INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

ISSN: 2582-6433

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

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.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

THE ROLE AND IMPACT OF DIGITAL PERSONAL DATA PROTECTION ACT (2023) ON DATA PROTECTION AND PRIVACY IN CYBER SPACE.

AUTHORED BY: SHRUTI BHATNAGAR
AMITY UNIVERSITY LUCKNOW UTTAR PRADESH

Abstract

The paper analyses the role and impact of the new digital personal data protection act (DPDP act) on data protection and privacy in cyber space. The act is one of its own kind and aims at protecting the personal data of the data principle. I will examine the DPDP act (2023), which is a significant piece of legislation ensuring the protection of digital personal data.

The first chapter contains the introduction part. The second chapter contains the need of privacy and its development over years. The third chapter contains the information about the DPDP act (2023) and its evolution over years. The fourth chapter contains the rights and obligations of the data principal and data fiduciaries. The fifth chapter contains the role and impact of DPDP act (2023) on data protection and privacy in cyber space. The sixth chapter contains the conclusion and suggestions.

Methodology

In my research on the role and impact of the DPDP Act on data protection and privacy in cyber space. I have adopted a doctrinal methodology as our foundational approach. This method involves an in-depth examination of the legal and regulatory frameworks governing the protection of digital personal data in the Indian context. We will deal with the intricacies of statutory provisions, legal statutes, and relevant case laws about digital personal data protection within the country.

Introduction

The introduction of the Digital Personal Data Protection Act of 2023 (DPDP Act) represents a transformative moment in data protection and privacy across the vast cyberspace. This landmark law redefined the digital governance landscape and provided a robust framework created to

ISSN: 2582-6433

protect individuals' data. Now that the digital world plays an important role in our daily lives and as the technology continues to evolve, the DPDP Act sets out the responsibilities and obligations of stakeholders in the cyberspace ecosystem, by addressing the critical interface between individual privacy rights and the rapid development of digital technology. The DPDP Act, that came into force on 09th August 2023, represents a comprehensive response to the growing challenges posed by the expansion of the digital footprint, where personal data is a currency of unprecedented value. The law not only reflects Indian government's commitment to strengthening its legal infrastructure, but also addresses the global need for improved data protection measures. The purpose of this introduction is to highlight the central role and far-reaching impact of the Act on the complex web of data protection and privacy in cyberspace. Since its enactment, the Act has been the subject of careful consideration, taking into consideration the need for technological innovation and the requirement to protect the rights of individual persons. This review of the role and impact of the Act examines its key provisions and considers how the Act addresses the delicate challenges of data protection in cyberspace. The law establishes the outlines of digital governance, reflects increased recognition of the need for robust data protection measures, and is the focus of an ongoing global debate about data privacy in the era of technology.

Historical background of the act

The history of privacy laws in India depicts a journey marked by evolving judicial interpretations, legislative developments, and the recognition of privacy as a fundamental right. The turning point in this trend came in 2017 with the K.S. Puttaswamy v. Union of India[1] judgement, in which the Supreme Court declared the right to privacy to be a fundamental right under Article 21 of the Constitution. This important ruling established the legal framework for India's comprehensive privacy protection.

Prior to the explicit recognition of the right to privacy, certain provisions in existing laws touched upon aspects of privacy. The Indian Penal Code of 1860 and the Information Technology Act of 2000 both included sections addressing privacy concerns in the physical and digital spheres, respectively.

However, the lack of a standalone, comprehensive law specifically dedicated to data protection and privacy led to a legislative vacuum. The need for a proper legal framework became

[1] Justice KS. Puttaswamy v. UOI, (SC 2017) 10 SCC 1 SC 4161

ISSN: 2582-6433

increasingly evident as technology advanced, and personal data became a valuable asset. Multiple attempts were made to pass a comprehensive privacy law, reflecting the challenges and complexities involved in aligning legal provisions with the dynamic nature of data privacy concerns. Finally, on 9th August 2023, India adopted the DPDP act, a comprehensive data protection and privacy law. The Act aims to create an organized and enforceable framework for personal data collection, processing, and protection, as well as to secure individuals' ownership on their personal and confidential information.

The history of privacy laws in India thus represents a progression from scattered legal provisions to the explicit recognition of privacy as a basic right, culminating in the enactment of a dedicated and comprehensive legislation—the DPDP Act. The evolution of this legislation demonstrates India's determination to adjust its legal framework to handle the complexities of privacy in the modern era of the internet.

Need of the act

In today's world, several interrelated factors have made the need for privacy paramount.

Digital Transformation: The extensive integration of technology in all aspects of human existence has led to unprecedented amounts of personal information being stored and shared online. Securing this digital trace is essential to prevent potential misuse and unauthorized access.

Cybersecurity Threats: The extent and sophistication of cyberattacks pose considerable risks to personal and sensitive information. Data security measures are critical for protecting individuals and organizations against data breaches, identity theft, and other cyber dangers.

Personal autonomy: Data protection is an essential part of maintaining personal autonomy and control over personal information. In a connected world where data is often shared across platforms, having control over one's data allows individuals to make informed decisions about their personal and professional lives.

Trust in digital transactions: As now activities, from financial transactions to medical consultations, occur online, maintaining privacy is critical in building trust among people to encourage them in doing digital interactions. Individuals are likely to engage in digital transactions if they are sure that their personal information will be treated securely.

Protection from Surveillance: The growth of surveillance technology has raised concerns about unwarranted interference with individuals' private lives. Data protection measures are required to combat excessive surveillance by governments, organizations, and malicious actors.

Legal and Ethical Considerations: Many nations recognize the right to privacy as a basic human

ISSN: 2582-6433

right. Respect for privacy is both a legal obligation, and an obligation to respect the dignity and personal space of individuals.

Preventing discrimination: In the time of big data and artificial intelligence, there is a risk that personal data can become a medium to discriminate against people based on gender, race and socio-economic status etcetera. Robust data protection measures can help reduce such risks.

Mental Health: Continuous disclosure and sharing of personal data can create psychological stress and feelings of vulnerability. Privacy provides individuals with the mental space to freely express themselves, make mistakes, and grow without fear of constant control. **Innovation and Creativity**: Privacy fosters an environment that promotes innovation and creativity. People are expected explore and experiment more when they feel their ideas and expression are protected from undue scrutiny.

In summary, the need for privacy in today's world protects individual autonomy, promotes trust in digital interactions, prevents cyber threats, maintains legal and ethical standards, and protects networking and digital essential for promoting general well-being in an increasingly socialized society.

Overview of the act[2]

The Digital Personal Data Protection Act, 2023, recently sanctioned by the President on August 11, 2023, marks a crucial development in safeguarding individuals' rights related to their personal data. The Act introduces key terms like 'Data Fiduciary' and 'Data Principal,' outlining their roles and responsibilities. Under Section 4, Data Fiduciaries can only process their personal data for lawful and legitimate purposes with explicit consent. Section 5 emphasizes notifying Data Principals before seeking consent, detailing the nature, purpose, and avenues for grievance redressal. Section 6 establishes stringent criteria for obtaining Data Principals' consent, ensuring it is free, accurate, informed and unconditional. Special provisions exist for processing a child's data, requiring parental consent and prohibiting actions detrimental to the child's well-being. Sections 8 and 10 enumerate the duties of Data Fiduciaries, emphasizing compliance, data accuracy, protective measures, and the appointment of key roles like independent Data Protection and Data Auditor Officer. Data Principals, as per Section 15, must comply with existing laws while exercising the rights, providing authentic information, and refraining from impersonation or filing frivolous complaints. The Act provides Data Principals various rights, like access to

[2] Chanlang Ki Bareh, Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) From Library Contexts, 44 Journal of Library & Information Technology 50-58 (2024).

ISSN: 2582-6433

information about their data (Section 11), the right to correction or erasure (Section 12), grievance redressal (Section 13), and the right to nominate a representative (Section 14). The creation of the Data Protection Board of India, detailed in Sections 27 and 28, equips the regulatory body with substantial powers, acting as an independent entity for complaint resolution, decision-making, and enforcement. Additionally, provisions for an Appellate Tribunal and Alternate Dispute Resolution are included. In essence, the Act establishes a robust framework ensuring responsible data processing, transparency, and redressal mechanisms, aligning with increasing data privacy requirements and tackling current digital concerns.

The role and impact of digital personal data protection act (2023) on data protection and privacy in cyber space[3]

Data fiduciary obligations: Section 4 defines the legal foundation for processing personal data, underlining that the data fiduciaries can process the personal data only in accordance with the DPDP Act's regulations and for permissible objectives. The Act defines lawful objectives as those that are not expressly prohibited by law, ensures that personal data is treated following legal requirements, and protects against unauthorised or illegal processing.

Under Section 5, data fiduciaries should provide clear and complete notice to the data principals about the usage of their personal data. These notices must include details regarding the personal data that is being processed, the intent and purpose of processing, the data principal's rights, and how to file a complaint. By providing openness and informed permission, this provision improves data principals' knowledge of how their data is handled and helps them to effectively exercise their privacy rights.

Section 6 describes the procedures to obtain consent from data principals for the processing of the personal data. Consent must be free, explicit, informed, unconditional, and unequivocal, indicating acceptance to the use of personal data for a specific purpose. Consent requests must be provided in clear and simple English, also the data principals can access them in their chosen language. Furthermore, the data principals have the right to withdraw their consent at any moment, and the process is as simple as it was to give consent.

This provision improves privacy by providing data owners to have control over their personal

[3] Digital Personal Data Protection Act (2023) available at:https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

ISSN: 2582-6433

information and also ensures that consent is obtained in an accountable and transparent way.

Section 7 describes the permissible usage of personal data by data fiduciaries. It defines particular requirements for the processing of personal data, such as gaining consent from data subjects, meeting legal responsibilities, reacting to emergencies, guaranteeing public safety, and protecting national security. This clause improves openness and accountability by establishing permissible reasons for data processing, and guaranteeing personal data is only used for lawful and specified purposes.

Section 8 puts numerous responsibilities on data fiduciaries to protect the rights of data principals. These responsibilities include hiring data processors under valid contracts, ensuring data consistency and precision, implementing safety measures to prevent breaches of data, notifying the Board and the affected data principals regarding any breaches, and removing personal data upon withdrawal of consent. By requiring these safeguards, the provision strengthens data protection processes and encourages accountability among data fiduciaries.

Section 9 specifically deals with the handling of personal data of children and people with disabilities. It requires data fiduciaries to get verified agreement from the parents or the legal guardians before processing children's data and forbids tracking, psychological monitoring, and personalized marketing to children. Furthermore, the clause allows the government to exclude some data fiduciaries from these requirements if they comply with safety criteria. This provision strengthens privacy protection for children and people with disabilities by putting vulnerable groups' well-being first.

Section 10 empowers the Central Government to identify key data fiduciaries based on criteria such as the volume and nature of personal data processed, dangers to data principals' rights, and possible effects on national security. Significant data fiduciaries must establish data protection officers, conduct frequent data assessments and audits, and take further steps to assure conformity with the DPDP Act. By subjecting key data fiduciaries to increased scrutiny and monitoring, this rule promotes data management and fosters an accountability culture in the handling of personal data.

Rights and duties of Data Principal: Section 11 grants data principals the right to request for a summary of the personal data being processed by a data fiduciary, the details of other fiduciaries and processing firms with access to the data, and any other relevant information concerning the personal data and its processing. This right promotes transparency and gives people more control over their personal data by allowing them to see how it is used and shared.

Section 12 allows data principals to correct erroneous or deceptive personal data, update

ISSN: 2582-6433

incomplete data, update out-of-date information, and request that their data be erased. By allowing persons to correct mistakes and outdated information, this right guarantees the reliability and accuracy of personal data, improving data quality and minimising the risk of erroneous judgments based on defective data.

Section 13 specifies data principals' right to easily accessible grievance redressal services supplied by the data fiduciaries or consent managers. This section enables the settlement of disputes and grievances relating to the processing of personal data, guaranteeing that individuals can take action in case of non-compliance with any of the provisions contained in the DPDP Act or any breach of their rights.

In the event of disability or death, data principals may designate another person to execute their rights. This provision ensures that personal data protection continues even in case of the data principal's incapacitation or death, so protecting their privacy interests.

Section 15 defines data principals' responsibilities, which include complying with applicable laws, providing legitimate information, and abstaining from impersonating or suppressing material information. By enforcing these obligations, the DPDP Act encourages ethical data practices and prohibits data principals from abusing or misusing personal information.

Establishment of data protection commission: The law establishes a data protection commission responsible for implementing the law. This independent body is led by a chairperson and members that are appointed by the government. It acts as a regulatory body with the power to receive and investigate complaints, issue enforceable orders and impose sanctions for violations. The provisions outlined in sections 27 to 28 of the Digital Personal Data Protection Act (DPDP Act) have a significant impact on data protection and privacy by the establishment of the Data Protection Board to improve the mechanisms for dealing with personal data breaches and complaints. Section 27 defines the Data Protection Board's powers and functions, including the ability to provide remedy for personal data violations, investigate complaints, and issue penalties for DPDP Act violations. Meanwhile, Section 28 stresses the Data Protection Board's independence and mandates that it operate as a digital office, expediting the process of accepting complaints, scheduling hearings, and issuing conclusions.

Furthermore, the DPDP Act establishes a detailed inquiry and investigation procedure, giving the Board powers similar as of a civil court, such as summoning witnesses, questioning them under oath, and granting interim orders. These provisions promote data security and privacy processes, building trust in data principals and promoting transparency among data fiduciaries.

The DPDP Act (2023) plays an important role in increasing data protection and privacy

ISSN: 2582-6433

mechanisms by establishing methods for appeals, mediation, and voluntary undertakings. Section 29 gives persons the right to appeal against orders or directives passed by the Data Protection Board to the Appellate Tribunal to guarantee that aggrieved parties have a procedure to contest decisions that may harm their privacy or data rights. The Appellate Tribunal is competent to hear appeals, alter or set aside orders, and assure quick resolution of disputes. In addition, Section 31 promotes mediation as an effective alternate for addressing complaints, giving a less aggressive approach to conflict resolution and fostering amicable solutions.

The DPDP Act (2023) plays a key role in increasing data protection and privacy mechanisms by establishing methods for appeals, mediation, and voluntary undertakings. Section 29 gives persons the right to appeal against orders or directives passed by the Data Protection Board to the Appellate Tribunal to guarantee that aggrieved parties have a procedure to contest decisions that may harm their privacy or data rights. The Appellate Tribunal is competent to hear appeals, alter or set aside orders, and assure quick resolution of disputes. In addition, Section 31 promotes mediation as an alternative method of addressing complaints, giving a less aggressive approach to conflict resolution and fostering amicable solutions.

This encourages parties to cooperate in finding ways to minimize the burden of formal judicial procedures. Furthermore, Section 32 establishes the concept of voluntary undertakings, where people or organizations can choose to commit to acts or refrain from particular behaviours relevant to data protection. The Data Protection Board's approval of voluntary undertakings serves as a preventive tool, allowing parties to resolve concerns and reduce future DPDP Act breaches. However, failure to fulfil the requirements of a voluntary undertaking may result in enforcement measures by the Board, emphasizing the necessity of data protection compliance. Overall, these measures contribute to a robust framework for defending data and privacy rights, promoting responsibility, and creating confidence in digital ecosystems.

Consent Mechanism: The law establishes a robust consent mechanism, making it a primary requirement for the lawful processing of personal data. Consent should be given freely, transparent, up-to-date, and unqualified.

The Act also introduces the concept of “Consent Managers”, registered with the Council, providing a transparent and accessible platform for data managers to manage their consent. He is the one who works on behalf of data principals to manage their consent preferences. Consent Managers are answerable to data principals and need to be recognized by the Board, guaranteeing

ISSN: 2582-6433

that data principals have reliable representatives to successfully manage their privacy preferences. Section 6 also requires data fiduciaries to establish that they got valid consent from data principals to process personal data. This requirement emphasizes the importance of complying with consent-related regulations and ensuring responsibility in the processing of data activities.

Cross-border data transfers[4]: The law addresses cross-border transfer of personal data, allowing them but empowering governments to restrict data transfers to specific countries or territories through Notification. The law also takes into account potential conflicts with industry law, and existing location regulations will take precedence if they provide better protection or restrictions. The introduction of cross-border transfer procedures, as outlined in Section 16(1) of the DPDP Act, has a significant influence on data protection and privacy standards. Under this section, the Chairperson has the power to oversee the implementation of different procedures, such as data transfer agreements and standard contractual terms, to permit authorized data transfers outside of India. This directive intends to improve personal data privacy by requiring strong safeguards, such as encrypting and security measures, during cross-border transfers. Furthermore, requiring prior consent or completing impact assessments helps to limit the privacy risks connected with such transfers by protecting personal data from illegal access or exploitation.

Extra-territorial applicability: The DPDP Act has broad extra-territorial applicability, include the processing of "digital personal data" outside India if such data relates to supply goods or services to Indian data controllers. This is in line with a global trend, similar to GDPR, of regulating the activities of entities across national borders.

Enhanced rights of data subjects: Data controllers are granted rights such as access, deletion and rectification. However, these rights are limited by certain international standards, with limited access to personal data summaries and processing activities. The right to erasure and rectification mainly applies to data processed that is processed be obtaining consent or voluntary disclosure.

Accountability and Data Security: The Act emphasizes on accountability, which requires the data fiduciaries to take appropriate technical and organizational measures for effective implementation. Emphasis is placed on data security, with trustees mandated to implement reasonable safeguards and notify the Board and affected parties in case of a data breach. **Parental consent for minors**: The law sets out specific obligations related to the processing of children's personal data. Data fiduciaries must obtain parent's consent before processing a child's data,

[4] Yogesh V Nayyar, Whitesmann's Digital Personal Data Protection Act, (1st ed. 2023).

ISSN: 2582-6433

reflecting a commitment to protecting minors' privacy online.

Exemptions for AI research and development[5]: The law includes exemptions for publicly available data and data processed for research purposes, thereby facilitating activities related to AI research and development. However, it should be clarified that the law will apply if the processing is used to make specific decisions for the data controller.

Powers and role of government: Act confers substantial powers on the Government, allowing it to make orders to block information in the public interest and to request information from Councils and authorized persons data entrustment. The government plays a regulatory role, passing delegated acts to specify the provisions of the law and control the regulation process.

Penalties for non-compliance: The Act provides for penalties for violations, ranging from fines to substantial sums. The Data Protection Board can impose sanctions based on the severity of the breach, providing a strong deterrent to non-compliance. Section 33 of the Act establishes measures for imposing monetary penalties on people or businesses found violating the Act or its regulations. This part acts as a strong deterrent to noncompliance and emphasizes the necessity of meeting data protection requirements. Monetary fines are intended to hold offenders accountable for severe breaches that risk personal data privacy and security. The amount of the penalty awarded by the Data Protection Board will be decided considering several elements specified in subsection (2) of the regulation. These elements include the kind, gravity, and severity of the breach caused, the kind and degree of sensitivity of the affected personal data, the frequency with which the breach occurred, and if the business benefited from it. In addition, the Board analyses the entity's mitigating actions to correct the breach, and the possible impact of the punishment. This strategy ensures that punishments are reasonable, and effective, and act as a deterrence against future violations. Also, Section 34 requires that all monetary fines collected by the Board be credited to the Consolidated Fund of India. This provides transparency as well as accountability in the management and utilisation of penalty proceeds, which aligns with fiscal responsibility ideals. By allocating penalty payments to the Consolidated Fund, the Act emphasizes the idea that penalties are used not merely as a punitive tool, but also to fund efforts targeted at improving data protection procedures and encouraging adherence with the DPDP Act. In summary, India's DPDP Act, 2023 has a significant impact on the management of personal data in cyberspace by establishing a strong legal framework, enhancing individual privacy and defining the obligations for entities processing personal data. It reflects a comprehensive

[5] Karishma Sundara & Nikhil Narendran, Protecting Digital Personal Data in India in 2023, 24 Computer Law Review International 9-16 (2023).

ISSN: 2582-6433

approach to data protection, aligned with global standards while addressing the unique challenges of the Indian digital landscape.

Conclusion

In conclusion, the Digital Personal Data Protection Act (DPDP) has the potential to significantly shape and influence the cybersecurity landscape in India. As evidenced by its provisions, the law addresses many different aspects of data protection, attempting to strike a balance between protecting individual rights and promoting an environment promoting innovation and trade. The Act provides a robust framework for protecting digital personal data, consistent with global standards while incorporating unique elements relevant to the Indian context. The emphasis on consent, fair use and accountability reflects a commitment to holding data stewards accountable and regulating the conduct of data fiduciaries. The recognition of the extraterritorial nature of data processing extends its jurisdiction to foreign entities that are processing personal data that belong to Indian citizens. However, concerns have arisen about some provisions that give broad powers to the central government. The potential for unchecked regulation and broad exemptions, including those for startups, pose challenges to the effectiveness of the law. Imposing rights on data controllers also creates incentives that are to be carefully considered. The inclusion of a transition period recognizes the practical challenges businesses face in complying with new regulatory requirements, demonstrating a considered approach to implementation. The Act's ultimate impact will depend on how it addresses these challenges, adapts to the emerging technology landscape, and receives stakeholder feedback. Once the DPDP Act comes into force in practice, continued collaboration with industry experts, business and civil society will be critical. This iterative process will allow the law to evolve, ensuring that it remains relevant to technological advances, meets emerging cybersecurity challenges, and effectively balances the interests of all parties. relevant in India's dynamic cyberspace.

Suggestions

Improve clarity and limit central government power: The DPDP Act should seek to clarify its provisions, reducing reliance on central government decisions. Establishing specific criteria and guidelines for regulatory development will help prevent arbitrary decisions, thereby ensuring a more transparent and accountable legal framework.

Setting clear exemption criteria: Legislation should establish clear and stringent criteria for granting exemptions to central government. This will prevent abuse of discretion and ensure that

ISSN: 2582-6433

exemptions are granted based on clearly defined parameters, thereby avoiding potential loopholes and excessive oversight measures.

Check exemptions for startups: While it is commendable to support the growth of startups, the Act should reassess the level of exemptions granted to them. Clear criteria need to be established to identify qualified startups, and a balance needs to be established between promoting innovation and ensuring data protection.

Addressing concerns about consent and fair use: The Act should consider provisions regarding presumed consent in certain circumstances (now called certain legal uses). Maintaining a balance between fair use and an individual's right to opt out is important to avoid undue invasion of privacy.

References

- Digital Personal Data Protection Act (2023) available at:https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
- Justice KS. Puttaswamy v. UOI, (SC 2017) 10 SCC 1 SC 4161
- Yogesh V Nayyar, Whitesmann's Digital Personal Data Protection Act, (1st ed. 2023).
- Chanlang Ki Bareh, Reviewing the Privacy Implications of India's Digital Personal Data Protection Act (2023) From Library Contexts, 44 Journal of Library & Information Technology 50-58 (2024).
- Karishma Sundara & Nikhil Narendran, Protecting Digital Personal Data in India in 2023, 24 Computer Law Review International 9-16 (2023).