on the misuse of power by the executive in light of the Right to Privacy.

In 2012, in the case of *K.S. Puttuswami & Anr. vs Union of India & Ors*.[12] The retd. Justice of Karnataka High Court Justice KS. Puttuswami filed a case against the constitutional validity of the Aadhar scheme. This case is the cornerstone of the 'Right to Privacy' jurisprudence in India. In this scheme, the people were given twelve-digit unique identification numbers based on their data collected in the form of biometric scans, retina scans, date of birth, address, etc. Meanwhile, some other petitions were also referred to the Supreme Court challenging the various aspects of the Aadhar scheme. In 2015 a question arose about the "Right to Privacy" and whether is it a fundamental right or not. Previously in the case of *MP Sharma vs Satish Chandra*[13], the constitutional bench of eight judges declared that the right to privacy was not a constitutional right. Some other benches of the Supreme Court recognized the right to privacy as a right but the strength of the bench in those cases was smaller than the MP Sharma case. Supreme Court in 2017, created history and unanimously declared the Right to Privacy as a fundamental right under Article 21 of the part III with a strength of nine judge bench. However, the bench subjected the right to privacy to reasonable restrictions and declared it not absolute.

III. Legislative Overview: -

The legislative odyssey of the Act, represents a seminal journey in India's legislative landscape, predominantly concerning data protection and privacy. The Act, came into effect on August 11, 2023, tracing back its origin to several pivotal events that

[11] PUCL v. Union of India, (1997) 1 S.C.C. 301
[12] K.S. Puttuswami v. Union of India, (2017) 10 S.C.C. 1
[13] *Id.* at 2.

unfolded in the past seven years. A meticulous exploration of this narrative offers profound insights into the development of data protection and privacy laws in India.

The legislative saga commences with the precedent-setting case of the Supreme Court on August 24, 2017, *K.S. Puttaswamy vs Union of India*[14], wherein the Right to Privacy for the very first time was recognized as a Fundamental Right. This judicial pronouncement set the stage for the formulation of a comprehensive legal framework for data protection in the nation.

Consequently, on July 31, 2017, the Justice B. N. Shrikishna Committee was set up by the Ministry of Electronics and Information Technology (MeitY), Government of India ('The Indian Government').[15] It was tasked to make recommendations on data protection in India in response to the growing concern, particularly in the wake of Aadhaar Controversy.[16]

On November 27, 2017, the Justice Shrikrishna Committee presented a White Paper on the Data Protection Framework for India[17], delineating fundamental principles and recommendations. The document outlined the need for a balanced approach to data protection, taking into account the individual interests, also interests of The Indian Government and businesses. It served as a roadmap proposing a framework based on principles such as informed consent, purpose limitation, data minimization, data security, and accountability.[18] It sparked discussions, controversies, and debates amongst stakeholders, highlighting complexities.

Subsequently, on July 27, 2018, the Justice Shrikisna Committee submitted the Draft Personal Data Protection Bill, 2018 ('the Bill, 2018') to the Ministry of Electronics and Information Technology (MeitY).[19] It received extensive feedback

[14] *Supra* note 12 at 2.
[15] PRS LEGISLATIVE RESEARCH, DIGITAL PERSONAL DATA PROTECTION BILL, 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#_edn8.
[16] *Id.* at 14.
[17] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., WHITE PAPER ON DATA PROTECTION FRAMEWORK FOR INDIA, (2017), https://www.meity.gov.in/white-paper-data-protection-framework-india-public-comments
[18] *Id.*
[19] PRS LEGISLATIVE RESEARCH, DIGITAL PERSONAL DATA PROTECTION BILL, 2018, https://prsindia.org/billtrack/draft-personal-data-protection-bill-2018

for marking a crucial step in strengthening data protection and privacy laws in India and aligning them with the global standards.[20]

The legislative journey gained momentum when the Personal Data Protection Bill, 2019 ('the Bill, 2019')[21] was tabled in the Lok Sabha on December 11, 2019. However owing to the intricate complexities the Bill, 2019 was referred to a Joint Parliamentary Committee (JPC)[22] on December 17, 2019, for detailed examination and recommendations.

The JPC was tasked with reviewing the provisions of the Bill, 2019 meticulously, asking inputs from stakeholders and make suggestions to address any concerns. The committee's mandate was to ensure the balance between the interests of individual, The Indian Government and businesses.[23] The JPC submitted its report on December 16, 2021 along with recommendations and revisions to the Bill, 2019.[24] It was a significant milestone with key features such as Data Subject Rights, Data Processing Principles, Data Localization, Data Protection Authority (DPA), and Penalties and Enforcement.[25] It was aimed at fortifying the Bill, 2019 and addressing various concerns raised during the process.

However, the Bill, 2019, along with the JPC recommendations was withdrawn from Parliament on August 3, 2022. Primarily the Bill, 2019, was withdrawn to make a way for addressing the evolving challenges in the digital landscape. Additionally, the withdrawal of the Bill, 2019, reflected the The Indian Government's commitment to addressing concerns of various stakeholders to ensure that the new

[20] The Wire, Justice Shrikrishna Committee Submits Draft Data Protection Bill, THE WIRE (July 28, 2018), https://thewire.in/law/privacy-bill-india-orwellian-state-justice-bn-srikrishna.
[21] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., PERSONAL DATA PROTECTION BILL, 2019, BILL NO. 373 OF 2019 (INDIA). https://www.meity.gov.in.
[22] Press Release, Ministry of Parliamentary Affairs, Joint Committee on the Personal Data Protection Bill, 2019 Seeks Views and Suggestions, PIB (Dec. [date], 2019), https://pib.gov.in/PressReleasePage.aspx?PRID=1601695.
[23] *Id.*
[24] PRS LEGISLATIVE RESEARCH, DIGITAL PERSONAL DATA PROTECTION BILL, 2019, https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019
[25] JOINT PARLIAMENTARY COMM., GOV'T OF IND., RECOMMENDATIONS ON THE PERSONAL DATA PROTECTION BILL, 2019, https://prsindia.org/files/bills_acts/bills_parliament/2019/Summary-JPC%20Report_PDP%20Bill,%202019.pdf

legislation meets the highest standards globally in the field of digital personal data.[26]

Withdrawal of the Bill, 2019, paved the way for a renewed approach, culminating in the drafting of the Digital Personal Data Protection Bill, 2022 ('the Bill, 2022').[27] Signalling a fresh phase in the legislative journey, The Indian Government initiated the drafting of a new legislation, to address the challenges and opportunities in the evolving technological ecosystem. It was aimed to incorporate key principles such as accountability, cross-border data flows and other emerging issues.

On November 18, 2022, the draft of the Bill, 2022 was released for public consultation, inviting ideas and opinions from stakeholders.[28] The inclusive approach by the legislation showcased its commitment to the evolving nature of data protection challenges and also ensured that the final legislation embodies diverse perspectives. This period provided an opportunity to review the draft Bill, 2022, analyse its provisions, and provide input on areas that require further modification. The feedbacks received were instrumental in refining the draft Bill, 2022 and enhancing its effectiveness.

The legislative journey reached its high-point on July 5, 2023, when the Cabinet accorded its approval to the Bill, 2023.[29] It culminated in a historic moment highlighting The Indian Government's unwavering commitment. The approval was a testament to extensive consultation, deliberations and refinements that shaped the bill.

Following the approval, the latest draft of the Bill, 2023 was tabled in Parliament on August 3, 2023. It received overwhelming support in both the houses. In Lok Sabha it was passed on August 7, 2023 and in Rajya Sabha on August 9, 2023.

[26] Press Release, Gov't of Ind., Withdrawal of Personal Data Protection Bill, 2019, PIB (Aug. 3, 2022), https://pib.gov.in/PressReleasePage.aspx?PRID=1845322

[27] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., DIGITAL PERSONAL DATA PROTECTION BILL 25 (2022), https://prsindia.org/billtrack/draft-the-digital-personal-data-protection-bill-2022.

[28] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., PUBLIC CONSULTATION FOR DIGITAL PERSONAL DATA PROTECTION BILL, (2022), https://www.meity.gov.in/writereaddata/files/Notice%20-%20Public%20Consultation%20on%20DPDP%202022_1.pdf.

[29] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., APPROVAL OF DPDP BILL 2023 BY CABINET (2023), https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023.

On August 11, 2023, the Bill, 2023 received Presidential assent and was published in the Official Gazette, officially becoming the DPDP Act.[30] It marked an important milestone in the history of the digital legal framework empowering individuals with greater control over their personal data and imposing accountability on the processors and fiduciaries.

IV. Scope and Applicability: -

The Act, encompasses a wide-ranging scope and applicability, which extends beyond India's borders if it pertains to the provision of goods and services to Data Principals[31] ("individuals to whom data relates") within India.[32] The extraterritorial applicability of the Act, ensures that data protection extends to individuals irrespective of their physical location, ensuring that even foreign entities processing data of Indian individuals are subject to the regulations.

Additionally, the Act covers digitized data as well as data which was collected in non-digital from at the beginning but subsequently digitized.[33] It widens the coverage of the Act by ensuring that all forms of data fall under the purview irrespective of their original format. However, the Act excludes from its scope personal data used by individual for any domestic purpose, made/caused publicly available by data principal themselves or by other parties obligated by law to do so.[34]

V. Principles and Rights: -

There are certain rights which are enumerated under the Act, for the protection of the interest of the data principals. These rights puts several restrictions and duties on the data fiduciaries and data processors in order to empower the data principals

[30] MINISTRY OF ELECS. & INFO. TECH., GOV'T OF IND., THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023, GAZ. NOT. NO. 25/2023-CG-DL-E-PART (2) (Aug. 11, 2023), https://egazette.gov.in/(S(4lkw3rtfqezkzecrbxvx2q3i))/SearchPublishDate.aspx?id=564621 (last visited 24 Mar. 2023).

[31] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, § 2(j)

[32] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §3(b)

[33] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §3(a)

[34] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §3(c)

and to protect their interest, such rights have to be put into consideration by the data fiduciary and the data processors while processing data. The rights are as follows:-

A. For the processing of any data of the data principal, the consent of the data principal must be taken and the consent shall be free, specific, informed, unconditional and unambiguous.[35] The data shall be processed in accordance and to extent as consent may be given and if any part of the consent violates any of the provision of this Act, then such consent till violating part shall be invalid *'ab initio'.*[36] Data principal can access the consent request in any of the language[37] specified in eighth schedule[38] of the Indian Constitution and can withdraw the consent anytime,[39] but the consequences of the same shall be borne by the data principal.[40]

B. The data principal has a right to obtain from the data fiduciary a summary of the personal data processed, activities undertaken to process,[41] identities of all the data fiduciaries with whom the personal data has been further shared, along with the description of the personal data so shared[42] and any other relevant information that may be needed.[43]

C. The data principal has a right of grievance redressal by approaching the appropriate data fiduciary or consent manager for not fulfilling their obligations or any kind of omission in protecting the personal data of the data principal.[44] The relevant authority which may have been approached shall respond to the data principal within the time as may be prescribed.[45]

[35] Digital Personal Data Protection Act, No. 22, Act of Parliament,2023, §6(1)
[36] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(2)
[37] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(3)
[38] (1) Assamese, (2) Bengali, (3) Gujarati, (4) Hindi, (5) Kannada, (6) Kashmiri, (7) Konkani, (8) Malayalam, (9) Manipuri, (10) Marathi, (11) Nepali, (12) Oriya, (13) Punjabi, (14) Sanskrit, (15) Sindhi, (16) Tamil, (17) Telugu, (18) Urdu (19) Bodo, (20) Santhali, (21) Maithili and (22) Dogri.
[39] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(4)
[40] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(5)
[41] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §11(a)
[42] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §11(b)
[43] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §11(c)
[44] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §13(1)
[45] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §13(2)

D. The data principal has a right to nominate the individuals who will assume the responsibility and authority of the data principal after the death of the data principal in accordance to the provisions of this Act.[46]

VI. Compliance Obligations: -

In the growing era of digitalization everything is being processed through digital media and most of the personal data of the service user is present online with the processing identities. The Act came up with an objective to put the data principals into a safe and secure place, where they can certainly assume that their data which is being processed by the various intermediaries and fiduciaries is not misused to get some gains[47] and certainly not used beyond the specified purpose[48] and legitimate use.[49] The Obligations are as follows.

A. The Data fiduciary can process the data, but only with the consent of the data principal for a lawful purpose[50] and a legitimate use.[51] The data fiduciary will be required to request for the consent, along with the purpose for such consent through a notice to the data principal.[52] If the data principal has anytime withdraws the consent, then the fiduciary or the processor shall within the reasonable time seize to process the data, except any law or rules for the time being in force in India allows such processing even after the withdrawal of the consent.[53]

B. The data fiduciary can only process the data for which the data principal has voluntarily given her consent.[54] The state instrumentalities can process the data for providing subsidy, benefit, service, certificate, license or permit.[55] State instrumentalities has great powers under this law, as they can process the data even without the consent of the data principal for the performance of any obligation under

[46] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §14
[47] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(o)
[48] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(za)
[49] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §4(1b)
[50] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §4(2)
[51] *Id.* at 36.
[52] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §5
[53] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(6)
[54] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(a)
[55] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(b)

any other law in India or for the interest of the sovereignty and integrity of India[56] or to get some information out of any individual in the name of interest of the state or following law.[57] Even in case of a medical emergency,[58] prevention of corporate espionage, or for the benefits and service sought by an employee,[59] the data can be processed without consent. The proposed draft of DPDP Rules, 2025 ('the rules') also suggest to expand the scope of the authority in terms of providing benefits, certificates, licenses, and permits to the individuals.[60]

C. The data fiduciaries shall be obliged to the provisions of this Act for the processing of personal data even in the case of any failure from the side of the data principal to assume its duties or In case of an agreement to the contrary.[61] The data fiduciary shall also use such technical and organizational measures[62] as necessary for the effective observance of the provisions of this Act. It must take such reasonable safeguards to protect the data of the data principal in its possession or with the data processor on behalf of it to prevent the breach of the data.[63] Even after all the safeguards such a data breach occurs, then the data fiduciary shall inform the board and each affected person about such a data breach,[64]so that reasonable steps can be taken to prevent further damage. The data fiduciary shall erase the personal data of the data principal on the fulfillment of the specified purpose unless such retention is not necessary under any law for the time being in force.[65]

D. It is the responsibility of the data fiduciary to provide the data principal with a grievance redressal mechanism in case any issue occurs to the data principal.[66]

E. The data fiduciary, must not undertake the processing of personal data of the child or a disabled person without the verifiable consent of the parent or the lawful

[56] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(c)
[57] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(d)
[58] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(f)
[59] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §7(i)
[60] Digital personal Data Protection Rules, 2025, Gazette of India, Rule 5 (Jan. 3, 2025).
[61] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(1)
[62] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(4)
[63] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(5)
[64] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(6)
[65] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(7)
[66] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(10)

guardian of such person.[67] It should also not undertake targeted advertising to the child, except if as the case may be prescribed under this Act.[68]

F. If a data fiduciary has been declared as a significant data fiduciary by The Indian Government under the section 10 (1) of the Act. Then such data fiduciary shall appoint a data protection officer,[69] who shall be based in India,[70] and he or she will be the one who will be responsible to the board of directors or similar governing body in case any issue arises with the data principal.[71]

G. The data fiduciary is obliged to appoint a data auditor who will evaluate the compliance of the provisions or rules made under this Act,[72] by the significant data fiduciary. It is also obliged to take a periodic data protection impact assessment[73] and other reasonable measures that are consistent with the provisions of this Act.[74]

VII. Cross Border Data Transfer: -

India's DPDP Act is a principle-based statute that delegates the details, procedures, and compliance specifics to delegated legislation issued before its enactment as law. Regarding the cross-border transfer of personal data, The Indian Government's stance on data localization has evolved after many deliberations and consultations. The first draft of India's data protection framework required a mirror copy of all sensitive and critical personal data to be stored within the territory of India which is already in possession with the entities outside India.[75]

Subsequent versions of the law progressively weakened this stance due to strong opposition from various stakeholders as it fundamentally disrupts online business operations. The Bill, 2021, permitted the transfer of personal data to certain

[67] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §9(1)
[68] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §9(3)
[69] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2a)(i)
[70] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2a)(ii)
[71] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2a)(iii)
[72] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2b)
[73] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2c)(i)
[74] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2c)(iii)
[75] Ministry of Electronics and Information Technology, Digital Personal Data Protection Bill, No. 113 of 2023, §. 40

countries 'whitelisted' by The Indian Government.[76] The final version took a different approach allowing personal data to be freely transferred to all countries except for those specifically identified by The Indian Government.[77]

Contrastingly, under the GDPR, data transfers are permitted to countries offering an adequate level of protection, as determined by the European Commission[78], through binding corporate rules[79] or by applying appropriate safeguards[80]. All these provisions under the GDPR establish the criteria for evaluating the permissibility of cross-border data transfers. Unlike the GDPR, the Act does not provide a basis for determining countries to which data transfers will be prohibited. Without mentioning any justifications like security standards, contractual clauses, or binding corporate rules, under the Act, The Indian Government will notify the restricted jurisdictions for transferring of data.

The Act, lays down certain exemptions for the restrictions on data transfers outside the country concerning certain processing activities.[81] The provision delineates specific scenarios where cross-border transfers of personal data, including countries notified by The Indian Government, are not subjected to restrictions. These exemptions are crucial for ensuring that legitimate uses of personal data are not hindered by overly restrictive regulations.

According to the Act, cross-border data transfers are necessary for enforcing legal rights or claims, such as in property disputes, matrimonial cases, immigration matters, and financial claims. It also allows for transfers concerning contracts with foreign entities, which is specifically relevant for the Indian outsourcing industry dealing with non-Indian personal data for foreign clients. Additionally, the Act allows transfer related to mergers, demergers, and acquisitions between Indian and foreign countries. It also allows for transfers to ascertain the financial position of a

[76] Ministry of Electronics and Information Technology, Digital Personal Data Protection Bill, No. 113 of 2023, §. 17
[77] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §16
[78] General Data Protection Regulation, 2016, A. 45
[79] General Data Protection Regulation, 2016, A. 47
[80] General Data Protection Regulation, 2016, A. 46
[81] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §17

defaulter to an institution and for regulatory, supervisory, or judicial functions.[82]

The Act, emphasizes that existing sectorial laws with additional requirements or higher degrees of protection will remain in effect.[83] It suggests that while The Indian Government's restrictions[84] serve as a baseline for data protection across all personal data categories, sectorial regulators have the authority to impose further restrictions as per the need for specific industry requirements. India has several sector-specific restrictions on cross-border data transfers, RBI's regulation on payment data, and other financial regulators such as SEBI and IRDAI have similar requirements for data related to transactions and insurance policies. Certain Government departments, the education sector, healthcare sector have guidelines that mandate the data to be stored within India to protect privacy, maintain confidentiality, and protect national interests.

VIII. Comparative Analysis: -

The GDPR[85] applies to establishments in the European Union (EU) that process personal data and also to organizations outside the EU processing personal data related to offering goods or services in the EU or monitoring individuals' behaviour.[86] The Act, also has both territorial and extra-territorial applications, however, under the Act offshore entities are exempted except for data security requirements, when processing personal data on behalf of a foreign data fiduciary and when the data only relates to foreign data principals.

The GDPR applies to personal data and processing activities, excluding anonymous data and personal use.[87] The Act, applies to digital and non-digitized personal data processing, excluding certain cases like personal use and data made public under Indian law. It also excludes certain processing activities relating to the enforcement of legal rights, mergers, and national security.

[82] *Id.*
[83] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §16(2)
[84] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §16(1)
[85] General Data Protection Regulation 2016, EU 2016/679, (Eng.)
[86] General Data Protection Regulation 2016, EU 2016/679, art. 3 (Eng.)
[87] General Data Protection Regulation 2016, EU 2016/679, art. 2 (Eng.)

GDPR defines personal data as information relating to an identified natural person or identifiable,[88] whereas, the Act, defines personal data as information about a natural person that can identify or relate to that person.[89]

The GDPR delineates "special categories of personal data" as information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for uniquely identifying a person, health information, and data on sex life or sexual orientation. It also includes personal data related to criminal convictions and offenses, which, although not categorized as special data, is subject to specific rules under EU or member state law. In contrast, the Act does not differentiate between categories of personal data and treats all personal data equally.

In the GDPR, a controller[90] is a natural or legal person, public authority, agency, or other body that determines the purposes and means of processing personal data, while a processor[91] is a party that processes data on behalf of the controller. A data subject is an identified or identifiable natural person. In contrast, the Act uses different terminology: a data fiduciary[92] is an individual, company, or entity that, alone or with others, determines how and why personal data is processed. A data processor,[93] on the other hand, is any entity or individual that processes personal data on behalf of a data fiduciary. The data principal[94] is the natural person to whom the data relates, including parents or guardians in the case of children or persons with disabilities. The Act, also introduces the concept of a consent manager[95], allowing data principals to manage their consent. Additionally, the Act identifies significant data fiduciaries[96] as specific classes of fiduciaries subject to additional obligations based on factors such as the nature and volume of data processed, risks to data principals, and threats to national security.

[88] General Data Protection Regulation 2016, EU 2016/679, art. 4(1) (Eng.)
[89] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(t) (India).
[90] General Data Protection Regulation 2016, EU 2016/679, art. 4(7) (Eng.)
[91] General Data Protection Regulation 2016, EU 2016/679, art. 4(8) (Eng.)
[92] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(i)
[93] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(k)
[94] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(j)
[95] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(g)
[96] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §2(z)

The GDPR outlines seven general principles, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability.[97] The Act, reflects similar principles, requiring personal data processing to be lawful and fair, with consent obtained through a clear affirmative act[98]. Data minimization is emphasized, limiting the collection of personal data to what is necessary.[99] Data should only be retained as long as necessary unless Indian law requires longer retention.[100] Purpose limitation ensures that personal data is only processed for specified purposes. Integrity requires data fiduciaries to ensure completeness, accuracy, and consistency of processed data. Confidentiality mandates data protection and security measures. Accountability requires compliance with provisions of the Act. Significant data fiduciaries must conduct audits and impact assessments as required by the Act and related Rules.[101]

The GDPR imposes specific requirements for obtaining consent from children under 16, or a younger age set by member state law, including obtaining consent from a parent or guardian for certain electronic services provided directly to children.[102] In contrast, the Act, defines a child as under 18 and requires "verifiable consent" from parents or guardians. It prohibits processing likely to harm a child's well-being or involves tracking, behavioural monitoring, or targeted advertising aimed at children. However, certain classes of data fiduciaries or purposes may be exempt from these restrictions, as determined by The Indian Government rules.[103]

The GDPR mandates that controllers and processors not based in the EU but subject to its regulations must designate a representative in the EU unless their processing activities are sporadic and do not involve extensive processing of sensitive data. Private entities must appoint a Data Protection Officer (DPO) only if their core activities include large-scale monitoring of individuals or processing of sensitive data. The DPO must possess the requisite independence and expertise to fulfil their

[97] General Data Protection Regulation 2016, EU 2016/679, art. 5 (Eng.)
[98] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §6(1)
[99] *Id.*
[100] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §8(7)(a)
[101] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10
[102] General Data Protection Regulation 2016, EU 2016/679, art. 8 (Eng.)
[103] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §9 (India).

duties and should have direct access to the highest levels of management. While outsourcing of DPO services is permissible, EU regulators recommend that DPOs be located within the EU.[104] In contrast, the Act mandates that all significant data fiduciaries appoint DPOs based in India.[105] These fiduciaries are determined by The Indian Government based on various factors such as the nature and volume of data processed and potential risks to data principals and national interests. The DPO is accountable to the significant data fiduciary's board of directors or governing body, with no explicit skill requirements outlined. Additional guidelines for DPO appointments may be provided through rules under the Act.

The GDPR requires controllers to report breaches to the DPA within 72 hours unless the breach poses no risk to individuals, and notifications can be incremental. Individuals must be notified without delay if the breach is likely to result in significant harm, and processors must promptly inform controllers of breaches.[106] In contrast, the Act requires data fiduciaries to report breaches to the board and affected data principals according to rules, with the reporting timeframe to be determined by regulations.

Regarding penalties, the GDPR allows member states to impose criminal sanctions for breaches, along with administrative fines of up to 20 million euros or four percent of global annual revenue. DPAs can also issue injunctive penalties, such as blocking processing or requiring data deletion, and individuals can seek compensation through the Courts, with representative actions possible for groups of individuals. However, the Act does not include criminal penalties but enforces monetary penalties for significant breaches, considering factors like the severity and duration of the breach and whether it resulted in any gain or loss. The board may accept voluntary undertakings from data fiduciaries during compliance proceedings, and The Indian Government can direct agencies or intermediaries to block access to a data fiduciary's services for repeated violations.

The Act, grants The Indian Government the authority to exempt The Indian Government agencies from certain provisions in the interest of national security and

[104] General Data Protection Regulation 2016, EU 2016/679, sec. 4 (Eng.)
[105] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §10(2)(a) (India).
[106] General Data Protection Regulation 2016, EU 2016/679, art. 33 (Eng.)

public order. It means that in some cases, the rights of data principals and obligations of data fiduciaries (excluding data security) will not apply, such as in processing for the prevention, investigation, and prosecution of offenses. The Act, also does not mandate the deletion of personal data after the processing purpose has been fulfilled. These exemptions could potentially lead to The Indian Government agencies collecting data about citizens for surveillance purposes, creating comprehensive profiles. It raises concerns about whether these exemptions would pass the proportionality test.

In the United Kingdom, the data protection legislation enacted in 2018 includes exemptions for national security and defense purposes.[107] However, activities like the bulk processing of personal data by The Indian Government bodies for intelligence and law enforcement purposes are governed by the Investigatory Powers Act of 2016.[108] Authorization for such activities is granted by the Secretary of State (Home Minister), subject to prior approval by a Judicial Commissioner, and must demonstrate necessity and proportionality. There are limits on data retention beyond the warrant period, and the law also allows for parliamentary oversight.

IX. Critique and Recommendations: -

The JPC under its report had given some recommendations regarding the Data Protection the Bill, 2019 concerning privacy rights and the effective operation of significant data intermediaries to circumvent data abuse in the digital age. The report laid down the foundation of legislation meeting global standards making India stand on a higher pedestal securing individual data and addressing contemporary digital issues. India had over 700 million active internet users aged two years and above as of December, 2022[109] and the number of internet users in India was forecast to continuously increase between 2024 and 2029 by in total of 60.5 million users.[110] JPC prognosticated the need for a stern legal framework to

[107] Data Protection Act 2018, c. 12, Ch. 3 (Eng.)
[108] Investigatory Powers Act 2016, c. 25 §§ 6-8 (Eng.)
[109] MINISTRY OF EXTERNAL AFFS., GOV'T OF IND., REPORT OF ECONOMIC DIPLOMACY DIVISION: INDIA HAD OVER 700 MN ACTIVE INTERNET USERS BY DEC '22, 25 (2023), https://indbiz.gov.in/india-had-over-700-mn-active-internet-users-by-dec-22-report/.
[110] J. Degenhard, Internet Users in India 2014-2029, STATISTA (Jan. 30, 2024), https://www.statista.com/forecasts/1144044/internet-users-in-india.

address the distressing situation of the data principals in the tremendously growing digital market, running on data working as fuel to it.

The recommendations are enumerated herein below: -

A. Right to be forgotten

Right to forget was given as a recommendation[111] by the JPC with the objective that, whatever the data is either The Indian Government data fiduciary or with the independent data fiduciary shall be deleted after the fulfilment of the purpose required. By this, a check and balance could be put on The Indian Government and the fiduciary concerned, so that they do not use such data for extra unauthorized purposes and the extra burden of the protection of the data over the fiduciary can also be avoided. The recommendation was ignored by the legislature while framing this Act and a provision was made for the retention of the data by the fiduciary even if the consent was withdrawn by the data principal.[112] This Act, does not elaborate any procedure or provisions about how the data which is being retained should be regulated, which in turn imposes a threat to the right to privacy of the individual. However, proposed draft of the Rules, 2025 suggested that, the data of data principal will be deleted if the he or she does not interact with the data fiduciary for the period of three years.[113] The rules also encompassed the exception of lawful purpose, which means, the above stated obligation can also be over passed where a lawful purpose exist. Therefore, it gives arbitrary power to The Indian Government agencies to put 360º surveillance over any person. Make some amendment under this Act or specify some stringent procedure through rules under this Act which will regulate, the retention and retained data so that it cannot be arbitrarily used.

B. Exemption to The Indian Government Agencies

The provisions of this Act, exempts The Indian Government agencies in the

[111] SOFTWARE FREEDOM L. CTR., SUMMARY OF JPC RECOMMENDATIONS ON PERSONAL DATA PROTECTION BILL, 2019, 25, https://sflc.in/summary-jpc-recommendations-personal-data-protection-bill-2019/.
[112] *Supra* note 64 at 6.
[113] Digital personal Data Protection Rules, 2025, Gazette of India, Rule 8 (Jan. 3, 2025).

name of the state and its instrumentalities from the application of the provisions (including the provision of consent) of this Act for the processing of the personal data of the data principals for the performance of any function in the name of the sovereignty, integrity, and security of the state.[114] It also gives power to The Indian Government through its instrumentalities to process the data of the data principals without their consent for the disclosure of any information.[115] Also, the proposed Rules, 2025 suggested to widen the authority of The Indian Government, wherein they were exempted from the application of this Act, if that are processing the data of the people for the research, archiving or statistical purposes.[116] These provisions of this Act, provide The Indian Government with the undisputed powers to process the data of any individual according to their wish which is not based on any statutory procedure. JPC recommended[117] that the 'such procedure' should be defined under this Act which can reasonably and fairly regulate the processing of data after such exemptions, because in the absence of a defined procedure, the powers given under this can be arbitrarily used which will in turn violate the Right to privacy as well as the principle of Fair Governance. Make a procedure through the rules under this Act, which will serve the purpose of this recommendation by the committee.

C. Proportionality test

Include, a proportionality test[118] in this Act or rules which will be made under this Act which can determine, to what extent The Indian Government or independent data fiduciary can retain or process the data of the data principal for any law time being in the force. It will put a restriction upon The Indian Government and its instrumentalities unrestricted powers under this Act.

D. Damages to the data principal

This Act, imposes several penalties upon the independent data fiduciary and data

[114] *Supra* note 56 at 6.
[115] *Supra* note 57 at 6.
[116] Digital personal Data Protection Rules, 2025, Gazette of India, Rule 15 (Jan. 3, 2025).
[117] *Indian Parl. Deb., Lok Sabha No. 17, at (Dec. 16, 2021) (Recommendation No. 56 – 'such procedure' shall be defined in the explanation under clause 35 of the Digital Personal Data Protection Bill, 2019).*
[118] *Supra* note 117 at 10.

processor through the schedule[119] made under this Act for the breach of any obligation that needs to be observed under this Act or any regulation that needs to be followed by the data fiduciary, and the imposed fine shall be deposited to the consolidated funds of India.[120] Does this penalty make any difference for the data principal who has suffered the actual loss of data, the answer is non-affirmative. Give a part (compensation) of the penalty which is imposed on the fiduciary, to the data principal which will make a difference for the people who have faced loss and will relieve them from such loss.

E. Inclusion of juristic person

The Data Protection Authority made under the Act, only has bureaucrats who hold membership and decide the cases, committee under its report recommended adding an attorney general of India, Directors of IIT and IIMs who can also add their expertise and diverse experience in the settlement of disputes, framing of rules, advisories.[121] The committee also recommended the inclusion of lawyers into the appellant tribunal, the objective behind it was that, this Act bars the jurisdiction of the civil Court and in turn gives the power to the appellant tribunal, which is ultimately serving the role of a Court. The non-inclusion of lawyers is irrational because in Courts, juristic personalities are there who serve justice and settle the disputes by the way of applying their knowledge and expertise in the various nuances of the law, Where as in the tribunal, the cases of right to privacy would be dealt by people who does not holds substantial jurisprudential knowledge. These decisions will not only prejudice to the notions of justice, but I will also make an unreasonable and non-sustainable impact on the society by which, the interest of the masses will be at risk. Amend the Act, which will in turn make a provision for the addition of more posts for the addition of lawyers or retired judges of the High Court or the Supreme Court judges who can put a wide view of the legal framework without concluding.

[119] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §33(1)

[120] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §34

[121] *Indian Parl. Deb., Lok Sabha No. 17, at (Dec. 16, 2021) (Recommendation No. 63 – Inclusion of academic, technical, and legal experts in the committee under the Digital Personal Data Protection Bill, 2019).*

F. Liability of State instrumentalities and authorities

The Act, only imposes penalties on private data fiduciaries but it does not impose any obligations and penalties on fiduciaries of a state that collects and processes the data of the individual at a much grand level as compare to private once. It gives the state instrumentalities exemptions from all the obligations, and if there will not be any obligations, in turn there will not be any penalty for the breach of the rules. Issue rules and procedures or apply the similar rules equally without any exception for regulating, processing and protection activities undertaken by the state instrumentalities[122] and impose penalties if the specified procedure which deals beyond exception gets breached by The Indian Government data fiduciary.

The above-mentioned recommendations are analogous to the recommendations made by the JPC. They were not considered by The Indian Government while making the provisions of this Act. Apart from the same, certain other provisions of this Act need to be critically analysed and need future recommendations so that the effective realization of the true essence of this Act can be possible.

G. Lawful Purpose over the Consent

The Act, was formulated to uphold the Right to Privacy which can also be traced back from the historical and legislative evolution of the Act. The consent, which is the most crucial provision of this Act, provides the data principal with the autonomy of giving or refusing the consent for data processing which ultimately makes her able to practice the right to privacy.[123] But under the same provision, The Indian Government and its instrumentalities have been given with the overriding powers over the Right to privacy of the individual. It enables The Indian Government to process the data of the data principal even without her consent for the lawful purpose.[124] The aforementioned arbitrary power not only poses a risk to her privacy but also curbs the Right to Life & Liberty,[125] as the

[122] *Indian Parl. Deb., Lok Sabha No. 17, at (Dec. 16, 2021) (Recommendation No. 85 – Procedure to regulate data with the Government must be specified under the Digital Personal Data Protection Bill, 2019).*
[123] *Supra* note 35 at 5.
[124] *Supra* note 53 at 5.
[125] INDIA CONST., art. 21

Right to privacy was upheld as a sub-right under Article 21 of the constitution in the case of K.S. Puttuswami V. Union of India, 2017.[126] Amend, the Act in a way, which can reverse this flaw and which can empower the data principal to effectively practice her right to privacy as a crucial fundamental right.

H. Faulty in Regulating the risk of The Indian Government instrumentalities

The Act, gives immense power to The Indian Government and its instrumentalities in the name of the integrity, sovereignty, and security of India. They can process the data of any individual without their consent and inform them about the same which is against the right to privacy. After assuming all these privileges, The Indian Government becomes the largest data fiduciary, and when they process the data arbitrarily they also incurs a responsibility to protect the data which is with them. There are high chances of a data breach in such cases and this Act, fails to recognise the risk that would be incurred by such Indian Government instrumentalities.[127] This Act, also fails to recognize the risk that would lie upon the data principal as after such a data breach she can be easily trapped in cybercrimes by the means of smart growing technology and artificial intelligence which can cause her unimaginable harm or damage.

I. Cross Border Data Transfer

The Act, allows the transfer of data outside the territory of India but prohibits the transfer of data to countries that are prohibited by The Indian Government through the notification. This way of prohibition does not ensure the protection of the data of the data individuals who are based in India, because their no surety that the countries with whom data has been shared sincerely observe adequate data privacy standards or that they by themselves will not misuse such data. In such cases, cybercriminals who won't be able to breach the data from Indian servers because of adequate observance of security standards can breach the same data from the countries who won't be observing adequate standards to protect against such data breaches. In such cases, even when observing proper

[126] *Supra* note 12 at 2.
[127] PRS LEGISLATIVE RESEARCH, DIGITAL PERSONAL DATA PROTECTION BILL, 2023, https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023#_edn8.

standards in India, the data principals still face losses because of such breaches outside India. Amend these provisions and allow data export to those countries which would be able to establish that they assume proper security standards and, undertakes that they would be directly responsible in case of such data breach and will cooperate accordingly to prevent further losses.

J. Violates the Right of the Data Principal

The Act, gives certain rights to the data principal which empowers them in a digitally growing era. While exercising such right the data principals can seek the summary of the data processed and the processing activities undertaken by the data fiduciary and the processor. In case any data has been shared by the data fiduciary with another data fiduciary, the data principal can also seek information about such data.[128] In contradiction to these rights, The Indian Government has been given an exemption under these rights through which they can seek the data of the data principal from another data fiduciary without giving any power to the data principal to exercise such rights as elaborated herein above.[129] By this exemption, The Indian Government has been assigned with undisputed power by which they can seek the data of any person without their permission and violates the true essence of this Act. Amend the exception given under this Act and put the rights of the data principal in terms of the informed consent at higher pedestal.

K. Duties for Data Principal

The Act, elaborates certain duties for the data principal by which they will be obliged to comply with all the laws which are applicable in the exercise of their rights.[130] Which means that they have to obey the arbitrary powers of The Indian Government in respect of the data processed. They are also obliged not to impersonate another person while giving information for specified purposes. The obligation causes discomfort and issues to the female data principal because it is sensitive for them to share such personal data in the times of artificial

[128] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §11(1)
[129] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §11(2)
[130] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §15

intelligence and other technologies where they can easily be victimized. Amend this provision of the Act to give more autonomy to the data principal.

L. Other Exemptions are arbitrary

The Indian Government is exempted from the provisions of this Act. They are allowed to process the personal data of the data principal without their consent or any right for the enforcing of any legal right, prevention, detection, investigation, or prosecution of any offense, in the interest of the sovereignty, integrity, and friendly relations with a foreign state, maintenance of public order or preventing incitement to any offense.[131] The parameters and the procedure to be observed for all these exceptions are not specified under this Act.[132] Which gives The Indian Government unregulated power and in cases where the appeals will be made to either the board or the tribunal against such arbitrary use of power, the impartiality in the decision also cannot be ruled about because the panel will consist of the employees who will be appointed by The Indian Government. This Act, also gives unregulated powers to The Indian Government in the case of a medical or national emergency to process the data of the people with their informed consent.[133] All these exemptions cause an apprehension in the mind of the people that their right to privacy is unprotected and can be violated by The Indian Government anytime. This imposes a threat to the democracy and right to privacy of the individual. Hence, amend these provisions in the light of the democratic rights of the people, so that more transparency and accountability can be achieved.

M. Undemocratic and arbitrary protection

This Act, lays down the provision of no suit, prosecution, or legal proceedings against The Indian Government or board or any of its members, officers, or employees for anything which is either done or intended to be done with good faith.[134] These provisions completely bar the data principal from exercising any

[131] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §17
[132] *Supra* note 119 at 11.
[133] *Supra* note 58 at 6.
[134] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §35

of the rights against The Indian Government data fiduciary and agencies. The word 'intended to be done' by its liberal interpretation means that even in case any fault arises on the part of The Indian Government in the event of a breach of data or violations of any rights, The Indian Government will have the unchallengeable immunity which saves it from any retaliation. Also, the extent of good faith is not defined under this Act, so it is left at the discretion of The Indian Government to decide what action is in good faith or not. Struck down this provision of the Act and subject The Indian Government equally to the provisions of this Act and liability if any arises.

N. Arbitrary powers of The Indian Government

The Indian Government under this Act, may call for any data from any data fiduciary and intermediary without informing the respected users of that data.[135] It is also allowed to remove any difficulties by the way of any notification in the official gazette, arising in the proper implementation of the provision of the Act.[136] By the way of liberal interpretation of the language of this provision, this Act, specifies that if any hindrance by the way of any law for the time being in force restricts or stops The Indian Government in the processing of any data The Indian Government can remove such restriction or hindrance by its discretionary powers. The undisputed and unregulated power of The Indian Government is a threat to the democracy and the right to privacy of the individual and for such reasons, regulate the powers enumerated under this Act and make provisions for such regulation by the way of stringent rules.

X. Conclusion: -

The endeavors have been made to comprehensively evaluate the Act in the light of constitutional provisions, JPC recommendations and GDPR under this article. With the help of the analysis, we came to a conclusion that, the several provisions of this Act, are in the gross violation of the constitutional principles and it gives arbitrary and undisputed powers to The Indian Government, by the virtue of which it can

[135] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §36
[136] Digital Personal Data Protection Act, No. 22, Act of Parliament, 2023, §43

override the rights of the data principal enumerated under the Act and the right to privacy guaranteed under the constitution. The provisions of this Act were made with the objective that, this law can achieve the global standards, but it failed to do so. The GDPR, a globally recognized law which is a milestone in the spectrum of digital laws contains a special provision about the cross border data transfer, which says that the data should be shared with only those countries which have effective data breach protection systems. It was not considered by the legislature while making of this Act and allows the cross border data transfer by a simple notification by The Indian Government without any evaluation procedure. It also ignored the crucial recommendations made by the JPC. Like, data localization, inclusion of juristic personality in the panel etc. It makes us conclude that, it is still not effective in realization of the objective with which it was made and needs further amendment, either in Act or through rules to make India a global hotspot for Data transaction.