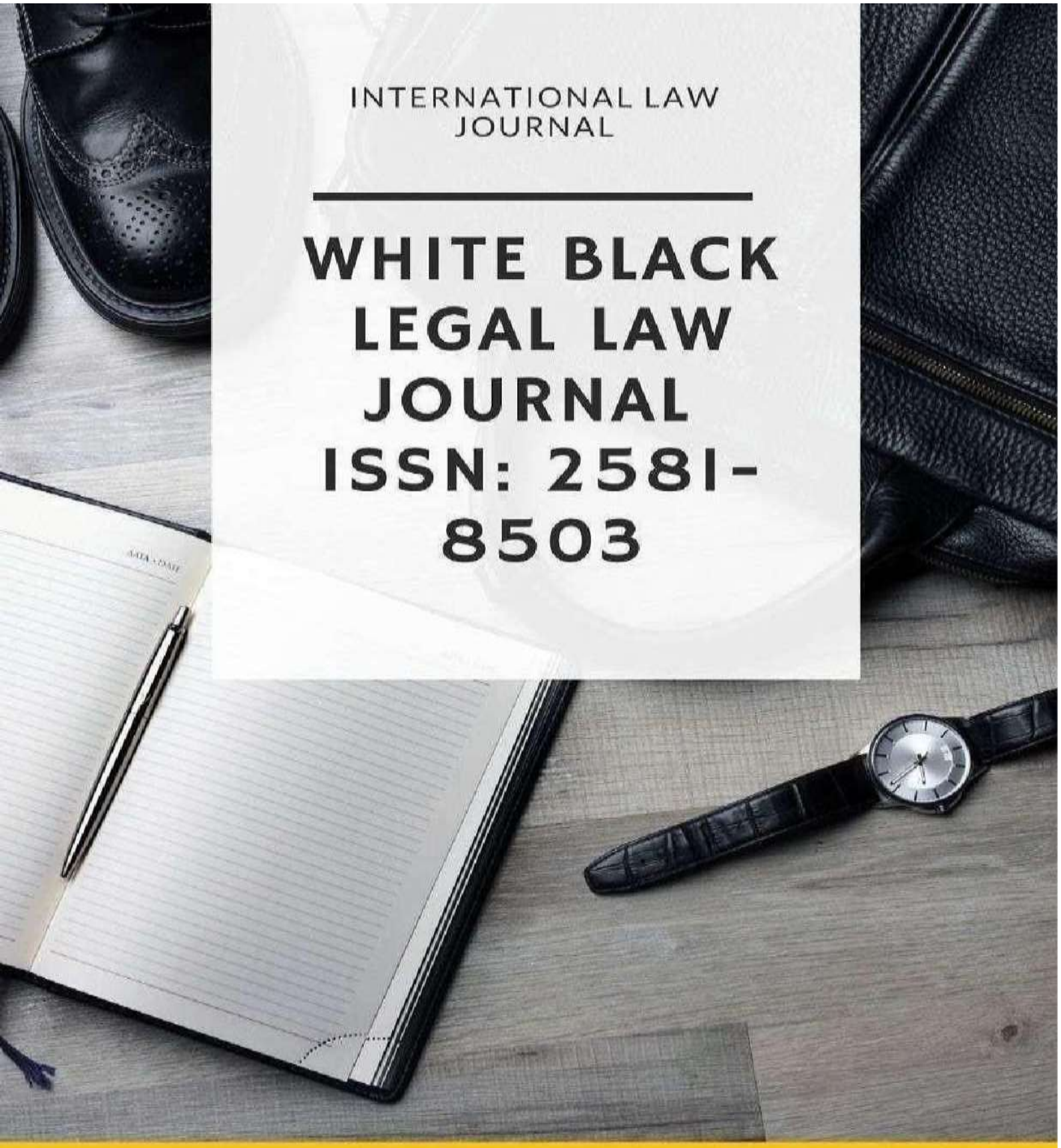

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

THE DPDP ACT, 2023 EXAMINED - BRIDGING GAPS: STRENGTHENING INDIA'S PRIVACY LAW

AUTHORED BY - REETIKA SHARMA & ISHA UPADHYAY
(KES' Shri Jayantilal H. Patel Law College, Mumbai)

ABSTRACT:

The Digital Personal Data Protection (DPDP) Act, 2023, represents a landmark shift in India's data privacy landscape, addressing the limitations of previous legal frameworks such as the IT Act, 2000. This paper critically examines the Act's key provisions, including consent mechanisms, data fiduciary obligations, data localization, and the role of the Data Protection Board. It evaluates the Act's impact on individual rights, business compliance, and national security while identifying ambiguities, enforcement challenges, and the discretionary powers granted to government authorities. It explores the Act's implications on individual rights, business compliance, and national security while identifying existing loopholes, such as ambiguity in consent definitions, government discretion, and enforcement challenges. A comparative analysis with the European Union's General Data Protection Regulation (GDPR) highlights differences in data subject rights and enforcement mechanisms, offering insights for legislative refinement. The study concludes with actionable recommendations to enhance the DPDP Act, emphasizing clearer definitions, stronger compliance measures, and improved cross-border data safeguards to foster a secure and innovation-driven digital ecosystem in India.

INTRODUCTION:

Personal data is sacrosanct, and it is essential to protect it. The emergence of New Age Technologies, particularly AI's interference with personal data without accountability has led to societal concerns. As our dependence on digital technologies continues to grow, so does the need for robust digital data protection. In this data journey, the fluid nature of data is a matter of concern; data is capable of quietly flowing in cross-border circulation as well as in internal ecosystems. Data does not only mean to an individual data but it is also about the data of companies as well as data that are important for national security too. Thus, the coverage of data does not stick to micro level but it has far reaching impact at macro level, if not protected well. Data Protection is the need of an hour. We can't deny the fact that our legislators had

formulated many laws like IT ACT 2000 and others to secure our data but the questions on this act is about: at what extend and is that act actually efficient enough to avoid the potential threat of the breach of data .The answer to these questions for some extend is in negation.
So the legislators had come up with the Digital Personal Data Protection (DPDP) Act 2023.

We will delve deep into what this Act is all about and does it actually resolve the loopholes of previous acts or does still there any intricacy in it too. So we will critically examine the Act, and also discuss the potential solution to some extent in resolving the issues that persist.

- Our first question, whenever we discuss or even mention the word Privacy, is ***What does this term Privacy*** means?

  The meaning of this term is very subjective in nature but we will going to discuss this idea in general perspective:

  Data privacy refers to the protection of personal information, ensuring that individuals have control over how their data is collected, processed, stored, and shared. It encompasses the right of individuals to keep their information private and secure, limiting unauthorized access or use by others.

  "Data privacy" usually refers to the handling of critical personal information, also called "personally identifiable information" (PII). This information can include social security numbers, health records, and financial data, including bank account and credit card numbers.

  In a business context, data privacy goes beyond the PII of employees and customers

- Then our second question: **Why data privacy is so important?**

  The world is now full of technology. Every individual has left their data somewhere and everyone of us have imprints on this technological world. As we discussed earlier that Data is not only limited to Individual but it also covers economic, societal and national data. And these parameters are discussed below:

  Digital Data Protection

1. Individual Empowerment and Privacy:

   Right to privacy - Digital data encompasses personal information, and its protection aligns with the fundamental right to privacy enshrined in the Indian Constitution.

   Control over personal data - Individuals deserve control over how their data is collected, used, and shared. Data protection empowers them to make informed choices

and prevent misuse.

- Mitigating risks - Unprotected data exposes individuals to privacy violations, identity theft, financial scams, and discrimination based on personal information.

2. Economic Growth and Sustainability:

- Building trust in the digital economy - Data breaches and privacy scandals erode trust in digital platforms and hinder online transactions, impacting e-commerce, digital payments, and other sectors.
- Protecting intellectual property - Sensitive data related to businesses, innovations, and trade secrets needs protection to encourage investment and fair competition.
- Cyber security resilience - Strong data protection practices enhance cyber security, reducing business disruptions and financial losses due to cyber attacks.

3. Social Development and Inclusion:

- Promoting responsible innovation - Data-driven initiatives in healthcare, education, and social welfare require ethical frameworks to ensure data security and prevent discrimination.
- Bridging the digital divide - Addressing data privacy concerns can encourage participation from vulnerable populations hesitant to engage in the digital space due to privacy fears.
- Combating online harms - Data protection measures help tackle cyber bullying, online harassment, and the spread of misinformation, fostering a safer online environment.

4. National Security and Sovereignty**:**

- Protecting critical infrastructure - Data related to national security, defense ,and essential services needs, robust protection from cyber threats and foreign espionage.
- Counter cybercrime - Strong data protection laws and international cooperation help combat cybercrime across borders, ensuring national security and international stability.
- Data localization - Balancing the need for global data flows with safeguarding sensitive information within India's borders is crucial for maintaining national sovereignty.
- Targeted Attacks - Critical infrastructure, government agencies, and businesses face

targeted attacks from state- sponsored actors or cybercriminals seeking strategic advantages, such as spear-phishing campaign targeting a government agency's email accounts to steal classified information.

➢ Navigating the Challenges of Data Protection in a Digital World

Now ,if privacy is so crucial for India and the world ,what are the challenges we can face with the breach of Data. We will only going to have a brief mention of the challenges, as our topic mainly concerned about the DPDP Act and its Loopholes. So few of them are mentioned below:

- Cyber security Attacks & Data Breaches and Leaks:

  Data breaches can lead to identity theft, financial fraud, and the exposure of personal information, causing significant harm to individuals or organization's reputation.

- E-commerce and Digital Payments Risks :

  These include compliance with stringent cross-border data transfer regulations, the need for data minimization and clear user consent, and implementing robust data security measures to protect sensitive payment information. Additionally, businesses must navigate complexities in managing third-party accountability, handling user rights like data portability and erasure, and safeguarding sensitive personal data (SPD).

- Data Localization Challenges:

  Data localization requirements may present challenges in ensuring secure storage and management of data within India, particularly for organizations with complex data processing operations.

- Lack of Awareness:

  Many individuals may lack awareness of digital privacy risks, safe online practices, and the importance of securing personal information, such as Consumers may also be unaware of their rights under the Act, such as data portability and the right to erasure, leading to potential misuse of their data.

- Emerging Technologies:

  The adoption of emerging technologies such as artificial intelligence (AI), machine learning, and blockchain introduces new privacy challenges, including algorithmic

bias and data manipulation, cross-border transfer of data, compliance with local privacy standards, and the evolving nature of cyber threats

- The fourth question that next arises is that: ***Do we have any act/law to regulate our data breach and ensure protection?***

It's also a wise decision to thorough ourselves with previous laws for having a better understanding of present legislation and to have better critical understanding.

In India, the concept of Data protection has evolved significantly over the past decade. Initially, the Information Technology Act of 2000, along with its amendment in 2008, laid the groundwork by ***addressing information security rather than comprehensive data protection.***

The IT Act has a narrow scope in addressing emerging issues like data breaches, cyber threats, and privacy violations in the digital sphere making it one of its major drawbacks. The Act does not contain specific provisions that would govern how businesses would gather, store, and use people's personal information, nor does it establish clear standards for guaranteeing people's consent and control over their data. Additionally, the 2000 Act also falls short in addressing the challenges posed by cross-border data transfers, data localization, and cutting-edge technologies like artificial intelligence and machine learning.

Moreover, the concept of data protection and privacy has been debated in the judicial courts with some addressing it as a fundamental right. In contrast, others were not admitting it as a right under Article 21 of the Indian Constitution.

The landmark judgment of the top Court in ***Justice K.S. Puttaswamy (Retd.) & Ors. v. Union of India*** in 2017, recognizing the right to privacy as a fundamental right, accelerated legislative efforts. This led to the drafting of the data protection bill, resulting in the introduction of the Digital Personal Data Protection Act of 2023.

T**he Digital Personal Data Protection Act, 2023 (DPDPA),** marks a significant milestone as India's first comprehensive legislation on data protection. This Act regulates the collection, use, and disclosure of personal data. Until this Act is fully operational, the Information Technology Act, 2000 (IT Act), and the Information

Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, continue to govern the Indian data protection framework.

- After this our fifth question is: ***What are some important features of DPDP Act,2023?***

  The DPDP Act builds upon its predecessor, which was the 'Digital Personal Data Protection Bill, 2022' released in November, 2022 ("2022 Bill"). While preserving its core concepts, the DPDP Act introduces strategic adjustments, some of which are minor, yet others are more substantial. And will critically examine about: ***What are the loopholes of this Act?***

1. CONSENT:

   Section 6. *(1) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.*

   (3) Every request for consent under the provisions of this Act or the rules made there under shall be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act.

   (4) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

   (5) The consequences of the withdrawal referred to in sub-section (4) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

   (g) "Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and

withdraw her consent through an accessible, transparent and interoperable platform

(7) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

(8) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

(9) Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.

(7) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—

(a) erase personal data, upon the Data Principal withdrawing her consent or as soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier;

The problem with privacy laws is that the definition of consent is not clear,what actually consent constitute of? Here we are also concerned for those data principals who are not aware of the importance of consent or rather say that themselves didn't give their consent. It can be better understood by the following example: Who would make her aware of all the circumstances when she has to initiate a data change, especially if she is, say, staying in a remote tribal village of the country and had given her data for applying for education elsewhere in the country?

If this digital native had gullibly trusted someone else to fill her education form on her behalf and her details were inadvertently inaccurate; would she be fined INR 10,000 for 'supplying' inaccurate information? Whether she is able to contextualized the consent policy and according to her level of understanding?

As well as in how much time the consent manager take to withdraw the consent as it is mentioned as may be prescribed, which again shows ambiguity in procedure being followed.

Further in section 7(a) what does the term reasonable means, the term itself shows the discretion ,which is sceptical to prejudice .

Section 9. *(1) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner*

as may be prescribed.

The verifiable consent, what does this term means whether it is any kind of document or which method might be used to securely get the consent.

Importantly, it requires such companies to get "verifiable consent" from parents before processing children's data. This not only takes away agency from teenagers by restricting their ability to access websites without parental consent but also puts companies in a tough spot as they will have to carry out some form of age verification (which itself would require collecting personal data such as government-issued IDs) of all their users. to ensure that they are not collecting personal data of any children without parental consent. The Bill allows for some companies to be exempt or have a lower age threshold if they process children's data in a way that is "verifiably safe." But it is not clear what fits this criteria and it creates two different standards for companies processing children's data. A seventeen-year old and an eight-year old should not be treated the same and a graded approach should be adopted by the Act.

2. CLARITY:

The Act applies uniformly to both sensitive data and non-sensitive data, including sensitive personal data. The lack of categorization of personal data into sensitive data and non-sensitive data is also created the problem of clarity and possibility of subjective interpretation ,which should not be done. As well as there are many terms/ definitions which are also not clear or scope is not particularly defined as discussed above.

3. DATA LOCALIZATION:

Section 3. *Subject to the provisions of this Act, it shall—*

(a) apply to the processing of digital personal data within the territory of India where the personal data is collected—

(i) in digital form; or

(ii) in non-digital form and digitised subsequently;

(b) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

Where would the personal data of digital natives be stored?

The fact that the DPDP Act allows data to flow freely to any country (except those on a 'negative list' to be specified by the government) is very liberating. However, the Act does not explicitly insist either on data localization or on its storage outside India. What is the implication of this ambiguity?

4. DATA PROTECTION BOARD:

Section 28. *(1) The Board shall function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed.*

(2) The Board may, on receipt of an intimation or complaint or reference or directions as referred to in sub-section (1) of section 27, take action in accordance with the provisions of this Act and the rules made there under.

The appointment, powers, discretion etc are caution.

A) In its present format, DPB is not a regulatory body and is restricted to only supervising data breach prevention, ordering corrective action, conducting investigations, and imposing fines for legal non-compliance. It lacks the authority to request information to monitor how enterprises run, or to issue binding regulations, rules, or conduct codes, which may limit its ability to address emerging issues and challenges in the data protection landscape.

B) ***Section 19.*** *(1) The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify.*

(2) The Chairperson and other Members shall be appointed by the Central Government in such manner as may be prescribed.

(3) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy,

law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

The board is composed of six members and a chairperson, all of whom are appointed by the Central Government on the recommendation of a selection committee. This may raise concerns about the potential influence of the government on the DPB's decisions and actions.

C) ***Section26.*** *The Chairperson shall exercise the following powers, namely:—*

(a) general superintendence and giving direction in respect of all administrative matters of the Board;

(b) authorise any officer of the Board to scrutinise any intimation, complaint, reference or correspondence addressed to the Board; and

(c) authorise performance of any of the functions of the Board and conduct any of its proceedings, by an individual Member or groups of Members and to allocate proceedings among them.

The DPB's chairperson is empowered to authorize any board member to execute "any of the functions of the board and conduct any of its proceedings" which might not prove to be an impartial process. The act also fails to specify and preserve an internal separation of functions between the members conducting inquiries and the authority of the chairperson.

5. CG EXCESSIVE DISCRETION:

A) A lot will depend upon how well the government upholds privacy rights especially since the central government has a huge amount of discretionary control over substantive matters such as:

Although there are situations where this is justified, such as during emergencies or disasters, but the legislation expands the range of these situations and the state gains considerable power over the digital natives.

For instance, if the Board has to investigate a misuse of personal data of the government, there will be a conflict of interest because the government is essentially the judge, jury, and executioner of its non-compliance.

For example : The Aarogya Setu app collects anonymized geolocation data, linked with personal details like profession, age, and sex, without clear justification. It lacks informed consent, and while the government mandates its use under the Disaster Management Act with penalties for non-compliance, there's no clarity on data security measures. The app's Terms disclaim liability for unauthorized data access, raising concerns about privacy. The Supreme Court has ruled that the Right to

Privacy is not absolute, but in this case, the government's actions seem excessive and unjustified.

B) ***Section 17(5),*** *The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification.*

The Act gives power to the Central Government to exempt any data fiduciary from complying with any part of the Act for a certain period, not exceeding five years from the date of commencement of the Act in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, or for preventing incitement to the commission of any cognizable offence relating to the above matters. The fear remains that in certain situations, the government's freedom may work against the privacy safeguards or the interests of the digital natives.

(3) The Central Government may, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (3) and (7) of section 8 and sections 10 and 11 shall not apply.

C) Similarly, the government can exclude companies from various regulations governing the handling of children's data by using its arbitrary rule-making powers.

6. DILUTION OF RTI:

There is a correlation between the data protection and public interest.

This data protection could make public authorities more cautious in releasing personal data under the RTI Act, potentially leading to a narrower interpretation of what constitutes 'public activity or interest'. That's why it's very crucial to have clarity with terms and scope. The DPDP Act amends the RTI Act of 2005 to state that the government is not obliged to disclose information that relates to personal information. Earlier this could be overridden in case of larger public interest. By making this amendment, the Act weakens the RTI Act as the government has one more broad ground to deny information requested.

"A new era of corruption will be introduced as personal data like assets and liabilities, education qualifications of corrupt officials, won't be sought under RTI

Act," MP Adhir Chowdhury pointed out in the parliament.

7. BUREAUCRATIC PROCESSES:

The DPDP Act introduces compliance requirements for data fiduciaries (Sections 8 and 10 outlines the general obligations and additional obligations for significant data fiduciaries), which could add layers of bureaucratic review for RTI requests involving personal data. This might lead to delays or additional hurdles in the RTI information request process, especially where personal data is involved.

8. IMPACT ON BUSINESS:

Small and medium enterprises (SMEs), in particular, may struggle with the high costs of compliance and the technological upgrades necessary to meet the new standards. One key issue is the vague definition of "sensitive personal data" and "data fiduciaries," which may create confusion on compliance requirements. For example, businesses may struggle to classify data correctly or determine who is responsible for securing it. Another loophole is the lack of clear enforcement mechanisms or timelines for data audits, potentially leading to inconsistent application of the law. These ambiguities could lead to increased legal risks and operational complexities for businesses as they navigate compliance.

9. RESEMALANCE CONTROVERSIAL SECTION 69A OF THE IT ACT:

Section 37. *(1) The Central Government or any of its officers specially authorised by it in this behalf may, upon receipt of a reference in writing from the Board that—(b) advises, in the interests of the general public, the blocking for access by the public to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to Data Principals within the territory of India, after giving an opportunity of being heard to that Data Fiduciary, on being satisfied that it is necessary or expedient so to do, in the interests of the general public, for reasons to be recorded in writing, by order, direct any agency of the Central Government or any intermediary to block for access by the public or cause to be blocked for access by the public any such information.*

The government's power to block content goes beyond the already controversial

Section 69A of the IT Act: Under Section 37, the government can block access to websites or content on advice from the Data Protection Board in case of repeated offences by the entity or in the "interests of the general public." This broad phrasing goes beyond the already controversial powers of the government to block content under section 69A of the Information Technology Act of 2000. Additionally, the powers of a Data Protection Board to advice on blocking "content" is problematic given that the Board is entrusted with issues related to data protection and "content" is a broader ambit that other regulations such as the IT Act already deal with.

10. The "as may be prescribed" Act**:**

The phrase "as may be prescribed" appears at least 31 times in the 21-page Act leaving a lot to delegated legislation. This allows the government to notify rules later on to clarify these provisions. Such rules don't go through the same parliamentary rigour as the bill itself, because of which these rules can be overbroad and go beyond the scope of the parent legislation, as is being argued about the IT Rules of 2021, which was issued under the IT Act of 2000.

11. COMPENSATION AND PENALTY:

Breach in observing the obligation of Data Fiduciary totake reasonable security safeguards to prevent personal data breach under sub-section (5) of section 8.: Penalty May extend to two hundred and fifty crore rupees.

The DPDP Bill requires companies to take "reasonable security safeguards" to prevent personal data breaches and failure to do so can attract the highest band of penalty of up to Rs 250 crores. But there is no clarity on what measures should be taken and what constitutes as "reasonable" safeguards.

Section 44 (2) *The Information Technology Act, 2000 shall be amended in the following manner, namely:—*

(a) section 43A shall be omitted;

No compensation for victims of personal data breaches: While the Data Protection Board can impose a penalty of up to Rs 250 crores on an entity for a personal data breach, none of this goes towards the user, who is the victim of the data breach. Additionally, the Act removes section 43A of the IT Act, 2000, which

provided for such compensation.

Breach in observance of the duties under section 15. May extend to ten thousand rupees. Also the provision of INR. As penalty for providing the inaccurate information is questionable because she herself might not aware of it and the amount cause financial burden on her, all this may affect her economic and societal situation.

There is no as such provision of financial compensation to her, if her data breaches.

- Furthermore, we can have analysis on ***how the international comparison is worthwhile to noted?***

The international comparison will assist us to know the best practices that exists to protect the data as well as provide us better solution to our loopholes and sometimes address that issues that might not be presented in India and can be cause of concern in future:

A Comparative Analysis of India's DPDP Act 2023 and the EU's GDPR: Bridging Global Data Protection Standards **:**

The **Data Protection and Privacy Act of 2023 (DPDP Act)** in India and the **General Data Protection Regulation (GDPR)** in the European Union are both comprehensive data protection laws, but they differ in several areas of approach, scope, and enforcement. Below is a comparative analysis:

Scope and Application :

India’s DPDP Act 2023

The DPDP Act aims to protect Indian citizens' privacy, covering both digital and physical data (Article 2). It applies to data controllers and processors, focusing on data within India or from entities targeting Indian consumers (Article 3). While it permits cross-border data transfers, the government has flexibility to regulate such flows for public interest (Article 8).

EU’s GDPR

The GDPR applies globally to entities processing the personal data of EU citizens (Article 3). It emphasizes individual rights like the right to erasure (Article 17), data portability (Article 20), and the right to object (Article 21). The regulation restricts data transfers to countries lacking adequate protection, using mechanisms such as adequacy decisions and standard contractual clauses (Article 45, Article 46).

Key Difference - The GDPR has a broader, extraterritorial reach with stricter data transfer rules (Article 45), while India's DPDP Act focuses on domestic data protection but allows more flexibility for international data flows (Article 8).

- Comparison of Data Subject Rights: India's DPDP Act 2023 vs. EU's GDPR:

India's DPDP Act 2023

1. Right to Privacy - Recognizes privacy but allows limitations for national security and public interest (Article 2).
2. Right to Access and Correction - Individuals can access and correct their data, though this right is more limited than in the GDPR (Article 4).
3. Data Portability - Grants the right to transfer personal data between service providers (Article 7).

EU's GDPR

1. Right to be Informed - Requires clear information on data usage at the time of collection (Article 13).
2. Right to Rectification, Erasure, and Portability - Includes rights to rectify, erase (right to be forgotten), port data, and object to processing (Articles 16, 17, 20, 21).
3. Right to Restriction of Processing - Allows individuals to restrict data processing in specific cases (Article 18).

The GDPR offers broader rights, including the **right to be forgotten**, while the **DPDP Act** provides more limited privacy protections.

- Consent Management: India's DPDP Act 2023 vs. EU's GDPR :

India's DPDP Act 2023

1. Consent-based Processing - Focuses on obtaining informed consent for processing sensitive personal data (Article 6).
2. Government Override - The government can override consent for national interest or public safety (Article 7).

EU's GDPR

1. Consent Requirements - Consent must be freely given, specific, informed, and

unambiguous, with the right to withdraw at any time (Article 7).

2. Consent Records - Organizations must keep clear records of consent (Article 7).

Key Difference - The GDPR demands more explicit and revocable consent, while the DPDP Act includes exceptions that may limit consent for national security or public safety

Regulatory Authorities: India's DPDP Act 2023 vs. EU's GDPR

India's DPDP Act 2023

1. Data Protection Board of India - Resolves complaints on data breaches and privacy violations, though its powers and independence are still evolving (Article 10).
2. Government Oversight - The government retains significant control over data processing, particularly for national security and public safety (Article 11).

EU's GDPR

1. European Data Protection Board (EDPB**)** - Ensures consistent enforcement of the GDPR across member states (Article 68).
2. Data Protection Authorities (DPAs) - Independent bodies with enforcement powers, collaborating within the EDPB on cross-border issues (Article 51).

Key Difference - The DPDP Act grants greater government oversight, while the GDPR emphasizes independent, non-political regulatory bodies.

SUGGESTIONS:

- Collaborative efforts among governments, law enforcement, and cyber security experts are crucial to address these threats.
- Strengthening cyber security frameworks and promoting awareness are essential to mitigate risks and safeguard digital ecosystems.
- Strongly suggest that these data protection measures should also be inculcated as an essential part of the startups from the very beginning.
- Utilizing strong encryption algorithms is fundamental to securing digital data Conducting regular audits of digital systems and monitoring for unusual activities can

help detect potential security breaches early on.

- The event of a cyber attack or system failure, having up-to-date backups ensures that information can be restored, minimizing potential data loss.
- Employee Training and Awareness is mandatory. Compliance Verification:
  - Assess compliance with relevant data privacy regulations and internal policies.
  - Identify and address compliance gaps and potential risks.
  - Prepare necessary documentation and reporting evidence.
- Strengthen Consent Mechanisms: Create thorough policies for obtaining and managing consent, including explicit consent for sensitive data. Give clear guidelines for consent forms, making sure they are understandable, transparent, and available to everyone.
- Enhance Data Localization Requirements: To ensure better control, security and privacy of data processed within India, broaden the scope of data localization to cover a wider range of data categories. Create a phased implementation strategy to address the real-world issues that businesses face.
- Establish Robust Cross-Border Data Transfer Mechanisms: Introduce specific guidelines and protections for international data transfers, such as the use of binding corporate rules, standard contractual clauses, or other recognized techniques, to guarantee the appropriate protection of personal data.
- Develop Comprehensive Data Breach Notification Requirements: In the event of a data breach, require organizations to immediately notify the people affected and the appropriate authorities. Include specific instructions on the type, timing, and format of this notification. To effectively handle data breaches, encourage organizations to implement strong incident response plans.
- There should be the provision of compensation to the person whose data breached. Clarity in terms/definitions which is also scrutinized in prescribed manner.
- The notice to be shown to users when obtaining consent is only required to state what personal data will be collected and for what purpose, unlike previous iterations of the bill, which required companies to state how long they will store data, if they will share it with third parties, where the data was collected from, details on any cross-border transfer of the data, etc.
- That for reform in data protection board a committee of three members must constitute of 1. PM OF India
- Member of opposition

- Former CJI OF INDIA
- This will lead to transparency in appointment of board and lead to independent authority at some extent

RECOMMENDATIONS:

- It must specify the **precise mechanisms and technical specifications for seamless data portability which it doesn't do under the current Act.** The smooth transfer of data between various platforms or service providers may face practical difficulties in the absence of clear guidelines.
- To account for new forms of personal data and developing technologies, the definition of sensitive personal data must be precise and thorough. The Act should also give crystal clear instructions on what precautions and other measures must be taken when handling sensitive personal data.
- Lack of clear enforcement provisions may make it more difficult for people to assert their rights and hold data fiduciaries liable for violations. The defence of data privacy rights could be jeopardized in the absence of a robust enforcement mechanism. **So there should be a clear enforcement and implementation of provisions. As well as there should be clear procedures and processes in place for data principals to use to exercise these rights.**
- It might also be more challenging to swiftly and effectively resolve disputes involving data protection due to the limited provisions for grievance redress and alternative dispute resolution mechanisms. **So the Act should be formulated broad enough to have ADR method accessible.**

CONCLUSION:

There is a lot of potential for the Digital Personal Data Protection Bill, 2022 to address India's growing privacy and data protection concerns. The bill seeks to build a more secure and reliable digital ecosystem by including extensive provisions and giving people more control over their data. But it's important to understand that for India's digital future, striking a balance between protecting individual privacy rights and encouraging innovation is essential. To maintain this balance, the law must be continuously improved and adjusted to address new issues and technological developments. India can safeguard individual rights while promoting innovation, economic growth, and a thriving digital ecosystem by putting strong data protection

and privacy laws into place.

REFERENCES:

- Blind, K., Niebel, C., & Rammer, C. (2024). The impact of the EU General data protection regulation on product innovation. *Industry and Innovation*, *31*(3), 311-351.
- Bräutigam, T., & Miettinen, S. (2016). Data protection, privacy and European regulation in the digital age. *Unigrafia OY, Helsinki*.
- Saber, M., & Tidfors, E. (2024). Convenience Over Privacy: Balancing Privacy and Personalization Across Generations.
- Jain, A. (2022). Confidentiality and Dissemination of Private Information: An Analysis of Indian Laws Pertaining to Data Protection. *Part 1 Indian J. Integrated Rsch. L.*, *2*, 1.
- ROY, A., & SREEKUMAR, D. A. (2024). Privacy in the digital era.
- Lakra, R., & Jha, N. (2024). Publicly Available Data in the DPDPA Act 2023: Interpretative, Constitutional and Comparative Perspectives. *Constitutional and Comparative Perspectives (August 22, 2024)*.
- Data-Protection-26-Privacy-Issues-in-India
- PRIVACY%20DATAJournal-with-cover-DG-message-%20(1).pdf
- https://archive.org/details/in.gazette.central.e.2023-08-11.248045
- https://www.researchgate.net/publication/371607585
- https://cag.gov.in/uploads/icisa_virtual_publishing/Journal-with-cover-DG-message-08-10-2024-06704c77f434894-25842653.pdf
- https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
- https://www.lawyersworldwide.com/wp-content/uploads/Digital-Personal-Data-Protection-Act-2023.pdf
- https://www.freelaw.in/legalarticles/Data-Protection-Laws-in-India-Current-Scenario-and-Future-Prospects-#:~:text=Enforcement%20Issues%3A%20The%20enforcement%20of,may%20lead%20to%20enforcement%20gap
- https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/