INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

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

Dr. Namita Jain

Head & Associate Professor

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

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

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

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

Avinash Kumar

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

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

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

 ISSN: 2582-6433

CRITICAL REVIEW OF DIGITAL DATA PROTECTION ACT, 2023

AUTHORED BY - BHOOMIKA NANDA

CRITICAL REVIEW OF DIGITAL DATA PROTECTION ACT, 2023

Digital transactions have revolutionized both economic and social interactions, making processes and data more efficiently accessible. However, this shift also brings an increase in cybercrimes, such as identity theft, data breaches, and financial fraud. The growing frequency and sophistication of these cyber threats underscore the critical need for robust digital data protection measures. The need for a Digital Data Protection Act is becoming increasingly evident as digital transactions and data processing expand across all aspects of life.

Through the years we have witnessed many such incidents where the personal data stored along with the government authorities and data fiduciaries have been put at risk of leak and misuse due to the lack of security in keeping such data safe.

- Illegal surveillance through the use of Pegasus spyware against opposition leaders, journalists, the legal community, businessmen, Government officials, scientists, rights activists, and others.
- The use of facial recognition technologies by the Delhi police to investigate the North East Delhi riots, the Kisan Rally (Lal Qila Riots), and the Jahangirpuri Riots cases. This is especially concerning following the Delhi Police's revelation that it treats all results above 80% similarity as positive results.
- Wide and disproportionate data collection as well as retention of biological and personal data under the Criminal Procedure Identification Act, 2022.
- Government's attempt to collect and compile both demographic as well as biometric data of residents and link it with several databases, including the electoral roll. Such a step not only undermines informational privacy but also enables mass surveillance that breaks data silos and increases the profiling of individuals.
- Monetisation and sale of our data, accessible to the Government as well as third parties, through the Vahan database under the Ministry of Road Transport and Highway Bulk Data Sharing Policy. Given the high intensity of data collection, storage and processing envisioned by the Government, risks of data misuse and monetisation, 360 degree

 ISSN: 2582-6433

profiling and surveillance is high in the absence of a law to determine the regulatory landscape of protection of personal and non-personal data.

- Amid the COVID-19 pandemic, the government's inclination towards online self-registration for vaccination without a walk-in facility arose fears of further entrenching inequities in access to the vaccine. On an even more concerning note, several states and hospitals across the country made Aadhaar mandatory for accessing diagnostics, medicines, oxygen supplies, and even the vaccine.
- The personal data of the people shared on search engines, e-commerce websites, etc are often passed on to or forwarded to other 3rd party data fiduciaries regarding whom the data principles are not made aware of, and thus resulting in leak of personal data and traps the data principles in banking frauds, employment frauds and also in the endless loop of spam calls.

Many countries have already implemented comprehensive data protection laws to address the challenges of digital data management. Some examples of these Acts are:

- **European Union** (General Data Protection Regulation (GDPR)) effective from May 2018, is one of the most stringent data protection laws globally. It provides extensive rights to individuals and imposes strict obligations on organizations regarding data collection, processing, and storage.
- **United States** (Various Sector-Specific Laws): t has sector-specific regulations such as the Health Insurance Portability and Accountability Act (HIPAA) for health data, the Children's Online Privacy Protection Act (COPPA) for children's data, and the California Consumer Privacy Act (CCPA) for consumer data in California.
- **Canada** (Personal Information Protection and Electronic Documents Act (PIPEDA)): PIPEDA governs how private-sector organizations collect, use, and disclose personal information in the course of commercial activities.
- **Australia** (Privacy Act 1988): This Act regulates how personal information is collected, used, and disclosed by Australian government agencies and private sector organizations.
- **Brazil** (General Data Protection Law (LGPD)): Effective from August 2020, the LGPD is Brazil's data protection law, inspired by GDPR, and aims to regulate the processing of personal data.
- **China** (Personal Information Protection Law (PIPL)): Enforced from November 2021, the PIPL regulates the collection and use of personal data in China, similar to GDPR.

 ISSN: 2582-6433

INDIA

The transition from the IT Act, 2000, to the new **Digital Personal Data Protection Act, 2023** marks a significant shift in India's approach to data privacy and protection. The introduction of this Act addresses many of the limitations of previous legislation and brings India closer to the global standards set by frameworks like the GDPR.[1]

the **Justice K. S. Puttaswamy v. Union of India** case of 2017 was a landmark decision that recognized the right to privacy as a fundamental right under the Indian Constitution. This judgment highlighted the need for a robust and comprehensive data protection framework in India, setting the stage for future legislation.

Since 2018, there have been efforts made by the Indian Government to introduce and implement a central legislation. After releasing multiple drafts of the proposed data protection bill over the years, 2023 finally saw the latest iteration of the legislation, titled the 'Digital Personal Data Protection Bill, 2023' ("**DPDP Bill**"), approved by the Lok Sabha on August 3, 2023. This was followed by the Rajya Sabha passing the DPDP Bill on August 9, 2023. Finally, on August 11, 2023, the President of India granted her assent to the same, and the Digital Personal Data Protection Act, 2023 ("**DPDP Act**") was notified and published in the Official Gazette of India.

India's Digital Personal Data Protection Act, 2023 (DPDPA) is a comprehensive privacy and data protection law that recognizes the right of individuals, referred to as data principals, to protect their personal data during the processing of that data for lawful purposes. The law culminates a seven-year journey that began when the Indian Supreme Court in the landmark judgment of ***Justice K.S. Puttaswamy and Anr. v. Union of India and Ors***, declared that the right to privacy is part of the fundamental right to life in India and that the right to informational privacy is part of this right. As of now, while the **Digital Personal Data Protection Act, 2023 (DPDP)** has been passed, it has not yet come into force.

The DPDPA includes provisions regarding consent, legitimate uses, breaches, data fiduciary and processor responsibilities, and individuals' rights over their data; and provides guidelines on processing, storing and securing personal data. It applies to all types of data linked to a person, including name, addresses, ID numbers and behavioral information (A person is defined as individual, undivided family, company, firm, association, the state and every "artificial juristic person"). But it doesn't apply to data made publicly available nor does it

[1] https://www.legal500.com/developments/thought-leadership/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023/

 ISSN: 2582-6433

specify restrictions on publicly available data scraping, such as for AI model training. Information that an individual has consented to share is considered protected, but not data indexed by search engines or social media sites. The law doesn't apply to paper data unless it's digitized or data collected for personal, artistic and journalistic use.

Under the **Digital Personal Data Protection Act, 2023 (DPDP)**, the processing of personal data must adhere to specific conditions to be considered lawful. These conditions focus on ensuring that data processing is conducted transparently and respects individuals' rights. DPDP Act, brought up to protect the personal data of the people, does carry along serious concerns regarding its constitutional validity that whether it provides the government agencies and authorities with unchecked and unfettered rights to access the personal data which results in violation of privacy.

Under the provision of DPDPA personal data may be processed only for a lawful purpose after obtaining the consent of the individual. The consent must be "free, specific, informed, unconditional and unambiguous with a clear affirmative action" and for a specific purpose. The data collected has to be limited to that necessary for the specified purpose. A notice (as specified u/s 5 of the act) must be given before seeking consent. The notice should contain details about the personal data to be collected and the purpose of processing. Consent may be withdrawn at any point in time. Whereas, for 'legitimate uses' mentioned u/s 7, including: (a) voluntary acceptance; (b) the provisioning of any subsidy, benefit, service, license, certificate, or permit by any agency or department of the Indian state, if the individual has previously consented to receiving any other such service from the state; (c) sovereignty or security; (d) fulfilling a legal obligation to disclose information to the state; (e) compliance with judgments, decrees, or orders; (f) medical emergency or threat to life or epidemics or threat to public health; and (g) disaster or breakdown of public order. For individuals below 18 years of age, consent will be provided by the parent or the legal guardian.

The act mentions that the rights of the data principal and obligations of data fiduciaries will not apply in specified cases like: (i) prevention and investigation of offences, and (ii) enforcement of legal rights or claims. The central government may, by notification, exempt certain activities from the application of the Bill. These include: (i) processing by government entities in the interest of the security of the state and public order, and (ii) research, archiving, or statistical purposes.

STORT COMINGS OF THE DPDPA

 ISSN: 2582-6433

The Act in its present form *prima facie* proposes to protect *Personal Data*, but there may be concerns with the implementation of the provisions technically. Such concerns include the following

1. The Act's excessive reliance on the phrase "as may be prescribed" raises significant concerns regarding the clarity and specificity of its provisions. The legislation exhibits an overabundance of delegated legislation, as it largely eschews detailed stipulations regarding its implementation. The recurrent use of the phrase "as may be prescribed"—appearing 28 times within a 21-page Act comprising 44 sections—suggests an undue reliance on this provision as a central feature of the DPDP Act. This pervasive ambiguity appears to afford the government considerable latitude to make arbitrary decisions and subsequently issue notifications to elucidate these provisions. Such notifications, however, do not undergo the same level of parliamentary scrutiny as the original bill, potentially resulting in rules that are overly broad and exceed the scope of the primary legislation. When a substantial portion of a legislative act is conditioned on the "as may be prescribed" provision, the act's robustness is compromised. This practice effectively grants the executive branch significant discretion, which undermines the transparency of the legislative process and impairs the public's capacity to fully comprehend the law's scope and implications.
2. The DPDP Act mandates that companies implement "reasonable security safeguards" to avert personal data breaches, as specified in sub-section (5) of section 8. However, the Act falls short in clarifying the precise meaning of "reasonable security safeguards," thereby creating ambiguity that invites varied interpretations and potential misuse. The Act does not delineate the parameters of what constitutes reasonable security safeguards nor does it obligate the Government to define these parameters through accompanying Rules. This lack of explicit guidance may result in superficial compliance, allowing entities to adopt minimal safeguards that could potentially undermine the effectiveness of the security measures and facilitate evasion of liability.
3. One problematic provision grants the government the authority to, "before the expiry of five years from the date of commencement of this Act," declare that any provision of this law shall not apply to certain data fiduciaries or classes of data fiduciaries for a period specified in the notification. This provision confers significant and broad discretionary power upon the government, which is not constrained by any guidance regarding the criteria for such exemptions, the categories of data fiduciaries that may be exempted, or the duration for which these exemptions may be valid. This lack of

 ISSN: 2582-6433

specificity and oversight raises concerns about the potential for arbitrary application and inconsistent enforcement of the Act's provisions.

4. Section 17(1)(c) of the Act provides exemptions from the requirements of notice and consent for data processing undertaken for the purposes of "prevention, detection, investigation, or prosecution of any offence or contravention of any law." While such exemptions are justifiable in certain contexts, Section 17(2)(a) introduces a broader and more sweeping exemption, allowing any government agency, as notified by the government, to be entirely exempted from the application of the law in matters relating to sovereignty, security, integrity, public order, and the prevention of incitement. This provision appears redundant in light of Section 17(1)(c) and underscores a legislative intent to grant a comprehensive exemption from the data protection law to specific state agencies. The broad nature of Section 17(2)(a) effectively indicates Parliament's intent to facilitate an extensive non-application of the data protection law to designated government entities, potentially diminishing the law's overall scope and effectiveness.
5. The DPDP Act introduces amendments to the Right to Information Act, 2005 (RTI Act), stipulating that the government is not required to disclose information that pertains to personal data. Given that requests under the RTI Act frequently involve personal details, the amendment to Section 8(1)(j) of the RTI Act, as effected by Section 44(3) of the DPDP Act, disrupts the established balance between privacy and the right to information. This modification appears to expand the discretionary authority of Public Information Officers (PIOs), allowing them to reject RTI requests on the grounds that the information sought pertains to personal data. This alteration may undermine the RTI Act's effectiveness, as highlighted by MP Adhir Chowdhury in Parliament, who cautioned that such amendments could lead to a "new era of corruption," where crucial personal information, such as assets, liabilities, and educational qualifications of officials, might be shielded from public scrutiny under the RTI Act.
6. Clause 3(c)(ii) of the Bill stipulates that the data protection law does not apply to personal data that is made publicly available by the user. For instance, if an individual posts their personal data on social media while expressing their views, the processing of such data would be exempt from the law's provisions. This creates a significant loophole, allowing companies to process publicly accessible personal data without obtaining consent or adhering to other regulatory requirements outlined in the Bill. Consequently, entities such as AI services—including OpenAI's ChatGPT and Google Bard—could scrape publicly available personal data from the internet to train their

 ISSN: 2582-6433

models. Moreover, this provision potentially enables the use of publicly accessible profile photos for facial recognition technologies, raising concerns about the unchecked and potentially intrusive use of such data.

7. The notice provided to users when obtaining consent under the Act is notably inadequate in informing them about the handling of their personal data. The current requirement stipulates that the notice must only specify the personal data being collected and the purposes for which it will be used. There is no mandate for companies to disclose additional critical information, such as the duration for which the data will be stored, whether it will be shared with third parties, or details concerning any cross-border transfers of the data. This lack of comprehensive information undermines users' ability to make fully informed decisions regarding their consent and raises concerns about transparency and the protection of personal data.

Analysis:

From the references to the Act outlined above, it is evident that the legislation endows the Union government with extensive discretionary powers, potentially undermining its core objectives of data protection. The Act provides broad exemptions to government agencies under the pretext of safeguarding national interests such as sovereignty, national security, public order, and foreign relations. This sweeping latitude raises concerns about the potential for misuse and unrestrained executive authority, which could result in undue infringements on individual privacy rights.

The extensive exemptions available to government entities could facilitate the circumvention of data protection requirements, thereby eroding the fundamental intent of the legislation. The Act's provisions allowing the Union government to exempt data fiduciaries or classes of data fiduciaries from its regulations could lead to selective evasion of obligations, compromising the legislation's effectiveness.

Additionally, there are no restrictions on the government's use of data, whether digital or non-digital (once converted into digital format), or on the duration of data retention. This absence of limitations means that data principals lack a 'right to be forgotten' with respect to government-held data.

 ISSN: 2582-6433

The Central Government's authority to request "such information" from the Board, any Data Fiduciary, or intermediary "for purposes of this Act" introduces broad and vague terminology. When viewed through a legislative lens, this expansive language suggests an embedded intent for government surveillance. The government's broad powers to exempt itself, demand information from companies, and retain data indefinitely could pave the way for mass surveillance practices.

These concerns are underscored by landmark judicial rulings affirming that the right to privacy is a fundamental right under the Constitution, though not absolute. The courts have consistently recognized the right to privacy as a critical component of individual freedoms, which the Act's unregulated powers may infringe upon

- The Supreme Court in *Justice K.S. Puttaswamy v. Union of India (2017)* [W.P. (Civil) No 494 of 2012, Supreme Court of India, August 24, 2017]. It was held that the right to privacy is an intrinsic part of the right to life and personal liberty under Article 21 of the Constitution of India. The judgment especially declared that, in this new technological era, the personal data of a person, especially his biometric data, forms valuable information and can be used by another having unauthorized access; hence, protection of informational privacy needs to be guaranteed. No party, even if it is the government, can have unauthorized access to the personal data of an individual.

In a few other landmark judgments where the Hon'ble courts held that surveillance on people without any fair, just and necessary reason also results in the violation of the right to privacy of the person.

- In the matter of *PUCL vs Union of India (AIR 1997 SC 568)*, commonly known as "**Telephone Tapping Case"**, the Supreme Court upheld that the power exercised by the CBI to intercept the telephonic conversation, in the absence of fair and reasonable procedural safeguards, was violative of the right to privacy. The court held that every person has the right to freely converse over the phone without the fear of intrusion.
- The government authorities investigating a case can't reveal bank details without valid grounds, *Ram Jethmalani & Others vs Union Of India (2011) 8 SCC 1*, popularly known as the **"Black Money Case"**, here the Supreme Court held that revealing an individual's bank account details without establishing grounds to accuse them of wrongdoing violates their right to privacy.

 ISSN: 2582-6433

- The Supreme Court in the case of *Kharak Singh v. State of Uttar Pradesh (1963)* has held that a person cannot be said to live his life when someone is keeping a continuous watch on him, even though he is not physically confined.

Conclusion:

The DPDP Bill allows the government to issue a notification to exempt any of its agencies from the Bill on grounds like the security of the State, maintenance of public order, etc. The provisions mentioned above, combined with the fact that the government can retain personal data for an unlimited period regardless of whether the purpose for which it was collected has been served, means that the government has a complete freedom to carry out mass surveillance. Furthermore, there is an automatic exemption for processing personal data for the prevention, investigation, etc., of crime, without the need for the government to issue any notification. It can be concluded that the DPDP Act is a much needed initiative to secure the personal data of the people but the act lacks proper enforcement, and rather encourages low accountability and diminishes the transparency of the government authorities and data fiduciaries. The exemptions to the State may have adverse implications for privacy, as the Bill may enable unchecked data processing by the State.

References:

1. https://thewire.in/government/what-lies-beneath-the-pr-blitz-on-the-new-data-protection-act
2. https://www.barandbench.com/law-firms/view-point/digital-personal-data-protection-act-2023-a-brief-analysis
3. https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/
4. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en